Distributed Computing Environment for AIX, Version 2.2:

Quick Beginnings

SC23-4188-00

Distributed Computing Environment for AIX, Version 2.2:

Quick Beginnings

SC23-4188-00

Note
Before using this document, read the general information under “Appendix B. Notices” on page 141.

First Edition (February 1998)

This edition applies to Version 2.2 of the *IBM Distributed Computing Environment for AIX* and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters.

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

IBM welcomes your comments. Send your comments to the following address:

International Business Machines Corporation

Department VLXA

11400 Burnet Road

Austin, Texas

78758

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

Contents

Figures

Tables

Welcome to DCE 2.2 for AIX

This book describes the IBM Distributed Computing Environment for AIX, Version 2.2 (DCE 2.2 for AIX), and explains how to plan for, install, and configure the product.

"Part 1. Understanding DCE 2.2 for AIX" on page 1 gives an overview of DCE 2.2 for AIX.

"Part 2. Planning for and Installing DCE 2.2 for AIX" on page 23 provides planning, installing, and configuring information. Information is provided for both server and client components.

"Part 3. Configuring, Starting, and Stopping DCE 2.2 for AIX" on page 79 explains how to use DCE 2.2 for AIX.

Typographic and Keying Conventions

This guide uses the following typographic conventions:

Bold **Bold** words or characters represent system elements that you must use literally, such as commands, options, and pathnames.

Italic *Italic* words or characters represent variable values that you must supply. *Italic* type is also used to introduce a new DCE term.

Constant width
Examples and information that the system displays appear in `constant width` typeface.

[ ] 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.

This guide uses the following keying conventions:

dcelocal

The OSF value *dcelocal* in this document equates to the AIX value **/opt/dcelocal**.

dceshare

The OSF value *dceshare* in this document equates to the AIX value **/opt/dcelocal**.

<Ctrl- *x***>** **or** ^ *x*

The notation **<Ctrl-** *x***>** or ^ *x* followed by the name of a key indicates a control character sequence. For example, **<Ctrl-C>** means that you hold down the control key while pressing **<C>**.

<Return>

The notation **<Return>** refers to the key on your terminal or workstation that is labeled with the word Return or Enter, or with a left arrow.

Part 1. Understanding DCE 2.2 for AIX

Chapter 1. Overview of DCE 2.2 for AIX

IBM Distributed Computing Environment for AIX, Version 2.2 (DCE 2.2 for AIX) is a member of the IBM Server Series family of products. The DCE 2.2 for AIX is based on OSF Distributed Computing Environment (DCE) technology (Release 1.2.2).

What Is DCE?

DCE provides a standard environment that supports distributed applications. It represents technologies selected by the OSF and has emerged as the leading industry standard for distributed services.

An application written to use DCE runs in any environment that supports the OSF DCE standard. DCE makes it possible for application developers to give users secure access to the wide range of information and services available within their network and also hides the complexity of the network environment.

Distributed computing services, as implemented in DCE, provide an important enabling software technology for the development of distributed applications. DCE makes the underlying network architecture transparent to application developers. It consists of a software layer between the operating system and network interface and the distributed application program. DCE provides a variety of common services needed for development of distributed applications, such as name and time services, and a standard remote procedure call (RPC) interface. DCE provides a means for application developers to design, develop, and deploy distributed applications.

A group of DCE machines that work together and are administered as a unit is called a *cell*. For example, imagine an organization comprised of several departments, each in a different building and operating on its own budget. Each department in such an organization could have its own DCE cell.

A DCE environment is a group of one or more DCE cells that can communicate with each other. A cell becomes a part of a DCE environment when it obtains access to one or more global directory services in which the other cells in the environment are registered.

If two cells for two different departments are a part of a DCE environment, then a user in one department's cell can access resources in another

department's cell although this access is typically less frequent and more restricted than access to resources within the user's own cell.

A DCE cell can be configured in many ways, depending on its users' requirements. A cell consists of a network connecting two kinds of nodes:

- **DCE user (client) machines** are general-purpose DCE machines. They contain software that enables them to act as clients to all of the DCE services.
- **DCE server machines** are equipped with special software enabling them to provide one or more of the DCE services. Every cell must have at least one of each of the following servers in order to function:
  - Cell Directory Server
  - Security Server

Other DCE servers can be present in a given DCE cell to provide additional functionality, such as a Global Directory Agent to enable the cell's directory server to communicate with other cells' directory servers and Distributed File Servers to provide an enterprise-wide distributed file system.

DCE 2.2 for AIX is a layer between the AIX operating system, network services, and a distributed application; it provides the services that allow a distributed application to interact with a collection of possibly heterogeneous computers, operating systems, and networks as if they were a single system; and includes a set of standard services, software interfaces, and tools that support the creation, use, and maintenance of distributed applications in a diverse computing environment.

DCE 2.2 for AIX has the same organization as OSF DCE. Part 1 of this book introduces the concept of a DCE cell and gives a brief summary of the way in which different machines participating in a Distributed Computing Environment are organized.

DCE 2.2 for AIX is based on the OSF DCE Release 1.2.2 code base and designed for the supported versions of the AIX operating system. See the *IBM DCE for AIX, Version 2.2: Release Notes* for a listing of the supported versions of the AIX operating system.

Product Contents

DCE 2.2 is available in the following Licensed Program Products:

- **DCE for AIX, Version 2.2** (DCE 2.2 for AIX) which includes the following:
  - **DCE Base Services for AIX, Version 2.2**
  - **DCE Security Services for AIX, Version 2.2**

  - **DCE Cell Directory Services for AIX, Version 2.2**
- **DCE Base Services for AIX, Version 2.2** (DCE 2.2 Base Services)
- **DCE Enhanced Distributed File System for AIX, Version 2.2**, (DCE 2.2 Enhanced DFS)
- **DCE NFS to DFS Authentication Gateway for AIX, Version 2.2** (DCE 2.2 NFS to DFS Gateway)
- **DCE User Data Masking Encryption Facility for AIX, Version 2.2** (DCE 2.2 User Data Masking Facility)
- **DCE Data Encryption Standard Library for AIX, Version 2.2** (DCE 2.2 DES Library)
- **DFS Starter Kit for AIX, Version 2.2** (DFS 2.2 Starter Kit)
  - **DCE for AIX, Version 2.2**
    - **DCE Base Services for AIX, Version 2.2**
    - **DCE Security Services for AIX, Version 2.2**
    - **DCE Cell Directory Services for AIX, Version 2.2**
  - **DCE Enhanced Distributed File System for AIX, Version 2.2**

DCE 2.2 Licensed Program Products

DCE 2.2 for AIX

DCE 2.2 for AIX is composed of the following components:

- **DCE Base Services for AIX** provides support for remote procedure calls, the client functionality for cell directory service and security, time, messaging and serviceability, and basic distributed file system services. This package also provides support for integrating DCE security services with AIX base operating system security. Because the DCE architecture is built on a threads-based model, a reentrant (threadsafe) version of the AIX C library, **libc_r.a**, is required for the DCE Base. The **libc_r.a** library is included with the AIX operating system. DCE administration tools are included for such functions as configuring a cell, adding and deleting users in a cell, and adding servers and clients to a cell.
  - **Client Services**
    - The **Remote Procedure Call (RPC)** facility enables you to create and run client and server applications. The RPC runtime service implements the network protocols by which the client and server sides of an application communicate.
    - **DCE Threads Compatibility Library for AIX** provides a programming model for building concurrent applications that perform many operations simultaneously. It provides support for multithreaded

applications (based on POSIX 1003.4a Draft 4) that use the DCE threading model. DCE Threads Compatibility Library for AIX is packaged with AIX.

- **Multithreaded Programming Environment** support allows multiple threads to call standard C library functions without interfering with one another.
- **Distributed Time Service (DTS)** provides synchronized time in the distributed network environment on the computers participating in a Distributed Computing Environment. DTS synchronizes a DCE host's time with Coordinated Universal Time (UTC), an international time standard.
- The **CDS client** provides the interface, **cdsclerk**, between CDS client applications and CDS servers.
- The **Security client** provides the following services:
  - **AIX Security Integration** coordinates the AIX base operating system security services with the DCE Security services. This allows a user to login to AIX and obtain DCE credentials at the same time. For more information about AIX Security Integration, see the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components.*
  - **GSSAPI Extensions** — GSSAPI extensions are a set of APIs that provide non-RPC applications the ability to use the DCE security authentication protocol. The GSSAPI can be used to establish credentials or extract Extended Privilege Attribute Certificates (EPAC) for a non-RPC application.
  - **Extended Registry Attributes**(ERA) — This expands the static registry attributes of Principal, Group, and Account to a dynamic set of registry attributes that can be customized to a cell.
  - The **Audit Service**: performs the logging of audit records based on specified criteria. The Audit Service has three basic components:
    - **Application Programming Interfaces** provide the functions that are used to detect and record critical events when the server services a client. They also are used to create tools that examine and analyze the audit event records.
    - **Audit Daemon** maintains the filters and the audit logs.
    - **Audit Management Interfaces** are used by the Administrator to specify how the Audit Daemon will filter the recording of Audit Events. This interface is available from the DCE Control Program (**dcecp**).
  - **Password Strength Server** (**pwd_strengthd**) allows you to control the following characteristics of user passwords:
    - Minimum password length
    - Whether a password can be all spaces

  - Whether a password can consist of alphanumeric characters only
  - Whether a user can use a user-created password or must use a system-generated password.

  You can extend these password strength policies in your cell by creating a password management server to perform customized password checking and generation. See the example in **/usr/lpp/dce/examples/pwdstren**. For additional information see the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components* for more information about the Password Strength Server and the *IBM DCE for AIX, Version 2.2: Application Development Guide—Core Components* for information on the Password Management API.

- The **Distributed File System client** provided with AIX DCE has been integrated with the AIX Virtual Memory Manager (VMM). This allows DFS to support the use of the mapped file functions **shmat()** and **mmap()** against files in the DCE DFS filespace. The Distributed File System allows users to access and share files stored on a File Server anywhere on the network without having to know the physical location of the file. Files are part of a single namespace. Therefore, no matter where in the network a user is, the file can be found using the same name.

– **DCE Web Administration Utilities** are made up of DCE Web Administration and DFS Web Secure. The DCE Administration interface allows you to administer DCE users, groups, organizations, and ACLs and DFS filesets, aggregates, and fileset servers from any client that has a web browser. The Web Utilities must be installed and configured on a workstation that has a Netscape Enterprise or a FastTrack 2.01 web server and a DCE client and optionally a DFS client configured within the cell. The advantage of this is that you can administer the DCE cell using a web browser from a machine that is not configured into the cell. The DFS Web Secure product provides DCE credentials to CGI programs and provides authenticated access to documents stored in DFS through web browsers.

– **System Management Interface Tool (SMIT)** for DCE:

  You can perform DCE system management tasks using SMIT or DCE commands. The DCE Compatibility fileset, **dce.compat**, must be installed before you can access the SMIT menus for DCE. SMIT uses interactive menus to guide users through many system management tasks.

  To access the SMIT menus for DCE, select **Communications Applications and Services** from the main SMIT menu. Then, select **DCE (Distributed Computing Environment)** from the Communications Applications and Services submenu.

– The **DFS Servers for AIX** package (**dce.dfs_server.rte**) supports exporting AIX JFS and AIX CD-ROM File Systems into the DFS file

space. The Distributed File System server supports file system sizes greater than 2GB. This allows aggregates, and filesets to be larger than 2GB. File sizes greater than 2GB are now supported on AIX 4.2.1.

– The **Online Documentation for DCE 2.2 for AIX** was enhanced to provide the following:
  - An online IBM documentation set in HTML format
  - An IBM documentation set in PostScript format
  - An IBM documentation set in ASCII format.

  For more information on these enhancements, refer to “Chapter 6. Obtaining Additional Information” on page 133.

– **DCE System Management** provides 2 management tools, DCE Event Management Services and the DCE SNMP SubAgent.
  - **Simple Network Management Protocol (SNMP)** provides network management support in the TCP/IP environment for monitoring DCE resources and services. System administrators and system management application programmers can use SNMP to easily monitor the DCE environment so that they can focus on making their resources and services more manageable. For more information about SNMP, see the *IBM DCE for AIX, Version 2.2: Application Development Guide—Introduction and Style Guide*
  - **Event Management Service (EMS)** provides asynchronous event support for DCE based applications. DCE EMS manages event services in a DCE cell. EMS consists of two parts — the **emsd** (EMS daemon) server and APIs to access event services through an interface to the suppliers, consumers, and event service administration for use by EMS clients. For more information about EMS, see the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components*

– **DCE for Application Developers (dcetools)** includes tools for DCE administrative and application development support. The development tool consists of a language (and its compiler) that supports the development of distributed applications following the client/server model. It automatically generates code that transforms procedure calls into network messages.

– The **DCE XDS/XOM for AIX**: provides application programming interfaces to the CDS namespace. A library of functions is available with which to access the Directory Services.

• **DCE Security Services for AIX** enables secure communications and controlled access to resources. It provides a set of the following security-related functions:

  – **Authentication Service** — enables two processes on different machines to be certain of each other’s identity.

- **Secure Communication** in which communication is protected by the integration of DCE RPC with the Security Service.
- **Authorization** in which access to resources is controlled by comparing the credentials conferred to a user by the Privilege Service with the rights to the resource, which are specified in the resource's Access Control List.
- **Privilege Server** — once identity has been established, the following checks are made: Is the user authorized to access a resource? What permissions are required, and does the user have those permissions? Authentication and authorization are generally invoked for the user through use of Authenticated RPC.
- **Access Control List Facility** — ACLs are lists of users who are authorized to access a given resource. An ACL API allows programmers to manipulate ACLs, and the dcecp **acl** commands or the **acl_edit** command allow users to modify ACLs associated with resources that they own, to whom (user or group) access is granted and what specific permissions are given.
- **Login Facility** — initializes a user's DCE security environment by authenticating the user to the Security Service by means of the user's password, then by returning security credentials that will authenticate the user to the required distributed services.
- **Security Replication** — enables the Master Registry Database to be replicated to one or more Slave Registry Databases. The dcecp **registry** commands or the **sec_admin** command are the interface used to view and manipulate the state of both Master and Slave replicas.

- The **Cell Directory Service for AIX** is a central repository for information about resources in the distributed system. Typical resources are users, machines, and RPC-based services. The information consists of the name of the resource and its associated attributes. Typical attributes include a user's home directory or the location of an RPC-based server.

  The Directory Service consists of the Cell Directory Service (CDS) and the Global Directory Agent (GDA). The Cell Directory Service manages a database of information about the resources in a group of machines called a DCE cell and provides location-independent naming for servers. The GDA enables intercell communications by locating cells which have been registered in the global naming environment.

  GDA Integration with LDAP is an extension to GDA that allows the resolution of non-DNS style foreign cell names. X.500 directories and any directories that support the LDAP protocol can be used to establish intercell communication. For more information about LDAP, see the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components.*
- **DCE Messages for AIX** provides messages for the DCE components.

DCE Enhanced Distributed File System for AIX

DCE Enhanced Distributed File System for AIX extends the services of the basic distributed file system with the DCE Local File System (DCE LFS), which supports extended functionality for administering the DFS filespace data. DCE EDFS includes a physical file system, the DCE Local File System (LFS), which supports special features that are useful in a distributed environment. DCE LFS gives you the ability to perform the following tasks:

- Replicate data
- Log file system data, enabling quick recovery after a crash
- Simplify administration by dividing the file system into easily managed units called filesets.
- Associate ACLs with files and directories.

In addition, DFS supports aggregates, filesets, and files with sizes greater than 2GB.

DCE NFS to DFS Authenticating Gateway for AIX

The **DCE NFS to DFS Authenticating Gateway for AIX** provides a bridge between NFS clients and DFS. NFS client users can gain authenticated access to the DFS filespace and DFS servers. This feature also provides a migration utility from NFS to DFS. In the AIX 4.1.3 release, the PC-NFS Authentication Service (**pcnfsd**) is now integrated with the NFS to DFS Authenticating Gateway to allow automatic DCE authentication from a PC-NFS client. The IBM NFS to DFS Gateway supports the DFS *@sys* and *@host* variables. See the *IBM DCE for AIX, Version 2.2: NFS/DFS Authenticating Gateway* for more information.

DCE User Data Masking Encryption Facility

DCE User Data Masking Encryption Facility enables RPC application data encryption using the User Data Masking Encryption Facility algorithm developed by IBM and can be exported outside of the United States. If you have installed either the **dce.priv.rte** feature or the **dce.cdmf.rte** feature, you are provided with a programming interface that allows you to encrypt RPC application data using the User Data Masking Encryption Facility algorithm. Export controls on User Data Masking Encryption Facility are less restrictive than those for DES, making User Data Masking Encryption Facility a viable alternative for customers unable to obtain a DES export license. See the RPC section of the *IBM DCE for AIX, Version 2.2: Application Development Reference* for usage information.

Data Encryption Standard

Data Encryption Standard (the **dce.priv.rte** feature) provides a programming interface that enables remote procedure call (RPC) application data

encryption. The **dce.priv.rte** feature utilizes the Data Encryption Standard (DES) algorithms that are part of the DCE Base Services for AIX.

IBM Enhancements to DCE

The following components contained in the previously listed DCE 2.2 Licensed Program Products are IBM enhancements and extensions to the AIX implementation of DCE:

- **Added Services:**
  - **System Management Interface Tool (SMIT) Functions**
  - **User Data Masking Encryption Facility**
  - **DCE Web Administration Utilities**
  - **Simple Network Management Protocol (SNMP)**
  - **Event Management Service (EMS)**
  - **AIX Security Integration**
  - **GDA Integration with LDAP**
- **Additional Commands**:
  - Configuration Commands:

    Notes:

    1. Use the new command format, however, the old command format is still supported.
    2. These commands are not compatable with the dcecp **host configure** and **host unconfigure** commands.

    chpesite
    Updates the **pe_site** file, which contains the addresses of the security servers that you use.

    clean_up.dce
    Cleans up recreatable database files, cache files, and credential files. This command is intended to be used if problems are encountered when trying to start DCE.

    config.dce
    Configures and starts DCE components. This command provides for a split configuration of clients. Administrative configuration and local configuration can be performed separately. See "Further Cell Configuration" on page 101 for more information.

    config.dfs
    Configures and starts DFS components. See "Further Cell Configuration" on page 101 for more information.

    migrate.dce
    Migrates DCE configuration data from previous releases for use

with the current release. There is no need to reconfigure when installing a new release of DCE. See “Migrating an AIX DCE Cell to DCE 2.2 for AIX” on page 74 for more information.

migrate.dfs
Migrates DFS configuration data from previous releases for use with the current release. There is no need to reconfigure when installing a new release of DFS.

mkbutc.dfs
Sets up the BackUp Tape Controller.

mkdceweb
Configures DCE Administration, DFS Web Secure, or both into a Netscape FastTrack 2.01 or Enterprise 2.01 web server. Configuring DCE Administration also configures DFS Web Secure into the web server.

mkfilesys.dfs
Registers and exports JFS, DCE LFS, and CD-ROM file systems on a DFS File Server machine.

mkreg.dce
Adds information about a DCE cell into the DOMAIN namespace.

rmbutc.dfs
Removes the setup of a BackUp Tape Controller.

rmdceweb
Unconfigures DCE Administration, DFS Web Secure, or both, from a Netscape FastTrack 2.01 or Enterprise 2.01 web server. Unconfiguring DFS Web Secure also unconfigures DCE Administration, if it was configured.

rmfilesys.dfs
Detaches and unregisters JFS, DCE LFS, and CD-ROM file systems on a DFS File Server machine.

rmreg.dce
Removes information about a DCE cell from the DOMAIN namespace.

show.cfg
Displays the local host’s DCE or DFS configuration or both configurations. The **dce** and **dfs** options allow display of only DCE or DFS information

start.dce
Starts the configured DCE components. This command makes sure that all components are started in the correct order.

start.dfs
Starts the configured DFS components. This command makes sure that all components are started in the correct order.

startnfs.dfs
Starts the DCE NFS to DFS Authenticating Gateway for AIX, ensures that the daemons are running, and loads the kernel extension.

stop.dce
Stops the configured DCE components. This command makes sure that all components are stopped in the correct order.

stop.dfs
Stops the configured DFS components. This command makes sure that all components are stopped in the correct order.

unconfig.dce
Removes configuration of DCE components. This command provides for a split unconfiguration, with which administrative unconfiguration and local unconfiguration can be performed separately. See “Further Cell Configuration” on page 101 for more information.

unconfig.dfs
Removes configuration of DFS components. This command provides for a split unconfiguration, with which administrative unconfiguration and local unconfiguration can be performed separately. See “Further Cell Configuration” on page 101 for more information.

– Cell Directory Service (CDS) Commands:

catraverse
Traverses the clerk cache.

cds_dbdump
Dumps CDS server database.

cdsd_diag
Starts the CDS Diagnostic utility for the server running on the local system.

cdsdel
Deletes recursively the namespace of a cell.

cdsli Lists recursively the namespace of a cell.

– RPC Commands:

rpcprotseqs
Determines the supported protocol on a given host.

rpcresolve
Recursively resolves the elements of a namespace entry.

– Security Commands:

rmxcred
Purge expired tickets from the credentials directory.

Standards Conformance

- **Standards Conformance Highlights** DCE 2.2 for AIX supports the standards listed below, but cannot claim conformance to these standards because some of them are not in final form or because conformance tests do not exist.

  Threads
  POSIX 1003.4a, draft 4

  RPC AES/DCE

  Authentication
  Kerberos Version 5, draft 4

  Authorization
  POSIX 1003.6, draft 12 (acls)

  Directory
  AES/Distributed Computing - Directory Services
  X/OPEN-X.400 API Association XDS API Draft 6

  Transport Glue
  RFC 1006, TPO-to-TCP

  Time RFC 1129, NTP

  DCE LFS
  POSIX 1003.1, file system specific chapters

Compatability with AIX

This section describes the compatability of DCE for AIX with the supported versions of AIX for the RISC System/6000.

- The **man** command is *not* supported to display current DCE reference documentation. However, **dceman**, which displays a single manual page for DCE commands and subroutines, is supplied and emulates the AIX **man** command. When the documentation package is installed, **dceman** is linked to the **/usr/bin** directory, along with **asciiview**, and **start_dcedoc**. The **dceman** command uses the same syntax as the **man** command; so, instead of typing **man** *dce_command*, users would type **dceman** *dce_command*, using any command or subroutine documented in the *IBM DCE for AIX, Version*

2.2: Administration Guide—Core Components, *IBM DCE for AIX, Version 2.2: Application Development Reference* or the *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference*.

- AIX Network Computing System (NCS) version 1.5.1 and the DCE Base Services for AIX can coexist on the same system because the DCE **dced** process provides the functionality that NCS applications expect from the **llbd** command.
- The AIX base operating security services have been integrated with the **DCE Security Services**. This integration is designed to present the typical end-user with a single-system image rather than separate images of a local UNIX system and a remote DCE system. There are some limitations to the integration, explained fully in the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components* ; however, most users will be able to acquire DCE credentials through AIX commands (like **login** and **su**), will be able to change their DCE passwords through the AIX **passwd** command, and will be able to retrieve UNIX-type information from the DCE registry through the standard AIX **libc.a** routines, **getpwnam()**, **getpwuid()**, **getgrnam()**, and **getgrgid()**. The more general routines, **getpwent()** and **getgrent()**, are not DCE-aware at this time.
- **Important Note on Changing Passwords**: AIX Password operations are directed toward the registry defined by the **registry** user attribute or, in the absence of a **registry** attribute definition, to the registry defined by the **AUTHSTATE** environment variable.

  Password operations are not directed to both local and DCE registries.

  Changing passwords for a DCE-only user is done through **dcecp**, but changing passwords (both DCE and local) for a synchronized user (a user defined both locally and in DCE) may be done with the AIX passwd command in a 2-step procedure:

  ```
  $ AUTHSTATE=DCE passwd
  $ AUTHSTATE=compat passwd
  ```

  Passwords must be kept synchronized for synchronized users, or else either DCE or local authentication will fail. Also, if a user exists locally on more than one machine, the local password must be synchronized on all machines.

  The nonintegrated DCE security commands like **dce_login** (for logging onto DCE) and **dcecp** for DCE password-changing and registry queries are still available. Of course, local access is prerequisite to using these commands.

  The local administrator must set up the system to enable DCE for AIX security integration; complete configuration instructions can be found in the *IBM DCE for AIX, Version 2.2: Administration Guide*.

- **DCE ACLs**: differ from AIX ACLs. DCE has its own commands, **acl_edit** and **dcecp**, to manipulate DCE ACLs on objects in the DCE namespace. The AIX commands (**acledit**, **aclget**, and **aclput**) do not work on objects in the DCE namespace, including files and directories in the DCE DFS filespace. AIX commands that back up and restore data do not maintain DCE ACLs on DCE LFS directories and files. Use the DCE DFS backup facility to back up and restore DCE LFS filesets.
- **DCE Distributed File System**:

  AIX 4.1 supports file system sizes greater than 2GB. This allows DFS to support aggregates and filesets of greater than 2GB. File sizes greater than 2GB are now supported on AIX 4.2.1.

  The following flags are not supported for the **open()** function call when the file resides in a DFS or DCE LFS file system:

  – **O_NSHARE**
  – **O_RSHARE**
  – **O_DEFER**.

  If these flags are specified in the **open()** call, they are ignored, and no error code is returned to the application.

  DFS does not support enforcement mode record locking. Using enforcement mode locking with DFS may lead to unpredictable results.

  It is possible to mount DCE LFS filesets locally using the AIX **mount** command. However, this practice is not recommended and should be used only in emergency situations by the DCE DFS system administrator.

  A DFS client disk cache is restricted to the AIX JFS file system. It is further restricted to a file system which is not using compression or fragmentation. The DFS **dfsd** command enforces this. Any attempts to use a non-AIX JFS file system result in **dfsd** failing with the following message:

  ```
  dfsd: cachedir filesystems must be JFS
  ```

  Any attempts to use a JFS file system with compression on results in **dfsd** failing with the following message:

  ```
  dfsd: cachedir filesystems can not use compression
  ```

  Distributing DFS binaries with the DCE DFS Binary Distribution machine (**upclient** and **upserver** processes) does not maintain the AIX install and update LPP history for those binaries.

  The AIX commands that manipulate JFS file systems, for example, **chfs**, **crfs**, **lsfs**, **rmfs**, and **mkfs,** do not work with DCE LFS aggregates and filesets. The **fsck** command should never be used against DCE LFS

aggregates. DCE LFS provides an equivalent command called **salvage**. DCE 2.2 for AIX has implemented **newaggr** and the new command **mkfilesys.dfs** to simplify creating and exporting DCE LFS aggregates and filesets. See the *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference* for more information about DCE LFS aggregates and filesets.

The AIX **mksysb** utility is not aware of the DCE LFS filesystem and does not preserve DCE LFS aggregates. The AIX logical volume information itself is backed up but upon restore, the DCE LFS aggregaates will not be usable. You will have to recreate the aggregates before you restore any fileset data.

If you are using **mksysb** to backup an AIX system that is configured as a DFS file server you may want to perform these additional steps to ensure you have a complete backup of your DCE LFS aggregates.

1. Stop DCE/DFS.
2. If the **/var/dce** (**/opt/dcelocal**) directory is on a separate filesystem that is not part of **rootvg**, thus not included in the **mksysb** backup, tar up the following list of files/dirs, this preserves all your DCE configuration information:

   ```
   /...
   /.:
   /:
   /etc/dce
   /etc/services
   /krb5
   /var/dce
   ```

   Note: You should exclude the DFS cache directory when backing up the above directories.
3. Dump all your AIX logical volumes that contain DCE LFS aggregates to tape using the **dd** command or an appropriate AIX logical volume command.

In the event that you need to reinstall a machine from the mksysb image:

1. Reboot and reinstall the machine.
2. If the **/var/dce** directory is a separate JFS filesystem that is not part of **rootvg**, untar the saved files from 2.
3. Create new logical volumes identical to the old ones for the DCE LFS aggregates and restore the saved logical volumes to the new ones using the **dd** command or an appropriate AIX logical volume command.
4. Make sure that the aggregates are still in the **/var/dce/dfs/dfstab** file and that mount points exist under **/var/dce/dfs/aggrs** for each of the DFS aggregates. When you restart DFS the aggregates will get exported to DFS.

Note: If you are reinstalling the same machine using an AIX **mksysb** backup tape and the DCE LFS aggregates are in an AIX volume group other than **rootvg** and you preserved all **non-rootvg** volume groups, you should be able to **varyonvg** the appropriate volume groups and not have to restore the individual logical volumes that contain the aggregates.

