

Distributed Computing Environment
for Windows NT, Version 2.2:



Quick Beginnings

Distributed Computing Environment
for Windows NT, Version 2.2:



Quick Beginnings

Note

Before using this document, read the general information under "Appendix D. Notices" on page 51.

Second Edition (November 1998)

This edition applies to Distributed Computing Environment for Windows NT, Version 2.2 and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters.

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

IBM welcomes your comments. A form for readers' comments may be provided at the back of this publication. If the form has been removed, you may send your comments to the following address:

International Business Machines Corporation
Department VLXA
11400 Burnet Road
Austin, Texas
78758

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

© **Copyright International Business Machines Corporation 1997, 1998. All rights reserved.**

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

Tables	v	Unconfiguring DCE for Windows NT	25
Welcome to DCE for Windows NT	vii	Uninstalling Full DCE or a Slim Client from Windows NT	26
Conventions	vii	Migrating to DCE for Windows NT, Version 2.2	26
Chapter 1. What is DCE for Windows NT	1	Chapter 4. Obtaining Additional Information	31
More About DCE	2	Books	31
DCE Features and Benefits	2	Online Information	31
Product Contents.	3	Online Documents	31
Licensed Program Products	3	Online Help Files	31
Components	3	Viewing HTML Books	32
Compatibility and Interoperability with Other DCE Systems	5	Appendix A. Overview of Example Programs	33
Supported Transport Protocols	5	Appendix B. DCE Configuration	37
Functions and Enhancements.	5	Configuring DCE for Windows NT.	37
New OSF DCE Release 1.2.2 Functions	6	Using DCEsetup	37
New IBM Functions in DCE for Windows NT, Version 2.2	7	DCE Cells	37
Functions Available from DCE for Windows NT, Version 2.0	9	Configuring Your System as a DCE Client	39
Unsupported OSF DCE Features	16	Configuring Your System a DCE Server	41
Limitations of Supported Services	17	Enabling or Disabling Integrated Login	44
Chapter 2. Planning for DCE for Windows NT	19	Automatically Starting DCE at Boot Time	45
License Requirement	19	Unconfiguring.	45
System Requirements	19	Clobbering.	47
Hardware Requirements	20	Viewing Log Files	47
Prerequisite Software Requirements	21	Appendix C. Slim Client Limitations.	49
Chapter 3. Installing DCE for Windows NT	23	Appendix D. Notices	51
Installing	23	Trademarks	52
Configuring DCE for Windows NT.	24	Index	53
Configuring a Slim Client for DCE for Windows NT	25		
Unconfiguring a Slim Client for DCE for Windows NT	25		

Tables

1. Memory and CPU Requirements for Server and Client Systems	20	3. Example Programs	33
2. Disk Space Requirements for Each Component	20		

Welcome to DCE for Windows NT

Distributed Computing Environment for Windows NT, Version 2.2, (hereinafter called DCE for Windows NT) is jointly developed by IBM and Digital Equipment Corporation, and is based on Open Software Foundation (OSF) DCE 1.2.2 with enhancements provided by both Digital and IBM. OSF's DCE is a comprehensive set of services that support the development, use, and maintenance of distributed applications and enables diverse systems to work together masking the technical complexities of the network from the end user.

This book describes DCE for Windows NT, Version 2.2, and includes the following chapters:

- “Chapter 1. What is DCE for Windows NT” on page 1 provides an overview of the product, and product contents.
- “Chapter 2. Planning for DCE for Windows NT” on page 19 provides the planning information.
- “Chapter 3. Installing DCE for Windows NT” on page 23 outlines the installation procedure.
- “Chapter 4. Obtaining Additional Information” on page 31 includes references to additional information.

Conventions

Knowing the conventions used in this book will help you use it more efficiently.

- **Boldface type** indicates the name of an item you need to select, the name of a command, text the user types, or an example in running text.
- *Italics type* indicates new terms, book titles, or variable information that must be replaced by an actual value.
- Monospace type indicates an example (such as a fictitious path or file name) or text that is displayed on the screen.

