HEWLETT PACKARD

HP 9000
Series 700/800
Computers

HP DCE/9000 Version 1.2 Release Notes

HP DCE/9000 Version 1.2

Release Notes

Printed in U.S.A.

January 1994

Mfg. No. 3190-90019

First Edition

NOTICE

The information contained in this document is subject to change without notice.

HEWLETT-PACKARD MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance or use of this material.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

About this document

This document describes HP DCE/9000 Version 1.2 and includes both Core Services and the optional DFS, GDS, and DFS-NFS Protocol Exportor Products.

Contents

1

About HP DCE/9000

About HP DCE/9000

This release notes document describes HP DCE/9000 Version 1.2. It is organized as follows:

- This chapter provides general information about this release; it also includes information for programmers.
- Chapter 2 discusses migration and compatibility issues for HP DCE/9000.
- Chapter 3 explains how to plan cell configuration and install the HP DCE/9000 Version 1.2 Core Services software.
- Chapter 4 explains how to configure and validate your DCE cell; this chapter also includes a brief overview of DCE administration.
- Chapter 5 explains how to use and administer the HP-UX DCE-Integrated login utilities.
- Chapter 6 discusses security administration on HP DCE/9000, particularly security replication.
- Chapter 7 contains miscellaneous information of use to DCE cell administrators.
- Chapter 8 discusses planning and configuration of the DCE Distributed File Service (DFS), a new feature of HP DCE/9000 Version 1.2.
- Chapter 9 discusses configuration and administration of the DCE Global Directory Service (GDS), a new feature of HP DCE/9000 Version 1.2.

This software release runs on HP 9000 Series 700 and 800 computers running HP-UX Version 9.03 (or greater) operating system software.

HP DCE/9000 Core Services Software

The HP DCE/9000 Version 1.2 is based on OSF DCE Version 1.0.3 source code, with bug fixes and HP-provided value-added functionality. This section describes the contents of this release.

OSF DCE Components Included in This Release

This release includes the following OSF DCE components:

- Remote Procedure Call (RPC) Facility, supporting both connection-oriented (TCP/IP) and connectionless (UDP/IP) transport protocols.
- User-space Threads, based on Draft 4 of POSIX 1003.4a, *Threads Extension for Portable Operating Systems.*
- Cell Directory Service (CDS), including CDS server replication.
- Access to the CDS namespace through the X/Open Directory Service (XDS) and X/Open Object Management (XOM) services. The OSF DCE 1.0.3 versions of the XDS, XOM, and **dua** libraries are a part of **libdce**, and the necessary XDS and XOM header files are provided.
- Security, including security server replication and additional security server replication functionality.
- Distributed Time Service (DTS); this release supports **ntp**, **null,** and **Spectracom** DTS time providers; it also supports global time servers and DCE time zones. (Support for the Spectracom time provider has been added by HP; see the next section, "Additional HP DCE/9000 Features", for details).
- The OSF Distributed File Service (DFS), a distributed client/server application that provides, through the DCE, access to files and directories across machine boundaries. Information about configuring DFS is included in this document and in the *OSF DCE Administration*

Guide – Extended Services, which is included with this release. HP DCE/9000 DFS is available as a separately-priced product.

- Global Directory Agent (GDA), using the Berkeley Internet Naming Daemon (BIND).
- Global Directory Services (GDS), a distributed, replicated directory service that is based on the X.500 international communication standard. HP DCE/9000 GDS is available as a separately-priced product.

In HP DCE/9000 Version 1.2, the DCE application library is provided as both a shared library (**libdce.sl**) and as an archive library (**libdce.a**). If you use the shared library, a DCE application can share a single copy of the library with other DCE applications that are running on the same host. If you use the archive library, each application binary will contain its own copy of DCE routines that it either directly or indirectly calls.

Additional HP DCE/9000 Features

The following features have been added to HP DCE/9000 by Hewlett-Packard:

- The SAM DCE Cell Administration (SDCA) utility has been replaced by a new, easier-to-use SAM-based DCE Cell Configuration (SDCC) utility. This tool is accessible via SAM (the HP-UX System Administration Manager) and is documented in online help.
- A set of DCE-integrated login utilities, that authenticate users via the DCE Security Registry instead of via **/etc/passwd** and **/etc/group**. HP DCE/9000 Version 1.2 includes improvements to **login**, **vuelogin**, **su**, **passwd**, **chsh**, **chfn**, **telnet**, and **rlogin**, as well as new DCE-integrated versions of **ftpd** and **vuelock**. Documentation for these utilities can be found in Chapter 5, *DCE-Integrated Login Utilities*.
- A set of DCE cell diagnosic tools, **camera**, **dceval**, **dcewhich**, and **dceping**.
- DTS, in addition to **null** and **ntp** time providers, now also supports the **Spectracom** radio clock time source. Hewlett-Packard has thor-

oughly tested the Spectracom model NETCLOCK/2 radio clock. For more information on the Spectracom time provider, contact:

Spectracom Corporation
101 Despatch Drive
East Rochester, NY 14445

Phone: 716-381-4827
FAX: 716-381-4998

- Two new sub-commands to the **sec_admin** interface, **become** and **change_master**, that allow you to easily move the master registry between cell member systems. See the **sec_admin**(8) man page for details.
- An enhanced version of the OSF CDS browser (**cdsbrowser**), with new functionality and an improved user interface. See the CDS Browser online help (accessible via the CDS Browser **Help** menu) for details.

Cell Configuration and Diagnostics

We supply two configuration tools with this release:

- **dce_config** is the cell configuration tool provided by OSF, with substantial modifications by Hewlett-Packard.
- SAM DCE Cell Configuration (SDCC), a SAM interface to **dce_config**. The SAM tool is the recommended configuration tool for HP DCE/9000.

This release also includes HP's DCE cell validation and diagnostic tools, which are not supplied by OSF: **dceval, dceping, dcewhich, camera**.

Version Identification

Version information for individual HP DCE/9000 Version 1.2 components may be obtained via **dce_version** (**/opt/dcelocal/etc/dce_version**). **dce_version** provides **what** strings (see **what**(1)) for many of the HP DCE/9000 binaries, libraries, and scripts.

dce_version will generate approximately 300 lines of output and may take a minute or longer to complete. Output may be re-directed to a file for later reference. For example:

/opt/dcelocal/etc/dce_version > save_version

The output of **dce_version** is filtered to contain only HP DCE/9000 version information.

The following is sample output from **dce_version**:

```
/opt/dcelocal/lib/libc_r_800.a:
/opt/dcelocal/lib/libc_r_800.sl:
/opt/dcelocal/lib/libdce.a:
HP DCE/9000 1.2  Module: libdce Domestic Date: Dec 17
1993 22:18:52
/opt/dcelocal/lib/libdce.sl:
HP DCE/9000 1.2  Module: libdce Domestic Date: Dec 17
1993 22:18:52
```

DES and DES-Hidden Versions of this Release

The DCE Security component uses the Data Encryption Standard (DES) algorithm as its default encryption algorithm. Because the United States State Department restricts the export of DES software, HP supplies two binary versions of this release:

- Domestic—this binary version uses the Data Encryption Standard (DES) encryption algorithm; it is available only to HP customers in the United States.

- International—this binary version hides the program entry points to DES; it is available to all HP customers.

  As well as hiding program entry points to DES, the International version of HP DCE/9000 disables the RPC data protection level "privacy" (which encrypts RPC argument values). If an Internation-version application specifies the "privacy" level of data protection, the Security runtime returns an error. This restriction does not apply to the Domestic version of this release.

Limitations of This Release

Some of the limitations described in this section reflect limitations of OSF DCE 1.0.3; others are limitations specific to this release.

Limitations of OSF DCE 1.0.3

Following are limitations of OSF DCE 1.0.3:

- There is no support for application localization (only English is supported), nor for application internationalization.
- The tool **passwd_import**, which imports user account information from **/etc/passwd** files to the Registry database, does not import the passwords themselves. Therefore, after you have used **passwd_import** to create skeletal DCE accounts in the Registry database, you must use the **rgy_edit** tool to add passwords to those accounts. This information is particularly important to customers who plan on using the DCE-integrated HP-UX login tools (**login**, etc.).

Unsupported Configurations

HP DCE/9000 Version 1.2 is not supported on diskless or trusted systems.

The HP DCE/9000 Distributed File Service (DFS) is not supported on multi-processor (MP) machines.

System Utilities Not Integrated with DCE Security

The following utilities are not integrated with DCE Security: **cron, at, rlogind, remshd, rexecd, lp.**

Interoperability and Compatibility

This section describes the interoperability of this release with various implementations of OSF DCE 1.0, and its compatibility with DCE-related technologies.

Compatibility with the HP DCE/9000 Version 1.1

Application binaries that run on the HP DCE/9000 Version 1.1 will run on HP DCE/9000 Version 1.2 unchanged.

For other compatibility and interoperability information regarding this release and HP DCE/9000 Version 1.1, see Chapter 2, *Migrating from HP DCE 1.1 to HP DCE 1.2.*

Interoperability with Other Implementations of OSF DCE 1.0

This release has been tested to ensure interoperability with implementations of OSF DCE 1.0 on the following platforms:

- DEC 3100 running OSF/1 Version 1.0.4
- IBM RS6000 running AIX Version 3.2
- DELL 486/ME running OS/2 Version 2.0
- DELL 486/ME running Gradient PC-DCE
- DELL 486/ME running DOS 3.3 + Windows/NT 3.1
- Sun SparcStation 10 running Solaris 2.2 using Transarc DCE 1.02
- IBM Powerstation 355 running AIX 3.2.4 with IBM 1.2 DCE

- DEC Alpha running OSF/1 Version 1.2

Hewlett-Packard's DCE configuration tools are not guaranteed to interoperate with other vendor's DCE implementations. In particular:

- The SDCC (SAM DCE Cell Configuration) utility will only configure HP Series 700/800 systems running HP DCE/9000 Version 1.2.
- SDCC may not reliably "discover" other vendor's systems which do not use **dce_config** for cell configuration.
- HP's version of **dce_config** is based on the OSF version, but contains enhancements specific to HP systems.

Interoperability of the DES and DES-Hidden Versions

The DES and DES-hidden versions of this release are interoperable with the following limitation: DES-based application servers or clients that specify the "privacy" RPC data protection level are not interoperable with servers or clients based on the DES-hidden version.

Neither DES nor DES-hidden versions of DCE are interoperable with any DCE version that has been built with the DES code omitted (instead of hidden). Some DCE ports from other vendors were built in this way in order to meet U.S. export requirements. If you are running a DCE port from another vendor, check with that vendor for details.

NCS 1.5.1 Compatibility

Most Network Computing System (NCS) Version 1.5.1 applications are compatible with this release – you need not rebuild them using **libdce**. The DCE Remote Procedure Call daemon (**rpcd**) incorporates the NCS Local Location Broker daemon (**llbd**) support that

NCS 1.5.1 applications require. Because the **llbd** daemon cannot coexist with **rpcd** in a cell, the DCE cell configuration tools stop **llbd** and run **rpcd** in its place.

Users of NCS-based software (such as NetLS, Omniback, HP MPower, and SharedPrint/UX) should see *Note for Users of NCS-based Software* in Chapter 4 for important HP DCE/9000 configuration information.

Kerberos Authentication Protocol Compatibility

The DCE Security authentication service implements the Kerberos Version 5 Revision 5 protocol specification. Although Kerberos Version 5 includes backward compatibility support for Kerberos Version 4, DCE Security does not implement this support.

The HP DCE/9000 Version 1.2 DCE-integrated login utilities can support Kerberos Version 4 as a secondary login protocol. See Chapter 5, *DCE-Integrated Login Utilities* for more information.

Cautions and Warnings Regarding This Release

HP DCE/9000 Version 1.2 Patch Available

Hewlett-Packard will provide a patch for HP DCE/9000 Version 1.2 to fix the following problems:

- The DFS commands **fts dump** and **fts restore** will fail and may cause a system crash in HP DCE/9000 Version 1.2.
- Some functionality used by the GDS tracing and logging facility is missing from HP DCE/9000 Version 1.2.
- XDS applications that use CDS as the underlying naming service are limited to 5 values per attribute. The limit at HP DCE 1.1 was 12; the limit of 12 is restored by the patch.

To obtain this patch, you should request one or more of the following patch numbers (depending on your system type) from your HP Service Representative or support channel. Hewlett-Packard expects these patches to be available at the time you receive HP DCE/9000 Version 1.2.

Table 1 **HP DCE/9000 Version 1.2 Patches**

PHSS_3626	S700 Domestic
PHSS_3627	S700 International
PHSS_3628	S800 Domestic
PHSS_3629	S800 International

Security and Remote Login Utilities

You may use standard UNIX remote login utilities (**remsh**, **rlogin**, **telnet**) to perform remote DCE cell administration. However, these utilities expose the cell administrator's password to network attackers whenever you perform a task on a remote system. If a network attacker obtains the password, the security of the cell's DCE services will be compromised. The most secure way to perform cell administration is to log in locally to each system you wish to administer.

Removing DCE Credentials

A user's DCE credentials are not automatically removed by exiting a shell or logging out. Unless you plan to leave background processes running that require your DCE credentials, you should manually remove your credentials before logging out by running the **kdestroy** utility. This will make the system more secure by decreasing the opportunity for someone to maliciously gain access to your network credentials.

If you do not use **kdestroy**, DCE credentials are retained in the directory **/opt/dcelocal/var/security/creds**. To avoid unnecessary disk space usage, inactive credential files should be periodically purged from this directory. To avoid removing active credential files, we recommend that you purge this directory during system reboot (from **/etc/rc**), before **rc.dce** is executed.

In HP DCE/9000 Version 1.2, the **kdestroy** command has been modified to allow destruction of credentials older than a specified number of hours. **kdestroy -e** *exp-period* may be run manually or regularly as a **cron** job to purge older credential files. See **kdestroy**(1) for syntax and usage information.

DCE-Integrated UNIX Login Utilities

The DCE-integrated versions of the HP-UX login utilities are installed, but are not activated, by the HP DCE installation and configuration procedure. This is because most systems will require considerable work transferring account information from **/etc/passwd** to the DCE Security Registry before the system will be useful. A script, **dce.login**, is supplied to activate the utilities once your system has been set up with the needed accounts. See Chapter 5, *DCE-Integrated Login Utilities*, for more information about using the **dce.login** script.

You should not use the **dce.login** script to activate the DCE-integrated login utilities until *after* you have set up the accounts necessary for your site in the DCE security service registry.

ANSI C Requirement for HP DCE/9000

Hewlett-Packard only supports use of the ANSI C compiler when building HP DCE applications. Hewlett-Packard cannot provide support for problems with HP DCE applications that were not compiled using ANSI C.

Setting NLSPATH Environment Variable

Users of HP DCE/9000 should set the NLSPATH shell environment variable to include **/usr/lib/nls/%L/%N**. See the **environ**(5) man page for details on NLSPATH syntax.

Documentation

Documentation for this release includes manuals, online man pages, and online help for the SAM DCE Cell Configuration Utility.

Manuals

The following manuals are included with HP DCE/9000 Version 1.2. Hewlett-Packard part numbers are listed in parentheses:

- Introduction to OSF DCE (B3190-90005)
- Understanding DCE (B3190-90018)
- OSF DCE User Guide and Reference (B3190-90017)
- HP DCE/9000 Release Notes (B3190-90019)
- OSF DCE Administration Guide Volume II – Core Components (B3190-90009)
- OSF DCE Administration Guide Volume III – Extended Services (B3190-90010)
- OSF DCE Administration Reference (B3190-90008)
- OSF DCE Application Environment Specification (B3190-90011)
- OSF DCE Application Development Guide (B3190-90006)
- OSF DCE Application Development Reference (B3190-90007)
- Guide to Writing DCE Applications (B3190-90012)
- Programmer's Notes on HP DCE Threads (B3190-90002)

The documentation set that accompanies this release consists of both OSF and HP manuals.

The prefaces of the OSF manuals list several OSF DCE publications that are not included in the Core Services manual set:

- *OSF DCE Porting and Testing Guide*

- *OSF DCE Release Notes*

  These manuals are intended for OSF DCE source code licensees, and are not needed by users of this release.

  The manual *OSF DCE Administration Guide Volume I – Introduction* is also not included with this release. The information contained in that manual is provided in these release notes.

Man Pages

Reference pages describing DCE commands and calls are available online in the form of man pages.

There are two styles of man page headers:

- "OSF" or "Open Software Foundation "–This header means that the man page originates from OSF and has not been changed by HP.
- "HP DCE "–This header means that the man page either originates from HP or is an OSF man page that HP has changed.

Man pages are provided in the following directories:

/opt/dcelocal/usr/man/man1.Z
/opt/dcelocal/usr/man/man2.Z
/opt/dcelocal/usr/man/man3.Z
/opt/dcelocal/usr/man/man4.Z
/opt/dcelocal/usr/man/man5.Z
/opt/dcelocal/usr/man/man7.Z
/opt/dcelocal/usr/man/man8.Z

To read man pages with the **man** command, you need to include **/opt/dcelocal/usr/man** in your MANPATH shell environment variable. For example, in the Korn shell, set the variable as follows:

export MANPATH=/opt/dcelocal/usr/man:/usr/man

If you have already set the MANPATH shell environment variable, set the variable as follows:

export MANPATH=/opt/dcelocal/usr/man:$MANPATH

You can set the MANPATH environment variable:

- For the current shell session, by issuing the "export MANPATH" command line (given above) at the shell prompt.
- Permanently, by putting the "export MANPATH" command line in the appropriate environment configuration file:
  - **.vueprofile** in a user's home directory (sets for that user).
  - **/usr/vue/config/Xsession** for all users on a system.

After setting the MANPATH environment variable, you can access a man page simply by typing

man *command*

where *command* is the desired command or call. The man pages may also be accessed through HP DCE Online Help, which is described in the next section.

Instructions for installing the HP DCE/9000 man pages are in Chapter 3, *Installing HP DCE/9000*.

HP DCE/9000 Online Help

HP DCE/9000 Version 1.2 provides a DCE Online Help feature. The DCE Online Help contains online help volumes about various aspects of HP DCE. Hyperlinks let you jump from one volume to another, display related topics within a help volume, and do special things, like display man pages. The DCE Online Help is integrated into the HP Help System, so you can access it from the HP VUE Front Panel help icon.

NOTE This feature is supported on X-based displays only; it is not available on ASCII terminals.

Help Contents

This version of HP DCE/9000 Online Help contains the following kinds of help:

- Guide to HP DCE/9000 hardcopy documentation. Provides a listing

and brief description of the manuals available for Version 1.2 of HP DCE/9000 and HP DCE/9000 Application Development Tools. Each manual's Table of Contents and Index are provided to help you quickly locate information about a particular aspect of HP DCE/9000.

- List of DCE man pages according to man section, with hyperlinks to the actual man pages. (**Note**: To access the man pages through HP DCE Online Help, you must set the MANPATH environment variable in either **$HOME/.vueprofile** or in **/usr/vue/config/Xsession**. See page 16 for details).
- Easy access to the online version of the release notes for both HP/DCE 9000 and HP/DCE 9000 Application Development Tools.
- Access to help on the CDS Browser and the HP DCE Sample Applications.
- A Customer Comments form so you can send us feedback about the HP DCE Online Help system.

NOTE The main menu of the Help Manager lists the HP DCE/9000 Application Development Tools Release Notes and HP DCE Sample Applications. These help topics are available only if the HP DCE/9000 Application Development Tools optional product is installed.

Accessing DCE Online Help

You can access the DCE Online Help from the HP VUE Front Panel or from a shell prompt.

To access the DCE Online Help from the VUE Front Panel,

1 Click on the Front Panel help icon (the "?"). A "Welcome to Help Manager" help window appears.

2 In the Help Manager window, click on the "HP DCE/9000, Version 1.2" product-family title. A list of the HP/DCE 9000 help volumes appears.

3 To display a help volume, click on its title.

To access the DCE Online Help from a shell prompt, enter this command:

/usr/vue/bin/helpview -h DCEwelcome

This displays an introductory help window that has hyperlinks to all of the other help volumes in the HP DCE Online Help system.

Note that you can press the **F1** key in any help window to get help on using the help system.

Online Help for HP DCE Cell Configuration Tool

The HP SAM DCE Cell Configuration (SDCC) tool includes context-sensitive online help. SDCC is a graphical interface to **dce_config**. The online help for SDCC assumes you understand basic DCE concepts and use of the HPUX 9.0 SAM interface.

Notes to Programmers

This section contains information for programmers, primarily about building and debugging HP DCE applications.

Building DCE Programs

When compiling and linking HP DCE applications, note the following:

NOTE Hewlett-Packard supports only ANSI C for creating HP DCE applications.

- In order for the correct header file contents to be used, define **_HPUX_SOURCE** when compiling your HP DCE application: **-D_HPUX_SOURCE.**
- You must define **_REENTRANT** when compiling HP DCE programs:
  - To ensure that the threadsafe routines such as **putc, putchar, getc,** and **getchar** are used instead of the nonthreadsafe macro versions defined in **stdio.h.**
  - To get definitions of new structures and to provide ANSI C prototype information for the new reentrant interfaces.
- If you include **<pthread.h>,** you must do so before other header files in your C source file. Also note that **<pthread.h>** defines **_REENTRANT.**
- Source code that is built into applications that use the CDS, RPC, or security APIs must include **<pthread.h>** . This is necessary because the DCE RPC runtime library creates a small number of private threads, on both the client and server sides of an application.
- You must use the **-I** option to ensure that the header files corresponding to the reentrant C library are used instead of the standard header files (**-I/usr/include/reentrant**). The DCE header files are included as **<dce/***header.h***>,** so that they may be found in **/usr/include/dce** without the need to include an explicit **-I** option to the C preprocessor.

- DCE applications must be linked with the following libraries in the following order: **-ldce -lndbm -lM -lc_r**

  Other libraries may be interspersed among and between these four, as long as **-lc_r** is last. Never link in **libc** when building a DCE application.

- **libdce** and **libc_r** are located in **/usr/lib**.
- When linking your DCE application with any shared library, including **libdce.sl,** you must use the following linker options:

  -Bimmediate -Bnonfatal

  (if calling the linker via **cc**, use **-Wl,-Bimmediate -Wl,-Bnonfatal**)

Notes on Debugging HP DCE Applications

The following are tips on debugging HP DCE applications. Also see *Programmer's Notes on HP DCE Threads* for additional information about debugging HP DCE Applications.

- HP DCE uses several HP-UX signals internally (SIGCHILD, SIGSYS, and SIGVTALARM). When debugging HP DCE servers or clients, you must ensure that these signals, when received, are passed along to the target process. If you are using DDE 2.0 or **xdb,** you can modify your debugger startup files as follows:

  ~/.dderc:
  alias ` after_debug [ignore SIGCHILD; ignore SIGSYS; ignore SIGVTALARM]

  ~/.xdbrc:
  z 12 rs # do not stop or report SIGSYS
  z 18 rs # do not stop or report SIGCHILD
  z 20 rs # do not stop or report SIGVTALARM

  Note: A DCE application should not catch, ignore, or block SIGSYS. See *Programmer's Notes on HP DCE Threads* and page 33 in these release notes for more information on the use of signals with HP DCE applications.

- Be sure the application has an exception handler installed that can field any RPC exceptions.
- Start **rpcd** with the **-D** option, which turns on the default RPC runtime debug output.
- Run the server side of your application under the debugger so that exceptions raised in server code will trap into the debugger rather than being reflected back to the client process via RPC. This makes it easier to identify bugs in the server that might otherwise appear to be client bugs.

Using HP DCE with C++ Applications

It is possible to use C++ to write DCE applications if proper precautions are taken. There are some serious limitations that the user must be aware of when using C++ and DCE. Most of these issues relate to lack of thread safety of C++ operations. We expect most of these issues to be resolved at the HP-UX 10.0 release.

The following list details practices to be avoided when using C++ to develop DCE applications. The list applies to HP C++ compiler version 3.20.

- Do not use C++ exceptions. The stack unwinding that occurs when a C++ exception is raised is not guaranteed to work in the presence of multiple RPC threads.
- Do not use thread unsafe C++ constructs in user created threads. These constructs include C++ iostream utilities and dynamic allocation of arrays using new and delete. In particular, these constructs should not be used in server manager routines unless the server is set up to spawn only one listener thread. Use of these constructs on the client side should be OK.
- DCE CMA exceptions should never be allowed to propagate into a C++ scope. Allowing this to happen could result in destructors failing to be executed. This can lead to memory leaks and unexpected behavior. For example, suppose some C++ code makes a call to a C function. Within this C function, a CMA exception can be raised. It is very important that the CMA exception also be caught within the C function.

If it is not, then the CMA exception could propagate into the C++ environment, resulting in unexpected behavior.

- The DCE header file idlbase.h contains a type declaration that is not properly processed by the C++ compiler. If any C++ code includes idlbase.h, the definition for the type handle_t in the file /usr/include/dce/idlbase.h should be modified similar to the following. Note that many other DCE header files include idlbase.h.

```
#ifdef _cplusplus
typedef struct {
        unsigned short offset;
} _priv_handle_data_t, *handle_t;
#else
typedef struct {
        unsigned short offset;
} *handle_t;
#endif
```

The C++ compiler will be fixed to properly compile idlbase.h in a future release. If the above change is not made, the compiler currently generates multiple mangled names for variables of the type handle_t. This results in obscure undefined variable errors.

By taking the above precautions, the user should be able to productively use C++ to write DCE applications.

Notes on Programming with HP DCE

The following are miscellaneous notes on programming with HP DCE. Also see *Programmer's Notes on HP DCE Threads* for additional information.

To-Be-Obsoleted libc_r Routines

Hewlett-Packard does not intend to support the following routines at HP-UX 10.0. If forward compatibility is a consideration, you may want to avoid using these routines when creating HP DCE applications:

Table 2 **To-Be-Obsoleted libc_r Routines**

clnt_spcreateerror_r	clnt_sperrno_r	clnt_sperror_r	endnetgrent_r
endrpcent_r	getnetgrent_r	getrpcbyname_r	getrpcbynumber_r
getrpcent_r	setnetgrent_r	setrpcent_r	

Appropriate Uses of the Cell Directory Service

The Cell Directory Service (CDS) is designed to store and retrieve server bindings in a DCE cell. This mission includes many assumptions about the volume of information that must be stored and about the types and frequency of access to that information. The CDS use of memory, disk, cache, network, timeouts, and performance tradeoffs are all optimized to this very specialized purpose.

The generality of the application programming interfaces to CDS mask this specialized purpose and makes CDS appear to be a general-purpose database system. But this is not the case, and the optimizations of CDS for its low-volume and weakly-replicated storage and retrieval of server bindings in a fairly static namespace are rarely optimal for other purposes. Moreover, other uses of CDS all directly compete with and interfere with its use and availability as a critical core component of the DCE system.

Application developers are frequently tempted to use CDS for the direct storage of information other than server bindings. For example, the developer of a telephone number directory service may consider using CDS to store the information directly. This is a bad idea, as the volume of information could overwhelm the in-memory CDS data structures, and very frequent read accesses could slow CDS performance and lock out DCE server lookup requests. A much better strategy would be to implement a database server designed specifically for the telephone number directory service, and then store the bindings of that server in CDS for lookup by clients. In this way, other uses do not compromise CDS in its intended use as a critical DCE component.

Cell Directory Service Programming Interfaces

The supported and documented programming interfaces to CDS are the RPC Name Service Independent (RPC_NS) interface and the X/Open Directory Service (XDS) interface. The RPC_NS function call prototypes are in the include file **/opt/dcelocal/share/include/dce/rpc.h**. The XDS function call prototypes are in the include file **/opt/dcelocal/share/include/xds.h**. The RPC_NS interface is the procedural interface used by the core DCE components and most applications. The XDS interface is an object-oriented interface appropriate for use with other X/Open standards such as X.500. Both the RPC_NS and XDS interfaces support many common namespace functions, but lack administrative capabilities such as the ability to create and delete directories and manage replication.

The CDS Control Program (**cdscp**), is the only supported and documented way to perform administrative functions in CDS such as creating and deleting directories and managing replication. **cdscp** can be called in a shell script, but is not a programming interface.

An *unsupported* and undocumented programming interface to CDS is the Cell Directory Service Programming Interface (CDSPI). CDSPI is the native internal interface to CDS that is used by **cdscp**. CDSPI provides a programmatic interface to all CDS functionality, including all administrative functionality. The CDSPI function call prototypes are in the include file **/opt/dcelocal/share/include/dce/cdsclerk.h**. This interface is subject to change, and so must be used only when functionality unavailable in the other interfaces is essential. Use of this interface should be carefully isolated so that updates to your applications that might be required by changes in future DCE releases can be easily accomplished.

Group Requirement for Writing CDS Namespace

All DCE programs that write portions of the CDS namespace (for example, programs that export their bindings), must run as principals that are members of the group **subsys/dce/cds-server**.

Problem with IDL and Conformant Arrays

HP DCE/9000 1.2 (and 1.1) **idl** and **i2dl**, based on OSF DCE 1.0.2, has a known defect relating to the use of conformant arrays. When a conformant array's element type has a string attribute, the **idl** generated stub file tries to allocate more memory than needed. For instance, given the following interface definition:

```
typedef [string] char string_t [MAX_STRING_LENGTH];
void read_strings (
    [in] handle_t h,
    [in] long size,
    [out, size_is(size)] string_t s[],
    [out] error_status_t *status); }
```

the **idl** generated server stub file will allocate size*MAX_STRING_LENGTH*sizeof(string_t) bytes of memory for the argument "s" instead of size*MAX_STRING_LENGTH*sizeof(char) bytes, which could result in the **rpc_s_fault_remote_no_memory** error:

382312582 (decimal), 16c9a086 (hex): fault remote no memory (dce / rpc)

The workaround is to remove the string attribute from the conformant array's element type. This will eliminate the potential for a memory allocation failure, at the expense of transmitting the entire **string_t** array over the wire (instead of transmitting only the characters up to and including the null character).

RPC Changes in OSF DCE 1.0.3

- The behavior of **rpcd** has been changed in DCE 1.0.3 so that requests from remote hosts to add or delete endpoints from the endpoint map will now be rejected (in previous versions of DCE, **rpcd** would fulfill such requests). The change has been made in order to prevent the possibility of unauthenticated users adding or deleting endpoints anywhere in a cell, simply by making calls through the RPC interface, or by issuing commands through **rpccp**.

  The effect of this change is that the **rpccp** commands **remove mapping** and **add mapping** will no longer work with remote endpoints,

while **rpccp show mapping** will still work. Note that the change has no effect on DCE configuration.

- The capability to restrict the assignment of endpoints to those in a user-specified set has been added to RPC in DCE 1.0.3. This allows DCE applications to operate in environments in which inter-network traffic is restricted to specified endpoints. The facility is activated by setting the RPC_RESTRICTED_PORTS environment variable with the list of endpoints to which dynamic assignment should be restricted before starting an RPC application. RPC_RESTRICTED_PORTS governs only the dynamic assignment of server and client ports by the RPC runtime. It does not affect well-known endpoints.

  The facility is turned on by setting the RPC_RESTRICTED_PORTS environment variable before starting an RPC application. The syntax of the variable is as follows:

  ```
  <entry> [COLON <entry>]*
  <entry> : <protseq_name> LEFT-BRACKET <ranges> RIGHT-BRACKET
  <ranges>: <range> [COMMA <range>]*
  <range> : <endpoint-low> HYPHEN <endpoint-high>
  ```

  For example:

  ```
  ncacn_ip_tcp[5000-5110,5500-5521]:ncadg_ip_udp[6500-7000]
  ```

  To use RPC_RESTRICTED_PORTS for DCE itself, set the environment variable before starting your cell. The environment variable must be set whenever you restart DCE.

  Note that this facility does not add any security to RPC and is not intended as a security feature. It merely facilitates configuring a network "firewall" to allow incoming calls to DCE servers.

RPC Authentication

The *DCE Application Development Guide* and *DCE Application Development Reference* may be misleading about what happens when an unauthenticated client calls a server that has specified authentication. In such a case, the RPC runtime will not perform any authentication, and the call will reach the application manager code. It is up to the manager to decide how to deal with the unauthenticated call.

Typically, servers and clients establish authentication as follows:

- The server specifies an authentication service for a principal identity under which it runs by calling **rpc_server_register_auth_info**(). The authentication service is specified by the **authn_svc** parameter of this call. Currently, servers may specify either DCE secret key authentication (by supplying either **rpc_c_authn_dce_secret** or **rpc_c_authn_default**), or no authentication (by supplying **rpc_c_authn_none**). The specified authentication service will be used if it is also requested by the client.
- The client sets authentication for a binding handle by calling **rpc_binding_set_auth_info**(). The choices are also currently either DCE secret key or no authentication. Client calls made on the binding handle attempt to use the specified authentication service.
- The server manager code calls **rpc_binding_inq_auth_client**() to extract any authentication information from the client binding for the call.

Whether the call actually wakes up in the server manager code or is rejected by the runtime depends on the following conditions:

- If the client specified no authentication, then none is attempted by the RPC runtime. The call wakes up in the manager code whether the server specified authentication or not. This permits both authenticated and unauthenticated clients to call authenticated servers. When the manager receives an unauthenticated call, it must make a decision about how to proceed.
- If the client specified DCE secret key authentication and the server specified no authentication, then the runtime will reject the call, and it will never reach the manager routine.
- If both client and server specified DCE secret key authentication, then authentication will be carried out by the RPC runtime transparently. Whether the call reaches the server manager code or is rejected by the runtime will depend on whether the authentication succeeds.

Although the RPC runtime is responsible for any authentication that is carried out, the fact that the runtime will always permit unauthenticated clients to reach the manager code means that a manager access function typically does need to make an authentication check. When the manager access routine calls

rpc_binding_inq_auth_client(), it should check for a return status of **rpc_s_binding_has_no_auth**. When such a status is returned, it means that the client has specified no authentication, and the manager access function will have to make an access decision based on this fact. Note that in such a case, no meaningful authentication or authorization information is returned from **rpc_binding_inq_auth_client**().

RPC Data Transfer Limitation

The bulk data transfer, e.g., IN/OUT-pipes, over the connection-oriented (TCP/IP) RPC protocol is limited by the performance difference between the client and server machines. If the receiver process is significantly slower than the sender process (and cannot process data fast enough), the receiver process's virtual memory usage may grow rapidly until the receiver process aborts with a **no more swapspace** error.

Restricting RPC Addresses

The runtime now looks for a RPC_SUPPORTED_NETADDRS environment variable, which allows a user/administrator to restrict the network addresses that a DCE server will advertise in the namespace/endpoint-map.

If this environment variable is set, only addresses in the list will be advertised in the namespace/endpoint map. Addresses not found on the list will be excluded from the server's list of available addresses.

The format of the RPC_SUPPORTED_NETADDRS string is as follows:

```
RPC_SUPPORTED_NETADDRS=protseq:netaddr[,protseq:ne-
taddr]
```

For example,assuming that host **myhost** is located at IP address 10.3.2.1, the Korn shell statements:

```
$ export RPC_SUPPORTED_NETADDRS=ip:myhost
```

or

```
$ export RPC_SUPPORTED_NETADDRS=ip:10.3.2.1
```

will force any servers started in the current shell to support only the addresses associated with the name **myhost** and the network address **10.3.2.1**.

Calling exec() from a DCE Application

Care must be used when calling **exec**() from a DCE application. HP DCE Threads sometimes sets open file descriptors to non-blocking mode, so that I/O calls block only the calling thread, not the entire process. This occurs unbeknownst to the application itself. HP provides wrappers for the **exec**() family of calls that, among other things, resets file descriptors to blocking mode if they were set non-blocking by HP DCE Threads and not the application.

For file descriptors that were inherited across **fork**(), this also has the effect of resetting the file descriptor to blocking mode in the parent as well as the child. If the parent is a threaded program, it can cause the parent to hang due to a blocking I/O call.

There are two possible work-arounds:

- If the process will not need the open file descriptor, set the close-on-exec flag for the file prior to calling **exec**(). The file descriptor will not be reset in this case.
- Avoid using the **exec**() wrapper, calling **exec**() directly instead. This is accomplished by undefining the appropriate macro, for example:

  #undef execle

  Note that if the **exec**() wrapper is circumvented, the new process may inherit file descriptors that are unexpectedly set non-blocking; some signals may be unexpectedly ignored or not ignored; and, if **exec**() is called without first calling **fork**(), the new process will probably be killed by SIGVTALRM as soon as it begins execution.