On a machine running DCE DFS, a user can belong to at most 31 groups on the local system in order to access DFS files as an authenticated user. For users that belong to more than 31 groups, **dce_login** does not set up authentication information with DFS. (The result is that all DFS requests occur as unauthenticated requests.)

- **Using AIX Journaled File Systems with DFS**: AIX Journaled File Systems (JFS) can be exported to the DCE DFS filespace. In the DFS documentation and the **fts** command output, this is referred to as a non-LFS partition or a non-LFS aggregate. The entire JFS file system is registered in the Fileset Location Database machine as one DFS fileset. Additional DFS filesets cannot be created within that JFS file system. In the DFS documentation, this is referred to as a non-LFS fileset.

  A JFS file system has to be locally mounted on the DFS file server machine before it is exported to the DFS filespace. The aggregate name used for the JFS file system has to be its local mount point, for example:

  ```
  /home
  ```

  DCE has implemented a new command, **mkfilesys.dfs**, to simplify exporting JFS file systems. See the **mkfilesys.dfs** command in the *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference* for more information about exporting JFS file systems (non-LFS partitions) to the DCE DFS file space.

  There are some limitations when using JFS file systems with DFS. The fileset management functions of creating backup filesets, moving filesets, and fileset replication are not supported for JFS filesets. JFS ACLs are not compatible with DCE ACLs. Only UNIX mode bits can be used to protect JFS files that have been exported to the DCE DFS file space. Foreign cell requests are always mapped to the anonymous user when accessing JFS directories and files in the DCE DFS file space.

- **Using AIX CD-ROM File Systems with DFS**: AIX CD-ROM File Systems can be exported to the DCE DFS filespace. In the DFS documentation and the **fts** command output, this is referred to as a non-LFS partition or a non-LFS aggregate.

  A CD-ROM file system has to be locally mounted on the DFS file server machine before it is exported to the DFS filespace. The aggregate name used for the CD-ROM file system has to be its local mount point, for example:

/cdrom

DCE for AIX has implemented a new command, **mkfilesys.dfs**, to simplify exporting CD-ROM file systems. See the **mkfilesys.dfs** command in the *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference* for more information about exporting CD-ROM file systems to the DCE DFS file space.

The same restrictions that apply to JFS file systems when they are exported by DFS also apply to CD-ROM file systems. Advanced data management functions such as cloning, replication, and fileset moves are not supported. ACLs are not supported. Additionally, fileset dump and restore are not supported. The DFS Backup System does not support backup or restore of CD-ROM file systems.

- **DFS and NFS**: AIX NFS and AIX DFS can coexist on the same machines and can export the same local AIX Journaled File Systems or CD-ROM File Systems.

  A DFS client machine can also run on an NFS server that exports the DFS global file space (**/...**). DFS must be started before running the **exportfs** command to export the global file space. System V locking is not supported from NFS clients against the DFS filespace being exported by an NFS server. An error code of ENOLCK is returned to the caller (NFS client).

  If you are not running the DCE NFS to DFS Authenticating Gateway for AIX, an access request from an NFS client is treated as an unauthenticated request. If you are running the DCE NFS to DFS Authenticating Gateway for AIX on the machine, however, an access request by an NFS client user who has established authentication mappings is treated as an authenticated request. See the *IBM DCE for AIX, Version 2.2: NFS/DFS Authenticating Gateway* for more information.
- **Debugging Multi-Threaded Applications**: The AIX **dbx** debugging comand has the capability to recognize and debug multiple threads. For more information on the debugger, see the *IBM DCE for AIX, Version 2.2: Application Development Guide—Core Components* .
- **C++ and DCE Compatibility**: The following discusses C++ and DCE compatibility.
  - **Compiling and Linking**: Using **C++** with DCE requires a few considerations, but generally nothing beyond what is required in using a C based library with C++. The primary factor is using the correct version of **xlC**. DCE requires at least **xlC** version 3.1.3 in order to link with the DCE libraries.

    When dce is installed, it will create a link **xlC_r4** to **xlC**. This should be used when compiling and linking DCE applications. This name determines the stanza in the **/etc/xlC.cfg** file that is used to control the

compiler configuration. Using the wrong version or the wrong linked name of the compiler can lead to problems at compile, link, and runtime.

- **DCE Exceptions**: DCE exceptions are separate from the exceptions provided by the C++ language specification. The primary limitation, in using DCE exceptions within C++ programs is that, when a DCE exception is raised, destructors will not be called as the stack is unwound. The programmer must make sure that the objects are freed explicitly when DCE exceptions are handled. This may eliminate the use of automatically allocated objects within segments of the application code.
- **C/C++ Interaction**: Again, as with any C functions called from C++, be sure to include DCE header files in external C declarations. This makes sure that the C++ linkage looks for the non-mangled C names, not C++ names.

  In C, memory is typically allocated using malloc. In C++, memory is allocated using new *object_type*. DCE adds **rpc_ss_allocate** for volatile data that needs to be freed by the system after an rpc returns. Care needs to be taken to make sure that memory allocated by one method is always freed using the corresponding routine.

  As with any C library used in C++, it can be difficult to maintain a *pure* object-oriented architecture. In many cases, the components in DCE are fairly object-oriented in design, but since most of the pieces of DCE are designed to work together, they often pass data structures between mostly unrelated functions. For example, a login handle is an opaque data type that has a core of several closely related functions to manage and maintain the login context. While this lends itself well to grouping the data and functions as an object, the handle will need to be passed either implicitly or explicitly to most other objects that might be created. Since it is bad form to expose a data value inside an object, a sophisticated design needs to be considered (possibly a handle or surrogate object).

Unsupported OSF DCE Features

The differences are grouped into sections by type. Each section is further subdivided into functional categories, which correspond with specific DCE services (such as Configuration, Security, and Cell Directory Services).

Unsupported Services:

- Security:
  - Transitive Trust in a cell hierarchy is not supported in this release.
  - The Public Key Certificate Management API is not supported in this release.

  - The Private Key Storage server is not supported in this release.
- Directory:
  - Hierarchical Cells are not supported in this release.
  - Global Directory Services (GDS) are not provided in this release. However, GDS can exist in the same cell and be used for intercell communications, if it is provided by another product.
- Distributed File System:
  - Distributed File Access Management (DFAM) is not supported.

Unsupported Commands:

- Configuration:

  The **dce_config** script has been replaced by other configuration commands and a SMIT interface. See the *IBM DCE for AIX, Version 2.2: Administration Commands Reference* for more information.
- Security:

  The **sec_salvage_db**, **rlogin**, **rlogind**, **rsh**, and **rshd** commands supplied by OSF are not supported in this release.
- Distributed Time Service:

  The **dtss-graph** command, which converts synch trace to PostScript, is not supported.

Unsupported Subroutines : The DFS APIs are not supported.

Limitations of Supported Services

There are several limitations for accounts configured to use Public Key authentication. These include:

- Public Key accounts cannot use the Password Strength Server.
- Public Key authentication will not work on a system configured to run as a Slim client.
- The key management API is for use only by applications using the shared-secret key authentication protocol. Applications using public key accounts must use the user-to-user protocol.
- When using GSSAPI, the DCE administrator must set up an account in the DCE registry database for the initiator and the acceptor. The following restrictions apply to the account for the acceptor:
  - The account for the acceptor must be set up to use a key in a keytab file as the account's password.
  - The account for the acceptor cannot be set up to use the user-to-user protocol.

– The account for the acceptor cannot be set up to use the public key authentication protocol.

No restrictions apply to the account for the initiator.

Part 2. Planning for and Installing DCE 2.2 for AIX

Chapter 2. Planning

System Requirements

All contents in the DCE 2.2 for AIX product requires the retail release of IBM AIX Version 4.1.5. or 4.2.1. See the *IBM DCE for AIX, Version 2.2: Release Notes* for a complete listing of supported versions of AIX.

Disk Space Requirements

See the **README** file for the most currently available lpp space requirements. Note that the sizes listed are approximations. You may be able to receive more accurate numbers from your IBM marketing representative.

The following Licensed Program Products (LPPs) require the following amounts of disk space.

Table 1. LPP disk requirements

LPP	Components	Installable Packages	Space in Mb
DCE for AIX, Version 2.2	**Base Services**	**dce.client**	**26.5**
		dce.compat	**1.5**
		dce.dfs_server	**7.5**
		dce.msg.en_US	**1.5**
		dce.pthreads	**0.5**
		dce.sysmgmt	**2.0**
		dce.tools	**5.0**
		dce.web	**19.0**
		dce.xdsxom	**1.0**
		dce.doc dce.doc.rte.ascii dce.doc.en_US.ascii dce.doc.en_US.html dce.doc.en_US.ps	**138.0** 0.10 13.0 21.0 104.0
	Security Services	**dce.security**	**5.0**
	Cell Directory Services	**dce.cds**	**2.0**

Table 1. LPP disk requirements (continued)

LPP	Components	Installable Packages	Space in Mb
DCE Base Services for AIX, Version 2.2		**dce.client**	**26.5**
		dce.compat	**1.5**
		dce.dfs_server	**7.5**
		dce.msg.en_US	**1.5**
		dce.pthreads	**0.5**
		dce.sysmgmt	**2.0**
		dce.tools	**5.0**
		dce.web	**19.0**
		dce.xdsxom	**0.9**
		dce.doc dce.doc.rte.ascii dce.doc.en_US.ascii dce.doc.en_US.html dce.doc.en_US.ps	**138.0** 0.10 13.0 21.0 104.0
DCE Enhanced Distributed File System for AIX, Version 2.2		**dce.edfs**	**6.0**
DCE NFS to DFS Authenticating Gateway for AIX, Version 2.2		**dce.dfsnfs**	**0.5**
DCE User Data Masking Encryption Facility for AIX, Version 2.2		**dce.cdmf**	**5.5**
DCE Data Encryption Standard Library		**dce.priv**	**5.5**
DFS Starter Kit for AIX, Version 2.2	**Base Services**	**dce.client**	**26.5**
		dce.compat	**1.5**
		dce.dfs_server	**7.5**
		dce.msg.en_US	**1.5**
		dce.pthreads	**0.5**
		dce.sysmgmt	**2.0**
		dce.tools	**5.0**

Table 1. LPP disk requirements (continued)

LPP	Components	Installable Packages	Space in Mb
		dce.web	**19.0**
		dce.xdsxom	**1.0**
		dce.doc dce.doc.rte.ascii dce.doc.en_US.ascii dce.doc.en_US.html dce.doc.en_US.ps	**138.0** 0.10 13.0 21.0 104.0
	Security Services	**dce.security**	**5.0**
	Cell Directory Services	**dce.cds**	**2.0**
	DCE Enhanced Distributed File System for AIX, Version 2.2	**dce.edfs**	**6.0**

Global and Cell Considerations

The purpose of this section is to assist you in planning for the installation and configuration of DCE. DCE provides System Management Interface Tool (SMIT) and configuration utilities to assist you. “Chapter 3. Installing DCE 2.2 for AIX Servers and Clients” on page 63 and “Configuring DCE and DFS” on page 81 describe the configuration process, including installing executable files, setting up a DCE cell, and configuring servers and clients.

This section discusses the following topics:

- “Planning Questions to Consider”
- “Establishing a Cell Name” on page 30
- “The Cell Namespace” on page 34
- “Planning for Access Control” on page 38
- “The Cell Filespace” on page 40.

Planning Questions to Consider

You need to consider a number of questions when planning for a distributed system.

Keep in mind the following global considerations as you plan for DCE:

- How much do you think your environment will grow in the next few years? Do you anticipate rapid or relatively slow expansion of your network?

  If you think your environment will grow rapidly, consider setting up several cells representing smaller units of your organization. You can manage these smaller units as your network expands. As explained previously, members of each cell share a common purpose, and the cell is a unit of administration and security. If you anticipate slow expansion of your network, you may be able to establish one or more cells based on the organization that exists now. Consider how many administrators you will need to maintain your DCE cell, based on anticipated future growth.
- How much information does your environment have that needs to be distributed? How much do the users in your network share information?

  If there is a large volume of information that needs to be shared within your network, consider the amount of disk space you require and the number of DFS File Server machines you need.
- How much information updating do you require? Do the users in your network mainly look up information, or do they create and change information at their workstations?

  If information changes frequently and users in your network depend on the accuracy of that information, you need to consider how much you rely on replication. It is better to go to a central source of information for data that changes frequently. If users look up information, but do not need to change the information that is shared with other users, you can rely more on replicated data.
- Is the most important data the most available? Have you made plans to replicate this data?

  CDS, the Security Service, and DFS maintain master copies of their respective databases. Each CDS directory can be replicated separately. In addition to DFS databases, individual DFS filesets or groups of filesets can be replicated. The Security Service supports replication of the entire registry database. Because other components depend on the information managed by the Security Service and parts of the CDS namespace, that data needs to be available at all times. For example, the special character string **/.:** (the cell root) is stored in CDS and must always be available.

  Keep in mind that while replicating data helps availability, there is a cost in terms of performance and the amount of administration required.
- If your network has a gateway, are servers located on the same side of the gateway as the clients that rely on those servers?

  CDS servers broadcast messages at regular intervals to advertise their existence to CDS clients in the network. Clients learn about servers by listening for these advertisements. Placing servers and the clients that rely on them on the same side of the gateway facilitates efficient updates of

information and a quick response to client requests. Additional administration is required if you rely on servers that are not available through the advertisement protocol, which is effective only in a local area network.

On a LAN that has no CDS servers, proxy advertisers will broadcast the addresses of CDS servers. This means that clients do not need to know the address of a CDS server at the time of configuration. The proxy advertiser will broadcast the address of the CDS server that it was configured with. Additional CDS server addresses can be added using the **cdscp define server** command.

Consider how fast and how expensive links are if you are administering a cell that includes users in different geographic locations. You may want to keep more information locally to reduce your dependence on transmitting information across links.

- Is communication limited to your own cell, or do you need to communicate with other cells?

  For your cell to communicate with other cells, you must:

  – Establish a unique Domain Naming Service global name for your cell
  – Define your cell in DNS
  – Have at least one GDA in your cell.

  Note: Global Directory Service (GDS) is not provided with this release of DCE 2.2 for AIX. However, this release can use GDS if it is provided by another product to locate other cells.

  You can set up a special account in your cell's Security registry for a foreign cell, indicating that your cell trusts the Authentication Service of the other cell, and a special account in the foreign cell's Security registry to represent your cell. (For information about setting up these special accounts, see the *IBM DCE for AIX, Version 2.2: Administration Guide*.) Even if you do not need to communicate with other cells now, consider whether you will need to communicate with other cells in the future. Be sure to establish a cell name with these future requirements in mind.

Your answers to these questions determine the basic requirements of your user environment. Use these requirements to help you decide on the optimum use of the DCE functions described in this and the following sections.

If you are using DCE 2.2 for AIX, note the following:

- **Resolving Differences between DCE and AIX Standard Accounts**:

  It is strongly recommended that any users and groups defined in the individual system **/etc/passwd** and **/etc/group** files be synchronized with users and groups in the DCE registry. Synchronization can be facilitated with the **passwd_export** and **passwd_import** utilities after initial cell

configuration. Any users who are not synchronized between the cell registry and the local files may not realize full benefit of the integration feature. On the other hand, this flexible integration scheme supports wandering users (users who are defined in the DCE registry, but not a local system). If a machine is configured to allow it, those wandering users may log onto the system and obtain DCE credentials and local access based on UNIX-relevant information in the registry.

When DCE creates the Security registry database, DCE includes some standard UNIX principals, groups, and accounts. These do not match those that are included on a typical AIX system. This mismatch can lead to problems if you plan to use the **passwd_export** command to keep **/etc/passwd** and **/etc/group** synchronized with the DCE registry.

If you will include only AIX machines in your cell, you can delete the standard principals, groups, and accounts from the registry and add those that match AIX principals, groups, and accounts.

If your cell will include more types of machines than AIX machines, you can either convert the standard accounts as described in the preceding paragraph or keep the accounts that DCE creates. Then, you can use the **/opt/dcelocal/etc/passwd_override** and **/opt/dcelocal/etc/group_override** files on individual machines to set up standard accounts and groups that match those expected by that machine's operating system. For more information about the override files, see the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components*

If you plan to convert standard UNIX accounts in the registry as described here, you should do so immediately after initial cell configuration to reduce the likelihood of producing orphans (objects owned by UUIDs that have been deleted).

- **DCE Application Core Files**: Because DCE applications are multithreaded, their core files become large. Each thread has its own stack and other associated information that are saved in the core file. If you want usable core files from your DCE application while you are developing and testing the applications, make sure you have permission to write large core files. You can use the **ulimit** command to temporarily change the maximum core file size for the current shell process, or you can use the **chuser** command to permanently change the maximum core file size for a particular user.
- **AIX System Dump Device Size**: To ensure that you can obtain complete system dumps on systems running DFS, create a separate AIX system dump device. The size you need will vary depending on the system memory configuration.

Establishing a Cell Name

Before you can configure your DCE cell, you need to establish a cell name. This section describes DCE naming syntax, naming conventions, and the procedure for obtaining a cell name.

Global Names

All DCE objects, including applications, machines, and users, have a global name. A global name is meaningful and usable from anywhere in the DCE environment. In DCE, global names begin with the special character string **/...**, which indicates the global root directory.

DNS Global Names: DCE also supports global directory operations through the use of DNS. Following is an example of a global name that uses the DNS format:

/.../seattle.xyz.com/sec/principal/smith

In DNS format, **/.../seattle.xyz.com** is the cell name, followed by the local cell portion of the name.

Cell-Relative Names

In the two previous examples, **sec/principal/smith** is that part of the global name that resides in the local cell. The **sec/principal/smith** part of the global name can be used to construct a cell-relative name. Cell-relative names, also known as local names, are meaningful only from within the cell where the name entry exists. Cell-relative names begin with the special character string /.:, which replaces the global part of the name (the cell name). If you are in the **seattle.xyz.com** cell, the following cell-relative name translates to the same global name shown in the previous examples:

/.:/sec/principal/smith

When you are entering a CDS name from the cell where that object is registered, you can use the cell-relative name. However, if you are entering a CDS name from another cell, you must use the global name, beginning with the character string **/...** (the global root).

CDS and DNS naming conventions are described in more detail in the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components*.

Choosing a DCE Cell Name

Choosing an appropriate DCE cell name is important for the following reasons:

- DCE cells that will ever participate in the global namespace must have unique names to differentiate them from cells in other organizations.
- A uniquely identified cell name is critical to the operation of DCE security; this name is the basis for authentication in your cell.

- DNS expects global cell names to have a certain format. Choose a name that conforms to DNS naming conventions.
- DCE does not currently support cells registered simultaneously in GDS and DNS.

Note that cell names are case insensitive; that is, the name **MyCell** is equivalent to the name **MYCELL**. (When comparing cell names, DCE routines change the names to all lowercase before making the comparison.)

Cell names must not contain an at sign (@). Two cells on the same LAN cannot have the same name. Cell names must also be restricted to characters in the DCE Portable Character Set.

DCE Cell Name Conventions for DNS: If you plan to use DNS as your global directory service either immediately or in the future, your DCE cell name must follow the ARPA Internet Domain System conventions for site names. If you are already an Internet site, you can create one or more cells subordinate to your Internet domain name, depending on how your site is organized.

The following conventions govern an Internet-style name:

- The name needs to have at least two levels (for example, **xyz.com** or **sctech.edu**). The names in the first two levels are registered with the Network Information Center (NIC), the naming authority for DNS names. Registration request information is detailed in "Obtaining a Unique DNS Cell Name" on page 33.
- Although there is no restriction on the length of a name, a short name is more convenient to type.
- The name can contain any number of fields in addition to the two required levels, conventionally separated by periods.
- The name needs to end in a suffix that indicates a kind of institution. This last field is the most significant one, in contrast to a GDS name, which begins with the most significant field. The standard suffixes are:
  - **.com** for businesses and other commercial organizations
  - **.org** for noncommercial organizations
  - **.edu** for educational institutions
  - **.gov** for government institutions
  - **.mil** for military institutions
  - **.net** for network support organizations
  - *.xx* for two-letter country codes (such as **.de** for Germany and **.fr** for France) that conform to the International Organization for Standardization (ISO).

See the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components* for further information about naming rules, including valid characters, restrictions, metacharacters, and maximum name sizes for CDS and DNS names.

Obtaining a DCE Cell Name

If you plan to create a private cell and do not ever intend for it to communicate with cells outside your organization, you are not required to obtain a globally unique cell name. However, in order for your cell to communicate with other cells outside your organization, you need to have a GDA running and, before you configure your cell, you need to obtain a globally unique cell name from the GDS or DNS global naming authorities. The name can be one that already exists and is in use, or you can specify that you need a new name. This registration must be completed before you begin to configure the cell namespace. It is recommended that you obtain a unique global name for your cell even if you do not initially use a global directory service to communicate with other cells so that you can do so in the future.

Obtaining a Unique DNS Cell Name: To obtain a unique DNS name, contact the administrator in charge of the subtree under which you want to name your cell. When you get a locally approved name, send a registration request to the Network Information Center (NIC) at the following Internet address, telephone number, FAX number, or mailing address:

HOSTMASTER@INTERNIC.NET

(703) 742-4777 between the hours of 7:00 a.m. and 7:00 p.m. Eastern Standard Time

FAX (703) 742-4811

Network Solutions, Inc., An SAIC Company

Attention: InterNIC Registration Services

505 Huntmar Park Drive

Herndon, VA 22070

Defining a Cell in DNS

After you obtain a unique name for a cell, configure the cell, and initialize the cell namespace, the next step in establishing intercell directory service is to create an entry for the cell in the global namespace. You can use the **cdscp** subcommand **show cell** to obtain data that you need to create or modify a cell entry in DNS. The data you obtain from the command is what CDS uses to contact servers in foreign cells. Use the **mkreg.dce** command to set up intercell. For information on setting up the intercell environment, managing intercell naming, and administering a multicell environment, see the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components* .

The Cell Namespace

An integral part of planning for a DCE cell is understanding the organization of your cell namespace. Consider the following as you plan the organization of a cell in your network:

- Are security requirements maintained?
- Does the organization of the cell facilitate network traffic where data sharing needs are the greatest?
- How will you manage the administrative accounts created for each DCE service during the configuration process?

Determining Cell Boundaries

In DCE, the boundaries of a cell are equivalent to the boundaries of the cell namespace. A small organization can consist of one cell. A large organization can have many cells. The primary factors in determining a cell's boundaries are the common purpose and trust shared by the cell's principals. Principals within a cell can belong to groups that share the same privileges. Members of a group share the same level of trust and are authorized to perform certain actions.

Because there is a set of administrative tasks associated with setting up and maintaining each cell, it is reasonable to keep the number of cells in your organization to a minimum. However, the level of trust shared by groups of principals is a more important consideration than administrative overhead.

Keeping Cells Stable

Once you decide how many cells you need and where the boundaries of those cells will be, make an effort to keep your cell structure stable. Servers are not easily moved from one cell to another; so, be sure to plan your namespace structure carefully in order to minimize reconfiguration. If you do need to move a host from one cell to another, you must:

- Move server processes from the host.
- Unconfigure the host from the old cell, using the **unconfig.dfs** and **unconfig.dce** commands.
- Use the **config.dce** and **config.dfs** commands to reconfigure the host in the new cell.

Types of Cell Namespace Entries

This section describes the different types of entries that comprise the cell namespace. These entries are created when you follow the default configuration path described in Configuring DCE and DFS. The cell namespace can be divided into the following parts:

- The CDS part of the namespace
- The Security part of the namespace
- The DFS part of the namespace (the filespace)
- The **dced** (per host) part of the namespace

Each DCE service maintains its own namespace within the DCE cell namespace. DFS maintains its own namespace to ensure consistency among many files. The Security Service maintains its own namespace to ensure that the DCE cell remains secure. Clients of these two services query CDS for binding information that enables them to find Security or DFS servers. The points where the binding information is stored serve as mount points in the CDS namespace for the namespaces that DFS and the Security Service manage. This transition point between two namespaces is called a junction. The **/.:/sec** directory is the junction from the CDS part to the Security part of the cell namespace, and the **/.:/fs** directory is the junction from the CDS part to the DFS part of the cell namespace.

The junction **/.:/hosts/***hostname***/config** is the junction from CDS to the **dced** (per host) part of the namespace.

Figure 1 shows the top level of the cell namespace. In some cases, the names in the cell namespace are fixed (or well known) and cannot be changed. In other cases, you can choose a different name from the one listed. In Figure 1, **/.:** and **cell-profile** are well-known names.

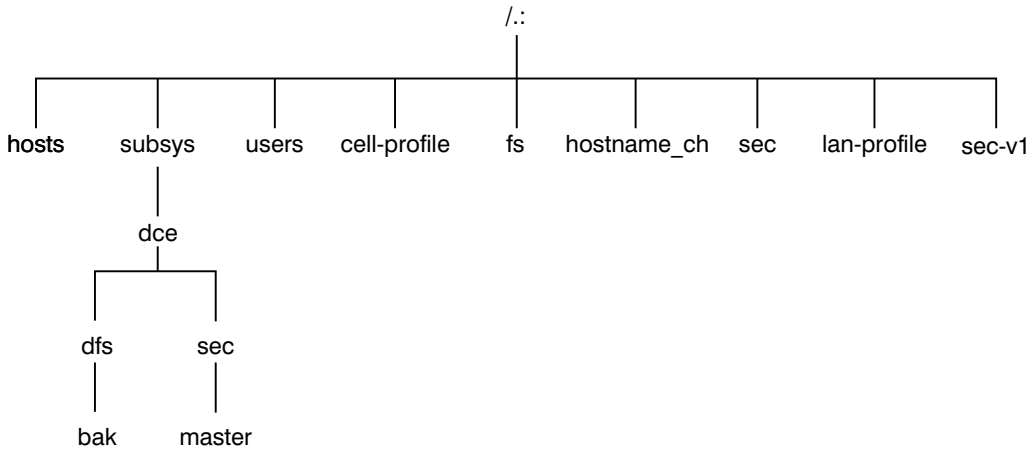

Figure 1. Top Level of the Cell Namespace

You can use the **cdsbrowser**, **dcecp**, **rpccp**, **cdscp**, or **cdsli** commands to view the CDS namespace, including the **sec** and **fs** junctions. You can use

commands such as **ls** to see the contents of the DFS part of the cell namespace and **dcecp** to see the contents of the Security portion of the CDS namespace.

CDS Namespace Entries: The DCE Cell Directory Service is a distributed, replicated database service that is used to store names and attributes of resources located in a DCE cell. This database consists of a hierarchical set of names called the namespace. Each CDS server maintains a portion of the namespace in a local database called a *clearinghouse* , which is optimized for local access. A clearinghouse is designed for relatively few **write** operations (such as creating or deleting directories and objects or exporting binding information), but many **read** operations (such as importing binding information). Note that a clearinghouse is automatically created during the configuration process for a CDS server. See "Configuring the Initial CDS Server" on page 90 for more information.

The CDS database is distributed and replicated among multiple CDS servers and multiple clearinghouses that must be kept consistent. Therefore, a large number of **write** operations can cause stress-induced CDS failures. Another cause of stress is using a large number of replicated CDS directories because updates must be propagated to all the read-only replicas. Use the **cdscp show server** command to display the number of **read** and **write** operations handled by a server since the service was started. This command allows you to monitor the level of activity and adjust the configuration if necessary.

As a directory service, CDS is designed to manage information that does not change often. For example, binding information stored in CDS does not include endpoints since endpoints change frequently. As you design applications, avoid the need to store highly dynamic data in the CDS namespace.

The CDS namespace contains entries for servers, hosts, CDS clearinghouses (collections of directory replicas stored at a particular server), RPC profiles, RPC groups, and subsystems. The entries have a CDS type of *directory* or *object*, indicating the kind of CDS object to which the name refers. A CDS directory is a container in which objects are stored. CDS uses directories to organize groups of object entries.

Profiles catalogued in the CDS namespace specify a search path through the Directory Service. The cell profile (**/.:/cell-profile**) stores the location of the servers that are available in the cell, regardless of physical location. In a geographically dispersed cell, servers can be located in different cities or even different countries. The LAN profile defines alternate servers that can be used in situations where geographic proximity is important. For example, **/.:/lan-profile** is the default LAN profile used by DTS. This profile contains entries for the DTS server local set. If a cell spans more than one LAN, another layer can be created below **/.:/lan-profile** to specify the location of the

profile for each part of the cell. For example, in a cell that encompasses two LANs, you can direct hosts on one LAN to **lanA-profile** and hosts on the other LAN to **lanB-profile**. For information on setting up multiple LAN profiles, see Configuring DCE and DFS.

