Planning and Configuring HP DCE 1.6

First Edition

E0397

B3190-90071
HP DCE/9000 Version 1.6
May 1997

Printed in: U.S.A.

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.

RESTRICTED RIGHTS LEGEND

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.2277013.

Hewlett-Packard Company 3000 Hanover Street Palo Alto, CA 94304 U.S.A.

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.22719(c)(1,2).

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

Contents

1. About HP DCE/9000 Version 1.6

Contents

Contents

2. Migrating to HP DCE 1.6

Contents

3. Before Installing HP DCE/9000 Version 1.6

4. Installing HP DCE 1.6

Contents

Contents

7. Notes on Cell Administration

Contents

About this document

This document describes features of HP DCE/9000 Version 1.6 specific to Hewlett-Packard. For features of standard DCE, see the OSF documentation.

This book is organized as follows:

- Chapter 1 provides an overview of HP DCE 1.6; it includes information about new features, limitation, interoperability and compatibility, changes at the next release, and documentation. Chapter 1 also includes information about DCE Account Manager, Cell Monitor, and the Password Management Server.
- Chapter 2 describes how to migrate from HP DCE 1.3, 1.4, 1.4.1, or 1.5 to HP DCE 1.6.
- Chapter 3 describes hardware and software prerequisites and preinstallation planning for HP DCE 1.6
- Chapter 4 describes installing HP DCE, including the products and file sets that make up HP DCE 1.6.
- Chapter 5 describes configuring HP DCE Cells; Chapter 5 also describes how to configure MC/ServiceGuard with HP DCE.
- Chapter 6 describes HP-UX integrated login and how to integrate it with HP DCE.
- Chapter 7 describes diagnostic tools for cell administration, the enhanced CDS browser, administrating CDS, establishing intercell communication, and miscellaneous notes about cell administration.
- Chapter 8 describes the HP DCE Measurement Service (DMS).

1 About HP DCE/9000 Version 1.6

HP DCE/9000 Version 1.6 (HP DCE 1.6) makes the functionality of OSF DCE Version 1.1 available on HP 9000 Series 700 and Series 800 systems running HP-UX 10.30. HP DCE 1.6 also includes new functionality and bug fixes.

HP DCE/9000 Core Services Software

HP DCE/9000 Version 1.6 is based on OSF DCE Version 1.1 source code, with bug fixes and 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 1.1 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 name space 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 Service, including security server replication and additional security server replication functionality, and the Audit Service.
- Distributed Time Service (DTS); this release supports **ntp**, **null,** and **Spectracom** DTS time providers; it also supports global time servers and DCE time zones.
- Global Directory Agent (GDA), using the Berkeley Internet Naming Daemon (BIND).

The DCE application library is provided as both a shared library (**libdce.sl**) and 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.

Hewlett-Packard strongly recommends the use of shared libraries when building DCE applications. In our opinion, the advantages of shared libraries — smaller executable size, reduced memory requirement, and the ability to make use of forthcoming improvements to **libdce** without rebuilding or relinking binaries — outweigh the modest performance penalty HP has measured when testing a high-volume transaction processing application linked with DCE shared libraries.

HP DCE/9000 Features Added by Hewlett-Packard

Features Added at Previous Releases of HP DCE

HP DCE 1.6 supports the following features that were added to HP DCE/ 9000:

- The HP DCE Account Manager (HP DCE 1.4 and later releases) provides a graphical interface for creating and administering the DCE registry. The Account Manager requires a bit-mapped display. There is no ASCII terminal support. Online help is provided for the Account Manager. See “HP DCE Account Manager” later in this chapter for more information on the Account Manager.
- The HP DCE Cell Monitor (HP DCE 1.4 and HP DCE1.5 only) provides a graphical display of the status of each node in a DCE cell.
- DCM, the DCE Configuration Manager (HP DCE 1.4 and later releases) allows you to configure the nodes in a DCE cell. This tool is accessible via SAM (the HP-UX System Administration Manager) and is documented in online help.
- A set of HP-UX Integrated login utilities that authenticate users via the DCE Security Registry instead of via **/etc/passwd** and **/etc/group**. HP DCE/9000 includes improvements to **login**, **dtlogin**, **su**, **passwd**, **chsh**, **chfn**, **telnet**, and **rlogin**, as well as new HP-UX Integrated versions of **ftpd** and **dtsession** and enhanced support for CDE/PAM. See Chapter 6 for more information about these utilities.
- The DCE cell diagnostic tool **dceping**.

- An enhanced version of the OSF CDS browser (**cdsbrowser**), which has been ported to Release 6 of the X11 Windows system and the Common Desktop Environment (CDE). The browser is accessible through SAM. See the CDS Browser online help (accessible via the CDS Browser **Help** menu) for details.
- Two sets of tools for developing DCE applications are available as separately priced options to HP DCE/9000. For DCE application development in C, HP DCE/9000 Application Development Tools includes a modified IDL compiler (I2DL), tracing and logging facility, error reporting facility, and sample applications. For DCE application development in C++, HP DCE/9000 Object-Oriented DCE (HP OODCE) includes an IDL++ compiler, tracing and logging facility, C++ class library, sample applications, include files, and modified header files for C++ application development.
- **cdsclerk** (new at HP DCE 1.5) no longer runs as separate processes. **cdsclerk** functionality has been merged into the **cdsadv** process. **cdsadv**, therefore, is now the only HP DCE CDS client process.
- **HP's dced** (new at HP DCE 1.5) supports the new **-r** option. This option starts **dced** in remote-update mode, which allows DCE cell administration tasks to be performed by an administrator on a remote machine. In order to help prevent attacks, the **dced** default behavior is to disallow any remote administration.
- HP has enhanced the **dcecp registry connect** command with two new options that support intercell login:

  -acctvalid Marks the local cell account as a valid account. A valid local cell account allows users from the foreign cell to login to nodes in the local cell. The default is invalid.

  -facctvalid Marks the foreign cell account as a valid account. A valid foreign cell account allows users from the local cell to login to nodes in the foreign cell. The default is invalid.

  See “Establishing Peer-to-peer Trust” in Chapter 7 for more information on these important new options.

- HP has added a new **-r** option, which refreshes a user's credentials, to **dce_login**. Users are encouraged to use **dce_login -r** rather than **kinit** to refresh their credentials, since **dce_login -r** uses the more secure DCE Third-party preauthentication protocol, whereas **kinit** uses the less secure Kerberos 5 Timestamps protocol.
- HP has changed the default behavior of its configuration tools to automatically enable audit filtering. In addition, the default behavior of **secd** has been changed to enable audit filtering at start-up, and a new **secd** option, **-noauditfilters**, had been added to disable audit filtering. See "Configuring the DCE Audit Service" in Chapter 5, and the *online secd* man page for more information.
- HP DCE Measurement Service (DMS) to monitor resource utilization and performance of HP DCE 1.6 servers.
- Support for large **uid**s.
- Support for context-switching 64-bit machine registers in DCE threads (**libcma** and **libdce**).

Features Added at HP DCE 1.6

The following features are new at HP DCE 1.6:

- Support for MC/ServiceGuard
- Enhanced support for CDE/PAM and HP-UX Integrated login

In addition, HP DCE 1.6 contains numerous bug fixes.

Features Removed at HP DCE 1.6

The following features were removed at HP DCE 1.6:

- Distributed File Service (see "Installation Notes" in Chapter 4 for information about unconfiguring DFS before installing HP DCE 1.6).
- Global Directory Service.
- HP DCE Cell Monitor.
- The DCE cell diagnostic tool **dceval**.

Version Identification

Version information for individual HP DCE/9000 Version 1.6 components may be obtained via the **/opt/dce/bin/dce_version** utility. This utility prints the version of the installed DCE and can also retrieve **what** strings (see *what (1)*) from HP DCE/9000 programs and libraries. See the *dce_version* man page for information on how to use **dce_version**.

Cell Configuration and Diagnostics

HP DCE supplies two configuration tools with this release:

- **dce_config** is the cell configuration tool provided by OSF, with substantial modifications by Hewlett-Packard.
- DCM, the DCE Configuration Manager, provides a SAM interface to cell management.
- HP's DCE cell validation and diagnostic tool **dceping**.

Common Desktop Environment (CDE) and Online Help

As of HP-UX 10.20 and later releases, the default environment is the Common Desktop Environment (CDE). (HP VUE was available with releases of HP-UX earlier than 10.30.) All HP DCE 1.6 online help and context-sensitive help works in CDE. If you print HP DCE 1.6 online help and context-sensitive help from CDE, the text is not formatted as it is on the screen; only text is printed (graphics are not printed).

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 the **dced** daemon and the DCE library (**libdce.1** and **libdce.a**):

- The U.S./Canada version is available only to HP customers in the United States and Canada. The U.S./Canada version of **libdce** supports use of DES to encrypt RPC argument values, via the "privacy" authentication level, and the use of DES to encrypt **gssapi** messages, via the **gss_seal** “confidentiality requested” flag. The U.S./Canada version of **dced** supports secure remote key table management.

- The Export version is available to all HP customers. The Export version of **libdce** disables the “privacy” authentication level in RPC, the **gss_seal** “confidentiality requested” flag, and all program entry points to DES routines. The Export version of **dced** does not support secure remote key table management.

If an application uses the Export version of the DCE library and specifies the “privacy” level or “confidentiality requested”, the library returns an error at run time. This restriction does not apply to the U.S./Canada version of this release.

See the *dced (1M)* man page for more information about remote key table management support in the two versions of the daemon.

NOTE Users of the Export version of HP DCE 1.6 should start **dced** with the **-c** option. See the *dced* man page for more information.

Limitations of This Release

Some of the limitations described in this section reflect limitations of OSF DCE 1.1; others are limitations specific to this release.

Limitations of OSF DCE 1.1

Following are limitations of OSF DCE 1.1:

- 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 **dcecp** tool to add passwords to those accounts. This information is particularly important to customers who plan on using the HP-UX Integrated login tools (**login**, etc.) with DCE.
- Transitive trust path generation and evaluation, as described in sections 33.1.2 and 33.1.4 of the *OSF DCE Administration Guide — Core Components* is not supported.
- Cell alias/rename is partially supported: creation of cell aliases (**dcecp cellalias create**) is supported; renaming of cells (**dcecp cellalias set**) is not supported. Disregard Sections 21.6.2 and 21.6.3 of the *OSF DCE Administration Guide — Core Components*.
- Cell alias names are not automatically propagated across cell boundaries. Use of cell aliases across cell boundaries is supported when the cell alias name is manually registered in the security name space.

HP DCE 1.6 Limitations on OSF DCE 1.1 Functionality

The following OSF DCE 1.1 functionality is not supported in HP DCE 1.6:

- Distributed File Service
- Global Directory Service

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, and its compatibility with previous versions of HP DCE, and with DCE-related technologies.

Binary Compatibility with Previous HP DCE Releases

HP DCE 1.6 supports binary compatibility with HP DCE 1.2.1 and later releases. Applications linked with the archived HP DCE 1.2, 1.2.1, and 1.3.1 **libdce** are fully compatible with applications built with HP DCE 1.6 libraries. These applications can share login contexts and credentials without loss of data.

In HP DCE 1.6 the DCE_SVC_DEBUG macro was changed to acquire a SVC mutex lock (in earlier releases, this took place in the serviceability library). As a result, HP DCE 1.5 applications that use the DCE_SVC_DEBUG macro are not binary compatible with HP DCE 1.6 applications. To enable binary compatibility, the HP DCE 1.5 applications must be recompiled with HP DCE 1.6 running on the HP-UX 10.30 operating system.

Binary compatibility for statically-linked HP DCE 1.2, 1.2.1, and 1.3.1 applications can be disabled, resulting in minor performance gains and slightly smaller credentials files. By default, binary compatibility is enabled when HP DCE 1.6 is installed and configured. You may disable binary compatibility on a per-host basis with the following commands:

```
#ps -ef|grep dced
#kill <dced PID#>
#/opt/dce/sbin/dced -r
#ps -ef|grep dced
#kill -SIGUSR1 <dced pid#>
#dcecp -local
dcecp> acl mod hostdata -change
{user hosts/$HOST/self criI} -local
dcecp> acl mod hostdata -io -change
{users hosts/$HOST/self cdprw} -local
dcecp> quit
#kill -SIGUSR1 <dced pid#>
dcecp>
dcecp> hostvar set -secbinarycompat off
```

To enable binary compatibility after it has been disabled, do the following:

1. Issue the command:

```
dcecp> hostvar set -secbinarycompat on
```

2. Stop and restart DCE daemons.
3. If using Integrated Login, log out and log in.

   If a statically-linked HP DCE 1.2, 1.2.1, or 1.3.1 application purges a login context (via **sec_login_purge_context**) which an HP DCE 1.6 application had created or refreshed, one of the credential files will not be deleted from the disk. This file is located in **/var/opt/dce/security/creds**. The file name will consist of the unique credential cache ID associated with the login context and a ".data.db" suffix. Administrators may remove this file manually if they wish.

For information about the U.S./Canada version of HP DCE, see the *HP DCE/9000 Version 1.6 U.S./Canda Version Release Note*.

Source Code Compatibility with Previous HP DCE Releases

There are no known source code incompatibilities between HP DCE 1.6 and previous releases.

Interoperability with Other Implementations of OSF DCE

This release has been tested to ensure interoperability with the implementations of OSF DCE on the platforms listed in Table 1-1:

Table 1-1 **HP DCE Interoperability With Other Platforms and DCE Implementations**

Platform	Operating System	DCE Implementation	OSF DCE Version
Digital Alpha	Digital UNIX 3.2-2	Digital DCE V 1.3 (Rev 51)	1.0.3
IBM RS6000	AIX 4.1.4.0	AIX DCE 2.1	1.1
Sun SPARC station	SunOS 5.4 Solaris 2.4	Transarc DCE 1.1	1.1
Dell 450/ME 486	Microsoft DOS 5.0 Microsoft Windows 3.0	Gradient DCE 1.0.2a, 1.0.3	1.0.2, 1.0.3
Dell 450/ME 486	Digital Windows NT	Digital DCE V 1.3	1.0.3
Dell 450/ME 486	IBM OS/2 2.1	IBM DCE 1.1	1.1

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

- The DCE Configuration Manager, DCM, will configure any other HP DCE/9000 Version 1.4x Series 700/800 system. It will also configure versions 1.5, 1.4, 1.4.1, 1.4.2, 1.3.1, 1.2, and 1.2.1 of HP DCE/9000, but some operations may not be supported.
- DCM will discover a cell in its entirety, including non-HP systems provided the non-HP systems have been correctly configured in the CDS name space. (DCM cannot configure non-HP systems.)
- DCM may be run from any DCE/9000 Version 1.6 system within the cell.
- 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 or the **gss_seal** “confidentiality requested” flag 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.

Kerberos Authentication Protocol Compatibility

The DCE Security authentication service implements Kerberos Version 5. DCE Security does not provide backward compatibility support for Kerberos Version 4.

Notes, Cautions and Warnings Regarding This Release

dcecp host Command

All of the operations of the **dcecp host** command are implemented. See the *host (8dce)* man page for syntax and details.

Security and Remote Login Utilities

You can 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 is compromised. The most secure way to perform cell administration is to log in locally to each system you want to administer. The use of Secure Internet Services (SIS) does not provide better security for the purpose of remote DCE cell administration.

Security and Credential Lifetime

DCE credentials consist of Kerberos tickets shared by principals and the security server. The security server encrypts the tickets with a server key. Usually, the credential lifetime for a Kerberos ticket is a defined expiration time.

Hewlett-Packard recommends using Kerberos tickets with a defined expiration time and changing the server keys frequently. Using tickets with an infinite lifetime makes it difficult to automatically change server keys without invalidating the outstanding tickets. It also defeats the automatic key garbage collection, which the **sec_key_mgmt_change_key** operation performs.

ANSI C Requirement for HP DCE/9000

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

This restriction also applies to applications on HP-UX 10.x systems built using the HP-UX user-space threads library (**libcma**).

dce_login -r Option

Starting with HP DCE 1.4, the **-r** option, which refreshes a user's credentials, was added to **dce_login**. Users are encouraged to use **dce_login -r** rather than **kinit** to refresh their credentials, since **dce_login -r** uses the more secure DCE Third-party preauthentication protocol, whereas **kinit** uses the less secure Kerberos 5 Timestamps protocol.

Removing DCE Credentials

A user's DCE credentials (stored in the directory **/var/opt/dce/security/creds**) 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.

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 the *kdestroy (1)* man page for syntax and usage information.

Credentials are automatically removed at system boot.

HP-UX Integrated Login Utilities

The HP-UX Integrated login utilities are installed, but are not activated, by the HP DCE installation and configuration procedure. This is because most systems will require the transfer of account information from **/etc/passwd** to the DCE Security Registry before the system will be useful.

A script, **/usr/sbin/auth.adm** is supplied to activate the utilities once your system has been set up with the needed accounts. See Chapter 6 for more information about using the **/usr/sbin/auth.adm** script.

Do not use the **auth.adm** script to activate the HP-UX Integrated login utilities until *after* you have set up the accounts necessary for your site in the DCE security service registry.

The DCE Audit Service

The DCE Audit Service was first released with HP DCE 1.4.x; the DCE Audit Service provides auditing capabilities for DCE Security and Time services.

By default, all audit events are disabled (not logged). As part of the default DCE configuration start-up, the DCEAUDITFILTERON environment variable is set. When set, the DCEAUDITFILTERON environment variable specifies that audit event filtering must be utilized to enable logging the desired set of audit events.