Process Forking

Process forking from within RPC applications that use the connection-oriented (TCP/IP) RPC protocol is not supported.

While it is generally safe for an application to perform a fork followed immediately by an **exec**(), the following sequence may not work for TCP/IP RPC programs:

- The TCP/IP RPC process forks.
- The child process tries to use RPC over the TCP/IP protocol before the **exec**().

Process forking from within RPC applications that use the connectionless protocol (UDP/IP) is supported, with the following restrictions:

- For client-side applications, the UDP/IP protocol is fork safe. It is the responsibility of the application developer to ensure that all other application threads are capable of crossing forks safely.
- On the server side, the only supported behavior is for a server thread to fork and exec, with no use of RPC in the child of the fork until after the exec.

Note that process forking may not be available in other vendors' DCE offerings that are based on OSF DCE 1.0.2 or earlier. If portability to other DCE 1.0.2-based offerings is a concern, restrict your source code to the fork-followed-by-exec model of operation. DCE products based on OSF DCE 1.0.3 and beyond will have UDP/IP process forking support.

File Locking

The HP DCE Threads **fcntl**() wrapper does not provide for thread-synchronous file locking. The entire process will block when a call to **fcntl**() specifies F_SETLKW and the file is currently locked by another process.

Note also that HP-UX file locks are a process-wide resource. For this reason, if multiple threads call **fcntl**() to lock the same section of a file, all the calls will succeed, and each thread will believe it holds the lock. However, only a single, process-wide lock is actually obtained—the first call obtains the lock, the second and subsequent

calls have no effect. If one thread releases this lock, the other threads will continue to believe the file is locked, when in fact the process no longer holds any lock on that section of the file.

Use mutex locks to ensure that only one thread at a time locks a particular file or section of a file.

The previous comments regarding file locking with **fcntl**() also apply to **lockf**(). **lockf**() is not wrapped by DCE Threads.

sec_id_parse_name()

In previous HP DCE releases, the **sec_id_parse_name** library call could be passed a NULL pointer or null string for the global principal name, and would return the local cell name. This behavior is maintained in HP DCE/9000 Version 1.2, but will not be supported in future HP DCE releases. Instead, pass "/.:" to obtain this result.

sec_login_valid_and_cert_ident()

The **sec_login_valid_and_cert_ident**() routine uses **fcntl**() for file locking, and should not be called by more than one thread at a time. If you must use **sec_login_valid_and_cert_ident**() in multiple threads, use a mutex to insure that only one thread at a time executes the call. No HP DCE programming interfaces call **sec_login_valid_and_cert_ident**() internally.

Applications that need to obtain credentials in multiple threads will generally only need to call **sec_login_validate_identity**(), which is not affected by **fcntl**().

semop()

The HP DCE Threads **semop**() will not increment the **semncnt** kernel variable. The value of **semncnt** should not be trusted when using **semop**() to perform semaphore operations.

signal()

Use of the **signal**() system call is not supported by HP DCE Threads, as it can interfere with signal handlers that are installed by Threads. In some cases, you can retain **signal**() calls in legacy code:

- Implement a wrapper for **signal**() that calls **sigaction**() and/or **sigwait**().
- Use **signal**() itself to install a handler for a signal, provided the signal is not SIGVTALRM, SIGCHLD, or SIGSYS, and provided no thread installs a handler for the signal with **sigaction**() or waits for the signal with **sigwait**().

system()

The HP DCE Threads **system**() wrapper does not block SIGCHLD. It does set the handler for SIGQUIT and SIGINT to SIG_IGN, but only for the calling thread. This behavior differs from the behavior of the standard HP-UX version of **system**().

vfork()

The HP DCE Threads **vfork**() wrapper cannot be circumvented. The methods used to circumvent other wrappers (defining _CMA_NOWRAPPERS_, undefining **vfork**, defining **vfork** to be **_vfork_sys**) do not work.

2

Migrating from HP DCE 1.1 to HP DCE 1.2

Migrating from HP DCE 1.1 to HP DCE 1.2

This chapter discusses migration procedures and compatibility issues in moving from HP DCE/9000 Version 1.1 (HP DCE 1.1) to HP DCE/9000 Version 1.2 (HP DCE 1.2). If you are installing HP DCE for the first time, proceed directly to Chapter 3, *Installing HP DCE/9000*.

If you have previously installed HP DCE/9000 Version 1.1, you may save your existing cell configuration and databases, install HP DCE/9000 Version 1.2, and then restore your former cell configuration. You may, instead, abandon your previous cell configuration and database information, update your systems to HP DCE 1.2, and configure a new cell from scratch.Both procedures are detailed in this chapter.

If you currently have an HP DCE release older than Version 1.1, and you wish to retain your cell configuration and databases, you must update to Version 1.1 before moving to Version 1.2.

Systems running HP DCE 1.1 will interoperate in a cell with systems running HP DCE/9000 Version 1.2. However, the HP DCE 1.2 SDCC (SAM DCE Cell Configuration) utility will *not* interoperate with the HP DCE 1.1 SDCA Tool – attempting any configuration operation with either tool in a mixed 1.1/1.2 cell may result in incorrect configuration or operation of the cell.

Migration compatibility between HP DCE 1.1 and HP DCE 1.2

- It is possible to individually migrate each system in an HP DCE 1.1 cell to HP DCE 1.2. Since HP DCE 1.1 and HP DCE 1.2 clients and servers are compatible, the systems may be migrated in any order over a period of time. However, Hewlett-Packard recommends that you migrate all of your cell member systems to HP DCE 1.2 as soon as you are able to do so.
- Neither the SDCA (SAM DCE Cell Administration) nor SDCC (SAM DCE Cell Configuration) utilities can be used to administer a mixed HP DCE 1.1/HP DCE 1.2 cell. Only the **dce_config** utility may be used to configure a mixed-version cell.
- Because of minor changes to the **dce_config** utility at HP DCE 1.2, scripts that were written to use the HP DCE 1.1 **dce_config** may have to be modified to work with HP DCE 1.2 **dce_config**.

HP DCE/9000 Migration Procedure

WARNING If you are using the HP DCE 1.1 DCE-integrated login utilities, see *Migration Notes for Integrated Login Users* on page 6 of this chapter before beginning your migration to HP DCE 1.2.

Migrating without retaining cell configuration

If you have HP DCE 1.1 on a system that you are updating, but you do not want to preserve your existing cell configuration:

1 Stop the cell using **dce_config** "STOP" at each cell member or run SDCA from SAM to stop the entire cell.

2 Use **dce_config** "REMOVE" or SAM to remove the cell databases.

3 Use **/etc/rmfn** to remove your HP DCE 1.1 filesets.

4 Proceed to Chapter 3, "Installing HP DCE/9000 ", in this document.

Migrating current cell configuration

If you have HP DCE 1.1 on your system, and you want to preserve your existing cell environment:

1 Copy the **/etc/rc.dce** file to **/etc/rc.dce_1.1**.

Do this for each cell member that you are migrating to HP DCE 1.2. The **rc.dce** file lists the daemons running on that cell member. The installation procedure loads a new **rc.dce** file and copies the settings

from **/etc/rc.dce_1.1** to the new file. If the installation does not find **/etc/rc.dce_1.1**, it cannot copy the settings and you will have to set the daemons by editing the newly installed **rc.dce** file.

2 If you are migrating a system that is running the security server (**secd**), stop **secd** by issuing the sec_admin> **stop** command on that system.

3 If you are migrating a server system, stop the cell using **dce_config** "STOP" at each cell member or run SAM to stop the entire cell. If you are migrating a client system, you only need to stop DCE on that system.

4 Save any customized files that you have made. User-customizable files are discussed in the next section.

5 Use **/etc/rmfn** to remove your HP DCE 1.1 filesets.

6 Proceed to Chapter 3, *Installing HP DCE/9000*.

7 After you have installed HP DCE 1.2, merge changes from your user-customizable files into the new HP DCE 1.2 versions.

User-customizable files in HP DCE 1.1

The following is a description of various user-customizable files in HP DCE 1.1.

1 DTS configuration is stored in **/etc/rc.dts**. If you wish to retain your previous DTS configuration, you must save the HP DCE 1.1 version of this file to a temporary location, and merge your changes into the HP DCE 1.2 version of **/etc/rc.dts**.

2 If you plan to use ENCINA with HP DCE 1.2, you should remove the following commented line from **/opt/dcelocal/hpadmin/etc/nondcesvc** before installing HP DCE 1.2:

```
# /.:/$(ENCINA_CDS_ROOT)/sfs/$(ENCINA_SFS_SERVER) NAMESPACE PROMPT
```

This line interferes with DCE and ENCINA customize scripts.

3 If you have customized the following configuration files for HP Camera and HP Admin, HP DCE 1.2 versions will be installed in

/etc/newconfig:

```
/opt/dcelocal/hpcamera/etc/snapshot.des
/opt/dcelocal/hpadmin/etc/nondcesvc
/opt/dcelocal/hpadmin/etc/wellknownif
```

After you have installed HP DCE 1.2, you must manually merge your customizations into the new files, and copy the resulting files back into **/opt/dcelocal/hpcamera/etc** and **/opt/dcelocal/hpadmin/etc**.

NOTE The versions of these files in /opt/dcelocal/hpcamera/etc and /opt/dcelocal/hpadmin/etc may be machine-modified during the HP DCE 1.2 install process. Do not simply copy the versions in /etc/newconfig over the versions in /opt/dcelocal; you must manually merge these files in order to be certain that all changes are retained.

4 The following CDS files may be user-customized to include new attributes and globalnames:

```
/opt/dcelocal/etc/cds_attributes
/opt/dcelocal/etc/cds_globalnames
```

These files are over-written during the HP DCE 1.2 install process. If you have customized these files at HP DCE 1.1, you must save those customizations and manually merge your changes into the HP DCE 1.2 versions of these files.

Migration Notes for Integrated Login Users

If you are using the HP-UX DCE-integrated login utilities at HP DCE1.1, you should do the following as part of your migration procedure:

1 Before stopping your cell (via **dce_config** STOP or SAM), check that **/etc/passwd.nodce** contains accurate account and password information for the system. If it does not, manually copy **/etc/passwd** to **/etc/passwd.nodce**. The STOP operation will move **/etc/passwd.nodce** back to **/etc/passwd**, so you must be certain that **/etc/passwd.nodce** contains accurate account and password information.

2 Before removing HP DCE 1.1, save your **/opt/dcelocal/etc/passwd_override** file to a temporary location, and restore it after you install HP DCE 1.2.

3 After you update to HP DCE 1.2, activate the DCE-integrated login utilities by running **dce.login install**. See the Chapter 5, *DCE-Integrated Login Utilities* for information about changes and improvements to these utilities at HP DCE 1.2.

3

Installing HP DCE/9000

Installing HP DCE/9000

This chapter describes the recommended procedures for installing and deinstalling HP DCE/9000 Version 1.2 software.

The procedures in this chapter involve using the **updist**, **update**, and **rmfn** tools in interactive mode. You can also use these tools from a command line in non-interactive mode. See the manpages *updist*(1M), *update*(1M), and *rmfn*(1M) for more information.

See the manual *Installing and Updating HP-UX 9.0,* for more information on all aspects of installation.

After completing the installation of HP DCE/9000 Version 1.2 software, you must configure your cell. Chapter 4 contains HP DCE/9000 cell configuration information.

Overview

The following is an brief overview of the installation process described in this chapter:

- Verify that hardware and software prerequisites are met at your site.
- Plan where you will install various HP DCE filesets.
- Load HP DCE software from media to a network distribution area using the **updist** tool.
- Install filesets on individual systems using the **update** tool.
- Remove unwanted filesets using **rmfn**.

Prerequisites

Hardware and Software Requirements

Any system that you want to make a member of a cell must meet certain hardware and software requirements. The system requirements are:

System Type	HP 9000 Series 700 or Series 800, including MP systems.
Operating System	HP-UX 9.03 (for Series 700 Systems) or HP-UX 9.04 (for Series 800 Systems) or later HP-UX release..
Kernel Configuration	The HP-UX kernel parameter **semmni** should be set to 64. For server systems, the HP-UX kernel parameter **maxfiles** must be at least 256. For systems running DFS, **bufpages** should be set to 10% of system memory: approximately 819 for 32-Mb systems; 1638 for 64-Mb systems. You can check and, if necessary, change these values via SAM (the HP-UX System Administration Manager). For Series 800 systems, also see S800 Kernel Parameter Recommendations, in this chapter.
Software Dependencies	You must have the BSDIPC-SOCKET fileset installed. These are optional filesets on HP-UX; BSDIPC-SOCKET can be found under the NET-CORE partition.
Memory	A minimum 32 Mb of memory is recommended for client-only systems; 64 Mb for server systems.
Swap Space	A minimum 50 Mb of swap space is recom-

	mended for client-only systems; at least 100 Mb is recommended for systems running one or more DCE servers. Device swap is strongly recommended over file system swap.
File System	HP DCE/9000 must be installed on a long-name file system. If you have a short-name file system, you must first run **convertfs**(1m) to convert your file system to long names.

S800 Kernel Parameter Recommendations

Hewlett-Packard has found that the following kernel parameter values may be useful for increasing performance on Series 800 systems, particularly when under high load conditions. These parameter settings may also be of use for Series 700 users.

Table 3 **Recommended Kernel Parameter Values for S800 Systems**

Parameter Name	Default Value	Suggested Value
MAXUPRC	100	128 or 256
MSGMAP	100	258 (MSGTQL + 2)
MSGMAX	8192	32768
MSGMNB	16384	32768
MSGSEG	1024	7168
MSGTQL	40	256
NBUF	1536	2048
NFLOCKS	200	256
NINODE	4096	8192
NPTY	60	128
NTEXT	256	512

Table 3 **Recommended Kernel Parameter Values for S800 Systems**

Parameter Name	Default Value	Suggested Value
SEMMAP	10	66 (SEMMNI + 2)
SEMMNI	10	64
SEMMNS	60	128
SEMMNU	30	64
SEMUME	10	32
SHMMNI	100	128
SHMSEG	12	32

Distribution Media

The HP DCE/9000 Version 1.2 software is shipped on a variety of distribution media, including 8mm DAT tapes and CD-ROM discs.

If you have purchased an international version of HP DCE/9000 on CD-ROM, you will need to have the appropriate codeword available prior to installation. The codeword allows you to access the software that you purchased. To obtain a codeword, follow the instructions on the codeword certificate that was shipped with the CD-ROM disc. No codeword is necessary for the domestic versions of HP DCE/9000.

See the manual, *Installing and Updating HP-UX 9.0*, for more information on distribution media.

Network Distribution Area

The first part of the installation procedure, which is described in "Loading HP DCE Software in a Network Distribution Area", involves loading software from distribution media to a network dis-

tribution area. The drive for the distribution media must be connected to a system that has approximately 30,000 Kbytes of available disk space.

See the manual, *Installing and Updating HP-UX 9.0*, for more information on setting up a network distribution area.

Preinstallation Planning

In general, preinstallation planning involves deciding how many cells to configure at your site, which systems to include in each cell, and where to run DCE services (Security, CDS, DTS, GDA, and the optional services DFS and GDS). This section gives you some guidelines for making decisions prior to installation.

Determining Cell Boundaries

Before installation you should map the boundaries of your cell by listing the systems that will compose your cell. You may find it practical or necessary to divide your site into more than one cell.

Consider the following factors when determining the cell boundaries:

- A major criterion for determining cell boundaries is to include principals that share a common purpose, have similar privileges, and require access to a common set of shared resources.
- Multiple cells require more administrative overhead in setting up and maintenance.
- If you decide to create more than one cell at your site, you must determine appropriate cell names to support inter-cell communication. See "Intercell Communications" for more information.

Intercell Communications

To implement intercell communications, you must start at least one Global Directory Agent (GDA) daemon per cell. You can start a GDA daemon when you configure your cell, as described in Chapter 4.

In addition, you must name your cells according to Domain Name Service (DNS) or GDS convention. When a query cannot be resolved within a cell, GDA passes the query to a DNS server, or queries GDS (if you have configured GDS). The following is an example of a cell name using the DNS format:

/.../xyz.abc.com

If your site is connected to the Internet and you want to obtain a unique DNS name, contact the administrator in charge of the domain under which you want to name your cell.

For more information on cell naming, see the *OSF DCE Administration Guide – Core Services.*

For configuration information, see "Configuring GDA Servers" in Chapter 4 and "Establishing Intercell Communication" in Chapter 7 of this release document.

DCE Services

This section outlines some considerations and restrictions on HP DCE/9000 Version 1.2 software that will help you map out the installation of your cell.

Core Services

Core Services are contained in the DCE-CORE and DCE-CMN filesets. Both filesets must be installed on every system in your cell. You can, however, save disk space by using a linked version (DCE-CORE-LINK) of the DCE-CORE fileset.

NOTE Hewlett-Packard does not recommend the use of linked versions of DCE software.

Security Services

Security server software is contained in the DCE-CORE fileset. The system(s) running the security server should be reliably accessible and physically secure. They should also have enough disk space to hold a registry database that could expand significantly over time as the number of users increases. See Chapter 6 of these release notes for information about disk space requirements for the registry database.

See the *OSF DCE Administration Guide – Core Services* for more information about DCE Security Services. See Chapter 6 of these release notes for HP-specific information about setting up replicated security servers.

Cell Directory Service Configuration

In configuring CDS servers and clients, pay careful attention to the HP DCE/9000 hardware requirements. Appropriate kernel configuration, memory, disk, and especially swap space are essential to the proper functioning of the CDS subsystem.

While it is possible to do tape backups of the CDS server database, this requires the CDS server to be shut down, and provides only a static snapshot of the namespace, which can easily be invalidated by subsequent changes in the cell configuration or namespace. Recovery from a problem again requires a server to be shut down, the database tape to be loaded, and then the restarting of the server with stale information. For these reasons, directory replication is the backup method of choice for CDS. Every cell should configure at least two CDS servers, and read-only replicas of all directories should be created on the backup server. In this configuration, backup is continuous, and recovery only involves switching the role of the servers.

Multiple CDS servers can be configured for specific purposes in the cell. Multiple CDS servers with read-only replicas of all directories in the namespace should always be present for backup and recovery

purposes. Performance considerations may also make the configuration of other CDS servers desirable. For instance, administrators of very busy cells or cells with large numbers of nodes should consider adding additional CDS servers to share the namespace processing load. Similarly, administrators of cells with groups of nodes separated by WAN links should consider providing a local CDS server for each group to enhance performance. Administrators with very large cells may want to partition the namespace among several CDS servers, replicating only the locally used directories, to distribute the storage overhead of the namespace. Selection of the proper CDS server in a cell for use by each group of clients can be configured with the use of profiles and groups.

Each of these CDS configuration strategies is documented in *DCE Administration Guide – Core Services.*

Time Services

It is recommended that you have at least three DTS Servers running in a cell, if the cell has three or more member systems. It is also recommended that you have at least one DTS Time Provider running in a cell.

If you are running AFS, be sure to run the AFS daemon (**afsd**) with the **-nosettime** option. Otherwise, **afsd** periodically resets the system's time. Also be sure that no other software that sets the time (like **ntp** or **timed**) is running on the systems in the cell.

See the *OSF DCE Administration Guide – Core Services* for more information about DCE Distributed Time Services.

At this release, intercell time synchronization is not supported.

Partitions and Filesets

The HP DCE/9000 Version 1.2 software is divided into two partitions: DCE-EE and DCE-EE-LINK. Table shows how the partitions divide into filesets and what the diskspace requirements are.

HP DCE/9000 Version 1.2 Partitions and Filesets

Partition	Fileset	Description	Approx. Size (KB)
DCE-EE	DCE-CMN	DCE Core Software Portion	16900
	DCE-CORE	DCE Core Software	22600 (USA) 29200 (International)
	DCE-MAN	DCE Manpages	2500
	DFS-CMN	DFS Core Software Common Partition	4300
	DFS-CORE	DFS Core Client/Server	6700
	DFS-KERN	Kernel Loader and DFS patches	330
	DFS-NFS	DFS to NFS Exporter Software	3000
	GDS-CORE	GDS Software	8500
DCE-EE-LINK	DCE-CORE-LINK	DCE Core Client/Software Links	7
	DCE-MAN-LINK	DCE Manpage Links	7
	DFS-CORE-LINK	DFS Core Client/Server Links	7

Please note the following:

- You must install DCE-CMN on every system in your cell.
- You must install either DCE-CORE or DCE-CORE-LINK on every system in your cell. (NOTE: When you select DCE-CORE or DCE-CORE-LINK with **update**, the tool automatically selects DCE-CMN for installation).
- If you intend to install linked versions of the filesets, see page 13 for some important guidelines.
- The **updist** and **update** tools check for adequate disk space before they install software.
- If the fileset containing the core software is named DCE-CORE-INT, you have the International version of HP DCE/9000 Version 1.2, in

which entry points to the Data Encryption Standard (DES) algorithm are hidden. See Chapter 1 of this release document for more information about Domestic and International HP DCE versions.

Guidelines on Installing DCE-EE-LINK Software

NOTE For maximum DCE reliability, Hewlett-Packard recommends that DCE software be installed on the local system disk, instead of via links.

If you install filesets under the DCE-EE-LINK partition (DCE-CORE-LINK and DCE-MAN-LINK), you should be aware of the following considerations:

- You must create soft links that point from the local system to a system that has a non-linked version of the software installed. Before installing a linked version of HP DCE/9000, issue the following commands from the **/opt** directory of the local host:

  ln -s dce1.2 dce
  ln -s */link_target/***opt/dcelocal dce1.2**

  where *link_target* is the pathname of the system where HP DCE is installed.

- Do not install both linked and non-linked versions of a fileset on a system. For example, do not install DCE-MAN and DCE-MAN-LINK on the same machine.

- Remove a fileset before installing its associated linked or non-linked version. For example, remove DCE-CORE before installing DCE-CORE-LINK. Or, remove DCE-CORE-LINK before installing DCE-CORE. Use **rmfn** to deinstall one version before installing the other version. See "Removing Software With rmfn" for information on using **rmfn**.

Loading HP DCE Software in a Network Distribution Area

The following procedure loads the HP DCE/9000 Version 1.2 software from media to a network distribution area using the **updist** tool. By default, **updist** loads software into the directory, **/netdist**, which it creates if **/netdist** does not already exist.

If you are installing HP DCE/9000 on a single system, you may choose to install software directly from media. In order to do this, the system on which you are installing HP DCE/9000 must be able to access the media device. If you wish to install directly from media, proceed to "Installing Software".

Note that **/netdist** must reside on a long-name file system. If necessary, use the **convertfs**(1M) command to convert a short-name file system to long-name.

The **updist** tool loads software from media to a destination directory on a local system. You cannot "push" the software from a local device to a remote system over a network file system like NFS or AFS. However, once the HP DCE/9000 Version 1.2 software is loaded in a **/netdist** directory on the local system, you can run **updist** on a remote system to "pull" the software to an additional network distribution area.

If your cell has a mixed environment of both Series 700 and 800 systems, you must create a separate network distribution area for each architecture. First specify the 700 system type and **updist** will load software into **/netdist/700**. Then run **updist** again, specifying the 800 system type. **updist** will then load software into **/netdist/800**.

NOTE You cannot create network distribution areas for both system types directly from the same CD-ROM media. You must first load the netdist area for the system type of the CD-ROM. Then you must load the network distribution area for the other system type, using the first netdist area (instead of the CD-ROM) as the source.

Before you begin, you should verify the following:

- Check that the network file distribution server daemon, **netdistd**, is available on the system that contains the network distribution area. See Appendix B in *Installing and Updating HP-UX 9.0* for information about creating and managing a netdist server. Also, see the manpage, **netdistd**(1M).
- If you are loading an international version of HP DCE/9000 from a CD-ROM drive, be sure you have the appropriate codeword. To obtain a codeword, follothe instructions on the codeword certificate that was shipped with the CD-ROM disc. No codeword is required for domestic versions of HP DCE/9000.

1 **Load media into the drive.**

The HP DCE/9000 Version 1.2 software is shipped on a variety of distribution media, including 8mm DAT tapes and CD-ROM discs.

2 **Start updist.**

Log in as root on the system that has the drive. Enter **/etc/updist** at a shell prompt.

You get a screen like the following. Use **<TAB>** or up/down arrow keys to highlight the options.

```
UPDIST          Main Menu
Highlight an item and then press  "Return" or  "Select
Item". To refresh the screen press CTRL-L.
-------------------------------------------------
Source:  Tape Device        Destination:  Local System
         /dev/update.src                  /netdist
-------------------------------------------------
     Change Source or Destination ->

     Select All Filesets on the Source Media ->
     Select Only Filesets Currently on your System ->
     Select/View Partitions and Filesets...

     How to Use Updist
```

The **updist** tool has general and context sensitive help if you need assistance on making selections, or on entering appropriate values. Also, see the manpage updist(1M) for more information.

3 **Set the source to the appropriate device.**

The default source is a tape device.

If you are using a CD-ROM, select **Change Source or Destination** from the main menu and then select **CD-ROM** from the sub-menu.

You must enter a valid codeword (for international versions of HP DCE/9000) and hardware id if you are loading from a CD-ROM device. You can get online information about obtaining those values by entering **Help** when the cursor is in the Codeword or Hardware ID fields of the CD-ROM sub-menu.

A codeword is not required for domestic versions of HP DCE/9000. If you are loading a domestic version of HP DCE/9000 from CD-ROM, you should answer no to the question "Do you want to enter your authorized codeword to access the protected software? ".

Do not change the destination from the default **/netdist**.

4 **Specify the appropriate system type.**

updist prompts you to choose between files that are compatible with Series 700 systems, or files that are compatible with Series 800 systems. If your media contains the Series 700 version of HP DCE/9000, choose **7**. If your media contains the Series 800 version of HP DCE/9000, choose **8**.

5 **Select the DCE partitions.**

Choose Select/View Partitions and Filesets from the main menu. You should see a submenu with entries similar to the following:

```
Selected     Name          Partition Description            Size
  n          DCE-EE        DCE Execution Environment       25498
  n          DCE-EE-LINKDCE Execution Environment Links      13
```

Select both the DCE-EE and DCE-EE-LINK partitions.

After selecting, you can check if you have enough disk space by selecting the Disk Space button, located on the bottom panel of the updist window.

NOTE

When you select the partitions that you wish to load, **updist** may warn that you do not have prerequisite filesets installed. These warnings may be ignored when creating a netdist area.

6 **Load the software.**

Select the **Start Loading** button, located on the bottom panel of the updist window. **updist** displays installation statistics as it loads the software. It appends error, warning, and other messages to the file at **/tmp/update.log** .

7 **Start or restart the netdist server daemon.**

If the netdist server daemon, **netdistd**, is already running, use kill(1) to stop it. Start the netdist server daemon by using the **/etc/netdistd** command. See the manpage, *netdist*(1M), for more information.

Installing Software

Once you have loaded HP DCE/9000 Version 1.2 software into a network distribution area, you can begin installing appropriate filesets and partitions on individual systems.

The following procedure involves invoking the **update** tool on each target system in a cell. When installation is complete, you can begin cell configuration, which is described in Chapter 4.

Before you begin, check the following:

- You must know the root password for each system in your cell.
- If the system is a functioning DCE server or client, stop the DCE software.
- Have the port number and system name of your netdist server available. The default is port number 2106. The port number can be changed as an option to the server startup command, **/etc/netdistd**. Check with the system administrator who started the netdist server daemon if the port number differs from the default.
- If you are installing any of the linked versions of the software, see "Guidelines on Installing DCE-EE-LINK Software" for some important considerations.
- You must install HP DCE/9000 Version 1.2 on a long-name file system. If you have a short-name file system, use the **convertfs**(1m) utility to convert it to long names.
- If you plan to do remote installs, you must be able to log in to the remote system with a utility like **telnet**, **rlogin**, or **remsh**. You cannot do a "push" installation to a remote system over a network file system such as NFS or AFS. In order to use a remote login utility, you must have HP 9000 ARPA Services running on both the local and remote systems. See the HP manual, *Using ARPA Services*, for more information.
- You should have determined where you plan to install HP DCE partitions and filesets. See "Preinstallation Planning" for planning considerations.

1 **Log in to the target system as root.**

If the target system is remote, you must first be able to log into the remote system with a remote login utility. See the HP manual, *Using ARPA Services*, for more information on remote logins.

Then log in as root.

2 **Start update.**

Enter **/etc/update** at a shell prompt.

You get a screen like the following. Use **<TAB>** or up/down arrow keys to highlight the options.

```
UPDATE              Main Menu
Highlight an item and then press  "Return" or  "Select
Item ". To refresh the screen press CTRL-L.
------------------------------------------------
Source:  Tape Device          Destination:  Local System
         /dev/update.src                    /
------------------------------------------------
     Change Source or Destination ->

     Select All Filesets on the Source Media ->
     Select Only Filesets Currently on your System ->
     Select/View Partitions and Filesets...

     How to Use Update
```

The **update** tool has general and context sensitive help if you need assistance on making selections, or on entering appropriate values. Also, see the manpage, update(1M), for more information.

3 **Set the source to your network distribution area.**

Select **Change Source or Destination** from the main menu. Then select **From Netdist Server to Local System.**

Specify the name , the port number, and system type of the system that is your network distribution server. Then select on the **Done** softkey at the bottom of the window.

NOTE

You should not change the default destination directory which is the root directory (/) of the target system. By default, **update** installs DCE software in the **/opt** directory in the root partition.

If there is insufficient disk space on the root device, you must create an **/opt** directory on a second device and then create an absolute link to it. For example:

```
mkdir /disk2/opt
ln -s /disk2/opt /opt
```

Make sure that the link is absolute (**/opt** to **/disk2/opt**) . **update** cannot follow relative links (**/opt** to **disk2/opt**).

The **update** main menu returns showing the source as a netdist server with the network address of the system that you specified.

4 **Select and load software.**

Choose Select/View Filesets and Partitions from the main menu. A list of the partitions available from the netdist server appears, along with instructions for selecting them. The display with the HP DCE partitions should be similar to the following:

```
Mark "y" or "n ". To pick and choose individual filesets
within a partition, press "View Filesets ". A "p" means
that some filesets have been selected within a partition.
Press "Start Loading" when selection is complete.

Source:    netserver.nn.site.org.com        Destination: /

Selected  Name         Partition Description          Size
   n      DCE-EE       DCE Execution Environment     34548
   n      DCE-EE-LINK  DCE Execution Environment Links  13
```

You can view the filesets that make up each partition by selecting the soft key labeled View Filesets. If you view the filesets under the DCE-EE partition, the display should look similar to the following:

```
            Filesets in partition: DCE-EE

Mark "y" or "n" to make a selection. Press "Partit'n
Screen" to return to the partition selection screen.
```

```
Selected     Name       Fileset Description                Size
  n          DCE-CMN    DCE Core Software Common Portion 6989
  n          DCE-CORE   DCE Core Software                  26039
  n          DCE-MAN    DCE Manpages                       1520
```

If you view the filesets under the DCE-EE-LINK partition, the display should look similar to the following:

```
                Filesets in partition:  DCE-EE-LINK

Mark  "y" or  "n" to make a selection. Press  "Partit'n
Screen" to return to the partition selection screen.

Selected     Name           Fileset Description          Size

  n          DCE-CORE-LINK DCE Core Software Links         7
  n          DCE-MAN-LINK  DCE Manpage Links               7
```

Before you install, note the following considerations:

- You must install DCE-CMN on every system in your cell.
- You must install either DCE-CORE or DCE-CORE-LINK on every system in your cell. Note that DCE-CORE and DCE-CORE-LINK are dependent on DCE-CMN. When you select DCE-CORE or DCE-CORE-LINK with **update**, the tool automatically selects DCE-CMN for installation.
- If you intend to install linked versions of the filesets, see "Guidelines on Installing DCE-EE-LINK Software" for some important guidelines.

After you select the software you want to load, you can check if there is enough disk space by selecting the Disk Space soft key. update also checks if there is enough disk space when you start loading the software. If you see either of the following messages:

```
It is recommended you free up n Kbytes

Loading the selected filesets results in less free disk
space
```

you can continue to load files but you should free up disk space later. If you see either of the following messages:

```
You MUST free up n Kbytes
```

```
Loading the selected filesets is impossible due to in-
sufficient space on one or more file systems...
```

you do not have sufficient disk space and cannot continue to load filesets.

See "How to Free Disk Space" in *Installing and Updating HP-UX 9.0* for methods of freeing up disk space.

As **update** loads files, it displays an estimate of how long the procedure will take to complete. When loading is complete, it exits and returns to the command line prompt.

5 **Check the update log file.**

update logs messages in **/tmp/update.log**. Look for messages that begin with ERROR, WARNING, or NOTE.

Refer to "Troubleshooting an Update" in *Installing and Updating HP-UX 9.0* for information on resolving problems.

You can verify the location of installed files by looking in the **/etc/filesets** directory. **update** automatically creates a file there with the same name as the installed fileset. For example, if you installed DCE-CMN, there will be a file called **/etc/filesets/DCE-CMN** that contains pathnames of all the files that were installed.

After you install the HP DCE/9000 Version 1.2 software on all the systems in your cell, you can begin to configure your cell. See Chapter 4 of this document for configuration information.

Removing Software With rmfn

The recommended method for removing HP DCE filesets and partitions is to use the **rmfn** tool. To use **rmfn** on a local system, log in as root and execute:

/etc/rmfn

If you want to remove software on a remote system, first log into the remote system using a utility like **telnet**, **rlogin**, or **remsh.**

The **rmfn** command displays an interface similar in format to the **update** tool's interface. Like **update**, the **rmfn** tool has general and context sensitive help if you need assistance on making selections, or on entering appropriate values. For more information see the manpage, **rmfn**(1M) and the section called **Remove Unwanted Software with rmfn(1M)** in *Installing and Updating HP-UX 9.0.*

Before you use **rmfn**, you should be aware of the following points:

- If you have any DCE daemons running, kill them before removing software.
- **rmfn** only displays the filesets and partitions that were installed with **update**. It reads what to delete from files that **update** creates in **/etc/filesets** and **/system.** If you have HP DCE software that was installed by other means (the prerelease version of HP DCE Developers' Environment, for example), you must remove it manually. Also be sure to remove any links.
- **rmfn** removes files but not directories. The directory tree structure for a fileset remains after the files are removed.
- After you remove the DCE-EE-LINK partition or its filesets with **rmfn**, check for the existence of **/opt/dcelocal/usr/man/cat?.Z** directories. If they exist, remove them manually. The **catman** command creates these directories when it formats man pages.
- **rmfn** logs messages in a file at **/tmp/rmfn.log**.

4

Configuring DCE Cells

Configuring DCE Cells

This chapter tells how to choose a DCE cell configuration tool and how to use the tools to configure, destroy (unconfigure), start, and stop cells. Two tools are discussed, the SAM-based DCE Cell Configuration tool, and the script-based **dce_config**.

This chapter also discusses how to install DCE login utilities, and how to set up intercell communication with DCE GDA.

To configure HP DCE/9000 software, you must have previously completed the installation procedure. See Chapter 3, *Installing HP DCE/9000* for planning and installation information.

NOTE If you are configuring DCE on systems running NCS-based software (such as NetLS, OmniBack, HP MPower, and Shared Print/UX), see see Note for Users of NCS-based Software on page 36 of this chapter.

Choosing a Cell Configuration Tool

SDCC and dce_config

HP DCE/9000 offers two cell configuration tools: a script-based tool, **dce_config**, and a SAM-based tool, SDCC. SAM (System Administration Manager) is an HP-UX menu-driven system administration program that includes several other system administration utilities, in addition to the DCE cell configuration component. We refer to the DCE component of SAM as the SAM DCE Cell Configuration (SDCC) utility.

SDCC is essentially a graphical front-end to **dce_config**. However, in addition to the ease-of-use that a graphical interface confers, SDCC has some important functional differences that offer advantages over running **dce_config**. Therefore, we recommend that you use SDCC, and not **dce_config**, to configure cells in almost all cases. (See the limitations listed on the next page for further details). Some of these advantages are:

- SDCC has a "template" mode that allows you to create prototype configurations that can be tested before actually creating them.
- SDCC checks systems before performing the configuration.
- SDCC prevents you from creating an invalid configuration.
- SDCC allows you to configure all HP DCE/9000 Version 1.2 systems in your cell remotely, from a single administrative node.
- SDCC "discovers" the configuration of a cell at startup, thus offering compatibility with **dce_config** and other control programs. However, SCDD may not reliably "discover" other vendor's systems which do not use **dce_config**.
- SDCC "remembers" the last successful configuration. This information is used only when the cell is "down" or critical DCE servers are not running.