Security Namespace Entries: The types of security entries are as follows:

principal
This type of entry contains an individual principal.

principal directory
This type of entry contains individual principals or one or more principal directories, or both.

group This type of entry contains an individual group.

group directory
This type of entry contains individual groups or one or more group directories, or both.

org This type of entry contains an individual organization.

org directory
This type of entry contains individual organizations or one or more organization directories, or both.

policy This type of entry contains a Security policy.

When you (or an application) are accessing an entry in the Security part of the namespace, the name of the entry alone provides enough information for the Security Service to work with. For example, the Security server knows that the login name is a principal name, registered in the Security part of the namespace; **/.:/***principal_name*, **/.../***cell_name/principal_name*, and *principal_name* are all valid ways of representing the name you use to log in.

When you use the **dcecp** command, you specify the type of object you will operate on. For example, to change account information associated with the principal **smith**, you specify that you want to operate on an account. You then enter the principal name **smith**. The **dcecp** command deals with the following types of objects related to Security:

- Principals
- Groups
- Organizations
- Accounts
- Xattrschemas

The *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components* explains how to use the **dcecp** command to display information related to principals, groups, organizations, accounts, and xattrschemas.

The **dcecp** also supports operations performed by **acl_edit**. The acl object of **dcecp** is used for this purpose. The **dcecp** command requires the object's fully qualified path name when modifying acls, as shown in the following example:

```
/.:/sec/principal/smith
```

and not simply the following:

```
smith
```

The following parts of the namespace comprise the security namespace:

/.:/sec/principal
/.:/sec/group
/.:/sec/org
/.:/sec/policy
/.:/sec/xattrschema

CDS Namespace Replication Considerations

Directory replication is the most reliable way to back up the information in your CDS namespace. Because the CDS data is replicated by directory, when you replicate a directory, all of the entries in it are automatically replicated. Use the **dcecp** control program to create replicas of directories at a CDS clearinghouse. Clearinghouses need to be created in the root directory (**/.:**) of the cell namespace.

Follow these guidelines for replicating parts of the cell namespace:

- The root directory (**/.:**) is automatically replicated (without child directories) when you create a clearinghouse.
- You should have at least two replicas of each CDS directory to ensure the entire namespace is available at all times. For further information about backing up CDS information, see the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components*.

Planning for Access Control

In planning for access control, it is important to keep the level of access control in your cell restrictive enough to ensure that security is maintained. A special set of individuals or a special group can be given permission to create accounts and groups in the root directory of the Security namespace. The **acct-admin** group is created when you configure DCE. **acct-admin** is the only group that can create accounts and groups in the root directory of the Security space.

While maintaining an adequate level of security in your cell, you also need to consider the requirements of administrators who are maintaining DCE services when you set access control levels. For example, if one person is responsible for administration of DFS in your cell, that person may need to add servers to the Security and CDS namespaces. On the other hand, an administrator responsible for the Security Service manages the Security server, but does not control the DFS filespace.

Following are some of the groups created when you configure DCE using SMIT or the **config.dce** command:

sec-admin
This group administers Security servers, cell registry functions, and other Security functions.

audit-admin
This group administers Audit servers and related audit functions.

cds-admin
This group administers CDS servers, CDS replication, and other CDS functions.

dced-admin
This group administers DCE host servers and ACLs.

dts-admin
This group administers DTS servers and related DTS functions.

dfs-admin
This group administers DFS File Servers and related DFS functions.

In addition to the administrative groups, individual users need permission to control some information kept in the registry database. For example, a user needs to be able to change its password, home directory, or login shell.

DCE Naming Considerations for Internationalization

Standard (OSF) DCE, restricts entries in the Security namespace, such as principal names, to the characters in the DCE Portable Character Set. See the Architectural Overview of DCE in the *IBM DCE for AIX, Version 2.2: Introduction to DCE* for the definition of the DCE Portable Character Set. IBM DCE provides an override capability which enables the use of non-portable characters.

This capability should be used only in environments that are homogeneous with respect to code set and only in environments in which all DCE installations support this extension. Security namespace entries that use non-portable characters are guaranteed to work correctly only when the code set of the entire enterprise is the same as that of the process under which the

names were created. To enable the use of non-portable Security names, the environment variable DCE_USE_NONPORTABLE_NAMES must be set to 1 before DCE is started, in all client and server processes in which DCE Security will run.

Certain other names, such as CDS directory names, can also be composed of characters from outside of the DCE Portable Character Set. Because DCE does not perform code set conversion on names, non-portable characters should be used only in environments which are, and will remain, homogeneous with respect to the code set. In environments which are not homogeneous with respect to code set, all DCE names must be restricted to the DCE Portable Code Set.

Subject to the previously mentioned restrictions and to the additional naming rules documented in the *IBM DCE for AIX, Version 2.2: Introduction to DCE* and the *IBM DCE for AIX, Version 2.2: Application Development Guide—Core Components*, the following names can contain characters outside of the Portable Character Set:

- CDS Object
- CDS Directory
- CDS Attribute
- CDS Link
- RPC idl_byte data
- RPC full name
- Principal
- Group
- Organization
- ERA
- DFS Filename

The Cell Filespace

This section contains guidelines for planning your cell's filespace.

The filespace begins under the cell root at the **/.:/fs** junction to DFS from the CDS namespace. The notation **/:** is set up by default to be equivalent to **/.:/fs**. Thus, the notation **/:/usr/***user_name* is equivalent to **/.:/fs/usr/***user_name*.

Some parts of DFS run in the host machine's kernel. This kernel function must be present on your machine before you run DFS. On AIX, this function is implemented as AIX kernel extensions that are loaded when you configure DFS on the machine.

DFS Administrative Domains

A DFS administrative domain is a collection of machines in the same cell configured for administration as a single unit. In a single cell, you can have one or many administrative domains, depending on the size of your organization. Organizing DFS server machines into different administrative domains simplifies the management of the cell filespace by creating smaller units for administration. All machines within an administrative domain must be in the same cell.

DFS Administrative Lists

DFS administrative lists are files that define the principals and groups that can perform actions affecting specific server processes on a server machine. There is one DFS administrative list for each DFS server process running on a machine. For example, a server's **admin.bos** file defines who has administrative rights to the BOS Server (**bosserver**), and thus determines who can manipulate and maintain server processes on that one server. Groups, as well as individual users, can be placed on an administrative list. Each server machine stores administrative lists for its processes on its local disk. A process automatically creates its initial administrative list when it is started if the list does not already exist on the local disk of the machine.

Determining the Roles of DFS Machines

Use the following recommendations when you assign roles to the DFS machines in your cell. The first DFS machine that you configure during DCE installation and configuration (described in Configuring DCE and DFS) needs to function as a System Control Machine. The System Control Machine is the server that distributes DFS administrative lists. Next, you configure a Fileset Location Database server, the server that maintains the fileset location database. Then, you configure a DFS File Server machine. Usually, the first DFS File Server is the machine on which you plan to put the root fileset (**root.dfs**). After configuring the DFS File Server, you should create the **root.dfs** fileset. Then, configure the machine as a DFS client. "Setting Up Filesets" on page 42 contains further information about **root.dfs**.

Machines that you configure as DFS servers run the processes required to be File Servers. Be sure the machine you choose has enough space to store DCE LFS filesets. The amount of free space you need depends on how much data you plan to store in DCE LFS filesets. Filesets on File Servers can store DFS client binaries in addition to user files. These filesets can also be distributed on other File Server machines in your cell. In addition, if your domain has only one server machine, this machine must run all processes and fill all required machine roles. For example, in addition to being a System Control Machine, this machine must be a File Server and a Fileset Location Database

server. If your domain has three or more DFS server machines, three machines need to store DFS databases. An odd number of DFS Fileset Location Database machines is recommended.

Setting Up the DFS File Tree

Follow recommended conventions when you set up your DFS file tree. Below **/.:/fs** are directories that help organize your DFS environment, such as:

- The **common** directory contains programs and files needed by users working on machines of all system types, such as text editors or online documentation files. The **common/etc** directory is a logical place to keep the central update sources for files used on all DFS client machines.
- The **public** directory contains files that users want to make available to everyone, including foreign and unauthenticated users.
- The **sys_type** directory contains binaries for each system type you use as a file server or client machine. If you plan to use the **@sys** variable in path names, you need to use standard names to represent system types.
- The **usr** directory contains the home directory of each DFS user in a cell and any foreign users granted a local account. Users and system administrators can protect this directory so that only locally authorized users can access it. If your cell is quite large, you can divide user home directories in multiple directory listings to facilitate quicker directory lookups.
- The **src** directory contains source filesets such as those for DFS source files.

Setting Up Filesets

Consider the following recommendations and restrictions when you set up filesets:

- Fileset names must be limited to 102 characters or less and are restricted to the DCE portable character set.
- Every cell must include **root.dfs**. The root fileset can be a DCE LFS fileset or it can be a non-LFS fileset (a non-DCE-LFS file system). See “Exporting Data” on page 116 for information on creating **root.dfs**.
- You should use a common prefix when naming related filesets. This aids in manipulating and grouping related filesets. It also relates the fileset’s name to its mount point.
- You can group filesets on the same partition of a File Server machine. This can localize the effects of an outage, but you also need to consider factors such as number of File Server machines and load balancing before grouping filesets.
- You can replicate filesets for load balancing and to make fileset contents more available. Replication is appropriate for filesets that are read much

more often than they are written, such as filesets containing installed executable files. Replication is not supported for non-LFS filesets.

- Consider the disk space a fileset requires before setting up filesets.

Using @sys and @host Variables

Follow the suggested conventions when using the **@sys** and **@host** variables in certain pathnames. When the Cache Manager encounters one of these variables, it substitutes a string consisting of the local machine's architecture and operating system type for **@sys** or the hostname for **@host**, causing a certain directory to be used. Using **@sys** and **@host** is helpful when you are constructing symbolic links from the local disk to DFS. You can create identical symbolic links on all machines, but each machine transparently accesses the files appropriate to its system name or hostname. The **cm sysname** command sets and displays the current value for **@sys**.

Client and Server Considerations

This section describes configurations for DCE client machines, the different types of DCE server machines and DCE Application Development Environment machines. A DCE Client machine can run client code of every DCE service. DCE server machines are configured to run a certain set of software. This software is made up of at least one daemon and, in some cases, one or more additional programs that comprise the server side of a DCE component. DCE server machines also run the software that makes up the DCE Client configuration.

The following topics are provided:

- "Determining Requirements for DCE Client Machines"
- "Determining Requirements for DCE Server Machines" on page 48
- "DCE Administration Utilities" on page 54.

Determining Requirements for DCE Client Machines

This section describes the planning considerations involved in setting up DCE Client machines. All DCE machines, including DCE server machines, are also DCE Clients.

The following subsections describe the executables that run on a DCE Client machine.

RPC Client Programs

A DCE Client contains the following RPC programs:

- The **dced** daemon must run on any machine that has an RPC server process that exports an interface with dynamic bindings. The **dced** daemon is used to register binding information.

  The **dced** daemon must be running before you configure any other DCE services that register their endpoints. DCE services need to register their endpoints with **dced**. Only one **dced** daemon is needed on a machine. In fact, only one **dced** daemon can run on a machine at a time, because **dced** uses a well-known port.

  Network interfaces, routing services, and other network services must be available before RPC starts. The **dced** daemon is started by the **start.dce** command. The **start.dce** command can be invoked from **/etc/inittab** by specifying the **-autostart yes** option on the **config.dce** command or by adding **/etc/dce/rc.dce** to this file. This will allow DCE services to be brought up each time the machine boots. See "Using SMIT to Start DCE, DFS, and NFS/DFS Authenticating Gateway Now and at System Restart" on page 130 for information on the SMIT menu for starting DCE 2.2 for AIX at reboot.

- The DCE control program (**dcecp**) is a utility that allows you to browse, update, add, and delete the RPC attributes of entries stored in the CDS namespace and the endpoints that are managed by local and remote **dced** daemons.

Security Service Client Programs

The **dced** daemon maintains the local machine principal identity by periodically refreshing the ticket-granting ticket for the machine's principal. This assures that the local root user or any daemon who inherits the machine identity has valid DCE credentials. The **dced** daemon also exports and implements a variety of interfaces, including password and group override support, certification of the security server, and pre-authentication support.

For more information about ticket-granting tickets, see *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components* .

CDS Client Programs

The DCE Client runs the following CDS processes:

- The CDS advertiser, the **cdsadv** process, allows applications to access and communicate with **cdsd**. It starts any needed CDS clerks (**cdsclerk**) and creates the cache shared by the local CDS clerks.
- The **cdsclerk** is an interface between CDS client applications and CDS servers. A clerk must exist on every machine that runs a CDS client application. One **cdsclerk** process runs for each AIX principal on a machine that accesses CDS. The CDS clerk handles requests from client applications to a server and caches the results returned by the server. Because results of

the server request are cached, the clerk does not have to go repeatedly to the server for the same information. All CDS clerks on a machine share one cache. One clerk can serve many client applications.

- The DCE control program (**dcecp**) can be used to browse, update and delete CDS entries, and manage the namespace. For more information, see the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components.*
- The CDS control program, **cdscp**, is a command interface used to control CDS servers and clerks and manage the namespace and its contents. The **cdscp** command interface was available with previous versions of DCE and is provided to ease migration to the use of the **dcecp** utility. For more information about the CDS control program, see the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components.*

DTS Client Programs

The DCE Client runs the following DTS processes:

- The **dtsd** daemon is set as a client or a server. On a client machine, **dtsd** synchronizes the local clock.
- The **dtscp** program allows you to administer DTS, including configuring the **dtsd** daemon as either a client or a server.

Slim Client Programs

In general, client systems have less available memory than server systems. If a client does not offer DCE services to other systems in the cell, it might not need all of the functions provided by the daemons started by the configuration of DCE sortware on the client system. To avoid starting unnecessary daemons on the client use the Slim client option.

Since no information about the Slim client is kept in the cell, administrator intervention, that is **cell_admin**, is not required to configure it. Instead use the **config.dce** command to configure the Slim client. Use the **start.dce** and **stop.dce** commands respectively to start and stop the Slim client. To unconfigure the Slim client use the **unconfig.dce** command.

The Slim client option reduces DCE memory consumption on client systems in several ways:

The Slim client runs a single instance of the CDS clerk with no other DCE daemons. Running a single instance of the CDS clerk is done by starting the clerk with the **-n** option. This starts a clerk without the CDS advertiser. However, if there are so many other DCE services and functions that can be run, how can a single CDS clerk be sufficient? The answer is that most DCE clients need only the following DCE functions:

- RPC calls (both authenticated and unauthenticated)

- DCE login
- CDS name lookups

For RPC calls and most logins, no DCE daemons are needed. These functions simply use RPC runtime routines and Security runtime routines.

For CDS name lookups, only a CDS clerk is necessary. With full DCE, CDS clerks are started by the CDS advertiser, requiring a CDS advertiser to be present. However, in DCE 2.2 for AIX, the **-n** option on the **cdsclerk** command starts a single instance of the CDS clerk without needing the advertiser. This clerk will not terminate after 20 minutes, as it does in full DCE. Additionally, when the clerk is started in this fashion, it takes over the role of the CDS advertiser in managing the CDS client cache.

Without an advertiser, the **cdsclerk** can not be managed by **dcecp** or **cdscp**. The following commands will fail:

```
cdscp show clerk
cdscp disable clerk
cdscp show cached clearinghouse
cdscp define cached server
cdscp show cached server
cdscp clear cached server

dcecp -c cdscache create
dcecp -c cdscache delete
dcecp -c cdscache show -server
dcecp -c cdscache show -clearinghouse
```

The services that compose **dced** and the functions that are disabled, because **dced** is not running on a DCE client system, are:

- **dced Endpoint Mapper Service** must run on any system providing a service that can be accessed through Remote Procedure Calls (RPCs). Such a server is called an RPC server. When a system issues an RPC to an RPC service, it uses the RPC runtime routines to send the request to a specific machine address and asks for the desired RPC service by name. After the RPC reaches the machine where the service resides, the Endpoint Mapper Service maps the RPC service name to the endpoint, or port number, of the specific program providing the service. After the endpoint is known, the client is bound to the specific RPC service and RPCs can be issued directly to that service.

  Although every DCE client system issues RPCs, most do not need the Endpoint Mapper Service, because they are probably not RPC servers. Therefore, the RPC-related limitation of not running **dced** on a client system is that it cannot be an RPC server.
- **Security Validation Service** provides the functions listed below. If a client system does not need these functions, it does not need the **dced** Security

Validation Service. Note that a **dce_login** and authenticated RPCs can still be issued on a system that does not have this service running.

  - **Security Server Certification**
  - **Third-party pre-authentication during dce_login**
  - **Keeping the machine context up to date**.
  - **Password and group overrides**

- **Security Integration**, **dceunixd**, and the DFS client can run on a Slim client. Be aware that because the certification service is not available, when a user logs in, the user's identity cannot be certified to have been issued by a legitimate security server and that security integration on a Slim client cannot use password and group overrides. Because the machine context is not available, security integration on a slim client uses unauthenticated access to the registry. Preferred Security Replica is not supported for the Slim client.
- **System Management Services**:

  The system management functions provided by DCE are listed below. Without **dced**, a client system cannot be remotely managed by means of these functions.

  - **Host Data Management**: This service maintains local files of host data (that includes the host name, cell name, and cell aliases) and a post-processor file. The post-processor file contains program names that are matched to other host data items. **dced** runs the program if the corresponding host data item changes.
  - **Server Control**: This service maintains data that describes the startup configuration and execution state for each server. It can also start or stop particular servers, and enable or disable specific services of servers. This service is not needed on a client that is not running any RPC servers.
  - **Key Table Management**: This service allows for the remote maintenance of a server's key tables. This service is not needed on a client that is not running any RPC servers.

DFS Client Programs

If DFS is configured, the DFS Client runs the following processes:

- The Cache Manager process, **dfsd**, initializes the Cache Manager in the kernel, alters configuration settings, and starts background daemons.

  The Cache Manager is responsible for the local caching of file and directory data on machines used as DFS clients. When the Cache Manager starts, it initializes the cache. When a client retrieves part of a file from a remote File Server, the Cache Manager keeps a copy of that part of the file on the client machine's local disk. As long as that part of the file does not change, the locally cached copy remains available to the client. A new copy is retrieved

from the File Server machine only when another process changes the cached portion of the file. The Cache Manager also caches directory and fileset location information.

- The **dfsbind** process performs the following tasks:
  - Obtains cell location information from CDS
  - Responds to security requests on behalf of the DFS kernel processes by making calls to the Security Server.

Note: DFS will not recognize any DCE credentials acquired on a DCE client machine before the DFS client is configured. After you configure the DFS client, you must run the **dce_login** command to have authenticated access to files and directories in the DFS file space. Refreshing the credentials with the **kinit** command is *not* sufficient. The **dce_login_noexec** command does *not* authenticate the issuer to DFS. If your machine is configured to support AIX/DCE integrated security operations, you can use AIX commands like **login** or **su** to acquire DCE credentials that are recognized by DFS after the DFS client has been configured.

Determining Requirements for DCE Server Machines

This section provides information about requirements for the different types of DCE server machines.

Files Installed on DCE Server Machines

The following subsections discuss the files that must be installed on each of the different DCE server machines and the approximate space required. Note that, because all DCE servers are also DCE Clients, the files described in "Determining Requirements for DCE Client Machines" on page 43 must also be installed on server machines. Therefore, add the appropriate server space requirements to the DCE Client machine space requirements to reach the approximate total space requirement for the configuration you are planning.

RPC Server Programs

There are no RPC server programs other than the programs that run on the DCE Client.

Security Server Processes

Every cell has one master DCE Security Service machine and can also have replica DCE Security Service machines. The following processes run on a DCE Security Service master or replica server machine:

- The Security Server, or **secd** process, implements the Authentication service, the Privilege service, and the Registry service.

- The **sec_create_db** program initializes the security database. The **config.dce** command passes a parameter indicating whether to create a master or replica Security server on the machine.
- The DCE control program (**dcecp**) is used for the registry, management, and maintenance of the Security server. Optionally, you can use the **sec_admin** program. See "DCE Administration Utilities" on page 54 for descriptions of these programs.

Keep the following considerations in mind when you are planning for security servers:

- The node that runs the master security server must be highly available and physically secure. Consider placing the master security server machine in a locked room and keeping a log to record who accesses the machine.
- Be sure to move the master security server before removing the node from the network or shutting down the node for an extended period of time. Modifications are made to the master security server and propagated to replicas throughout your cell. If the master security server is unavailable, no updates can be made. For more information see ″Handling Network Reconfigurations″ in the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components.*
- A cell can have only one master security server. If you plan to make one cell out of several existing cells with independent master security servers, you must first merge their registries.

For further information about planning for the DCE Security service, see the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components.*

If the host that contains the master security server goes down, hosts that have replica DCE Security Servers can still provide registry information; so, consider having a number of replicas in your network. Use factors such as the number of machines in your cell, the reliability of the machines that run security servers, and your cell's available resources to determine how many replica security servers you need to have.

CDS and GDA Server Processes

A CDS server stores and maintains object names within a cell and handles requests to create, modify, and look up data. There must be a GDA server running in a cell in order for the cell to communicate with other cells.

The following processes run on a CDS server machine:

- The CDS daemon, **cdsd**, is the CDS server process.

- The **cdsadv**, in addition to receiving server advertisements to find out what servers are available as it does on a DCE Client machine, on a CDS Server machine also sends server advertisements.
- The DCE control program (**dcecp**) for the management and maintenance of the CDS software. In addition, the **cdscp** program for controlling and displaying information about CDS clerks and servers See "DCE Administration Utilities" on page 54 for descriptions of these programs.

In preparing for CDS, you need to select server nodes that store and maintain the clearinghouses (CDS databases) in the cell.

Keep the following guidelines in mind in order to achieve reliability, optimum performance, and data availability:

- Choose dependable nodes. A CDS server needs minimal downtime and needs to restart quickly. The CDS server needs to be one of the first systems available on the network because client applications and other DCE servers rely on the CDS server for up-to-date information. The CDS server initializes the CDS namespace when you configure DCE.
- Use reliable network connections. This helps to ensure that all servers maintaining directory replicas can be reached when CDS performs a skulk. Skulks are periodic updates that check for consistency across all replicas.
- Consider the size of your cell and how geographically dispersed the cell is when deciding how many CDS servers you need. You should have at least two copies (one master and one read-only replica) of each CDS directory to ensure access to data if one of the servers becomes unavailable.
- Each CDS server maintains at least one clearinghouse. All clearinghouses contain a copy of the root in addition to other directories replicated there.
- You need to make replication decisions based on where the contents of directories are referenced. Put replicas where the contents are read and put masters where the contents are written.

The **gdad** daemon is the GDA server, which sends lookup requests for cell names to the DNS and returns the results to the CDS clerk in the cell that initiated the request.

In a DCE configuration using DNS, CDS must be able to contact at least one GDA to access a global directory service. The GDA can be on the same machine as a CDS server, or it can exist independently on another machine. You can have two or more **gdad** daemons running in a cell to ensure GDA availability.

DTS Server Programs

The DCE Client configuration already contains all the files necessary for a DTS server machine, with the exception of the optional time provider.

- The **dtsd** daemon (which can be installed on a DCE Client machine) is configured to run as a server. As a server process, **dtsd** synchronizes with other DTS servers, in addition to synchronizing the local clock, as it does on a client machine.
- The **dts_***device_name***_provider** specifies the communications between the DTS server process and the time-provider process. For *device_name*, substitute the device you are using, which can be a radio, clock, or modem, or another source of UTC time for DTS. A time provider is optional. If you use a time provider, it must connect to a server process.

Consider the following guidelines when planning your DTS implementation:

- Each cell should have at least three DTS servers. At least three DTS servers are needed in order to detect if one of them is faulty when they are queried for the time. It is preferable to have four or more DTS servers to provide redundancy. The additional servers increase the accuracy of time synchronization. However, increasing the number of servers queried for the time also increases the activity on the network. The administrator must balance the level of accuracy with the amount of network activity.
- A time provider is optional in DTS; however, cells that must be closely synchronized with a time standard need to have at least one time provider.
- Servers need to be located at the sites with the greatest number of different network connections.
- If there are less than three time servers configured in the cell, one of the following commands should be used:

  dtscp set servers required *n*
  (where *n* is the number of time servers in the cell)
  dcecp -c dts modify -minservers *n*
  (where *n* is the number of time servers in the cell)

  This will prevent a warning message from being logged every time the server attempts to sync.

There are many network configuration decisions that affect DTS planning. The *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components* contains details about the total DTS planning process, including configuration planning for Local Area Networks (LANs), extended LANs, and Wide Area Networks (WANs) as well as an explanation of the criteria you need to use when selecting a time source for your network to use.

DFS Server Programs

DCE supports configuration of the following types of DFS server machines:

- System Control Machine
- Fileset Location Database Server
- File Server
- Fileset Replication Server
- Backup Database machine.

DFS File Servers can assume different roles. The DFS space requirements may vary, depending on the role of a particular machine. DFS machines that export data for use in the global namespace can run the following server processes:

- The **flserver** process maintains a complete list of fileset locations in the Fileset Location Database (FLDB). The FLDB is a cell-wide database that maps filesets to the servers on which they are located. There must be at least one **flserver** process running in a cell.
- The **fxd** daemon is a user-space process. The **fxd** daemon starts the kernel processes that implement the File Exporter.
- The **ftserver** process allows system administrators to create, delete, duplicate, move, back up, or restore entire filesets with one set of commands.
- The **bosserver** process reduces system administration demands by constantly monitoring the processes running on its File Server machine. The **bosserver** process can restart failed processes automatically; it provides a convenient interface for administrative tasks.
- The **repserver** process manages replicas of filesets on all File Server machines.
- The **upserver** process controls the distribution of common configuration files to all other DFS server machines in a domain.
- The **upclient** process contacts the **upserver** process to verify that the most recent version of each DFS configuration file is being used.
- The **dfsbind** process is described in “Determining Requirements for DCE Client Machines” on page 43.
- The **bakserver** process maintains the Backup Database where information used to backup and restore filesets resides.

This section describes the following DFS configurations: A System Control machine, a Fileset Location Database machine, a File Server machine, a Binary Distribution machine, and a DFS client that is also a private File Server machine.

A System Control machine distributes system configuration information, such as administrative lists, shared by all DFS server machines in an administrative domain. This machine runs the **upserver** process and the **bosserver** processes.

A Fileset Location Database machine runs the **flserver** and the **bosserver** processes. The Fileset Location Database machine tracks the locations of all filesets and records the locations of filesets in the FLDB. The **flserver** process can run on the same machine as the File Server.

A File Server machine is used to export DCE LFS and non-LFS data for use in the global namespace. This machine must run the **fxd**, **ftserver**, and **bosserver** processes. To act as a Fileset Replication Server, it must run the **repserver** process. File Server machines also run the **upclient** process to receive configuration file updates. The client process, **dfsbind**, must also run on this machine.

As explained previously, a DFS client machine runs the **dfsd** and **dfsbind** processes. Optionally, a DFS client machine can be configured as a private File Server to export its local file system for use in the global namespace. This machine must run the **fxd**, **ftserver**, and the **bosserver** processes.

A private File Server machine is controlled by the owner of the machine, not by the system administrator. It normally maintains its own DFS administrative lists. The purpose of a private File Server machine is to allow individual users to export a small number of filesets.

The **config.dfs**, **start.dfs**, **stop.dfs**, and **unconfig.dfs** commands will configure, start, stop, and unconfigure the deamons appropriate for each component or server role.

Figure 2 on page 54 shows a DFS configuration that uses a File Server machine to run the Fileset Location Database machine and a System Control machine. A second machine is a File Server machine only. One DFS client machine is configured as a private File Server to export filesets for use in the global namespace. Note that the first machine is configured to perform multiple roles.

Note: Figure 2 on page 54 shows DFS alone. In addition, each client would run the processes described previously in this chapter. A complete cell would also include servers for the minimum DCE configuration.