To enable auditing, the **auditd** server process must be started on any system where auditing is desired. As part of the standard DCE configuration start-up for **auditd**, a set of audit filters is specified for the Security, DTS and **auditd** server processes. (You can modify these filters as necessary for your site.).

You will need to do some planning to determine the degree of audit proper for your site, and to allow for disk space overhead for your audit logs. If you want to do some auditing, such as logging and tracking modifications to the security registry database, audit filtering is highly recommended. By using audit filtering, it is possible to change the types of events being audited dynamically, without needing to restart the servers for the changes to take effect.

Administrators should periodically monitor the size of the Security audit logs on the Security server machines. Each audit trail log consists of two files — the actual trail log file and the associated index file. These logs are in:

```
/var/opt/dce/security/sec_audit_trail
/var/opt/dce/security/sec_audit_trail.md_index
```

Other older audit logs may also be present. These can be found under the same directory, but have a date and time stamp format inserted into the name. As an example:

```
sec_audit_trail.1995-08-31-15-19-52
sec_audit_trail.1995-08-31-15-19-52.md_index
```

For detailed information on the DCE Audit Service, see the *OSF DCE Administration Guide and Reference*. For Audit Service configuration information see Chapter 5 of this manual.

Setting LANG and NLSPATH Environment Variables

English-language users of HP DCE/9000 should set the NLSPATH environment variable to include **/usr/lib/nls/C/%N** or should set NLSPATH to include **/usr/lib/nls/%L/%N** and LANG to **C**. Users who want to use another language should set the NLSPATH environment variable to include **/ usr/lib/nls/%L/%N** and LANG to their preferred language. See the *environ (5)* and *locale (1)* man pages for details on LANG and NLSPATH syntax.

dcecp in Local Mode

When you run **dcecp** in “local” mode (that is, when you start **dcecp** with the **local** option) on a host with **dced** in partial-service mode, there is a possibility that a **dcecp ‘acl modify -add’** command will not work. The interactive **dcecp** session may hang or a Bus Error may be returned. One workaround for this condition is to run **dcecp** in normal mode on a host that is running **dced**, also in normal mode, and then execute **dcecp** again. Alternatively, you can quit out of local mode between **acl modify -add** commands, as follows:

```
dcecp -local
dcecp> acl modify -local foo1 -add ...
dcecp> quit
dcecp -local
dcecp> acl modify -local foo2 -add ...
dcecp> quit
```

dcecp secval Change

For HP DCE 1.6, **dcecp**'s **secval activate** and **secval deactivate** commands are asynchronous. They return before the actual change takes place within **dced**. Therefore, you should use the **secval status** command to verify the state change. Prior to this release, **secval activate** and **secval deactivate** were synchronous and did nott return until the actual state change finished in **dced**. Although future HP DCE/9000 releases may reimplement synchronous **secval activate** and **deactivate** commands, the verification by **secval status** is still recommended.

HP DCE/9000 Interoperability with SharedPrint/UX

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

Features Changing at the Next Release

This section describes OSF DCE and HP DCE features that will not be supported in future releases of HP DCE.

Network Computing System (NCS) Version 1.5.1 compatibility will *not* be supported in the next release of HP DCE:

You should also be aware of likely migration to the POSIX 1003.1c standard for threads.

The rest of this section describes the NCS compatibility and likely changes to support POSIX 1003.1c threads.

NCS 1.5.1 Compatibility

Network Computing System (NCS) Version 1.5.1 applications are compatible with this release. The DCE Remote Procedure Call daemon (**dced**) incorporates the NCS Local Location Broker daemon support (formerly provided by **llbd** or **rpcd**) that NCS 1.5.1 applications require. Because neither the **llbd** or **rpcd** daemon can coexist with **dced** in a cell, the DCE cell configuration tools stop **llbd** or **rpcd** and run **dced** in its place.

Users of NCS-based software (such as NetLS, Omniback, HP MPower, and SharedPrint/UX) should see the section entitled “Note for Users of NCS-based Software” in Chapter 5 for important HP DCE/9000 configuration information.

Future Support for POSIX 1003.1c Threads

The Threads API in HP DCE is likely to migrate eventually from Draft 4 of the POSIX threads standard to the final, ratified 1003.1c standard. This migration will result in source incompatibility, and it is recommended that application developers plan now for this transition. HP plans to preserve binary compatibility and to provide tools to assist in source code migration. However, developers can prepare for this change as follows:

1. Isolate new threads API usage to macros or wrapper APIs.
2. Minimize the use of signals and use only POSIX semantics when programming with signals.

For example, we recommend that threaded applications use only the functions **sigaction**(), **sigprocmask**(), and **sigwait**().

HP DCE 1.6 Documentation

Documentation for HP DCE 1.6 consists of printed and online materials. For a complete list of documentation, including part numbers, see the *HP DCE/9000 Version 1.6 Release Note*.

Printed Documentation

The printed documentation for HP DCE 1.6 consists of HP DCE 1.6 manuals, the OSF DCE documentation set, and two books by O'Reilly and Associates.

The following manuals are written by Hewlett-Packard:

- *Planning and Configuring HP DCE 1.6* (part number B3190-90071) describes the HP changes and additions to OSF DCE 1.1; it also describes installing and configuring HP DCE 1.6 and how to migrate from previous releases of HP DCE to HP DCE 1.6. This document describes both HP DCE 1.6 clients and servers.
- *HP DCE/9000 Version 1.6 for HP-UX 10.30 Release Note* (part number B3190-90070) describes the HP DCE 1.6 documentation set, known problems with HP DCE 1.6, limitations of HP DCE 1.6, required patches (if any), and similar information.
- *HP DCE/9000 Version 1.6 U.S./Canada Software for HP-UX 10.30 Release Note* (part number B3864-90005) describes the US/Canada version of HP DCE 1.6.
- HP DCE/9000 Version 1.6 Application Development Tools for HP-UX 10.30 Release Note (part number B3193-90021) describes two optional products that comprise the HP DCE 1.6 Application Development Tools for HP-UX 10.30. The DCE-C-Tools product assists in the development of HP DCE 1.6 programs written in C. The DCE-OO-Tools product assists in the development of object-oriented programs written in C++.

The OSF DCE 1.1 documentation set published by Prentice-Hall includes the following manuals:

- *Introduction to OSF DCE* (B3190-90046)
- *OSF DCE Command Reference* (B3190-90063)

- *OSF DCE Administration Guide Volume 2 — Core Components* (B3190-90048)
- *OSF DCE DFS Administration Guide and Reference* (B3190-90049)
- *The OSF DCE Application Development Reference* (B3190-90037)
- *OSF DCE Application Development Guide Volume 1 — Introduction and Style Guide* (B3190-90038)
- *OSF DCE Application Development Guide Volume 2 — Core Components* (B3190-90039)
- *OSF DCE Application Development Guide Volume 3 — Directory Services* (B3190-90040)

The following books are published by O'Reilly & Associates:

- *Understanding DCE* (B3190-90018)
- *Guide to Writing DCE Applications* (B3190-90029)

For general information on installing software on HP-UX 10.30 systems, see *Installing HP-UX 10.30 and Updating HP-UX 10.X to 10.30* (B2355-90126).

For general information about programming with threads on HP-UX 10.30, see *Programming with Threads on HP-UX* (B2355-90060).

Online Documentation

The online documentation for HP DCE 1.6 consists of release notes, man pages, HP DCE online help, and embedded online help for the HP DCE Cell Administration tools.

Online Release Notes

An online version of the U.S./Canada release note (*HP DCE/9000 Version 1.6 U.S./Canada Software for HP-UX 10.30 Release Note)* is provided in the directory **/opt/dce/ newconfig/RelNotes**. This directory also contains the release note for the HP DCE client software (*HP DCE/9000 Version 1.6 Client Software for HP-UX 10.30 Release Note*.) The Client Software release note is provided online only.

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.

HP DCE man pages are in the following directories:

```
/opt/dce/share/man
/opt/dce/usr/man
/usr/share/man
```

To read DCE man pages by using the **man** command, include the path names listed above in your MANPATH shell environment variable.

NOTE Use the following command to display the *dts_update* man page:

```
man dts_update
```

HP DCE Online Help

HP DCE/9000 offers a DCE Online Help feature that provides information about various aspects of HP DCE. DCE Online Help is integrated into the HP Help System, so you can access it from the CDE Front Panel help icon.

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

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

- Guide to HP DCE/9000 hardcopy documentation. Provides a list of the manuals available for HP DCE/9000.
- Access to HP DCE/9000 Man Pages.

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 From CDE

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

To access the DCE Online Help from the Front Panel, follow these steps:

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 1.6" 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/dt/bin/dthelpview -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.

Embedded Online Help for HP DCE Cell Administration Tools

The HP DCE DCM, Account Manager, and CDS Browser tools are provided with online help.

HP DMS also has context-sensitive help as provided by HP GlancePlus.

HP DCE Administration Tools

The administration tools are Account Manager, DCM (the Distributed Configuration Manager), and the HP CDS Browser. The Account Manager provides a graphical interface for creating objects in the DCE registry and for administering the DCE registry. HP's DCE Configuration Manager provides a graphical interface for configuring a DCE cell; the HP DCE CDS Browser provides a graphical display for browsing and editing the CDS name space.

All of the HP DCE Administration Tools have extensive online help.

You can invoke the HP DCE Account Manager and the HP CDS Browser from SAM by selecting the **DCE Cell Management** icon.

HP DCE Account Manager

The Account Manager provides a graphical user interface for managing the DCE Registry. With the Account Manager, you can:

- Create and manage users (principals with or without accounts)
- Create and manage groups and organizations
- Manage Registry Policy (Registry IDs, Tickets, Password and Account policy)
- Create and manage Registry Attribute Types (Extended Registry Attributes)
- Manage ACLs (Access Control Lists) on the above

HP DCE Account Manager Documentation

Documentation for the Account Manager is provided as online help.

You may also want to view the *dcecp* man pages. To read the DCE man pages with the man command, you must include **/opt/dce/usr/man** in your MANPATH shell environment variable.

Installing the Account Manager

The Account Manager is included in the DCE-ACCT-MGR fileset. You must install this fileset on each system on which you want to run the Account Manager.

NOTE The Account Manager requires a bit-mapped display; it does not run on ASCII terminals. Also, small bit-mapped displays (such as some PC displays), which may cut off portions of dialog boxes, are unsupported.

Running the Account Manager

If you are running the Account Manager locally, you do not need to set the DISPLAY environment variable ($DISPLAY). If you are running the Account Manager from a remote machine, however, use the following command to set the DISPLAY environment variable to the local machine:

```
export DISPLAY=<localhostname>:0.0
```

If $DISPLAY is not set, the following warning displays:

```
Warning: You are viewing the Account Manager using a remote X
display. Passwords and other confidential information will pan
over the network in clear text, and may be seen by network pirates.
You may wish to exit the Account Manager and run it from a local X
display.
```

Start the Account Manager with the following command:

```
/opt/dce/bin/acctmgr
```

If you want to perform privileged operations (such as registry modifications) with the Account Manager, you must run the Account Manager as the DCE cell_admin principal.

The Account Manager can also be started as follows from SAM:

1. Log in as **root**.
2. Execute **sam** from a shell prompt.
3. Select (double click on) **DCE Cell Management**.
4. Select (double click on) **DCE Account Manager**.

Tips for New Users

- Log into DCE before starting the Account Manager, or use the Login option from within the Account Manager.
- Establish your preferences in the Options “Preferences” dialog box when you initially start the Account Manager.

If you are administering a very large cell, read “Managing Very Large Cells with Account Manager” below.

- It is recommended that you bring up the Assistant from the File menu when you initially start the Account Manager, and iconize it when not in use.
- Where possible, use batch operations and profiles to automate time-consuming repetitive tasks, such as adding multiple users that have similar characteristics.

Managing Very Large Cells with Account Manager

DCE interfaces can be slow to retrieve lists for very large DCE deployments (For example, if the DCE registry is managing many thousands of users). The performance of the Account Manager will be affected in this case. To aid the Account Manager’s performance for very large deployments, take the following steps:

1. In the Options/Preferences dialog, enable the option to “Display -User/Group/Org/Attribute_Type List as Text instead of Icons.”

   The Account Manager requires major resources to map very large lists into iconic display, and this option is needed to bypass that step.

2. In the Options/Preferences dialog, disable the option to “Display -User/Group/Org/Attribute_Type List at Start Up”. This step should be done if any of the following are true:

   - You know the names of the objects you want to manage.
   - You will manage only a subset of objects (for example, users in a certain group).
   - You will ask the Account Manager to read in the list of objects to manage from a file (see #3 below).

   In this step, the first time that you navigate the Account Manager to an object management screen (for example, User Management), the list will be empty.

   Then proceed as follows:

   - If you know the names of the objects to manage, select the appropriate Action. You will be prompted to enter the object name or names.

- If you wish to read in names from a file, or retrieve a partial listing (such as all users in group XXX), select Options/Specify List.

3. If the retrieval of large lists degrades Account Manager performance, you may wish to assist the Account Manager by retrieving the list during an off-time using the **dcecp** command and saving the list to a file. This file could be generated automatically (for example, nightly by a **cron** job).

   Here is a sample script to retrieve and sort the DCE users list:

   ```
   dcecp -c "principal catalog -simplename" | sort > usrlist
   ```

   Once the list has been retrieved, you can read in the list to the Account Manager display from a file. In this case, you must first do step 2 above to set the Preferences dialog; if you do not set the Preferences dialog, the Account Manager will automatically begin to retrieve all objects when you navigate to an object area. Then you navigate to the object area, for example, User Management. To load the list from the local file, select Options/Specify List. In the Specify Users List dialog, select the option “From File” to read in the list.

Account Manager Limitations and Exceptions

The following are limitations and exceptions to Account Manager at HP DCE 1.6:

- User inputs for defining and attaching Registry Attribute types may cause improper tool operation if the inputs contain the following special characters:

{	left curly brace
}	right curly brace
[	left square bracket
]	right square bracket
“	double quotation mark
\	backslash

For other inputs (for example, defining user names and group names), the quote and backslash may cause problems. An example of an illegitimate iname is: **\dos\dir**.

- The Account Manager is not internationalized.
- Descriptive text for Registry Attribute Types is currently limited to three lines of text. The tool provides no way to view descriptions which occupy more than three lines.
- A profile that is created from a View operation (such as “View User”) does not correctly handle an alias name. As a workaround, create profiles including aliases only from Add operation dialogs.
- Cross-cell administration is not supported.
- Importation of user account information from **/etc/passwd** is not supported.
- If a profile directs the removal of a group or organization member, the list of members is retrieved prior to removal, even if preferences state that lists should not be automatically retrieved.

HP Password Management Server

A Password Management Server implements policies for password strength. Sites can implement site-specific policies by writing their own Password Management Server, and attaching appropriate Extended Registry Attributes (ERAs) to the principals that are subject to these policies.

A Password Management Server must implement the interface described in **dce/rsec_pwd_mgmt.idl**.

In order to be configurable by **dce_config** or DCM, the Password Management Server must conform to the following guidelines:

- There must be only one Password Management Server per cell.
- The Password Management Server must execute on the same machine as the master DCE Security Server.
- The binary must be named **pwd_strengthd**.
- The binary must be located in /**opt/dce/sbin**.
- There must be a single option, **-v**, on the command line.
- The server must log any information it generates to **/var/opt/dce/security/pwd_strengthd.log**.
- The server must export its interfaces to CDS in **/.:/subsys/dce/pwd_mgmt/pwd_strength**.
- The server must use keytab file in **/krb5/pwd_strength_tab**.
- The server must use principal name and CDS entry name of **pwd_strength**.
- The server must not depend on any other environment variables or files that must be configured.

Example Sources

Password Management Server sources are supplied in **/opt/dce/share/hpexam**. These are the sources used to build the Password Management Server supplied with the HP DCE release.

Certain files that contain proprietary SecureWare algorithms have been omitted, but stubs are supplied that allow the resulting server to build. Note that certain values of the **pwd_SecureWare_chk** ERA (specifically, values **1** and **2**) are unsupported, and will result in failures to pass strength checking if you attempt to use the example server as described in the documentation. The logfile entry will report that the **pwd_SecureWare_chk** level is not supported.

Build Process

The source code directory for **pwd_mgmt** and the files in it are installed write protected. To build this application, copy the files into a private, writable directory you create. This way the original files will continue to be available for you or others to consult.

cd to the private, writable directory where you copied the source files and type:

```
make -f Makefile.example
```

Your system's **/bin/make** command should successfully build the client and server programs using the Makefile provided, if modified as above.

Unlike the other sample applications, where you are encouraged to generate a new UUID when you make modifications, you must not make changes to **rsec_pwd_mgmt.idl**. **secd** is linked with the client stub for the **rsec_pwd_mgmt** interface so changing the interface UUID will cause communication problems between **secd** and your Password Management Server.

Administrative Setup

The **dce_config** and **pwd_config** files supplied with this DCE release are set up to configure and start up a Password Management Server that conforms to the guidelines listed above.

In order to have the policies implemented by any Password Management Server apply to a given principal, the administrator must attach instances of the following two Extended Registry Attributes to the principal's node in the DCE Registry:

pwd_val_type

The **pwd_val_type** attribute controls the type of password management that applies to a given principal. The values are:

0 — Check passwords entered by this principal using the DCE Registry policy only.

1 — Check passwords entered by this principal using the Password Management Server.