- SDCC includes complete online documentation.

Limitations of SDCC

While using SDCC is completely compatible with using the **dce_config** script, there are a few limitations to SDCC.

- When you add a new system to your DCE cell, you must run SDCC on a node that is already part of your cell. In other words, the operation of adding a new node to a cell must be performed on a node that is already part of the cell.
- If you stop a cell that has DFS servers, each node that provides DFS must be rebooted before SDCC can restart the cell. After rebooting the DFS nodes, you can either use SDCC's "Restart Cell" or start DCE via **dce_config** or by running the system's **/etc/rc.dce** script.
- SDCC cannot restart a cell that has DFS Servers and whose Initial CDS server and Master Security server are not on the same node. Cells that have DFS servers and have separate nodes for the Initial CDS server and the Master Security server must be started via **dce_config** or by running the system's **/etc/rc.dce** script, after rebooting the DFS system(s).
- When SDCC examines the cell, it initiates a "discovery" process to determine the status of the cell. If the cell is down, or critical DCE servers are down, the discovery process may fail and SDCC will revert to the last successful configuration.
- SDCC does not support all possible DCE configurations. You can only use SDCC if your Master Security server, your Initial Cell Directory Server, and your DFS servers are all HP systems running HP DCE/9000 Version 1.2.

Configuring Cells with SDCC

Overview of SDCC Functionality

The SDCC tool enables you to perform the following cell configuration tasks:

- Create a cell of one or more systems. SDCC provides a "template" mode that simplifies cell creation.
- User authentication of cell configuration operations.
- Add and remove client systems (systems running DCE client software only) to an existing cell from any system in the cell.
- Add replicated security servers to an existing cell.
- Add additional CDS servers to an existing cell. You can add new systems to the cell as CDS servers, or reconfigure existing cell members as CDS servers.
- Add or modify local or global DTS servers or DTS clients in the cell and modify **ntp**, **spectracom**, or **null** DTS time providers in the cell.
- Add or remove GDA servers on existing cell nodes.
- Stop all DCE daemons on all cell members or selected cell members. (Requires HP DCE/9000 Version 1.2 on the cell members.)
- Restart all DCE daemons (except DFS) on all cell members or selected cell members. (Requires HP DCE/9000 Version 1.2 on the cell members.)
- Destroy (unconfigure) an existing cell.

At the heart of SDCC is an *object list* screen that displays a list of all cell members and their attributes. The attributes include: a cell member's name, the DCE services (if any) configured on the member, and a status that indicates whether or not all configured DCE daemons on the member are running. You perform tasks on selected cell

members by selecting (highlighting) the desired members in the list and then selecting the appropriate actions from an **Actions** pull-down menu.

By using the "List" pull-down menu, you can switch to a "template" mode that allows you to create prototype DCE cell configurations that can (and must) be tested for validity before actually being created.

Important Security Warning

SDCC uses standard UNIX remote login utilities to perform remote administration . This does cause the cell administrator's password to be sent over the network whenever you perform a task on a remote system. If someone is very closely monitoring the network traffic, they could obtain the password and the security of the cell's DCE services will be compromised. Note, however, that using SDCC is no more or less secure than using standard UNIX remote login utilities directly.

Requirements for Running SDCC

If you choose SDCC, you should verify that the systems in your cell meet the following requirements:

- All systems from which you wish to perform cell configuration tasks must have SAM installed. SAM is an optional fileset in HP-UX 9.0 that can be found under the OS-ADMIN partition.
- All systems must have the host name of each node (the administrative node and cell members) in their **.rhosts** and **/etc/hosts.equiv** files. The **.rhosts** file must be located in the root user's home directory, usually the / directory. For more information about **.rhosts** files, see *Using ARPA Services* (B1014-90006), and the **remsh**(1) and **hosts.equiv**(4) man pages.
- All systems that you wish to administer via SDCC must be running HP DCE/9000 Version 1.2. Cell member systems running HP DCE

1.1 or other vendors' DCE implementations may be "discovered" by SDCC, but they cannot be acted upon.

Running SDCC

To run SDCC:

1 Log in as **root**.

2 Execute **sam** from a shell prompt.

3 Select and open **DCE Cell Management** on the main SAM menu.

The system on which you use SAM to configure a cell must be a cell member. Also, after you create the cell, you *cannot* use that system to create or administer another cell; you can only administer the original cell (until that cell is destroyed).

In a configured and running cell, if the primary DCE services (Initial CDS and Master Security) are running on HP systems (as opposed to other vendor's systems), you can configure additional HP DCE 1.2 clients into the cell from any HP 1.2 cell member system.

Online Help for SDCC

Comprehensive, context-sensitive online help is provided for SDCC, as it is for all functional areas of SAM. Consult the online help for details about using SDCC; detailed information about SDCC is *not* provided here or in a separate manual.

NOTE The SDCC online help assumes a basic familiarity with DCE terms and concepts, as described in the manual *Introduction to DCE*.

For detailed information about using the SAM online help system, activate the Help button on the main SAM menu, select **General SAM Information** in the Topic Hierarchy section of the Help screen, and then select the **How to Use SAM Help** help topic. You can also access this help topic by selecting **Using Help** on a SAM Help pull-

down menu. This menu appears on SAM *object list* screens.The SAM help system functions differently in X Windows and HP VUE environments than on ASCII terminals. The **How to Use SAM Help** help topic discusses both display environments.

To help get you started, here's a capsule summary of the ways to access SAM online help:

- The **Help** pulldown menu. This menu appears on SAM object-list screens. The pulldown menu contains four selections: Overview, Keyboard, Using Help, and Product Information. The Overview help provides an overview of the functional area or subarea to which the object-list screen corresponds.
- The **Help** button. This button appears on most SAM dialog screens and menus. It provides help on the particular dialog or menu.
- On-item help. On-item help provides help on a particular menu selection or on a particular field, button, or list on a screen. To access on-item help, you select (highlight) the particular item by clicking on it with the mouse or using the TAB key, and then press F1.
- Hyperlinks. In an X Windows or HP VUE environment, the online help text typically contains links to other help topics. A link is indicated by an underlined word or phrase in the help text. To display the linked help topic, you click on the underlined text. On ASCII terminals, the titles of any linked help topics appear in a See Also section. To display these topics, you select the topic title with the TAB key, and then press the RETURN key.

Printing the SDCC Online Help

In X Windows or HP VUE environments, you can print individual help topics within SDCC by activating the **Print** button on a help topic screen. Or you can use the **helpprint** (1X) command at a shell prompt. On ASCII terminals, you can only use the **helpprint** command; the print button is not available.

Using the Print Button

To use the print button, you must first create a **helpprint** X resource. Here's one way to do this:

1 Open the **Toolboxes** popup menu from the VUE front panel.

2 Click on the **General** icon.

3 Click on the **System_Admin** icon. Then open it by choosing the appropriate open menu item on the Actions pulldown menu.

4 Click on the **EditResources** icon. Then choose the **EditResouces** menu item on the Action pulldown menu. This creates a temporary file listing the contents of the current X resources and opens the file for editing.

5 Add the following line to the file :

***helpPrint: /usr/vue/bin/helpprint**

6 Save the file and exit the editor.

The print button prints the help topic at the default printer. It does not display any confirmation prompts or status messages.

Using the helpprint Command

You can use the **helpprint** command to print all or selected sets of SDCC help topics. The entire set of help topics is called a *help volume*. The full pathname of the SDCC help volume is:

/usr/sam/help/C/dce/dce.hv

The following **helpprint** command prints the entire SDCC help volume:

/usr/vhelp/bin/helpprint -printer *printer_name* **-helpType 1 **
**-locationId _hometopic -R -helpVolume **
/usr/sam/help/C/dce/dceconf.hv

The order of the SDCC help topics in this printout does have some logical sequence, but it is really just a collection of the individual help topics and does not form a manual in the traditional sense. See the **helpprint** man page for more information.

SDCC Cell Configuration Files

The SDCC tool creates a *cell configuration file* on every system that is a member of a cell. The pathname of the file is **/usr/sam/WORKSPACE/dce/config_file.ext**. SDCC uses these files internally to identify cell members and their configurations if it could not determine the configuration during the discovery process.

NOTE Under normal circumstances, you should not delete, manually modify, or move the configuration file on any cell member. If you do, attempts to modify the cell's configuration with SDCC may not succeed and may cause unpredictable and undesirable results.

Extraneous SDCC Error Messages

When using SDCC to unconfigure a node or cell, you may see one or more of the following messages in the logfile viewing screen:

```
Could not access the FLDB for attributes
Error: no servers appear to be up (dfs / ubk)
Could not access the FLDB for attributes
Error: no servers appear to be up (dfs / ubk)
Could not get info about site <node_name> (668147726,
2063808808)
Error: no servers appear to be up (dfs / ubk)
```

These error messages are generated by an underlying command. If SDCC returns with "Successfully unconfigured <node_name>", these messages may be ignored.

Configuring Cells with dce_config

The following procedures explain how to configure server and client systems using the menu-driven **dce_config** tool. The text shows the complete menu at its first occurrence; thereafter it shows only the menu name and current selection, prompts, and recommended input values (in **boldface**).

As you perform each step, various status messages are displayed. This document shows only the prompts; it may not show all status messages.

Note that this section assumes a basic familiarity with DCE terms and concepts, as described in the manual *Introduction to DCE*.

The sections on pages 11 - 34 include complete information on configuring cells with the **dce_config** script.

Starting dce_config

1 Log in as **root** on the system you wish to configure.

2 Make sure that **/etc** is in your command search path:

```
# PATH=/etc:$PATH; export $PATH  (Bourne/Korn shell)
% setenv PATH  /etc:$PATH  (C shell)
```

3 Run the **dce_config** script:

 # dce_config

```
DCE Main Menu  (on hostname)
0. INSTALL
1. CONFIGURE   -configure and start DCE daemons
2. START       -re-start DCE daemons
3. STOP        -stop DCE daemon
4. UNCONFIGURE -remove a host from CDS and SEC data-
bases
5. REMOVE      -stop DCE daemons and remove data files
created by DCE daemons
```

```
99.     EXIT

selection:
```

NOTE **dce_config** is not capable of configuring remote systems (except for the Unconfigure operation). When running **dce_config**, you must always log in on the system you wish to affect.

Initial Cell Configuration

When creating an HP DCE cell, servers must be configured before clients. First configure a Security server, then a CDS server, Time servers, and finally a single Time provider. Then you may configure clients.

When planning a DCE cell, note that you must configure a CDS client on any Security server system that is not running a CDS server. You must also configure a Time client on any system that is not running a Time server. Be sure to configure these clients only after you have configured all servers.

Client configuration is discussed in "Configuring Security and CDS Client Systems."

1 From the DCE Main Menu, choose CONFIGURE:

```
DCE Main Menu  (on hostname)

selection: 1  (CONFIGURE)
DCE Configuration Menu (on hostname)
1.     Initial Cell Configuration
2.     Additional Server Configuration
3.     DCE Client

98.     Return to previous menu
99.     Exit
selection:
```

2 From the DCE Configuration Menu, choose Initial Cell Configuration:

```
DCE Configuration Menu (on hostname)
```

selection: **1** (Initial Cell Configuration)

S:****** Configuring initial cell.

Initial Cell Configuration (on hostname)

```
1. Security Server
2. Initial CDS Server

98. Return to previous menu
99. Exit

selection:
```

3 Configure the Security Server:

Initial Cell Configuration

selection: **1** (Security Server)

S:****** Configuring Security Server

4 If this is your very first cell configuration, or if you have previously run REMOVE, answer **n** to the following question. If you are re-configuring a cell, answer **y**:

Do you wish to first remove all remnants of previous DCE configurations for all components (y/n)? You should do so only if you plan on re-configuring all existing DCE components now: (n)

5 Enter a cell name:

Enter the name of your cell (without /.../): **xyz.abc.com**

6 dce_config will prompt you with a warning. If **rpcd** was recently running with the TCP protocol sequence, then wait until 4 minutes have elapsed since **rpcd** was stopped before continuing from this prompt:

WARNING: If rpcd was recently running and was using the TCP protocol sequence to listen for calls to the server, then a TCP shutdown period of up to 4 minutes is required before restarting rpcd, in order to avoid "cannot bind socket" errors. Press <RETURN> to continue, CTRL-C to exit: **<RETURN>**

7 At the following prompt, enter any string and press <RETURN> .

Enter keyseed for initial database master key:

8 dce_config prompts you to choose the Cell Administrator's principal name and password. The default principal name for the Cell Administrator is cell_admin:

Enter desired principal name for the Cell Administrator: (cell_admin) Enter desired password for the Cell Administrator:

9 dce_config prompts you for the starting point for UNIX user and group ID's that will be generated by the DCE Security Service. This step prevents the DCE Security Service from generating IDs that are already in use by your system. Type <RETURN> to choose the default value, or enter a value of your choice:

S:****** The current highest UNIX ID for persons is *N*. Enter the starting point to be used for UNIX ID's that are automatically generated by the Security Service when a principal is added using "rgy_edit ": (*N*+100) **<RETURN>**

S:****** The current highest UNIX ID for groups is *N*. Enter the starting point to be used for UNIX ID's that are automatically generated by the Security Service when a group is added using "rgy_edit ": (*N*+100) **<RETURN>**

dce_config then starts up **secd** and **sec_clientd** and initializes the registry database.

S:****** Starting secd...

S:****** Starting sec_clientd

S:****** Waiting for node self-identity to be established...

S:****** Initializing the registry database...

This system is now configured as the master Security server. You must now create a CDS server, either on this system or on another system:

- If the CDS server for this cell will be on another system, repeat steps 1 and 2 that system, and continue with step 10 below.
- If the CDS server is on the same system as the Security server, con-

tinue with step 10 below.

10 From the DCE Configuration Menu:

DCE Configuration Menu

selection: **1** (Initial Cell Configuration)

11 From the Initial Cell Configuration menu, choose Initial CDS Server:

Initial Cell Configuration (on *hostname*)

selection: **2** (Initial CDS Server)

This routine starts up **cdsadv** and **cdsd**, initializes the namespace, and sets ACLs for all new namespace entries.

S:****** Configuring initial CDS Server...

S:****** Please wait for user authentication and authorization...
S:****** Starting cdsadv...

S:****** Starting cdsd -a

12 dce_config asks whether is should create a LAN profile for use in dividing clients and servers into profile groups for higher performance in multi-LAN cells. If you choose to have a LAN profile created, dce_config asks for the name of the local LAN. The name you provide is arbitrary, and is used by **dce_config** to store LAN profile information.

Create LAN profile so clients and servers can be divided into profile groups for higher performance in a multi-lan cell? (n) **y**

What is the name of the LAN? **lan_250**

Creating LAN profile...

Finished creating LAN profile.

S:****** Setting ACLs for all new namespace entries.

Configuring DTS Servers

Time servers should be configured in any cell of more than one system. A minimum of three Time servers is recommended for any cell with three or more member systems. See the *OSF DCE Administration Guide – Core Services* for a discussion of the optimum placement of servers in a cell with gateway or WAN links. DTS servers may be configured on any system in the cell.

When **dce_config** is first run on a system, the HP-UX environment-variable TZ is read to determine the HP-UX local time zone. **dce_config** then automatically selects a matching DCE local time zone and creates the link for **/opt/dcelocal/etc/zoneinfo/localtime**. A different time zone can be chosen — see the **localtime**(5) man page for details.

To configure a DTS server on a system not already configured as a Security or Directory server, start **dce_config** (as **root**) on that system and then continue with step 1 below. To configure a DTS server on a system already configured as a Security or Directory server, continue with step 1 below.

1 Configure the DTS daemon:

DCE Configuration Menu

selection: **2** (Additional Server Configuration)

Additional Server Configuration

```
1. Additional CDS Servers(s)
2. DTS
3. DFS System Control Machine
4. DFS Private File Server
5. DFS File Server
6. DFS Fileset Location Database Server
7. GDA Server
8. Replica Security Server

98. Return to previous menu
99. Exit
```

```
selection:
```

selection: **2** (DTS)

The DTS Configuration Menu is displayed:

```
DTS Configuration Menu

1. DTS Local Server
2. DTS Global Server (only in multi-lan cells.)
3. DTS Clerk
4. DTS Time Provider

98. Return to previous menu
99. Exit
```

2 For servers on the same LAN, select the DTS Local Server:

3 selection: **1** (DTS Local Server)

For a discussion about the use of DTS global servers for time servers communicating between LANs, see the *OSF DCE Administration Guide*. Where appropriate, select the DTS global server:

selection: **2** (DTS Global Server)

Either selection starts the **dts** daemon (**dtsd**) and **dtstimed**

4 Configure a DTS time provider on one of the time servers in a cell.

The DTS **null** time provider configures a system to trust its own clock as an accurate source of time. The DTS **ntp** provider obtains an accurate source of time from some other system outside the cell. The **spectracom** time provider uses a local hardware device as a time provider. See the *OSF DCE Administration Guide* for more information on time providers.

5 Select the DTS Time Provider:

selection: **4** (DTS Time Provider)

The following menu is displayed:

```
DTS Time Provider Menu
```

```
1. Configure a NULL time provider
2. Configure a NTP time provider
3. Configure a spectracom time provider

98. Return to previous menu
99. Exit

selection:
```

6 Select NULL or NTP or SPECTRACOM:

selection: **1** (NULL time provider)

or

selection: **2** (NTP time provider)

or

selection: **3** (spectracom time provider)

If you select the NTP time provider, the following prompt appears:

Enter the hostname where the NTP server is running:

You have now completed configuration of the server systems.

If you select the spectracom time provider, the following prompt appears:

Enter the device name where the TP is connected.

You have now completed configuration of the server systems.

Configuring Additional CDS Servers

Follow this procedure if you wish to configure additional CDS servers:

1 From the DCE Configuration Menu, choose Additional Server Configuration:

DCE Configuration Menu (on *hostname*)

selection: **2**

S:****** Configuring additional server.

S:****** Please wait for user authentication and authorization.

2 Enter the name of your cell:

Enter the name of your cell (without /.../): **xyz.abc.com**

S******: Starting rpcd...

NOTE If **rpcd** was recently running and was using the TCP protocol sequence to listen for calls to the server, rpcd may take up to four minutes to restart.

3 . Enter the hostname of your cell's security server:

What is the name of the Security Server for this cell?

NOTE When configuring a multi-system cell, **dce_config** checks that system times are within 120 seconds of each other. However, **dce_config** does not recognize time zones. When configuring a cell across time zones, first set the environment variable CHECK_TIME to **n**.

4 Make sure the contents of the **pe_site** file is identical on both the server and the client. The **dce_config** script checks this, but prompts for your confirmation. Identical **pe_site** files are normally generated automatically, but you should confirm this yourself, particularly during your initial set-up. If the **pe_site** files are not identical, you should start this procedure again.

Ensure the /opt/dcelocal/etc/security/pe_site file matches that on the server...

Press <RETURN> to continue, CTRL-C to exit: **<RETURN>**

5 Enter the Cell Administrator's principal name (the default is cell_admin) and password:

Enter Cell Administrator's principal name: (cell_admin) Enter password:

6 The Additional Server Configuration menu appears. Choose Addition-

al CDS Server:

Additional Server Configuration Menu

selection: **1** (Additional CDS Server(s))

S:****** Configuring additional CDS server.

S:****** Starting sec_clientd

S:****** Waiting for node self-identity to be established...

7 Enter the name of the cell CDS server. If the cell has more than one CDS server, choose one:

What is the name of a CDS server in this cell (if there is more than one, enter the name of the server to be cached if necessary)? **cds_server_host**

Create LAN profile so clients and servers can be divided into profile groups for higher performance in a multi-lan cell? (n) **n**

The routine then starts the CDS client daemon, and prompts for the name of the CDS clearinghouse. Enter a name of your choice.

What is the name for this clearinghouse? **host.ch**

S:****** Initializing the name space for additional CDS Server...

S:****** Setting ACLs for the CDS clearinghouse /.:/host.ch...

8 dce_config asks if more directories should be replicated. If you answer **y**, **dce_config** prompts for a list of directories to be replicated:

Should more directories be replicated? (n) **y** Enter a list of directories to be replicated, separated by spaces, and terminated by <RETURN>

Notes on Configuring Additional CDS Servers

Immediately after configuring an additional CDS server, you should skulk the root directory using the **set directory /.: to skulk** command as **cell_admin** in **cdscp**. This will initiate the propagation of a consistent copy of the changed root directory information to all the CDS servers, and will prevent problems which might arise from use

of inconsistent information before this propagation. The use of several CDS servers may increase the time required to complete the propagation of this information.

Configuring Security and CDS Client Systems

Before configuring clients, first configure your server systems. Then use this procedure to configure client systems.

You must configure a CDS client on any Security server system that is not running a CDS server. To configure a client system, you need to know the name of the Security server and the initial CDS server for the cell.

Note that this procedure does not create a DTS clerk (client). For information on creating DTS clerks, see "Configuring DTS Clerks".

1 Start **dce_config** on the system that you wish to configure with DCE client(s).

2 Enter the DCE Configuration Menu:

DCE Main Menu

selection: **1** (CONFIGURE)

3 Run the client configuration routine:

DCE Configuration Menu

selection: **3** (DCE Client)

4 dce_config asks if you wish to remove all remnants of previous DCE configurations. If you are configuring this system for the first time or have previously run Remove, answer **n**. Otherwise, answer **y**.

5 Enter the name of your cell:

Enter the name of your cell (without /.../): **xyz.abc.com**

S******: Starting rpcd...

NOTE If **rpcd** was recently running and was using the TCP protocol sequence to listen for calls to the server, then a TCP shutdown period of up to 4 minutes is required before restarting rpcd, in order to avoid "cannot bind socket" errors. If necessary, wait at the WARNING: prompt until 4 minutes have elapsed.

6 Enter the hostname of your cell's security server:

What is the name of the Security Server for this cell?

7 Make sure the contents of the **pe_site** file is identical on both the server and the client. The **dce_config** script checks this, but prompts for your confirmation. Identical **pe_site** files are normally generated automatically, but you should confirm this yourself, particularly during your initial set-up. If the **pe_site** files are not identical, you should start this procedure again.

Ensure the **/opt/dcelocal/etc/security/pe_site** file matches that on the server...

Press <RETURN> to continue, CTRL-C to exit: **<RETURN>**

8 Enter the Cell Administrator's principal name (the default is cell_admin) and password:

```
Enter Cell Administrator's principal name:
(cell_admin)
Enter password:
```

The routine then starts up the Security client daemon, **sec_clientd**.

9 Enter the name of the cell CDS server. If the cell has more than one CDS server, choose one:

What is the name of a CDS server in this cell (if there is more than one, enter the name of the server to be cached if necessary)? **cds_server_host**

Create LAN profile so clients and servers can be divided into profile groups for higher performance in a multi-lan cell? (n) **n**

The routine then starts the CDS client daemon.

Configuration of the CDS and Security client system is complete.

If this client system is not running a DTS daemon, proceed to the next section, *Configuring DTS Clerks.*

Configuring DTS Clerks

If you are using DTS as your time synchronization mechanism, you must configure a DTS clerk (client) on any system that is not running a DTS server. A DTS clerk is *not* started automatically via the **dce_config** "DCE Client" menu option; you must explicitly start a DTS clerk from the "DTS" menu under "Additional Server Configuration ".

1 Start **dce_config** on the system that you wish to configure with a DTS clerk.

2 Enter the DCE Configuration Menu:

DCE Main Menu

selection: **1** (CONFIGURE)

3 Choose the Additional Server Configuration Menu:

DCE Configuration Menu

selection: **2** (Additional Server Configuration)

4 Choose the DTS menu:

Additional Server Configuration

selection: **2** (DTS)

S******: Configuring DTS...

5 Choose DTS Clerk:

DTS Configuration Menu

selection: **3** (DTS Clerk)

S******: Configuring DTS Clerk...

S******: Starting dtsd...

S******: Starting dtstimed...

S******: This node is now a DTS clerk.

Configuring GDA Servers

The DCE Global Directory Agent (GDA) facilitates communication between DCE cells. This section describes how to start the GDA server. Before you start a GDA server, see "Establishing Intercell Communication" in Chapter 7 information about establishing intercell communication with GDA.

A GDA server can only be configured on an existing client system or CDS server system.

1 Start **dce_config** on the GDA server system.

2 From the DCE Configuration Menu, choose Additional Server Configuration:

selection: **2** (Additional Server Configuration)

3 Choose GDA Server:

selection: **7** (GDA Server)

The system configures the GDA server and starts the GDA server daemon, **gdad**.

Creating a Security Server Replica

A feature of HP DCE/9000 is Security Server Replication, which provides for improved cell performance and reliability. These steps will allow you to create a security replica via **dce_config**. For detailed information about administering and maintaining security replicas, see Chapter 5 of these release notes.

1 From the DCE Configuration Menu:

DCE Configuration Menu

selection: **2** (Additional Server Configuration)

2 From the Additional Server Configuration Menu, choose Replica Security Server:

Additional Server Configuration (on *hostname*)

selection: **8** (Replica Security Server)

S******: Configuring Security Replication Modifying acls on /.:/sec/replist...

Modifying acls on /.:/subsys/dce/sec...

Modifying acls on /.:/sec...

Modifying acls on /.:...

Modifying acls on /.:/cell-profile...

Enter keyseed for initial database master key:

start slave security server (secd)...

The default name for the replica is **subsys/dce/sec/**$HOSTNAME. If you wish to change the name of the security replica that is created by **dce_config**, change the value of SEC_REPLICA, either in the file **/opt/dcelocal/etc/dce_com_env** or in the shell environment from which **dce_config** is run. Note that you must do this *before* running **dce_config**.

Removing Client Systems from the Cell

To remove a configured client system from a cell, use the UNCONFIGURE option on the DCE Main Menu. The UNCONFIGURE operation can be executed on any system in the cell. A prompt will ask for the name of the client system to be unconfigured. The UNCONFIGURE option removes the target machine from the cell Security database and the CDS namespace. After you have unconfigured the client system, run **dce_config** on the client system and use the REMOVE option from the DCE Main Menu.

DCE daemons must be running on the system executing the UNCONFIGURE option. If daemons have been stopped, use the START option on the DCE Main Menu to restart them before using UNCONFIGURE.

A successfully-configured client system can be unconfigured locally. If there were any errors in configuring the client system as a security or directory service client, then the client must be unconfigured from some other system in the cell.

You cannot use the UNCONFIGURE option on a Security or Directory Server system. The only way to remove a node that has a Security or Directory Server from a cell is to reconfigure the entire cell.

1 Start **dce_config** on the client system.

2 Select UNCONFIGURE from the DCE Main Menu:

DCE Main Menu (on *hostname*)

selection: **4** (UNCONFIGURE)

S:****** Attempting to unconfigure a node from the cell name space...

3 Enter the hostname of the client:

Enter hostname of node to be unconfigured:

4 The system explains that unconfiguring a node will remove the node's ability to operate in a cell, and asks if you wish to continue:

Do you wish to continue (y/n)? **y**

5 Enter the principal name and password of the Cell Administrator for your cell:

Enter Cell Administrator's principal name: (cell_admin) Enter password:

dce_config deletes the registry entries and CDS entries for the client, then displays the DCE Main Menu.

6 You must now perform the REMOVE option on the client system. If you ran the UNCONFIGURE operation on a system other than the client, start **dce_config** on the client system. On the client system,

select REMOVE from the DCE Main Menu:

selection: **5** (REMOVE)

7 The system explains that removing a node destroys the node's ability to operate in a cell, and asks if you wish to continue:

Do you wish to continue (y/n)? **y**

The REMOVE option stops all running DCE daemons and removes all previous configuration files on the local machine.

8 If you wish to restart the client, follow the instructions in "Configuring Security and CDS Client Systems."

Removing and Reconfiguring the DCE Daemons

This section tells how to remove and reconfigure the DCE daemons. You will need to perform this procedure, for example, if you wish to stop a cell, if you wish to change the name of a cell, if a configuration does not succeed, or if a server system crashes.

If you wish to remove and reconfigure a client, first unconfigure and remove the client from the cell, then reconfigure the client. You may remove and reconfigure a client without reconfiguring the other members of a cell.

Removing a Security or CDS server requires that you reconfigure the entire cell. To reconfigure an entire cell, first perform the **dce_config** REMOVE operation on each cell member. You may then reconfigure the cell.

1 On the system you wish to affect, run **dce_config**.

2 Select REMOVE from the DCE Main Menu:

DCE Main Menu (on *hostname*)

selection: **5** (REMOVE)

Attempting to stop all running DCE daemons...

Successfully stopped all running DCE daemons...

Attempting to remove all remnants of previous DCE configurations...

Successfully removed all remnants of previous DCE configurations for all components...

Re-initializing the dce_config environment

3 If you are unconfiguring an entire cell, repeat steps 1 and 2 on each cell member.

4 If you wish to reconfigure the cell, do so as described starting with the section "Initial Cell Configuration". Reconfigure the cell only after you have run the REMOVE option on each cell member.

dce_config Error and Message Logging

dce_config and its component scripts write log messages containing errors, warnings, action summaries, and action details. Some log messages are written to **stdout**; log messages are also written to **/tmp/dce_config.log**. Log messages have different priorities, based on content, which determine both where the messages are logged and how they are formatted. The following table describes log message types (in priority order from highest to lowest), their format, and their content.

Table 4 **dce_config Message Categories**

Priority	Format	Content
ERROR	ERROR: <message>	Result of an operation was not as expected, and is possibly fatal. Always followed by a prompt for user to continue or quit.

Table 4 **dce_config Message Categories**

Priority	Format	Content
WARNING	WARNING: <message>	Information the user should be aware of before proceeding. Non-fatal. Always logged to display and to log file. Always followed by a prompt for user to continue or quit unless DO_CHECKS = "n".
SUMMARY	S:****** <message>	Highlevel summary of action being taken or action completed. Always logged to log file. Also logged to display unless DC_DISPLAY_THRESHOLD is WARNING or ERROR.
VERBOSE	V: <message>	Low-level summary of actions being taken, user queries and responses, or actual commands execute that do not affect configuration or node state. Logged to log file unless DC_LOG_THRESHOLD is DETAIL or higher. NOT logged to display unless DC_DISPLAY_THRESHOLD is VERBOSE or lower.
DEBUG	DEBUG: <message>	Actual commands executed that show only where in the dce_config script the actions are taking place. Also used for recording sleep commands.

ERROR messages are always followed by a prompt for user to continue or quit. If **dce_config** is being run using a "here" file for input, the environment variable EXIT_ON_ERROR should be set to **y** and exported to prevent errors from causing the "here" file to get out of sync with **dce_config**. (Also, CHECK_TIME should be set to **n** and exported when running **dce_config** from a "here" file.)

SUMMARY messages containing "Executing:" provide a record of exactly what commands were used to configure the cell.

VERBOSE messages containing "User query:" or "User entry:" contain a complete record of user entries in executing **dce_config**. The top of the log files contains a set of VERBOSE messages showing the settings of environment variables. These can all be used to reproduce a user's execution of **dce_config**.

DEBUG messages frequently contain error message text, since error text is passed to script functions for display if an error occurs. Do not confuse these messages with actual error occurrences. Only ERROR: or WARNING: messages indicate actual occurrence of a problem.

Component Scripts and Environment Variables for dce_config

This section contains information useful for those who wish to run **dce_config** from custom scripts. Included in this section is a description of the special-purpose component scripts that are called by **dce_config**, as well as a list and description of the environment variables that allow you to supply configuration input to **dce_config**.

dce_config Component Scripts

In a custom configuration script, you may wish to directly call the following **dce_config** component scripts. Each of these scripts resides in **/etc**:

- **dce.clean**: Kills running HP DCE daemons. Cannot be run remotely; must be run on affected DCE client or server node. Should be run before reconfiguring DCE.
- **dce.rm**: Removes data and configuration files created by DCE daemons after initial configuration. Should be run before re-configuring DCE. Cannot be run remotely; must be run on affected DCE client or server node.
- **dce.unconfig** *hostname*: Removes DCE client on *hostname* from the Security and Directory service databases. Should be run before reconfiguring DCE on a client system.
- **dce_com_env**: Sets common DCE environment variables.
- **dce_com_utils**: Common internal routines used by DCE utilities.
- **dce_config_env**: Sets common environment variables used by **dce_config**.
- **dce_config_utils**: Common internal routines used by **dce_config**.

- **rc.dce [boot]:** Starts HP DCE daemons. Cannot be run remotely; must be run on DCE client or server node. The **boot** parameter is optional; if supplied, **rc.dce** starts up **rpcd** without prompting the user with a 4 minute shutdown warning, and will immediately exit if an error occurs. The **boot** parameter should be set if **rc.dce** is executed from **/etc/rc**.
- **rc.dts**: Starts HP DCE DTS daemons. Called by **rc.dce**.
- **rc.dfs**: Starts HP DCE/DFS daemons. Called by **rc.dce**.
- **dfs_config**: Called through **dce_config** to perform DFS configuration tasks.
- **dfs.clean**: Kill running HP DCE/DFS daemons. Some daemons cannot be killed by dfs.clean, and can only be killed by rebooting the system.
- **dfs.rm**: Removes data and configuration files created by DCE/DFS daemons after initial configuration. Should be run before re-configuring DFS. Cannot be run remotely; must be run on affected DFS client or server node.

dce_config Environment Variables

dce_config recognizes the following environment variables. If these environment variables are set and exported before **dce_config** is run in interactive mode, the corresponding prompts for information will be skipped.

- CACHE_CDS_SERVER: Name of a CDS server in cell to cache. Need not be the initial CDS Server.
- CACHE_CDS_SERVER_IP: IP address of $CACHE_CDS_SERVER.
- CELL_ADMIN: Principal name of the Cell Administrator; either for an existing cell or for a to-be-configured cell.
- CELL_ADMIN_PW: Password for the Cell Administrator, either for an existing cell or for a to-be-configured cell.
- CELL_NAME: Name of your cell (without /.../).
- CHANGE_PW: This internal variable tracks whether **dce_config** receives the warning "Password must be changed" to indicate the cell administrator password is the same as the default password. Initial

value is **n**; do not alter this initial value.

- CHECK_TIME: Set to **y** to have time checked and possibly synchronized; **n** otherwise. Default is **y**. If **dce_config** is executed from a "here" file, CHECK_TIME should be set to **n** since time checking uses a **telnet** command that causes input from the "here" file to be lost. Note that SDCC and **dce_config** do not recognize time zones. If configuring a cell across time zones, set CHECK_TIME to **n**.
- CONFIG_DFS_CLIENT: Set to **y** if you wish to configure this node as a DFS client while configuring it as a client of the other services; **n** otherwise. If not set, user is prompted for response.
- CONFIG_PROTSEQ: Communication protocol used for some **dce_config** operations.This variable is set to **ncadg_ip_udp** by default for use of the UDP protocol, which works in almost all cases. Change to **ncacn_ip_tcp** if only TCP protocol routing is available. (For DFS to function, UDP must be available).
- DC_DISPLAY_THRESHOLD: Minimum priority log message from dce_config that are written to stdout. Default is SUMMARY. ERROR and WARNING messages are always displayed. Possible values, in priority order: ERROR, WARNING, SUMMARY, DETAIL, VERBOSE, DEBUG.
- DC_LOG_THRESHOLD: Minimum priority log message from **dce_config** that are written to **/tmp/dce_config.log**. Default: DEBUG (all messages). ERROR, WARNING, and SUMMARY messages are always logged. Possible values, in priority order: ERROR, WARNING, SUMMARY, DETAIL, VERBOSE, DEBUG.
- DEFAULT_MAX_ID: Maximum Unix ID value supported by DCE Security Registry. Can be set to any value. Default value is 32767. A value larger than the default prevents accounts with ID's larger than 32767 from accessing DCE cells that use the default. A value smaller than default prevents foreign accounts with ID's larger than 32767 from accessing the cell.
- DEFAULT_PW: Default password used when the registry is created. Used only for logging in the cell administrator for the first time (within **dce_config**). A cell administrator can change the default by editing the value of DEFAULT_PW in the script. Default is **-dce-**.
- DIR_REPLICATE: Supports replication of additional directories

when configuring additional CDS Servers. If set to "n" it will not prompt if additional directories need to be replicated.