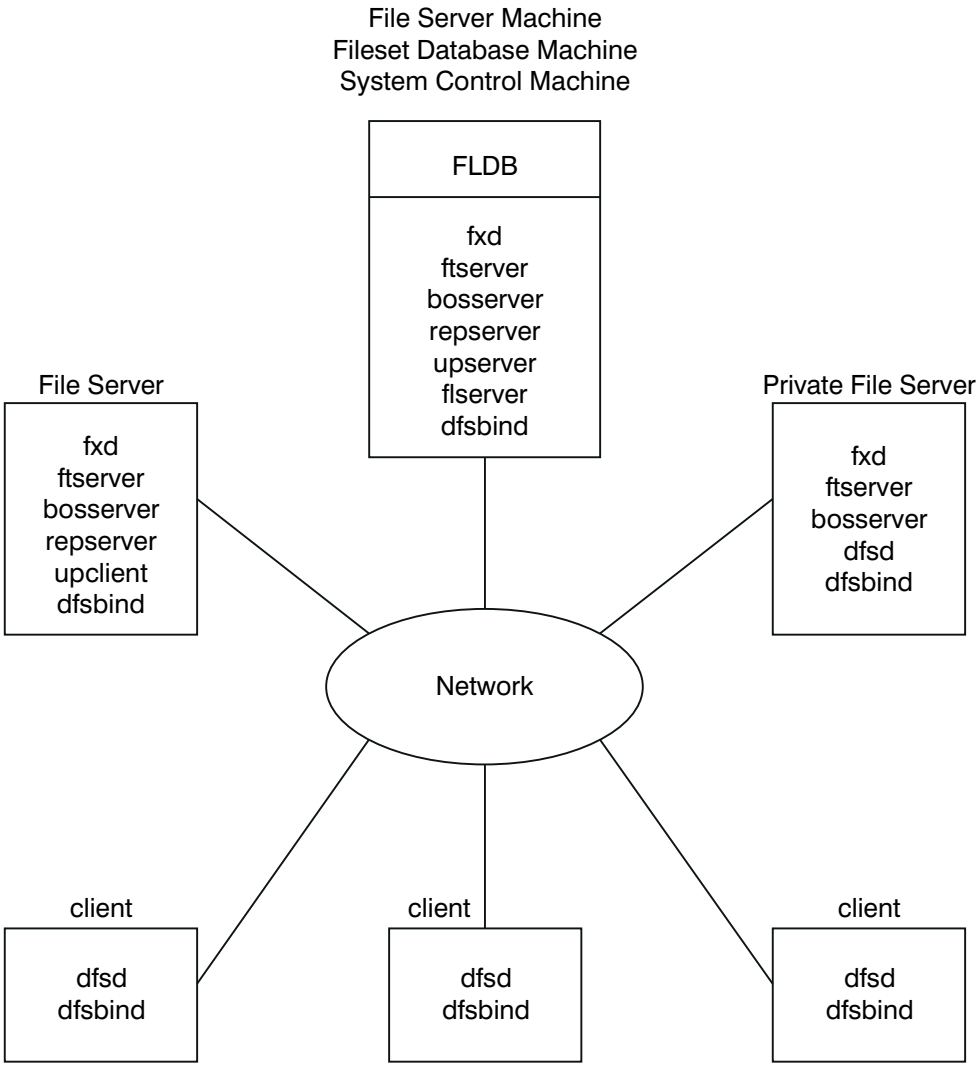

Figure 2. An Example DFS Configuration

DCE Administration Utilities

This section describes the system administration utilities that can assist you in performing DCE administrative tasks.

DCE Control Program

The DCE control program **dcecp** creates, maintains, and manages RPC, CDS, Security, DTS, EMS, and DCED objects. For more information on **dcecp**, see

the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components* and the *IBM DCE for AIX, Version 2.2: Administration Commands Reference* .

RPC Administration Programs

The DCE Remote Procedure Call Service provides the following administration utilities:

- The **dced** daemon is used to register binding information.
- The DCE control program (**dcecp**) allows you to browse, update, add, and delete the RPC attributes of entries stored in the CDS namespace and the endpoints that are managed by local and remote **dced** daemons.

See the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components* and the *IBM DCE for AIX, Version 2.2: Administration Commands Reference*for more detailed information about these programs.

DCE Security Service Administration Programs

The DCE Security Service provides the following administration utilities:

- The **dcecp acl** command displays, adds, modifies, and deletes ACL entries for a specific object. The *IBM DCE for AIX, Version 2.2: Administration Commands Reference* contains detailed information about using the **dcecp acl** command.
- The **dcecp account**, **group**, **organization**, **principal**, **registry**, **user**, and **xattraschema** commands allow you to edit the registry database or the local registry. Almost all editing of the registry database must be done with these commands. The *IBM DCE for AIX, Version 2.2: Administration Commands Reference* explains the use of the commands.
- The **passwd_import** command allows you to create registry entries based on the group and password files from machines that do not implement DCE Security.
- The **passwd_export** command allows you to update the UNIX **/etc/passwd** and **/etc/group** files with current user information obtained from the registry.
- The **passwd_override** and **group_override** files allow you to establish overrides to the information contained in the registry.
- The **rmxcred** command purges expired tickets from the credentials directory.
- The **dcecp registry** command helps you manage server replicas of the registry, change the master server site, and reinitialize a slave server. This command also helps you manage the security server and its database. You can perform tasks such as generating a new master key for the database and stopping the security server.

CDS Administration Programs

CDS provides the following administration utilities:

- The **cdscp** program is described in "CDS Client Programs" on page 44.
- The **cdsli** gives a DCE user the ability to recursively list the namespace of cells.
- The **cdsdel** deletes recursively the namespace of cells.
- The CDS Browser, **cdsbrowser**, is a program based on Motif that lets you view the contents and structure of a namespace.
- The DCE control program, **dcecp**, can be used to browse, update, and delete CDS entries, and to manage the namespace. It replaces **cdscp**.

  The **mkreg.dce** command enters information about your DCE cell into the database maintained by your domain name server (the **named** daemon).

  The **rmreg.dce** command removes information from the database maintained by your domain name server (the **named** daemon) that were added by the **mkreg.dce** command.

SVC Administration Programs

The **svcdumplog** program prints the contents of a serviceability binary log file as readable txt. For more information on **svcdumplog**, see the *IBM DCE for AIX, Version 2.2: Administration Commands Reference.*

DTS Administration Programs

- The **dtscp** command controls the interface you can use to configure and manage DTS. It is already included in the DCE Client software.
- The **dtscp** program allows you to administer DTS, including configuring the **dtsd** daemon as either a client or a server.

DFS Administration Programs

DFS provides the following administration utilities:

- The **salvage** process checks the DCE LFS file system for internal consistency and corrects errors it finds.
- The **fts** commands help you manage filesets.
- The **bak** and **butc** commands help you perform backup tasks.
- The **bos** commands help you contact the Basic OverSeer (BOS) Server used to monitor processes on server machines in your cell. You can also use the **bos** commands to perform some Security tasks.
- The **cm** commands help you customize the Cache Manager and examine features of DFS.

- The **scout** program helps you monitor the File Exporters running on File Server machines. You may want to install Scout only on the system administrator's DFS client machine.
- The **dfsexport** command makes DCE LFS aggregates and non-LFS partitions available to remote users through the use of the File Exporter.
- The **growaggr** command can increase the size of a DCE LFS aggregate (after the logical volume has been increased).
- The **mkbutc.dfs** command configures the Backup Tape Controller on a machine in one command. This command can be issued for each Backup Tape Controller in the cell. The bak server is updated no matter where it is running in the cell. The local file **TapeConfig** is updated as well as the **User-Defined Configuration** file, if it has been created.
- The **mkfilesys.dfs** command registers and exports JFS file systems, DCE LFS aggregates, and CD-ROM file systems on a DFS File Server machine
- The **newaggr** command can format an AIX logical volume for use as DCE LFS.
- The **rmbutc.dfs** command unconfigures the Backup Tape Controller on the machine in one command. This command can be issued for each Backup Tape Controller in the cell. The bak server is updated no matter where it is running in the cell. The local file **TapeConfig** is updated and the **User-Defined Configuration** file is removed, if it had been created previously using the **mkbutc.dfs** command.
- The **rmfilesys.dfs** command detaches and unregisters JFS file systems, DCE LFS aggregates, and CD-ROM file systems on a DFS File Server machine.

DCE/DFS Web Utilities for AIX

DCE 2.2 for AIX provides two components to extend your Netscape web servers by providing DCE credentials to your web transactions. DFS Web Secure allows users to access documents residing in DFS as well as provides DCE credentials to CGI programs accessed through a web browser. DCE Administration allows you to manage DCE and DFS objects from a frame-enabled web browser.

DFS Web Secure: The DFS Web Secure product extends your Netscape FastTrack 2.01 or Enterprise 2.01 web server to provide DCE authentication to your web transactions, enabling you to use a web browser to access documents stored in DFS or run Common Gateway Interface (CGI) programs that require DCE credentials, such as DCE Administration.

DFS Web Secure does not require the DFS Client to be available (installed, configured, or running) on the web server workstation. If the DFS Client is not available, DFS Web Secure will still provide DCE credentials to DCE Administration and other CGIs that are configured for DCE authentication in

the web server configuration files. However, if the DFS Client is not available, users will not be able to access documents stored in DFS through their web browsers.

With DFS Web Secure you can:

- access documents stored in DFS (those that reside with a URL beginning with **/:**, **/.:**, or **/...**). For example, to access the **/:/burnside.html** document through a web server named **antietam**, users would enter the following URL in their web browser:

  ```
  http://antietam/:/burnside.html
  ```

- provide DCE credentials to a CGI program. For example, with a tcl program called changeusers.tcl that makes batch changes to a group of DCE accounts, administrators would place the changeusers.tcl program into a directory that has been configured for CGI access in the web server configuration files. When a user runs the CGI program through the web browser, it gains the DCE credentials under the DCE userid that the web browser user is logged in as.

  With the DCE Administration CGI programs, administrators can gain all the functionality of managing DCE users, groups, and organizations, as well as manage permissions and DFS filesets.

For more information on DFS Web Secure, see the *DFS Web Secure Product Guide*, available through your web browser after installing and configuring DFS Web Secure. This guide will be accessible through the following URL:

http://*servername***/dceweb**

DCE Web Administration: IBM's DCE/DFS Web Administration is a tool for administering your DCE or DFS environment. It can simplify administration tasks such as creating users, modifying group membership, setting up filesets, and working with permissions on files or any DCE object.

You can perform these administrative actions from any frame-enabled web browser. A Netscape FastTrack 2.01 or Enterprise 2.01 web server must be installed and configured, and DFS Web Secure must be installed.

Application Development Environment

You can configure a DCE machine for the development of DCE applications. This configuration requires adding to the basic DCE Client configuration several include (**.h**) and interface specification (**.idl**) files, along with the **idl** compiler. The files and the compiler are included in the **dce.tools.appdev.adt** package available in the DCE for Application Developers licensed program

product. You can also use the **sams** utility to include support for messaging and serviceability in your applications. The **sams** utility is included in the **dce.tools.appdev.adt** package.

Location of Installed DCE Files

The files used by DCE are grouped in the following locations:

- The **/opt/dcelocal** subdirectories
- Conventional UNIX subdirectories.

Some information needs to be kept locally on a machine for reliability and to ensure security is maintained. For example, when you configure DCE, the file that contains the name of your cell must be on the machine that is being configured. This file is stored in the **/opt/dcelocal** subtree.

The **/opt/dcelocal** subtree is created when you install DCE components.

In some cases, files are installed into directories such as **/usr/lib**, **/usr/bin**, or **/bin** for performance reasons. In other cases, symbolic links can be used from the conventional UNIX subdirectories to **/opt/dcelocal**.

This section contains the following topics:

The /opt/dcelocal Subtree

In order to initially boot a server and configure the cell, the appropriate files for mandatory servers (CDS and Security) need to be available on that server machine (in the **/opt/dcelocal** subtree). It is strongly recommended that copies of the minimum set of programs and data files installed during the default DCE installation procedure be kept locally on server machines for stand-alone operation and emergency maintenance.

The contents of the **/opt/dcelocal** subtree can vary from machine to machine inside a DCE cell to accommodate and serve specific configurations. In addition, every machine must have local access to certain files so each machine can run as a stand-alone system if the machine is disconnected or partitioned from the cell. The appropriate files on DCE servers that have to be local to the server machine must be stored under **/opt/dcelocal**. Client-related data files are stored below **/opt/dcelocal/etc** (static configuration data) and **/opt/dcelocal/var/adm**. All server-specific data files are located in the **/opt/dcelocal/var/***dce-component-name* directory.

The **/opt/dcelocal** subtree is populated and initialized during DCE installation and configuration.

Conventional UNIX Directories

Some files and directories used by DCE are accessible in conventional UNIX directories. These DCE files and directories need to be accessible in conventional locations so users can conveniently access frequently used utilities and data, such as **idl** from the **/usr/bin** directory and **localtime** from the **/etc/zoneinfo** directory. Header files are accessible in **/usr/include** or in its subdirectory, **/usr/include/dce**, and libraries, such as **libdce.a**, are kept in **/usr/lib**.

File Locations

The installation process for DCE 2.2 for AIX places files in the following locations:

/usr/lpp/dce
All DCE files except those in the remainder of this list.

/usr/lpp/dcedoc
All DCE for AIX documentation files and their related tools.

/etc/dce
The following files:

- **rc.dce**
- **dce.clean**
- **rc.dfs**
- **dfs.clean**
- **rpc.clean**
- **rc.nfsdfs**

/etc/dce/rspfiles
Configuration response files

/etc/zoneinfo
Timezone rules for DTS.

/tmp/dce
Temporary location for configuration processing

/usr/lib/nls/msg/en_US
English message catalogs.

/usr/include
Include files (mostly under **/usr/include/dce**)

/usr/lib
libdce.a, **libcfgdce.a**, **libdcelibc_r.a**, **libdcepthreads.a**, and **libidlcxx.a**

/usr/lib/security
The **DCE** load module for AIX/DCE integrated security operations.

/usr/lib/drivers
DFS kernel extensions.

/usr/sbin
Commands for loading the DFS kernel extensions.

/opt/dcelocal/ is set up as a symbolic link to **/usr/lpp/dce**. **/opt/dcelocal/var** is set up as a symbolic link to **/var/dce**. **/opt/dcelocal/etc** is set up as a symbolic link to **/etc/dce**. **/opt/dcelocal/tmp** is a symbolic link to **/tmp/dce**. A link for each of the DCE commands is placed in **/usr/bin**.

In addition, SMIT objects are loaded into the Object Data Manager (ODM) database.

File Systems to Create and Mount

You will probably want to create new AIX JFS file systems in order to use DCE effectively:

/var/dce
All DCE components store information in the **/var/dce** directory. If the **/var** file system fills up, DCE and other subsystems that depend on **/var** (such as the mail and spooler sybsystems) cannot operate correctly.

You should create a new file system mounted over **/var/dce** before you install DCE. You should reserve about 30 megabytes for **/var/dce** for your initial DCE configuration.

/var/dce/directory
The CDS server stores the clearinghouse files, which contain this server's portion of the namespace, and local data in this directory.

If this machine is configured as a CDS server, it is recommended that you create a new file system mounted over **/var/dce/directory** before you install DCE.

You should reserve about 30 megabytes for the server's use.

If you do not plan to create a separate files system for the CDS server, you should add the additional 30 megabytes to **/var/dce**.

/var/dce/security
This is where the Security Server stores the registry,

credentials, and local data. If this machine will be a Security Server, you should add an additional 10 megabytes to **/var/dce** for the server's use.

DFS client cache

If the machine will be configured as a DFS client and you plan to configure DFS to use on-disk caching, you should create a new file system to hold the DFS cache files. This must be an AIX JFS filesystem which is not using compression or fragmentation. The default directory is **/var/dce/adm/dfs/cache**, but you can specify a different directory when you configure DFS. The default cache size is 10MB, but you can change this during configuration. If you do not want to create a separate file system, ensure that the file system where you plan to place the DFS cache has enough room to hold the cache or configure the DFS cache to be in-memory.

If you do not plan to create a separate file system for the DFS cache directory and you use the default cache directory, you should add room for the DFS cache to **/var/dce**.

Files stored in **/var/dce** are any files particular to the individual machine. You should monitor the space usage in **/var/dce** (and any associated separate files systems) to make sure it does not fill up. To clean up expired credentials files in **/var/dce**, use the **/usr/lpp/dce/bin/rmxcred** command. The DCE Auditing and Servicability facilities also use space in **/var/dce**. See the *IBM DCE for AIX, Version 2.2: Administration Commands Reference* for more information on **rmxcred** and DCE Auditing.

Chapter 3. Installing DCE 2.2 for AIX Servers and Clients

Use the following sections for installation:

Installable Packages

Following is a summary of the installable filesets for the DCE 2.2 for AIX packages. For more detailed descriptions, see "Chapter 1. Overview of DCE 2.2 for AIX" on page 3.

- dce.cdmf — User Data Masking Package

  dce.cdmf.rte
  User Data Masking
- dce.cds — Cell Directory Server Package

  dce.cds.rte
  Cell Directory Server
- dce.client — Base Services Package

  dce.client.core.rte
  Client Services

  dce.client.core.rte.admin
  Client Administration Tools

  dce.client.core.rte.cds
  Client CDS Tools

  dce.client.core.rte.config
  Client Configuration Tools

  dce.client.core.rte.rpc
  Client RPC Tools

  dce.client.core.rte.security
  Client Security Tools

  dce.client.core.rte.time
  Client Time Tools

  dce.client.core.rte.zones
  Client Time Zones

dce.client.dfs.rte
DFS Client Services

- dce.compat — DCE SMIT Package

dce.compat.cds.smit
SMIT Cell Directory Server

dce.compat.client.core.smit
SMIT Client Tools

dce.compat.client.dfs.smit
SMIT DFS Client Services

dce.compat.security.smit
SMIT Security Server

dce.compat.dfs_server.smit
SMIT DFS Servers

dce.compat.dfsnfs.smit
SMIT NFS to DFS Authenticating Gateway

dce.compat.edfs.smit
DCE SMIT Enhanced DFS

dce.compat.sysmgmt.ems.smit
DCE SMIT Event Management Services

dce.compat.sysmgmt.snmpagt.smit
DCE SMIT SNMP Subagent

dce.compat.web.admin.smit
DCE SMIT Web Secure Admin

- dce.dfs_server — DFS Servers Package

dce.dfs.server.rte
DFS Servers

- dce.dfsnfs — NFS to DFS Authenticating Gateway Package

dce.dfsnfs.rte
NFS to DFS Authenticating Gateway

- dce.doc_DCE — Online Documentation

dce.doc.rte.ascii
DCE ASCII Browser and **dceman**

dce.doc.en_US.ascii
DCE ASCII Browser Files

dce.doc.en_US.html
HTML Documentation Files

- dce.msg.en_US — Messages Package

dce.msg.en_US.pthreads.rte
Threads Compatibility Library Messages

dce.msg.en_US.client.core.rte
Base Messages

dce.msg.en_US.client.dfs.rte
DFS Client Messages

dce.msg.en_US.compat.cds.smit
SMIT Cell Directory Server Messages

dce.msg.en_US.compat.client.core.smit
SMIT Base Messages

dce.msg.en_US.compat.dfsnfs.smit
SMIT NFS to DFS Authenticating Gateway Messages

dce.msg.en_US.compat.edfs.smit
DCE SMIT Enhanced DFS Messages

dce.msg.en_US.compat.sysmgmt.ems.smit
DCE SMIT Event Management Messages

dce.msg.en_US.compat.security.smit
SMIT Security Server Messages

dce.msg.en_US.compat.sysmgmt.snmpagt.smit
DCE SMIT SNMP Subagent Messages

dce.msg.en_US.compat.edfs.rte
DCE Enhanced DFS Messages

dce.msg.en_US.dfs_server.rte
Base DFS Server Messages

dce.msg.en_US.sysmgmt.ems.rte
DCE Event Management Services Messages

dce.msg.en_US.sysmgmt.snmpagt.rte
DCE SNMP SubAgent Messages

dce.msg.en_US.web.admin.rte
DCE Web Administration Messages

dce.msg.en_US.web.secure.rte
DCE Web Secure Messages

- dce.priv — Privacy Level Protection Feature Package

dce.priv.rte
Privacy Level Protection Feature

- dce.pthreads — Threads Compatibility Library Package

dce.pthreads.rte
Threads Compatibility Library

- dce.security — Security Server Package

dce.security.rte
Security Server

- dce.sysmgmt — DCE System Management Package

dce.sysmgmt.ems.rte
DCE Event Management Services

dce.sysmgmt.snmpagt.rte
DCE SNMP SubAgent

- dce.tools — DCE for Application Developers

dce.tools.admin.rte
Administration Tools

dce.tools.appdev.adt
Application Development Tools

- dce.web — DCE World Wide Web Security Package

dce.web.secure.rte
DCE Web Secure

dce.web.secure.dat
DCE Web Secure Default Data

dce.web.admin.rte
DCE Web Secure Admin GUI

dce.web.admin.dat
DCE Web Secure Admin GUI Default Data

- dce.xdsxom — X.500 API Library Package

dce.xdsxom.rte
X.500 API Library

Prerequisite Software

Table 2 on page 67 lists the DCE 2.2 for AIX filesets in the order in which they are installed. See the *IBM DCE for AIX, Version 2.2: Release Notes* for the latest requisite levels of software.

Note: Those software names beginning with dce are at the same release level as the shipped DCE product.

Table 2. Installation filesets and prerequisite software

Fileset You Are Installing	**Prerequisite[1], Corequisite[2], and Instreq[3] Software Names**	**Prerequisite Software Description**
dce.pthreads.rte	bos.rte[1]	AIX Base Operating System (BOS) Runtime (4.X.X.X)
dce.pthreads.rte	bos.rte.libpthreads[1]	libpthreads Library (4.X.X.X)
dce.client.core.rte	bos.net.tcp.client[1]	TCP/IP Client Support (4.X.X.X)
dce.client.core.rte	xlC.rte[1]	C Set # for AIX Application Runtime (3.X.X.X)
dce.client.core.rte	bos.adt.lib[1]	Base Application Development Libraries (4.X.X.X)
dce.client.core.rte	dce.pthreads.rte[1]	DCE Threads Compatibility Library for AIX
dce.client.core.rte	dce.client.core.rte.config[2]	DCE Client Configuration Tools
dce.client.core.rte	dce.client.core.rte.security[2]	DCE Client Security Tools
dce.client.core.rte	dce.client.core.rte.cds[2]	DCE Client CDS Tools
dce.client.core.rte	dce.client.core.rte.time[2]	DCE Client Time Tools
dce.client.core.rte	dce.client.core.rte.zones[2]	DCE Client Time Zones
dce.client.core.rte	dce.client.core.rte.admin[2]	DCE Client Administrative Tools
dce.client.core.rte	dce.client.core.rte.rpc[2]	DCE Client RPC Tools
dce.client.core.rte.admin	dce.client.core.rte[1]	DCE Client Services
dce.client.core.rte.cds	dce.client.core.rte[1]	DCE Client Services
dce.client.core.rte.config	dce.client.core.rte[1]	DCE Client Services
dce.client.core.rte.rpc	dce.client.core.rte[1]	DCE Client Services
dce.client.core.rte.security	dce.client.core.rte[1]	DCE Client Services
dce.client.core.rte.time	dce.client.core.rte[1]	DCE Client Services
dce.client.core.rte.zones	dce.client.core.rte[1]	DCE Client Services

Table 2. Installation filesets and prerequisite software (continued)

Fileset You Are Installing	Prerequisite[1], Corequisite[2], and Instreq[3] Software Names	Prerequisite Software Description
dce.client.dfs.rte	dce.client.core.rte[1]	DCE Client Services
dce.client.dfs.rte	bos.up.rte[3] or bos.mp[3]	Base Operating System Uniprocessor Runtime (4.X.X.X) or Base Operating System Multiprocessor Runtime (4.X.X.X) Note that these are only installed on 4.2.X.X levels of AIX.
dce.cdmf.rte	dce.client.core.rte[1]	DCE Client Services
dce.priv.rte	dce.client.core.rte[1]	DCE Client Services
dce.security.rte	dce.client.core.rte[1]	DCE Client Services
dce.cds.rte	dce.client.core.rte[1]	DCE Client Services
dce.dfs_server.rte	dce.client.dfs.rte[1]	DCE DFS Client Services
dce.dfsnfs.rte	dce.client.dfs.rte[1]	DCE DFS Client Services
dce.dfsnfs.rte	bos.net.nfs.server[1]	Network File System Server (4.X.X.X)
dce.doc.rte.ascii	dce.pthreads.rte[1]	DCE Threads Compatibility Library for AIX
dce.doc.en_US.ascii	dce.doc.rte.ascii[1]	DCE ASCII Browser and **dceman**
dce.doc.en_US.html		Web Browser
dce.doc.en_US.ps		
dce.edfs.rte	dce.dfs_server.rte[1]	DCE DFS Servers
dce.tools admin.rte	dce.client.core.rte[1]	DCE Client Service
dce.tools appdev.adt	dce.client.core.rte[1]	DCE Client Service
dce.xdsxom.rte	dce.pthreads.rte[1]	DCE Threads Compatibility Library for AIX
dce.compat.cds.smit	dce.cds.rte[1]	DCE Cell Directory Server
dce.compat.cds.smit	dce.compat.client.core.smit[1]	DCE SMIT Client Tools
dce.compat.client.core.smit	dce.client.core.rte[1]	DCE Client Service

Table 2. Installation filesets and prerequisite software (continued)

Fileset You Are Installing	Prerequisite[1], Corequisite[2], and Instreq[3] Software Names	Prerequisite Software Description
dce.compat.client.dfs.smit	dce.client.dfs.rte[1]	DCE DFS Client Services
dce.compat.client.dfs.smit	dce.compat.client.core.smit[1]	DCE SMIT Client Tools
dce.sysmgmt	dce.client.core.rte[1]	DCE Client Service
dce.sysmgmt	dce.compat.client.core.smit[1]	DCE SMIT Client Tools
dce.compat.security.smit	dce.security.rte[1]	DCE Security Server
dce.compat.security.smit	dce.compat.client.core.smit[1]	DCE SMIT Client Tools
dce.compat.dfs_server.smit	dce.dfs_server.rte[1]	DCE DFS Servers
dce.compat.dfs_server.smit	dce.compat.client.core.smit[1]	DCE SMIT Client Tools
dce.compat.edfs.smit	dce.edfs.rte[1]	DCE Enhanced DFS Services
dce.compat.edfs.smit	dce.compat.client.core.smit[1]	DCE SMIT Client Tools
dce.compat.dfsnfs.smit	dce.dfsnfs.rte[1]	DCE NFS to DFS Authenticating Gateway
dce.compat.dfsnfs.smit	dce.compat.client.core.smit[1]	DCE SMIT Client Tools
dce.web.admin.rte	dce.web.secure.rte[1]	DCE Web Secure,
dce.web.admin.rte	dce.web.admin.dat [2]	DCE Web Secure Administration GUI Default Data
dce.web.admin.dat	dce.web.secure.dat[1]	DCE Web Secure Default Data
dce.web.admin.dat	dce.web.admin.rte[2]	DCE Web Secure Administration GUI
dce.web.secure.rte	dce.client.core.rte[1]	DCE Client Services
dce.web.secure.rte	dce.web.secure.dat[2]	DCE Web Secure Default Data
dce.web.secure.dat	dce.web.secure.rte[1]	DCE Web Secure
dce.sysmgmt.ems.rte	dce.client.core.rte[1]	DCE Client Services
dce.sysmgmt.snmpagt.rte	dce.client.core.rte[1]	DCE CLient Services
dce.msg.en_US.pthreads.rte	dce.pthreads.rte[3]	DCE Threads Compatibility Library for AIX
dce.msg.en_US.client.core.rte	dce.client.core.rte[3]	DCE Client Service

Table 2. Installation filesets and prerequisite software (continued)

Fileset You Are Installing	Prerequisite[1], Corequisite[2], and Instreq[3] Software Names	Prerequisite Software Description
dce.msg.en_US.client.dfs.rte	dce.client.dfs.rte[3]	DCE DFS Client Service
dce.msg.en_US.compat.cds.smit	dce.compat.cds.smit[3]	DCE SMIT Cell Directory Server
dce.msg.en_US.compat.client.core.smit	dce.compat.client.core.smit[3]	DCE SMIT Client Tools
dce.msg.en_US.compat.dfsnfs.smit	dce.compat.dfsnfs.smit[3]	DCE SMIT NFS to DFS Authenticating Gateway
dce.msg.en_US.compat.edfs.smit	dce.compat.edfs.smit[3]	DCE SMIT Enhanced DFS Services
dce.msg.en_US.compat.security.smit	dce.compat.security.smit[3]	DCE SMIT Security Server
dce.msg.en_US.compat.sysmgmt.ems.smit	dce.compat.sysmgmt.ems.smit[3]	DCE SMIT Event Management Messages
dce.msg.en_US.compat.sysmgmt. \ snmpagt.smit	dce.compat.sysmgmt. \ snmpagt.smit[3]	DCE SMIT SNMP Subagent Messages
dce.msg.en_US.dfs_server.rte	dce.dfs_server.rte[3]	DCE DFS Servers
dce.msg.en_US.edfs.rte	dce.edfs.rte[3]	DCE Enhanced DFS Services
dce.msg.en_US.web.admin.rte	dce.web.admin.rte[3]	DCE Web Secure Administration GUI
dce.msg.en_US.web.secure.rte	dce.web.secure.rte	DFS Web Secure Messages
dce.msg.en_US.sysmgmt.ems.rte	dce.sysmgmt.ems.rte[3]	DCE Event Management Services
dce.msg.en_US.sysmgmt.snmpagt.rte	dce.sysmgmt.smnpagt.rte[3]	DCE SNMP SubAgent

Table 2. Installation filesets and prerequisite software (continued)

Fileset You Are Installing	Prerequisite[1], Corequisite[2], and Instreq[3] Software Names	Prerequisite Software Description
Notes: The following language file sets can be substituted for the **en_US** file set: **Ja_JP**, **Zh_TW**, **es_ES**, **Es_ES**, **ja_JP**, **ko_KR**, or **zh_TW**. [1]Prerequisite fileset(s) must be installed prior to the the fileset that you want to install. (The fileset can not be installed before the prerequisite fileset.) [2]Corequisite (Coreq) fileset(s) must be available to be installed when the fileset that you want to install is installed. (The order in which the filesets are installed is not important.) You can not deinstall one fileset with deinstalling others that it coreqs, or that coreq it. [3]Filesets that instreq other filesets will only be installed if the instreq'ed fileset is installed or available for installation. The fileset that is instreq'ed has no dependency upon the fileset instreq's it. (The order in which the filesets are installed is not important.) The fileset that instreq'ed another can be removed. The fileset that was instreq'ed can not be removed without removing the one that instreq'ed it.		