2 — Principal may either choose a password (which is then checked with the Password Management Server), or can use a password that has been generated by the Password Management Server (no additional strength checking is done).

3 — Principal must use a password generated by the Password Management Server.

The HP Account Manager can facilitate the administration of ERAs.

pwd_mgmt_binding attribute

The **pwd_mgmt_binding** attribute specifies the binding to the Password Management Server that will be used for this principal. In future releases, more than one Password Management Server may be supported, but for now, the value of the **pwd_mgmt_binding** attribute must always be:

```
{pwd_mgmt_binding {{dce /.:/pwd_strength pktprivacy secret name} \
{/.:/subsys/dce/sec/pwd_mgmt/pwd_strength}}} \
```

pwd_SecureWare_chk

HP’s default implementation of the Password Management Server uses an additional Extended Registry Attribute to control the level of strength checking algorithm that will be applied to a given principal. The values are:

0 — Use DCE Registry algorithm only (such as, depending on DCE registry policies, check password length, blanks, alphanumeric).

1 — In addition to checking against the DCE Registry algorithm, use a proprietary SecureWare algorithm that verifies the password meets certain tests for non-triviality (not a circular shift of the principal’s name or its reverse, contains at least 2 alphanumeric characters, contains at least one non-alphanumeric character).

2 — In addition to the two previous checks, use a proprietary SecureWare algorithm that verifies the password is not a word (and is not a palindrome, does not contain the same characters as any group or principal name in the DCE Registry, and is not found in the **spell** program’s dictionary).

If a principal does not have an instance of **pwd_SecureWare_chk** attached, then the Password Management Server uses the DCE Registry algorithm only.

The example Password Management Server does not support values **1** or **2** for **pwd_SecureWare_chk**, since these use proprietary SecureWare algorithms. If a principal is configured with a **pwd_SecureWare_chk** value of **1** or **2**, the principal will be unable to change passwords, and the logfile **/var/ opt/dce/security/pwd_strength.log** will report that the **pwd_SecureWare_chk** level is not supported.

An example of a **dcecp** command for configuring a principal with these attributes is:

```
dcecp -c principal modify esmerelda -add { \
 {pwd_val_type 1} \
{pwd_mgmt_binding { \
{dce /.:/pwd_strength pktprivacy secret name} \
{/.:/subsys/dce/sec/pwd_mgmt/pwd_strength} \
} \
} \
{pwd_SecureWare_chk 0} \ }
```

You must set the minimum length of the password using the DCE Registry policies:

```
dcecp -c registry modify -change {pwdminlen 6}
```

Examples of other DCE Registry password policy attributes in **dcecp** syntax are:

{pwdalpha no}

{pwdspaces no}

{pwdexpdate none}

{pwdlife unlimited effective 5 days}

Only the **pwdminlen**, **pwdalpha**, and **pwdspaces** attributes are checked by the Password Management Server; the DCE Registry checks the remaining attributes itself.

2 Migrating to HP DCE 1.6

This chapter discusses migration procedures and compatibility issues for migrating to HP DCE 1.6 running on HP-UX 10.30.

Migration Paths

HP DCE 1.6 supports four direct migration paths from HP-UX 10.01 and 10.10 to HP-UX 10.30. Earlier versions of HP DCE that run on versions of HP-UX before 10.01 can also be migrated to HP DCE 1.6, but not directly. The direct migraton paths are listed in Table 2-1.

Table 2-1 **Supported Migration Paths to HP DCE Version 1.6**

From		To	
HP DCE Version	**Running on**	**HP DCE Version**	**Running on**
1.3.1 or 1.4 Client	HP-UX 10.01	1.6	HP-UX 10.30
1.4 Server	HP-UX 10.01	1.6	HP-UX 10.30
1.4.1 Server	HP-UX 10.10	1.6	HP-UX 10.30
1.4.1 Client	HP-UX 10.10	1.6	HP-UX 10.30
1.5 Server	HP-UX 10.20	1.6	HP-UX 10.30
1.5 Client	HP-UX 10.20	1.6	HP-UX 10.30

NOTE HP DCE 1.6 does not support direct migration from versions of HP DCE that run on HP-UX 9.x (HP DCE 1.2, 1.2.1, and 1.4.2). However, you can migrate from these versions by first migrating to HP DCE 1.3.1 or 1.4 on HP-UX 10.01 and then migrating that system to HP DCE 1.6 on HP-UX 10.30.

If you have HP DCE/9000 Version 1.3.1, 1.4, or 1.4.1 installed, you can save your existing cell configuration and databases, install HP DCE/9000 Version 1.6, and then restore your former cell configuration. Or, you can discard your previous cell configuration and database information, update your systems to HP DCE 1.6, and configure a new cell from scratch. Both procedures are detailed in this chapter.

NOTE HP DCE 1.6 does not support the Distributed File Service. Therefore, if your earlier version of HP DCE had DFS installed and configured, you will be notified during the HP DCE installation that DFS is no longer supported and has been disabled.

NOTE HP DCE 1.6 does not support the Global Directory Service.

Contents of HP DCE Client and Server

The subsets of HP DCE 1.6 commonly referred to in this document and elsewhere as client and server consist of the following DCE components:

Client	**Server**
dced	cdsd
cdsadv	secd
dtsd	gdad

NOTE

At HP DCE 1.4x, **dced** replaced **rpcd** and **sec_clientd**; and **cdsclerk** functionality was incorporated in **cdsadv**.

Migration Compatibility

This section covers the compatibility of HP DCE 1.2, 1.2.1, and 1.3.1 with HP DCE Version 1.6.

- Because HP DCE 1.6, clients and servers are binary compatible with HP DCE 1.5 and previous releases, your systems can be migrated to HP DCE 1.6 in any order over a period of time. However, do not move the Security Registry to “dce1.1” mode before all your security servers have been updated to HP DCE 1.6.
- DCM (SAM DCE Configuration Manager) and the **dce_config** utility can be used to configure a mixed-version cell.
- Because of minor changes to the **dce_config** utility at HP DCE 1.4, scripts that were written to use the HP DCE 1.2, 1.2.1, or 1.3.1 **dce_config** may have to be modified to work with HP DCE 1.4 and later releases of **dce_config**.

Migrating the Cell Directory Service from HP DCE 1.3.1

NOTE This section applies only to migrating from HP DCE 1.3.1 to HP DCE 1.6 (because HP DCE 1.3.1 is based on OSF DCE 1.0.3).

You should be aware of the following CDS considerations when migrating to HP DCE 1.6:

- Installation of HP DCE 1.6 automatically attempts to preserve any CDS defined cached servers from previous configurations of HP DCE. However, if a newly migrated HP DCE 1.6 node returns warnings about being unable to locate a CDS server, it may be necessary to manually specify the server location with a **dcecp cdscache create** command.
- To make full use of HP DCE 1.6 features, the directory version number of the root directory must be manually advanced to **4.0** after all CDS servers in the cell have been upgraded to HP DCE 1.6. (To determine the current directory version number, use the **dcecp directory show /.:** command, and look for the **CDS_DirectoryVersion** attribute.)

  The procedure for doing this is discussed in “Managing CDS Directories - Upgrading the Directory Version on a Directory”, in the *OSF DCE Administration Guide — Core Components*. This procedure makes use of the following **dcecp** commands:

  ```
  dcecp> directory modify /.: -add {CDS_UpgradeTo 4.0}
  dcecp> directory synchronize /.:
  dcecp> clearinghouse verify /.:/<clearinghouse_name>
  dcecp> directory synchronize /.:
  ```

  Note that the **dcecp clearinghouse verify** command must be run for every clearinghouse in the cell, and must be run directly on the CDS server node hosting each clearinghouse. The command will not work from a remote node.

Migrating Remote Administration of dced from HP DCE 1.3.1

When migrating from HP DCE 1.3.1, a cell administrator must create the **subsys/dce/dced-admin** group before installing HP DCE/9000 1.4.x, 1.5, and 1.6. Otherwise, the remote administration of **dced** will be disabled. To create this group log in as **cell_admin**, and execute the following **dcecp** commands:

```
dcecp> group create subsys/dce/dced-admin
dcecp> group add subsys/dce/dced-admin -member\
<cell_admin>
dcecp> acl modify /.:/sec/group/subsys/dce/dced-admin\
-add {group acct-admin rctDnfmM}
```

Migrating from HP DCE 1.2, 1.2.1 or 1.4.2 on HP-UX 9.x to HP DCE 1.6

You must perform this migration in two steps, as follows:

1. Migrate to HP DCE 1.3.1 or HP DCE 1.4 on HP-UX 10.01.

   Step 1 is described in the appropriate version of *Planning and Configuring HP DCE* and the related release notes.

2. Migrate the system created in step 1 to HP DCE 1.6 on HP-UX 10.30.

   Step 2 is described in this chapter.

For information about migrating from HP-UX 9.x to HP-UX 10.x, see *Upgrading from HP-UX 9.x to 10.x* (part number B3782-90073).

Migrating an HP DCE 1.3.1 or 1.4 Client on HP-UX 10.01 to HP DCE 1.6 on HP-UX 10.30

This section describes the procedure for migrating an HP DCE 1.3.1 or 1.4 client on HP-UX 10.01 to HP DCE 1.6 on HP-UX 10.30.

See *Managing HP-UX Software with SD-UX* and the *swcopy (1M), swinstall (1M),* and *swremove (1M)* man pages for complete information on all aspects of HP-UX 10.x installation.

For information about migrating from HP-UX 10.x to HP-UX 10.30, see *Installing HP-UX 10.30 and Updating HP-UX 10.x to HP-UX 10.30* (part number B2355-90126).

Migration Procedure

HP highly recommends that you do a system backup before starting to do an update.

To migrate an HP DCE 1.3.1 or 1.4 client-only system to HP DCE 1.6, perform the following steps:

1. Stop DCE on the system using **dce_config** STOP; if DFS is running, ignore any warnings concerning running processes.
2. Upgrade the system from HP-UX 10.01 to HP-UX 10.30.
3. Restart DCE; DCE client software is bundled with HP-UX 10.01 and later releases.

Migrating an HP DCE 1.4.1 Client on HP-UX 10.10 to HP DCE 1.6 on HP-UX 10.30

See *Managing HP-UX Software with SD-UX* and the *swcopy (1M)*, *swinstall (1M)* and *swremove (1M)* for complete information on all aspects of HP-UX 10.x installation.

For information about migrating from HP-UX 10.x to HP-UX 10.30, see *Installing HP-UX 10.30 and Updating HP-UX 10.x to HP-UX 10.30* (part number B2355-90126).

Migration Procedure

HP highly recommends that you do a system backup before starting to do an update.

To migrate an HP DCE 1.4 client-only system to HP DCE 1.6, perform the following steps:

1. Stop DCE on the system using **dce_config** STOP; if DFS is running, ignore any warnings concerning running processes.
2. Upgrade the system from HP-UX 10.10 to HP-UX 10.30.
3. Restart DCE; DCE client software is bundled with HP-UX 10.01 and later releases.

Migrating an HP DCE 1.4 Server on HP-UX 10.01 to HP DCE 1.6 on HP-UX 10.30

This section describes the procedure for migrating an HP DCE 1.4 server on HP-UX 10.01 to HP DCE 1.6 on HP-UX 10.30.

See *Managing HP-UX Software with SD-UX* and the *swcopy (1M), swinstall (1M)* and *swremove (1M)* man pages for complete information on all aspects of HP-UX 10.x installation.

For information about migrating from HP-UX 10.x to HP-UX 10.30, see *Installing HP-UX 10.30 and Updating HP-UX 10.x to HP-UX 10.30* (part number B2355-90126).

Migration Procedures

HP highly recommends that you do a system backup before starting to do an update.

Migrating a System Without Retaining Cell Configuration

If you are migrating an HP DCE 1.4 server on HP-UX 10.01 to HP DCE 1.6 on HP-UX 10.30, 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 DCM from SAM to stop the entire cell.
2. Use **dce_config** REMOVE or run the DCE Configuration Manager from SAM to remove the cell databases.
3. Upgrade the system from HP-UX 10.01 to HP-UX 10.30.
4. Install HP DCE 1.6 server software as described in Chapter 4, and reconfigure DCE.

Migrating a System and Preserving Current Cell Configuration

If you are migrating an HP DCE 1.4 server on HP-UX 10.01 to HP DCE 1.6 on HP-UX 10.30, and you want to preserve your existing cell configuration, perform the following steps:

1. If you are migrating a security server system, stop **secd** using the **dcecp -c registry stop** <*replica-name*> command.
2. Stop DCE on the system, using the **dce_config** STOP command from the main menu; if DFS is running, ignore any warnings concerning running processes.

CAUTION

Hewlett-Packard recommends that you create a single network source area (depot) containing HP-UX 10.30 and HP DCE 1.6 server software, so you can simultaneously install HP-UX 10.30 and HP DCE 1.6. If you do not install HP-UX 10.30 and HP DCE 1.6 at the same time, your old HP DCE 1.4 servers will be automatically started when your system reboots after HP-UX 10.30 installation completes. This is an unsupported configuration.

3. Prepare the network source area (depot) using **swcopy**. The depot should contain both HP-UX 10.30 and HP DCE 1.6 software.
4. Upgrade the system from HP-UX 10.01 to HP-UX 10.30. If you installed from a unified network source area as recommended above, installation of HP DCE 1.6 is complete.

NOTE

If you did not install from a unified network source area, you must continue with Steps 5 through 7.

5. Perform this step *only* if you did not install HP-UX from a unified network source area as recommended above. Stop DCE on the system, using the **dce_config** STOP command from the main menu.
6. Perform this step *only* if you did not install HP-UX from a unified network source area as recommended above.

   Install HP DCE 1.6 as described in Chapter 4. (If DFS is running, you must reboot after the install.)

7. Perform this step *only* if you did not install HP-UX from a unified network source area as recommended above.

   Restart DCE using the **dce_config** START command from the **dce_config** main menu or using DCM.

Migrating an HP DCE 1.4.1 Server on HP-UX 10.10 to HP DCE 1.6 on HP-UX 10.30

See *Managing HP-UX Software with SD-UX* and the *swcopy (1M)*, *swinstall (1M)* and *swremove (1M)* man pages for complete information on all aspects of HP-UX 10.x installation.

For information about migrating from HP-UX 10.x to HP-UX 10.30, see *Installing HP-UX 10.30 and Updating HP-UX 10.x to HP-UX 10.30* (part number B2355-90126).

Migration Procedures

HP highly recommends that you do a system backup before starting to do an update.

Migrating a System Without Retaining Cell Configuration

If you are migrating an HP DCE 1.4.1 server on HP-UX 10.10 to HP DCE 1.6 on HP-UX 10.30, 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 DCM from SAM to stop the entire cell.
2. Use **dce_config** REMOVE or run the DCM from SAM to remove the cell databases.
3. Upgrade the system from HP-UX 10.10 to HP-UX 10.30.
4. Install HP DCE 1.6 software as described in Chapter 4, and reconfigure DCE.

Migrating a System and Preserving Current Cell Configuration

If you are migrating an HP DCE 1.4.1 server on HP-UX 10.10 to HP DCE 1.6 on HP-UX 10.30, and you want to preserve your existing cell configuration, perform the following steps:

1. If you are migrating a security server system, stop **secd** using the **dcecp -c registry stop** <*replica-name*> command.
2. Stop DCE on the system, using the **dce_config** STOP command from the main menu; if DFS is running, ignore any warnings concerning running processes.

CAUTION Hewlett-Packard recommends that you create a single network source area (depot) containing HP-UX 10.30 and HP DCE 1.6 software, so you can simultaneously install HP-UX 10.30 and HP DCE 1.6. If you do not install HP-UX 10.30 and HP DCE 1.6 at the same time, your old HP DCE 1.4.1 servers will be automatically started when your system reboots after HP-UX 10.30 installation completes. This is an unsupported configuration.

3. Prepare the network source area (depot) using **swcopy**. The depot should contain both HP-UX 10.30 and HP DCE 1.6 software.
4. Upgrade the system from HP-UX 10.10 to HP-UX 10.30. If you installed from a unified network source area as recommended above, installation of HP DCE 1.6 is complete.

NOTE If you did not install from a unified network source area, you must continue with Steps 5 through 7.

5. Perform this step *only* if you did not install HP-UX from a unified network source area as recommended above.

   Stop DCE on the system, using the **dce_config** STOP command from the main menu.
6. Perform this step *only* if you did not install HP-UX from a unified network source area as recommended above.

   Install HP DCE 1.6 as described in Chapter 4. (If DFS is running, you must reboot after the install.)
7. Perform this step *only* if you did not install HP-UX from a unified network source area as recommended above.

   Restart DCE using the **dce_config** START command from the **dce_config** main menu or using DMC.

Migrating an HP DCE 1.5 Server on HP-UX 10.20 to HP DCE 1.6 on HP-UX 10.30

See *Managing HP-UX Software with SD-UX* and the *swcopy (1M)*, *swinstall (1M)* and *swremove (1M)* man pages for complete information on all aspects of HP-UX 10.x installation.

For information about migrating from HP-UX 10.x to HP-UX 10.30, see *Installing HP-UX 10.30 and Updating HP-UX 10.x to HP-UX 10.30* (part number B2355-90126).

Migration Procedures

HP highly recommends that you do a system backup before starting to do an update.

Migrating a System Without Retaining Cell Configuration

If you are migrating an HP DCE 1.5 server on HP-UX 10.20 to HP DCE 1.6 on HP-UX 10.30, 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 DCM from SAM to stop the entire cell.
2. Use **dce_config** REMOVE or run the DCM from SAM to remove the cell databases.
3. Upgrade the system from HP-UX 10.20 to HP-UX 10.30.
4. Install HP DCE 1.6 software as described in Chapter 4, and reconfigure DCE.