- DO_CHECKS: Set to **n** to prompt when a non-fatal warning is encountered. Default is **y**.
- EXIT_ON_ERROR: Set to **y** to exit from dce_config if a fatal error is encountered. Default is **n**. This can prevent a "here" file from getting out-of-sync with **dce_config**.
- GID_GAP: Increment above highest currently-used GID at which the Registry Service will start assigning automatically-generated GID's. Default is 100.
- HOST_NAME_IP: IP address of node on which **dce_config** is running.
- HPDCE_DEBUG: Set to **1** starts daemons in the foreground.
- KEYSEED: Keyseed for initial database master key.
- LAN_NAME: Internal name of the LAN (in the LAN profile) when using multiple LANs. Use when configuring a CDS server
- LOW_GID: Value at which the Registry Service will start assigning automatically-generate d GID's. Default is the value of the highest currently used GID plus $GID_GAP. If $LOW_GID is less than or equal to the highest currently used GID, a warning is issued, and user is prompted to enter a new value (which can be the value of $LOW_GID).
- LOW_UID: Value at which the Registry Service will start assigning automatically-generate d UID's. Default is the value of the highest currently used UID plus $UID_GAP. If $LOW_UID is less than or equal to the highest currently used UID, a warning is issued, and user is prompted to enter a new value (which can be the value of $LOW_UID).
- MULTIPLE_LAN: Set to **y** to configure this node with multiple LAN capability. Use when configuring a CDS server. Default is **n**.
- NTP_HOST: Hostname on which the NTP server is running.
- TP_DEV: Name of device to which Spectracom time source is attached. Example: /dev/tty00.

- REMOVE_PREV_INSTALL: Set to **y** to remove all remnants of previous DCE installations for all components before installing a security server. Use only in installing the security server software. Default is **n**.
- REMOVE_PREV_CONFIG: Set to **y** to remove all remnants of previous DCE configurations for all components before configuring a client or an initial CDS server. Default is **n**.
- REP_CLEARINGHOUSE: Name for new clearinghouse.
- SEC_SERVER: Name of the security server for this cell.
- SEC_SERVER_IP: IP address for $SEC_SERVER.
- SYNC_CLOCKS: Set to **y** to synchronize client clock with that of the security server; **n** otherwise. If not set, and clocks are out of sync by more than $TOLERANCE_SEC, user is prompted for whether to synchronize. This variable is irrelevant if CHECK_TIME is set to **n**.
- TOLERANCE_SEC: Number of seconds client node system clock is allowed to differ from security server system clock before warning that clocks are not in sync and allowing input to synchronize. Default is 120 seconds. Note: Security and Cell Directory services require less than a 5 minute difference between any two nodes in the cell.
- UID_GAP: Increment above highest currently-used UID at which the Registry Service will start assigning automatically-generated UID's. Default is 100.
- UNCONFIG_HOST_PRESET: Hostname of node to be unconfigured.

Starting HP DCE/9000 at System Boot

The HP DCE/9000 configuration tools (SDCC and **dce_config**) save the configuration information for each cell member by modifying the file **/etc/rc.dce**. To start DCE daemons automatically on system reboot, you should run **/etc/rc.dce** from **/etc/rc**. If you run the **/etc/dce.login install** utility, which is described in Chapter 5, *DCE-Integrated Login Utilities*, this will be done for you automatically.

Users of NCS-based software should see "Note for Users of NCS-based Software" for important information about starting NCS and HP DCE/9000 daemons on system reboot.

If you de-install HP DCE/9000, you should remove the reference to **/etc/rc.dce** from **/etc/rc**. The utility **/etc/dce.login uninstall** will automatically do this for you.

Note for Users of NCS-based Software

Users of NCS-based software must take the following precautions when configuring HP DCE/9000:

1 Before configuring HP DCE/9000, stop any servers for NCS-based applications.

2 Stop **glbd** (via **drm_admin** "stop") if it is running.

3 Stop **llbd** (via **kill**(1)).

4 Configure HP DCE/9000.

5 Run **/etc/netncsrc** to restart NCS daemons.

6 Restart any servers for NCS-based applications.

Starting NCS and DCE Applications at System Boot

At system boot, HP DCE/9000's **rpcd** daemon must be started in place of **llbd** and before other NCS daemons. Users of NCS-based software should take the following precautions to ensure NCS and HP DCE/9000 compatibility:

1 Move the code that invokes **netncsrc** from **/etc/netlinkrc** to **/etc/rc**.

2 Move the code that invokes **netlsrc** from **/etc/netlinkrc** to **/etc/rc** (*after* the code that invokes **netncsrc**).

3 Place the reference to **/etc/rc.dce** in **/etc/rc**, *before* the references to **netncsrc** and **netlsrc**. **/etc/rc.dce** must be invoked *before* **/etc/netncsrc** and **/etc/netlsrc**.

rpcd and **llbd** cannot co-exist because they listen on the same system port. However, only **rpcd** must be run when using both HP DCE and NCS, because **rpcd** incorporates **llbd** support for NCS 1.5.1 applications.

Note that when you install HP DCE/9000, you do not have to disable **llbd**-startup. If **rpcd** is running, **llbd** will fail, but this error can be ignored. Leaving **llbd**-startup enabled ensures that NCS applications will continue to run if HP DCE/9000 is de-configured or de-installed.

HP DCE/9000 Interoperability with HP MPower and SharedPrint/UX

HP MPower 1.2 or earlier and applications built using version 3.12 or earlier of the HP MPower Audio Library require that the file **/tmp/llbdbase.dat** exist. This file is normally created by **llbd**, but is not created by **rpcd**. If you are running HP DCE/9000 and HP MPower 1.2 or earlier, you must manually create this file by adding the line

```
touch /tmp/llbdbase.dat
```

to **/etc/rc**, before **/etc/rc.dce** is invoked.

SharedPrint/UX 1.3 or earlier will not operate with HP DCE/9000.

5

DCE-Integrated Login Utilities

DCE-Integrated Login Utilities

HP DCE/9000 includes a set of DCE-integrated login utilities. These utilities authenticate users via the DCE Security Registry, giving users DCE credentials upon HP-UX login. If DCE is not available, users are authenticated via **/etc/passwd**, but are not given DCE credentials.

The DCE-integrated login utilities include **login**, **vuelogin**, **vuelock**, **su**, **ftpd**, **passwd**, **chsh**, **chfn**, **telnet**, and **rlogin**. **ftpd** and **vuelock** are new to HP DCE/9000 Version 1.2; all other DCE-integrated login utilities have been improved since HP DCE/9000 Version 1.1.

Use of these utilities is optional; they are installed but not activated when HP DCE/9000 is installed. If you wish to use them instead of the standard HP-UX login utilities, carefully read and follow the instructions in this section.

Overview of New Features

The DCE-integrated login utilities provide the following functionality:

- The integrated utilities attempt to first authenticate a user via DCE. If DCE is unavailable, the user is authenticated via **/etc/passwd**. The utilities make it possible for system administrators to use DCE as the primary source of user information.
- Users' home directories may reside in DFS.
- In an HP VUE environment, each window created during a VUE session inherits the user's DCE credentials. (Otherwise, a user would have to run **dce_login** in every window in which DCE and/or DFS operations are desired.)
- DCE-integrated **ftpd** enables **ftp** access to permission-protected DFS file systems.
- Integrated **vuelock** refreshes DCE credentials upon unlocking the VUE session. If DCE is unavailable, the screen can still be unlocked; the user password is verified via the **/etc/passwd** file.

Deciding Whether to Use the DCE Login Utilities

When deciding whether to install the DCE-integrated login utilities, consider the following:

- The DCE-integrated login utilities must be deployed in a stable system environment. The system relies on periodic automated updates of **/etc/passwd** to mirror current DCE registry information. Therefore, DCE must be left configured and the DCE cell must be maintained. The network must remain reliable 24 hours a day.
- The DCE registry will export information to **/etc/passwd** via **passwd_export**. On each DCE-integrated system, a **cron** job will run every hour to accomplish this task.
- All users of a system must have a DCE account, including users who are declared in **passwd_override**.
- All account administration must be done through the DCE registry. Changes made to local /etc/passwd files will be lost as the cron job updates /etc/passwd with an image of the DCE registry.
- NIS access is disabled for password and group mapping.
- The system must not be configured with HP-UX commercial security (i.e. the DCE-integrated utilities are not integrated with the shadow password file).

Operation of the DCE Login Utilities

The DCE-integrated login utilities function the same as their HP-UX counterparts, with the following exceptions:

- Most commands provide additional messages when DCE authentication is unavailable and standard HP-UX authentication is used.
- The **passwd**, **chfn**, and **chsh** utilities manipulate the DCE registry and the **passwd_override** file. They will fail if DCE network registry cannot be reached. These commands synchronously change the DCE registry or the **passwd_override** file, but the propagation of this change to **/etc/passwd** may be delayed as long as one hour (depending on when the **cron** job is run).
- User **root** cannot change passwords in the DCE Registry. The network administrator must login as the cell administrator and use **rgy_edit** to change other user accounts and passwords.
- User passwords are limited to 128 characters for **ftp**, otherwise passwords can be up to 512 characters.
- DCE-integrated login utilities take longer to execute and require more system resources than the HP-UX equivalents.
- For operations that do not require the user to enter a password, no DCE credentials are obtained. Examples include:
  - **su** when executed by root
  - **rlogin** when a **.rhosts** file authorizes access
  - anonymous **ftp**

Preparing to use the DCE Login Utilities

Before activating the DCE login utilities on a system, you must do the following:

- Configure the system as a DCE cell member.
- Set up valid accounts in the DCE Registry for all users that require login access to the cell, or local login access to cell member systems. Use either **rgy_edit** or **passwd_import** to set up accounts. Be aware that **passwd_import**:
  - Creates accounts for all entries in **/etc/passwd** but marks the accounts invalid. After using **passwd_import**, the cell administrator must use **rgy_edit** to assign a password to each account and to mark each account as valid.
  - Does not create accounts from NIS information.
- Create entries in **/opt/dcelocal/etc/passwd_override** for any accounts (such as printing or backup services) that require access to your system, but not to the DCE cell. Entries may be copied directly from **/etc/passwd** and appended to **/opt/dcelocal/etc/passwd_override**. The **dce.login** script will automatically create an override entry for **root**; however, you must create override entries for any **root** aliases.
- The **passwd_override** file can also be used to disable access to the local system for selected users or groups. See the **passwd_override** man page for details.

See the man pages **rgy_edit**(8) and **passwd_import**(8) or the *OSF DCE Administration Guide – Core Components* for more information on importing and exporting account information, and on creating and modifying DCE registry accounts.

Activating DCE Login Utilities

The integrated login utilities are provided in the DCE-CMN fileset. They are installed, but not activated, when HP DCE/9000 is installed.

The binary names for the DCE-integrated login utilities are listed in Table 5.

Table 5 **DCE-integrated login binaries**

/bin/login.dce	/bin/su.dce
/bin/passwd.dce	/bin/dceexec
/usr/bin/chfn.dce	/usr/bin/chsh.dce
/usr/vue/bin/vuegreet.dce	/usr/vue/bin/vuelogin.dce
/usr/vue/bin/vuesession.dce	/etc/ftpd.dce
/usr/vue/bin/vuelock.dce	

A script, **/etc/dce.login**, is provided to activate the DCE-integrated login utilities. Until you run **dce.login**, your standard HP-UX login utilities are used.

To activate the integrated login utilities in each DCE cell member system:

1 Be sure that you have completed the steps in Preparing to use the DCE Login Utilities.

2 Login as **root**.

3 **dce_login** as **cell_admin.**

4 Run **dce.login install.**

5 Reboot the system.

dce.login install does the following:

- Ensures that the DCE Registry Service does not hide encrypted password fields exported by **passwd_export**.
- Ensures that a **root.system.none** account exists in the DCE Security Registry and is valid.
- Ensures that **rc.dce** is run as part of a system boot.
- Copies the root account entry in **/etc/passwd** to **/opt/dcelocal/etc/passwd_override**.
- Saves the **/etc/passwd** file in **/etc/passwd.nodce** and the **/etc/group** file in **/etc/group.nodce** (if these files do not already exist).
- Executes **passwd_export** every hour as a **cron** command. You can adjust this frequency by editing the **passwd_export** entry in **/usr/spool/cron/crontabs/root**. Frequencies greater than once per hour are not recommended.
- Sets up the configuration file **/etc/login.conf** to ensure that DCE is used for **vuelogin** and **login** authentication.
- Hard-links the HP-UX **login** utilities to the DCE-integrated versions and saves a copy of the native HP-UX login utilities by appending a **.nodce** suffix to the original binaries.

  Installation terminates with an error message when any of these steps fails.

  If you are using HP VUE on the system, when **dce.login** completes successfully, reboot your system *before* you log out. This is required to start the DCE-integrated **vuelogin** utility.

De-activating DCE Login Utilities

You can de-activate the DCE login utilities and restore the original HP-UX versions as follows:

1 Log in as **root** (you do not need to be **cell_admin**)

2 Run **dce.login uninstall**

3 Run **passwd_export** to update the local **/etc/passwd** file from the DCE registry (optional).

4 Reboot the system.

The **uninstall** option does the following:

- Deletes the **cron** command that executes **passwd_export.**
- Provides the option of deleting the call to **rc.dce** in the **/etc/rc** script.
- Provides the option of restoring the original **/etc/passwd** and **/etc/group** files.
- Removes the **/etc/login.conf** configuration file.
- Restores the login utilities to the original non-DCE versions.

If an error occurs during any step, an error message is displayed and you have an option to exit or continue to the next step. After successfully running **dce.login uninstall**, reboot your system to start the non-DCE version of **vuelogin** (if your system is running HP VUE).

Notes, Cautions, and Warnings

- Both **dce.login install** and **dce.login uninstall** can be re-executed without harmful results. If **dce.login install** fails to complete, you should re-execute it until it completes successfully, or run **dce.login uninstall**. Failure to do this may cause the login utilities to behave unpredictably.
- Immediately after you run **dce.login install**, if you log out of the system before rebooting, you will not be able to log in via the VUE login screen. You will have to log in from another system via a network login utility (**telnet** or **rlogin**) and reboot. Alternatively, you may be able to log in via the VUE login screen by first clicking on the **Options** button on the VUE login screen and selecting the **No Windows** option. You may then be able to log in via the VUE login screen. Then reboot the system to start the DCE-integrated **vuelogin**.
- If you run the DCE-integrated login utilities and decide to upgrade HP-UX, you should re-execute **dce.login install** after the HP-UX upgrade.
- To avoid a possible problem with logging in via the HP VUE "No Windows" mode, DCE cell member systems that run the DCE-integrated login utilities should default to run-level 4 at boot-time. This is accomplished by modifying the following line in **/etc/inittab**:

  ```
  init:4:initdefault
  ```

  See the **inittab**(4) man page for more information about run levels.
- Do not use SAM (the HP-UX System Administration Manager) to administer users and groups. Use **rgy_edit** instead.
- Do not activate Auditing or Trusted Systems (shadow password file, commercial security).
- If DCE is unavailable, the **passwd_export cron** job that is set up by **dce.login install** will fail and generate an email error message. To stop these error messages, remove the **cron** job by running **dce.login uninstall** after you stop or remove DCE. If you later restart DCE, be sure to re-run **dce.login install** to bring the system **/etc/passwd** file up-to-date with the DCE registry.

- During the DCE-validation process, the DCE-integrated login utilities obtain certified network credentials. However, the "final" DCE credentials obtained are not marked as network-certified. Because network-certification is obtained during the validation process, these DCE credentials may be treated as certified.
- If your DCE password is longer than 8 characters, and the password you enter at login begins with the same 8 characters but is not identical, the login will succeed but will not provide DCE credentials.
- If a user is logged in as a valid DCE user, then logs in (via **su** or **ftp**) as another user who is in the override file, the DCE identity of the original user will still be used for DFS.
- The DCE-integrated login utilities do not allow the use of global names for users and principals (i.e. **/.../mycell/myname**). The user logging in must have an account in the DCE registry of the local cell.
- The default home directory for cell_admin is "/". Because **cell_admin** does not have write privileges to this directory, login may fail. The **cell_admin** account should be given a writable home directory through either the DCE security registry or the **passwd_override** file.
- The DCE-integrated login utilities may not work when the system disk is full or disk quotas are exeeded. DCE requires disk space for the creation of temporary files.
- The DCE credentials are not removed when the user logs out. DCE credentials may be removed via the **kdestroy** utility.

AFS and Kerberos Authentication

The DCE-integrated login utilities can also provide authentication to AFS 3.2 and/or Kerberos 4.0 at login time. You can choose this service when **dce.login install** is run, or by editing the file **/etc/login.conf** (see the **login.conf** man page for details).

Authentication to AFS and/or Kerberos has the following requirements and restrictions:

- All administrative code for AFS and/or Kerberos must be available and operational on the system.
- AFS and Kerberos cells must be configured and operational.
- DCE, AFS and/or Kerberos passwords must be identical.
- If AFS and/or Kerberos authentication is activated, the DCE-integrated **passwd** command will act on all passwords. Only failure on changing the DCE password is fatal.
- Some DCE, AFS, and Kerberos commands have the same name. The pathnames of the various commands will differ, and will be installation-specific.

NOTE

Although Hewlett-Packard provides the capability for AFS and Kerberos Authentication in the DCE-Integrated Login Utilities, Hewlett-Packard does not support the operation of AFS or Kerberos. Before calling Hewlett-Packard for support in this area, you must verify that any incorrect behavior you notice occurs only when using the DCE-Integrated Login Utilities and not when using native AFS and/or Kerberos commands to obtain credentials. You must furthermore verify that you are running the version of AFS and/or Kerberos supported by the DCE Integrated Login Utilities, and that all the other requirements and restrictions listed above are met.

Support of AFS and Kerberos Authentication is not provided in DCE-Integrated version of **ftpd**.

DCE and Anonymous FTP

If you are using the integrated login utilities on a system that supports anonymous ftp, be aware of the following:

- An ftp account must exist in the DCE registry. This account need not be password-validated for DCE use, but it must exist. Create this account using **rgy_edit**, or use the **passwd_import** utility from a system that is supporting anonymous ftp (i.e. run **passwd_import** from a machine that has an entry for the ftp user in **/etc/passwd**).
- An anonymous ftp directory cannot exist in a permissions-protected DFS file system, because no DCE credentials are obtained for the anonymous ftp user. An anonymous ftp directory can exist in a DFS file system with open permissions. However, when putting a file into DFS via anonymous ftp, the resulting file will be owned by user **nobody**, since DFS finds no credentials to identify the anonymous ftp user.
- DCE accounts are global to a DCE cell. If anonymous ftp is supported anywhere in the cell, the ftp account is known throughout the cell. In the case that you would like to explicitly disable anonymous ftp to a local machine, an override entry should be placed in the **passwd_override** file for the ftp user. (Typically, an entry in **passwd_override** is created by cutting and pasting the ftp entry from **/etc/passwd** into the **passwd_override** file). To disable ftp on the local machine, change the **passwd_override** entry to contain the word "OMIT" in the passwd field of the entry. For example, **/opt/dcelocal/etc/passwd_override** contains the line:

  ```
  ftp:OMIT:500:10:anonymous ftp:/users/ftp:/bin/false
  ```

  See the **passwd_override** man page for further details about using the OMIT keyword
- If you would like to maintain a local anonymous ftp account on a DCE cell member system, place an entry for the anonymous ftp account in the **passwd_override** file on that system. Note that the home directory for the local anonymous ftp account must reside on the local system, and that an entry for user **ftp** must exist in the DCE registry.

Automating dce.login

dce.login can be executed non-interactively by first setting and exporting the following environment variables.

dce.login recognizes the following environment variables in both **install** and **uninstall** modes:

- EXIT_ON_ERROR: Set to **y** to exit from **dce.login** if a fatal error occurs. The default is **n**. This environment variable should be used when executing **dce.login** via a "here" document to prevent it from getting out-of-sync with **dce.login**.
- DO_CHECKS: Set to **y** to have **dce.login** prompt when a non-fatal warning is encountered. The default is **y**. If this is set to **n**, **dce.login** does not issue any prompts and is executed with default values for the variables listed next.

dce.login install recognizes the following environment variables:

- VALIDATE_ROOT: Set to **y** to have **dce.login** make sure that the root.system.none account is valid. The default is the value of DO_CHECKS.
- ENSURE_NOT_HIDE: Set to y to have dce.login ensure that the property of exported passwords is set to "NOT HIDDEN". The default is the value of DO_CHECKS. Note that if the exported passwords are hidden, the DCE login utilities will not be able to fall back to **/etc/passwd** if DCE login fails.
- AFS_LOGIN, KRB_LOGIN: Set to y to have dce.login set up the DCE login utilities to do AFS 3.2 and Kerberos V4 authentications, respectively. If DO_CHECKS is set to y, dce.login prompts for whether or not to activate those authentications. If DO_CHECKS is set to n, then the default of these variables is NULL, in which case dce.login sets up the login utilities as described in file **/etc/login.conf**. If **/etc/login.conf** does not exist, then the DCE login utilities are set up to do DCE authentication only.

dce.login uninstall recognizes the following environment variables:

- RESTORE_PWD: Set to y to have dce.login restore the original /etc/passwd and /etc/group files. If DO_CHECKS is set to y, dce.login prompts for whether or not to restore the original files. If DO_CHECKS is set to n, then the default of this is n. Before the original password file are restored, the root password will be updated to the one in /opt/dcelocal/etc/passwd_override.
- PRESERVE_RC: Set to y to have dce.login preserve the rc.dce entry in /etc/rc script that starts DCE during boot time. If DO_CHECKS is set to y, dce.login prompts for whether or not to remove the entry. If DO_CHECKS is set to n, then the default of this is n.

6

Administering HP DCE/9000 Security

Administering HP DCE/9000 Security

This chapter discusses procedures for creating and administering replicated security servers in HP DCE/9000.

Overview

A Security Server and its registry database can be replicated within a cell. Each instance of a Security Server in a cell maintains a working copy of the database. The combination of a Security Server and its data (the registry database) is referred to as a *replica*. Having several replicas in a cell can enhance performance and reliability.

Master and Slave Replicas

Each cell can have only one **master** replica but numerous **slave** replicas. The master replica accepts updates to its database from clients and handles subsequent propagation of changes to all other replicas. Slave replicas accept only reads from clients. For example, either a master or a slave replica can provide account information to a client program such as **/bin/login**. However, if you are adding an account or changing password information, those updates can be handled only by the master replica. The Security tools that access the replicas automatically bind to the type of replica required for the operation they are performing.

The process of updating the database differs slightly between the master replica and slave replicas. The figures titled "The Master Replica Update Process" and "Slave Replica Update Process" illustrate the master and slave update processes. The processes are described in the sections that follow the figure.

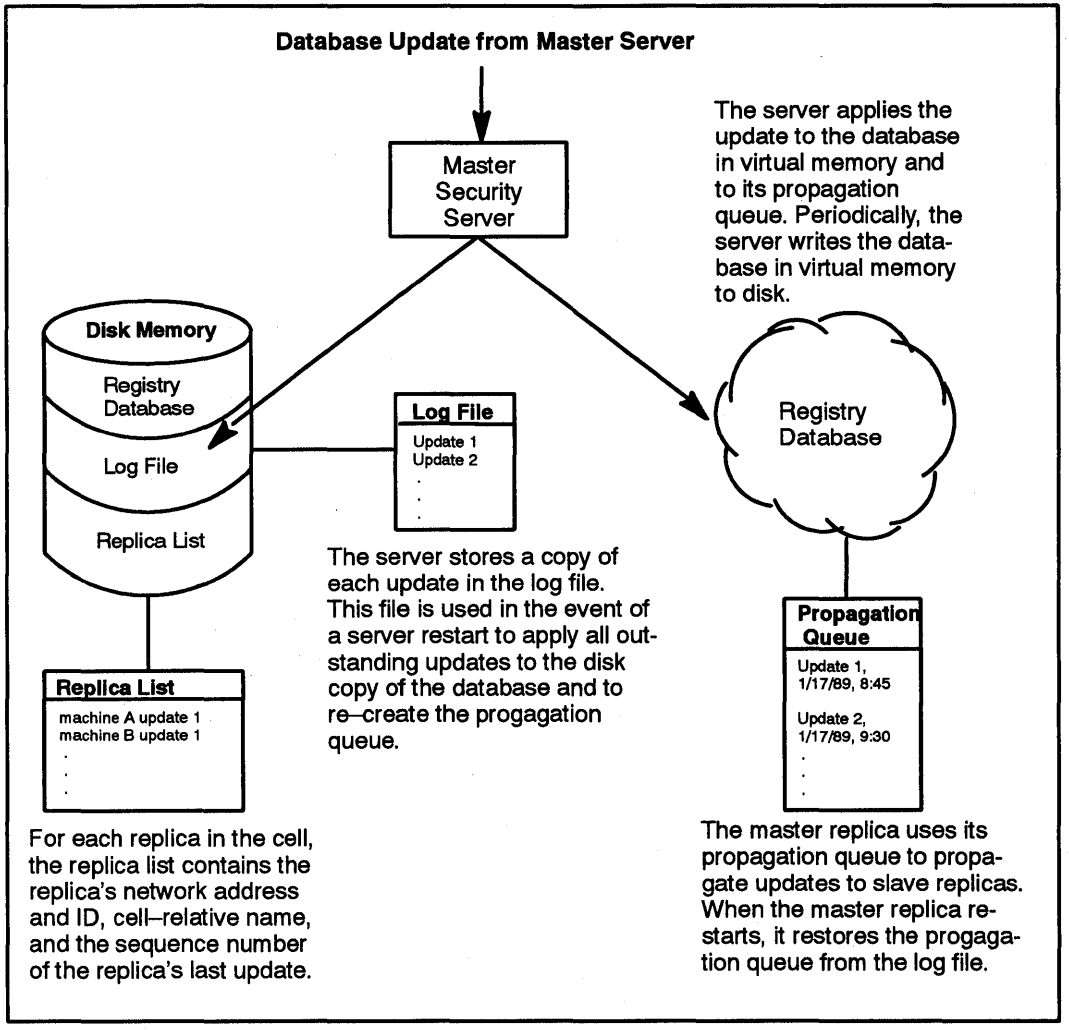


Figure 1. Master Replica Update Process

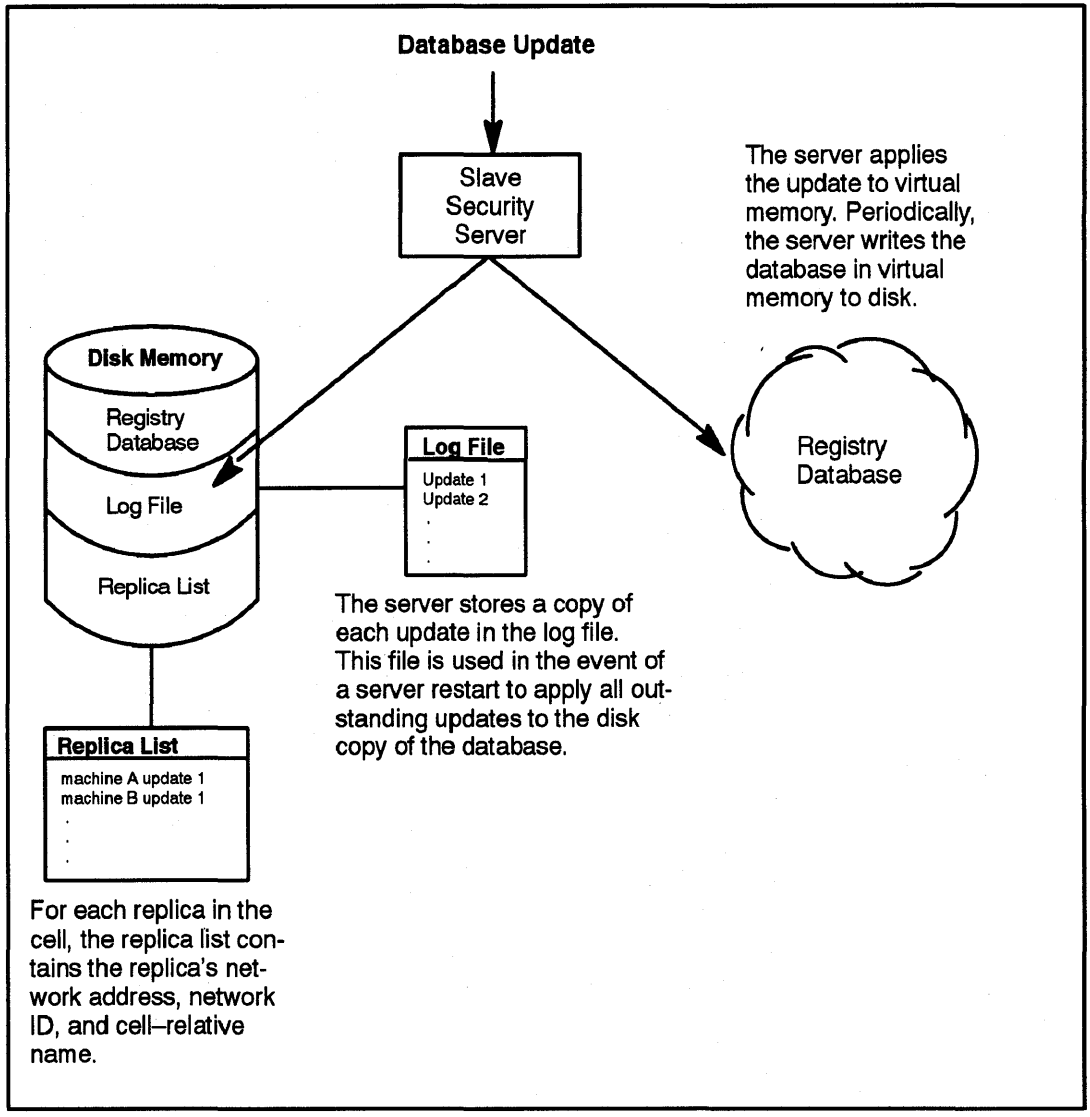


Figure 2. Slave Replica Update Process

While propagations are pending, all replicas are accessible even if they are not completely up-to-date. In other words, even replicas to which the changes were not yet applied are available. This replication mechanism ensures that all replicas remain available for login validation and for read operations even when changes are in the process of being propagated.

Handling Database Updates

When a master or slave replica receives updates, it applies the update to its database in virtual memory, and saves a copy of the update in a log file stored on disk. Updates accumulate in the log file in sequence number order. If a server restarts unexpectedly, the log file assures that no updates are lost.

Periodically, the replica writes the database in virtual memory to disk thus bringing the disk copy up to date. Then, if the replica is a slave, it clears the log file of all updates. If the replica is the master, it clears the log file of all updates that have been propagated to the slave replicas. Updates that have not been propagated to the slaves are retained and used to reconstruct the propagation queue if necessary.

Only the master replica maintains a propagation queue, used to hold changes to be propagated to the slave replicas. When the master replica receives an update, it adds it to the propagation queue in addition to its virtual memory database and its log file. Each update in a propagation queue is identified by a sequence number and a timestamp. The sequence number is used internally to track the propagation of updates to slave replicas. The timestamp is provided to show users the date and time of updates.

When a master or slave replica restarts, it initializes its database in virtual memory and then applies any outstanding updates in the log file to its database. If the replica is the master replica, it also recreates the propagation queue from the log file so that any outstanding slave updates can be propagated. This mechanism assures that no updates are lost when a server is shut down.

Propagating Database Changes

To propagate updates to the slave replicas, the master replica first updates its copy of the database using the process described in "Handling Database Updates." Then, the master attempts to propagate the update to each slave replica on its replica list. The replica list contains each slave replica's ID and network address. It also contains the sequence number of the last update made to the slave. The master replica always propagates in sequence number order. By examining the sequence number associated with a replica in its replica list, and the sequence numbers of the updates in its propagation queue, the master can determine which of the updates on its propagation queue must be propagated to which slave. This mechanism helps ensure that the unavailability of a single slave replica does not interfere with updates to the rest of the slave replicas.

If the propagation of an update does not succeed on the first attempt, the master replica tries periodically until it succeeds. When the update succeeds, the master changes the sequence number associated with the updated replica on its replica list. When an update is propagated to all the slave replicas, the master removes the update from its propagation queue. Use the **sec_admin lrep -prop** command or **sec_admin lrep -all** command to display the propagation management information the master maintains for each replica.

If the master replica loses communication with a slave replica for a protracted period of time, you must explicitly initialize a slave replica's database using the **sec_admin initrep** subcommand. (See the **sec_admin** reference page for details on using the **sec_admin initrep** subcommand.)

Replica Authentication

Like all DCE objects, the master and slave replicas must authenticate to each other. To do this, the master carries the identity of **dce-rgy**, one of the principals created when the database is created

by **sec_create_db**. Slaves carry the identity of the host machine on which they exist. This identity must have **i, m,** and **I** permissions to the **/.:/sec/replist** object.

sec_admin command changes

The **sec_admin** command now includes subcommands for administering replicas:

info	Displays status of the default replica.
lrep	lists replicas on the default's replica list.
monitor	Lists replicas at specified time intervals.
destroy	Destroys the current default replica.
site	Sets or displays the default cell and default replica.
delrep	Deletes a replica.
initrep	Reinitializes a replica.
stop	Stops a replica.
state	Puts the master replica into and out of maintenance state.
master_key	Generates a new master key used to encrypt principal keys.
change_master	Move the master registry to another server system.
become -master	Change a replica to a master registry.

The **rgy_edit** command is for making changes to the registry database entries. The **sec_admin** command cannot add, delete, or modify information in the database.

The **dce_config** command script contains a new menu item in the Additional Server Configuration menu. The new item, **Replica Security server**, does the following:

- Obtains the name of the new security replica.
- Starts **rpcd** if it is not already running.
- Configures this machine as a Security client.

- Configures this machine as a CDS client.
- Modifies ACLs on the security replist so that this host may become a security replica.
- Modifies ACLs on the CDS security directory and security group so that this host can add its name to the security directory and security group.
- Executes **sec_create_db** to create a stub security database. Later, the master will initialize this database.
- Starts the security server on this machine. The master, or another up-to-date replica, will initialize this new server's database.

The **sec_create_db** command has been expanded to provide subcommands for creating replicas:

- **-master** Creates a database for the master replica.
- **-slave** Creates a database for the slave replica.

All **sec_create_db** options can be used with the **-master** subcommand. However, only **-myname**, **-keyseed**, and **-verbose** options can be used with the **-slave** subcommand.

Setting up the Registry

Many steps are performed by the HP DCE cell configuration tools (**SDCA** or **dce_config**) and some are performed by using security commands. The basic steps are:

1 Plan the network configuration.

2 Create the master registry database (performed by SDCA or **dce_config** during system configuration).

3 Start the master replica (performed by SDCA or **dce_config** during system configuration).

4 Populate the registry database (performed by you using the **rgy_edit** command). First set policies and procedures, then add names and accounts.

5 Create a slave database and start the slave replica (performed by SDCA or **dce_config** during system configuration).

6 Set up cron to run **passwd_export** on all DCE-based machines to ensure that local **password** and **group** files are kept consistent with the registry (performed by you using standard UNIX commands).

Planning a Configuration

Choose a site for the master replica and sites for the slave replicas. These sites will run **secd**, the Security Server. Machines running **secd** must be up and available at all times. It is especially important that the machine where the master replica runs is available throughout the network.

The machine size required to run **secd** depends on the platform and operating system. Choose machines large enough to accommodate future growth of the registry database. The machines must have enough memory and disk space for the registry database and enough backing storage. We have found the following requirements to be sufficient:

- For each principal: 1000 bytes of physical memory
  700 bytes of disk space
- For each account: 700 bytes of physical memory
  300 bytes of disk space

Because **sec_salvage_db** loads all of the security registry information into memory for processing, its memory utilization increases as the number of principals/accounts increases. For very large registry databases, ensure that the machine running **sec_salvage_db** is configured with enough swap space. Roughly 3000 bytes per principal is required.

The master security server site and the slave security server sites will run **rpcd**, **secd**, and **sec_clientd**. If a cell is running a cell directory service, all hosts in the cell will run the **cdsadv**.

The security client host will run **rpcd** and **sec_clientd.**

Creating the Master Registry Database

When you initially configure your cell's Security Server, SDCC or **dce_config** invokes the **/opt/dcelocal/bin/sec_create_db** command to create the master replica. When **sec_create_db** creates a new master replica, it initializes its database with names and accounts.