To use the **dce.tools.appdev.adt** fileset for building DCE applications, the following filesets or equivalent options must be installed:

bos.adt.syscalls
System Calls Application Development Toolkit

bos.adt.includes
Base Application Development Include Files

bos.adt.lib
Base Application Development Libraries

XlC.rte
C Set ++ AIX Application Runtime

Installing DCE 2.2

This section discusses DCE 2.2 installation.

Software Processes to Stop

If you are upgrading an existing installation, run **dce.clean all** to stop any running DCE/DFS processes. Also, manually shut down any applications that run on DCE/DFS. If you are running DFS, you must reboot your system to completely shut down DFS.

Running the Easy Installation Program

With the AIX operating system, you can install software more easily by using software bundles. A software bundle contains a list of software products that are suited for a particular use. The following procedure shows how to install DCE for AIX using this feature. It can be run either at the system console or remotely and run either under X Windows or from an ASCII terminal.

1. Log in as root.
2. Enter:

   ```
   smit easy_install_bundle
   ```
3. Specify the installation device or directory for the installation media by pressing **PF4** to display a list. Select the input device you want.
4. Press **Enter**.
5. Select **Media-defined**.
6. Press **Enter**.
7. Press **Enter** again. The DCE Bundles are installed into **/usr/sys/inst.data/sys_bundles**.
8. Press **PF3** to cancel.
9. Press **F4** to get the new list of software bundles to install.

   App-Dev
   DCE-CDS
   DCE-Client
   DCE-Management
   DCE-Security
   DCE-Starter
   DCE-Tools
   Media-Defined
   Pers-Prod

   See Table 3 on page 73 for the content of each DCE bundle selection.
10. Select the ones that you want to install.
11. Press **Enter**.
12. Press **Enter** again.

Table 3. DCE Software Bundles

Software Bundle	Bundle Name	Name and Filesets
DCE-CDS	DCE-CDS.bnd	**CDS Bundle** dce.compat.cds.smit dce.cds.rte
DCE-Client	DCEClient.bnd	**DCE Client Bundle** dce.client.core.rte dce.xdsxom.rte dce.pthreads.rte dce.compat.client.core.smit dce.client.dfs.rte dce.dfs_server.rte dce.compat.dfs_server.smit dce.compat.client.dfs.smit
DCE-Management	DCE-Management.bnd	**DCE Management Bundle** dce.sysmgmt.ems.rte dce.sysmgmt.snmpagt.rte dce.compat.sysmgmt.ems.smit dce.compat.sysmgmt.snmpagt.smit dce.web.secure.rte dce.web.secure.dat dce.web.admin.rte dce.web.admin.dat dce.compat.web.admin.smit
DCE-Security	DCE-Security.bnd	**Security Bundle** dce.security.rte dce.compat.security.smit dce.client.core.rte.security

Table 3. DCE Software Bundles (continued)

Software Bundle	Bundle Name	Name and Filesets
DCE-Starter	DCE-Starter.bnd	**DCE Starter Bundle** dce.client.core.rte dce.xdsxom.rte dce.pthreads.rte dce.compat.client.core.smit dce.client.dfs.rte dce.dfs_server.rte dce.compat.client.dfs.smit dce.compat.dfs_server.smit dce.security.rte dce.cds.rte dce.edfs.rte dce.compat..security.smit dce.compat.cds.smit dce.compat.edfs.smit
DCE-Tools	DCE-Tools.bnd	**DCE Tools Bundle** dce.tools.admin.rte dce.tools.appdev.adt

Special Installation Instructions

For information about installation procedures, see the *RISC System/6000 Installation Guide* which you received with your AIX Operating System. This book contains information on the **installp** command.

Migrating an AIX DCE Cell to DCE 2.2 for AIX

Because DCE 2.2 for AIX is dependent upon AIX 4.1.5 or higher, one of these versions must be installed on your machines to migrate from DCE 1.3, 2.1, or 2.1 + PTFs for AIX to DCE 2.2 for AIX. You can do this migration without a reconfiguration of your existing DCE cell by using the following procedures. You are not required to migrate your machines in a specific order, but please pay close attention to the limitations on DCE Security server functionality as described in Step 3 on page 76, **Migrating DCE Security Replicas**. Read this entire section before beginning the migration procedure.

1. **Before Migrating:**
   a. In DCE 2.2 for AIX, each workstation in a DCE cell keeps configuration information about the DCE clients and servers running on the local machine. This information is stored locally in the **dced** server configuration database.

      During migration, the migration commands attempt to add entries for the currently configured servers to the configuration database. In order for the migration to succeed, however, the machine context (hosts/*dce_hostname*/self) requires the necessary permissions on the server configuration database to insert entries.

      Before you attempt to migrate a machine to DCE 2.2 for AIX, you must ensure that the machine context has control, read, insert, and insert-privileged permissions on the local machine's server configuration ACL

      You can verify this by running the following command:

      ```
      dcecp -c acl show /.:/hosts/dce_hostname/config/srvrconf
      ```

      where is the DCE hostname of the machine to be migrated.

      The output of this command should resemble this:

      ```
      {unauthenticated -r--}
      {user hosts/dce_hostname/self criI}
      {group subsys/dce/dced-admin cri-}
      {any_other -r--}
      ```

      The machine context must have all the permissions as listed above. If the account does not have these permissions, you may run one of the following commands to grant the required permissions. You must first login as the cell administrator or any other account that has the permissions to modify this ACL.

      If an entry does not exist for the self account:

      ```
      dcecp -c acl modify /.:/hosts/dce_hostname/config/srvrconf -add {user hosts/dce_hostname/self criI}
      ```

      If an entry does exist but is not complete:

      ```
      dcecp -c acl modify /.:/hosts/dce_hostname/config/srvrconf -change {user hosts//self criI}
      ```

      Note: If the **dced** databases have been reinitialized since installing the **dce.client.core.rte** fileset version 2.1.0.15 or the machine was reconfigured into a DCE cell after installing the **dce.client.core.rte** version 2.1.0.15, the appropriate ACLs should already be set.

   b. In case you need to recover your pre-migration DCE configuration, back up all data below the directories and subdirectories:

```
/var/dce
/krb5
/etc/dce
```

c. Install AIX 4.1.5 or higher, including the PTFs which are prerequisites for DCE. These prerequisites are listed in the *IBM DCE for AIX, Version 2.2: Release Notes*. Use the **Migration** version of AIX Install.

2. **Migrating DCE Clients:**

   a. Stop DCE. See "Stopping DCE and DFS Daemons" on page 132 for information on stopping DCE.

   b. Install DCE 2.2 for AIX. Choose the same server and client packages that you had installed for your previous level of DCE for AIX on this machine.

   c. Start DCE/DFS by running **start.dce**. **start.dce** will invoke **migrate.dce** to migrate all DCE configuration data to the DCE 2.2 for AIX format. Because AIX Security Integration (**dceunixd**) was not supported by previous configuration tools, it will be migrated only if it can be detected in the **/etc/inittab** file. If **start.dce all** is specified, DFS data will be migrated by **migrate.dfs**.

3. **Migrating DCE Security Replicas:**

   DCE Security replica servers can be migrated using the steps documented in Step 2, *Migrating DCE Clients*. We recommend that you migrate all security replicas in your cell prior to enabling DCE 2.2 for AIX function on your master security server. When planning your migration, keep the following limitations in mind:

   a. If security replicas are migrated prior to the migration of the master security server, they will run with only your previous level of DCE for AIX function enabled. When the DCE 2.2 for AIX function is enabled on the security master using the **dcecp** command (given in Step c on page 77 under *Migrating the DCE Security Master*), these security replica servers will also enable the DCE 2.2 for AIX function.

   b. If the DCE 2.2 for AIX function is enabled on the master security server prior to the migration of all security replicas, any replicas which are running your previous level of DCE for AIX will be shut down. These security replicas cannot support DCE 2.2 for AIX function.

4. **Migrating DCE CDS Servers:**

   a. Ensure that all CDS Master directory replicas located on this machine are replicated on at least one other CDS server machine in the cell. If you wish to support updates to these CDS directories during the migration process, move these master directory replicas to another CDS server.

   b. Perform the tasks in Step 2, *Migrating DCE Clients*.

5. **Migrating the DCE Security Master:**

a. To minimize the impact to ongoing cell operations, ensure that at least one Security Server replica is running before you commence. This will support continuing security server **query** operations, though **update** operations will not be supported during the time the Master Security server is down.

   If the machine which is your security master server is also a CDS server, ensure that all CDS Master directory replicas located on this machine are replicated on at least one other CDS server machine in the cell. If you wish to support updates to these CDS directories during the migration process, move these master directory replicas to another CDS server.

b. Perform the tasks documented in Step 2 on page 76, *Migrating DCE Clients.*

   At this point in the migration process, all your previous level of DCE for AIX functions remain operable, but DCE 2.2 for AIX functions are not yet enabled.

c. Enable DCE 2.2 for AIX function, by executing the following command:

   ```
   /usr/bin/dcecp -c registry modify -version {secd.dce.1.2.2}
   ```

   It is recommended that you issue this command only after all security replica servers in your cell have been migrated to DCE 2.2 for AIX.

d. After you have migrated the Master Security Server, you need to validate any intercell accounts that exist in the DCE registry. This can be done by using the following command while logged in as the cell administrator:

   dcecp -c account modify krbtgt/*cell_name* **-change {acctvalid yes}**

   Where *cell_name* is the name of the foreign cell. If you do not validate these accounts, intercell access from non-AIX OSF 1.2.2 clients to the foreign cell will fail.

6. **Migrating DTS Servers**

   To correctly migrate DTS servers, follow the tasks described in 2 on page 76 , *Migrating DCE Clients.* Note that any time providers in use on the system will not be recognized by the migration tool. To continue using a time provider, it may be necessary to manually reconfigure it after the migration is completed.

7. **Migrating DFS Clients or Servers**

   After the DCE core services on your DFS client or server are migrated, you can bring up DFS using **start.dfs** without any additional configuration. DCE LFS aggregates which were on your DFS servers prior to the AIX Migration installation can be reused with DCE 2.2 for AIX.

Uninstalling DCE 2.2

Before uninstalling DCE for AIX, Version 2.2, you must unconfigure your machine. See “Unconfiguring DCE and DFS Components” on page 122 for information about unconfiguration.

At the SMIT **Maintain_Software** panel:

1. Select **Remove Software Products**
2. Select **The Software to Remove**

   Enter the name of the software you want to uninstall. **F4** will display a list of all the installed software.
3. Select **OK** or **Do**.

Suggested Reading

For information about AIX installation procedures, see the *RISC System/6000 Installation Guide* , which you received with your AIX Operating System.

For information on configuring a DCE cell, see the “Configuring DCE and DFS” on page 81 and the **config.dce** and **config.dfs** commands in the *IBM DCE for AIX, Version 2.2: Administration Commands Reference* and in the *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference* respectively.

For information about unconfiguring individual DCE components, see the **unconfig.dce** and **unconfig.dfs** commands in the *IBM DCE for AIX, Version 2.2: Administration Commands Reference*and in the *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference* respectively.

For information on configuring and unconfiguring DCE Web Utilities, see the **mkdceweb** and **rmdceweb** commands in the *IBM DCE for AIX, Version 2.2: Administration Commands Reference.*

Part 3. Configuring, Starting, and Stopping DCE 2.2 for AIX

Chapter 4. Configuring DCE 2.2 for AIX Servers and Clients

Configuring DCE and DFS

The following sections describe creating and configuring a DCE cell:

- "Overview of Configuration"
- "Initial Cell Configuration" on page 88
- "Further Cell Configuration" on page 101
- "DFS Configuration" on page 110
- "Unconfiguring DCE and DFS Components" on page 122
- "Chapter 5. Starting and Stopping DCE 2.2 for AIX" on page 129

These sections include server and client components for the following DCE services: Security Service, Cell Directory Service (CDS), Distributed Time Service (DTS), Remote Procedure Call (RPC), Global Directory Agent (GDA), and Distributed File System (DFS).

For information on setting up the intercell environment, managing intercell naming, and administering a multicell environment, see the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components* .

Overview of Configuration

The configuration of a DCE cell occurs in two phases. During the first phase, or *initial cell configuration*, certain tasks must be performed to initialize the cell. During the second phase, generic tasks can be performed to configure (or reconfigure) additional features into the cell.

A DCE cell requires the following components:

- One Security server
- One CDS server

It is recommended that there also be at least one DTS server (although three or more DTS servers are preferred for accuracy of time synchronization).

The Security and CDS servers must be configured to initialize any cell. After the cell is up and running, you generally will not have to repeat any of these configuration tasks.

Additional components that can be configured into a cell are the following:

- DCE and DFS clients
- Secondary CDS servers
- Replica Security Servers
- Audit Services
- Global Directory Agents (GDAs)
- DTS Servers
- DFS servers
  - System Control machine
  - Fileset Database machine
  - File Server machine
  - Backup Database machine
  - Fileset Replication Server machine.
- DCE NFS to DFS Authenticating Gateway for AIX
- Simple Network Management Protocol (SNMP)
- Event Management Service (EMS)
- Password Strength Server
- Security Integration (**dceunixd**)

The configuration of these additional components is a task you can perform throughout the lifetime of the cell after initialization.

Keep the following items in mind when you are configuring a cell:

- For better performance and reliability install the Master Security server and the Initial CDS server on different machines.
- Clients can be configured in one of three ways:

  Split Configuration

  This type of configuration is used when the DCE cell administrator is unlikely to have root user access to every machine in the cell. It is comprised of two distinct sets of operations:

  admin This type of configuration updates the namespace and security registry with information about the new client. The cell administrator must run the config.dce command from a machine within the existing cell. It can not be run from the new client machine. The cell administrator does not need root user authority to run the admin portion of configuration.

  local This type of configuration creates the necessary files on the local machine and starts the daemons for the new client. The admin part of config.dce must have been run first or

the local configuration will fail when trying to contact the cell. The user must have root authority on the machine, but does not need to have any authority in the DCE cell.

Full Configuration
This type of configuration is the default. Full configuration includes both admin and local configuration steps. The DCE cell administrator must have root authority on the local machine being configured into the cell.

Slim Client Configuration
This type of configuration can be used when the client system does not offer DCE services to other systems in the cell. No admin configuration is required for a slim client. It also reduces the amount of memory needed by the client.

- Before configuring a machine into a cell, make sure that the machine's clock is within five minutes of the cell's master Security server's clock. If the machine's clock is skewed more than five minutes, authentication errors may result, and configuration may fail. If you have already configured at least one DTS server in the cell, you can use the **-sync_clocks** flag to perform the synchronization for you automatically.

  Note: When configuring DFS Fileset Database machines and DFS Backup Database machines, the clocks on these machines must be within 10 seconds of each other.
- If you want to reconfigure a particular component (or an entire machine) with new parameters, you must unconfigure it to remove the existing configuration before setting up the new configuration.
- To enable intercell communication, you must also register the cell's name into a global directory, such as the Domain Name System (DNS). For information on the intercell environment, see the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components*.
- You can perform initial and additional configuration tasks using System Management Interface Tool (SMIT). SMIT uses interactive menus (rather than a command-line interface) to guide users through configuration and other system management tasks. The following sections provide step-by-step procedures for cell configuration using SMIT.

DCE 2.2 for AIX also provides the following commands to perform these same configuration tasks at the command line:

chpesite
Updates the **pe_site** file, which contains the addresses of the security servers that you use.

clean_up.dce
Cleans up recreatable database files, cache files, cred files. Is intended to be used if problems are encountered when trying to start DCE.

config.dce
Configures and starts DCE components. This command provides for a *split configuration of clients*. Administrative configuration and local configuration can be performed separately. See "Further Cell Configuration" on page 101 for more information.

config.dfs
Configures and starts DFS components. See "Further Cell Configuration" on page 101 for more information.

migrate.dce
Migrates DCE configuration data from previous releases for use with the current release. There is no need to reconfigure when installing a new release of DCE.

migrate.dfs
Migrates DFS configuration data from previous releases for use with the current release. There is no need to reconfigure when installing a new release of DFS.

mkbutc.dfs
Sets up the BackUp Tape Controller.

mkdceweb
Configures DCE Administration and DFS Web Secure or both into a Netscape FastTrack 2.01 or Enterprise 2.01 server.

mkfilesys.dfs
Registers and exports JFS, DCE LFS, and CD-ROM file systems on a DFS File Server machine.

mkreg.dce
Adds information about a DCE cell into the DOMAIN namespace.

newaggr
Formats AIX logical volumes as LFS aggregates.

rmbutc.dfs
Removes the setup of a BackUp Tape Controller.

rmdceweb
Unconfigures DCE Administration and DFS Web Secure or both from a Netscape FastTrack 2.01 or Enterprise 2.01 server.

rmfilesys.dfs
Detaches and unregisters JFS, DCE LFS, and CD-ROM file systems on a DFS File Server machine.

rmreg.dce
Removes information about a DCE cell from the DOMAIN namespace (DNS).

show.cfg
Displays the local host's DCE or DFS configuration. The **dce** and **dfs** options allow display of only DCE or DFS information

start.dce
Starts the configured DCE components. This command makes sure that all components are started in the correct order.

start.dfs
Starts the configured DFS components. This command makes sure that all components are started in the correct order.

startnfs.dfs
Starts the DCE NFS to DFS Authenticating Gateway for AIX, ensures that the daemons are running, and loads the kernel extension.

stop.dce
Stops the configured DCE components. This command makes sure that all components are stopped in the correct order.

stop.dfs
Stops the configured DFS components. This command makes sure that all components are stopped in the correct order.

unconfig.dce
Removes configurations of DCE components. This command provides for a *split unconfiguration*, with which administrative configuration and local configuration can be performed separately. See "Further Cell Configuration" on page 101 for more information.

unconfig.dfs
Removes configurations of DFS components. This command provides for a *split unconfiguration*, with which administrative configuration and local configuration can be performed separately. See "Further Cell Configuration" on page 101 for more information.

For detailed information on these commands, refer to the *IBM DCE for AIX, Version 2.2: Administration Commands Reference* and the *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference*.

User-Supplied Commands

The DCE 2.2 for AIX config/unconfig/start/stop code now provides support for user-supplied commands. User-supplied commands can be executed before or after, or before and after configuration, unconfiguration, start and stop of both DCE and DFS. The intent of this support is to allow you to run your

own commands without having to modify the scripts that are shipped with the DCE and DFS products. When future releases of these products are installed, your user- supplied commands will automatically run with the new releases.

Perform the following:

Write your command to do what you need. When executed, the configuration commands,(**config.dce**, **unconfig.dce**, **start.dce**, **stop.dce**, **config.dfs**, **unconfig.dfs**, **start.dfs**, and **stop.dfs**), set the environment variable, **"callers_cmd_line"**, (including all the parameters with the exception of the cell administrator's password) to the command line. For example, when configuring DCE, if the command executed is:

```
"config.dce -cell_name mycellname -admin_pwd -dce-
sec_srv cds_srv"
```

The **callers_cmd_line** environment variable is set to:

```
"-cell_name mycellname -admin_pwd <****>
sec_srv cds_srv"
```

This environment variable may be useful to your command script.

Create the file **/opt/dcelocal/tcl/user_cmd.tcl**. This file should contain the appropriate subset of the following entries:

For DCE:

- **set pre_config_dce** — the " full path to your pre-DCE configuration command and any arguments"
- **set post_config_dce** — the "full path to your post-DCE configuration command and any arguments"
- **set pre_unconfig_dce** — the "full path to your pre-DCE unconfiguration command and any arguments"
- **set post_unconfig_dce** — the "full path to your post-DCE unconfiguration command and any arguments"
- **set pre_start_dce** — the "full path to your pre-DCE start command and any arguments"
- **set post_start_dce** — the "full path to your post-DCE start command and any arguments"
- **set pre_stop_dce** — the "full path to your pre-DCE stop command and any arguments"
- **set post_stop_dce** — the "full path to your post-DCE stop command and any arguments"

For DFS:

- **set pre_config_dfs** — the “full path to your pre-DFS configuration command and any arguments”
- **set post_config_dfs** — the “full path to your post-DFS configuration command and any arguments”
- **set pre_unconfig_dfs** — the “full path to your pre-DFS unconfiguration command and any arguments”
- **set post_unconfig_dfs** — the “full path to your post-DFS unconfiguration command and any arguments”
- **set pre_start_dfs** — the “full path to your pre-DFS start command and any arguments”
- **set post_start_dfs** — the “full path to your post-DFS start command and any arguments”
- **set pre_stop_dfs**— the “full path to your pre-DFS stop command and any arguments”
- **set post_stop_dfs** — the “full path to your post-DFS stop command and any arguments”

Note: Use # to include a comment on its own line. Use ;# to include a comment on a line of code.

The configuration, unconfiguration, start, and stop code will look for the **/opt/dcelocal/tcl/user_cmd.tcl** file and the following variable names:

pre_config_dce	**pre_unconfig_dce**	**pre_start_dce**	**pre_stop_dce**
post_config_dce	**post_unconfig_dce**	**post_start_dce**	**post_stop_dce**
pre_config_dfs	**pre_unconfig_dfs**	**pre_start_dfs**	**pre_stop_dfs**
post_config_dfs	**post_unconfig_dfs**	**post_start_dfs**	**post_stop_dfs**

Examples:

```
#Set some environment variables before configuring DCE
set pre_config_dce "/usr/bin/set_env_vars"

#The following command runs the App XYZ config command
#App XYZ must be configured after DCE
set post_config_dce "/usr/bin/APP_XYZ_config -arg1 arg1_value -arg2 arg2_value"

#The following command runs the App XYZ start command
#App XYZ must start after DCE
set post_start_dce "/usr/bin/APP_XYZ_start"

#Stop App ABC before stopping DFS
set pre_stop_dfs "/usr/bin/APP_ABC_stop"
```

Environment Variables

Environment variables are variables used by DCE that customers can set themselves. See the *IBM DCE for AIX, Version 2.2: Administration Guide—Introduction* for more information about DCE environment variables.

Initial Cell Configuration

To initialize a cell, you must perform these basic tasks in order:

1. Configure the master Security server machine. See "Configuring the Master Security Server".
2. Configure the initial CDS server machine. See "Configuring the Initial CDS Server" on page 90.
3. Configure a CDS client on the master Security server. See "Configuring a CDS Client on the Master Security Server" on page 100.

In the procedures that follow, ensure that the *dce_hostname* of each machine is unique within the cell. The *dce_hostname* is the name that is listed in the hosts directory (**hosts/***dce_hostname*) in the namespace. The **config.dce** command allows you to assign a *dce_hostname* independent of a machine's host name on the network. By default the host name of the machine is used.

Attention: If you attempt to configure two machines that have the same *dce_hostname*, you will have to unconfigure and reconfigure DCE on both machines. If one of these machines is either the Security server or the initial CDS server, you will have to unconfigure and reconfigure DCE on *every* machine in the cell.

The following sections provide detailed procedures for performing these initial configuration tasks using SMIT. (See the *IBM DCE for AIX, Version 2.2: Administration Commands Reference* for information on commands that you can use to perform these same configuration tasks at the command line.)

Configuring Servers

This section discusses the following:

- "Configuring the Master Security Server"
- "Configuring the Initial CDS Server" on page 90

Configuring the Master Security Server

To configure the master Security server for a cell, perform the following steps on the machine that is designated as the master Security server:

1. As root, start SMIT with the **mkdcesrv** fastpath:

   ```
   smit mkdcesrv
   ```

   or perform the following sequence of SMIT menu options:

```
1. Communications Applications and Services
2. DCE (Distributed Computing Environment)
3. Configure DCE/DFS
4. Configure DCE/DFS Servers
```

2. Select the **SECURITY Server** option.
3. Select the **primary** option.
4. At the **CELL name** prompt, enter the name of the cell. For each cell, the first time you run this menu and enter a name at this prompt, you establish the cell name. You will use the cell name later in other configuration menus.

   Note: The cell name cannot be changed during the lifetime of the cell.
5. If you do not want to use the default *cell_admin*, enter the name of the cell administrator's account at the **Cell ADMINISTRATOR's account** prompt. If you do not use the default *cell_admin*, however, you will have to respecify the name of the cell administrator's account again whenever you perform configuration tasks in the future.
6. Select the *dce_hostname* for this machine in the **Machine's DCE HOSTNAME** field. If no name is selected, the TCP/IP hostname, including domain, will be used.
7. If you want to merge your current **/etc/passwd** and **/etc/group** files into your new DCE registry, you may encounter UNIX ID conflicts. To avoid these conflicts, enter new values (if necessary) in the appropriate fields for the starting point and the maximum value for UNIX IDs assigned to principals, groups, and organizations. The defaults are the values displayed. Because UNIX IDs cannot be changed once the Security Service has created accounts, you should set the values for the starting point and the maximum value for UNIX IDs now, when the registry is first created.
8. Select yes or no in the Start daemons at System restart field to indicate that the DCE daemons should or should not be automatically started at system reboot.
9. Select the protocols that DCE should be configured with in the Protocol field. Once selected, the same protocols must be used for subsequent configurations.
10. Select the security server name for this machine in the Security Server Name field. If no name is selected, the DCE hostname will be used.
11. Select **Do**.
12. When prompted, enter the password to be assigned to the initial account created in the registry database. Make a note of the password for the cell administrator's account, because it is required to perform other configuration tasks. This password is also assigned to the DCE account for root that is granted privileged authority by DFS.

At this point, **dced** and the master Security server are configured on the machine. You can return to this machine later to configure CDS and DTS.

Configuring the Initial CDS Server

There can be only one *initial* CDS server for each cell. To configure the initial CDS server for a cell, perform the following steps on the machine that is designated as the initial CDS server:

1. As root, start SMIT with the **mkdcesrv** fastpath:

   ```
   smit mkdcesrv
   ```

   or perform the following sequence of SMIT menu options:

   ```
   1. Communications Applications and Services
   2. DCE (Distributed Computing Environment)
   3. Configure DCE/DFS
   4. Configure DCE/DFS Servers
   ```

2. Select the **CDS (Cell Directory Service) Server** option.
3. Select the **initial** option.
4. If this machine is not the master Security server:
   a. At the **CELL name** prompt, enter the name of the cell.
   b. At the **SECURITY Server** prompt, enter the TCP/IP hostname or IP address of the machine that is the master Security server. (The TCP/IP hostname or IP address is not necessarily the same as the *dce_hostname*.)

   If this machine is the master Security server, these fields are automatically filled in with the proper values.
5. If you are not using the default *cell_admin*, enter the name of the cell administrator's account at the **Cell ADMINISTRATOR's account** prompt.
6. If the cell will contain multiple LANs and require the use of global DTS servers, enter the name of the LAN profile this machine should use at the **LAN PROFILE** prompt. However, if this is the same machine as the Security server, the field will already be filled in.
7. Select the *dce_hostname* for this machine in the **Machine's DCE HOSTNAME** field. If no name is selected, the TCP/IP hostname, including domain, will be used.
8. Select **yes** or **no** in the **Start daemons at System restart** field to indicate that the DCE daemons should or should not be automatically started at system reboot.
9. In the **Protocol** field, select the protocols with which DCE should be configured. Once selected, the same protocols must be used for subsequent configurations.
10. Select **Do**.