Migrating a System and Preserving Current Cell Configuration

If you are migrating an HP DCE 1.5 server on HP-UX 10.20 to HP DCE 1.6 on HP-UX 10.30, and you want to preserve your existing cell configuration, perform the following steps:

1. If you are migrating a security server system, stop **secd** using the **dcecp -c registry stop** <*replica-name*> command.
2. Stop DCE on the system, using the **dce_config** STOP command from the main menu; if DFS is running, ignore any warnings concerning running processes.

CAUTION Hewlett-Packard recommends that you create a single network source area (depot) containing HP-UX 10.30 and HP DCE 1.6 software, so you can simultaneously install HP-UX 10.30 and HP DCE 1.6. If you do not install HP-UX 10.30 and HP DCE 1.6 at the same time, your old HP DCE 1.5 servers will be automatically started when your system reboots after HP-UX 10.30 installation completes. This is an unsupported configuration.

3. Prepare the network source area (depot) using **swcopy**. The depot should contain both HP-UX 10.30 and HP DCE 1.6 software.
4. Upgrade the system from HP-UX 10.20 to HP-UX 10.30. If you installed from a unified network source area as recommended above, installation of HP DCE 1.6 is complete.

NOTE If you did not install from a unified network source area, you must continue with Steps 5 through 7.

5. Perform this step *only* if you did not install HP-UX from a unified network source area as recommended above.

   Stop DCE on the system, using the **dce_config** STOP command from the main menu.
6. Perform this step *only* if you did not install HP-UX from a unified network source area as recommended above.

   Install HP DCE 1.6 as described in Chapter 4. (If DFS is running, you must reboot after the install.)
7. Perform this step *only* if you did not install HP-UX from a unified network source area as recommended above.

   Restart DCE using the **dce_config** START command from the **dce_config** main menu or using DMC.

3 Before Installing HP DCE/9000 Version 1.6

This chapter describes prerequisites and preinstallation considerations for installing HP DCE/9000 Version 1.6 (HP DCE 1.6) software.

You should read this chapter before installing HP DCE/9000 Version 1.6 software. After reading this chapter, proceed with the installation instructions in Chapter 4, “Installing HP DCE/9000.”

After completing the installation of HP DCE/9000 Version 1.6 software, you must configure a DCE cell if you have not done so already. Information on HP DCE/9000 cell configuration may be found in Chapter 5, “Configuring HP DCE.”

Overview

The following is a brief overview of the HP DCE installation process:

NOTE If you are performing an upgrade rather than a new installation, see Chapter 2, “Migrating to HP DCE 1.6”.

- 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.
- Install filesets on individual systems.
- If necessary, remove unwanted filesets using **swremove**.

Prerequisites

Hardware and Software Requirements

Any HP 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.
Operating System	HP-UX 10.30.
Kernel Configuration	See “Series 700 and 800 Kernel Parameter Recommendations” in this chapter for recommended kernel parameter settings. You can check and, if necessary, change these values via SAM (the HP-UX System Administration Manager).
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 recommended 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.

Series 700 and 800 Kernel Parameter Recommendations

Hewlett-Packard has found that the default kernel parameter values for a 10.30 system installed with Runtime bundles are sufficient for running HP DCE 1.6 clients and servers under normal conditions (small cells with hundreds of users) with the following exceptions:

- **maxfiles** must be increased to a minimum of 256 for all systems.
- The default value for **maxdsize** is sufficient except in cases where you have many tens of thousands of users. At this point you should monitor the process size of your **secd** and **cdsd**. If the process size approaches the **maxdsize** value, **maxdsize** should be increased.

Kernel parameter tuning is highly application dependent. It is expected that you might need to modify your kernel parameters based upon your specific applications needs.

Distribution Media

The HP DCE/9000 Version 1.6 software is shipped on DAT tape and CD-ROM.

The international version of HP DCE/9000 on CD-ROM requires you 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 *Managing HP-UX Software With SD-UX* for more information on distribution media.

Network Distribution Area

The first part of the installation procedure involves loading software from distribution media to a network distribution area or depot. The drive where the distribution media is loaded must be connected to a system that has sufficient disk space available. To calculate the disk space required, refer to Tables 3-1 and 3-2 at the end of this chapter.

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, and GDA). 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, require access to a common set of shared resources, and can share a common administrative domain.
- 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 intercell 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 5, “Configuring HP DCE”.

In addition, you must name your cells according to Domain Name Service (DNS) convention. When a query cannot be resolved within a cell, GDA passes the query to a DNS server. 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 Chapter 5, “Configuring HP DCE”.

DCE Services

This section outlines some considerations and restrictions on HP DCE/9000 Version 1.6 software that will help you map out the installation of your cell.

Client Core Services

Core Services are contained in the DCE-Core product. This product must be installed on every system in your cell.

Security Services

Security server software is contained in the DCE-SEC-Server product. 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. HP has found the following guidelines to be sufficient:

For each principal:	1440 bytes of physical memory 330 bytes of disk space
For each account:	1580 bytes of physical memory 240 bytes of disk space

More information about DCE Security Services may be found in the *OSF DCE Administration Guide — Core Services*.

Cell Directory Service Configuration

In configuring CDS servers and clients, pay careful attention to the HP DCE/ 9000 hardware requirements for the DCE product. (See “Hardware and Software Requirements” in this chapter.) Appropriate kernel configuration, memory, disk, and especially swap space are essential to the proper functioning of the CDS subsystem.

Tape backups of the CDS server database are extremely important for recovery from catastrophic problems. HP strongly recommends regular tape back ups of all CDS server databases, especially those containing any master replicas. Tape backups and restorations require the CDS server in question to be temporarily shut down.

Most CDS problems, however, do not require resorting to tape backup. Directory replication provides continuous online backup for most failures, with faster recovery and less stale data. This makes directory replication highly desirable for all DCE cells. 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 name space 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 name space 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 name space among several CDS servers, replicating only the locally used directories, to distribute the storage overhead of the name space.

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

Time Services

A minimum of three DTS servers is recommended for any cell with three or more member systems. If you use an external time provider, you can have only one of these 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.

HP DCE Installed Software

The HP DCE/9000 Version 1.6 software is divided into products and filesets. Tables 3-1 and 3-2 show the HP DCE 1.6 filesets, arranged according to product, and gives the approximate disk space requirement for each file set. Table 3-1 includes the products that are bundled with HP-UX; Table 3-2 contains the products distributed on the Applications Release media. Note that the information in Tables 3-1 and 3-2 is also available from **swinstall**.

Note the following:

- You must install DCE-Core on every system in your cell.
- The **swcopy** and **swinstall** tools check for adequate disk space before they install software.

Table 3-1 HP DCE/9000 Version 1.6 Products and Filesets—Core HP-UX

Product	Fileset	Description	Dependencies	Approx. Size (Kb)
DCE-Core	DCE-CORE-DTS	DCE Distributed Time Service	DCE-Core.DCE-CORE-RUN	813
	DCE-CORE-HELP	DCE Online Help	none	189
	DCE-CORE-NOTES	DCE release notes	none	474
	DCE-CORE-RUN	DCE Core Client	DCE-Core.DCE-CORE-SHLIB	12786

Product	Fileset	Description	Dependencies	Approx. Size (Kb)
	DCE-CORE-SHLIB	DCE and Threads Shared Libraries	none	5146
	DCE-JPN-E-MSG	Japanese localized message catalogs	none	381
	DCE-JPN-S-MSG	Japanese localized message catalogs	none	381
	DCEC-ENG-A-MAN	DCE Core Man Pages	DCE-Core.MACR-ENG-A-MAN	838
	MACR-ENG-A-MAN	DCE Man Page Macros	none	23
Integrated Login	AUTH-COMMON	Integrated Login Common Portion	none	343
	AUTH-DCE	HP DCE Authentication	DCE-Core.DCE-CORE-RUN Integrated|Logon. AUTH-COMMON	365
KRB-Support	KRB-SUPP-MAN	Man Pages for Enhanced Kerberos Support	none	8
	KRB-SUPP-NOTES	Kerberos Support white paper	none	337
	KRB-SUPP-RUN	Enhanced Kerberos support commands	DCE-Core.DCE-CORE-RUN	527

Table 3-2 HP DCE/9000 Version 1.6 Products and Filesets—Applications Release

Product	Fileset	Description	Dependencies	Approx. Size (Kb)
DCE-CoreAdmin	DCE-ACCT-MGR	HP Account Manager	DCE-Core.DCE-CORE-RUN	1818
	DCE-CDSBROWSER	CDS Browser Tool	DCE-Core.DCE-CORE-RUN	1558
	DCE-CONFIG-MGR	DCE Configuration Manager	DCE-Core.DCE-CORE-RUN	1071
	DCE-CORE-DIAG	DCE Diagnostic Tools	DCE-Core.DCE-CORE-RUN	240
	DCE-SGUARD[a]	DCE - MC/ServiceGuard Integration Templates	none	64
DCE-CoreTools	DCE-BPRG	Basic IDL, Includes, & Archive Libraries	DCE-Core.DCE-CORE-RUN	9413
	DCEP-ENG-A-MAN	DCE Basic Tools Man Pages	none	1870
	THD-ENG-A-MAN	Threads Man Pages	DCE-Core.MACR-ENG-A-MAN	177
DCE-C-Tools	DCE-C-TOOLS	HP DCE C Application Tools	none	1950
	DCE-TOOLS-LIB	HP DCE Programming Libraries	DCE-CoreTools. DCE-BPRG	189
DCE-CDS-Server	CDS-SERVER	CDS Server	DCE-Core.DCE-CORE-RUN	1420

Product	**Fileset**	**Description**	**Dependencies**	**Approx. Size (Kb)**
	CDSS-ENG-A-MAN	CDS Server Man Pages	DCE-Core.MACR-ENG-A-MAN	16
DCE-Domestic	DCE-DOM-BPRG	DCE Domestic Programming Libs	DCE-CoreTools. DCE-BPRG	6428
	DCE-DOM-NOTES	DCE Domestic Release Notes	none	11
	DCE-DOM-RUN	DCE Domestic runtime	DCE-Domestic. DCE-DOM-SHLIB DCE-Core.DCE-CORE-SHLIB	316
	DCE-DOM-SHLIB	DCE Domestic Library	DCE-Core.DCE-CORE-SHLIB	4339
DCE-OO-Tools	DCE-OO-HELP	HP OODCE Online Help	none	1513
	DCE-OO-TOOLS	HP OODCE Application Tools	DCE-C-Tools.DCE-TOOLS-LIB	3541
DCE-SEC-Server	SEC-SERVER	Security Server	DCE-Core.DCE-CORE-RUN	7037
	SECS-ENG-A-MAN	DCE Security Server Man Pages	DCE-Core.MACR-ENG-A-MAN	19

a. Provided as a customizable set of templates and scripts to integrate DCE services with the MC/ServiceGuard product. See “Integrating DCE Services with MC/ServiceGuard” in Chapter 5 for more information.

4 Installing HP DCE 1.6

This chapter outlines the recommended procedures for installing and deinstalling HP DCE/9000 Version 1.6 software.

If you are performing an upgrade rather than a new installation, see Chapter 2, “Migrating to HP DCE 1.6”.

The procedures outlined in this chapter use the graphical and textual user interface versions of the **swcopy**, **swinstall**, and **swremove** tools. You can also use these tools from a command line.

See the manual *Managing HP-UX Software With SD-UX* and the *swcopy (1M)*, *swinstall (1M)* and *swremove (1M)* man pages for more information on all aspects of installation.

After installing HP DCE/9000 Version 1.6 software, you must configure a DCE cell if you have not done so already. Information on cell configuration is in Chapter 5, “Configuring DCE Cells.”

Overview

Here is a brief overview of the installation steps:

1. Read Chapter 3, “Before Installing HP DCE 1.6”.
2. Load HP DCE software from media to a network source area using **swcopy**.
3. Install filesets on individual systems using **swinstall**.

Loading HP DCE Software in a Network Source Area

Before installation of HP DCE/9000 Version 1.6 software on a network, the software typically is transferred from the media on which it was shipped to a network source area, or depot. This section tells how to perform this transfer using the **swcopy** tool.

Before loading HP DCE, you should be aware of the following:

- If you are installing HP DCE/9000 on a single system, and your system has access to a media device, you can choose to install software directly from media. If you want to do this, proceed to “Installing Software” in this chapter.
- If your software was shipped with a codeword certificate, you must obtain a codeword from Hewlett-Packard before you load the software into a depot. To obtain a codeword, follow the instructions on the codeword certificate that was shipped with the CD-ROM disk.

Software Loading Procedure

This section outlines the steps you must follow to load HP DCE 1.6 software into a network source area using the **swcopy** graphical or textual user interface.

See *Managing HP-UX Software With SD-UX*, as well as the *swcopy (1M)* man page, for detailed information on the general process of creating a net work source area, and on the **swcopy** command-line interface. Also, the **swcopy** graphical user interface has general and context sensitive help if you need assistance in making selections, or in entering appropriate values.

Perform the following steps to load HP DCE 1.6 software into a network source area:

1. Load media into the drive.
2. Log in as **root**.
3. Start /usr/sbin/swcopy.
4. Specify the target depot path in the “Select Target Depot Path” popup window.

NOTE If you are performing this install as a step in migrating a server system from a previous version of HP DCE, create a single depot containing the HP DCE 1.6 software and the DCE client software that is bundled with HP-UX 10.30. See Chapter 2 for information on migrating from a previous HP DCE version. The target depot path is the pathname to the directory where you want the HP DCE software to be loaded. As a general rule, you should accept the HP-UX default **/var/spool/sw**.

5. Specify the source hostname and source depot path in the “Specify Source” popup window.

   The source hostname is the name of the machine on which the media device is mounted; the source depot path is the device pathname.

   When you have specified these fields, a list of the products and bundles available in that source depot (i.e., on the media) is displayed in the “Software Selection” window.

6. Select the DCE products to load.

   After you select (double-click on) the DCE bundle, a list of the DCE products is displayed. Mark all the listed DCE products for loading.

7. Load the software into the depot.

   Select “Copy” from the Actions menu.

   If your software media was shipped with a codeword certificate, follow the instructions on the certificate to obtain a codeword before you load the software into the depot. Before you load software that requires a codeword, you must enter a valid codeword and hardware ID. If a codeword is not required for your software, answer “no” to the question “Do you want to enter your authorized codeword to access the protected software?”.

Installing Software

Installation Notes

Once you have loaded HP DCE/9000 Version 1.6 software into a network distribution area, use the **swinstall** tool to install appropriate filesets on individual systems.

CAUTION

HP DCE 1.6 on HP-UX 10.30 does not support DFS. If you plan to upgrade a DFS Server system to HP-UX 10.30, unconfigure DFS from the node before installing HP-UX 10.30. Otherwise, the earlier DFS installation and configuration will cause confusion during the HP-UX install process.

The installation procedure invokes **swinstall** on each target system in a cell. When installation is complete, you can begin cell configuration, which is described in Chapter 5, “Configuring DCE Cells”.

Before you begin, make sure that you have the following information.

- 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.
- Know the name of your network source system, as well as the source depot path name.
- You must install HP DCE/9000 Version 1.6 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 installation, you must be able to log in to the remote system using 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.

Installation Procedure

Perform the following steps to install HP DCE 1.6 software from a network source area:

1. Log in to the target system as **root**.
2. Run **swinstall**.

   ```
   /usr/sbin/swinstall
   ```

   The **swinstall** tool has general and context sensitive help if you need assistance on making selections, or on entering appropriate values. Also, see the *swinstall (1M)* man page for more information.
3. In the Specify Source window, specify the source host and depot.
4. In the Software Selection window, select the products/bundles you want to install.

   If you are doing an upgrade, and you want to match the software currently on the target system, select “Match What Target Has” from the Actions Menu.
5. Select “Install” from the Actions menu.
6. Check the swinstall log file and resolve any problems.

   Press the “Logfile” button in the Install Analysis popup window. Look for messages that begin with ERROR, WARNING, or NOTE.

   Refer to *Managing HP-UX Software with SD-UX* for information on resolving install problems.
7. Install the software.

   Press the OK button in the Install Analysis popup window to proceed with installation.

   After you install the HP DCE/9000 Version 1.6 software on all the systems in your cell that are to be updated, you can begin to configure your cell. See Chapter 5, “Configuring DCE Cells”, for information on cell configuration.

5 Configuring HP 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 DCE Configuration Manager, DCM, and the **dce_config script**.

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

To configure HP DCE/9000 software, you must have previously installed HP DCE. See Chapter 3, “Before Installing HP DCE/9000 Version 1.6” for planning information; see Chapter 4, “Installing HP DCE 1.6” for installation information.

NOTE

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

Choosing a Cell Configuration Tool

HP DCE/9000 offers two cell configuration tools: a script-based tool, **dce_config**, and a SAM-based tool, DCM (DCE Configuration Manager). 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.

DCM and dce_config

DCM is essentially a graphical front-end to **dce_config**. However, in addition to the ease-of-use that a graphical interface confers, DCM has some important functional differences that offer advantages over running **dce_config**. Therefore, we recommend that you use DCM, and not **dce_config**, to configure cells in almost all cases. (See “Limitations of DCM,” the next subsection, for further details.)