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

In the event that you ever need to create a new master registry database, you can invoke **sec_create_db** directly. (You must be root to run **sec_create_db**.) Note that it is highly unusual to re-create a master database but you may need to re-create a slave database if the slave is destroyed.

sec_create_db Format

The **sec_create_db** command has the following format:

sec_create_db
{**-master** | **-slave**}
-**my**[**name**] *my_server_name*
[-**k**[**eyseed**] *keyseed*]
[-**cr**[**eator**] *creator_name*]
[-**cu**[**nix_id**] *creator_unix_id*]
[-**u**[**uid**] *cell_unix_id*]
[-**p**[**erson_low_unix_id**] *unix_id*]
[-**g**[**roup_low_unix-id**] *unix_id*]
[-**o**[**rg_low_unix-id**] *unix_id*]
[-**ma**[**x_unix_id**] *unix_id*]
[-**pa**[**ssword**] *default_password*]
[-**v**[**erbose**]

-master	Specifies that the master replica's database should be created. All other **sec_create_db** options can be used with the **-master** option.
-slave	Specifies that a slave replica's database should be created. Only the **-myname**, **-keyseed**, and **-verbose** options can be use with the **-slave** option.
-**my**[**name**] *my_server_name*	Is a name you assign to the Security Server (**secd**) on this machine. It is used by the Naming Service to locate this cell's Security Server. (Required)
-**k**[**eyseed**] keyseed	Is a character string you enter that is used to seed the random key generator in order to create the master key for the database you are creating. The master key is used to encrypt all account passwords. Each instance of a replica (master or slave) has its own master key. You can

	change the master key using the **sec_admin** command. See the **sec_admin** reference page for information on the use of **sec_admin**. If you do not enter this option, **sec_create_db** prompts for it.
[-**cr**[**eator**] *creator_name*]	Is the name of the registry creator. The registry creator is the initial privileged user of the registry database. (You can give equivalent privileges to another user at any time by using the acl_edit command to change the registry database ACL.) When the registry is created, default ACL entries for registry objects are also created. These entries give the most privileged permissions to the principal named in the -**cr** option. If the principal named as the registry creator is not one of the reserved names, **sec_create_db** adds the principal and an account for that principal. If you do not enter this option, the initial privileged user of the registry database is root.
[-**cu**[**nix_id**] *creator_unix_id*]	Is a UNIX number that you specify to be assigned to the registry creator. If you do not enter this option, the registry creator's UNIX number is assigned dynamically.
[-**u**[**uid**] *cell_unix_id*]	Is the cell's UUID. If you do not enter this UUID, it is assigned dynamically.
[-**p**[**erson_low_unix_id**] *unix_id*]	Starting point for UNIX IDs that are automatically generated when a principal is added using the **rgy_edit** command. (You can explicitly assign a lower UID than this number; this lower limit applies only to automatically generated UIDs.)

[-g[**roup_low_unix-id**] *unix_id*]	Starting point for UNIX IDs that are automatically generated when a group is added using the **rgy_edit** command. (You can explicitly enter a lower UNIX ID than this number; this lower limit applies only to automatically generated UIDs.)
[-o[**rg_low_unix-id**] *unix_id*]	Is the starting point for UNIX IDs that are automatically generated by the Security Service when an organization is added using the rgy_edit command. (You can explicitly enter a lower UNIX ID than this number; this lower limit applies only to automatically generated UNIX IDs.)
[-**ma**[**x_unix_id**] *unix_id*]	Is the highest number that can be assigned as a UNIX ID when a principal, group, or organization is added. No UNIX IDs higher than this number are assigned automatically and you cannot specifically enter numbers higher than this number. The maximum UNIX ID stays in place until you change it with the rgy_edit prop command.
[-**pa**[**ssword**] *default_password*]	Is the default password assigned to the accounts created by sec_create_db. If you do not specify a default password, -dce- is used. (Note that the hosts/local_host_name/principal_name.none.none, krbtgt/cell_name.none.none, and nobody.none.none accounts are not assigned the default password, but instead a randomly generated password.)
[-v[**erbose**]	Run in verbose mode and generate a verbose transcript of all activity.

Example of a sec_create_db Run

The following example shows the **sec_create_db** command run to create the master database and the information that **sec_create_db** displays as it runs. Note that because the **-k** option is not entered, **sec_create_db** prompts for the master key seed string. This string is not displayed as it is entered.

% sec_create_db -v -myname /.../dresden.com/sub-sys/dce/sec/master -master

```
Enter keyseed for initial database master key: <enter
up to 1024 characters>
SECD Checkpoint on Tue Sep 24 11:44:12 1991
.... saving rgy
.... saving acct
.... saving person
.... saving group
.... saving org
.... saving replicas
.... saving acl
End SECD Checkpoint on Tue Sep 24 11:44:13 1991
SECD Checkpoint on Tue Sep 24 11:44:15 1991
.... saving rgy
.... saving acct
.... saving person
.... saving group
.... saving org
.... saving acl
End SECD Checkpoint on Tue Sep 24 11:44:17 1991
```

The Results of sec_create_db

The master registry database created by **sec_create_db** contains the principals, groups, and organizations and the accounts listed in the following two tables.

Table 6 **Initial Persons, Groups, and Organizations**

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

Table 7 **Initial Accounts**

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

Some of the objects initially created by **sec_create_db** are reserved and cannot be deleted. These are listed below

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

When you run the **sec_create_db** command to create the master registry database, you can name the principal who has the most privileged access to the registry. This person is known as the "registry creator." If the registry creator you name is not one of the default principals, **sec_create_db** adds the account rgy_creator.none.none,

where rgy_creator is the principal you named as the registry creator. If you do not name a registry creator, **sec_create_db** assigns the most privileged registry access to the **root system none** account.

With one exception, all of the accounts created by the **sec_create_db** command are assigned randomly-generated passwords and are marked as invalid. Before these principals can log in to these accounts, you must use the **rgy_edit** command to change the account passwords and to mark the accounts as valid. Note that you can use the **rgy_editchange** subcommand **-rp** option to generate new random passwords. The exception is that the account created for the registry creator is valid and is assigned the DCE default password (-dce-). Change the default password to ensure the security of the registry creator account.

In addition to the group memberships implied by the accounts created by **sec_create_db**, the principals are also made members of the groups listed in the table titled "Group Memberships Created by **sec_create_db**."

Table 8 **Group memberships created by sec_create.db**

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

Starting the Master Replica

After SDCA or **dce_config** creates the master replica, it starts the master security server. To start the master replica (**secd**) explicitly, use the following steps:

1 Log in as **root** on the machine that will run the master replica.

Use **ps** to ensure that an **rpcd** is running on the machine. If one is not, start one. To do so, ensure you are root and enter:

/opt/dcelocal/bin/rpcd

Start the master replica by entering

/opt/dcelocal/bin/secd.

Populating the New Registry Database

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

Setting Policies and Properties

Use the **rgy_edit prop**, **po**, and **au** subcommands to view policies and properties and change them as desired, as described in the reference pages for those commands.

Adding Accounts

After a new registry database is created, it contains only the principals, groups, organizations, and accounts added as initial information by **sec_create_db**. Use **rgy_edit** to add any other names and accounts that your site requires. You can do this now or at any time later.

Creating Slave Replicas

After the master replica database has been created and started and its database has been populated, you run **SDCA** or **dce_config** at the slave sites to create the slave replicas and start them. To create and start a slave replica, SDCA or **dce_config** first ensures that the sites are running **rpcd**, **sec_clientd**, and the appropriate CDS servers. It then executes the following **sec_create_db** command:

/opt/dcelocal/bin/sec_create_db -slave -myname *my_server_name*

First the command creates a database for the new slave replica. The database consists of only stub files. The command then locates the master replica and adds the new slave to the master's replica list. The master marks the new replica for initialization. Finally SDCA or **dce_config** starts **secd** and ensures that it starts automatically each time the machine reboots.

The value for *my_server_name* is set by the environment variable SEC_REPLICA, which is set by default to the hostname of the system where the replica resides. If you wish to change the name of the security replica that is created by **dce_config** or SDCA, change the value of SEC_REPLICA in the file **/opt/dcelocal/etc/dce_com_env**. If you use **dce_config** to configure your cell, you may instead change the value of SEC_REPLICA in the shell environment from which **dce_config** is run.

You must run SDCA or **dce_config** at each machine on which you want to configure a slave replica.

Registry Permissions Required by Replicas

To initialize and function correctly, slave replicas must have **i, m,** and **I** permissions for the **replist** object (**/.:/sec/replist**). A slave server runs under the identity of the machine on which it runs. A machine's identity is the local host principal name in the form **host/***hostname***/self**.

The required ACL entry is added when the **dce_config** tool initially configures your cell's Security Server and when you use the tool to create new slave replicas. The entry has the form **user:host/***hostname***/self:imI**.

Because a master registry can later become a slave, the above entries are also added for master replicas.

Verifying the Replicas are Running

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

1 Invoke **sec_admin**

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

2 Issue the **lrep** command with the **-state** option to display all Security Servers and their status

```
sec_admin> lrep -state
Default replica:/.../giverny.com/subsys/dce/sec/master
Default cell:/.../giverny.com

subsys/dce/sec/mug
  State:                  in service - slave
  Last update time:       Tue Jun 22 14:39:57 1993
  Last update's seqno:    0.215
subsys/dce/sec/master (master)
```

```
State:                  in service - master
Last update time:       Tue Jun 22 14:39:57 1993
Last update's seqno:    0.215
```

Starting sec_clientd on Registry Client Machines

When you run **dce_config**, it starts **sec_clientd** on Security client machines. To start **sec_clientd** explicitly, use the following steps:

1 Log in as root on the client machine.

Use **ps** to ensure that an **rpcd** is running on the machine. If one is not, start one. To do so, ensure you are root and enter

/opt/dcelocal/bin/rpcd

Start **sec_clientd** by entering

/opt/dcelocal/bin/sec_clientd

Set up **sec_clientd** so that it starts automatically when the machine is rebooted.

Establishing Uniform UNIX IDs

If you share files with other systems that do not use the registry, ensure that names, UNIX IDs, and account information are consistent between the registry and the foreign system's **passwd** and **group** files. (For the purposes of this discussion, "file sharing" can take the form of direct access or indirect file transfer via media such as tar tapes.)

We provide a tool called **passwd_import** that helps you to identify and resolve conflicts of names, UNIX IDs, and account information. If you plan to share files between systems controlled by the registry and systems that are not, we recommend you run **passwd_import** now to minimize the number of changes you have to make. Typically,

you run **passwd_import** in a mode that adds IDs to the registry to match the IDs on the foreign systems; afterward, you run the **find** and **chown** commands to ensure that the IDs stored in the file systems match those stored in the registry. See the **passwd_import** reference page for details on how to run **passwd_import**.

Performing Routine Maintenance

This section describes Security maintenance procedures performed on a regular basis and the basic use of the **sec_admin** command, a command used for many replica maintenance tasks.

Using the sec_admin Command

The **sec_admin** command is a tool for replica administration. Most **sec_admin** subcommands are directed to a default replica. When **sec_admin** is invoked, it automatically binds to a replica in the local cell. This replica becomes the default replica.

You can use the site subcommand to change the default replica and, optionally, the default cell. When you use the **site** command, you can supply the name of a specific replica, or you can simply supply the name of a cell. If you supply a cell name, **sec_admin** binds to a replica in that cell randomly. If you supply a specific replica name, **sec_admin** binds to that replica.

The site subcommand format is: **site [name [-u[pdate]**

The **-u** option directs site to bind to the master replica in the cell specified by name.

Invoking sec_admin

When you invoke **sec_admin**, it displays the current default replica's full global name, the cell in which the replica exists, and the replica's state. Then it displays the sec_admin> prompt.

```
$sec_admin
Default replica:/…/dresden.com/subsys/dce/sec/music
Default cell:/…/dresden.com
sec_admin>
```

At the sec_admin> prompt, you can enter any of the **sec_admin** subcommands described in the *DCE Administrator's Reference* **sec_admin** reference page.

Changing the Default Replica and Cell

To change the default replica enter site command and the name of the new default replica. You can supply any of the following names:

- A cell name (for example, **/.../dresden.com**) - if you enter a cell name, the named cell becomes the default cell. The **sec_admin** command randomly chooses a replica to bind to in the named cell, and that replica becomes the default replica.
- The global name given to the replica when it was created (for example **/.../dresden.com/subsys/dce/sec/rs_server_250_2**) - A global name identifies a specific replica in a specific cell. That cell becomes the default cell and that replica the default replica.
- The replica's name as it appears on the replica list (that is, its cell-relative name, for example, **subsys/dce/sec/rs_server_250_2**) - That replica becomes the default replica and the cell in which the replica exists becomes the default cell.
- The network address of the host on which the replica is running (for example, **ncadg_ip_udp:15.22.144.248**) - The replica on that host becomes the default replica, and the cell in which the host exists becomes the default cell.

Automatic Binding to the Master

Some of the **sec_admin** subcommands can act only on the master replica and thus require binding to the master. If you execute a subcommand that acts only on the master and the master is not the default replica, **sec_admin** attempts to bind to the master replica in the current default cell automatically. If this attempt is successful, **sec_admin** displays a warning message informing you that the default replica has been changed to the master registry. The master

registry will then remain the default replica until you change it with the site subcommand. If the attempt to bind is not successful, **sec_admin** displays an error message, and the subcommand fails.

Displaying Replica Information

The info subcommand displays status information about the default replica. The subcommand format is: **info [-full]**

If you enter no options, **info** displays:

- The default replica's name and the name of the cell in which the replica exists.
- Whether the replica is a master or a slave.
- The replica's state. A given replica can be in only one of the following states at a time:
  - Uninitialized - The database is a stub database that has not been initialized by the master replica or another up-to-date replica.
  - Initializing - The replica is in the processes of being initialized by the master replica or another up-to-date replica.
  - In Service - The replica is available for use.
  - Saving Database - The replica is in the process of saving its database to disk.
  - Copying Database - The replica is in the process of initializing (copying its database to) another replica.
  - In Maintenance - The replica is unavailable for updates but will accept queries.
  - Changing Master Key - The replica is in the process of having its master key changed.
  - Closed - The replica is in the process of stopping.
  - Deleted - The replica is in the process of deleting itself.
- The date and time the replica was last updated and the update sequence number.

The **-full** option displays all the above information and the following information:

- The default replica's unique identifier.

- The replica's network addresses.
- The unique identifier of the cell's master replica.
- The master sequence number, which is the sequence number of the event that made the replica the master.
- The network addresses of the cell's master replica.
- If the replica is the master replica, the update sequence numbers that are still in the propagation queue and have yet to be propagated.

Changing the Master Replica

In HP DCE/9000 Version 1.2, the security server supports the **sec_admin change_master** command. This command is sent to the current master (old master) with an argument that identifies which slave replica is to become the new master.

When **sec_admin change_master** is invoked, the current master sends all pending updates and its propagation queue to the new master. The new master reads the current master's replica list to get extra information that is needed by the master to manage propagation to the slaves. When the new master has received all necessary information from the current master, it becomes the master and the current master becomes a slave.

The **change_master** command is the preferred method of selecting a new master; no information is lost when **change_master** is used.

The security server also supports the **sec_admin become -master** command. **become -master** forces the default replica to become the master. This new master will re-initialize all other replicas so that their databases will be consistent.

The **become -master** command should only be used when the old master has been destroyed. It is not recommended for use when the master is unreachable because of a network failure or because the server has temporarily gone down. The **become -master** command can cause data to be lost.

After issuing the **become -master** command the old master should be force-deleted from the replica list (via **sec_admin delrep -force**).

The **become -slave** command is not available in this release. Perform the following steps to convert an old master to a slave:

1 Stop **secd** if it is running.

2 **rm -f /opt/dcelocal/var/security/.mkey**
rm -rf /opt/dcelocal/var/security/rgy_data/

3 Reconfigure as slave replica.

Examples

The following examples illustrate the use of **change_master** and **become -master**:

```
sec_admin> change_master -to subsys/dce/sec/rep1
Do you wish to continue (y[es]) or abort this operation
(n[o])? y
sec_admin> lrep
subsys/dce/sec/master
subsys/dce/sec/rep1 (master)


sec_admin> become -master
Do you wish to continue (y[es]) or abort this operation
(n[o])? y
```

Changing the Registry Master Key

All passwords stored in a registry database are encrypted by a master key. (The master key is created when you create a registry database using **sec_create_db**). Using the **sec_admin master_key** subcommand, you can change the master key and re-encrypt all passwords using the new master key. Each replica (master and slave) maintains its own master key to access the data in its copy of the registry.

You should change each replica's master key on a regular basis. Before you run **sec_admin**, ensure you are logged in to an administrative account. Then, perform the following steps to change the master key on the default replica:

1 Invoke **sec_admin**

```
/opt/dcelocal/bin/sec_admin
Default replica:/…/giverny.com/subsys/dce/sec/art_server_1
Default cell:/…/giverny.com
sec_admin>
```

2 Enter the **master_key** subcommand

```
sec_admin> master_key
```

The **sec_admin** command changes the master key for the default replica and re-encrypts all passwords.

Checking Status of Propagation to the Slaves

Use the **sec_admin lrep -prop** command to check the status of the master's propagations to the slaves:

1 Invoke the **sec_admin** command:

```
$ /opt/dcelocal/bin/sec_admin
Default replica: /…/giverny.com/subsys/dce/sec/rep1
Default cell: /…/giverny.com
```

2 Bind to the master:

```
sec_admin> site /.: -u
Default replica: /…/giverny.com/subsys/dce/sec/master
Default cell: /…/giverny.com
```

3 Display the propagation management information that the master maintains for each replica. This information lists whether the master has a backlog of updates to send to a replica, the sequence number and timestamp of the last update the master successfully delivered to the replica, and the status of the master's last communication with the replica. Display the information as follows:

```
sec_admin> lrep -prop
Default replica: /.../giverny.com/subsys/dce/sec/master
Default cell: /.../giverny.com

subsys/dce/sec/master (master)

subsys/dce/sec/rep1
  Propagation state:          ready for updates
  Last update delivered:      Mon Jun 22 09:26:45 1993
  Number of outstanding updates:0
  Last comm status:           successful completion
sec_admin>
```

Checking Status of all Replicas

Use the **sec_admin lrep -all** command to check the health of all replicas, including propagation information:

1 Invoke the **sec_admin** command:

```
$ /opt/dcelocal/bin/sec_admin
Default replica: /.../giverny.com/subsys/dce/sec/rep1
Default cell: /.../giverny.com
```

2 .Bind to the master:

```
sec_admin> site /.: -u
Default replica: /.../giverny.com/subsys/dce/sec/master
Default cell: /.../giverny.com
```

3 Display information about the master and each replica. The **sec_admin lrep -all** command performs two functions:

- It reads the master's replica list to get the current propagation management information for each replica. This includes whether the master has a backlog of updates to send to a replica, the sequence number and timestamp of the last update the master successfully delivered to the replica, and the status of the master's last communication with the replica.
- It provides information about the state of each slave replica.

To display the information:

```
sec_admin> lrep -prop
Default replica: /.../giverny.com/subsys/dce/sec/master
Default cell: /.../giverny.com

subsys/dce/sec/master (master)
  Instance id: 77bc953c-5482-11cc-b316-080009352555
    Addresses:          ncadn_ip_tcp:15.22.49.84[]
                        ncadg_ip_udp:15.22.49.84[]
    State:              in service - master
  Last update received at:Tue Jun 22 09:42:48 1993
  Last update's seqno: 0.148

subsys/dce/sec/rep1
  Instance id: c5cb7790-5485-11cc-8220-08000932b6f8
    Addresses:          ncadn_ip_tcp:15.22.49.136[]
                        ncadg_ip_udp:15.22.49.136[]
    State:              in service - master
  Last update received at:Tue Jun 22 09:42:48 1993
  Last update's seqno: 0.148
  Propagation state:    ready for updates
  Last update delivered:Tue Jun 22 09:42:48 1993
  Last update's seqno: 0.148
  Number outstanding updates:0
  Last comm status:successful completion

sec_admin>
```

Note that during periods of heavy update activity discrepancies can occur between what the master reports about a replica and what the replica reports about itself. This is because the information is not gathered atomically. Discrepancies disappear when update activity stops.

NOTE In a mixed HP DCE 1.1-HP DCE 1.2 cell, if the master Security Server is HP DCE 1.2, a pre-HP DCE 1.2 **sec_admin lrep** will not be able to correctly display the states "becoming slave" and "duplicate master".

Truncating the Propagation Queue

Use the **sec_admin initrep** command to truncate the propagation queue when a replica has been unreachable for a long time and there is an accumulation of updates for delivery to the replica:

1 Invoke the **sec_admin** command:

```
$ /opt/dcelocal/bin/sec_admin
Default replica: /.../giverny.com/subsys/dce/sec/rep1
Default cell: /.../giverny.com
```

2 Bind to the master:

```
sec_admin> site /.: -u
Default replica: /.../giverny.com/subsys/dce/sec/master
Default cell: /.../giverny.com
```

3 Mark the replica for initialization. The master will oversee the replica's re-initialization when the replica becomes reachable. Mark the replica as follows:

```
sec_admin> initrep subsys/dce/sec/rep1
sec_admin>
```

Backing Up and Restoring the Registry Database

Because the Security Server maintains current data in memory and saves the data to disk only periodically, you must use the exact procedures described here to back up the registry database.

Only the master replica database and its master key file need to be backed up. Use the procedures described in this section when you back up the entire disk on which the master replica and its master key are stored and when you back up only the master's database files and its master key file.

Procedures to Backup the Registry Database

To run the backup procedures, ensure you are logged into the DCE via an administrative account. To back up the registry database, perform the following steps:

1 Invoke **sec_admin**

```
$ /opt/dcelocal/bin/sec_admin
Default replica:/.../giverny.com/subsys/dce/sec/art_server_1
Default cell:/.../giverny.com
sec_admin>
```

2 Ensure that the **sec_admin** default replica is the master. (The name of the default replica and whether it is the master or a slave is displayed by **sec_admin** when it is invoked.) If the master replica is not the default replica, use the **sec_admin** site command to make it so. For example in the cell **giverny.com** to make the master replica the default replica, enter:

```
sec_admin> site /.../giverny.com -u
```

The **-u** option specifies that **sec_admin** should bind to the master replica in the cell /.../giverny.com.

3 Put the master replica in the maintenance state

```
sec_admin> state -maintenance
```

Putting the master replica in a maintenance state causes the master to save its database to disk and refuse all updates.

4 Backup the master registry by backing up either the entire volume or the **dcelocal/var/security/rgy_data** tree (the registry database) and the **dcelocal/var/security/.mkey** file (the file that contains the

master key used to encrypt all keys in the registry database). Note that because the **dcelocal/var/security/.mkey** file contains the master key, restoring a backup of the registry database is useless unless the **dcelocal/var/security/.mkey** file is also restored.

The exact commands used for the backup are a matter of personal preference. However, if you write both the database and the master key file to the same tape, store the tape in a locked area with restricted access. Alternatively, you can write the database and the key file to separate tapes and store each tape in a different location.

1 When the backup completes, take the master replica out of maintenance state

```
sec_admin> state -service
```

The server resumes accepting updates.

Procedures to Restore the Registry Database

This section describes how to restore the master replica's database files and its master key file. These procedures assume that the database is being restored to the same machine from which it was backed up.

To restore the registry database, perform the following steps:

1 Log in as **root** at the master registry site.

2 If **secd** is running, stop it.

3 Copy the backup up files from the backup media to the machine. If you have backed up only the registry datafiles and the master key files, be sure to copy the registry database to the **dcelocal/var/security/rgy_data** tree and the master key file to **dcelocal/var/security/.mkey**. Note that because the **dcelocal/var/security/.mkey** file contains the master key, restoring a backup of the registry database is useless unless the **dcelocal/var/security/.mkey** file is also restored.

4 Restart the server by invoking **secd** with the **-restore_master** op-

tion. This command will start **secd** and cause the master to mark all slaves to be re-initialized.

/opt/dcelocal/bin/secd -restore -master

5 Verify that **secd** starts automatically at system startup.

NOTE If you restore only a master key file and do not change the master key, you can simply copy the master key file from the backup media without performing the other steps in the restore procedures.

Performing Network Reconfigurations

The information in this section describes only the differences between the corresponding chapter of the *OSF DCE Administration Guide – Core Services* and the current HP DCE/9000 release.

Removing a Server Machine from the Network

If you are planning to remove a machine that runs a slave replica from the network or to shut it down for an extended period, delete the replica at that site as follows:

1 Invoke **sec_admin**.

2 Issue the **sec_admin delrep** subcommand to bind the master replica in the current cell, if necessary, and instruct the master replica to delete the slave. The master will send a delete request to the slave.

```
sec_admin> delrep subsys/sec/server_250_1
```

3 Issue the **sec_admin lrep** command to the master to verify the slave is deleted. This command lists replicas on the master's replica list. When the master receives the request to delete the slave, the slave appears on the replica list as marked for deletion.

```
sec_admin> lrep
subsys/dce/sec/master
subsys/sec/server_250_1 (marked for deletion)
subsys/sec/server_250_2
```

4 When the replica has actually been deleted, it no longer appears on the list.

```
sec_admin> lrep
subsys/dce/sec/master
subsys/sec/server_250_2
```

Upon successful completion of the **sec_admin** delete request, the master does the following:

- Marks the replica as deleted.
- Propagates the deletion to all replicas on its replica list.
- Delivers the delete request to the replica.
- Removes the replica from its replica list.

Moving a Master Registry

A master registry can be moved to another node (the target) via **sec_admin change_master**. If the master registry is unavailable, a security slave can be converted to a master via **sec_admin become -master** on the target slave node. See *Changing the Master Replica* on page 28 of this chapter or the **sec_admin**(8) man page for information about these commands.

If you wish to move the master registry to a target node that is not configured as a security slave (i.e. a DCE client system), the target must first be configured as a security slave via **dce_config** or SDCC. Note that the master security server must be available in order to convert a DCE client system to a slave security server.

If the master **secd** is unavailable and you wish to move the master registry to a DCE client system, you must perform the following procedure. This procedure should be used only if circumstances prevent the master system from being reliable and/or available.

1 If you have a backup copy of the master registry database, restore the backup to the client node and proceed with step 6. Otherwise, proceed with the next step.

2 On the current master system, change the permission of the following

server node files to 644 so they can be copied to the client node:

/opt/dcelocal/var/security/.mkey
/opt/dcelocal/var/security/rgy_data/*

DO NOT use **chmod -R 644 /opt/dcelocal/var/security/** because it changes the permissions of data files that must not be changed.

3 Create the following directory on the client node and change its permission to 755:

/opt/dcelocal/var/security/rgy_data

4 Copy the following server files to the client node:

/opt/dcelocal/var/security/.mkey/opt/dcelocal/var/security/rgy_data/*

5 Restore the permissions to 600 on the following client files:

/opt/dcelocal/var/security/.mkey/opt/dcelocal/var/security/rgy_data/*

6 Update the server's entry in the client node's **/opt/dcelocal/etc/security/pe_site** file to reflect the client's (new master's) network address. Once the file is changed, copy the results to the old master (old server) node. The following is an example **pe_site** (the network address is 15.21.249.14):

```
/.../gamera 56568234-6e4c-11cc-80e808000935293c\
     @ncacn_ip_tcp:15.21.249.14[]
```

Get the client node's network address via either **nslookup** *client_node_name* or **netstat -in** at the client node.

7 Start **secd** on the client node. If, while starting **secd**, you receive the error message:

```
Registry: Fatal Error - Cannot establish DCE registry
identity...Registry Server Unavailable
```

then restart **secd**. The client node will become the new master. If you used a backup tape to restore the database, you must start **secd** with the **-restore_master** option. This option reinitializes all slave repli-

cas during the master restore. Allow five minutes for **secd** to complete initialization, or if you use the **-v** option, until the following message displays during output when **secd** is re-registering itself:

```
SECD Exporting bindings to /…/gamera/subsys/dce/sec/master
```

8 Change the **pe_site** on any other nodes in the cell to reflect the network address of the new master.

9 Kill **sec_clientd** and restart it on every node.

Changing the Network Address of a Machine Running secd

The network address of a machine can change. For example, replacing an ethernet card can change the machine's network address. A network address change can occur:

- Either on a master server or on a slave server
- Simultaneously on a master server and a slave server

Network address change occurs on master or slave server

During server initialization, the security server (master or slave) can detect address changes and can perform the necessary updates to the master's replica list and to the cell namespace. However, the security server does not automatically update the machine's **/opt/dcelocal/etc/security/pe_site** file. This file is required for binding by the security service to itself.

Therefore, after a machine's address has changed and before restarting **secd**, it is necessary to edit the **pe_site** file by modifying entries that contain the old address to use the new address. If the master's address changed, the **pe_site** file of every node in the cell (including the master) must be changed to reflect the new address. If a slave's address changed, that slave's **pe_site** file must be changed.

Network address change occurs simultaneously on master and slave server

A master and slave(s) will not be able to reach each other if the master is trying to notify the slaves of it's address change while a slave is trying to notify the master of the slave's address change. To avoid this problem, make sure the address change of one server (either master or slave) is propagated to all servers before the address of another server is changed.

After the machine's address has been changed, restart **secd** on that machine. Use the **sec_admin** command to monitor the propagation of the address change. Use the **sec_admin site** to bind to a site whose replica list you want to check for the new address. Use **sec_admin lrep -addr** to view that site's copy of the addresses on the replica list. When the new address is displayed, use **sec_admin site** again to bind to the next replica you want to verify and perform the **lrep -addr** again. When you have verified that both the master and slave receiving address changes have been updated with the first address change, it is safe to proceed with the next network address change.

If you are unable to prevent simultaneous network address changes by the master and a slave, the only way to restore communication between the master and slave is to delete the slave, then recreate it.

Delete the slave using one of the following methods, depending on your circumstances:

- If you anticipate a simultaneous address change, while the master and slave are still communicating, delete the replica by first binding to the master then deleting the slave:

```
sec_admin> site /.:/subsys/dce/sec/master
sec_admin> delrep subsys/dce/sec/slave_name
```

- If the master and slave **secd** processes are still running but are not communicating (due to simultaneous address changes or another reason), then bind to the slave and destroy it, and bind to master and remove the replica list entry for the slave:

```
sec_admin> site /.:/subsys/dce/sec/slave_name
sec_admin> destroy subsys/dce/sec/slave_name
```

```
sec_admin> site /.:/subsys/dce/sec master
sec_admin> delrep subsys/dce/sec/slave_name-force
```

- If the slave **secd** is not running or if you are unable to bind to the slave site using **sec_admin**, then manually delete the slave and the entry for the slave on the master's replica list:

  On the slave machine, kill **secd** if it is still running, then run:

  ```
  rm -f /opt/dcelocal/var/security/.mkeyrm -rf /opt/
       dcelocal/var/security/rgy_data/

  rpccp> show group /.:/sec
  rpccp> remove entry /.:/subsys/dce/sec/
       replica_name_to_be_removed
  rpccp> remove member /.:/sec -m/.:/subsys/dce/sec/
       replica_name_to_be_removed
  ```

  On any DCE client machine, bind to the master and remove the slave's entry:

  ```
  sec_admin> site /.:/subsys/dce/sec/master
  sec_admin> delrep subsys/dce/sec/slave_name -force
  ```

  After deleting the slave and changes to the network address have been made, recreate the slave using **dce_config**. DO NOT use SAM because it will not recognize that the slave was deleted. Therefore SAM may not allow reconfiguration of the same slave.

Troubleshooting and Recovery Procedures

The **secd -locksmith** option starts **secd** in locksmith mode. Use this option only on the master replica.

If the master replica loses communication with a slave replica for a long period of time, and the propagation queue becomes too long, use the **sec_admin** command to have the master reinitialize the slave by giving it a fresh copy of the entire database when communication is restored. You can explicitly initialize a slave replica's database using the **sec_admininitrep** subcommand. (See the **sec_admin** reference page for details.)

Steps for Restarting a Security Server in Locksmith Mode

Perform the steps on the master replica's node. Step 1 in the *OSF DCE Administration Guide* has changed. The modified step 1 is:

1 Shut down the security server.

- If you cannot log in with administrative privileges and access the **sec_admin** command to shut down the server, log in as root on the machine on which the server is running and kill the Security server process.
- If you are able to log in with administrative privileges, use the **sec_admin** command to shut down the security server.

Follow the remaining steps in the Administration Guide.

Forcibly Deleting a Slave Replica

The **delrep -force** subcommand deletes the slave replica from the master's replica list. The master then propagates the delete request to the other replicas. Since this operation never communicates with the deleted replica, use the **-force** option only when the replica dies and cannot be restarted. If a forcibly deleted replica continues operation, use the **sec_admin destroy** subcommand to stop the server and delete its database or simply stop **secd** and delete or rename its database.

Use the following steps to forcibly delete a registry replica:

1 Invoke **sec_admin**.

```
/opt/dcelocal/bin/sec_admin
Default replica:/.../giverny.com/subsys/dce/sec/art_server_2
Default cell:/.../giverny.com
sec_admin>
```

2 Use the **delrep** subcommand with the **-force** option to delete the replica. The following example shows the replica deleted from **/.../giverny.com/dce/subsys/dce/sec/lit_server_2**:

```
sec_admin> delrep subsys/dce/sec/lit_server_2 -force
```

If the default replica is not the master, **sec_admin** automatically binds to the master.

3 Use the **site** subcommand to determine if the deleted replica is still in operation.

4 If the replica is in operation, you can use the **destroy** subcommand to stop the replica and destroy its database. First use the **site** command to set the default replica to the replica to be destroyed.

```
sec_admin>   site subsys/dce/sec/lit_server_2
Default replica:/.../giverny.com/subsys/dce/sec/lit_server_2
Default cell:/.../giverny.com
```

5 Use the **destroy** subcommand to stop the replica and delete its database. When you use the **destroy** subcommand, you must enter the name of the replica you want to stop. The replica you specify must be the same as the current default replica to confirm the deletion.

```
sec_admin>    destroy subsys/dce/sec/lit_server_2
sec_admin>
```

Alternatively, you can destroy the replica by deleting or renaming its database.

7

Notes on Cell Administration

Notes on Cell Administration

This chapter contains an overview of the diagnostic tools and administrative interfaces that are available in HP DCE/9000. In addition, it contains notes about other topics concerning cell administration.

Diagnostic Tools

The HP DCE/9000 release includes a group of HP-developed diagnostic tools. These tools provide information on the status of a client machine within its cell. New functionality has been added to each of these tools since the previous release of HP DCE/9000.

The following is a brief description of the HP DCE diagnostic tools:

- **dcewhich** displays the location of the DCE services in a cell.
- **dceping** verifies that a local client can communicate with DCE and other services within a cell. You may specify services that you want **dceping** to contact by modifying the system-wide file **/opt/dcelocal/hpadmin/etc/nondcesvc**, or the per-user file **$HOME/.nondcesvc**. (See the man page **nondcesvc**(4)). You may either list the names of the services in these files or list the name of an executable that **dceping** would run to determine the names of the services to ping. In addition, you may embed, in the service name, environment variables which are expanded with their value at the time dceping is run. If a variable is not in the current environment, **dceping** does not attempt to contact the corresponding service.

  dceping may also be used to ping services on a platform different from HP or in a different cell (in this case proper cross-cell communication path must have been previously setup). As long as you specify the service's name in the right format (as specified in **nondcesvc**(4)), **dceping** will contact these services.
- **dceval** runs a series of tests that verify whether or not a local client can participate in a cell. It validates installation, configuration, and connectivity of a DCE client to the core DCE Services.

  dceval can be extended to validate applications different from the core DCE. It is expected that vendors that develop applications on top of DCE would extend **dceval** to validate their applications. Therefore, depending on which DCE related products installed on your machine have extended **dceval** for their applications, **dceval** would validate the core DCE and such applications.
- **camera** is a diagnostic tool that takes a snapshot of the hardware and

software configuration of a local machine. This snapshot is a collection of information about the current state of the machine's operating system, network, and distributed environment. The data in a snapshot is stored as a **shar** file for easy email transfer. Once sent to the support engineer, the data is then unpacked and used for analysis in problem determination. Camera can be tailored to run all or some of the diagnostic scripts supplied by listing the scripts to run in the **camera** description file, **/opt/dcelocal/hpcamera/etc/snapshot.des**. **camera** is extensible in that one can write a custom set of diagnostic data collection scripts and enable them in the description file. See the man page **snapshot.des**(4) for details.

A limitation of the present release is that you can no longer invoke **dceval** and **camera** from the System Administration Manager (SAM) interface. **dceval** and **camera** were available through the SAM interface in the earlier HP DCE releases.

For additional details and command-line syntax, see the manpages **dcewhich**(8), **dceping**(8), **dceval**(8), and **camera**(8).