11. When prompted, enter the cell administrator's password.

At this point, RPC, the initial CDS server, and a CDS clerk are configured on the machine. (If this machine is the master Security server, only the initial CDS server and a CDS clerk are actually configured in this section.) You can return to this machine later to configure DTS.

Note that a clearinghouse is automatically created when you configure a CDS server. Although it is possible to define multiple clearinghouses for a CDS server, you should have only one during normal operation. If you are moving a clearinghouse from one CDS server to another, however, you can temporarily define a second clearinghouse on the original server. See the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components* for more information on moving a clearinghouse.

Configuring Clients

This section discusses the following:

Typically, you need to configure many clients into a DCE cell. Configuring clients entails two distinct sets of operations:

- Tasks that require *cell administrator* authority within the DCE cell
- Tasks that require *root user* authority on the machine that is to be configured as a DCE client.

These tasks are separated into a *split configuration of clients* because a DCE cell administrator is unlikely to have root user access to every machine in a cell.

Configuring DCE/DFS Clients

The DCE and DFS clients can be configured in one of three ways: Split, Full, or Slim.

Split Client configuration for Security clients (**sec_cl**) and CDS clients (**cds_cl**) is a two-part process. (The cell administrator may not have root access to the client machines, or the root user may not have cell administrator access.) The two parts are the following:

- The cell administrator runs the **admin** portion from any machine in the cell to update the CDS namespace and security registry.

- The root user of the client machine runs the **local** portion to create necessary files and to start client daemons for all client components.

Admin Client Configuration

To do the **admin** portion of configuring a DCE client, the cell administrator performs the following steps from any machine in the cell:

1. Start SMIT with the **mkdceclient** fastpath:

   ```
   smit mkdceclient
   ```

   or perform the following sequence of SMIT menu options:

   ```
   1. Communications Applications and Services
   2. DCE (Distributed Computing Environment)
   3. Configure DCE/DFS
   4. Configure DCE/DFS Clients
   ```

2. Select **admin only configuration for another machine**.
3. Enter the names of the DCE clients you want to configure. For **admin** configuration, the only two selections are **sec_cl** and **cds_cl**. All other client configuration is done on the client machine and does not require cell administrator authority.
4. If you are not using the default *cell_admin*, enter the name of the cell administrator's account at the **Cell ADMINISTRATOR's account** prompt.
5. If the cell contains multiple LANs and requires the use of global DTS servers, enter the name of the LAN profile the client machine should use at the **LAN PROFILE** prompt.
6. Identify which machine is being configured as a client by entering its TCP/IP hostname or IP address in the **Client Machine's DCE IDENTIFIER** field.
7. Select the *dce_hostname* for the client machine in the **Client Machine's DCE HOSTNAME** field. If no name is selected, the TCP/IP hostname, including domain from Step 6, will be used.Select **Do**.

At this point, the namespace entries and security registry database have been updated. It is now necessary to run the **local** portion of configuration to complete the process.

Local Client Configuration

To do the **local** portion of configuring a DCE/DFS client (after the **admin** portion is completed), perform the following steps as root on the client machine:

1. Start SMIT with the **mkdceclient** fastpath:

   ```
   smit mkdceclient
   ```

or perform the following sequence of SMIT menu options:

```
1. Communications Applications and Services
2. DCE (Distributed Computing Environment)
3. Configure DCE/DFS
4. Configure DCE/DFS Clients
```

2. Select **local only configuration for this machine**.
3. Ensure that the **CELL name** field is filled in with the appropriate values.
4. Enter the names of the DCE clients you want to configure. For local configuration **rpc**, **sec_cl**, **cds_cl**, **audit**, **snmp**, and **dfs_cl** can be selected.
5. If the machine is on a separate LAN from any CDS server and cannot send broadcast packets to a CDS server or if you are not sure if the machine is on a separate LAN, enter the TCP/IP hostname or IP address of the Master Security server at the **MASTER SECURITY SERVER** prompt.
6. If the machine is on a separate LAN from any CDS server and cannot send broadcast packets to a CDS server. or if you are not sure if the machine is on a separate LAN, enter the TCP/IP hostname or IP address of the CDS server at the **CDS Server (If in a separate network)** prompt.
7. Select the *DCE_hostname* for this machine at the **Machine"s DCE HOSTNAME** prompt. If no name is selected, the TCP/IP hostname, including the domain, will be used.
8. If the machine is on a separate LAN and you want the CDS client to rebroadcast the location of the CDS server, at the **Rebroadcast CDS Server Location** prompt, select **<F4>** to list the choices, then select **true**. The default is **false**.
9. If you want to start the DCE daemons at a system reboot, at the **Start daemons at System restart** prompt, select **<F4>** to list the choices, then select **false**. The default is **false**.
10. At the **Protocols** prompt, select the protocols you want to use for DCE configuration. Once selected, the same protocols must be used for subsequent configurations. If you will be configuring any DFS components on this machine, you must use the **udp** protocols.

    Note: Step 11, through Step 24 on page 95 apply only if you are configuring a DFS client (**dfs_cl**). For an AIX diskless machine, configure an in-memory DFS cache. For more information about the parameters, see **dfsd** in the *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference*.

11. For the **DFS CACHE on disk or in memory** field, select the location you prefer for the DFS client cache.
12. For the **DFS cache SIZE (in kilobytes)** field, enter the size to be used for the DFS client cache.

For an on-disk cache, this value should not exceed 85% of the disk space on the file system where the cache is to be located.

For an in-memory cache, this value should not exceed 25% of the machine's available memory.

13. In the **DFS cache DIRECTORY (if on disk)** field, specify the directory where the DFS client cache files should be kept. If you selected **memory** in Step 11 on page 93, this field is ignored.

    It is recommended that you create a separate file system for the DFS client cache if you are keeping it on disk (see "File Systems to Create and Mount" on page 61).

14. If you want to change the number of entries used for recording status on DFS files in the cache, change the value in the **Number cache status entries** field. The default is **300**.
15. If you want to change the number of backround daemons running on this machine, change the value in the **Number of Background daemons running on this machine** field. The default is **2**.
16. If you want to change number of backround daemons dedicated to servicing token revocation RPC requests from File exporters, change the value in the **Daemons servicing token revocation RPC requests** field. The default is **2**.
17. If you want to change the number of dcache entries in memory, change the value of **Number of dcache entries in memory** field. The default is **100**.
18. If you want to change the cache chunk size, change the value in the **Chunk Size** field. The default is **14** for memory cache or **15** for disk cache.
19. If you want to change the number of entries allocated for the Cache Manager's name lookup cache, change the value in the **Cache Manager lookup entries** field. The default is **256**.
20. If you want persistent requests, select **true**. The default is **false**.
21. If you want to change the timeout on the persistent requests, change the value in the **Time-out for persistent requests** field. The default is **86400** (seconds).
22. If you want to change the initial DCE RPC authentication level for communications between the cache manager and file servers within the same cell, change the value in the **Initial DCE RPC Authentication level - same cell** field. The default is **pkt**. Select **<F4>** to list the available protection levels.
23. If you want to change the minimum acceptable DCE RPC authentication level for communications between the cache manager and file servers

within the same cell, change the value in the **Minimum DCE RPC Authentication level - same cell** field. The default is **none**. Select **<F4>** to list the available protection levels.

24. If you want to change the initial DCE RPC authentication level for communications between the cache manager and file servers within foreign cells, change the value in the **Initial DCE RPC Authentication level-foreign cell** field. The default is **pkt_integ**. Select **<F4>** to list the available protection levels.
25. If you want to change the minimum acceptable DCE RPC authentication level for communications between the cache manager and file servers within the same cell, change the value in the **Minimum DCE RPC Authentication level-foreign cells** field. The default is **pkt**. Select **<F4>** to list the available protection levels.
26. If you want the local machine's clock to be synchronized before any components are configured, at the **Synchronized Clocks** prompt, select **<F4>** to list the choices, then select **true**. The default is **false**.
27. Enter the time server you want to use for synchronization at the **Time Server to Synchronize Clocks with** prompt. The time server can be any DTS server in the cell.
28. Select **Do**.

At this point, the selected clients are configured on the machine.

Full Client Configuration

If you are both the *cell administrator* and the *root user* of a machine currently being configured as a client, you can perform a **full client** configuration, which incorporates both the **admin** and **local** portions of configuration.

To perform the **full** configuring of a DCE/DFS client, take the following steps as root on your machine:

1. Start SMIT with the **mkdceclient** fastpath:

   ```
   smit mkdceclient
   ```

   or perform the following sequence of SMIT menu options:

   ```
   1. Communications Applications and Services
   2. DCE (Distributed Computing Environment)
   3. Configure DCE/DFS
   4. Configure DCE/DFS Clients
   ```

2. Select **full configuration for this machine**.
3. Ensure that the **CELL name** field is filled in with the appropriate values.
4. Enter the names of the DCE clients you want to configure. For full configuration all clients are available for selection.

5. If the machine is on a separate LAN from any CDS server and cannot send broadcast packets to a CDS server or if you are not sure if the machine is on a separate LAN, enter the TCP/IP hostname or IP address of the Master Security server at the **MASTER SECURITY SERVER** prompt.
6. If the machine is on a separate LAN from any CDS server and cannot send broadcast packets to a CDS server. or if you are not sure if the machine is on a separate LAN, enter the TCP/IP hostname or IP address of the CDS server at the **CDS Server (If in a separate network)** prompt.
7. Select the *DCE_hostname* for this machine at the **Machine's DCE HOSTNAME** prompt. If no name is selected, the TCP/IP hostname, including the domain, will be used.
8. If the machine is on a separate LAN and you want the CDS client to rebroadcast the location of the CDS server, at the **Rebroadcast CDS Server Location** prompt, select **<F4>** to list the choices, then select **true**. The default is **false**.
9. If you want to start the DCE daemons at a system reboot, at the **Start daemons at System restart** prompt, select **<F4>** to list the choices, then select **true**. The default is **false**.
10. At the **Protocols** prompt, select the protocols you want to use for DCE configuration. Once selected, the same protocols must be used for subsequent configurations. If you will be configuring any DFS components on this machine, you must use the **udp** protocols.

    Note: Step 11 through Step 23 on page 97 apply only if you are configuring a DFS client (**dfs_cl**). For more information about the parameters, see **dfsd** in the *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference* .

11. For the **DFS CACHE on disk or in memory** field, select the location you prefer for the DFS client cache.
12. For the **DFS cache SIZE (in kilobytes)** field, enter the size to be used for the DFS client cache.

    For an on-disk cache, this value should not exceed 85% of the disk space on the file system where the cache is to be located.

    For an in-memory cache, this value should not exceed 25% of the machine's available memory.
13. In the **DFS cache DIRECTORY (if on disk)** field, specify the directory where the DFS client cache files should be kept. If you selected **memory** in Step 11, this field is ignored.

    It is recommended that you create a separate file system for the DFS client cache if you are keeping it on disk (see "File Systems to Create and Mount" on page 61).

14. If you want to change the number of entries used for recording status on DFS files in the cache, change the value in the **Number cache status entries** field. The default is **300**.
15. If you want to change the number of backround daemons running on this machine, change the value in the **Number of Background daemons running on this machine** field. The default is **2**.
16. If you want to change number of backround daemons dedicated to servicing token revocation RPC requests from File exporters, change the value in the **Daemons servicing token revocation RPC requests** field. The default is **2**.
17. If you want to change the number of dcache entries in memory, change the value of **Number of dcache entries in memory** field. The default is **100**.
18. If you want to change the cache chunk size, change the value in the **Chunk Size** field. The default is **14** for memory cache or **15** for disk cache.
19. If you want to change the number of entries allocated for the Cache Manager's name lookup cache, change the value in the **Cache Manager lookup entries** field. The default is **256**.
20. If you want persistent requests, select **true**. The default is **false**.
21. If you want to change the timeout on the persistent requests, change the value in the **Time-out for persistent requests** field. The default is **86400** (seconds).
22. If you want to change the initial DCE RPC authentication level for communications between the cache manager and file servers within the same cell, change the value in the **Initial DCE RPC Authentication level - same cell** field. The default is **pkt**. Select **<F4>** to list the available protection levels.
23. If you want to change the minimum acceptable DCE RPC authentication level for communications between the cache manager and file servers within the same cell, change the value in the **Minimum DCE RPC Authentication level - same cell** field. The default is **none**. Select **<F4>** to list the available protection levels.
24. If you want to change the initial DCE RPC authentication level for communications between the cache manager and file servers within foreign cells, change the value in the **Initial DCE RPC Authentication level-foreign cell** field. The default is **pkt_integ**. Select **<F4>** to list the available protection levels.
25. If you want to change the minimum acceptable DCE RPC authentication level for communications between the cache manager and file servers within the same cell, change the value in the **Minimum DCE RPC Authentication level-foreign cells** field. The default is **pkt**. Select **<F4>** to list the available protection levels.

26. If you want the local machine's clock to be synchronized before any components are configured, at the **Synchronized Clocks** prompt, select **<F4>** to list the choices, then select **true**. The default is **false**.
27. Enter the time server you want to use for synchronization at the **Time Server to Synchronize Clocks with** prompt. The time server can be any DTS server in the cell.
28. Select **Do**.

Slim Client Configuration

Ensure that the **CELL name** field is filled in with the appropriate values.

Notes:

1. The cell administrator's password is not needed when configuring a Slim Client.
2. Only a DFS Client and Integrated Login can be configured with a Slim Client.

To do configure a DCE Slim Client perform the following steps as root on the client machine:

1. Start SMIT with the **mkdceclient** fastpath:

   ```
   smit mkdceclient
   ```

   or perform the following sequence of SMIT menu options:

   ```
   1. Communications Applications and Services
   2. DCE (Distributed Computing Environment)
   3. Configure DCE/DFS
   4. Configure DCE/DFS Clients
   ```

2. Select **Slim Client configuration for this machine**.
3. At the **CELL name** and **SECURITY Server** prompts, enter the names of the cell and the TCP/IP hostname or IP address of the master Security server for the cell.
4. Enter the names of the clients you want to configure. Select **<F4>** to view a list.
5. Enter the *dce_hostname* for this machine as assigned by the cell administrator in the **Client Machine DCE HOSTNAME** field. If no name was explicitly assigned, leave this field blank so that the default will be used. (The default is the full TCP/IP hostname, including the full domain name.)
6. If the machine is on a separate LAN from the initial CDS server and cannot send broadcast packets to it, enter the TCP/IP hostname or IP address of the initial CDS server at the **CDS Server (if in a separate network)** prompt. The CDS server can be either the initial CDS server or a secondary CDS server that is already configured. If you are not sure if it is

on a separate LAN, enter the TCP/IP hostname or IP address of a CDS server at the **CDS Server (if in a separate network)** prompt.

7. The value of the **Rebroadcast CDS Server Location** is ignored by the **config.dce** command because there is no CDS Client. At the **Rebroadcast CDS Server Location** prompt, select **<F4>** to list and then select either **true** or **false**.
8. If you want DCE/DFS start to start at system reboot, select **yes** at the **Start daemons at System restart** field.
9. Specify the protocols that should be used in the **Protocol** field.

   Note: Step 10, Step 11, and Step 12 apply only if you are configuring a DFS client (**dfs_cl**). For an AIX diskless machine, configure an in-memory DFS cache. For more information about the parameters, see **dfsd** in the *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference*.

10. For the **DFS CACHE on disk or in memory** field, select the location you prefer for the DFS client cache.
11. For the **DFS cache SIZE (in kilobytes)** field, enter the size to be used for the DFS client cache.

    For an on-disk cache, this value should not exceed 85% of the disk space on the file system where the cache is to be located.

    For an in-memory cache, this value should not exceed 25% of the machine's available memory.
12. In the **DFS cache DIRECTORY (if on disk)** field, specify the directory where the DFS client cache files should be kept. If you selected **memory** in Step 10, this field is ignored.

    It is recommended that you create a separate file system for the DFS client cache if you are keeping it on disk (see "File Systems to Create and Mount" on page 61).
13. If you want to change the number of entries used for recording status on DFS files in the cache, change the value in the **Number cache status entries** field. The default is **300**.
14. If you want to change the number of backround daemons running on this machine, change the value in the **Number of Background daemons running on this machine** field. The default is **2**.
15. If you want to change number of backround daemons dedicated to servicing token revocation RPC requests from File exporters, change the value in the **Daemons servicing token revocation RPC requests** field. The default is **2**.
16. If you want to change the number of dcache entries in memory, change the value of **Number of dcache entries in memory** field. The default is **100**.

17. If you want to change the cache chunk size, change the value in the **Chunk Size** field. The default is **14** for memory cache or **15** for disk cache.
18. If you want to change the number of entries allocated for the Cache Manager's name lookup cache, change the value in the **Cache Manager lookup entries** field. The default is **256**.
19. If you want persistent requests, select **true**. The default is **false**.
20. If you want to change the timeout on the persistent requests, change the value in the **Time-out for persistent requests** field. The default is **86400** (seconds).
21. If you want to change the initial DCE RPC authentication level for communications between the cache manager and file servers within the same cell, change the value in the **Initial DCE RPC Authentication level - same cell** field. The default is **pkt**. Select **<F4>** to list the available protection levels.
22. If you want to change the minimum acceptable DCE RPC authentication level for communications between the cache manager and file servers within the same cell, change the value in the **Minimum DCE RPC Authentication level - same cell** field. The default is **none**. Select **<F4>** to list the available protection levels.
23. If you want to change the initial DCE RPC authentication level for communications between the cache manager and file servers within foreign cells, change the value in the **Initial DCE RPC Authentication level-foreign cell** field. The default is **pkt_integ**. Select **<F4>** to list the available protection levels.
24. If you want to change the minimum acceptable DCE RPC authentication level for communications between the cache manager and file servers within the same cell, change the value in the **Minimum DCE RPC Authentication level-foreign cells** field. The default is **pkt**. Select **<F4>** to list the available protection levels.
25. Select **Do**.

At this point, the selected clients are configured on the machine.

Configuring a CDS Client on the Master Security Server

If you configured the master Security server and the initial CDS server on the same machine, you can skip this section because a CDS client was configured when you configured the initial CDS server.

Otherwise, to configure a CDS client on the master Security server, perform the following steps on the machine that is the master Security server:

1. As root, start SMIT with **mkdceclient** fastpath:

   ```
   smit mkdceclient
   ```

or perform the following sequence of SMIT menu options:

```
1. Communications Applications and Services
2. DCE (Distributed Computing Environment)
3. Configure DCE/DFS
4. Configure DCE/DFS Clients
```

2. Select **full configuration for this machine**.
3. At the **CLIENTS to configure** prompt, select **<F4>** to list and then select **cds_cl**. Select **Ok**.
4. Ensure that the **CELL name** and **SECURITY Server** fields are filled in with the appropriate values.
5. If the master Security server is on a separate LAN from the initial CDS server and cannot send broadcast packets to it, enter the TCP/IP hostname or IP address of the initial CDS server at the **CDS Server (if in a separate network)** prompt. (The TCP/IP hostname or IP address is not necessarily the same as the *dce_hostname*.) If you are not sure if it is on a separate LAN, enter the TCP/IP hostname or IP address of the initial CDS server at the **CDS Server (if in a separate network)** prompt.
6. If you are not using the default *cell_admin*, enter the name of the cell administrator's account at the **Cell ADMINISTRATOR's account** prompt.
7. If the cell contains multiple LANs and requires the use of global DTS servers, enter the name of the LAN profile this machine should use at the **LAN PROFILE** prompt.
8. Ensure that the Machine's **DCE HOSTNAME** field is filled in the appropriate name.
9. If this CDS client is on a separate LAN and you want it to rebroadcast the location of the CDS server, at the **Rebroadcast CDS Server Location** prompt, select **<F4>** to list and then select **true**.
10. All other fields should be filled in because the machine is already configured.
11. Select **Do**.
12. When prompted, enter the cell administrator's password.

At this point, a CDS client is configured on the machine.

Further Cell Configuration

After cell initialization is completed, you may have to perform additional configuration tasks on an ongoing basis as changes are made to the cell. For example, you may want a new machine to be added to the cell as a client. Or you may decide to configure a secondary CDS server to provide faster or more reliable access to the namespace.

Typically, you need to configure many clients into a DCE cell. Configuring clients entails two distinct sets of operations:

- Tasks that require *cell administrator* authority within the DCE cell
- Tasks that require *root user* authority on the machine that is to be configured as a DCE client.

These tasks are separated into a *split configuration of clients* because a DCE cell administrator is unlikely to have root user access to every machine in a cell.

The following sections provide detailed procedures for performing additional configuration tasks.

Configuring DTS Servers

To configure DTS local or global servers, perform the following steps on each machine designated as a DTS server:

1. As root, start SMIT with the **mkdcesrv** fastpath:

   ```
   smit mkdcesrv
   ```

   or perform the following sequence of SMIT menu options:

   ```
   1. Communications Applications and Services
   2. DCE (Distributed Computing Environment)
   3. Configure DCE/DFS
   4. Configure DCE/DFS Servers
   ```

2. Select the **DTS (Distributed Time Service) Server** option.
3. At the **Type of SERVER** prompt, select **<F4>** to list and then select the appropriate type of server. Note that a DTS server cannot be configured on the same machine as another DTS server or a DTS client.
4. At the **Type of COURIER** prompt, select **<F4>** to list and then select the appropriate type of courier.
5. Ensure that the **CELL name** field is filled in with the appropriate values.
6. If you are not using the default *cell_admin*, enter the name of the cell administrator's account at the **Cell ADMINISTRATOR's account** prompt.
7. If the machine is on a separate LAN from the initial CDS server and cannot send broadcast packets to it, enter the TCP/IP hostname or IP address of the Master Security server at the SECURITY Server prompt. If you are not sure if it is on a separate LAN, enter the TCP/IP hostname or IP address of the Master Security server at the SECURITY Server prompt.
8. If the machine is on a separate LAN from the initial CDS server and cannot send broadcast packets to it, enter the TCP/IP hostname or IP address of the initial CDS server at the **CDS Server (if in a separate network)** prompt. If you are not sure if the machine is on a separate LAN, enter the TCP/IP hostname or the IP address of the initial CDS server at the **CDS Server (if in a separate network)** prompt.

9. If the cell contains multiple LANs and requires the use of global DTS servers, enter the name of the LAN profile this machine should use at the **LAN PROFILE** prompt. (If this machine is the master Security server or the initial CDS server, this step is not necessary because a CDS client is already configured.) However, if this is the same machine as the Security server, the field will already be filled in.
10. Select the *dce_hostname* for this machine in the **Machine's DCE HOSTNAME** field. If no name is selected, the TCP/IP hostname, including domain, will be used.
11. If the machine is on a separate LAN and you want the CDS Client to rebroadcast the location of the CDS server, at the **Rebroadcast CDS Server Location** prompt select **<F4>** to list, then select **true**.
12. Select **true** or **false** in the **Start daemons at System restart** field to indicate that the DCE daemons should or should not be automatically started at system reboot.
13. In the **Protocol** field, select the protocols with which DCE should be configured. Once selected, the same protocols must be used for subsequent configurations.
14. Select **Do**.
15. When prompted, enter the cell administrator's password.
16. If there are less than three time servers configured in the cell, the following command should be used:

    ```
    dcecp -c dts modify -minservers n
    ```

    where *n* is the number of time servers in the cell.

    This prevents the logging of a warning message every time the server attempts to sync.

At this point, a DTS server is configured on the machine, along with **dced**, a Security client, and a CDS client which were configured as part of DCE client configuration.

Configuring a DTS Client on the Master Security Server or the Initial CDS Server

If you configured a DTS server on the same machine as the master Security server or the initial CDS server (or both), you can skip this section because DTS was started when you configured the DTS server.

Otherwise, to configure a DTS client on the master Security server and the initial CDS server, perform the following steps on those machines:

1. As root, start SMIT with the **mkdceclient** fastpath:

   ```
   smit mkdceclient
   ```

or select the following sequence of SMIT menu options:

1. **Communications Applications and Services**
2. **DCE (Distributed Computing Environment)**
3. **Configure DCE/DFS**
4. **Configure DCE/DFS Clients**

2. Select **full Configuration for this machine**.
3. At the **CLIENTS to configure** prompt, choose **<F4>** to list and select **dts_cl**. Then select **Ok**.
4. If you are not using the default *cell_admin*, enter the name of the cell administrator's account at the **Cell ADMINISTRATOR's account** prompt.

   All other fields should be automatically filled in with the appropriate values because of a previous configuration on the machine.
5. Select **Do**.
6. When prompted, enter the cell administrator's password.

   At this point, a DTS client is configured on the master Security server and initial CDS server machines, completing cell initialization.

Configuring Secondary CDS Servers

After you have configured an initial CDS server, you may want to configure one or more *secondary* CDS servers to provide faster or more reliable access to the namespace.

A Secondary CDS Server allows administrators to create replicas of CDS Directories for backup and availability purposes. When you configure a Secondary CDS Server, a replica of the root directory and its contents is automatically created.

The only child directory below the root that is automatically replicated into the new Secondary CDS Server is the **/.:/subsys/dce/sec** directory. This directory is replicated because it contains the binding information to locate the Master Security Server. This action increases accessibility to the Security Server even when the initial CDS Server is unavailable. See the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components* for information about CDS replicas and how to create them.

To configure a secondary CDS server, perform the following steps on each machine designated as a secondary CDS server:

1. If the machine is not already a DCE client, follow the steps outlined in "Configuring DCE/DFS Clients" on page 91 to configure it as a DCE client.
2. As root, start SMIT with **mkdcesrv** fastpath:

   ```
   smit mkdcesrv
   ```

   or perform the following sequence of SMIT menu options:

1. **Communications Applications and Services**
2. **DCE (Distributed Computing Environment)**
3. **Configure DCE/DFS**
4. **Configure DCE/DFS Servers**

3. Select the **CDS (Cell Directory Service) Server** option.
4. Select the **additional** option.
5. If you are not using the default *cell_admin*, enter the name of the cell administrator's account at the **Cell ADMINISTRATOR's account** prompt.
6. Because the machine is already configured as a DCE client, all other fields should be automatically filled in with the appropriate values. Select **Do**.
7. When prompted, enter the cell administrator's password.

At this point, **dced**, a secondary CDS server, a CDS client, and a DTS client are configured on the machine. When you configure a secondary CDS server, only the **root** and the **/.:/subsys/dce/sec** directories are replicated. See the *IBM DCE for AIX, Version 2.2: Administration Guide* for information on replicating other directories.

Configuring Security Replica Servers

A security replica server is a read-only copy of the master Security server. Advantages of using a security replica server include easing the load on the master Security server and preserving the cell in case the master Security server becomes disabled.

To configure a security replica server, perform the following steps on each machine designated as a security replica server:

1. If the machine is not already a DCE client, follow the steps outlined in "Configuring DCE/DFS Clients" on page 91 to configure it as a DCE client.
2. As root, start SMIT with **mkdcesrv** fastpath:

   ```
   smit mkdcesrv
   ```

   or perform the following sequence of SMIT menu options:

   1. **Communication Applications and Services**
   2. **DCE (Distributed Computing Environment)**
   3. **Configure DCE/DFS**
   4. **Configure DCE/DFS Servers**

3. Select the **SECURITY Server** option.
4. Select the **secondary** option.
5. If you are not using the default *cell_admin*, enter the name of the cell administrator's account at the **Cell ADMINISTRATOR's account** prompt.
6. If you want to give the Security Replica a name, enter your choice in the **Security Server name** field. If you do not specify a name, the default is

the *dce_hostname* of the machine. You should use the default unless you are completely sure that the name you specify is unique throughout the entire cell.

If the machine is already configured as a client, all other fields will be filled in.

7. Select **Do**.
8. When prompted, enter the cell administrator's password.

At this point, **dced**, a Security client, a Security Replica, and a CDS client are configured on the machine.

Configuring the Global Directory Agent

The Global Directory Agent (GDA) allows intercell communication by locating a foreign cell which has been registered into the Domain Naming System (DNS) global directory service. Only one GDA is required to be configured within the cell to allow intecell communication, but more can be configured to increase availabilty.

To configure the GDA on a machine, perform the following steps on the machine:

1. If the machine is not already a DCE client, follow the steps outlined in "Configuring DCE/DFS Clients" on page 91.
2. As root, start SMIT with **mkdcesrv** fastpath:

   ```
   smit mkdcesrv
   ```

   or perform the following sequence of SMIT menu options:

   ```
   1. Communications Applications and Services
   2. DCE (Distributed Computing Environment)
   3. Configure DCE/DFS
   4. Configure DCE/DFS Servers
   ```
3. Choose the **GDA (Global Directory Agent)** option.
4. If you are not using the default *cell_admin*, enter the name of the cell administrator's account at the **Cell ADMINISTRATOR's account** prompt.
5. Because the machine is already configured as a DCE client, all other fields should be automatically filled in with the appropriate values. Select **Do**.
6. When prompted, enter the cell administrator's password.