Advantages of DCM

Some of the advantages of DCM are:

- DCM has a template mode that allows you to create prototype configurations that can be tested before actually creating them.
- DCM checks systems before performing the configuration.
- DCM prevents you from creating an invalid configuration.
- DCM allows you to configure all HP DCE/9000 Version 1.2, 1.2.1, 1.3.1, 1.4, 1.4.1, 1.4.2, 1.5, and 1.6 systems in your cell remotely, from a single administrative node. However, DCM does not configure and may not *discover* all aspects of other vendors’ system configuration.
- DCM remembers the last successful configuration. This information is used only when the cell is “down” or critical DCE servers are not running.
- DCM includes complete online documentation.

Limitations of DCM

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

- When DCM 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 DCM will revert to the last successful configuration.
- DCM does not ask if you want to create a LAN profile.
- DCM does not permit you to enter the name of the clearinghouse when you create a CDS replica. It defaults to *hostname*.**ch**. It also, therefore, does not ask if more directories should be replicated.

Configuring Cells with DCM

Overview of DCM Functionality

DCM enables you to perform the following cell configuration tasks:

- 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 vendors' systems), you can configure additional HP DCE 1.2, 1.2.1, 1.3.1, 1.4, 1.4.1, 1.4.2, 1.5, or 1.6 clients into the cell from any HP DCE 1.6 cell member system.
- Create a cell of one or more systems. DCM 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.
- Restart all DCE daemons on all cell members or selected cell members.
- Destroy (unconfigure) an existing cell.

At the heart of DCM is an *object list* screen that displays a list of all cell members and their attributes. The attributes include a cell member's name, and the DCE services (if any) configured on the member. 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 menu.

By using the List 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

CAUTION DCM uses standard UNIX remote login utilities to perform remote administration. This causes 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 DCM is no more or less secure than using standard UNIX remote login utilities directly. (Secure Internet Services (SIS) do not provide better security for the purpose of remote DCE cell administration.)

Requirements for Running DCM

If you choose to configure your cell with DCM, you should verify that the systems in your cell meet the following requirements:

- All systems from which you want to perform cell configuration tasks must have SAM installed.
- 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 want to administer via DCM must be running HP DCE/9000 Version 1.2 , 1.2.1, 1.3.1, 1.4, 1.4.1, 1.4.2, 1.5, or 1.6. DCM does not configure and may not "discover" all aspects of other vendors' system configuration.

Running DCM

To run DCM:

1. Log in as **root**.
2. Execute **sam** from a shell prompt.

3. Select (double click on) **DCE Cell Management**.
4. Select (double click on) **DCE Configuration Manager**.

   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 vendors' systems), you can configure additional HP DCE 1.2, 1.2.1, 1.3.1, 1.4, 1.4.1, 1.4.2, 1.5, or 1.6 clients into the cell from any HP DCE 1.6 cell member system.

Online Help for DCM

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

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

To access the DCM online help, select (single click on) the **DCE Configuration Manager** icon in SAM. Then press F1. Alternatively, open (double click on) **DCE Configuration Manager**, and then select "Introduction to Cell Configuration."

For informatoin about using the SAM online help system, use the **Help** pulldown menu on the SAM screen.

Printing the DCM Online Help

You can print the DCM online help from CDE. The help, however, is not formatted as it is on the screen: only text is printed (graphics are not printed).

You can print individual help topics within DCM online help using the Print button on a help topic screen.

You can use the **-dthelpprint** command at a shell prompt to print the entire help volume. The full pathname of the DCM help volume is:

```
/opt/dce/lib/dcm/C/help/dceconf.sdl
```

On ASCII terminals, you can only use the **dthelpprint** command; the print button is not available. See the *dthelpprint (1X)* man page for more information.

Configuring Cells Using 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 following sections include complete information on configuring cells using the **dce_config** script.

Starting dce_config

1. Log in as **root** on the system you want to configure.
2. Run **dce_config**.

The DCE Main Menu is displayed.

```
DCE Main Menu (on hostname)
1. CONFIGURE -configure and start DCE daemons
2. START -re-start DCE daemons
3. STOP -stop DCE daemons
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 (but is capable of unconfiguring) systems remotely. System configuration must be done locally on each client/server system. When running **dce_config**, you must always log in on the system you want to configure.

Initial Cell Configuration

NOTE

In HP DCE 1.6, **dce_config** sets the DCEAUDITFILTERON environment variable to enable audit filtering, which limits the range of audit event types logged. It you want to disable or change the default settings provided by **dce_config**, you must do so before starting any server that provides data to the Audit Service. See “Configuring the DCE Audit Service” in this chapter and “The DCE Audit Service” in Chapter 1.

NOTE

HP DCE 1.6 does not support DFS. Therefore, you can ignore references to DFS that still appear in configuration menus. If you choose DFS Client from the DCE Configuration Menu, for example, a message displays that the bits are not loaded.

When creating an HP DCE cell, servers must be configured before clients. First configure a Security server, then a CDS server, a Time server, 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 Client Systems: Security, CDS, and DTS” later in this chapter.

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 Initial Cell Configuration:

   ```
   DCE Configuration Menu (on hostname)
   selection: 1 (Initial Cell Configuration)


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


   Initial Cell Configuration (on hostname)
   1. Initial Security Server
   2. Initial CDS Server
   3. Initial DTS Server


   98. Return to previous menu
   99. Exit

   selection:
   ```

3. Configure the Security Server:

   ```
   Initial Cell Configuration

   selection: 1 (Security Server)

   S:****** Configuring initial 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 reconfiguring a cell, answer **y**:

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

5. Enter a cell name:

   ```
   Enter the name of your cell (without /…), xyz.abc.com

   S:****** Stopping rpcd...
   S:****** Starting dced...
   S:****** Initializing dced...
   S:****** Since the glbd daemon was restarted and/or
   llbd and rpcd were replaced by the endpoint
   mapper, NCS applications may need to be
   restarted.
   ```

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

   ```
   Enter keyseed for initial database master key:
   ```

7. **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:
   ```

8. **dce_config** prompts you for the starting point for UNIX user and group IDs 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 IDs
   that are automatically generated by the Secu rity Ser-
   vice 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 IDs 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 initializes the registry database.

   ```
   S:****** Starting secd…
   S:****** Checking for active sec_client service...
   S:****** Starting sec_client service...
   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 on that system, and continue with step 10 below.
   - If the CDS server is on the same system as the Security server, continue with step 9 below.

CAUTION

Do not configure an additional CDS Server or a replica of a CDS Server on the same system as your Security Server. Such a configuration is illegal and unsupported.

9. From the Initial Cell Configuration menu, choose Initial CDS Server:

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

   ```
   Initial Cell Configuration (on hostname)
   ```

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

```
S:****** Configuring initial CDS Server…
S:****** Please wait for user authentication and
authorization…
S:****** Checking for active sec_client service...
```

10. **dce_config** asks whether it 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
```

```
S:****** Starting cdsadv...
S:****** Starting cdsd...
S:****** Creating LAN profile…
S:****** Setting ACLs for all new namespace
entries...
```

This system is now configured as a CDS server. You must now create a DTS server, either on this system or on another system.

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 **/ etc/opt/dce/zoneinfo/localtime**. A different time zone can be chosen: see the *localtime (5)* man page for details.

To configure a DTS server on this system, or on another system:

- If the DTS server for this cell will be on another system, repeat steps 1 and 2 on that system, and continue with step 11 below.
- If the DTS server will be on this system, continue with step 11 below.

11. From the Initial Cell Configuration menu, choose Initial DTS Server:

    ```
    selection: 3

    S:****** Configuring initial DTS services
    S:******Please wait for user authentication and
    authorization...
    S:****** Checking for active sec_client service...

    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

    selection:
    ```

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

    ```
    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**).

13. 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.

14. 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:
    ```

15. Select NULL, 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 host name where the NTP server is running:
    ```

    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 want 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.
   ```

NOTE When configuring a multi-system cell, **dce_config** checks that system times are within 120 seconds of each other.

2. The Additional Server Configuration menu appears. Choose Additional CDS Server:

   ```
   Additional Server Configuration Menu
   selection: 1 (Additional CDS Server(s))
   S:****** Configuring additional CDS server
   A CDS server must have already been configured.
   ```

3. **dce_config** prompts for the name of an existing 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_node

S:****** Checking for active sec_client service...
S:****** Starting cdsadv...
```

4. **dce_config** asks whether it 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) n

   S:****** Starting cdsd...

   S:****** Waiting for registry propagation...

   S:****** Initializing the name space for additional
   CDS server...
   Modifying ACLs on /.:/hosts/hostname/cds-server
   ```

5. After starting the CDS client daemon, **dce_config** prompts for the name of the CDS clearinghouse. Enter a name of your choice.

   ```
   What is the name for this clearinghouse? hostname_ch

   S:****** Modifying ACLs on /.:/host_ch…
   ```

6. **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, sepa-
   rated by spaces, and terminated by <RETURN>
   ```

Notes on Configuring Additional CDS Servers

Immediately after configuring an additional CDS server, you should, while logged in as **cell_admin**, skulk the root directory using the following command:

```
dcecp -c directory synchronize /.:
```

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 Client Systems: Security, CDS, and DTS

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 systems(s) running the Security server and the initial CDS server for the cell.

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.

You must have the following information to configure a client:

- The host name of any security server in the cell
- The cell administrator's principal name and password
- The host name of a CDS server in the cell

1. Start **dce_config** on the system that you want 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 want 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 host name of your cell's security server:

   ```
   What is the name of a Security Server running in the
   cell you
   wish to join? sec_server_node
   S:****** Starting dced...
   S:****** Initializing dced...
   ```

6. After starting and initializing the Security client daemon, **dce_config** asks for the name of a node with which it can synchronize the clock on this node: Enter < **RETURN**> to get the default (the master security machine in the cell).

   ```
   Enter a machine to synchronize with:
   (sec_server_node) <RETURN>
   ```

   ```
   Time on host is within specified tolerance (120 secs)
   of time on sec_server_node.
   S:****** Checking for active sec_client service...
   S:****** Starting sec_client service...
   S:****** This node is now a security client.
   S:****** Starting cdsadv...
   ```

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
   ```

   ```
   S:****** This node is now a CDS client.
   ```

8. After configuring the CDS client, **dce_config** asks how the node should be configured for DTS. 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.

   ```
   Should this machine be configured as a DTS Clerk, DTS
   Local Server, or DTS Global Server? (default is DTS
   Clerk) (clerk, local, global, none) <RETURN>
   ```

   ```
   S:****** Starting dtsd...
   S:****** This node is now a DTS clerk
   ```

   Configuration of the Security, CDS and DTS client system is now complete.

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 for information about establishing intercell communication with GDA.

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 improved cell performance and reliability. These steps will allow you to create a security replica via **dce_config**.