NOTE Before using **camera**, you should log in to DCE (via **dce_login**) as the DCE cell administrator.

Enhanced CDS Browser

HP DCE/9000 supplies an enhanced version of the CDS Browser. The CDS Browser is a tool for viewing and editing the contents of a namespace. It runs on workstations with windowing software based on the OSF/Motif user interface.

The HP DCE/9000 CDS Browser provides a superset of the functionality available in the OSF-supplied CDS Browser. Documentation for the product is provided in the form of context-sensitive online help.

NOTE The OSF DCE User's Guide describes the OSF version of the CDS Browser. The HP CDS Browser provides more functionality, different icons, and online help.

Features of the HP DCE/9000 CDS Browser

At HP DCE/9000 Version 1.2, the system of HP CDS Browser menus have been reorganized,the CDS Browser icons have been redesigned, additional functionality has been added, and features that aid localization have been included.

The following standard (OSF DCE) features for viewing the structure and contents of a namespace enable you to

- display the namespace
- expand and collapse selected directories
- filter the namespace display
- navigate the namespace

Additional features available with the HP DCE/9000 CDS Browser enable you to manage and control the components of the CDS and the contents of the namespace. The HP CDS Browser provides the functionality of **cdscp** (**cds** control program), the **acl_edit** program for CDS objects, and some of the capabilities of **rpccp** (**rpc** control program), including **create**, **show**, and **export bindings**. With the HP DCE/9000 Version 1.2 CDS Browser, you can

- create, delete, and edit namespace entries
- view attributes of namespace entries
- view and edit ACL permissions of namespace entries
- view and set CDS Browser options
- manage replica locations
- log in to DCE

Overview of Enhanced Features

Creating and Deleting Entries

Menu options enable you to create and delete clearinghouse entries, directories, object entries, softlinks, RPC entries, RPC group entries, RPC profile entries, and RPC server entries.

The menu prompts for appropriate information for creation and deletion tasks and requires confirmation before deletions are performed.

Showing CDS Entry Attributes

Menu options enable you to display an attribute list and list the attributes for a specified entry.

Editing CDS ACL Entries

Menu options allow you to control user access to the following CDS components:

- clearinghouses
- directories
- object entries
- soft links

You can view, edit, or delete CDS permissions on specified components. The CDS permissions are read, write, insert, delete, test, control, and administer.

Editing DCE Options

Menu options enable you to display and set the following CDS options:

- Use of cache data
- Authenticated/unauthenticated access
- Trust of all servers
- Data confidence level
- Communication timeout limit
- Cache data timeout limit

You can also set defaults for these options, and can toggle confirmation of non-destructive dialogs.

Manage Replica Locations

You can create a replica of a directory, change the location of a master replica, display information about a replica, and delete a replica from a clearinghouse.

Log in to DCE

You can log in to DCE, either as yourself or as another user, when you need authentication to perform actions. If you lose authentication during an HP CDS Browser session, you can log in to DCE without exiting the browser.

User Interface Enhancements

Icons

When you start the Browser, an icon representing the root directory is the first item to be displayed in the window. Directories, softlinks, and object entries all have distinct icons associated with them. For HP DCE/9000 Version 1.2 , the icons have been redesigned. The icons are described in the CDS Browser online help in the Online Reference topic under the heading "HP CDS Browser Icons".

For information about how the icons were created and how they can be modified,see the **cdsbrowser**(8) reference page.

Default Action on Double Clicking

The HP DCE/9000 CDS Browser provides additional "default" actions for double clicking on CDS entries. For example, double clicking on group or profile entries causes the group or profile editor to appear; double clicking on an object, **rpc_entry**, or softlink entry accesses the Attribute List window. Double clicking on a directory entry expands or collapses the directory.

CDS Browser Documentation

CDS Browser Online Help

Access to the documentation is available through the **Help** option in the CDS Browser menu bar and **Help** buttons in the CDS browser dialog boxes. The CDS Browser online help is also available from the VUE Front Panel help icon (the "**?** "). To access the DCE Online Help from the VUE Front Panel,

1 Click on the Front Panel's help icon (the "**?** "). A "Welcome to Help Manager" help window appears.

2 In the Help Manager window, click on the "HP DCE/9000, Version 1.2" product-family title. A list of the HP/DCE 9000 help volumes appears.

3 Click on **Using the HP CDS Browser**.

CDS Browser Reference Page

HP CDS Browser now supports X resources that permit you to customize or localize the HP CDS Browser. These attributes are described the **cdsbrowser**(8) reference page.

cdsbrowser(8) also contains information about the message catalog, icons, online help, the extent to which the HP CDS Browser can be localized, login security, and privilege required to perform various actions with the browser.

Administering CDS

This section contains information on administering CDS that is supplements the information in the *OSF DCE Administration Guide – Core Services* and *OSF DCE Administration Reference*.

Deleting a Clearinghouse

Before performing a **cdscp delete clearinghouse** command on a **cds** server machine, you must move or delete any directory master replicas that are contained in the clearinghouse. If the clearinghouse contains any directory master replicas, a **cdscp delete clearinghouse** command will fail with the error message **entry does not exist**.

The **cdscp show clearinghouse** command shows which directory replicas (both master and read-only) are contained within a particular clearinghouse. The **cdscp show directory** command shows whether the directory replica in a particular clearinghouse is a master or read-only copy. Only master replicas will cause this error.

Skulking Directories

CDS propagates updated namespace information among all directory replicas with periodic automatic skulks so that consistent information is available throughout the namespace. To conserve network bandwidth, these automatic skulks take place only every few hours.

Manual changes to the namespace should always be accompanied by manual skulks to immediately propagate these changes and additions. This will avoid errors (such as **entry not found**) which can arise when clients access directory replicas which have not yet received updates for recently changed objects.

Immediately after you create or delete a clearinghouse, you should skulk the root directory. Immediately after you create or delete a directory, object, or link, you should skulk the parent directory. Similarly, immediately after you create or delete a read-only replica of a directory, you should skulk that directory.

Note that skulks can take a few minutes to reach all parts of a cell, so do not expect instant availability of updated information.

Known CDS Problems in HP DCE 1.2

Out-of-Swap Problems

CDS can fail if a CDS server or client system runs out of swap space. Symptoms may include error messages such as "Requested operation would result in lost connectivity to root directory", and **cdsadv** crashes with client cache corruption.

Swap space should be one of the first suspects in CDS troubles. If a CDS problem is linked to a possible shortage of swap space, free or configure more swap space, and then follow the CDS Restart Procedure below to bring the node back on-line in the cell.

Corrupted Client Cache

On some occasions following a reboot, crash, or power outage, CDS will fail to recover and restart successfully. Symptoms will include error messages such as **entry not found** with an empty client cache, or repeated **cdsclerk** crashes with client cache corruption. If you find a cleared or corrupted cache after a system reboot, follow the CDS Restart Procedure below to bring the node back on-line in the cell.

CDS Restart Procedure

To restart CDS, do the following as **root** and **cell_admin**:

1 Invoke the CDS control program

```
$ cdscp
```

2 Stop CDS server process if present

```
cdscp> disable server
```

3 Stop CDS client processes

```
cdscp> disable clerk
```

4 Exit the CDS control program

```
cdscp> exit
```

5 Delete the client cache

```
$ rm /opt/dcelocal/var/adm/directory/cds/cds_cache.*
```

6 Restart CDS client processes

```
$ cdsadv
```

7 Restart CDS server process if it was present

```
$ cdsd
```

8 Issue "cdscp define cached server <server_node_name> tower \ <server_protocol (ncacn_ip_tcp or \ ncadg_ip_udp)>:<server_ip_address>" command to provide the address of a CDS server

```
$ cdscp define cached server server_15 tower\
ncadg_ip_udp:11.22.33.44
```

You may ignore any "Cached Server clearinghouse already exists" errors.

9 Verify proper operation

```
$ cdscp show dir /.:
```

This should yield at least 20 lines of detailed output.

Establishing Intercell Communication

The information in this section supplements the information in the *OSF DCE Administration Guide – Core Services*, and describes how intercell communication should be configured in an HP-UX environment.

Communication between DCE cells is facilitated by the **gdad** daemon, which implements the Global Directory Agent (GDA). When a client in a local cell wants to access another cell that the local cell does not already recognize, the request is passed to **gdad**, which looks up and returns information about how to find the remote cell. This information is cached, so that **gdad** is not asked repeatedly for the same information.

gdad finds information about the remote cell by querying a Domain Name Service (DNS) database. DNS is not part of DCE; it is a widely-used distributed naming service, implemented on HP-UX by the **named** daemon, and documented in **named**(1M) and in Internet RFCs 1032, 1033, 1034, and 1035. **gdad** can also query GDS, which is a separately-priced option with HP DCE/9000 Version 1.2.

These procedures describe configuring GDA so that it can find the DNS server or servers where cell information is stored, creating DNS "resource records" that describe the cells you want GDA to be able to locate, and establishing peer-to-peer trust between two cells.

Specifying DNS Servers that GDA Should Query

GDA must be told which DNS nameservers (i.e., instances of **named**) to query for information about foreign cells. The nameserver at localhost is usually preferred, as only localhost provides recursive

query service—if localhost doesn't have the requested data, localhost will query other nameservers until it either finds the requested data or exhausts the list of nameservers that it knows about.

Using localhost reduces the requirement to keep GDA informed when nameserver configurations change, and allows GDA to always receive a response with a single query. In some environments, however, you may want to point GDA at a non-local server or servers, rather than at localhost.

gdad uses the following algorithm to identify which nameserver or nameservers to query:

1 gdad first reads the file **/opt/dcelocal/etc/named.ca**, which, if present, should contain one or more NS (NameServer) records and associated A (Address) records. These records specify, in DNS "master" format, the nameserver(s) that **gdad** should query. Master format is described in **named**(1M).

2 If **named.ca** is not found or does not contain NS records, then **gdad** looks for nameservers in **/etc/resolv.conf**. The format of **resolv.conf** is described in **resolver**(4).

3 If neither **/opt/dcelocal/etc/named.ca** nor **/etc/resolv.conf** exists, or if neither file contains nameserver information, then **gdad** defaults to localhost. Note that if **gdad** defaults to localhost, **named** must be running on the local machine.

If the GDA configuration information is changed, **gdad** must be stopped and restarted so that it will pick up the new configuration data.

Choosing DNS Servers for GDA to query

When choosing DNS Servers for GDA to query, be aware that GDA is not sophisticated enough to obtain part of the needed data from one nameserver and part of the data from another nameserver. The needed data consists of resource records associated with a cell's domain name and resource records associated with the domain name(s) of the host(s) on which a cell's CDS servers are running. GDA must be able to obtain all of this information from a single nameserver.

For example, a CDS server for a cell named "cell.cells.xyz.com" could be running on a machine called "machine.xyz.com ". If **gdad** cannot find at least one nameserver that can answer queries for both "cell.cells.xyz.com" and "machine.xyz.com ", it will not be able to obtain a single response containing all needed data.

To ensure that a given nameserver will be able to provide all needed data, be sure that either:

- Cell names and host names are part of the same DNS "zone" (database); or,
- If cell names and host names are in different zones, a nameserver must be configured such that it is a server for both zones. (It does not matter whether the server is a primary server, secondary server, or both, as long as both zones are available).

In some cases it may be sufficient to point GDA at a nameserver that serves the zone containing cell names, and obtain hostname A (Address) records from that server's cache data. If the nameserver is frequently used to look up hostnames, it is likely that A records for "popular" hosts will be in cache. However, it is generally unwise to rely on a particular resource record being found in cache — this is **not** a recommended or supported configuration.

Creating DNS resource records for a DCE cell

Each cell that is to be accessed via GDA must have certain information about the cell's CDS server(s) stored in DNS. DNS is a distributed, hierarchical database that stores information as one or more "resource records" associated with a particular domain name. The DNS resource records are added to the DNS database, and make the cell visible to GDA.

NOTE

Creating and maintaining DNS databases is a complex task that is beyond the scope of these release notes. The DNS resource record(s) for your cell must be added to the DNS database by your local DNS administrator, or by a person familiar with DNS and **named**.

The example in this section uses "absolute" (dot terminated) domain names. This syntax, although verbose, always works. DNS also allows names to be specified relative to the "current domain," which is context-dependent. Contact your DNS administrator before using relative names.

To establish a DNS resource record for a cell, do the following:

1 dce_login as the cell administrator for the cell you want to create records for:

dce_login cell_admin *<cell_admin_passwd>*

2 Run the **cdscp show cell** command. For example:

cdscp show cell /.../cell.xyz.com as dns

```
SHOW
CELL /.../cell.xyz.com
AT 1993-01-15-17:15:15 TXT 1 EE527190-F153-11CB-9CE3-
00000912C483 \
Master /.../cell.xyz.com/hostname_ch \
 ECF7E0FA-F153-11CB-9CE3-00000912C483
```

There may be more than one TXT record for a cell; each clearinghouse in the cell has its own TXT record. Each TXT record appears on a single line (without the slashes that appear in this example).

3 For each TXT record in the output of show cell, create a line in a text file similar to:

cell.xyz.com. IN TXT *"TXT_data hostname.xyz.com"*

TXT_data is the TXT data from **cdscp show cell** (note that this data must be entered on a single line), and *hostname.xyz.com* is the full domain name of the CDS server system that maintains that clearinghouse. The quotation marks are literal, and the absolute name of the host must be used (in this case) without the trailing dot.

4 In the same text file, create a line for each different *host-*

name.xyz.com. that you have added to the TXT records. For example:

cell.xyz.com. IN MX 1 *hostname.xyz.com.*

5 Add these records to your DNS database, or give these records to your DNS administrator.

Establishing peer-to-peer trust

Peer-to-peer trust means that a principal from one cell is trusted by another cell, in that the second cell trusts that the first cell has authenticated the identity of that principal. Use the following procedure to enable peer-to-peer trust between cells.

1 Check that both cells are running **gdad**, and that the DNS resource records for both cells are in the DNS database.

2 dce_login as cell administrator to one of the two cells.

3 Use the **rgy_edit cell** command:

rgy_edit=> **cell /.../<*cell_name*>**
Enter group name of the local account for the foreign cell: **none**
Enter group name of the foreign account for the local cell: **none**
Enter org name fo the local account for the foreign cell: **none**
Enter org name of the foreign account for the local cell: **none**
Enter your password: <*local_cell_admin_passwd*>
Enter account id to log into foreign cell with: **cell_admin**
Enter password for foreign account: <*foreign_cell_admin_passwd*>
Enter expiration date [yy/mm/dd or 'none']: (none) <RETURN>
Principals and Accounts have been created rgy_edit=>

DTS Documentation Discrepancies

Discrepancies in the OSF DCE 1.0.2 dtscp man pages

Hewlett-Packard has discovered the following discrepancies between the documention for **dtscp** (in the online OSF DCE man pages) and the actual behavior of the **dtscp** interface.

The man pages incorrectly specify the following:

- that the advertisement interval is given in the **show all characteristics** command.
- that local servers are given in the **show all characteristics** command.
- that current time, local servers, and global servers are given in the **show all status** command.
- the **show local time differential factor** command is specified as **show time differential factor.**
- the **show server times not intersecting** command is specified as **show faulty servers detected.**
- the **show local times not intersecting** command is specified as **show local faults detected.**
- the **show time representation mismatches detected** command is specified as **show time representation version mismatches detected.**
- the **show invalid messages detected** command is not valid.

Discrepancies in the OSF DCE 1.0.2 dtscp help text

Hewlett-Packard has discovered several discrepancies between the **dtscp** help text and the actual behavior of the **dtscp** interface. The **dtscp** help text does not specify the following commands:

- **show automatic tdf change**
- **show clock resolution**
- **next tdf change**
- **show time provider present**

Miscellaneous Notes

This section contains miscellaneous information about this release.

- The DTS adjust time daemon is called **dtstimed**. This name prevents a potential conflict with the (nonDTS) **adjtimed** daemon used by NTP and TIMED.
- To better integrate HP DCE with existing HP-UX systems, HP has added new functionality to the **passwd_export** utility. Before exporting groups from the DCE registry to the **/etc/group** file, HP **passwd_export** looks for the file **/opt/dcelocal/etc/sys.group** and prepends any group information from that file to the new **/etc/group** file. This allows an administrator to effectively override group information from the network registry on the local system. Because existing HP-UX groups conflict with the groups defined by the DCE architecture, HP has supplied a template file, **/opt/dcelocal/etc/sys.group,** that is installed on every HP-UX system when DCE is configured. This ensures that the **/etc/group** file created by **passwd_export** will have the correct group IDs for the groups that HP-UX software relies on. For example, bin::2 will be prepended to the new group file from the template file before bin::3 is exported from the DCE registry to the group file. Existing HP-UX utilities that expect **bin** to be group ID 2, will then find the correct entry first in the **/etc/group** file.
- The UUID-generation facility needs to open and read **/dev/lan0** in order to obtain the local host's IEEE 802 address (which is used to generate UUIDs). HP's DCE configuration tools ensure that **/dev/lan0** is world-readable. However, if you update the filesets **UX-CORE** or **LAN** after installing and configuring HP DCE, you should verify that **/dev/lan0** is readable by world.

8

Planning and Configuring the Distributed File Service (DFS)

Planning and Configuring the Distributed File Service (DFS)

The OSF Distributed File Service (DFS) is a distributed client/server application that provides, through the DCE, access to files and directories across machine boundaries. Information about configuring DFS is included in this document and in the *OSF DCE Administration Guide – Extended Services*, which is included with this release.

The Distributed File Service (DFS) is a separately-priced option with HP DCE/9000 Version 1.2.

About the Distributed File Service (DFS)

Hardware and Software Requirements

In addition to the requirements listed in Chapter 3, DFS has the following system requirement:

Kernel Configuration

The HP-UX kernel parameter **bufpages** should be set to 10% of available system memory. Since bufpages is set in units of 4K pages, the formula for its value is

bufpages = (system memory (bytes) x 0.10) / 4096.

For a system with 32 MB of memory, this becomes:

bufpages = (32 MB x 0.10) / 4096

= 819.2

=~ 819

Notes, Cautions and Warnings for DFS

- When you install the DFS-KERN fileset, the HP-UX kernel will be rebuilt and the system will be rebooted. This will happen automatically when **/etc/update** is run. You need only install the DFS-KERN fileset once, even if you re-install HP DCE/9000 Version 1.2.
- While it is possible to configure your DFS client as having its local cache memory resident, this is not recommended. It is more efficient to configure disk based cache, and let the local file system maintain this resource.

When selecting the size of disk cache, the default of 10000 will create a 10 MB cache. Better performance may be realized by using a disk cache of 50 to 100 MB, especially for frequent access of many files by multiple users.

- **dce_config** and the SDCC tool cannot successfully stop DFS daemons. To stop DFS, you must comment out the invocation of **/etc/rc.dfs** from **/etc/rc.dce** (or comment out the invocation of **/etc/rc.dce** from **/etc/rc**, if you wish to stop DCE entirely), and reboot the system.
- Care must be taken when choosing pathname arguments to the HP-UX **mkdir -p** command, which tries to create each directory in the path you specify. Thus:

  ```
  mkdir -p /.../xyz.abc.com/fs/users/kk/foo
  ```

  will fail because nothing can be created in the CDS part of the namespace (/... and /.../xyz.abc.com). Note that in most installations "/:" is a link to "/.../xyz.abc.com/fs", and that the following command will work:

  ```
  mkdir -p /:/users/kk/foo
  ```

  because the first directory "mkdir -p" tries to create is "users", which should succeed (assuming the correct UNIX permissions).
- The DFS namespace is visible to HP-UX file system commands such as **cd** and **ls**. However, the global cell namespace only becomes visible as names are used on the system. For example,

  ```
  ls /...
  ```

  will not show any sub-directories the first time it is used. However, doing:

  ```
  ls /.../mycell
  ```

  (where "mycell" is a cellname) followed by:

  ```
  ls /...
  ```

  will show "mycell". These names are cached by DFS until the node is rebooted. Note that although you can use some commands (such as **cd** and **ls**) to look at this part of the namespace, you cannot make any changes to it (e.g., via **mkdir** or **rm**).

- DFS requires the User Datagram Protocol of the Internet Protocol suite (UDP/IP). DFS will not function across an IP router which filters out UDP traffic. Nearly all IP routers are configured to permit UDP traffic, so this restriction will not pose a problem for most sites.
- DFS on HP DCE/9000 Version 1.2 does not support the LFS (Episode) file system. Only UFS is supported.
- HP DCE/9000 Version 1.2 is not supported on Hewlett-Packard Multi-Processor (MP) systems.
- Certain fileset operations in DFS (**fts dump**, **fts restore,** and **fts move**) are not supported in HP DCE/9000 Version 1.2. Attempting these commands may cause a system crash.
- When DFS daemons are running, the system load average base will be four (4) instead of zero (0). This will cause load-monitoring utilities such as **xload** and **uptime** to display erroneously high system load averages. You may subtract four from the load average given by such utilities to determine the true system load average.

Planning for the DCE Distributed File Service (DFS)

You can configure the following types of DFS server machines:

- A System Control machine distributes system configuration information that is shared by all DFS server machines in a cell. System Control machines can also be used as Binary Distribution machines.
- A Fileset Location Database machine tracks and records the locations of all filesets. At least one is required in each cell.
- A File Server machine exports UFS data to the global DFS namespace. At least one File Server machine is required in each cell; the File Server machine will be configured automatically when you configure the FLDB machine.
- A Private File Server also exports file system data to the global DFS namespace. A Private File Server machine is controlled by the owner of the machine, not by the system administrator. The purpose of a Private File Server machine is to allow individual users to export a small number of filesets. A Private File Server does not support replicated filesets.

Although you must configure at least one Fileset Location Database machine, and the accompanying File Server machine, all other DFS server machines are optional.

NOTE If you use the SDCC (Sam DCE Cell Configuration) tool to configure DFS, you must configure a system control machine. A system control machine is optional when you use dce_config to configure DFS.

Before you begin DFS configuration, be sure to:

- Make the planning decisions described in the *OSF DCE Administration Guide – Extended Services*. These decisions include the following:
  - Determining which machine and file system to use for **root.dfs**
  - Defining DFS server and client roles
  - Determining the cache size on DFS client machines
  - Setting up your cell's DFS tree structure

- Create the file system for the **root.dfs** fileset. You can create the file system manually using HP-UX file system commands (e.g. **newfs**), or you can use an existing filesystem. You should configure the first (if more than one) Fileset Location Database Server on the machine that exports **root.dfs**.

Configuring DFS

This section presumes that you have already configured a cell running HP DCE/9000 Version 1.2 with (at least) Security and CDS services. For instructions on using the SAM-based DCE Cell Configuration Tool to configure a cell, choose the **Help** menu in the SAM DCE Cell Configuration window. For instructions on using **dce_config** to configure a cell, see Chapter 4, Configuring HP DCE/9000.

We suggest that you use the SAM DCE Cell Configuration Tool to configure DCE and DFS. Instructions for using the SAM DCE Cell Configuration Tool are available online via the **Help** menu item in the SAM DCE Cell Configuration window.

The following sections describe how to configure DFS using the **dce_config** utility.

Configuring a System Control Machine

A System Control Machine is not required. If you want to configure a System Control machine, perform the following steps:

1 As **root**, run **dce_config**. From the DCE Main Menu, choose CONFIGURE:

```
DCE Main Menu (on hostname)

selection: 1 (CONFIGURE)

DCE Configuration Menu (on hostname)
1. Initial Cell Configuration
2. Additional Server Configuration
3. DCE Client
4. DFS Client

98. Return to previous menu
99. Exit
```

```
selection:
```

2 From the DCE Configuration Menu, choose **Additional Server Configuration**:

```
DCE Configuration Menu (on hostname)
selection: 2

Enter Cell Administrator's principal name:(cell_admin)
Enter password:
```

3 From the DCE Additional Server Configuration Menu, choose **DFS System Control Machine**:

```
Additional Server Configuration Menu (on hostname)

1.  Additional CDS Server(s)
2.  DTS
3.  DFS System Control Machine
4.  DFS Private File Server
5.  DFS File Server
6.  DFS Fileset Location Database Server
7.  GDA Server
8.  Replica Security Server

98. Return to previous menu
99. Exit

selection: 3
S:****** Configuring System Control Machine...

S:****** Loading kernel extensions...
S:****** rpc_config: installed krpc device at major
number 71
```

4 **dce_config** asks whether the LFS (Episode) kernel extensions should be loaded, and whether LFS should be initialized. LFS is not supported at this release of HP DCE/9000, so answer **n**.

```
Should the LFS kernel extension be loaded? (n)? n
Should LFS be initialized? (n)? n
```

```
S:****** Modifying the registry database for DFS serv-
er operation...
S:****** Starting bosserver...
S:****** Creating BOS admin lists.
S:****** Starting upserver...
```

When the configuration is complete, **dce_config** displays the Additional Server Configuration Menu.

Configuring a DFS Fileset Location Database

Each cell that uses DFS requires at least one Fileset Location Database Server machine. If you are configuring a DFS System Control machine, you should do so before configuring the DFS Fileset Location Database Server.

To configure a Fileset Location Database machine, perform the following steps:

1 From the Additional Server Configuration Menu, choose 6 (DFS Fileset Location Database Server).

```
Additional Server Configuration Menu (on hostname)
selection: 6

S:****** Configuring DFS Fileset Location Database
Server...

Enter Cell Administrator's principal name:(cell_admin)
Enter password:
```

2 **dce_config** asks whether the LFS (Episode) kernel extensions should be loaded, and whether LFS should be initialized. LFS is not supported at this release of HP DCE/9000, so answer **n** to both questions.

```
Should the LFS kernel extension be loaded? (n)? n
Should LFS be initialized? (n)? n
```

```
S:****** Modifying the registry database for DFS serv-
er operation...
>>> group member added
>>> group member added

Current site is: registry server at
/.../test_cell/subsys/dce/sec/master
Domain changed to: group

Current site is: registry server at
/.../test_cell/subsys/dce/sec/master
Domain changed to: group

S:****** Starting bosserver...
Checking for a Ubik sync site in hosts/node_name
Host /.:/hostsnode_name/ is now the sync site
```

3 **dce_config** prompts for the name of the system control machine. If your cell does not use a system control machine, enter the name of the local machine. This name must exactly match the output of the **hostname** command.

```
Enter the name of the system control machine:
```

4 **dce_config** prompts for the name of the DFS file set. **root.dfs** is the default name. When configuring the first (or only) FLDB server, **root.dfs** should be specified.

```
Enter the fileset name (root.dfs): root.dfs
```

5 **dce_config** prompts for the filesystem type for the DFS file set. This release of HP DCE/9000 does not support the Episode (LFS) file system, so choose Native File System.

```
Enter the filesystem type for root.dfs:
1. Native File System (e.g. UFS, JFS)
2. Episode File System (LFS):
selection: 1
```

6 **dce_config** prompts for device name for the aggregate to be exported. On HP-UX, this will be a name of the form **/dev/dsk/5s0** for Series 700 systems or **/dev/vg00/lvol4** for Series 800 systems.

```
Enter the device name for the aggregate to be exported
(i.e. /dev/lvXX):
```

7 **dce_config** prompts for the aggregate name. The aggregate name is the mounted file system name, not the physical device name. You can use the **bdf** or **mount** commands to find the pathname at which a disk is mounted

```
Enter the aggregate name (/export):
```

8 **dce_config** prompts for a numerical aggregate ID. The aggregate ID number must be unique on that system. The aggregate ID for **root.dfs** is generally **1**.

```
Enter the aggregate ID (1):
```

9 **dce_config** displays information about the aggregate and about the servers it is starting:

```
number of sites: 1
   server      flags    aggr   siteAge  principal  owner
host_name.ch.acme.  RW  1      0:00:00     <nil>
FLDB entry created for fileset root.dfs (0,,1) on ag-
gregate 1 of node_name
S:****** Starting dfsbind...
S:****** Starting fxd...
fx: FX server starts listening...
```

Configuration of the FLDB (Fileset Location Database) Server machine and the first File Server is now complete.

Configuring a File Server and a Private File Server

The steps to configure a File Server and a Private File Server are the same. In the steps that follow, a Private File Server is configured to illustrate the sequence of prompts and actions. However, you can use the same instructions to configure a File Server.

To configure a File Server or Private File Server, perform the following steps:

1 From the Additional Server Configuration Menu, choose 4 (DFS Private File Server) or 5 (DFS File Server).

```
Additional Server Configuration Menu (on hostname)
selection: 4

S:****** Configuring DFS Private File Server...

Enter Cell Administrator's principal name:(cell_admin)
Enter password:
```

2 **dce_config** asks whether LFS (Episode) should be loaded. LFS is not supported at this release of HP DCE/9000, so answer **n**.

```
S:****** Loading kernel extensions...

Should the LFS Kernel Extension be loaded (n)? n
Should LFS be initialized? (n)? n

S:****** Modifying the registry database for DFS serv-
er operation...
S:****** Starting bosserver...
S:****** Creating ftserver...
```

3 **dce_config** prompts for the name of the System Control machine. If your cell does not use a system control machine, enter the name of the local machine. This name must exactly match the output of the **hostname** command.

```
Enter the name of the system control machine:
```

4 **dce_config** prompts for the filesystem type for the aggregate to be exported. This release of HP DCE/9000 does not support the Episode (LFS) file system, so choose Native File System.

```
Enter the filesystem type for the aggregate to be ex-
ported
1. Native File System (e.g. UFS, JFS)
2. Episode File System (LFS):
selection: 1
```

5 **dce_config** prompts for device name for the aggregate to be exported. On HP-UX, this will be a name of the form **/dev/dsk/5s0** for Series

700 systems or **/dev/vg00/lvol4** for Series 800 systems.

```
Enter the device name for the aggregate to be exported
(i.e. /dev/lvXX):
```

6 **dce_config** prompts for the pathname of the device on which the selected file system is stored. You can use the **bdf** or **mount** commands to find the pathname at which the disk specified in step 5 is mounted.

```
Enter the mount path for the aggregate (e.g. /usr/us-
ers):
```

7 **dce_config** prompts for an aggregate name and numerical aggregate ID. Both of these items are arbitrary values, but must be unique on the machine being configured.

```
Enter a unique aggregate name (e.g. user.jlw):
Enter a unique numerical aggregate ID:
```

8 **dce_config** now exports the chosen file system and displays instructions on where to find information about exporting additional file systems.

```
S:****** Exporting device_name through DFS...
If you wish to export additional aggregates, do so af-
ter completing this script by using the appropriate DFS
administration commands described in the DFS Admin
Guide.
Press <RETURN> to continue, CTRL-C to exit: <RETURN>

S:****** Starting fxd...
fs: FX server starts listening...
```

Configuration of the DFS File Server is now complete.

Configuring a DFS Client

A DFS Client machine must have been previously configured as a DCE client. To configure a DFS client machine, perform the following steps on a DCE client system:

1 From the DCE Main Menu, choose CONFIGURE:

```
DCE Main Menu (on hostname)

selection: 1 (CONFIGURE)

DCE Configuration Menu (on hostname)
1. Initial Cell Configuration
2. Additional Server Configuration
3. DCE Client
4. DFS Client

98. Return to previous menu 99. Exit
selection:
```

2 From the DCE Configuration Menu, choose 4 (DFS Client):

```
DCE Configuration Menu (on hostname)
selection: 4

Enter Cell Administrator's principal name:(cell_admin)
Enter password:

S:****** Loading kernel extensions...
S:****** rpc_config: installed krpc device at major
number 71
```

3 **dce_config** asks whether LFS (Episode) should be initialized. LFS is not supported at this release of HP DCE/9000, so answer **n**.

```
Should LFS be initialized? (n)? n
```

4 Choose whether the cache is in system memory or on the local disk.

```
Is the cache:
1. in memory
2. on the local disk
selection:

S:****** Starting dfsbind...
```

5 Choose a cache size. The default cache size is 10MB. Note that at least 10 MB of free disk space must be reserved for on-disk cache.

```
Enter the size of the cache (10000):
```

6 Choose a directory to hold the cache (the default directory is a reasonable choice):

```
Enter the name of the cache directory (/opt/dcelo-
cal/var/adm/dfs/cache):

S:****** Starting dfsd...
dfs: TKN server is listening...
dfsd: start sweeping disk cache files...
dfsd: All DFS daemons started.
```

DFS Client configuration is now complete.

dfs_config Environment Variables

dfs_config recognizes the following environment variables. If these environment variables are set and exported, **dfs_config** will skip the corresponding prompts for information when run in interactive mode.

AGG_DEV_NAME: if set, is the device name for the aggregate to be exported (e.g. /dev/lvXX). This is also used as the device name for filesets.

AGG_FS_TYPE: if set, is the type of the filesystem for the aggregate to be exported. "native" means the native file system (e.g. UFS, JFS). "episode" means the Episode (LFS) file system. This is also used as the file system type for filesets.

AGG_MOUNT_PATH: if set, is the mount path for the aggregate (e.g. /usr/users).

AGG_NAME: if set, is the name to be used for the aggregate to be exported (e.g. user.jlw).

AGG_ID: if set, is the unique numerical aggregate ID for the exported aggregate.

CLIENT_CACHE_LOC: "mem" means cache is in memory. "disk" means cache is on the local disk.

CACHE_DIR_DISK: if set, is the pathname of the directory to use for a local disk cache (if one is used).

CACHE_SIZE_DISK: if set, is the number of bytes to use for a local disk cache (if one is used).

CACHE_SIZE_RAM: if set, is the number of bytes to use for an in memory cache (if one is used).

DFS_SERVER_INSTALL: One of four values: "scm" - System Control Machine "privatefs" - Private File Server "fs" - File Server "fldb" - Fileset Location Database Server

EPI_FORMAT_PART: "y" if user wishes the format a partition as an Episode aggregate. "n" otherwise.

EPI_FORCE_INIT: "y" if user wishes to force the initialization of a partition as an Episode aggregate, possibly losing data. "n" otherwise.

INIT_LFS: "y" if user wants to initialize the LFS (using epiinit). "n" otherwise.

INSTALL_OPT_SERS: "y" if user wants to install optional DFS servers (e.g. bak, butc, upclient). "n" otherwise.

INSTALL_OPT_CLIENT: "y" if user wants to install the optional client binaries (cm, bos, and fts). "n" otherwise.

LOAD_LFS_KEXT: "y" if user wants to load the LFS kernel extension. "n" otherwise.

ROOT_FILESET_NM: if set, is the root fileset name.

SCM_NAME: if set, is the name of the system control machine to be used during configuration.

Unauthenticated Access to the DFS Namespace

You may export the DFS namespace "/..." to NFS. This can be done as with any other NFS mount point.

To export the DFS namespace via SAM, perform the following steps:

1 As **root**, invoke SAM on a DFS client.

2 Select **Networking/Communications->Networked Filesystems ->Local File Systems Exported**.

3 Pull down the **Actions** menu and select **Add**.

4 Enter "/..." as the local file system to export and select "Ok". "/..." will be exported via NFS from that DFS client.

5 Now you may NFS mount "<host>:/..." on any other host in order to access the DCE/DFS namespace. As root, do

```
$ mkdir /...
$ mount <host>:/... /...
```

<host> is the hostname of a DFS client.

It may be necessary to increase the mount timeout value (timeo).

6 To complete the namespace, create a link to the DFS root.dfs fileset as

```
$ ln -s /.../<cellname>/fs /:
```

where "<cellname>" is the name of the cell in which the DFS client exporting "/..." resides. Use the "/:" link on the DFS client as a guide. This will provide the same view of "/:" as seen from any DFS client in the cell "<cellname>".

Access to the DFS namespace via this method is unauthenticated. Permission for this access is that of "other". For example, you will be able to list directories and read files that grant read and execute permissions to other. Furthermore, even if other have write permission, files and directories created will be owned by the unknown user and group (id = -2).

To obtain a secure method of authenticated access to the DFS namespace, see the next section, Authenticated Access to the DFS Namespace.

Authenticated Access to the DFS Namespace

HP DCE/9000 Version 1.2 provides a protocol exporter for DCE-authenticated access to the DFS access via an NFS client. This is a separately-priced option to HP DCE/9000 Version 1.2.

NOTE

The DFS NFS protocol exporter daemons requires version 3.00 or later of the HP C++ shared library (/usr/lib/libC.sl). If you do not already have this library on your system, it is provided with HP DCE 1.2 in /opt/dcelocal/libC.sl, and should be copied from there into /usr/lib.