At this point, the GDA is configured on the machine. To enable intercell communication, see the information on the intercell environment in the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components*. Also, see the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components* for information on registering a cell globally.

Configuring EMS Servers

To configure an EMS server perform the following steps:

1. If the machine is not already a DCE client, follow the steps outlined in "Configuring DCE/DFS Clients" on page 91.
2. As root, start SMIT with the **mkdcesrv** fastpath:

   ```
   smit mkdcesrv
   ```

   or select the following sequence of SMIT menu options:

   ```
   1. Communications Applications and Services
   2. DCE (Distributed Computing Environment)
   3. Configure DCE/DFS
   4. Configure DCE/DFS Servers
   ```
3. Choose the **EMS Server** option.
4. Because the machine is already configured as a DCE client, all other fields should be automatically filled in with the appropriate values. You will not be prompted for the cell administrator's password when the DCE client is already configured.
5. Select **Do**.

At this point, an EMS server is configured on the machine, along with **dced**, a Security client, and a CDS client which were configured as part of DCE client configuration.

Configuring SNMP Servers

To configure an SNMP server perform the following steps:

1. If the machine is not already a DCE client, follow the steps outlined in "Configuring DCE/DFS Clients" on page 91.
2. As root, start SMIT with the **mkdcesrv** fastpath:

   ```
   smit mkdcesrv
   ```

   or select the following sequence of SMIT menu options:

   ```
   1. Communications Applications and Services
   2. DCE (Distributed Computing Environment)
   3. Configure DCE/DFS
   4. Configure DCE/DFS Servers
   ```
3. Choose the **SNMP Server** option.
4. Because the machine is already configured as a DCE client, all other fields should be automatically filled in with the appropriate values. You will not be prompted for the cell administrator's password when the DCE client is already configured.
5. Select **Do**.

At this point, an SNMP server is configured on the machine, along with **dced**, a Security client, and a CDS client which were configured as part of DCE client configuration.

Configuring DCE 2.2 for AIX Security Integration

Use the following steps to configure a system for security integration operations:

1. If the machine is not already a DCE client, follow the steps outlined in Configuring DCE/DFS Clients.
2. As root, start SMIT with the mkdcesrv fastpath:

   ```
   smit mkdcesrv
   ```

   or select the following sequence of SMIT menu options:

   ```
   1. Communications Applications and Services
   2. DCE (Distributed Computing Environment)
   3. Configure DCE/DFS
   4. Configure DCE/DFS Servers
   ```
3. Choose the **DCE UNIXD Server** option.
4. If you are not using the default cell_admin, enter the name of the cell administrator's account at the **Cell ADMINISTRATOR's account** prompt.
5. Because the machine is already configured as a DCE client, all other fields should be automatically filled in with the appropriate values. Select Do.
6. When prompted, enter the cell administrator's password.

At this point, a **dceunixd** server is configured on the machine, along with dced, a Security client, and a CDS client which were configured as part of DCE client configuration. To set up the machine to use DCE security see the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components* for complete details.

Configuring Audit Servers

To configure an Audit server perform the following steps:

1. If the machine is not already a DCE client, follow the steps outlined in "Configuring DCE/DFS Clients" on page 91.
2. As root, start SMIT with the **mkdcesrv** fastpath:

   ```
   smit mkdcesrv
   ```

   or select the following sequence of SMIT menu options:

   ```
   1. Communications Applications and Services
   2. DCE (Distributed Computing Environment)
   3. Configure DCE/DFS
   4. Configure DCE/DFS Servers
   ```
3. Choose the **Audit Server** option.

4. Because the machine is already configured as a DCE client, all other fields should be automatically filled in with the appropriate values. You will not be prompted for the cell administrator's password when the DCE client is already configured.
5. Select **Do**.

At this point, an Audit server is configured on the machine, along with **dced**, a Security client, and a CDS client which were configured as part of DCE client configuration.

Configuring Password Strength Servers

To configure a Password Strength server on a machine, perform the following steps on the machine:

1. If the machine is not already a DCE client, follow the steps outlined in "Configuring DCE/DFS Clients" on page 91.
2. As root, start SMIT with the **mkdcesrv** fastpath:

   ```
   smit mkdcesrv
   ```

   or select the following sequence of SMIT menu options:

   ```
   1. Communications Applications and Services
   2. DCE (Distributed Computing Environment)
   3. Configure DCE/DFS
   4. Configure DCE/DFS Servers
   ```
3. Choose the **Password Strength Server** option.
4. If you are not using the default **cell_admin**, enter the name of the cell administrator's account at the **Cell ADMINISTRATOR's account** prompt.
5. If you are not using the default password strength server arguments, enter the arguments at the **Password Strength Argument** prompt.
6. If you are not using the default password strength server, enter the password strength server command, including the full path, at the **Password Strength Server Command** prompt.
7. If you are not using the default password strength server protection level, select **<F4>** to list the available protection levels at the **Password Strength Level of Protection** prompt , select the appropriate level.
8. If you are not using the default password strength server, enter the password strength principal at the **Password Strength Server Principal** prompt.
9. Because the machine is already configured as a DCE client, all other fields should be automatically filled in with the appropriate values.
10. Select **Do**.
11. When prompted, enter the cell administrator's password.

At this point, a password strength server is configured on the machine, along with **dced**, a Security client, and a CDS client which were configured as part of DCE client configuration.

DFS Configuration

Configuring DFS in a DCE cell takes several steps. You should follow the steps in the order presented, although you can configure multiple machines of one role before moving on to the next. You can also come back later to configure another machine of a given role. For example, you can configure multiple Fileset Location Database machines before configuring the first File Server machine, but you cannot configure any File Server machines before you have configured the first Fileset Location Database machine.

For information on configuring a DFS client, see "Configuring DCE/DFS Clients" on page 91. For more information on DFS, see the *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference.*

These general steps are followed by detailed explanations.

1. Configure one or more DFS System Control machines. For detailed information, see "Configuring a DFS System Control Machine" on page 111.

   The permissions for many DFS administrative tasks are controlled by the DFS administrative lists (**admin.fl**, **admin.ft**, and so on). You can maintain these lists individually on each machine or you can maintain them on a central machine (the System Control machine) and have the other DFS server machines get copies of their lists from it. Using a System Control machine to distribute administrative lists is highly recommended.

   You can configure multiple domains of authority by configuring multiple System Control machines. The domain each DFS server machine belongs to is determined by the System Control machine from which it is receiving its administration lists.

2. Configure one or more DFS Fileset Database machines. For detailed information, see "Configuring a DFS Fileset Database Machine" on page 112.

   The Fileset Location Database machines maintain the Fileset Location Database, the mechanism by which DFS clients can find out which File Server machine actually holds the files being requested.

   One Fileset Location Database machine is required in each DCE cell using DFS. Multiple Fileset Location Database machines in the cell provide availability and load balancing of the data. For most cells, three Fileset

Location Database machines are recommended because three machines are usually sufficient for the tasks. If you configure more than three, an odd number is preferable.

3. Configure one or more File Server machines. For detailed information, see "Configuring a DFS File Server Machine" on page 112.

   The File Server machines are the ones that actually export data to DFS clients. They are configured by first starting the File Server daemons and then exporting LFS aggregates and JFS file systems and their filesets. It is recommended that you create the **root.dfs** fileset first (**root.dfs** is the root of the cell's filespace).

   You can have any number of File Server machines in the cell.

4. Configure one or more Fileset Replication Server machines. For details, see "Configuring a Fileset Replication Server" on page 114.

   A Fileset Replication Server uses the **repserver** process to manage replicas of filesets on File Server machines.

5. Configure one or more Backup Database machines (optional). For detailed information, see "Configuring a DFS Backup Database Machine" on page 115 .

   The Backup Database machines maintain the Backup Database, which is used for managing individual and periodic backups of DFS files.

   Backup Database machines are optional (required only if you want to take advantage of the backup capabilities of DFS). Multiple Backup Database machines provide for availability of the data. For most cells, three Backup Database machines are recommended because they are sufficient for the tasks. If you configure more, an odd number is preferable.

Configuring a DFS System Control Machine

To configure a machine as a DFS System Control machine using SMIT, perform the following steps:

1. As root, start SMIT with **mkdcesrv** fastpath:

   ```
   smit mkdcesrv
   ```

   or choose the following sequence of SMIT menu selections:

   a. **Communications Applications and Services**
   b. **DCE (Distributed Computing Environment)**
   c. **Configure DCE/DFS**
   d. **Configure DCE/DFS Servers**

2. Select the **DFS (Distributed File Service) System Control Machine** menu option.

3. Because the machine is already configured as a DCE client, fields should be automatically filled in with the appropriate values. If they are not, use the instructions in "Configuring DCE/DFS Clients" on page 91 to determine the values to enter.
4. Select **Do**.
5. When prompted, enter the cell administrator's password.

At this point, the machine is configured as a System Control machine; **dced**, a Security client, and a CDS client are also configured, if they had not been configured previously.

Configuring a DFS Fileset Database Machine

To configure a machine as a DFS Fileset Location Database machine using SMIT, perform the following steps:

1. As root, start SMIT with the **mkdcesrv** fastpath:

   ```
   smit mkdcesrv
   ```

   or select the following sequence of SMIT menu options:

   ```
   1. Communications Applications and Services
   2. DCE (Distributed Computing Environment)
   3. Configure DCE/DFS
   4. Configure DCE/DFS Servers
   ```
2. Choose the **DFS Fileset Database Machine** menu option.
3. If you want this machine to use DFS's **upclient** daemon to receive its administration lists from a System Control machine, enter the name of that machine in the **DFS System CONTROL machine identification** field. Use its *dce_hostname* (for example, **/.:/hosts/peach**). If you leave this field blank, this machine maintains its own administration lists. If this machine has already been configured as a System Control machine, this field is ignored.
4. Because the machine is already configured as a DCE client, fields should be automatically filled in with the appropriate values. If they are not, use the instructions in "Configuring DCE/DFS Clients" on page 91 to determine the values to enter.
5. Select **Do**.
6. When prompted, enter the cell administrator's password.

At this point, the machine is configured as a Fileset Location Database machine; **dced**, a Security client, and a CDS client.

Configuring a DFS File Server Machine

After you finish this configuration and any other DFS configurations that you need, ensure that you refer to "Exporting Data" on page 116.

To configure a machine as a DFS File Server machine using SMIT, perform the following steps:

1. As root, start SMIT with the **mkdcesrv** fastpath:

   ```
   smit mkdcesrv
   ```

   or select the following sequence of SMIT menu options:

   ```
   1. Communications Applications and Services
   2. DCE (Distributed Computing Environment)
   3. Configure DCE/DFS
   4. Configure DCE/DFS Servers
   ```

2. Select the **DFS File Server Machine** menu option.
3. If you want members of a certain DCE group to have administration authority over the filesets on this machine (but not on all DFS File Server machines, specify that group's name in the **Additional GROUP to administer filesets on this machine** field. Principals and groups specified in the **admin.ft** administration list have authority on all filesets on all File Server machines in the domain; this field allows you to specify an additional group that has authority only on this machine.
4. If you are not using the default **cell_admin**, enter the name of the cell administrator's account at the **Cell ADMINISTRATOR'S accoun**t prompt.
5. If you want to start the DCE daemons at a system reboot, select **<F4>** at the **Start daemons at System restart** prompt to list the choices, then select **true**. The default is **false**.
6. If you want this machine to use DFS's **upclient** daemon to receive its administration lists from a System Control machine, enter the name of that machine in the **DFS System CONTROL machine identification** field. Use its DCE hostname (for example, **/.:/hosts/peach**). If you leave this field blank, this machine maintains its own administration lists. If this machine has already been configured as a System Control machine, this field is ignored.
7. If you want change the number of main kernel processes running on this machine, change the value of the **Number of main kernel processes to run** field. The default is **8**.
8. If you want to change the number of token-revocation kernel processes to run on the machine, change the value of the **Number of token-revocation kernel processes to run** field. The default is **2**.
9. If you want the file exporter to forego token state recovery on restart, change the value in the **File exp. forego token state recovery on restart** field to **true**. The default is **false**.
10. If you want to change the minimum acceptable DCE RPC authentication level for communications between the file exporter and clients within the same cell, change the value in the **Minimum DCE RPC Authentication level - same cell** field. The default is **none**. Select **<F4>** to list the available protection levels.

11. If you want to change the maximum acceptable DCE RPC authentication level for communications between the file exporter and clients within the same cell, change the value in the **Maximum DCE RPC Authentication level - same cell** field. The default is dependent upon the encryption level installed on the system. If **dce.priv.rte** is installed, it is **pkt_privacy**; otherwise, if **dce.cdmf.rte** is installed, it is **cdmf**. If neither is installed, it is **pkt_integrity**. Select **<F4>** to list the available protection levels.
12. If you want to change the minimum acceptable DCE RPC authentication level for communications between the file exporter and clients in foreign cells, change the value in the **Minimum DCE RPC Authentication level-foreign cell** field. The default is **none**. Select **<F4>** to list the available protection levels.
13. If you want to change the maximum acceptable DCE RPC authentication level for communications between the file exporter and clients foreign cells, change the value in the **Maximum DCE RPC Authentication level-foreign cell** field. The default is dependent upon the encryption level installed on the system. If **dce.priv.rte** is installed, it is **pkt_privacy**; otherwise, if **dce.cdmf.rte** is installed, it is **cdmf**. If neither is installed, it is **pkt_integrity**. Select **<F4>** to list the available protection levels.
14. Because the machine is already configured as a DCE client, fields should be automatically filled in with the appropriate values. If they are not, use the instructions in "Configuring DCE/DFS Clients" on page 91 to determine the values to enter.
15. Select **Do**.
16. When prompted, enter the cell administrator's password.

At this point, the machine is configured as a DFS File Server machine; **dced**, a Security client, and a CDS client.

This procedure configures only the daemons necessary for the File Server, but no data is yet being exported form the machine to clients. For information on how to export data, see "Exporting Data" on page 116 and then see "Exporting a JFS File System from a DFS File Server" on page 118.

Configuring a Fileset Replication Server

First, ensure that a File Server is configured. See "Configuring a DFS File Server Machine" on page 112

To configure a DFS Fileset Replication Server using SMIT, perform the following steps:

1. As root, start SMIT with the **mkdcesrv** fastpath:

   ```
   smit mkdcesrv
   ```

or select the following sequence of SMIT menu options:

```
1. Communications Applications and Services
2. DCE (Distributed Computing Environment)
3. Configure DCE/DFS
4. Configure DCE/DFS Servers
```

2. Select the **DFS Fileset Replication Server Machine** menu option.
3. If you are not using the default *cell_admin*, enter the name of the cell administrator's account at the **Cell ADMINISTRATOR'S account** prompt.
4. Select **Do**.
5. When prompted, enter the cell administrator's password.

At this point, the machine is configured as a DFS Fileset Replication Server machine. This procedure configures only the daemon necessary for the replica (**repserver**). For information on actually replicating the data, see the *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference.*

Configuring a DFS Backup Database Machine

This option is available only if the DCE 2.2 for AIX Enhanced Distributed File System LPP has been installed.

To configure a machine as a DFS Backup Database machine using SMIT, perform the following steps:

1. As root, start SMIT with the **mkdcesrv** fastpath:

   ```
   smit mkdcesrv
   ```

   or select the following sequence of SMIT menu options:

   ```
   1. Communications Applications and Services
   2. DCE (Distributed Computing Environment)
   3. Configure DCE/DFS
   4. Configure DCE/DFS Servers
   ```

2. Select the **DFS Backup Database Machine** menu option.
3. If you are not using the default **cell_admin**, enter the name of the cell administrator's account at the **Cell ADMINISTRATOR'S accoun**t prompt.
4. If you want to start the DCE daemons at a system reboot, select **<F4>** at the **Start daemons at System restart** prompt to list the choices, then select **false**. The default is **false**.
5. If you want this machine to use DFS's **upclient** daemon to receive its administration lists from a System Control machine, enter the name of that machine in the **DFS System CONTROL machine identification** field. Use its DCE name (for example, **/.:/hosts/peach**). If you leave this field blank, this machine maintains its own administration lists. If this machine has already been configured as a System Control machine, this field is ignored.

6. Because the machine is already configured as a DCE client, fields should be automatically filled in with the appropriate values. If they are not, use the instructions in “Configuring DCE/DFS Clients” on page 91 to determine the values to enter.
7. Select **Do**.
8. When prompted, enter the cell administrator’s password.

At this point, the machine is configured as a DFS Backup Database machine: **dced**, a Security client, a CDS client, and a DTS client are also configured, if they had not been configured previously. This procedure configures only the daemon necessary for the backup (**bakserver**). For information on actually backing up the data, see the *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference* .

Exporting Data

To make data available from the file servers you have just configured (see “Configuring a DFS File Server Machine” on page 112), you must export data and create filesets from a File Server using DCE LFS, DCE DMLFS, AIX JFS, or AIX CD-ROM. The first fileset you create should be **root.dfs**.

The **root.dfs** fileset is the top-level fileset in DFS. You must configure **root.dfs** in order to set up the DFS namespace from the File Server machine. You can configure a DCE LFS, a DCE DMLFS, or an AIX JFS as the **root.dfs**, but if you select an AIX JFS fileset, you cannot use the fileset replication feature of DFS.

Exporting a DCE LFS Aggregate from a DFS File Server

This option is available only if the DCE 2.2 for AIX Enhanced Distributed File System LPP has been installed.

To export an LFS Aggregate from a machine that has been configured as a DFS File Server, perform the following steps:

1. Authenticate as a DCE user with proper authority to perform DFS aggregate and fileset tasks:

   dce_login *cell_admin*
2. As root, start SMIT with the **dfslfs** fastpath:

   smit dfslfs

   or select the following sequence of SMIT menu options:

   1. **Communications Applications and Services**
   2. **DCE (Distributed Computing Environment)**
   3. **Configure DCE/DFS**
   4. **Configure DCE/DFS Servers**

3. If you have not already created an AIX logical volume to be converted into an LFS aggregate, select the **Add / Change / Show / Remove AIX Logical Volumes** menu option and follow the normal procedures for creating one. Then return to the **Add / Delete LFS Aggregates and Filesets** menu.
4. Choose the **Export an Aggregate from the Local Machine** menu option.
5. At the **INITIALIZE device for LFS?** select box, select one of the following:

   1 no If you are about to export a logical volume that has already had the **newaggr** command run on it to convert it to an LFS aggregate.

   2 yes If you are about to export a logical volume that has just been created and has never had the **newaggr** command run on it, or if this is a logical volume that previously served as an LFS aggregate and you want to remove the data stored on it by reinitializing it.
6. In the **DEVICE to export as aggregate** field, give the device name for the logical volume (for example, **/dev/lv08**).
7. In the **Aggregate NAME** field, give the name you want the aggregate to be called.
8. In the **Aggregate ID** field, specify the ID to be used for this aggregate. This number must be unique among all JFS file systems and LFS aggregates exported from this machine. If you leave this field blank, the next available ID number is used.

   If you specified **1 no** at the **INITIALIZE device for LFS?** select box, skip to step b. Otherwise, continue with the next step.
9. In the **BLOCK size (in bytes)** field, specify the size each LFS block in the aggregate should be. This number must be a power of 2 between 1024 and 65,536; all possible options are given in the list for this field. The default value for this field is 8192.

   See **newaggr** in the *IBM DCE for AIX, Version 2.2: Administration Commands Reference* for more information on LFS block sizes.
10. In the **FRAGMENT size (in bytes)** field, specify the size to be used for allocation units in the aggregate. This number must be a power of 2 between 1024 and the value specified for **BLOCK size (in bytes)**. Possible options are given in the list for this fields; do not select a number larger than the block size selected in step 9 (in the **BLOCK size (in bytes)** field). The default value for this field is 1024.

    See **newaggr** in the *IBM DCE for AIX, Version 2.2: Administration Commands Reference* for more information on LFS fragment sizes.

    a. In the **Normal or verbose OUTPUT during device initialization?** field, select either **normal** or **verbose**, depending upon the amount of information you want from the **newaggr** command as it initializes the logical volume.

    b. Select **Do**.

At this point, the LFS aggregate is initialized (if you requested this action) and exported. No filesets have been created in the aggregate yet; see "Creating LFS Filesets" on page 120 for information on the procedure to create filesets so that clients can create and access DFS data.

Exporting a JFS File System from a DFS File Server

Note: Ensure that no file system activity is taking place on a JFS file system that you are exporting to the DFS file space. Otherwise, an inconsistent DFS token state can occur. When you configure the DFS File Server to export JFS file systems, you must start DFS at system start time to ensure that the DFS token state is correct.

To export an AIX Journaled File System from a machine that has been configured as a DFS File Server, follow these steps:

1. Authenticate as a DCE user with proper authority to perform DFS administration tasks:

   dce_login *cell_admin*

2. As root, start SMIT with the **dfsjfs** fastpath:

   smit dfsjfs

   or select the following sequence of SMIT menu options:

   1. **Communications Applications and Services**
   2. **DCE (Distributed Computing Environment)**
   3. **Configure DCE/DFS**
   4. **Configure DCE/DFS Servers**

3. If you have not already created a JFS file system, select the **Add / Change / Show / Delete AIX JFS File Systems** menu option and follow the normal procedures for creating one. Then return to the **Add / Delete JFS File Systems** menu.

   Notice that if you are exporting a previously existing JFS file system, any data on it is not affected; it becomes available to DFS clients when the file system is exported and mounted in the DFS file space.

4. Select the **Export a File System from the Local Machine** menu option.
5. In the **DEVICE to export** field, give the name of the device on which the JFS file system is located (for example, **/dev/lv09**).
6. In the **FILESET to register in file system as** field, give the name you want the fileset in this file system to be called. The first fileset in the cell should be named **root.dfs**; other filesets can have any name you want.
7. If you want the fileset to be made available to DFS clients right away, specify the location in the DFS filespace where the fileset should be placed in the **MOUNT POINT for fileset** field. If you do not specify the mount point now, you can create one later by issuing the **fts crmount** command on any machine configured as a DFS client.

If you are defining the **root.dfs** fileset, leave this field blank. The **root.dfs** fileset is automatically mounted at **/.:/fs** when it is defined.

Note: To use the **MOUNT POINT for fileset** option, ensure that the *cell_admin* has permission to insert into the parent directory.

8. In the **Aggregate ID to assign to file system** field, specify the ID to be used for this partition. This number must be unique among all AIX file systems and LFS aggregates exported from this machine. If you leave this field blank, the next available ID number is used.
9. Select **Do**.

At this point, the JFS file system is exported as you specified. Check that the appropriate user and group ownership and permission bits are associated with the DFS mount point for the fileset.

Exporting a CD-ROM File System from a DFS Server

To export a CD-ROM file system from a machine that has been configured as a DFS File Server, follow these steps:

1. Authenticate as a DCE user with proper authority to perform DFS administration tasks:

   ```
   dce_login cell_admin
   ```

2. As root, start SMIT with the **dfscdrom** fastpath:

   ```
   smit dfscdrom
   ```

   or select the following sequence of SMIT menu options:

   ```
   1. Communications Applications and Services
   2. DCE (Distributed Computing Environment)
   3. Configure DCE/DFS
   4. Configure DCE/DFS Servers
   ```

3. If you have not already created the CD-ROM file system, select the **Add/Change/Show/Delete CD-ROM File Systems** menu option and follow the normal procedures for creating one. Then, return to the **Add / Delete CD-ROM File System** menu.

   Notice that if you are exporting a previously existing CD-ROM file system, any data on it is not affected; it becomes available to DFS clients when the file system is exported and mounted in the DFS file space.
4. Select the **Export a File System from the Local Machine** menu option.
5. In the **DEVICE to export** field, give the name of the device on which the CD-ROM file system is located (for example, **/dev/cd0**).
6. In the **FILESET to register file system** as field, give the name you want the fileset in this file system to be called. It is *not* recommended that a CD-ROM file system be the **root.dfs** fileset for the cell.

7. If you want the fileset to be made available to DFS clients right away, specify the location in the DFS filespace where the fileset should be placed in the **MOUNT POINT for fileset** field. If you do not specify the mount point now, you can create one later by issuing the **fts crmount** command on any machine configured as a DFS client.

   Note: To use the **MOUNT POINT for fileset** option, ensure that the *cell_admin* has permission to insert into the parent directory.
8. In the **Aggregate ID to assign to file system** field, specify the ID to be used for this partition. This number must be unique among all the AIX file systems and LFS aggregates exported from this machine. If you leave this field blank, the next available ID number is used.
9. Select **Do**.

At this point, the CD-ROM file system is exported as you specified.

Creating LFS Filesets

To create a fileset in an LFS aggregate on a DFS File Server, perform the following steps:

1. Authenticate as a DCE user with proper authority to perform DFS aggregate and fileset tasks:

   dce_login *cell_admin*
2. As root, start SMIT with the **dfslfs** fastpath:

   smit dfslfs

   or select the following sequence of SMIT menu options:

   1. **Communications Applications and Services**
   2. **DCE (Distributed Computing Environment)**
   3. **Configure DCE/DFS**
   4. **Configure DCE/DFS Servers**
3. Select the **Create a Fileset in an Aggregate on the Local Machine** menu option.
4. In the **FILESET name** field, give the name you want the fileset in this partition to be called. The first fileset in the cell should be named **root.dfs**; other filesets can have any name you want.
5. In the **AGGREGATE to contain fileset** field, give the name of an existing aggregate in which the fileset should be created.
6. If you want the fileset to be made available to DFS clients right away, specify the location in the DFS filespace where the fileset should be placed in the **MOUNT POINT for fileset** field. If you do not specify a mount point now, you can create one later by issuing the **fts crmount** command on any machine configured as a DFS client.

If you are defining the **root.dfs** fileset, leave this field blank. The **root.dfs** fileset is automatically mounted at **/.:/fs** when it is defined.

7. Select **Do**.

At this point, the fileset is created as specified. The owning user and group of the root directory for a newly created fileset is always the DCE root principal and the DCE system group. The initial access rights are the UNIX mode bits **rwx------ (700)**and no explicit DCE ACLs are set. The fileset's quota limit is 5000 kilobytes. Depending upon the fileset's intended usage, you may need to modify these values. After mounting the fileset in the DFS filespace, modify the fileset mount point's user and group ownership, the initial access rights, and the fileset quota limit as appropriate. Use the AIX **chown** and **chgrp** commands to set the user and group ownership. Use the dcecp **acl** commands to view and modify the access control list including the Initial Object (io) and Initial Container (ic) ACLs. Use the **fts lsquota** and the **fts setquota** commands to view and change the fileset's quota limit.

Configuring DCE Web Utilities for AIX

The Web Utilities must be installed and configured on a workstation that has a Netscape Enterprise or a FastTrack 2.01 web server and a DCE client and optionally a DFS client configured within the cell. The DCE Web Utilities for AIX can be configured using SMIT.

To Configure DCE Web Utilities Using SMIT:

From the main SMIT panels:

1. Select **Communication Application and Services**.
2. Select **DCE (Distributed Computing Environment)**.
3. Select **Configure / Unconfigure Web Administration**.
4. Select **Configure the Web Administration**.
5. At the **Netscape Directory** panel:
   - Enter the home directory where your Netscape server is installed in the **Netscape Directory** field. The default is **/usr/ns-home**.
6. At the **Configuration** panel:
   - Enter the ID of the Netscape server in the **Netscape server ID** field.
   - Enter your *userid* in the **User ID** field.
   - Select **false** in the **Allow unauthenticated DFS access** field. **False** is the default.
   - Select **All** in the **Components to configure** field. **All** is the default to configure DFS Web Secure and DCE Administration.
7. Press **Enter** to begin configuration.

The *netscape server home directory* is the home directory where your Netscape server is installed. The default Netscape home directory is **/usr/ns-home**. The *netscape server* identifies the location of the Netscape server. This is from the **Server Identifier** field specified to the Netscape Administration Server when the server was installed. The *userid* is the operating system user account name for the Netscape server to run under.

The component can be **secure** for DFS Web Secure, **admin** for DCE Administration, or **all** for DFS Web Secure and DCE Administration. Configuring **admin** will also configure DFS Web Secure. For more information see the *IBM DCE for AIX, Version 2.2: Administration Commands Reference* or the *DFS Web Secure Product Guide* online documentation.