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
   S:****** starting slave security server (secd)…
   ```

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

3. **dce_config** prompts for a name for the security replica. Enter whatever name you wish:

   Enter the Security Replica name (without **subsys/dce/sec**): **sec_rep_node**

   ```
   S:****** Modifying acls on /.:/sec/replist…
   S:****** Modifying acls on /.:/subsys/dce/sec…
   S:****** Modifying acls on /.:/sec…
   S:****** Modifying acls on /.: …
   S:****** Modifying acls on /.:/cell-profile…
   ```

4. **dce_config** prompts for a key seed; enter any sequence of characters:

   ```
   Enter keyseed for initial database master key:
   ```

Configuring the DCE Audit Service

At HP DCE 1.4.2, the **dce_config** utility automatically enabled audit filtering by setting DCEAUDITFILTERON before starting any DCE servers; in addition, when you invoke the “Auditing” command from the **dce_config** “Additional Server Configuration” menu, **dce_config** specifies a set of default audit filters before starting **auditd**, the audit daemon. You can use the **dcecp audfilter** command to delete or modify these default filters, or to create new filters. See the *-audfilter (1M)* man page for more information on how to do this.

NOTE If you want to enable auditing, you must explicitly start the audit daemon by selecting **9** (Auditing) from the **dce_config** “Additional Server Configuration” menu. Not starting the audit daemon is functionally equivalent to setting DCEAUDITOFF, effectively disabling auditing.

If you want to disable auditing completely, set the DCEAUDITOFF environment variable to 1 on each node where you intend to run a DCE server before starting the cell’s servers.

Removing Systems from the Cell

NOTE

You cannot use the **dce_config** UNCONFIGURE option to remove a Master Security Server or Initial CDS Server system from a cell. You must either use the DCM to do this, or reconfigure the entire cell. You can use the **dce_config** UNCONFIGURE option to remove Additional CDS Server or Replica Security Server systems from a cell.

To remove a configured system (except a Master Security Server or Initial CDS Server 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 system to be unconfigured. The UNCONFIGURE option removes the target machine from the cell Security database and the CDS name space. After you have unconfigured the system, run **dce_config** on the 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.

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 host name of the client:

   ```
   Enter hostname of node to be unconfigured: hostname
   ```

4. The system explains that unconfiguring a node will remove the node’s ability to operate in a cell, and asks if you want 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 want 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 want to restart the client, follow the instructions in “Configuring Client Systems: Security, CDS, and DTS”.

Removing and Reconfiguring the DCE Daemons

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

If you want 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.

NOTE

You cannot use the **dce_config** UNCONFIGURE option to remove a Master Security Server or Initial Directory Server system from a cell. You must either use the DCM to do this, or reconfigure the entire cell. You can use the **dce_config** UNCONFIGURE option to remove Additional CDS Server or Replica Security Server systems from a cell.

1. On the system you want 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 want 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 **/var/opt/dce/config/dce_config.log**.

Log messages have different priorities, based on content, which determine both where the messages are logged and how they are formatted. 5-1 describes log message types (in priority order from highest to lowest), their format, and their content.

Table 5-1 **dce_config Message Categories**

Priority	Format	Content
ERROR	ERROR:<message>	Result of an operation that was not as expected, and is probably fatal. Always followed by a prompt for user to continue or quit.
WARNING	WARNING:<message>	Information the user should be aware of before proceeding. Always 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*”.

Priority	**Format**	**Content**
SUMMARY	S:******<message>	High-level summary of action being taken or action completed. Always logged to log file. Also logged to display unless DISPLAY_THRESHOLD is WARNING or ERROR.
VERBOSE	V:<message>	Low-level summary of actions being taken, user queries and responses, or actual commands executed that do not affect configuration or node state. Logged to log file unless LOG_THRESHOLD is DETAIL or higher. Not logged to display unless 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. Frequently contain error message text, since error text is passed to script functions for display if an error occurs. Do not confuse these message with actual error occurrences.

Additional Notes About Log Messages

ERROR messages—if **dce_config** is being run using a here-document (**dce_config** << *input_file*) or when using **dce_config -e config.env -c config.cmd**, the environment variable EXIT_ON_ERROR should be set to **y** and exported to prevent errors from causing the here-document 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-document.) See the *ksh (1)* man page for more information about here-documents.

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**.

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 want to run **dce_config** from custom scripts. This section includes 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 want to directly call the following **dce_config** component scripts. Unless otherwise noted, these scripts reside in **/opt/dce/bin** or **/etc/opt/dce**:

- **dce_shutdown**: 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 reconfiguring 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**.
- **/sbin/init.d/dce[start | stop]:** Starts or stops HP DCE daemons. Cannot be run remotely; must be run on DCE client or server node.
- **/etc/rc.config.d/dce**: Read by **/sbin/init.d/dce** to determine which daemons to start.

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, possible corresponding prompts for information will be skipped.

- REMOTE_ADMIN: If you set the variable REMOTE_ADMIN to **y** (using a command such as "export REMOTE_ADMIN=y") before you run **dce_config** or **dcm** on an HP DCE 1.6 system, then **dced** is started with the command **dced -b -r** and **/etc/rc.config.d/dce** is updated to include DCED_SWITCHES= -r. You can also set REMOTE_ADMIN in the **config.env** file if you run **dce_config** non-interactively.
- 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 with a here-document, CHECK_TIME should be set to **n** since time checking uses a **telnet** command that causes input from the here-document to be lost.

- 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** only if TCP protocol routing is available.
- DISPLAY_THRESHOLD: Minimum priority log messages 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.
- LOG_THRESHOLD: Minimum priority log messages from **dce_config** that are written to **/var/opt/dce/config/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 IDs larger than 32767 from accessing DCE cells that use the default. A value smaller than the default prevents foreign accounts with IDs 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-document 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 GIDs. 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: Key seed 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 GIDs. 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-generated UIDs. 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: Host name 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 UIDs. Default is 100.
- UNCONFIG_HOST_PRESET: Host name of node to be unconfigured.

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 **/sbin/init.d/ncs** start to restart NCS daemons.
6. Restart any servers for NCS-based applications.

Integrating DCE Services with MC/ServiceGuard

MC/ServiceGuard is a Series 800 product that was introduced at HP-UX 10.0. MC/ServiceGuard provides an environment in which, if a node fails, services (applications) can be up and running again on another node very quickly.

This section provides background information on MC/ServiceGuard, and explains detailed planning and configuration steps necessary to utilize MC/ServiceGuard to increase the availability of the DCE core services. The process and considerations provided here are also easily extended to DCE-based application servers.

Readers of this section should already have a license for the MC/ServiceGuard product and be familiar with the contents of *Managing MC/ServiceGuard* (B3936-90003), which describes the features and capabilities of MC/ServiceGuard and provides a general conceptual framework for planning, configuring, and operating an MC/ServiceGuard cluster.

Background

The DCE infrastructure depends on three core services, all of which are necessary for the proper operation of a DCE Cell: the Security Service, the Naming Service, and the Time Service. In a properly configured DCE cell, each of these services is distributed and replicated, in order to increase the availability and scalability of the DCE infrastructure. This means that each service actually consists of multiple servers running on separate hosts. Should any single server become unavailable, clients can quickly locate and use another server (replica) that provides the same service.

The Security and Naming services replicate only their read operations. That is, while a client can choose between any of the replicas to obtain information, it must go to a specific replica — the master replica — to perform a write operation. The master replica is then responsible for informing the other (read-only) replicas of the change.

While the replication mechanisms of the Security Service and the Naming Service differ in design and implementation, they share this master-slave approach. Therefore, while both services can be considered highly available for read operations, they do present a single point of failure for write operations.

The Time Service, on the other hand, does not present the same level of vulnerability. Most mission critical installations will configure more than the minimum necessary time servers with multiple time providers. This being the case, the loss of a single time server is usually not critical. Installations should not establish an MC/ServiceGuard configuration for the purpose of maintaining the Time Service alone.

DCE-based applications can also present a single point of failure, unless the developers provide for the replication of data and functions between multiple servers. Since replication is a complicated and complex process, many application designers may choose to depend on a “fail over” approach such as MC/ServiceGuard to provide availability, rather than develop and maintain their own replication mechanisms.

In summary, you only need to use MC/ServiceGuard to increase the availability of DCE Core Services and DCE-based services that are not replicated. In the case of the DCE Core services, these are the write functions provided by the DCE master Security and Naming replicas.

Planning Considerations

In your planning for MC/ServiceGuard, you must consider the following characteristics of DCE and DCE-based programs:

- The DCE runtime and daemons do not themselves support the concept of dynamic IP addresses.
- Normal DCE programming practice assumes that all IP addresses on the host should be used for endpoints for exported services.

The DCE runtime determines the available IP addresses on the node during the execution of any of the **rpc_server_use_*** routines. These routines are used in every DCE server to select the protocols over which the server will provide services. A side effect of this call is that the list of IP addresses supported by the node is established for use later when determining the binding vector. When this vector is obtained by a server main routine and registered in the endpoint map, the endpoint map will contain entries for every IP address identified earlier during the **rpc_server_use_*** call. In addition, should this binding vector be exported to the name space, the name space entry will also identify every IP address on the node as providing the service associated with that entry.

While it is possible to edit the contents of the binding vector before using it to register endpoints or add entries in the name space, few, if any, DCE server programs actually edit the binding vector. In addition, the DCE runtime does not re-determine the list of available IP addresses during the course of server execution, and, again, DCE servers do not, as a general rule, go through their initialization sequence a second time. As a result, for all the DCE core servers and most known application DCE servers, the IP addresses used by the server are set once during initialization, including all the IP addresses available on the node. The addresses do not change once set.

In an MC/ServiceGuard environment, these characteristics might be problematic. Suppose a node had several packages running on it, each based on a DCE service and each with its own IP address. The DCE servers in each package would not only register endpoints using their own IP address, but will also include the IP address of all the other packages configured on the node at the time the server started up. Since all the DCE core services cache IP addresses and store them in their internal databases, the result is a potentially large number of invalid entries, adversely affecting performance, causing the generation of a large number of misleading log messages, and potentially causing the failure of the DCE infrastructure. These considerations and their affects do not preclude the use of MC/ServiceGuard with DCE by any means; they do, however, require that system administrators be particularly careful when planning, configuring, and operating a DCE-MC/ServiceGuard installation.

Through an environment variable, the DCE runtime provides the means to restrict the IP addresses identified by the **rpc_server_use_*** routines. Used correctly, this variable can alleviate the adverse effects of the characteristics noted above.

Planning for a DCE-MC/ServiceGuard Installation

Planning for a package that includes one or more DCE servers is primarily a process of identifying the disk and network resources necessary for the operation of the server. The planning process should follow the steps outlined in *Managing MC/ServiceGuard*. Especially important is that you read and understand the section in Chapter 4 entitled “Writing Network Applications as HA Services” before beginning the planning process.

Hardware Requirements for a DCE-MC/ServiceGuard Configuration

By their very nature, DCE and DCE applications are distributed, and therefore depend heavily on network resources. Each node in the cluster should have multiple redundant LAN cards connected to multiple LANs. Also, all the normal hardware configuration guidelines outlined in *Managing MC/ServiceGuard* should be followed when planning for your hardware configuration.

Implementation Alternatives for a DCE-MC/ServiceGuard Installation

The basic configuration, which is supported by the templates, is the DCE host failover. In this configuration, ServiceGuard moves an entire DCE host from one physical node to another.

An alternative configuration is the individual core server failover. In this configuration, the DCE cluster includes a primary host and several smaller hosts. Each of the smaller hosts can perform one or more of the functions normally performed by the primary host. In the event of a system failure for the primary host, ServiceGuard moves only the core servers on the smaller hosts from their individual physical nodes to other physical nodes. For example, in a DCE cluster with individual server hosts for the Security Service and the Name Service, ServiceGuard can move the **secd** or **cdsd** servers individually to a new host rather than moving the entire primary host to another node.

Another alternative configuration is the redesignation of master servers through ServiceGuard scripts. This approach involves changing the role of the existing replicas, making them the master servers, instead of moving the databases to new locations.

Other alternative configurations are possible, but they are not discussed here. See *Managing MC/ServiceGuard* (B3936-90003) for more information about alternative configurations.

The remaining sections in this chapter describe the basic configuration only.

The DCE-SGUARD template fileset is available on the CD-ROM that ships with the DCE product. See Table 3-2 in Chapter 3 and “Supported Templates for MC/ServiceGuard Integration with DCE” in this chapter for more information about filesets.

Supported Templates for MC/ServiceGuard Integration with DCE

As part of the DCE product, HP DCE 1.6 provides a fileset (DCE-SGUARD) that contains a set of customizable ServiceGuard templates and scripts to integrate MC/ServiceGuard with DCE services. This set of templates includes the DCE processes **dced**, **cdsadv**, **secd**, and **cdsd** within a single package. Each process is monitored separately, and local restart and local network switchover are supported.

NOTE Do not attempt to use the templates in an installation without first customizing them.

The templates and scripts are as follows:

dcepkg.conf—package definition file generated by MC/ServiceGuard. You must supply the ServiceGuard node names, DCE services, and the network name and address.

rc.dcepkg—package control script generated by MC/ServiceGuard. You must supply the ServiceGuard node names, DCE services, and the network name and address. You can also specify customer defined functions.

dce—DCE configuration file, which is copied from **/etc/rc.config.d/dce** to the DCE/ServiceGuard package directory. You can set the environment variable RPC_SUPPORTED_NETADDRS to the package IP address.

dce.start—package startup script, which MC/ServiceGuard calls when the package is activated.

dce.restart—package restart script, which the DCE service monitor uses to start an individual DCE service.

dce.monitor—DCE Service monitor, which ServiceGuard launches to monitor DCE daemons.

First, the DCE service monitor checks to see if the server is running, and, if it is not, the DCE service monitor starts it. Then, the DCE service monitor goes into a loop and checks to ensure that the server process is running. Finally, the DCE service monitor performs a DCE level **ping** on the server interface.

rc.dcepkg.log—a log file that is created in the package directory during DCE package startup through MC/ServiceGuard, individual DCE services restart upon failure, and package failover.

Planning for the DCE Package

When planning for a DCE-MC/ServiceGuard installation, keep the following considerations in mind:

- Enough disk space to hold the DCE installation, log files, and core files should be allocated in the logical volumes assigned to the package. See Chapter 3 of this manual for recommendations regarding disk space requirements.
- Every node in the cluster will need to be configured with adequate swap space for a DCE server configuration. The minimum recommended swap space is 100MB, but this figure may need to be modified based on actual need. The kernel configuration should be validated on an operational system and adjusted if necessary.
- Network switching and package switching should normally be enabled. Depending on the services included in the package and the requirements of the system, node and service fail fast may be enabled as well.
- There are a number of different ways to define the DCE package. The simplest way is to include the execution of the **rc.dce** start script at the end of the package run script, the **dce_shutdown** utility at the start of the package stop script, and a definition of a simple monitoring script as the “service” to be executed This simple monitoring script should periodically check for the existence of the configured DCE servers, and return with a non-zero exit status if any of the servers fail.

DCE Configuration for Integration with ServiceGuard

DCE configuration for integration with ServiceGuard is performed in the following steps:

1. Configuring the ServiceGuard cluster
2. Configuring DCE
3. Configuring the package
4. Distributing the package
5. Starting the ServiceGuard cluster
6. Starting the package on the ServiceGuard cluster

The following subsections describe these steps in more detail.

Configuring the ServiceGuard Cluster

Before configuring DCE for integration with ServiceGuard, you must install ServiceGuard. Then, install the DCE software on the primary and secondary nodes separately.

1. To configure the primary and secondary nodes in a ServiceGuard cluster, enter the following command:

   ```
   cmquerycl -v -C /etc/cmcluster/cmclconfig.ascii \
   -n <primary_node> -n <secondary_node1> \
   -n <secondary_node2> ...
   ```

   This command creates the template script **/etc/cmcluster/cmclconf.ascii**. Modify the script parameters to reflect your desired configuration, after which, the script seldom needs modification.

2. To determine if ServiceGuard daemons are running so that the DCE initial configuration program (**dce_config**) detects the presence of ServiceGuard enter the following command:

   ```
   cmruncl -v -n [primary node] -n [secondary node]
   ```

3. Identify the hostname and IP address to be dedicated to the packages. To manually add the IP address to the cluster's primary node, enter the following command:

   ```
   cmmodnet -a -i [package IP] [SUBNET]
   ```

Configuring DCE

Perform the following steps to configure DCE on your system if the ServiceGuard is running:

1. Create a volume group for the DCE data file (for example : **/dev/vgdce**).
2. Manually activate the volume group to be accessed from the primary node (for example: **vgchange -a e /dev/vgdce**).
3. Identify the filesystems and logical volumes for the package filesystem definition. These should reside in the shared disk.

   For most installations, HP recommends that the three directory trees **/krb5**, **/var/opt/dce**, and **/etc/opt/dce** be set up as logical volumes after the DCE software has been installed, but before DCE has been configured on the ServiceGuard cluster.

   Before running the DCE initial configuration program, manually mount these logical volumes on shared disk to be accessed from the primary node.
4. Once **dce_config** is invoked, it asks if the DCE Core services will be run under a ServiceGuard package. Answer **yes**. Then **dce_config** prompts for a “package hostname.” Enter the package hostname. From this point on, the **dce_config** script proceeds normally.
5. When the DCE configuration procedure is complete, the daemons for the core services are automatically started. Use **dce_config** to manually shutdown the DCE services that are running standalone.
6. Unmount and deactivate the volume group, which is in the shared disk.
7. Manually remove the IP address from the cluster with the following command:

   ```
   cmmodnet -r -i <package_IP> <SUBNET>
   ```

8. Halt the ServiceGuard cluster with the following command:

   ```
   cmhaltcl -f
   ```

Configuring the Package

Create a package for the DCE services that ServiceGuard can monitor with the following steps:

1. Create a directory for the DCE package name as follows:

   ```
   mkdir /etc/cmcluster/<pkg-name>.conf
   ```

2. Generate and modify the package configuration script for DCE as follows:

   ```
   cmmakepkg -p
   /etc/cmcluster/<pkg-name>/<pkg-name>.conf
   ```

   This command creates a template for <*pkg-name*>.

3. Edit this template for the DCE package by supplying the necessary information (for example: PACKAGE_NAME, NODE_NAME). Use the sample file **dcepkg.conf** for reference.

4. Create a control script for the package as follows:

   ```
   cmmakepkg -s /etc/cmcluster/<pkg-name>/rc.<pkg-name>
   chmod 755 /etc/cmcluster/<pkg-name>/rc.<pkg-name>
   ```

   Each package has a control script that starts and stops services for the package.

5. Modify the DCE Package information in the control script (**rc.**<*pkg-name*>) to include the logical volume name, IP address, service name, service and monitoring script names (for example: **dce.start** and **dce.monitor**).

   Read the sample control script **rc.dcepkg** carefully and make the similar change in the new control script (rc.<*pkg-name*>).

6. Copy the standard DCE configuration file to your package directory. Enter the following command:

   ```
   cp /etc/rc.config/dce /etc/cmcluster/<pkg-name>/dce
   ```

7. Modify the configuration file **/etc/cmcluster/**<*pkg-name*>/**dce** to restrict IP address to package IP address. To do this, set the environment variable RPC_SUPPORTED_NETADDRS.
8. Create the package startup script using **dce.start** as a sample template. Set the environment variable SG_DCE_BASE_DIR to **/etc/cmcluster/**<*pkg-name*>.
9. Create the DCE monitor script using **dce.monitor** as a sample template. Set the environment variable SG_DCE_BASE_DIR to **/etc/cmcluster**/<*pkg-name*>.
10. Create the DCE daemon restart script using **dce.restart** as a sample template. Set the environment variable SG_DCE_BASE_DIR to **/etc/cmcluster**/<*pkg-name*>.

Distributing the Package

To distribute the package follow these steps:

1. Distribute the package configuration and control scripts across the nodes. From the primary node, enter:

```
rcp -r /etc/cmcluster/<pkg-name> \
<secondary_node>:/etc/cmcluster/<pkg-name>
```

2. Verify that the configuration scripts are correct. From the primary node, enter:

```
cmcheckconf -C /etc/cmcluster/cmclconfig.ascii \
-P /etc/cmcluster/<pkg-name>/<pkg-name>.conf
```

NOTE This command fails if the ServiceGuard daemons are running.

3. Apply the configuration on the cluster. From the primary node, enter:

```
cmapplyconf -v -f -C /etc/cmcluster/cmclconfig.ascii \
-P /etc/cmcluster/<pkg-name>/<pkg-name>.conf
```

NOTE This command fails if the ServiceGuard daemons are running.

Starting the ServiceGuard Cluster

The ServiceGuard cluster can be started automatically after a system boot. To do this, modify **/etc/r.config.d/cmcluster** and set the environment variable AUTOSTART_CMCLD to 1.

1. To manually start the ServiceGuard cluster services, enter:

   ```
   cmruncl -v -n <primary_node> -n <secondary_node>
   ```

2. To view the cluster status, enter:

   ```
   cmviewcl -v
   ```

Starting the Package on the ServiceGuard Cluster

Configured packages are started automatically on their primary nodes when the ServiceGuard cluster is started. Packages on the ServiceGuard cluster can be halted manually. To restart a package, use SAM or follow these steps.

1. To restart the package on a specified host, enter:

   ```
   cmrunpkg -n <host> <package name>
   ```

2. To reenable packet switching after halting the package, enter:

   ```
   cmmodpkg -e <host> <package name>
   ```

See *Managing MC/ServiceGuard* for procedures on using SAM to administer MC/ServiceGuard clusters and packages.

Summary of DCE-MC/ServiceGuard Installation and Configuration

The following steps summarize the process of installing and configuring DCE with MC/Service Guard.

1. Install the MC/ServiceGuard cluster.
2. Start the MC/ServiceGuard cluster.
3. Identify and mount the shared volumes manually from the primary node.

4. Identify the hostname and IP address to be dedicated for the DCE package.
5. Manually activate the package IP address from the primary node using the **cmmodnet** command.
6. Configure DCE Core Services.
7. When the above configurations are complete, the DCE daemons will start up automatically. Stop them manually using **dce_config**.
8. Manually unmount and deactivate the shared volume.
9. Manually deactivate the package IP address from the primary node using the **cmmodnet** command.
10. Configure the DCE package scripts.
11. Apply the Package Configuration on the ServiceGuard cluster.
12. Start the ServiceGuard cluster.

6 HP-UX Integrated Login

This chapter describes the HP-UX Integrated Login product, which became available with HP-UX 10.0. In addition, this chapter discusses how to use the HP-UX Integrated Login product with UNIX and other authentication technologies.

Overview

At release 10.0, HP-UX made available a new HP-UX Integrated Login product that differs from the DCE-Integrated Login Utilities provided on HP-UX 9.x systems. Whereas DCE-Integrated Login Utilities are tightly coupled with DCE, HP-UX Integrated Login is designed to modularly combine UNIX login with various authentication technologies, including DCE.

HP-UX Integrated Login combines UNIX login with other authentication technologies. It provides a generic interface which login applications can use to interface with various user-authentication technologies.

NOTE Connection initiated via Secure Internet Services (SIS) will not result in DCE credentials on the server.

This release offers the following authentication technologies:

- UNIX mechanism (**/etc/passwd**)
- DCE Security Services

On a system using HP-UX Integrated Login, the authentication technology is configured by a system administrator. The configuration chosen is known as the “authentication policy” and all Integrated Login utilities on the system enforce that policy. An authentication policy specifies the following:

- The *login technology*— The preferred user-authentication technology for granting access to the local system.
- The *fallback technology*— The backup authentication technology, which is used when the preferred login technology is unavailable or fails.
- *Additional technologies*— Technologies, in addition to the login technology, for which user authentication should be done once access to the local system is granted.

HP-UX Integrated Login allows system administrators to utilize authentication technologies other than the traditional UNIX scheme (**/etc/passwd**) to better secure their machines. It also provides flexibility, as system administrators can vary the configurations of machines depending on desired levels of security. As an example, consider a DCE cell. One system in the cell might be configured to grant system access using the traditional UNIX mechanism, and then obtain DCE credentials as an additional technology. Another system might, for greater security, have DCE configured as the login technology, using UNIX login only as a fallback technology.

Use of HP-UX Integrated Login is optional. All integrated utilities retain standard HP-UX behavior until HP-UX Integrated Login is activated. If you wish to use HP-UX Integrated Login, carefully read and follow the instructions in this chapter.

Deciding Whether to Use HP-UX Integrated Login

Use HP-UX Integrated Login:

- If you want to use an authentication technology other than the traditional UNIX mechanism as the login technology. For this release, this means using DCE Security Services.
- If you want to obtain additional credentials from other authentication technologies after machine access is granted via the login technology. For this release, this means getting DCE credentials after logging in via the UNIX mechanism.
- If each user can have the same password across all configured technologies.
- If you want to configure DCE as the login technology, see “Deciding Whether to Integrate DCE with HP-UX Integrated Login” in this chapter.

Operation of Integrated Login Utilities

The Integrated Login utilities are **login**, **dtlogin**, **dtsession**, **su**, and **ftpd**. The utilities **passwd**, **chfn**, and **chsh** are also integrated to facilitate the manipulation of registries (such as the registries for technologies used by HP-UX Integrated Login.) The Secure Internet Services (SIS) version of **ftpd** is not integrated. The SIS versions of **rlogin** and **telnet** provide the integrated login service when login on the remote system requires a password.

- The Integrated Login utilities attempt to first authenticate a user via the login technology. If the login technology is not available or fails, and a fallback technology is configured, the user is authenticated via the fallback technology. If none of the authentications succeed, then the user is denied access to the local system. Note that fallback will not occur if the login technology specifically denies access to a user (such as the user name is recognized, but the password is incorrect; or a time-based authorization does not allow the user to log in at that time).
- After a user is successfully logged in, the Integrated Login utilities attempt to authenticate the user to all additional technologies configured. Any failure in this step is not fatal. The user is still allowed to log in and is appropriately warned of the failures.
- Upon unlocking the HP-CDE session, the integrated **dtsession** attempts to refresh all credentials a user has obtained through integrated **dtlogin**.
- If **passwd** successfully changes a user's password in the login registry, it also attempts to make the change in the registries of all other technologies configured.
- **chfn** and **chsh** change a user's finger and shell information only in the registry for the primary (**-l**) login. The DCE registry is the primary registry if you configure Integrated Login with **-l dce**.

Activating HP-UX Integrated Login

The Integrated Login utilities are provided in the AUTH-COMMON file set. They are installed, but not activated, when the file set is first loaded. However, when you update the file set, if HP-UX Integrated Login has been activated prior to the file set being updated, the integrated utilities remain active after the update.

The binary names for the integrated utilities are:

/usr/lbin/ftpd.auth

/usr/bin/chfn.auth

/usr/bin/chsh.auth

A script, **/usr/sbin/auth.adm**, is provided to activate HP-UX Integrated Login and configure a system authentication policy. Until activated, all Integrated Login utilities retain standard HP-UX behavior. For the utilities without separate binaries, **auth.adm** activates Integrated Login by creating an appropriate **/etc/pam.conf** file.

When using HP-UX Integrated Login with the default DCE registry, users who configure DCE as the primary login technology should not configure UNIX as a fallback technology. See “Configuring ux as a Fallback Technology for DCE” later in this chapter for more information.

To activate HP-UX Integrated Login and configure an authentication policy, follow these steps:

1. Log in as **root**
2. Issue the **auth.adm** command, as follows:

```
/usr/sbin/auth.adm -i[nstall] -l tech_name [-b tech_name]\
[-a tech_name[:tech_name]...]\
[-p tech_name:param=value[:param=value]...]...
```

   where

   -l tech_name specifies the authentication technology to be used for system login. This specification is required.

   ux—To specify the UNIX mechanism (**/etc/passwd**)
   dce—To specify the DCE Security Service

-b *tech_name* specifies the authentication technology to be used for fallback login. This technology is used when the preferred login technology is unavailable or fails. This specification is optional. If no fallback technology is explicitly configured, there will be no fallback login in case of unavailability or failure of the login technology.

-a *tech_name[:tech_name]* specifies the authentication technologies from which to obtain additional credentials after system login. This specification is optional.

-p *tech_name:param=value[:param=value]* specifies the values of parameters applicable to an authentication technology being configured. Parameters of different technologies can be specified by repeating the -p[arameter] option. The list of configurable parameters is as follows:

TIMEOUT — Timeout (in seconds) on communications with authentication technology. Default values are:

u—120 seconds
dce—120 seconds

WARNPWDEXP — Password expiration warning period (in days). If the user's password is due to expire within the specified number of days, the user receives a warning message during login. This parameter applies to DCE technology only. If this parameter is not specified, no warning is given.

FORCEPWDCHANGE — Password force-change period (in days). If the user's password is due to expire within the specified number of days, the user is forced to change the password before login is allowed. This parameter applies to the DCE technology only. If this parameter is not specified, a password change is not forced.

FORWARDABLETGT — Enable DCE TGT to be forwardable. When forwarding a user's DCE TGT from machine A to machine B, it enables the user from machine A to reuse its Kerberos credentials on machine B. A parameter value is required, but its content is ignored. This parameter applies to DCE technology only.

Default values are used when no parameter values are specified.

The following example commands activate HP-UX Integrated Login and set the configuration as described:

```
/usr/sbin/auth.adm -install -l dce -b ux
```

Configuration is set to log in the user upon successful password verification by DCE. If DCE is not available, login is effected via **/etc/passwd**. Note that this strategy works only if the HP-UX and DCE passwords are identical.

```
/usr/sbin/auth.adm -install -l ux -a dce
```

Configuration is set to log in the user upon successful password verification by **/etc/passwd**. This configuration specifies that after machine access has been granted, a DCE login should also be performed.

3. Inspect the file **/var/adm/ilogin/auth.adm.log** for ERROR messages. If there are ERROR messages, correct the error conditions and repeat step 2.
4. **auth.adm** performs the following actions during the activation process:
   - Verifies that the policy is an acceptable one.
   - Activates the login technology.
   - Activates the fallback technology.
   - Activates additional technologies.
   - Makes the Internet super-server **inetd** invoke **ftpd.auth** instead of **ftpd** by modifying the **/etc/inetd.conf** file.
   - Records the configured authentication policy in a policy file, **/etc/auth.conf**. This file triggers the Integrated Login utilities to enforce the authentication policy. If **auth.conf** does not exist or its content is corrupted, the login utilities that have separate binaries fall back to standard HP-UX behavior. The policy file follows a predefined format. *Do not edit this file.* To change a policy on a system, reconfigure it with the new policy using the **auth.adm** command.
   - Saves the current version of **pam.conf** and creates a new version; the behavior changes as soon as the new **/etc/pam.conf** has been created.

The activation process terminates with an error message when any of these steps fail. One exception to this is the activation of additional technologies. If **auth.adm** fails to activate any of the additional technologies, it continues on after issuing a warning message and removing the corresponding technology from the authentication policy.

Deactivating HP-UX Integrated Login

To deactivate HP-UX Integrated Login and remove the authentication policy on a system, do the following:

1. Log in as **root** and issue the following command:

   ```
   /usr/sbin/auth.adm -u[ninstall]
   ```

   auth.adm restores the old version of **/etc/pam.conf**; the behavior of the utilities without separate binaries changes as soon as the old **/etc/pam.conf** has been restored.

2. Inspect the file **/var/adm/ilogin/auth.adm.log** for ERROR messages. If there are ERROR messages, correct the error conditions and repeat step 1.

Inquiring about Authentication Policy

To inquire about the authentication policy of a system running HP-UX Integrated Login, run the command:

```
/usr/sbin/auth.adm -q[uery][-f filename]
```

The command will print the authentication policy to **stdout**, or -*filename* if **-f** *filename* is specified. You do not have to be **root** to run this option of the command.

Notes, Cautions, and Warnings

- HP-UX Integrated Login on 10.x is not an upgraded version of DCE-Integrated Login Utilities for 9.x systems. Its activation tool is **/usr/sbin/auth.adm**. You cannot use **dce.login**, the 9.x activation tool for DCE-Integrated Login, to activate HP-UX Integrated Login.
- When changing passwords using **passwd**, the password format rules imposed by the login technology restrict the format of newly-entered passwords. A new password that is acceptable to the login technology might be rejected by an additional technology which has more stringent password format rules. To ensure that passwords in all registries can be synchronously changed, configure the login technology to have the password format rules used by the strictest technology employed on that machine.

  To change passwords in just one registry, run **/usr/bin/passwd** with the **-r** option. The syntax is as follows.

  ```
  /usr/bin/passwd -r tech_name [username]
  ```

  where *tech_name* is one of the approved abbreviations of authentication technologies. For example, the following command changes the DCE password of the logged-in user:

  ```
  /usr/bin/passwd -r dce
  ```

  Beginning with DCE 1.3.1, HP-UX Integrated Login provides support for HP-UX Commercial Security. However, note the following restriction and caution. To activate Integrated Login on a Commercial Security Trusted System, you must specify **ux** as the login technology. Other login technologies can be configured to perform additional authentications after machine access has been granted by the Commercial Security authentication mechanism. If you have configured Integrated Login on a standard system with a login technology other than **ux**, do not convert that system to a Commercial Security Trusted System. The following example command activates Integrated Login on a Commercial Security Trusted System with DCE as an additional authentication technology:

  ```
  /usr/sbin/auth.adm -i -l ux -a dce
  ```

Synchronization of passwords between DCE and an HP-UX Commercial Security Trusted System cannot be achieved through the **passwd_export cron** job. Such synchronization can only be achieved by separately modifying a user's DCE and HP-UX passwords to be the same.

DCE passwords are global to a network, whereas the Commercial Security passwords are local to a single system. To change a password when using DCE with Commercial Security, first change it for HP-UX and DCE on one system. This can be done in one step with the **passwd** command, provided the new password chosen is acceptable to both HP-UX and DCE. Then change it on all the other HP-UX systems on which you have an account by using the **passwd** command with the **-r** option.

- CDE cross-cell login initiates fail-safe sessions only. You cannot obtain a full CDE session if you want to do cross-cell authentication.

NOTE Users logged in to a foreign cell cannot use the **passwd** command to change a password.

Integrating DCE with HP-UX Integrated Login

HP DCE/9000 provides support for integrating DCE with HP-UX Integrated Login. The binaries for this functionality are included in the AUTH-DCE file set.

Overview of HP-UX Integrated Login Features

The HP-UX Integrated Login utilities provide the following features:

- If DCE is configured as the login technology, the Integrated Login utilities authenticate users via the DCE Security Registry, giving users DCE credentials upon HP-UX login. This makes it possible for system administrators to use DCE as the primary source of user information.
- If DCE is configured as an additional technology, the Integrated Login utilities attempt to get DCE credentials for a user after the user successfully logs in via another technology.
- In HP-CDE, each window created during an HP-CDE session inherits the user's DCE credentials. (Otherwise, a user would have to run **dce_login** in every window in which DCE operations are desired.)
- Integrated **dtsession** refreshes DCE credentials upon unlocking the HP-CDE session.

Deciding Whether to Integrate DCE with HP-UX Integrated Login

If you want to configure DCE as the login technology with HP-UX Integrated Login, consider the following:

- The system environment must be stable. Therefore, DCE must be left configured and the DCE cell must be maintained. The network must remain reliable 24 hours a day.
- 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.

- NIS access is disabled for password and group mapping.
- The system must not be configured with HP-UX Commercial Security.

For a discussion of the Integrated Login support for Commercial Security and how to configure it, see "Notes, Cautions, and Warnings" earlier in this chapter.

Operation of the HP-UX Integrated Login Utilities

The HP-UX Integrated Login utilities function in the same way as their HP-UX counterparts, with the following exceptions:

- Most commands provide additional messages when DCE authentication is unavailable.
- The **passwd**, **chfn**, and **chsh** utilities manipulate the DCE registry. They will fail if the DCE network registry cannot be reached. These commands synchronously change the DCE registry. The **passwd** command supports the password generation and password strength checking features provided by HP DCE Version 1.6 servers. However, if DCE is configured as an additional technology, you cannot use **passwd** to change a DCE password that is required to be generated. You must use **dcecp** instead.
- User **root** cannot change account information (such as passwords, finger information, and shell programs) of other users in the DCE Security Registry. The cell administrator must login as **cell_admin** and use **dcecp** or the HP-UX Integrated utilities (such as **passwd**, **chfn** or **chsh**) to change other users' information.
- Unlike user **root**, the cell administrator must provide **cell_admin**'s password when using the HP-UX Integrated **passwd** to change other users' passwords in the DCE Security Registry.
- User passwords are limited to 128 characters for **ftp**; otherwise, passwords can be up to 512 characters.
- HP-UX 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 an **.rhosts** file authorizes access

- Anonymous **ftp**

Preparing to Integrate DCE with HP-UX Integrated Login

Before integrating DCE with HP-UX Integrated Login on a system, you must prepare as follows. You can configure DCE as either the login technology or as an additional technology.

If you plan to configure DCE as the login technology:

- Configure the system as a DCE cell member.
- Set up a valid **root** account in the DCE Security Registry.
- Set up valid accounts in the DCE Security Registry for all users that require login access to the cell, or local login access to cell member systems. Use either **dcecp** or **passwd_import** to set up accounts.
- Decide whether to configure **ux** as the fallback technology, and, if so, whether to export DCE Registry data to **/etc/passwd** via a **passwd_export** entry in your **crontab** file. It is recommended that you use this mechanism to keep the local password file synchronized with the DCE Registry, in the event that fallback login is needed. (See “Activating HP-UX Integrated Login” in this chapter for further information.)
- Create entries in **/etc/opt/dce/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 **/etc/opt/dce/passwd_override**. The activation process 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.
- If necessary, use the **/etc/opt/dce/sys.group** and **/etc/opt/dce/group_override** files to override the entries in **/etc/group**. Use **group_override** to override **/etc/group** entries that have an account in the DCE Registry; use **sys.group** for those that do not.

The default **/etc/opt/dce/sys.group** file contains:

```
root::0:
other::1:
sys::3:
adm::4:
lp::7:
```

The default **/etc/opt/dce/group_override** file contains:

```
bin::2:
daemon::5:
mail::6:
```

If you plan to configure DCE as an additional technology:

- Configure the system as a DCE cell member.
- Set up valid accounts in the DCE Security Registry for all users that require login access to the cell. Use either **dcecp** or **passwd_import** to set up accounts.

When using **passwd_import** to set up accounts from **/etc/passwd**, 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 **dcecp** to assign a password to each account and to mark each account as valid.
- Does not create accounts from NIS information. However, you can run **passwd_import** on the source file used to generate the NIS map to import NIS information into DCE. You still have to mark valid and assign a password to each imported account.

See the *dcecp (8)* , *passwd_export (8)*, and *passwd_import (8)* man pages 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.

Configuring HP-UX Integrated Login with DCE

To integrate DCE with HP-UX Integrated Login in each DCE cell member system:

- Be sure that you have completed the steps in the previous section “Preparing to Integrate DCE with HP-UX Integrated Login”.
- Follow the instructions given in the section entitled “Activating HP-UX Integrated Login”. When issuing the command to activate HP-UX Integrated Login, substitute the string “dce” for the required *tech_name* field when specifying the authentication policy.

If DCE is specified as the login technology, **auth.adm** performs the following actions:

- Verifies that the system is not configured with HP-UX Commercial Security.
- Verifies that a **root** account exists in the DCE Security Registry.
- Copies the root account entry in **/etc/passwd** to **/etc/opt/dce/ passwd_override**.

During this process you are asked whether or not you want to set up a **cron** job to export information from the DCE Security Registry to **/etc/passwd**. If you choose to set up the **cron** job, the activation process also:

- 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 using the **crontab(1)** command. Frequencies greater than once per hour are not recommended.

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

Configuring ux as a Fallback Technology for DCE

You can configure **ux** as a fallback technology to allow system access when DCE, as a login technology, is not available (DCE down or network problem). If you wish to replicate information of the DCE Security Registry in **/etc/passwd**, do the following:

- Make sure the DCE Security Registry is not set up to hide exported passwords. When exported passwords are hidden, **passwd_export** does not export the encrypted passwords from the DCE Security Registry to **/etc/ passwd**. You can verify this property of the DCE Security Registry by running **dcecp** and issuing the command **registry show** at the prompt. You can disable hidden passwords by issuing the command **registry modify -hidepwd no** at the prompt. To change this property, you must have **cell_admin** DCE credentials.

NOTE If you wish to take advantage of the increased security provided by the DCE Security Registry hidden passwords policy, do not configure **ux** as a fallback technology. Specify DCE as the primary login technology, with no fallback login technology.

- Set up a **cron** job to export information from the DCE Security Registry to **/etc/passwd**. You are asked, during the activation process, whether or not to set up such a **cron** job. With your approval, a **passwd_export cron** job is set up to run every hour. You can adjust this frequency by using the **crontab**(1) command. Frequencies greater than once per hour are not recommended.
- If you wish to prevent a certain user from logging in to the local system, create an entry for that user in the **passwd_override** file and place the word “OMIT” in the password field of the entry. **passwd_export** will exclude those entries from **/etc/passwd** when transferring information from the DCE Security Registry.

Users who configure DCE as the primary login and UNIX as the backup technology should be aware that the UNIX backend is useful as a backup only for names and passwords that meet UNIX requirements, restrictions, and semantics. Also, be aware that configuring the UNIX backend as a backup technology can cause the following known problems:

- If the DCE registry enforces hidden passwords (which it does by default), an asterisk (*) is placed in **/etc/passwd** for all entries and the UNIX backup will be unable to process any password. Therefore, configuring UNIX as the fallback login technology will fail to authenticate the user and cause confusion when attempting to change a password. Unless you plan not to enforce hidden passwords, do not configure UNIX as the backup technology.
- The UNIX backend will fail for any username longer than eight characters, which is the maximum length for a UNIX username. Specifically, this means that:
  - ✓ If the primary login technology fails (for example, if **secd** is down) the UNIX backup technology will deny system access to users with long usernames.
  - ✓ If **secd** is down, the UNIX backup technology will not allow users to use the **su** command to access accounts that have long usernames.
  - ✓ If **secd** is running and the user enters the **passwd** command to change the password for an account with a long username, the UNIX backup technology will not process the password change. Specifically, the following messages will display:

    ```
    Password successfully changed in DCE registry
    Invalid login name.
    ```

    The first line in the message indicates that the password has been changed in DCE. The second line indicates that the password information in **/etc/passwd** is unchanged because of the UNIX restriction on the long usernames.
  - ✓ If **secd** is running, DCE will deny access to the machine to any users with long usernames whose accounts are set to **pwdvalid no**, or who use the **force_pwd_expiry** <*n*> feature and whose passwords will expire within *n* days.
- DCE allows cell_admin to change the password of any other principal. However, UNIX does not allow this behavior. Therefore, if a user logs in as **cell_admin** and tries to change another user's password, the following message will display:

  ```
  Password successfully changed in DCE registry
  Permission denied.
  ```

As shown in the preceding message, the password has been changed in DCE, but not in **/etc/passwd.** *To resynchronize the passwords, the user must login as* **root** *and run the* **passwd -r files** *command. This command changes the password in the* **/etc/passwd** *file only***.**

- UNIX allows the **root** user to **su** to any other user's account without prompting **root** for a password. DCE, however, cannot issue credentials without a password. Therefore, the **su** operation will appear to succeed, but the new user will not have DCE credentials.

Unconfiguring DCE from HP-UX Integrated Login

To unconfigure DCE without deactivating HP-UX Integrated Login, perform the steps in the section "Activating HP-UX Integrated Login", and specify a different authentication policy. To unconfigure DCE and deactivate HP-UX Integrated Login, follow the steps in the section "Deactivating HP-UX Integrated Login."

Notes, Cautions, and Warnings About Using HP-UX Integrated Login with DCE

- After configuring HP-UX Integrated Login with DCE as the login technology, do not activate HP Commercial Security. For Integrated Login support of Commercial Security and how to configure it, see "Notes, Cautions, and Warnings".

- If the **passwd_export cron** job has been set up and DCE becomes unavailable, the **cron** job will fail and generate an e-mail error message. To stop these error messages, remove the **cron** job by unconfiguring DCE from HP-UX Integrated Login after you stop or remove DCE.

- If you have set up a **passwd_export cron** job to update **/etc/passwd** with DCE Registry data, any changes you make to **/etc/passwd** will be lost when the **cron** job updates **/etc/passwd**.

- When DCE is unavailable and HP-UX Integrated Login is configured to fall back to **/etc/passwd**, if **/etc/passwd** has been updated with information from the DCE Security Registry, and the first 8 characters of the password a user enters at login match the first 8 characters of that user's DCE password, then the login will succeed even though the password entered may not be identical to the DCE password. The user will not, however, have DCE credentials.

- If you are logged in to DCE from a foreign cell, note that you cannot use the **passwd** command to change your password.
- The HP-UX Integrated Login utilities may not work when the system disk is full or disk quotas are exceeded. DCE requires disk space for the creation of temporary files.
- DCE credentials are not automatically removed when the user logs out. The administrator can set up a **cron** job to remove credentials when users log out as described in "Removing DCE Credentials" in Chapter 1.
- CDE requires that users have permission to write to their home directories. By default, **dcecp** and the Account Manager set a user's home directory to "/". To enable users other than **root** to write to their home directories, change the default home directory ("/") to a home directory that the user can write to, such as **/users/foo**. Failure to take this action could prevent users from accessing the system.
- If you are using cross-cell authentication to log in to a foreign cell, note that CDE cross-cell login initiates fail-safe sessions only. You cannot obtain a full CDE session that includes cross-cell authentication.
- Principals with a **passwd_override** entry (for example, **root**) cannot use the **passwd** command to change passwords in the **passwd_override** file. This can be done in two steps. First, use the **passwd -r files** command to change the password in the **/etc/passwd** file. Then, as **root**, cut and paste the appropriate password entry from **/etc/passwd** into **passwd_override.**
- By default, the HP DCE 1.6 Security Server disables logins for principals whose passwords have expired, and intervention by **cell_admin** is required before the principal can log in. If you want to allow a principal to log in with an expired password, attach an instance of the **passwd_override** ERA to that principal. See the *OSF DCE Administration Guide — Core Components* and the WARNPWDEXP and FORCEPWDCHANGE parameters in the section "Activating HP-UX Integrated Login" earlier in this chapter for information on how to manage password expiration.

DCE and Anonymous FTP

If you are using the HP-UX 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 **dcecp**, or use the **passwd_import** utility from a system that is supporting anonymous **ftp** (such as from a machine that has an entry for the **ftp** user in **/etc/ passwd**).
- 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, **/etc/opt/dce/ 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.

AFS and Kerberos Authentication

Support for AFS and Kerberos Authentication is not provided in this release of HP-UX Integrated Login.

7 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 Tool — dceping

HP DCE/9000 includes an HP-developed diagnostic tool, **dceping**. **dceping** provides information on the status of a client machine within its cell. The following is a brief description of **dceping**.

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 **/etc/opt/dce/hpadmin/nondcesvc**, or the per-user file **$HOME/.nondcesvc**. (See the *nondcesvc (4)* man page.) 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.

For additional details and command-line syntax, see the *dce_which (8)* and *dceping (8)* man pages.

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 name space. 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

The standard (OSF DCE) features for viewing the structure and contents of a name space enable you to:

- Display the name space
- Expand and collapse selected directories
- Filter the name space display
- Navigate the name space

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 name space. The HP CDS Browser provides the functionality of the **dcecp** for **cds*** and **acl** objects, and some of the capabilities of **dcecp** for **rpc** objects. With the HP CDS Browser, you can:

- Create, delete, and edit name space entries
- View attributes of name space entries
- View and edit ACL permissions of name space entries
- View and set CDS Browser options
- Manage replica locations
- Log in to DCE

Overview of Enhanced HP DCE CDS Browser Features

Creating and Deleting Entries

Menu options enable you to create and delete clearinghouse entries, directories, object entries, soft links, 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 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 time-out limit
- Cache data time-out 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 the Browser starts, an icon representing the root directory is the first item to be displayed in the window. Directories, soft links, and object entries all have distinct icons associated with them. 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)* man 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 soft link 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.

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 in the *cdsbrowser (8)* man 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 supplements the information in the *OSF DCE Administration Guide —Core Services* and *OSF DCE Administration Reference*.

Deleting a Clearinghouse

Before removing a CDS server clearinghouse, you must move or delete any directories having master replicas in the clearinghouse. If you do not do this, the clearinghouse removal operation fails, thereby preventing unintended loss of data.

Appropriate administration commands for clearinghouses and directories can be used to identify, move, or delete master replicas as required, in order to remove a clearinghouse.

Skulking Directories

CDS propagates updated name space information among all directory replicas with periodic automatic skulks so that consistent information is available throughout the name space. To conserve network bandwidth, these automatic skulks take place only every few hours.

Manual changes to the name space, such as the creation or deletion of any name space object or directory, should always be followed 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.

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

Resource Problems

It is important to configure sufficient resources for DCE according to the instructions in this manual. CDS can fail if a CDS server or client system runs out of system resources such as swap space, disk space, or kernel resources. Symptoms usually include a **cdsadv** or **cdsd** crash with one of a variety of error messages (which may not directly indicate the source of the problem.)

If a CDS problem is linked to a shortage of resources, stop DCE, free or configure more resources, and then restart DCE to bring the node back on-line in the cell.

Clock Reversal Problems

CAUTION

Timestamps are used in the CDS database to establish the order of events in changes to the name space. If the date/time on a DCE node is manually set backward more than a few minutes, the CDS database can become corrupted, crashing **cdsd**, and leaving the cell unusable. This is unrecoverable unless you have a recent backup. It is therefore imperative that manual clock resetting be avoided on DCE nodes.

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)* man page and in Internet RFCs 1032, 1033, 1034, and 1035.

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 name servers (such as instances of **named**) to query for information about foreign cells. The name server at localhost is usually preferred, as only localhost provides recursive query service—if localhost doesn’t have the requested data, localhost will query other name servers until it either finds the requested data or exhausts the list of name servers that it knows about.

Using localhost reduces the requirement to keep GDA informed when name server 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 name server or name servers to query:

1. **gdad** first reads the file **/etc/opt/dce/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 name server(s) that **gdad** should query. The master format is described in the *named (1M)* man page.
2. If **named.ca** is not found or does not contain NS records, then **gdad** looks for name servers in **/etc/resolv.conf**. The format of **resolv.conf** is described in the *resolver (4)* man page.
3. If neither **/etc/opt/dce/named.ca** nor **/etc/resolv.conf** exists, or if neither file contains name server 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 name server and part of the data from another name server. 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 name server.

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 name server 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 name server 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 name server 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 name server that serves the zone containing cell names, and obtain hostname A (Address) records from that server's cache data. If the name server 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 this document. 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).

(You can also derive this information, though in a different format, using the **dcecp directory show** command.)

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*"

   Where:

   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 *hostname.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 a principal from one cell is trusted by another cell; the second cell trusts that the first cell has authenticated the identity of the 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 **dcecp registry connect** command:

```
dcecp> registry connect /.../<foreign_cell_name> \
-facct cell_admin \
-facctpw <foreign_cell_admin_pwd>\
-group none\
-fgroup none\
   -org none\
   -forg none\
   -mypwd <local_cell_admin_pwd>
```

NOTE

At HP DCE 1.6, intercell logins by members of trusted cells are disabled by default to protect against insecure intercell logins. (This differs from standard OSF DCE 1.1 behavior.) If you want to permit intercell logins, specify one or both of the following options to the **dcecp registry connect** command:

-acctvalid — Marks the local cell account as a valid account. A valid local cell account allows users from the foreign cell to login to nodes in the local cell. The default is invalid.

-facctvalid — Marks the foreign cell account as a valid account. A valid foreign cell account allows users from the local cell to log in to nodes in the foreign cell. The default is invalid.

For example, to enable peer-to-peer trust between two cells and permit intercell logins in both directions between them:

```
dcecp> registry connect /.../<foreign_cell_name> \
-facct cell_admin\
-facctpw <foreign_cell_admin_pwd>
-acctvalid\-facctvalid\-group none\-fgroup none\
-fgroup none\
-org none\
-forg none\
-mypwd <local_cell_admin_pwd>
```

See “Creating Trust Relationships” in the *OSF DCE Administration Guide — Core Components* for detailed information on establishing peer-to- peer trust. See the online version of the *dcecp_registry* man page for information on the **acctvalid** and **facctvalid** options.

Miscellaneous Notes

This section contains miscellaneous information about HP DCE/9000 cell administration.

- 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 **/etc/ opt/dce/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, **/etc/opt/dce/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.
- DCE utilities and applications open **/dev/lan0** (or, depending on the configuration of the local host’s network interfaces, another **/dev/lan*** file) in order to obtain the local host’s IEEE 802 address. This address is used to generate UUIDs. HP’s DCE configuration tools ensure that **/dev/lan*** is world-readable. However, if you update the filesets UX-CORE or LAN after installing and configuring HP DCE, you should verify that **/dev/lan*** is readable by world.

8 HP DCE Measurement Service

This chapter describes the HP Distributed Measurement Service which permits you to monitor resource utilization of HP DCE 1.6 servers that run as **root**.

Overview of DMS

DMS provides performance instrumentation for DCE servers and for the server side of applications that use DCE Remote Procedure Calls (RPCs). When DMS is enabled, it collects data about RPCs that execute in the target process. The collected data is actually displayed using HP GlancePlus.

HP GlancePlus is a performance monitoring tool that provides visual information to help you identify potential or existing problems involving a system's CPU, memory, or LAN utilization. You can use GlancePlus to define critical processing thresholds and to set alarms that are triggered when the targets are approached. For information about HP GlancePlus, see *Getting Started with GlancePlus* and the GlancePlus online help. You can access the GlancePlus online help either from GlancePlus or from the Help Manager on the Front Panel.

DMS is based on the Open Software Foundation RFC 33.0 *Standardized Performance Instrumentation and Interface Specification for Monitoring DCE-Based Applications* (July 1995). DMS provides measurement of resource utilization (such as response time of components, error counts and rates, service counts and rates, queuing behavior, and so forth) and processing time (such as service time, queuing time, etc.) for DCE RPCs.

DMS Restriction

DMS has the following restriction:

A server runs as **root** if it is started by a process running as **root** or if it is owned by **root** and the **setuid** permission bit is set.

NOTE

In HP DCE 1.6, DMS can be enabled *only* for servers that run as **root**. Applications servers that do not run as **root** are not displayed in the DCE information fields of HP GlancePlus.

CAUTION

Do not run a server as **root** unless the server was designed to run as **root**.

DMS Prerequisite

You must install HP GlancePlus on the system where you intend to run DMS.

Enabling and Disabling DMS

DMS operates in three different modes:

- Disabled
- Inactive (the default)
- Active

You disable DMS by setting the environment variable DMS_FORCEOFF to any value and exporting the variable. (The software checks that DMS_FORCEOFF exists, not that the variable has any particular value.) DMS is also disabled when the effective-user-id (**euid**) of a process is not **root**.

DMS is inactive by default. DMS is inactive when a DCE process is running, DMS_FORCEOFF is not set, there is no instance of HP GlancePlus executing, and the process **euid** is **root**.

DMS is active when a DCE process is running, DMS_FORCEOFF is not set, and at least one instance of HP GlancePlus is executing, and the process **euid** is **root**.

Performance Considerations of DMS

If DMS is installed on your system, but disabled, it has no significant impact on the system or on the performance of the server.

If DMS is inactive, there is no significant performance impact on the system.

When DMS is active, there is normally a performance decrease of less than 5%; in some cases, HP GlancePlus and swapping may cause a throughput decrease of greater than 5%.

DMS Documentation

DMS documentation, like HP GlancePlus documentation, is in the form of online context-sensitive help. You can access the GlancePlus online help from the Help Manager (the “ **?**”) on the Front Panel.

Accessing DMS Data

After you start GlancePlus with the **gpm** command, you can select screens that display DCE metrics.

Five HP GlancePlus screens display DCE metrics:

- DCE Global Activities Window — Provides global status of DCE services on your system.
- DCE Process List Window — Provides a list of all DCE processes on your system running with **euid** equal to **root**.
- DCE Process Activity Window — Provides very detailed information about a DCE process selected in the Process List window.
- DCE Interface Window — Provides detailed information about the DCE interfaces for a DCE process selected in the DCE Process List Window.
- DCE Operation Window — Provides detailed information about the DCE operations in progress within a selected DCE Interface. You may choose which metrics are displayed in this window.

The following sections provide a brief description of the information provided in the windows. For more information, see the online help provided with DMS.

The DCE Global Activities window provides overview statistics for an RPC server; the remaining windows provide detail information about various DCE activities.

DCE Global Activity Window

The DCE Global Activity window displays detailed summary information about all of the DCE activities occurring on your system. The window includes two areas of focus:

- DCE activities of general interest — These metrics provide a global view of the DCE services running on your system.
- DCE summary information — These metrics provide a high-level view of total DCE activity on your system, including all DCE server requests and machine resource utilization for the DCE service.

For a definition of any metric, select the metric name by clicking on it using the right mouse button; a pop-up help window appears containing the definition of the metric.

DCE Process List Window

The DCE Process List Window displays a list of all processes running on your system that are DCE servers. For each process displayed, several metrics are available by default. You can customize the metrics displayed using the “Choose Metrics” command under the “Configure” pull-down menu. Each process shown can be selected or filtered.

For a selected process, you can obtain more detailed information. You generate this information by selecting the “Reports” pull down in this window and selecting “Process DCE Interface” or “Process Activity”. You can also select “Process Activity” by double-clicking on a process.

DCE Process Activity Window

The DCE Process Activity Window displays very detailed process information for a selected DCE process. All metrics available for the selected DCE process are displayed in a single window.

DCE Interface Window

NOTE Interface and operation names are not available in HP GlancePlus until after the first call to an interface. After the first call to an interface, the interface name and all of its operation names become available, but GlancePlus won’t pick up the interface and operation names unless you close the window and then re-open it. Interfaces, such as **rpc_mgmt** (which is exported by every DCE server and client), whose UUIDs and version numbers match interfaces that have previously been registered and named are available even before being called within a given process.

The DCE Interface Window displays a list of the interfaces associated with a DCE process. For each process displayed, several metrics are available by default. You can customize the metrics displayed using the “Choose Metrics” command under the “Configure” pull-down menu.

For a selected interface, you can generate a report on the DCE operations the system is performing with that interface. You generate the DCE Operations report by selecting the “Reports” pull down in this window and then selecting “DCE Operations”.

DCE Operations Window

The DCE Operations Window displays a list of the DCE operations the system is performing within a selected DCE interface. For each process displayed, several metrics are available by default. You can customize the metrics displayed using the “Choose Metrics” command under the “Configure” pull-down menu.