The authenticated DFS NFS protocol exporter allows a user of a system that is not running DCE/DFS to access files in a DFS cell through the NFS-mounting of "/...". In order to gain authenticated access to the DFS cell, the user must have a valid account in the DCE registry and must use the **dfs_login** command on the NFS client from which they wish to become authenticated.

The **dfs_login** command obtains a Kerberos5 ticket from the DCE security service. This ticket forms the user's DCE credentials. **dfs_login** sends this ticket with the user's local user identity (UID) to the DFS NFS exporter system (the system that is providing the "/..." mount point). The **drasd** server receives the remote credentials and maps the user's UID and host to the DCE credential obtained with the Kerberos5 ticket. This mapping is used by the exporter to provide access to the DFS name space.

The Kerberos tickets will have an lifetime of 8 hours (unless otherwise specified via the **-l** option to **dfs_login**). **dfs_login** must be run again to renew the expired tickets. A mapping obtained via **dfs_login** can be destroyed by the **dfs_logout** command.

Credentials for DCE-authenticated NFS access are for a particular user on a particular system. A user attempting authenticated access from more than one system must run **dfs_login** on each system from which authenticated access is desired.

If **dfs_login/dfs_logout** is not installed on an NFS client system, authenticated access to DFS can still be obtained. (This is true for HP 9000 Series 700 and Series 800 systems only). To obtain authentication without using **dfs_login**, you must remote login to the exporter system and using the **atcp** command. The **atcp** command allows a user to establish a DCE credential mapping by specifying the remote host and user identity (UID) along with the DCE account that is to be associated with that user. The **atcp** command can also be used to list, query and delete mappings for remote users, but requires that it be run by **root** to do so. See **atcp**(8) for usage and syntax information.

The DFS NFS protocol exporter includes the following binaries (and corresponding man pages).

Installed on the DCE DFS exporter system (filesets DCE-CMN, DCE-CORE):

- **/opt/dcelocal/bin/atcp**
  A local interface to the NFS exporter credential mappings for the NFS exporter. **atcp** allows a local user to view/add/modify/destroy the NFS/DCE mappings.
- **/opt/dcelocal/bin/drasd**
  Server that uses Kerberos to allow the remote creation of DCE/Kerberos authentication tickets that are used to establish credential mappings on the DFS NFS exporter.

Installed on the NFS system (fileset DFS-NFS):

- **/usr/bin/dfs_login**
  Allows users on NFS client machines to establish DCE credentials on the NFS exporter machine.
- **/usr/bin/dfs_logout**
  Allows users on NFS client machines to remove DCE credentials obtained via **dfs_login**.

Configuring an Exporter Machine

1 Add the **dlog/udp** service to the internet services database, either in each system's **/etc/services** or the corresponding NIS services maps,

as follows:

```
dlog    180/dlog
```

2 Configure your client to run a **bosserver** (see **bosserver**(8)), as described in the next section:

3 On the DFS client, add a DCE registry account for the **drasd** server. Run **rgy_edit** as DCE principal **cell_admin** and local **root**. *hostname* is the exporter system name; *cell-pw* is the DCE cell administrator password.

```
rgy_edit> domain group
rgy_edit> add subsys/dce/dlog-admin
rgy_edit> domain principal
rgy_edit>  add  hosts/<hostname>/dlogrgy_edit>  domain
account
rgy_edit> add hosts/<hostname>/dlog \
 -g subsys/dce/dlog-admin -o none -pw <cell-pw> \
 -mp <cell-pw>
rgy_edit> min -o none -pw <cell-pw> -mp <cell-pw>
rgy_edit> ktadd -p hosts/<hostname>/dlog -pw <cell-pw>
rgy_edit> ktadd -p hosts/<hostname>/dlog -a -r
```

4 Create a bos job to run the drasd server.

```
bos create -server /.:/hosts/<hostname> -process \
 dras -type simple -cmd "/opt/dcelocal/bin/drasd"
```

Configuring a bosserver

Only do this on a system that is NOT running a **bosserver**. If your system is exporting aggregates, you are already running a **bosserver** and this is not necessary. You will need to be authenticated as DCE **cell_admin** to perform these tasks.

1 Add the host to run the **bosserver** to the DCE registry and setup the correct ACL on the entry:

```
rgy_edit=> domain principal
rgy_edit=> add hosts/<host>/dfs-server
rgy_edit=> domain account
rgy_edit=> add hosts/<host>/dfs-server -g |
```

```
 subsys/dce/dfs-admin -o none -pw $<cell-pw> \
 -mp <cell-pw>
rgy_edit=> ktadd -p hosts/<host>/dfs-server -pw \
 <cell-pw>
rgy_edit=> ktadd -p hosts/<host>/dfs-server -a -r
rgy_edit=> quit

$ acl_edit /.:/sec/principal/hosts/<host>/dfs-server\
  -m group:subsys/dce/dfs-admin:rcDnfmag
```

2 Cleanup any stale **bos** configuration (as **root**):

```
$ rm -f /opt/dcelocal/var/dfs/BosConfig
$ rm -f /opt/dcelocal/var/dfs/admin.*
```

3 Startup the **bosserver**, initially unauthenticated (as **root**):

```
$ /opt/dcelocal/bin/bosserver -noauth &
```

[Wait for bos server to start, about 30 seconds]

4 Add the minimal set of information to the bos server's admin list

```
$ /opt/dcelocal/bin/bos addadmin \
  -server /.:/hosts/<host> -adminlist \
   admin.bos -group subsys/dce/dfs-admin
```

5 Turn on **bosserver** authorization checks:

```
$ /opt/dcelocal/bin/bos setauth \
  -server /.:/hosts/<host> -authchecking on
```

Configuring an NFS Client Machine

To set up authenticated access to DFS from an NFS client system, do the following on the client system:

1 Install the DFS-NFS fileset on the NFS client system. The DFS-NFS fileset contains the **dfs_login** and **dfs_logout** commands.

2 Create the Kerberos5 config files, **/krb5/krb.conf** and **/krb5/krb.realms**.

The **/krb5/krb.conf** file can be copied from a system in the DCE cell. The **/krb5/krb.realms** file is used by the Kerberos runtime to translate host domains to the corresponding Kerberos realm. In this case the Kerberos realm is the same as the DCE cell.

Each line is made up as "[domain-part] [krb-realm]"

Here is an example **krb.realms** file:

.CH.APOLLO.HP.COM dfs_group.cell.ch.hp.com
.CH.APOLLO.HP.COM. dfs_group.cell.ch.hp.com
CH.APOLLO.HP.COM dfs_group.cell.ch.hp.com

Note that the case is significant for the realm name.

9

HP DCE/9000 Global Directory Service (GDS)

HP DCE/9000 Global Directory Service (GDS)

This chapter describes the recommended procedures for installing, starting, administering, and troubleshooting HP DCE/9000 Global Directory Services (GDS).

For more information on GDS terms and concepts, refer to the *Introduction to OSF DCE*, the *OSF DCE Administration Reference*, and the *OSF DCE Administration Guide – Extended Services* manuals.

Installing GDS

This section describes the hardware and software requirements for HP DCE/9000 GDS and references procedures used to install the GDS fileset.

After completing the installation, you must configure GDS. This information is also contained in this chapter.

Overview

The following is a brief overview of the installation process described in this section:

1 Verify that hardware and software prerequisites are met at your site.

2 Install the GDS fileset.

Prerequisites

Hardware and Software Requirements

Any system that you want to add GDS to must meet certain hardware and software requirements. The system requirements are:

System Type	HP 9000 Series 700 or Series 800.
Operating System	HP-UX 9.X.
Software Dependencies	All of DCE's libraries.
Memory	20 Mb for only GDS is recommended. Any amount of memory less than 20 Mb may cause performance degradation.
Disk Space	15 Mb of disk space is needed to install GDS.

Installing Software

Once you have made sure you have met all the hardware and software requirements, you can begin installing the GDS fileset, GDS-CORE, on the system. Refer to Chapter 3, "Installing HP DCE/9000" for more information on the installation process.

Configuring GDS

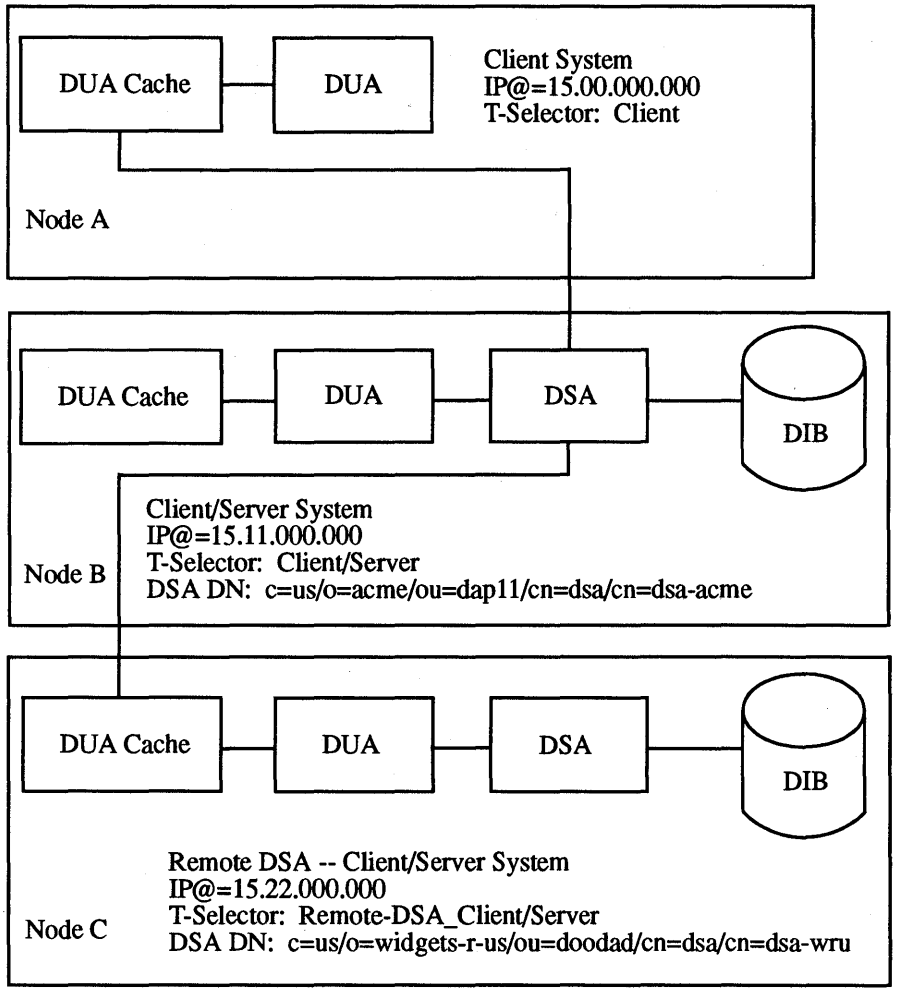
This section describes how to use the tools to configure HP DCE/9000 GDS.

To configure the GDS software, you must have completed the installation procedures. See the previous section for installation information.

Note that this section assumes a basic familiarity with GDS terms and concepts, as described in the *OSF DCE Administration Guide – Extended Services* manual.

Overview

In this section, examples are given for configuring Node B, a client/server system (with Node C as a remote DSA), and Node A, a client system.



You will be using the menu-based tool **gdssysadm**. **gdssysadm** allows you to create, change, delete, and display the GDS configuration data; administer the database; activate and deactivate the directory system installation; save and restore data to a disk, tape, or file; display directory system status information; and activate and deactivate the tracing system. This section will describe its configuration capabilities.

Be sure that the first directory ID configured is directory ID 1. If directory ID 1 does not exist, GDS will not run. After directory ID 1 is configured, it can be changed but cannot be deleted.

When configuration data is changed or deleted, **gdssysadm** changes or deletes the directory ID information in the **/opt/dcelocal/etc/gdsconfig** file.

For the new configuration data to take affect, the system must be deactivated and reactivated. You can only change and delete configuration data when the system is deactivated.

To configure GDS, you must complete the following steps:

1 Configure the GDS directory system.

2 Activate the directory system.

3 Initialize the directory service.

The following sections explain how to configure the GDS client/server and client. The text shows the complete menu at its first occurrence; thereafter, it shows only the menu name and current selection, prompts, and recommended input values (in **boldface**). After you make a selection, either press RETURN or the **f2** softkey (unless otherwise noted).

Configuring the GDS Client/Server

To fully configure the GDS client/server, you must complete the following steps (each step is explained in this section):

1 Configure the GDS client/server directory system.

2 Activate the GDS client/server directory system.

3 Initialize the GDS client/server directory service.

Configuring the GDS Client/Server Directory System

To configure the GDS client/server directory system, do the following:

1 Start **gdssysadm**.

2 Configure the directory system.

Starting gdssysadm

a. Log in as **root** on the system you wish to configure (Node B).

b. Make sure that **/opt/dcelocal/bin** is in your command search path:

 # export PATH=/opt/dcelocal/bin:$PATH (Bourne/Korn shell)

% setenv PATH /opt/dcelocal/bin:$PATH (C shell)

c. Make sure the NLSPATH environment variable is set to **/opt/dcelocal/nls/msg/en_US.ASCII/%N.cat**:

 # export NLSPATH=/opt/dcelocal/nls/msg/en_US.ASCII/%N.cat

% setenv NLSPATH /opt/dcelocal/nls/msg/en_US.ASCII/%N.cat

d. Make sure the TERM environment variable is set to **hpterm**:

#export TERM=hpterm

%setenv TERM hpterm

e. Run **gdssysadm**:

 # gdssysadm

```
(diradm)          DIRECTORY SYSTEM

a - Administration of the directory information tree
c - Configuration of a directory system
b - Activation of a directory system installation
d - Deactivation of a directory system installation
s - Saving of local data to diskette/tape/file
r - Restoring of saved data from diskette/tape/file
f - Further functions

Your selection! >
```

Configuring the Directory System

a. From diradm, choose c for configuration:

```
diradm

Your selection! > c

(confpar)          DIRECTORY SYSTEM          Configuration

Which configuration mode ?:  Creation of configuration data
```

b. From confpar, choose Creation of configuration data (use the space bar to scroll through selections):

```
confpar

Which configuration mode?: Creation of configuration data

(confpar)          DIRECTORY SYSTEM          Configuration

For which directory ID should the operation be
performed ? (1-20): 1
```

c. From confpar, choose 1 as the directory ID:

```
confpar

For which directory ID should the operation be
performed ? (1-20): 1

(confpar)          DIRECTORY SYSTEM          Configuration

Which configuration type ?: Client system

How many clients have access to the directory system at the
same time ? (1-256): 16_
```

d. From confpar, choose Client-Server system as the configuration type (use the space bar to scroll through selections) and use the default value for the number of clients that have access to the directory system at the same time (16):

```
confpar

Which configuration type ?: Client-Server system

How many clients have access to the directory system at the
same time ? (1-256): 16

(confpar)          DIRECTORY SYSTEM          Configuration

How many server processes should be activated ? (1-256): 2__

Do you want to distribute 'update' information ?: No
```

e. From confpar, use the default values for the number of activated server processes (2) and updating the master information (no):

```
confpar

How many server processes should be activated ? (1-256): 2

Do you want to distribute 'update' information ?: No
```

You have successfully configured the directory system.

If you receive the error message "Error: Configuration information already exists!", then the directory system information for directory ID 1 already exists in the **/opt/dcelocal/etc/gdsconfig** file. You can modify the information by choosing "Changing of configuration data" for the configuration mode. Be sure to deactivate and reactivate the system after modifying the information.

Activating the GDS Client/Server Directory System

To activate the GDS client/server directory system, do the following:

1 Start **gdssysadm**.

2 Activate the directory system installation.

Starting gdssysadm

Refer "Starting gdssysadm" in the "Configuring the GDS Client/Server Directory" section.

Activating the Directory System

a. From diradm, choose b to activate the directory system:

```
diradm

Your selection! > b
```

You have successfully activated the directory system.

If you receive the error message "Error: The directory system is active!", then the directory system has already been activated.

To make your current additons or changes active, you must first deactivate the system and then reactivate it.

Initializing the GDS Client/Server Directory Service

To initialize the GDS client/server directory service, do the following:

1 Start **gdssysadm**.

2 Add the client address to the DUA cache.

3 Add the local DSA object name to the DUA cache.

4 Add the remote DSA object name(s) (including the PSAP) to the DUA cache.

If you want to test the GDS client/server locally, complete steps 1 - 3. Step 4 expands the connection to a remote DSA in the distributed environment.

Starting gdssysadm

Refer "Starting gdssysadm" in the "Configuring the GDS Client/Server Directory System" section.

Adding the Client Address to the DUA Cache

a. From diradm, choose a for administration:

```
diradm

Your selection! > a

(Mask 1)          DIRECTORY SYSTEM          Logon

USER IDENTIFICATION:                  Directory ID: 1_

Password:

Country-Name:          __
Organization-Name:     ________________
Org.-Unit-Name:        ________________
Common-Name:           ________________

Options: Logon to the Default DSA
```

b. Press RETURN to move the cursor to the Options field and choose Logon to the DUA Cache (use the space bar to scroll through the selections):

```
Mask 1        (Logon)

Options: Logon to the DUA Cache

(Mask 3)          DIRECTORY SYSTEM          Administration

ADMINISTRATION FUNCTIONS:

0 Exit
1 Object Administration
2 Cache Update

Which function ? 1
```

If you receive the error message "Schema from DSA cannot be read!", press RETURN. You can safely ignore this message because the DSA object name has not yet been added to the DUA cache (you will add the DSA object name later in this section).

c. From Mask 3, choose 1 for object administration:

```
Mask 3        (Administration)

Which function ? 1

(Mask 4)          DIRECTORY SYSTEM          Object Administration

OPERATIONS

0 Exit
1 Add Object
2 Remove Object
3 Display Objects
4 Display Local and Default DSA
5 Add Client Address
6 Display Client Address
7 Delete Default DSA
8 Add Alias

Which operation ? 1__
```

d. From Mask 4, choose 5 to add the client address:

```
Mask 4        (Object Administration)

Which operation ? 5

(Mask 7a)         DIRECTORY SYSTEM          Add Client Address

P-Selector: _____________________
S-Selector: _____________________
T-Selector: Client_____________________

NSAP-address 1: TCP/IP!internet=127.0.0.1+port=21010___
NSAP-address 2: _____________________________________
NSAP-address 3: _____________________________________
NSAP-address 4: _____________________________________
NSAP-address 5: _____________________________________
```

e. From Mask 7a, enter Client/Server for the T-Selector and TCP/IP!internet=127.0.0.1+port=yyyyy for the NSAP-address 1 where 127.0.0.1 is the IP address used for local loopback and yyyyy is any available port number. Then, press the **f2 MENU** softkey:

Mask 7a (Add Client Address)

T-Selector: **Client/Server**

NSAP-address 1: **TCP/IP!internet=127.0.0.1+port=21015**

You have successfully added the client address to the DUA cache. Go on to the next section to continue initializing the GDS client/server.

Adding the Local DSA Object Name to the DUA Cache

a. From Mask 4, choose 1 to add an object:

```
Mask 4        (Object Administration)

Which operation ? 1

(Mask 5)          DIRECTORY SYSTEM          Add Object

Structure Rule                    Name structure

02 Country-Name                   02
03 Organization-Name               02-03
04 Org.-Unit-Name                 02-03-04
05 Common-Name                     02-03-04-05
06 Common-Name                     02-03-04-06
      Org.-Unit-Name
07 Common Name                     02-03-04-05-07
08 Locality-Name                  02-08
09 Common-Name                     02-09-09
10 Common-Name                     02-08-10
      Street-Address

Which structure rule ? 7__
```

b. From Mask 5, choose 7 for the structure rule:

```
Mask 5        (Add Object)

Which structure rule ? 7

(Mask 6)          DIRECTORY SYSTEM          Add object

Object Name

Country-Name          _
Organization-Name     _____________________
Org.-Unit-Name        _____________________
Common-Name           _____________________
Common-Name           _____________________

Structural Object class: Application-Entity
Auxiliary object class: NO
```

c. From Mask 6, enter the local DSA object name (DSA DN), choose Directory-Service-Agent for the structural object class (use the space bar to scroll through the selections), and use the default for auxiliary object class (no):

Mask 6 (Add Object)

Country-Name **us**
Organization-Name **acme**
Org.-Unit-Name **dap11**
Common-Name **dsa**
Common-Name **dsa-acme**

Structural Object class: **Directory-Service-Agent**
Auxiliary object class: **NO**

(Mask 6d) DIRECTORY SYSTEM Add Object

Presentation-Address
CDS-Cell
CDS-Replica
Common-Name
DSA-Type
Description
Knowledge-Information
Locality-Name
Master-Knowledge
Org.-Unit-Name
Organization-Name
See-Also
Suppl.-Applic.-Context
User-Password

d. From Mask 6d, use the arrow keys to move the cursor to DSA-Type (Presentation-Address is highlighted by default), select DSA-Type by pressing RETURN, and then press the **f2 MENU** softkey:

Mask 6d (Add Object)

Presentation-Address
DSA-Type

(Mask 7) DIRECTORY SYSTEM Add Object

Attributes:

Name : DSA-Type
Value: _____
_____
Name : _____
Value: _____
_____
Name : _____
Value: _____
_____

e. From Mask 7, enter default/local' as the DSA-Type value (the value must be default/local' when you are adding the local DSA object name to the DUA cache; you are defining the DSA from step c as the local and default DSA). Press the **f2 MENU** softkey:

Mask 7 (Add Object)

Value: **default/local'**
(Mask 7a) DIRECTORY SYSTEM Add Object

P-Selector: _____
S-Selector: _____
T-Selector: _____

NSAP-address 1: _____
NSAP-address 2: _____
NSAP-address 3: _____
NSAP-address 4: _____
NSAP-address 5: _____

f. From Mask 7a, enter Client/Server for the T-Selector and TCP/IP!internet=15.11.000.000+port=yyyyy for the NSAP-address 1 where 15.11.000.000 is the system's IP address and yyyyy is any available port number. Then, press the **f2 MENU** softkey:

Mask 7a (Add Object)

T-Selector: **Client/Server**

NSAP-address 1: **TCP/IP!internet=15.11.000.000+port=21010**

You have successfully added the local DSA object name to the DUA cache. The directory system now works locally. In order to connect to an additional DSA within the distributed environment, continue on with the next section to finish initializing the GDS client/server

Adding the Remote DSA Object Name to the DUA Cache

a. From Mask 4, choose 1 to add an object:

```
Mask 4        (Object Administration)

Which operation ? 1

(Mask 5)          DIRECTORY SYSTEM          Add Object

Structure Rule                    Name structure

02 Country-Name                   02
03 Organization-Name               02-03
04 Org.-Unit-Name                 02-03-04
05 Common-Name                     02-03-04-05
06 Common-Name                     02-03-04-06
      Org.-Unit-Name
07 Common Name                     02-03-04-05-07
08 Locality-Name                  02-08
09 Common-Name                     02-09-09
10 Common-Name                     02-08-10
      Street-Address

Which structure rule ? 7__
```

b. From Mask 5, choose 7 for the structure rule:

```
Mask 5        (Add Object)

Which structure rule ? 7

(Mask 6)          DIRECTORY SYSTEM          Add object

Object Name

Country-Name          __
Organization-Name     ____________________
Org.-Unit-Name        ____________________
Common-Name           ____________________
Common-Name           ____________________

Structural Object class: Application-Entity
Auxiliary object class: NO
```

c. From Mask 6, enter the remote DSA object name (DSA DN), choose Directory-Service-Agent for the structural object class (use the space bar to scroll through the selections), and use the default for the auxiliary object class (no):

Mask 6 (Add Object)

Country-Name **us**
Organization-Name **widgets-r-us**
Org.-Unit-Name **doodad**
Common-Name **dsa**
Common-Name **dsa-wru**

Structural Object class: **Directory-Service-Agent**
Auxiliary object class: **NO**

(Mask 6d) DIRECTORY SYSTEM Add Object

Presentation-Address
CDS-Cell
CDS-Replica
Common-Name
DSA-Type
Description
Knowledge-Information
Locality-Name
Master-Knowledge
Org.-Unit-Name
Organization-Name
See-Also
Suppl.-Applic.-Context
User-Password

d. From Mask 6d, press the **f2 MENU** softkey (Presentation-Address is highlighted by default):

Mask 6d (Add Object)

Presentation-Address

(Mask 7a) DIRECTORY SYSTEM Add Object

P-Selector: _____
S-Selector: _____
T-Selector: _____

NSAP-address 1: _____
NSAP-address 2: _____
NSAP-address 3: _____
NSAP-address 4: _____
NSAP-address 5: _____

e. From Mask 7a, enter Remote-DSA_Client/Server for the T-Selector and TCP/IP!internet=15.22.000.000+port=yyyyy for the NSAP-address 1 where 15.22.000.000 is the remote system's IP address and yyyyy is any available port number. Then, press the **f2 MENU** softkey:

Mask 7a (Add Object)

T-Selector: **Remote-DSA_Client/Server**

NSAP-address 1: **TCP/IP!internet=15.22.000.000+port=21025**

You have successfully added the remote DSA object name to the DUA cache and initialized and configured the GDS client/server within a distributed environment.

Configuring the GDS Client

To fully configure the GDS client, you must complete the following steps (each step is explained in this section):

1 Configure the GDS client directory system.

2 Activate the GDS client directory system.

3 Initialize the GDS client directory service.

Configuring the GDS Client Directory System

To configure the GDS client directory system, do the following:

1 Start **gdssysadm**.

2 Configure the directory system.

Starting gdssysadm

a. Log in as **root** on the system you wish to configure (Node A).

b. Make sure that **/opt/dcelocal/bin** is in your command search path:

 # export PATH=/opt/dcelocal/bin:$PATH (Bourne/Korn shell)

% setenv PATH /opt/dcelocal/bin:$PATH (C shell)

c. Make sure the NLSPATH environment variable is set to **/opt/dcelocal/nls/msg/en_US.ASCII/%N.cat**:

 # export NLSPATH=/opt/dcelocal/nls/msg/en_US.ASCII/%N.cat

% setenv NLSPATH=/opt/dcelocal/nls/msg/en_US.ASCII/%N.cat

d. Make sure the TERM environment variable is set to **hpterm**:

#export TERM=hpterm

%setenv TERM hpterm

e. Run **gdssysadm**:

 # gdssysadm

```
(diradm)          DIRECTORY SYSTEM

a - Administration of the directory information tree
c - Configuration of a directory system
b - Activation of a directory system installation
d - Deactivation of a directory system installation
s - Saving of local data to diskette/tape/file
r - Restoring of saved data from diskette/tape/file
f - Further functions

Your selection! >
```

Configuring the Directory System

a. From diradm, choose c for configuration:

```
diradm

Your selection! > c

(confpar)          DIRECTORY SYSTEM          Configuration

Which configuration mode ?:  Creation of configuration data
```

b. **From confpar, choose Creation of configuration data (use the space bar to scroll through selections):**

```
confpar

Which configuration mode?: Creation of configuration data

(confpar)          DIRECTORY SYSTEM          Configuration

For which directory ID should the operation be
performed ? (1-20): 1
```

c. **From confpar, choose 1 as the directory ID:**

```
confpar

For which directory ID should the operation be
performed ? (1-20): 1

(confpar)          DIRECTORY SYSTEM          Configuration

Which configuration type ?: Client system

How many clients have access to the directory system at the
same time ? (1-256): 16
```

d. From confpar, choose Client system as the configuration type (use the space bar to scroll through selections) and use the default value for the number of clients that have access to the directory system at the same time (16):

```
confpar

Which configuration type ?: Client system

How many clients have access to the directory system at the
same time ? (1-256): 16
```

You have now successfully configured the directory system.

If you receive the error message "Error: Configuration information already exists!", then the directory system information for directory ID 1 already exists in the **/opt/dcelocal/etc/gdsconfig** file. You can modify the information by choosing "Changing of configuration data" for the configuration mode. Be sure to deactivate and reactivate the system after modifying the information.

Activating the GDS Client Directory System

To activate the GDS client directory system, do the following:

1 Start **gdssysadm**.

2 Activate the directory.

Starting gdssysadm

Refer "Starting gdssysadm" in the "Configuring the GDS Client Directory System" section.

Activating the Directory System

a. From diradm, choose b to activate the directory system:

```
diradm

Your selection! > b
```

You have successfully activated the directory system.

If you receive the error message "Error: The directory system is active!", then the directory system has already been activated.

To make your current additons or changes active, you must first deactivate the system and then reactivate it.

Initializing the GDS Client Directory Service

To initialize the GDS client directory service, do the following:

1 Start **gdssysadm**.

2 Add the client address to the DUA cache.

3 Add the remote DSA object name (including the PSAP) to the DUA cache.

Starting gdssysadm

Refer "Starting gdssysadm" in the "Configuring the GDS Client Directory System" section.

Adding the Client Address to the DUA Cache

a. From diradm, choose a for administration:

```
diradm

Your selection! > a

(Mask 1)          DIRECTORY SYSTEM          Logon

USER IDENTIFICATION:                  Directory ID: 1_

Password:

Country-Name:          __
Organization-Name:     ____________________
Org.-Unit-Name:        ____________________
Common-Name:           ____________________

Options: Logon to the Default DSA
```

b. Press RETURN to move the cursor to the Options field and choose Logon to the DUA Cache (use the space bar to scroll through the selections):

```
Mask 1        (Logon)

Options: Logon to the DUA Cache

(Mask 3)          DIRECTORY SYSTEM          Administration

ADMINISTRATION FUNCTIONS:

0 Exit
1 Object Administration
2 Cache Update

Which function ? 1
```

If you receive the error message "Schema from DSA cannot be read!", press RETURN. You can safely ignore this message because the DSA object name has not yet been added to the DUA cache (you will add the DSA object name later in this section).

c. From Mask 3, choose 1 for object administration:

```
Mask 3        (Administration)

Which function ? 1

(Mask 4)          DIRECTORY SYSTEM          Object Administration

OPERATIONS

0 Exit
1 Add Object
2 Remove Object
3 Display Objects
4 Display Local and Default DSA
5 Add Client Address
6 Display Client Address
7 Delete Default DSA
8 Add Alias

Which operation ? 1__
```

d. From Mask 4, choose 5 to add the client address:

```
Mask 4        (Object Administration)

Which operation ? 5

(Mask 7a)         DIRECTORY SYSTEM          Add Client Address

P-Selector: _____________________
S-Selector: _____________________
T-Selector: _____________________

NSAP-address 1: _____________________________________
NSAP-address 2: _____________________________________
NSAP-address 3: _____________________________________
NSAP-address 4: _____________________________________
NSAP-address 5: _____________________________________
```

e. From Mask 7a, enter Client for the T-Selector and TCP/IP!internet=127.0.0.1+port=yyyyy for the NSAP-address 1 where 127.0.0.1 is the IP address used for local loopback and yyyyy is any available port number. Then, press the **f2 MENU** softkey:

Mask 7a (Add Client Address)

T-Selector: **Client**

NSAP-address 1: **TCP/IP!internet=127.0.0.1+port=21775**

You have successfully added the client address to the DUA cache. Go on to the next section to continue initializing the GDS client.

Adding the Remote DSA Object Name to the DUA Cache

a. From Mask 4, choose 1 to add an object:

```
Mask 4        (Object Administration)

Which operation ? 1

(Mask 5)          DIRECTORY SYSTEM          Add Object

Structure Rule                    Name structure

02 Country-Name                   02
03 Organization-Name              02-03
04 Org.-Unit-Name                 02-03-04
05 Common-Name                    02-03-04-05
06 Common-Name                    02-03-04-06
      Org.-Unit-Name
07 Common Name                    02-03-04-05-07
08 Locality-Name                  02-08
09 Common-Name                    02-09-09
10 Common-Name                    02-08-10
      Street-Address

Which structure rule ? 2__
```

b. From Mask 5, choose 7 for the structure rule:

```
Mask 5        (Add Object)

Which structure rule ? 7

(Mask 6)          DIRECTORY SYSTEM          Add object

Object Name

Country-Name          __
Organization-Name     ____________________
Org.-Unit-Name        ____________________
Common-Name           ____________________
Common-Name           ____________________

Structural Object class: Application-Entity
Auxiliary object class: NO
```

c. From Mask 6, enter the remote DSA object name (DSA DN), choose Directory-Service-Agent for the structural object class (use the space bar to scroll through the selections), and use the default for the auxiliary object class (no):

Mask 6 (Add Object)

Country-Name **us**
Organization-Name **acme**
Org.-Unit-Name **dap11**
Common-Name **dsa**
Common-Name **dsa-acme**

Structural Object class: **Directory-Service-Agent**
Auxiliary object class: **NO**

(Mask 6d) DIRECTORY SYSTEM Add Object

Presentation-Address
CDS-Cell
CDS-Replica
Common-Name
DSA-Type
Description
Knowledge-Information
Locality-Name
Master-Knowledge
Org.-Unit-Name
Organization-Name
See-Also
Suppl.-Applic.-Context
User-Password

d. From Mask 6d, use the arrow keys to move the cursor to DSA-Type (Presentation-Address is highlighted by default), select DSA-Type by pressing RETURN, and then press the **f2 MENU** softkey:

Mask 6d (Add Object)

Presentation-Address
DSA-Type

(Mask 7) DIRECTORY SYSTEM Add Object

Attributes:

Name : DSA-Type
Value: _____
_____

Name : _____
Value: _____
_____

Name : _____
Value: _____
_____

e. From Mask 7, enter default' as the DSA-Type value (you are defining the DSA from step c as the default DSA). Press the **f2 MENU** softkey:

Mask 7 (Add Object)

Value: **default'**
(Mask 7a) DIRECTORY SYSTEM Add Object

P-Selector: _____
S-Selector: _____
T-Selector: _____

NSAP-address 1: _____
NSAP-address 2: _____
NSAP-address 3: _____
NSAP-address 4: _____
NSAP-address 5: _____

f. From Mask 7a, enter Client/Server for the T-Selector and TCP/IP!internet=15.11.000.000+port=yyyyy for the NSAP-address 1 where 15.11.000.000 is the system's IP address and yyyyy is any available port number. Then, press the **f2 MENU** softkey:

Mask 7a (Add Object)

T-Selector: **Client/Server**

NSAP-address 1: **TCP/IP!internet=15.11.000.000+port=21785**

You have successfully added the remote DSA object name to the DUA cache and configured and initialized the GDS client within a distributed environment.

Initializing the Directory Using Files

You can initialize the directory without using **gdssysadm** by creating a script and reading it into the tool **gdsditadm**. The following scripts complete all steps in the "Initializing the Client/Server Directory Service and the "Initializing the Client Directory Service" sections. Similar scripts are also available online in the directory **/opt/dcelocal/usr/examples/gds**.