Unconfiguring DCE and DFS Components

Occasionally, certain situations require that you unconfigure (or remove configuration and database files for) a particular DCE or DFS component from a machine. For example, if you want to reconfigure a particular component with new parameters, you must unconfigure it to remove the existing configuration before setting up the new configuration. If you unconfigure a DFS client or a DFS File Server, you need to reboot the machine before reconfiguring with new parameters. Or, if configuration of a component failed and it is only partially configured, you must remove the partial configuration before attempting configuration again.

Other situations require that you unconfigure an entire machine (that is, unconfigure all DCE components from the machine). For example, if you want to transfer a machine from one cell to another, you must remove the configurations for the old cell from the machine before setting up the configurations for the new cell.

In rare cases, you may want to unconfigure an entire cell. If you unconfigure a cell, you should also unregister its name from the global namespace.

Attention: After you unconfigure a secondary CDS server (**unconfig.dce cds_second**), you must wait two hours before you reconfigure a secondary CDS server with the same name. The master CDS server refreshes its identity at two-hour intervals.

The following section provides more information on unconfiguring DCE components.

DFS Considerations Before You Reconfigure a Cell

In the event that you must reconfigure a DCE cell, you may reuse the DCE LFS aggregates and filesets from the original cell. This requires preserving

aggregates and the **/opt/dcelocal/var/dfs/dfstab** file on each DFS File Server machine when the cell is unconfigured (the **stop.dfs** command leaves this file in **/opt/dcelocal/var/dfs**). After you reconfigure the DFS File Server machine in the new cell, use the **dfsexport** command to export the aggregates listed in the dfstab file. Then use the **fts syncfldb** command to update the Fileset Location Database with information about the filesets.

ACLs on DCE DFS files and directories contain the UUID of the local cell. When you reconfigure a cell, a new UUID is generated for the cell even if you use the same cell name. Therefore, if you create DCE LFS files and directories in a cell, reconfigure that cell, and export the files and directories in the new cell, then the ACLs will still contain the UUID for the previous cell.

To avoid this situation, pass the UUID of the old cell to the **sec_create_db** command when you are reconfiguring. Edit the **/opt/dcelocal/tcl/dcedcf/cfg_dce.tcl** command on the machine that is to be the Master Security server with the following steps:

1. Search for the line that runs the **SECCREATEDB_CMD** command in the config_sec_srv_main routine. (Do not change the options on the **SECCREATEDB_CMD** in **config_sec_rep_main**)
2. Add to this line the following:

   ```
   -uuid old_uuid
   # Where old_uuid is the UUID of the previous configuration
   ```

3. Reconfigure your cell.

   Note: You must reboot any machines running a DFS client or DFS File Server. If possible, the reboot needs to be done before you reconfigure your cell.

You can determine the UUID for a cell before you unconfigure it by issuing the **klist** command. The line that displays the name of the cell also displays its UUID.

If you have already unconfigured the cell, you can repair the DCE LFS ACLs by using the **acl_edit cell** command. For more information, see the *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference.*

You may have to perform additional cleanup to eliminate ACL entries for specific users and groups from the previous cell's configuration if the users or groups no longer exist or if their UUIDs have changed.

Considerations Before Unconfiguring

You should exercise caution in unconfiguring DCE components, especially if you are removing components which perform services required by other components. Unconfiguring a component will partially or completely disable other components which are dependent upon it.

There are special cases which you should take into consideration when unconfiguring DCE components:

- The master Security server and the CDS server that contain the master replica of the **/.:/** directory are the basis of any cell. If you unconfigure one or both of these servers, you have to unconfigure and rebuild your entire cell.
- To unconfigure a CDS server that has a master replica of any directory, you must use the **local** option.

  See the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components* for more information on changing the location of a directory's master replica.
- The Fileset Location Database is the basis of any cell's DFS system. If you select the last remaining Fileset Location Database machine to unconfigure, SMIT issues a warning message and asks if you want to continue with unconfiguration.
- Before unconfiguring a DFS file server, filesets residing on the DFS file server should be either moved to another DFS file server or deleted, and any replica sites should be removed. In situations where this in not possible, for example, when a local unconfiguration has already been done on the DFS file server machine or a hardware problem exists, use the **fts rmsite** and **fts delfldbentry** commands to remove any replica sites and fileset entries associated with this machine. Then use the **admin unconfiguration** option to complete the unconfiguration of the DFS file server machine.

When you unconfigure DCE and DFS components on a machine, two types of operations are performed:

- Local operations (updating configuration files and stopping daemons)
- Administrative operations (updating the Security registry, the CDS namespace, the DFS Fileset Location Database, and DFS administration lists maintained on a remote system control machine).

Just as configuration is separated into **admin** and **local** portions, so is most of unconfiguration. The exceptions are the master Security server (**sec_srv**) and any CDS server (**cds_srv** or **cds_second**) that contains a master replica of a directory in one of its clearinghouses.

When you unconfigure DCE and DFS components on a machine, if all the local operations can be undone, the machine itself is considered to be unconfigured. However, if attempts to undo administrative operations fail, the machine is not fully unconfigured from the cell; entries for the machine may still exist in the CDS namespace, registry database, or DFS databases. On a full unconfiguration if attempts to undo administrative operations fail, a list of the failed operations is printed so you can manually perform these operations

and remove references to the machine from the namespace, registry database, and DFS databases. From another machine configured in your cell, you can run **admin** unconfiguration for operations that failed so that you can clean up the DCE registry database and the namespace.

Refer to the *IBM DCE for AIX, Version 2.2: Administration Commands Reference* for complete information on the DCE commands referenced above. Refer to the *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference* for complete information on the DFS commands referenced above.

Split Unconfiguration

Sometimes it is beneficial to use a feature known as the *split unconfiguration of clients*, which allows the root user to perform the unconfiguration steps on the local machine while the cell administrator cleans up the rest of the cell. A **local** unconfiguration is useful in the following situations:

- If the cell for which a machine is configured is inaccessible or you do not have the password for that cell administrator's account, you need only to remove the local configuration files from the machine to reconfigure it for a new cell.
- If the configuration of a machine is so broken that it cannot reach the Security server to be authenticated to perform remote operations, you can limit unconfiguration to local items.
- If you are unconfiguring a Master Security server that contains the master replica of a directory, you can deal only with local items.
- If you are unconfiguring a CDS server that contains the master replica of a directory, you can deal only with local items.

The cell administrator should run the **admin** portion of unconfiguration from a machine in the cell to complete the unconfiguration process. A full client that has been locally unconfigured cannot be configured back into the cell until the admin portion of unconfiguration has been done.

Steps for Unconfiguring DCE and DFS

To unconfigure one or more DCE components from a machine, perform the following steps:

1. As root, start SMIT with the **unconfig.dce** fastpath:

   ```
   smit rmdce
   ```

   or select the following sequence of SMIT menu options:

   ```
   1. Communications Applications and Services
   2. DCE (Distributed Computing Environment)
   3. Unconfigure DCE/DFS
   ```

2. At the **Type of Unconfiguration** select box, select one of the following:

- **full unconfiguration for this machine**
- **local only unconfiguration for this machine**
- **admin only unconfiguration for another machine**

3. If you are not using the default *cell_admin*, enter the name of the cell administrator's account at the **Cell ADMINISTRATOR's account** prompt.
4. At the **COMPONENTS to Remove** panel enter or select from the pull-down list, the components that you want to remove.

   For the **admin only unconfiguration**, enter the *dce_hostname* of the machine for which you are unconfiguring components in the **Client Machine's DCE HOSTNAME** field.

   For the **full unconfiguration** and **local unconfiguration**, the **Remove DEPENDENT Components?** field defaults to **No**. You should change this field to **Yes** only if you have selected a component and are *sure* that you want to unconfigure every component that depends on the presence of the component you selected. For example, all components depend on the presence of **dced**. Therefore, if you select **dced** as the only client to unconfigure and change **Remove DEPENDENT Components?** to **Yes**, the result will be the same as if you had selected **All** for **COMPONENTS to Remove**.

   Note: If you are unconfiguring a Password Strength server, you must enter its ID in the **Principal ID for Password Strength Server** filed.
5. For the **full unconfiguration** and the **local only unconfiguration**, the **OVERRIDE Dependency Checking?** field defaults to **No**. You should change this field to **Yes** only if you are *sure* that you want to unconfigure a component without unconfiguring other components that are dependent on it. For example, if you unconfigure RPC but leave **sec_cl** and **cds_cl** configured, these two will not be able to function properly.
6. Select **Do**.
7. If prompted, enter the cell administrator's password for the **full unconfiguration** and the **admin unconfiguration**.

Unconfiguring DCE Web Utilities

You **must** unconfigure DFS Web Secure before uninstalling it. Unconfiguration returns the Netscape servers to a non-DFS state by removing DFS Web Secure information.

DCE Web Utilities can be unconfigured by using SMIT.

To Unconfigure DCE Utilities Using SMIT:

From the main SMIT panels:

1. Select **Communication Application and Services**.

2. Select **DCE (Distributed Computing Environment)**.
3. Select **Configure / Unconfigure Web Administration**.
4. Select **Unconfigure the Web Administration**.
5. At the **Netscape Directory** panel:
   - Enter the home directory where your Netscape server is installed in the **Netscape Directory** field. The default is **/usr/ns-home**.
6. At the **Unconfiguration** panel:
   - Enter the ID of the Netscape server in the **Netscape server ID** field.
   - Enter your *userid* in the **User ID** field.
   - Select **false** in the **Allow unauthenticated DFS access** field. **False** is the default.
   - Select **All** in the **Components to unconfigure** field. **All** is the default to unconfigure DFS Web Secure and DCE Administration.
7. Press **Enter** to begin unconfiguration.

For more information see the *IBM DCE for AIX, Version 2.2: Administration Commands Reference* or the *DFS Web Secure Product Guide* online documentation.

Chapter 5. Starting and Stopping DCE 2.2 for AIX

Starting DCE and DFS Daemons

You can use either the command line or the SMIT interface to start DCE and DFS daemons.

Using the Command Line to Start Daemons

The **start.dce** and **start.dfs** commands start DCE and DFS daemons for configured DCE and DFS components respectively. Before starting DCE and DFS daemons, you must be logged in as root.

To start all daemons for configured DCE and DFS components, enter the following at the command line:

```
start.dce all
```

To start all daemons for configured DCE components, enter either of the following commands at the command line:

```
start.dce core
start.dce
```

To start all daemons for configured DFS components, enter either of the following commands at the command line:

```
start.dfs all
start.dfs
```

To start specific configured components, add the component name, such as **cds_srv**, to the command:

```
start.dce cds_srv
```

The **start.dfs** command will start all the appropriate deamons for a specified DFS component. For example:

```
start.dfs dfs_cl
```

will start the **dfsbind** and the **dfsd** daemons.

Notes:

1. If the Master security server and the Initial CDS server are on different machines and both have been stopped, use the following steps to restart DCE:

Machine 1
(rpc, sec_cl, sec_srv, cds_cl, and any other dce or dfs components)

Machine 2
(rpc, sec_cl, cds_srv, cds_cl, and any other dce or dfs components)

a. Machine 1: **start.dce rpc sec_cl sec_srv**
b. Machine 2: **start.dce rpc sec_cl cds_cl cds_srv**
c. Machine 1: **start.dce all**
d. Machine 2: **start.dce all**

2. For DFS client and File Server machines, if DFS had been previously running on the machine, you need to reboot the machine before restarting DFS if either of the following conditions occurred after DFS was stopped:
   - A new fix level or version of DFS was installed on the machine.
   - The DFS client or File Server was reconfigured.

Using SMIT to Start DCE, DFS, and NFS/DFS Authenticating Gateway Now and at System Restart

You can run **start.dce** now to start all configured DCE and DFS daemons. You can also run **start.dce** at system restart if the appropriate entries are in **/etc/inittab**.

Note: For compatability and to be consistent with other AIX commands, the **rc.(_)** commands are put into **/etc/inittab**. **rc.dce** will invoke **start.dce** and **rc.dfsnfs** will invoke **startnfs.dfs**. Use SMIT to add or delete these entries.

1. As root, start SMIT:
   ```
   smit mkdceitab
   ```
2. Select the DCE/DFS items to start. Select **<F4>** to view a list. Then select one of the following:

   dce To start only the DCE daemons

   dce and dfs
   To start both the DCE and the DFS daemons

   dce, dfs, and NFS/DFS Authenticating Gateway
   To start DCE, the DFS, and DCE NFS to DFS Authenticating Gateway for AIX.

   none To remove the **rc.dce** and **rc.dfsnfs** entries from **/etc/inittab**.
3. Select now, system restart, or both:

   now To run **start.dce** and **startnfs.dfs** (if appropriate) immediately

system restart
To add the proper **rc.dce** command and **rc.dfsnfs** (if appropriate) to **/etc/inittab**

both To run **start.dce** and **startnfs.dfs** (if appropriate) immediately and add the proper **rc.dce** command and **rc.dfsnfs** (if appropriate) to **/etc/inittab**.

4. Select **Do**.

Based on your selections, the following actions take place:

Selection	Selection	Result
dce	now	**start.dce core** runs right away.
dce and dfs	now	**start.dce all** runs right away.
dce	system restart	**rc.dce core** is added to **/etc/inittab**.
dce and dfs	system restart	**rc.dce all** is added to **/etc/inittab**.
dce	both	**start.dce core** runs right away and **rc.dce core** is added to **/etc/inittab**.
dce and dfs	both	**start.dce all** runs right away and **rc.dce all** is added to **/etc/inittab**.
dce, dfs, and NFS/DFS Authenticating Gateway	now	**start.dce all** and **startnfs.dfs** run right away.
dce, dfs, and NFS/DFS Authenticating Gateway	system restart	**rc.dce all** and **rc.dfsnfs** are added to **/etc/inittab**.
dce, dfs, and NFS/DFS Authenticating Gateway	both	**start.dce all** and **startnfs.dfs** run right away and **rc.dce all** and **rc.dfsnfs** are added to **/etc/inittab**.
none	system restart	**rc.dce core** or **rc.dce all**, and **rc.dfsnfs** are removed from **/etc/inittab**.
none	both	**rc.dce core** or **rc.dce all**, and **rc.dfsnfs** are removed from **/etc/inittab**.

Note: There are options on the **config.dce**, **config.dfs**, and **startnfs.dfs** commands to turn autostart on or off.

Stopping DCE and DFS Daemons

The **stop.dce** and **stop.dfs** commands stop DCE and DFS daemons for configured DCE and DFS components. To stop DCE and DFS daemons, you must be logged in as root.

To stop all daemons for configured DCE and DFS components, enter the following at the command line:

```
stop.dce all
```

To stop all daemons for configured DCE components, enter one of the following at the command line:

```
stop.dce core
stop.dce
```

To stop all daemons for configured DFS components, enter one of the following at the command line:

```
stop.dfs all
stop.dfs
```

To stop specific daemons for configured DCE and DFS components, add the daemon's name to the **stop.dce** or **stop.dfs** command and enter the following at the command line:

```
stop.dce dts_cl
```

The **stop.dfs** command will stop all the appropriate daemons for a specified DFS component. For example:

```
stop.dfs dfs_cl
```

will stop the **dfsbind** and the **dfsd** daemons.

Chapter 6. Obtaining Additional Information

This chapter describes the sources of information that can be useful when you are using DCE 2.2 for AIX.

Books

The DCE 2.2 for AIX library contains a printed copy and an online version of the *IBM DCE for AIX, Version 2.2: Quick Beginnings*and a printed copy of the *IBM DCE for AIX, Version 2.2: Release Notes*. All other supporting product documentation is provided only in online format.

Online Information

Extensive online documentation is shipped as part of the DCE for AIX product.

HTML Books

The manuals included with this product are in Hypertext Markup Language (HTML) softcopy format. The softcopy format makes it easier to share the library across your site.

Although you can use any browser that supports HTML 3.2, a Netscape browser is provided with the Operating System. For instructions on installing and using the browser, see the AIX documentation.

The following IBM DCE books are available online:

- *IBM DCE for AIX, Version 2.2: Quick Beginnings*
- *IBM DCE for AIX, Version 2.2: Introduction to DCE*
- *IBM DCE for AIX, Version 2.2: Application Development Guide—Introduction and Style Guide*
- *IBM DCE for AIX, Version 2.2: Application Development Guide—Core Components*
- *IBM DCE for AIX, Version 2.2: Application Development Guide—Directory Services*
- *IBM DCE for AIX, Version 2.2: NFS/DFS Authenticating Gateway*
- *IBM DCE for AIX, Version 2.2: Application Development Reference*
- *IBM DCE for AIX, Version 2.2: Administration Guide—Introduction*
- *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components*

- *IBM DCE for AIX, Version 2.2: Administration Commands Reference*
- *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference*
- *IBM DCE for AIX, Version 2.2: Problem Determination Guide*
- *IBM DCE for AIX, Version 2.2: High Availability Cluster Multi-Processing Guide for DCE and DFS*

Help Files

DCE 2.2 for AIX provides assistance for system management tasks in the form of SMIT helps. It also provides HTML helps for the DCE/DFS Administration Graphical User Interface (GUI).

Print and Order Books

IBM DCE Publications

In addition to the hardcopy editions of the *IBM DCE for AIX, Version 2.2: Quick Beginnings* and *IBM DCE for AIX, Version 2.2: Release Notes* IBM supplies PostScript files on the CD-ROM for each of the online DCE 2.2 documents for those customers who want the option of having printed documentation.

OSF DCE Publications

For printed books that are not specific to a particular product, OSF publishes the following DCE publications through The Open Group:

- Open Software Foundation. *Introduction to OSF DCE*
- Open Software Foundation. *OSF DCE User's Guide and Reference*
- Open Software Foundation. *OSF DCE Administration Guide: Core Components*
- Open Software Foundation. *OSF DCE Administration Guide: Extended Services*
- Open Software Foundation. *OSF DCE Administration Reference*
- Open Software Foundation. *OSF DCE Application Development Guide*
- Open Software Foundation. *OSF DCE Application Development Reference*

Although not written specifically for AIX products, these publications may provide helpful information. These OSF DCE publications are available through bookstores and mail order companies. The following mail order company is in no way associated with IBM, and IBM makes no claim about the services this company provides:

O'Reilly & Associates, Inc., 103A Morris Street, Sebastopol, CA 95472.
Phone: 800-988-9938 (US and Canada), 707-829-0515,
FAX: 707-829-0104 between 7 am and 6 pm PST weekdays.
Internet: order@ora.com

The following O'Reilly books may also be useful:

- Hu, Wei. *DCE Security Programming* , 1st. ed. Sebastopol, CA: O'Reilly & Associates, 1994.
- Rosenberry, Ward. *Understanding DCE* , 2nd. ed. Sebastopol, CA: O'Reilly & Associates, 1993.
- Shirley, John. *Guide to Writing DCE Applications* , 2nd. ed. Sebastopol, CA: O'Reilly & Associates, 1994.

Using DCE 2.2 for AIX Documentation

The DCE 2.2 for AIX product includes user, administration, and application development documentation that is accessible online. The documentation is provided in two formats: As HTML files that are viewable with the any browser that supports HTML 3.2 and as flat ASCII files that are viewable with the IBM ASCII Browser, **asciiview**.

See "Appendix A. Online Documentation" on page 137 for more information about the filesets that must be installed to access the DCE for AIX online documentation.

The start_dcedoc program

The **start_dcedoc** program defaults to the appropriate viewer for your interface based on your **$DISPLAY** environment variable. You can also use flags to specify which viewer you want **start_dcedoc** to attempt to start. The flags are **-g** for a graphics interface and **-a** for an ASCII interface.

Users can also start **asciiview** directly without using **start_dcedoc**.

Viewing the HTML Documentation

Users with graphic interfaces can use a web browser such as the **Netscape Navigator** browser, which is included with the AIX operating system, to read the DCE documentation HTML files. The **Netscape Navigator** browser provides hypertext linking, navigation utilities, a hypertext index, graphical display of artwork, search and print facilities, a bookmark function, and an NLS-enabled online help utility. See the AIX documentation for information on installing the **Netscape Navigator** browser.

If you have installed the documentation files locally, use your web browser to view the DCE HTML documentation by opening the file:

```
/usr/lpp/dcedoc/html/en_US/index.html
```

Note: en_US can be substituted with the appropriate locale name.

If you have **DFS Web Secure** installed and configured into a **Netscape** web server, go to the URL:

http://*servername***/dceweb**

From that web page select **dce docs**.

Starting the IBM ASCII Browser

Users with ASCII interfaces can use the IBM ASCII Browser, **asciiview**, to read the flat ASCII DCE documentation files online. The browser allows structured access to all the books in the DCE library from a central menu. Users can select a book by title and then choose entries from the book's table of contents. The repeated retrieval of different books and chapters is also supported, allowing users to move through the DCE documentation library without having to exit and restart the Browser.

To start the IBM ASCII Browser using an ASCII interface, enter **asciiview** on the command line.

Note to InfoExplorer users: If you use InfoExplorer on a graphics terminal to read AIX publications, you can also start the **xview** viewer from within your InfoExplorer session by doing the following:

1. Select the **Books** button.
2. On the **List of Books** screen, page down to the **Applications Books** section.
3. Select the **Distributed Computing Environment Books** link to start **xview**.

ASCII terminal users need to start the ASCII Browser in one of the methods described above.

Printing the PostScript Books

If you prefer hardcopy documentation, a set of uncompressed PostScript files are included on the product CD. You can print these books directly from the CD. Go to the location **/usr/lpp/dcedoc/ps/en_US/** and select the .ps file that you want to send to your printer. See "Appendix A. Online Documentation" on page 137 for a listing of the publications and their file prefixes.

Note: en_US can be substituted with the appropriate locale name.

Appendix A. Online Documentation

The following table identifies the documents by file prefix:

Prefix	Title
a3u2h	*IBM DCE for AIX, Version 2.2: Application Development Guide—Introduction and Style Guide*
a3u2i	*IBM DCE for AIX, Version 2.2: Application Development Guide—Directory Services*
a3u2j	*IBM DCE for AIX, Version 2.2: Application Development Guide—Core Components*
a3u2k	*IBM DCE for AIX, Version 2.2: Application Development Reference*
a3u2l	*IBM DCE for AIX, Version 2.2: Problem Determination Guide*
a3u2m	*IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference*
a3u2p	*IBM DCE for AIX, Version 2.2: Quick Beginnings*
a3u2q	*IBM DCE for AIX, Version 2.2: Administration Guide—Core Components*
a3u2r	*IBM DCE for AIX, Version 2.2: Administration Guide—Introduction*
a3u2s	*IBM DCE for AIX, Version 2.2: Introduction to DCE*
a3u2t	*IBM DCE for AIX, Version 2.2: NFS/DFS Authenticating Gateway*
a3u2u	*IBM DCE for AIX, Version 2.2: Administration Commands Reference*
a3u2v	*IBM DCE for AIX, Version 2.2: High Availability Cluster Multi-Processing Guide for DCE and DFS*

The following files are contained in the Online Documentation package:

Fileset:

dce.doc.en_US.ascii

Directory: /usr/lpp/dcedoc/3270
Directory: /usr/lpp/dcedoc/3270/en_US
File: /usr/lpp/dcedoc/3270/en_US/booklist
File: /usr/lpp/dcedoc/3270/en_US/a3u2hmst.list3270
File: /usr/lpp/dcedoc/3270/en_US/a3u2imst.list3270
File: /usr/lpp/dcedoc/3270/en_US/a3u2jmst.list3270
File: /usr/lpp/dcedoc/3270/en_US/a3u2kmst.list3270
File: /usr/lpp/dcedoc/3270/en_US/a3u2lmst.list3270
File: /usr/lpp/dcedoc/3270/en_US/a3u2mmst.list3270
File: /usr/lpp/dcedoc/3270/en_US/a3u2pmst.list3270

File: /usr/lpp/dcedoc/3270/en_US/a3u2qmst.list3270
File: /usr/lpp/dcedoc/3270/en_US/a3u2rmst.list3270
File: /usr/lpp/dcedoc/3270/en_US/a3u2smst.list3270
File: /usr/lpp/dcedoc/3270/en_US/a3u2tmst.list3270
File: /usr/lpp/dcedoc/3270/en_US/a3u2umst.list3270
File: /usr/lpp/dcedoc/3270/en_US/a3u2vmst.list3270

Note: en_US can be substituted with the appropriate locale name.

Fileset:

dce.doc.en_US.html

Directory: /usr/lpp/dcedoc/html
Directory: /usr/lpp/dcedoc/html/en_US
Directory: /usr/lpp/dcedoc/html/en_US/index.html
File: /usr/lpp/dcedoc/html/en_US/README
File: /usr/lpp/dcedoc/html/en_US/A3U2HMST.HTM.TAR.Z
File: /usr/lpp/dcedoc/html/en_US/A3U2IMST.HTM.TAR.Z
File: /usr/lpp/dcedoc/html/en_US/A3U2JMST.HTM.TAR.Z
File: /usr/lpp/dcedoc/html/en_US/A3U2KMST.HTM.TAR.Z
File: /usr/lpp/dcedoc/html/en_US/A3U2LMST.HTM.TAR.Z
File: /usr/lpp/dcedoc/html/en_US/A3U2MMST.HTM.TAR.Z
File: /usr/lpp/dcedoc/html/en_US/A3U2PMST.HTM.TAR.Z
File: /usr/lpp/dcedoc/html/en_US/A3U2QMST.HTM.TAR.Z
File: /usr/lpp/dcedoc/html/en_US/A3U2RMST.HTM.TAR.Z
File: /usr/lpp/dcedoc/html/en_US/A3U2SMST.HTM.TAR.Z
File: /usr/lpp/dcedoc/html/en_US/A3U2TMST.HTM.TAR.Z
File: /usr/lpp/dcedoc/html/en_US/A3U2UMST.HTM.TAR.Z
File: /usr/lpp/dcedoc/html/en_US/A3U2VMST.HTM.TAR.Z
File: /usr/lpp/dcedoc/html/en_US/dcedoc_22.htm

Note: en_US can be substituted with the appropriate locale name.

Fileset:

dce.doc.en_US.ps

Directory: /usr/lpp/dcedoc/ps
Directory: /usr/lpp/dcedoc/ps/en_US
File: /usr/lpp/dcedoc/ps/en_US/README
File: /usr/lpp/dcedoc/ps/en_US/a3u2hmsx.ps
File: /usr/lpp/dcedoc/ps/en_US/a3u2imsx.ps
File: /usr/lpp/dcedoc/ps/en_US/a3u2jmsx.ps
File: /usr/lpp/dcedoc/ps/en_US/a3u2kmsx.ps
File: /usr/lpp/dcedoc/ps/en_US/a3u2lmsx.ps
File: /usr/lpp/dcedoc/ps/en_US/a3u2mmsx.ps
File: /usr/lpp/dcedoc/ps/en_US/a3u2pmsx.ps
File: /usr/lpp/dcedoc/ps/en_US/a3u2qmsx.ps

File: /usr/lpp/dcedoc/ps/en_US/a3u2rmsx.ps
File: /usr/lpp/dcedoc/ps/en_US/a3u2smsx.ps
File: /usr/lpp/dcedoc/ps/en_US/a3u2tmsx.ps
File: /usr/lpp/dcedoc/ps/en_US/a3u2umsx.ps
File: /usr/lpp/dcedoc/ps/en_US/a3u2vmsx.ps

Note: en_US can be substituted with the appropriate locale name.

Fileset:

dce.doc.rte.ascii

Directory: /usr/lpp/dcedoc
Directory: /usr/lpp/dcedoc/bin
File: /usr/lpp/dcedoc/bin/asciiview
File: /usr/lpp/dcedoc/bin/dceman
File: /usr/lpp/dcedoc/bin/start_dcedoc
Symlink: /usr/bin/asciiview to /usr/lpp/dcedoc/bin/asciiview
Symlink: /usr/bin/dceman to /usr/lpp/dcedoc/bin/dceman
Symlink: /usr/bin/start_dcedoc to /usr/lpp/dcedoc/bin/start_dcedoc

Appendix B. Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make them available in all countries in which IBM operates. 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. Subject to IBM's valid intellectual property or other legally protectable rights, any functionally equivalent product, program, or service may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

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
500 Columbus Avenue
Thornwood, NY 10594
USA

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
Department LZKS
11400 Burnet Road
Austin, Texas 78758
USA

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

Trademarks

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

AIX
IBM
InfoExplorer
RISC System/6000

DFS is trademark of Transarc Corporation

Netscape and Netscape Navigator are trademarks of Netscape Communications Corporation

Open Software Foundation, OSF, the OSF logo, OSF/1, OSF/Motif, and Motif are registered trademarks of the Open Software Foundation, Inc.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names, which may be denoted by a double asterisk (**), may be trademarks or service marks of others.

Index

Special Characters

A

B

C

D

E

T

U

V

W

X

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SC23-4188-00