Initializing the Client/Server Directory Service

The following script adds the client address, the local DSA object name, and the remote DSA object name to the DUA cache. The example script is named **client_server_initdir.gds**.

client_server_initdir.gds

```
:*************************************************************************************:
:*** To run this script, client_server_initdir.gds, enter:                         ***:
:*** gdsditadm < client_server_initdir.gds                                         ***:
:*** This script helps to initialize directory id 1 as a                          ***:
:*** Client/Server system                                                          ***:
:*** This script will set up the local system as                                   ***:
:***    DSA Name:  /c=us/o=acme/ou=dap11/cn=dsa/cn=dsa-acme                        ***:
:***    ip-address:  15.11.000.000                                                 ***:
:***    port number:  21010                                                        ***:
:*** This script also configures the remote server machine with the                ***:
:*** following information                                                         ***:
:***    DSA Name:  /c=us/o=widgets-r-us/ou=doodad/cn=dsa/cn=dsa-wru                ***:
:***    ip-address:  15.22.000.000                                                 ***:
:***    port number:  21025                                                        ***:
:*************************************************************************************:

:****** TEST  (INITIALIZE CACHE)  ******:
:directory id:1
:password:
:Country:
:Organization:
:Organizational unit:
:common name:
:options0:Logon to the DUA Cache
:*****Select Object Administration*****:
:Funtion:1
:***Adding the client address to the local DUA cache***:
:Operation:05
```

```
:P-Selector:
:S-Selector:
:T-Selector:Client/Server
:Net-address 1:TCP/IP!internet=127.0.0.1+port=21015
:Net-address 2:
:Net-address 3:
:Net-address 4:
:Net-address 5:
:*****Adding the local DSA object name to the DUA cache*****:
:***Add Object us/acme/dap11/dsa/dsa-acme to the DUA cache***:
:Operation:01
:Object Type Number:07
:country:us
:organization:acme
:Organizational Unit:dap11
:Common-Name:dsa
:Common-Name:dsa-acme
:ObjectClass:Directory-Service-Agent
:Auxiliary Object Class:NO
:Attribute Name1:Presentation-Address
:Attribute Name2:DSA-Type
:Attribute Name3:
:Attribute Name4:
:Attribute Name5:
:More:
:attribute Name:DSA-Type
:attribute Value:default/local'
:attribute Value:
:attribute Name:
:attribute Value:
:attribute Value:
:attribute Name:
:attribute Value:
:attribute Value:
:P-Selector:
:S-Selector:
:T-Selector:Client/Server
:Net-address 1:TCP/IP!internet=15.11.000.000+port=21010
:Net-address 2:
:Net-address 3:
:Net-address 4:
:Net-address 5:
:*****Adding the remote DSA object name to the DUA cache*****:
:**Add object us/widgets-r-us/dooddad/dsa/dsa-wru to the cache**:
:Operation:01
:Object Type Number:07
:country:us
:organization:widgets-r-us
```

```
OrganizationalUnit:doodad
:Common-Name:dsa
:Common-Name:dsa-wru
:ObjectClass:Directory-Service-Agent
:Auxiliary Object Class:NO
:Attribute Name1:Presentation-Address
:Attribute Name2:
:Attribute Name3:
:Attribute Name4:
:Attribute Name5:
:More:
:P-Selector:
:S-Selector:
:T-Selecotr:Remote-DSA_Client/Server
:Net-address 1:TCP/IP!internet-15.22.000.000+port=21025
:Net-address 2:
:Net-address 3:
:Net-address 4:
:Net-address 5:
:operation:00
:Function:0
:*****End of script client_server_initdir.gds *****:
```

Initializing the Client Directory Service

The following script adds the client address and the remote DSA object name to the DUA cache. The example script is named **client_initdir.gds.**

client_initdir.gds

```
:*****************************************************************************:
:*** To run this script, client_initdir.gds, enter:  gdsditadm < client_initdir.gds  ***:
:*** This script helps to initialize directory id 1 as a                          ***:
:*** Client system                                                                ***:
:*** This script will set up the default system as                                ***:
:***    DSA Name:  /c=us/o=acme/ou=dap11/cn=dsa/cn=dsa-acme                       ***:
:***    ip-address:  15.11.000.000                                                ***:
:***    port number:  21785                                                       ***:
:*****************************************************************************:
:****** TEST  (INITIALIZE CACHE)  ******:
:directory id:1
:password:
:Country:
:Organization:
:Organizational unit:
:common name:
:options():Logon to the DUA Cache
:*****Select Object Administration*****:
:Funtion:1
:***Adding the client address to the local DUA cache***:
:Operation:05
:P-Selector:
:S-Selector:
:T-Selector:Client
:Net-address 1:TCP/IP!internet=127.0.0.1+port=21775
:Net-address 2:
:Net-address 3:
:Net-address 4:
:Net-address 5:
:*****Adding the local DSA object name to the DUA cache*****:
:***Add Object us/acme/dap11/dsa/dsa-acme to the DUA cache***:
:Operation:01
:Object Type Number:07
:country:us
:organization:acme
:Organizational Unit:dap11
:Common-Name:dsa
:Common-Name:dsa-acme
:ObjectClass:Directory-Service-Agent
:Auxiliary Object Class:NO
```

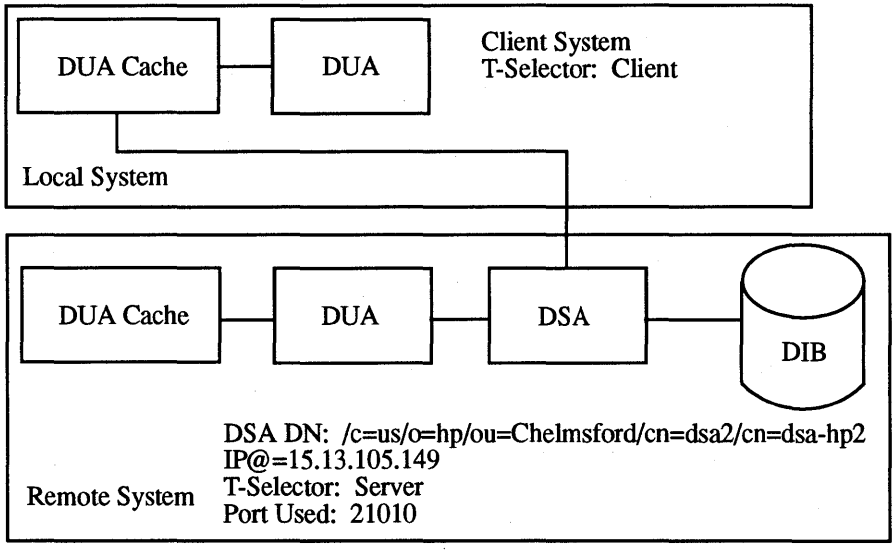
```
:Attribute Name1:Presentation-Address
:Attribute Name2:DSA-Type
:Attribute Name3:
:Attribute Name4:
:Attribute Name5:
:More:
:Attribute Name:DSA-Type
:attribute Value:default'
:attribute Value:
:attribute Name:
:attribute Value:
:attribute Value:
:attribute Name:
:attribute Value:
:attribute Value:
:P-Selector:
:S-Selector:
:T-Selector:Client/Server
:Net-address 1:TCP/IP!internet=15.11.000.000+port=21785
:Net-address 2:
:Net-address 3:
:Net-address 4:
:Net-address 5:
:*****End of script client_initdir.gds *****:
```

Online Examples

The following are online example files found in the **/opt/dcelocal/usr/examples/gds** directory: dap.cmd, loop_back.cmd, nodeA.cmd, nodeB.cmd, gds_intercell_demo.sh, and profile.demo. Each file can be modified and used to configure your system.

dap.cmd

The file /opt/dcelocal/usr/examples/gds/dap.cmd configures the local system as a client system and uses an already configured remote system. Each system has the following characteristics which can be modified:



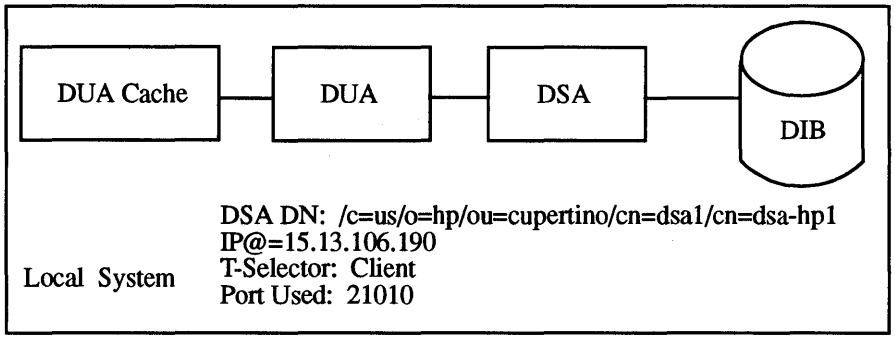
The remote system must already be configured before running dap.cmd.

To set up a client system on your local system, modify dap.cmd and type the following:

gdsditadm < dap.cmd

loop_back.cmd

The file /opt/dcelocal/usr/examples/gds/loop_back.cmd configures the local system as a client/server system. The local system has the following characteristics which can be modified:

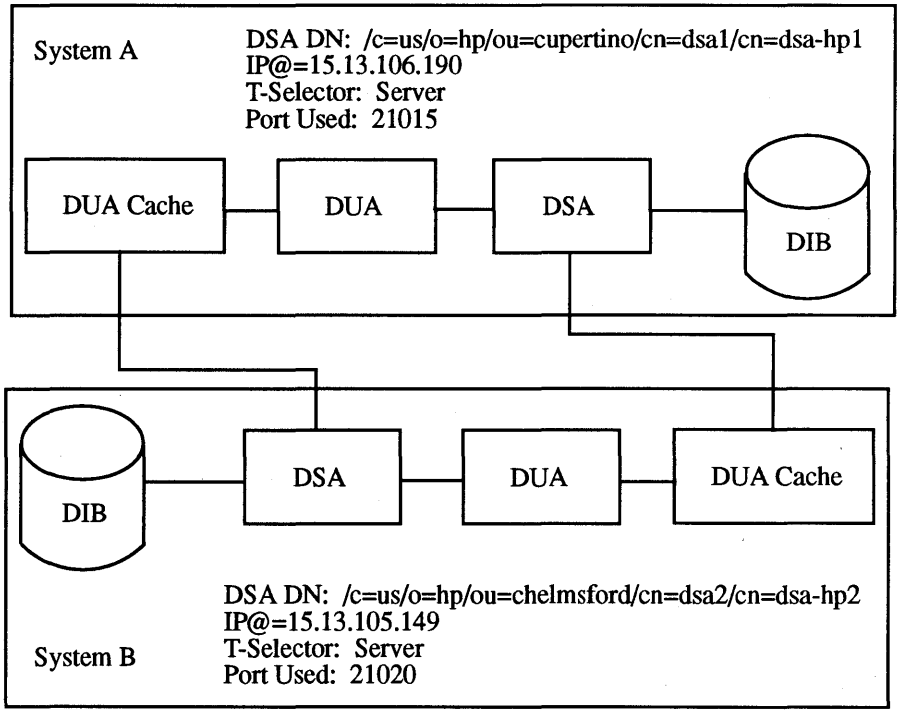


To set up a client/server system on your local system, modify loop_back.cmd and type the following:

gdsditadm < loop_back.cmd

nodeA.cmd and nodeB.cmd

The files /opt/dcelocal/usr/examples/gds/nodeA.cmd and /opt/dcelocal/usr/examples/gds/nodeB.cmd configure two systems as client/server systems. nodeA.cmd must be run on System A and nodeB.cmd must be run on System B. Each system has the following characteristics which can be modified:



To set up the client/server system on System A, modify nodeA.cmd on System A and type the following:

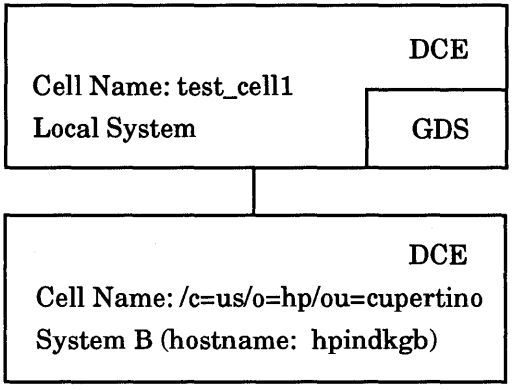
gdsditadm < nodeA.cmd

To set up the client/server system on System B, modify nodeB.cmd on System B and type the following:

gdsditadm < nodeB.cmd

gds_intercell_demo.sh and profile.demo

The files /opt/dcelocal/usr/examples/gds/gds_intercell_demo.sh and /opt/dcelocal/examples/gds/profile.demo configure the local system for intercell communication. The local system has the cell name configured as a CDS name space while System B has the cell name configured as an X.500 name space.



Do the following on the local system:

1 Check that DCE is running and the cell name is configured as a CDS cell name space (for example, CELL=test_cell1).

2 Check that the gdad process (GDA server) is running on the local system.

3 Set up remsh (remote shell) between the local system and System B.

4 Modify the remote variables in profile.demo (hostname, DCE administration account, and password).

5 Save directory ID 1 if GDS is already configured (gds_intercell_demo.sh will overwrite any existing information for directory ID 1).

6 Run **dce_login <dce_admin> <dce_password>**.

Do the following on System B:

1 Check that DCE is running and the cell name is configured as an X.500 cell name space (for example, CELL=c=us/o=hp/ou=cupertino). System B's cell name must contain the following attribute types: country, organization, and organizational unit.

GDS does not have to be installed on System B.

To configure the local system to communicate with System B, on the local system, type:

gds_intercell_demo.sh

If the script successfully runs, the following displays:

```
-------------------------------------------------------------------------------
|                  *** DEMO ***                                               |
|                                                                             |
|           DCE INTERCELL COMMUNICATION OVER GDS                              |
|                                                                             |
-------------------------------------------------------------------------------
Checking DCE processes... done.
Checking GDS processes activate... done.
Creating directory id ... done.
Bringing up GDS processes... done.
Initializing directory id ... done.
Getting remote cell information... done.
Adding intercell object ... done.
Executing rgy_edit() ... done.

---------- Verify intercell communication ----------
cmd: cdscp show cell /.../c=us/o=osf/ou=lab as gds
                    SHOW
                      CELL   /.../c=us/o=osf/ou=lab
                        AT   1993-12-14-13:16:49
    Namespace Uuid = 61b11e68-f8b8-11cc-bb97-08000948fb12
  Clearinghouse Uuid = 5ff264f6-f8b8-11cc-bb97-08000948fb12
Clearinghouse Name = /.../c=us/o=osf/ou=lab/hpindkgb_ch
          Replica Type =   Master


                        Tower = ncacn_ip_tcp:15.13.105.149()
                      Tower = ncacn_ip_tcp:15.13.105.149()
                      Tower = ncadg_ip_udp:15.13.105.149()
```

```
                Tower = ncadg_ip_udp:15.13.105.149[]
          ****************************
cmd: cdscp show dir /.../c=us/o=osf/ou=lab/subsys

                  SHOW
            DIRECTORY  /.../c=us/o=osf/ou=lab/subsys
                    AT  1993-12-14-13:16:54
    RPC_ClassVersion = 0100
             CDS_CTS = 1993-12-14-21:07:20.246920100/08-00-09-48-fb-12
             CDS_UTS = 1993-12-14-21:07:21.095973100/08-00-09-48-fb-12
     CDS_ObjectUUID = 74b32c9a-f8b8-11cc-bb97-08000948fb12
        CDS_Replicas = :
 Clearinghouse UUID = 5ff264f6-f8b8-11cc-bb97-08000948fb12
                Tower = ncacn_ip_tcp:15.13.105.149[]
                Tower = ncacn_ip_tcp:15.13.105.149[]
                Tower = ncadg_ip_udp:15.13.105.149[]
                Tower = ncadg_ip_udp:15.13.105.149[]
          Replica type = master
 Clearinghouse Name = /.../c=us/o=osf/ou=lab/hpindkgb_ch
          CDS_AllUpTo = 1993-12-14-21:07:21.218418100/08-00-09-48-fb-12
    CDS_Convergence = medium
    CDS_ParentPointer = :
          Parent's UUID = 61b11e68-f8b8-11cc-bb97-08000948fb12
                Timeout = :
             Expiration = 1993-12-14-13:07:20.250
             Extension = +1-00:00:00.00010.000
              MyName = /.../c=us/o=osf/ou=lab/subsys
 CDS_DirectoryVersion = 3.0
     CDS_ReplicaState = on
     CDS_ReplicaType = master
        CDS_LastSkulk = 1993-12-14-21:07:21.218418100/08-00-09-48-fb-12
      CDS_LastUpdate = 1993-12-14-21:07:23.767064100/08-00-09-48-fb-12
      CDS_RingPointer = 5ff264f6-f8b8-11cc-bb97-08000948fb12
           CDS_Epoch = 75031a98-f8b8-11cc-bb97-08000948fb12
  CDS_ReplicaVersion = 3.0
------------------- done --------------------
```

Administering GDS

This section describes how to use the tools to administer HP DCE/9000 GDS.

Overview

You have several options when administering GDS:

1 Run **gdssysadm** from the menu-driven interface.

2 Run **gdssysadm** from the command line.

3 Run **gdsditadm** from the command line.

4 Run **gdscacheadm** from the command line.

Running gdssysadm from the Menu-Driven Interface

From the **gdssysadm**'s menu-driven interface, you can do the following:

1 Administer the directory information tree (this topic is covered in the "Object Administration" section in the *OSF DCE Administration Guide – Extended Services* manual).

2 Configure the directory system (this topic is covered in the "Configuring GDS" section).

3 Activate the directory system installation.

4 Deactivate the directory system installation.

5 Save local data to a disk, tape, or file.

6 Restore saved data from a disk, tape, or file.

7 Display directory system status information.

8 Activate tracing (this topic is covered in the "Troubleshooting GDS" section).

9 Deactivate tracing (this topic is covered in the "Troubleshooting GDS" section).

Starting gdssysadm

To start **gdssysadm**, do the following:

a. Log in as **root** on the system you wish to configure.

b. Make sure that **/opt/dcelocal/bin** is in your command search path:

 # export PATH=/opt/dcelocal/bin:$PATH (Bourne/Korn shell)

% setenv PATH /opt/dcelocal/bin:$PATH (C shell)

c. Make sure the NLSPATH environment variable is set to **/opt/dcelocal/nls/msg/en_US.ASCII/%N.cat:**

 # export NLSPATH=/opt/dcelocal/ nls/msg/en_US.ASCII/%N.cat

% setenv NLSPATH=/opt/dcelocal/ nls/msg/en_US.ASCII/%N.cat

d. Make sure the TERM environment variable is set to **hpterm**:

#export TERM=hpterm

%setenv TERM hpterm

e. Run **gdssysadm:**

 # gdssysadm

```
(diradm)          DIRECTORY SYSTEM

a - Administration of the directory information tree
c - Configuration of a directory system
b - Activation of a directory system installation
d - Deactivation of a directory system installation
s - Saving of local data to diskette/tape/file
r - Restoring of saved data from diskette/tape/file
f - Further functions

Your selection! >
```

Activating the Directory System Installation

To activate the directory system installation, do the following:

a. Start **gdssysadm**.

b. From diradm, enter b:

```
diradm

Your selection! > b
```

If you receive the error message "The directory system is active!", press RETURN. The directory system is already activated. If you made any changes to the configuration, you must first deactivate and then reactivate the directory system for these changes to take affect.

Deactivating the Directory System Installation

To deactivate the directory system installation, do the following:

a. Start **gdssysadm**.

b. From diradm, enter d:

```
diradm

Your selection! > d
```

If you receive the error message "The directory system isn't active!", press RETURN. The directory system is already deactivated.

Saving the Local Data to a Disk, Tape, or File

To save the local data to a disk, tape, or file, do the following:

a. Start **gdssysadm**.

b. From diradm, enter s:

```
diradm

Your selection! > s

(savepar)          DIRECTORY SYSTEM          Save Data

For which directory ID do you wish to
save the local data ? (1-20): 1

On which medium do you wish to save the local data ? Diskette
```

c. To save the local data to a disk (or tape), select the directory ID number and Diskette (or Tape) for the medium on which you wish to save the local data (use the space bar to scroll through the selections). After pressing RETURN, enter a password if you want to protect the saved data files, and choose if you want to format the disk (use the space bar to scroll through the selections):

```
savepar       (Save Data)

For which directory ID do you wish to
save the local data ? (1-20): 1

On which medium do you wish to save the local data ? Diskette

Security password, if required: _____

Do you wish to format the media ? No
```

All the local data files from the local DSA and DUA cache belonging to the directory system are saved.

d. To save the local data to a file, select the directory ID number and File for the medium on which you wish to save the local data (use the space bar to scroll through the selections). After pressing RETURN, enter the file name and a password if you want to protect the saved data files:

```
savepar        (Save Data)

For which directory ID do you wish to
save the local data ? (1-20): 1

On which medium do you wish to save the local data ? File

Name of the file : _____________________________

Security password, if required: _____________
```

All the local data files from the local DSA and DUA cache belonging to the directory system are saved.

Restoring Saved Data from a Disk, Tape, or File

To restore saved data from a disk, tape, or file, do the following:

a. Start **gdssysadm.**

b. From diradm, enter r:

```
diradm

Your selection! > r

(respar)          DIRECTORY SYSTEM          Restore Data

For which directory ID do you wish to restore the
local data ? (1-20): 1

From which medium should the data be read ? Diskette
```

c. To restore the saved data from a disk (or tape), select the directory ID number and Diskette (or Tape) for the medium from which the data should be read (use the space bar to scroll through the selections). After pressing RETURN, enter the password if you used one to protect the saved data files:

```
respar        (Save Data)

For which directory ID do you wish to restore the
local data ? (1-20): 1

From which medium should the data be read ?: Diskette

Security password: _____

Attention: Your existing data will be overwritten !!!
```

All the local data in the local DSA and DUA cache belonging to the directory system are overwritten. All the data saved on the disk or tape are restored.

d. To restore the saved data from a file, select the directory ID number and File for the medium from which the data should be read (use the space bar to scroll through the selections). After pressing RETURN, enter the file name and a password if you want to protect the saved data files:

```
savepar        (Save Data)

For which directory ID do you wish to restore the
local data ? (1-20): 1

From which medium should the data be read ?: File

Name of the file : _____________________________

Security password: _____________

Attention: Your existing data will be overwritten !!!
```

All the local data in the local DSA and DUA cache belonging to the directory system are overwritten. All the data saved in the file are restored.

Displaying Directory System Status Information

To display directory status information (directory system status, list of processes, tracing status), do the following:

a. Start **gdssysadm**.

b. From diradm, enter f:

```
diradm

Your selection! > f

(diradm)          DIRECTORY SYSTEM

i - Display of directory system status information
l - Activation of the 'trace' system
t - Deactivation of the 'trace' system

Your selection! > i
```

c. From diradm, enter i:

```
diradm

Your selection! > i

(info)          DIRECTORY SYSTEM          Status Information

The directory system is active (existing processes ->):
1 DUA cache process
1 C-stub process
1 S-stub process(es)
2 DSA process(es)
1 IPC monitoring process

Status of the 'trace' system: active

To continue please press <CR>
```

The information displayed is for a client/server system.

Administering GDS from the Command Line

The DUA cache, directory database, and directory system can be administered from the command line using the following commands: **gdscacheadm** (cache administration program), **gdsditadm** (directory database administration program), and **gdssysadm** (directory system administration program). Running these commands without specifying any options starts the menu interface.

You can find a description of the options for these commands in the "Directory Service Commands" chapter of the *OSF DCE Administration Reference* manual.

Troubleshooting GDS

This section describes the tracing and logging that is available with HP DCE/9000 GDS. It also contains a brief list of error messages, causes, and actions.

Tracing and Logging

Each can generate its own log file. Tracing must be activated from **gdssysadm** before these log files are generated.

Activating and Deactivating Tracing and Logging

Tracing and logging can be activated or deactivated for all GDS processes or for just **gdssysadm**.

Activating and Deactivating Tracing and Logging for All GDS Processes

To activate or deactivate tracing and logging for all GDS processes, do the following:

1 Start **gdssysadm**.

   a. Log in as **root**.

   b. Make sure that **/opt/dcelocal/bin** is in your command search path.

   c. Make sure that the NLSPATH environment variable is set to **/opt/dcelocal/nls/msg/en_US.ASCII%N.cat**.

   d. Make sure the TERM environment variable is set to **hpterm**.

e. At the HP-UX prompt, type **gdssysadm**.

```
(diradm)          DIRECTORY SYSTEM

a - Administration of the directory information tree
c - Configuration of a directory system
b - Activation of a directory system installation
d - Deactivation of a directory system installation
s - Saving of local data to diskette/tape/file
r - Restoring of saved data from diskette/tape/file
f - Further functions

Your selection! >
```

2 **From diradm, choose f for further functions:**

```
diradm

Your selection! > f

(diradm)          DIRECTORY SYSTEM

i - Display of directory system status information
l - Activation of the 'trace' system
t- Deactivation of the 'trace' system

Your selection! >
```

3 **From diradm, choose either l to activate tracing and logging or t to deactivate tracing and logging for all GDS processes.**

Activating and Deactivating Tracing and Logging for Just gdssysadm

To activate or deactivate tracing and logging for just **gdssysadm**, do the following:

1 Start **gdssysadm**. See steps 1a - 1e from the previous section ("Activating and Deactivating Tracing and Logging for All GDS Processes") for instructions on how to start **gdssysadm**.

2 From diradm, choose either X to activate tracing and logging or x to deactivate tracing and logging for just **gdssysadm**. These choices do not appear on the diradm menu.

Log Files

The following is a list of the processes that are activated or deactivated for tracing and logging and the directory name where the process' log file is located:

Process	Directory Name
Cache	/opt/dcelocal/var/adm/directory/gds/cache
C-stub	/opt/dcelocal/var/adm/directory/gds/cstub
S-stub	/opt/dcelocal/var/adm/directory/gds/stub
DSA	/opt/dcelocal/var/adm/directory/gds/dsa/dir<id>
gdssysadm	/opt/dcelocal/var/adm/directory/gds/adm
Monitor	/opt/dcelocal/var/adm/directory/gds/adm
gdscacheadm or gdsditadm	$D2_LOG_DIR or $HOME if D2_LOG_DIR is not set

Reading Log Files

Some log files must be read using special tools. The following is a list of the log file names and the tool used to read the log file. Log files not listed are readable ASCII files.

File Name	Tool
log_<pid>.l1, log_<pid>.l2, ...	gdsstep <file name>
CMXLa<pid>, CMXLb<pid>, ...	gdscmxl -DXV <file name>

where <pid> is the process ID number.

NOTE If GDS is deactivated and reactivated, all old log files are deleted and new log files are created.

Error Messages

Error Message	'*' not allowed in object name
Cause	An * (asterisk) has been entered in the object name.
Action	Remove the asterisk from the object name.

Error Message	Attribute value not allowed
Cause	The attribute value entered is not in the expected format.
Action	Make sure the attribute value is in the expected format. For example, the attribute name DSA-Type only accepts the following values: default', local', or default/local'.

Error Message	Cache entry for default or local DSA fails
Cause	A connection to the DSA or DUA cache cannot be made.
Action	Make sure the directory system is activated and that the directory ID specified for the DSA or DUA cache exists.

Error Message	Can't format media volume
Cause	The media (tape or disk) cannot be formatted.
Action	Check that the media is loaded and not write-protected.

Error Message	Can't read data from file
Cause	The file from which data is being read does not exist, does not contain the files for the specified directory ID, or has been corrupted.
Action	Make sure that the directory ID is correct, the file exists, and that the data is being read from the correct file (the file contains the information for the specified directory ID). If the directory ID is correct and you are using the correct file, the file may have been corrupted. Restore a copy of the file from backup and try restoring the data again.

Error Message	Can't read data from media volume
Cause	The media (tape or disk) from which data is being read does not exist, does not contain the files for the specified directory ID, or has been corrupted.
Action	Make sure that the directory ID is correct, the media exists, and that the data is being read from the correct media (the media contains the information for the specified directory ID). If the directory ID is correct and you are using the correct media, the media may have been corrupted.

Error Message	Can't read file list
Cause	The media (tape or disk) or file from which data is being read does not contain the files for the specified directory ID.
Action	Make sure that the directory ID is correct and that the data is being read from the correct media or file (the disk, tape, or file contains the information for the specified directory ID).

Error Message	Can't read file list from file
Cause	The file from which data is being read does not exist, does not contain the files for the specified directory ID, or has been corrupted.
Action	Make sure that the directory ID is correct, the file exists, and that the data is being read from the correct file (the file contains the information for the specified directory ID). If the directory ID is correct and you are using the correct file, the file may have been corrupted. Restore a copy of the file from backup and try restoring the data again.

Error Message	Can't read file list from media volume
Cause	The media (tape or disk) from which data is being read does not exist, does not contain the files for the specified directory ID, or has been corrupted.
Action	Make sure that the directory ID is correct, the media exists, and that the data is being read from the correct media (the media contains the information for the specified directory ID). If the directory ID is correct and you are using the correct media, the media may have been corrupted.

Error Message	Can't write data to file
Cause	Data cannot be written to the file specified.
Action	Check that the directory to which you are writing exists and that you have write permissions for that directory.

Error Message	Can't write data to media volume
Cause	Data cannot be written to the media (tape or disk) specified.
Action	Check that the media is loaded, formatted, and is not write-protected.

Error Message	Configuration information already exists
Cause	The configuration information for the directory ID you have specified already exits.
Action	Try modifying the existing information for the directory ID instead of creating it; or create the same information for a new directory ID. If you modify existing information, be sure to deactivate and reactivate the system so that these modifications are read in.

Error Message	Configuration information doesn't exist
Cause	The configuration information for the directory ID you supplied does not exist or the directory system is not configured or activated.
Action	Make sure that the directory ID is correct and make sure that the system is configured and activated. If you are trying to save information, make sure that the directory ID is configured for the directory system. If you are trying to restore information, make sure that the data is being read from the correct medium (the disk, tape, or file contains the information for the specified directory ID).

Error Message	The directory system is active
Cause	You tried to activate an already active directory system or you are trying to delete configuration data while the directory system is active.
Action	If you are trying to activate new configuration information, deactivate the system before reactivating it. If you are trying to delete configuration data, deactivate the system first. Then delete the configuration data. Otherwise, the system is already active and does not need to be activated.

Error Message	The directory system isn't active
Cause	You tried to deactivate an already deactivated directory system.
Action	The system is already deactivated. Press RETURN to continue.

Error Message	The directory system isn't configured
Cause	You are trying to perform a function on a system that isn't configured.
Action	Configure the directory system.

Error Message	End of list of selected AT entries reached
Cause	There is no more information to display.
Action	Press RETURN to continue. To exit the display, press the **f7 CANCEL** softkey.

Error Message	End of list reached
Cause	There is no more information to display.
Action	Press RETURN to continue. To exit the display, press the **f7 CANCEL** softkey.

Error Message	Error while reading NLS file; msg_set = 1 msg_no = 1 Fatal ERROR: While accessing NLS file!!!
Cause	The NLSPATH environment variable is not set.
Action	Make sure the NLSPATH environment variable is set to **/opt/dcelocal/nls/msg/en_US.ASCII/%N.cat**: **#export NLSPATH=/opt/dcelocal/nls/msg/en_US.ASCII/%N.cat** (Bourne/Korn shell) **%setenv NLSPATH=/opt/dcelocal/nls/msg/en_US.ASCII/%N.cat** (C shell)

Error Message	Error while reading shadowing jobs
Cause	You are trying to update the DUA cache of a non-existent directory ID.
Action	Make sure the directory ID is correct.

Error Message	File doesn't exist
Cause	The file name you specified does not exist.
Action	Make sure the file name and directory path you specified are correct. Also, make sure you have write permission for the file.

Error Message	(rgy_edit) Incomplete cell add - Clock skew too great (dce/krb)
Cause	The clocks of the remote and local system differ by a large margin.
Action	Set the clock on your local system to match the clock on the remote system.

Error Message	(rgy_edit) Incomplete cell add - Registry server unavailable.
Cause	The local system cannot communicate with the security server.
Action	Make sure the system that is running the security is up and running. On the local system, make sure that the **gdad** and **secd** processes are running.

Error Message	Input not finished with ‘
Cause	One or more values entered for the attributes does not end with an ‘ (apostrophe).
Action	Make sure to add an ‘ (apostrophe) at the end of each value. If this value is in hexadecimal format, the value must start with an x’ (the letter “x” followed by an apostrophe) and end with an ‘ (apostrophe).

Error Message	Internal error
Cause	The IP address or port number specified does not exist or the incorrect net address syntax was used.
Action	Check that the IP address is valid and the port number is not being used. Also check the syntax of the net address for typographical errors including incorrect use of upper or lowercase letters.

Error Message	Invalid CDS-Cell value
Cause	You have entered an incorrect CDS-Cell value.
Action	Enter a valid CDS-Cell value.

Error Message	Invalid configuration information
Cause	The configuration information supplied is not valid.
Action	Enter valid configuration information. If you are restoring information, make sure that the data is being read from the correct medium (the disk, tape, or file contains the information for the specified directory ID).

Error Message	Invalid Directory-ID
Cause	You have entered an incorrect directory-ID number.
Action	Valid directory-ID numbers range from 1 to 20. Enter a number from 1 to 20.

Error Message	Invalid input
Cause	You entered incorrect information.
Action	Check that you have entered information for the required fields and that it is in the correct format.

Error Message	Invalid net address size
Cause	The size of the net address is incorrect.
Action	Make sure the values entered are correct. For example, a valid NSAP address is "TCP/IP!internet=15.11.000.000+port=12345" and an invalid NSAP address is "TCP/IP!internet=15.11.000.000+port123456".

Error Message	Invalid net address syntax
Cause	The net address entered is not in the correct format.
Action	Use the correct net address syntax. For example, a valid NSAP address could be "TCP/IP!inter-net=15.11.000.000+port=21010". Also check the syntax of the net address for typographical errors including incorrect use of upper or lowercase letters.

Error Message	No connection to DSA/DUA-Cache available
Cause	A connection to the specified DSA or DUA cache cannot be made.
Action	Make sure the directory system is activated and that the directory ID specified for the DSA or DUA cache exists.

Error Message	No objects found
Cause	Information for the object name specified cannot be found.
Action	Make sure that the object name entered is correct. If the object exists, make sure that you are logged in to the DSA or DUA cache where this object exists.

Error Message	No PSAP-Address for client entered
Cause	The PSAP-Address for the client has been entered.
Action	Enter the client's PSAP-Address.

Error Message	Not all parts of the object name are defined
Cause	A field for the object name is blank.
Action	Fill in all the fields for the object name.

Error Message	Object (or superior object) doesn't exist
Cause	The object specified does not exist or the system is not activated.
Action	Make sure the object name entered is correct and that the system is activated.

Error Message	Operation effects multiple DSAs (which is prohibited)
Cause	You are using a directory ID that does not exist.
Action	Use another directory ID.

Error Message	Schema from DSA cannot be read
Cause	The DSA you are trying to read data from may not exist or the system is not activated.
Action	If you are logging on to the DUA cache or DSA for the first time, you can safely ignore this message. Otherwise, check that the directory ID exists, that the configured client address and the local/remote DSA object name are correct, and that the system is activated.

Error Message	The selected function can't be executed
Cause	You are trying to perform a function on a system that is not configured.
Action	Configure the directory system.

Error Message	There is no auxiliary object class for the selected object class
Cause	An auxiliary object class does not exist for the specified object name.
Action	Make sure the object name specified is correct. Otherwise, press RETURN to continue.

Error Message	Top of list reached
Cause	There is no more information to display.
Action	Press RETURN to continue. To exit the display, press the **f7 CANCEL** softkey.

Error Message	Unknown net address type
Cause	The incorrect net address syntax was used.
Action	Check the syntax of the net address for typographical errors including incorrect use of upper or lowercase letters.

Error Message	Unknown operation
Cause	You have entered an incorrect operation.
Action	Enter an operation from the options listed.

Error Message	Wrong selection
Cause	You have entered an incorrect selection.
Action	Enter your selection from the options listed.

WIN AN HP CALCULATOR!

Your comments help us determine how well we meet your needs. Returning this card with your name and address enters you in a quarterly drawing for an HP calculator*.

HP DCE/9000 Version 1.2 Release Notes
B3190-90019 E0194

What operating system and hardware do you use? (Type: `uname -rvm` and write the displayed information on the following line.)

_____ _____ _____

How much have you used this manual?

_____ Extensively _____ Often _____ Occasionally _____ Not at all

----fold here----------fold here----

Complete this section only if you have used this manual. Use the column labeled "NC" if you have no comment or opinion regarding that topic.

	Agree				Disagree		NC
The manual is well organized.	○	○	○	○	○	○	○
It is easy to find information in the manual.	○	○	○	○	○	○	○
It tells me clearly what I need to know.	○	○	○	○	○	○	○
It is easy to perform step-by-step procedures.	○	○	○	○	○	○	○
Overall, the manual meets my expectations.	○	○	○	○	○	○	○

Please take the time to describe any problems you've had or any suggestions that would improve our product/manual. Use additional pages if needed. The more specific your comments, the more useful they are to us. Thank you.

Comments:

----fold here----------fold here----

○ **Check here if you would like a reply.**

** Offer expires 01/01/96.*

↑ *Please tape here* **Please print/type the following information** *Please tape here* ↑

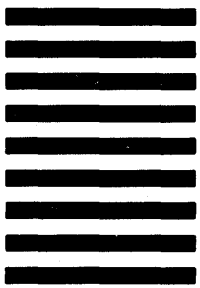
Name: _____ Telephone: _____

Company: _____

Address: _____

City: _____ State: _____ Zip Code/Country: _____

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST CLASS MAIL PERMIT NO. 37 LOVELAND, COLORADO

POSTAGE WILL BE PAID BY ADDRESSEE

Learning Products HP-UX
Hewlett-Packard Company
3404 East Harmony Road
Fort Collins CO 80525-9988

HP DCE/9000 Version 1.2 Release Notes
B3190-90019 E0194

Printed in USA E0194

Manual Part No.
B3190–90019

Manufacturing
Part No.
B3190–90019