Chapter 1. What is DCE for Windows NT

Distributed Computing Environment for Windows NT, Version 2.2 is based on the functions of the previous DCE for Windows NT, Version 2.0 and the new functions present in OSF DCE 1.2.2. This release offers new functions as well as enhancements to existing functions, which include:

- Kerberos V5 Interoperability (new to this release)
- Public Key Certificate Login support (new to this release)
- Slim Client (new to this release)
- CDS Preferencing (new to this release)
- DHCP client support (new to this release)
- RPC Code Set Conversion (new to this release)
- Operation in a Multiple Network Interface Card Environment (new to this release)
- Tunable Timeout Values for Configuration (new to this release)
- Tunable Timeout Values for RPC (new to this release)
- Microsoft Visual C++ Version 5.0 Support (new to this release)
- VisualAge C++ Support (introduced in the 2.0 release)
- Improved installation and configuration through InstallShield, prerequisite and corequisite checking, and GUI configuration (introduced in the 2.0 release)
- Unattended install (Silent Install) and cell configuration (introduced in the 2.0 release)
- Improved system management functions, including EMS, SNMP, access control list GUI, and user assistance aids (introduced in the 2.0 release)
- Integrated login between DCE and Windows NT (introduced in the 2.0 release)
- Improved cache for better performance (introduced in the 2.0 release)
- Expanded RAS capability (introduced in the 2.0 release)
- Improved data privacy feature for encryption of user data (introduced in the 2.0 release)

DCE for Windows NT is Year 2000 ready. When used in accordance with its associated documentation, it is capable of correctly processing, providing, and receiving date data within and between the twentieth and twenty-first centuries, provided all other products (software, hardware, and firmware) used with the product properly exchange date data.

For a complete list of the enhancements, see “Functions and Enhancements” on page 5.

Some features of the OSF 1.2.2 release are not supported by DCE for Windows NT, Version 2.2. See “Unsupported OSF DCE Features” on page 16 for a listing of the unsupported functions.

More About DCE

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

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

The DCE software includes a set of standard services; software interfaces, and tools that support the creation, use, and maintenance of distributed applications in a diverse computing environment.

DCE Features and Benefits

Distributed computing services, as implemented in DCE, provide an important enabling software technology for the development of distributed applications. Key benefits include the following:

- DCE makes the underlying network architecture transparent to application developers. It consists of a software layer between the operating system and network interface and the distributed application program.
- DCE provides a variety of common services needed for development of distributed applications, such as name and time services, and a standard remote procedure call interface.
- DCE provides a means for application developers to design, develop, and deploy distributed applications.

DCE for Windows NT provides these added benefits:

- It supports the Microsoft Windows NT Version 4.0 with service pack 3 and up. This allows deployment of DCE name servers or security servers on Windows NT, so that entire DCE cells can be based on Windows NT systems.

- It provides Windows-based GUIs and integrated online help for common DCE tasks. This makes configuration and management of DCE components quick and easy.

Product Contents

DCE for Windows NT is designed for the Microsoft Windows NT, Version 4.0 operating system and is based on the OSF DCE Release 1.2.2 code base. Like its IBM software server predecessors (DCE for AIX, and Directory and Security Servers for OS/2 Warp), DCE for Windows NT includes distributed computing technologies.

Licensed Program Products

DCE for Windows NT is available in the following Licensed Program Products:

- **DCE for Windows NT, Version 2.2** which includes the following:
 - IBM DCE Runtime Services for Windows NT
 - IBM DCE Cell Directory Server for Windows NT
 - IBM DCE Security Server for Windows NT
 - IBM DCE Application Development Kit for Windows NT
 - IBM DCE Slim Client for Windows NT
 - IBM DCE Client including Distributed File System for OS/2 Warp, Version 4
 - IBM DCE Runtime Services for Windows 95
 - IBM DCE Application Developer's Kit for Windows 95
- **DCE Runtime Services for Windows NT, Version 2.2**
 - IBM DCE Runtime Services for Windows NT
 - IBM DCE Slim Client for Windows NT
- **DCE Application Development Kit and Runtime Services for Windows NT, Version 2.2** which includes the following:
 - IBM DCE Application Development Kit for Windows NT
 - IBM DCE Runtime Services for Windows NT
 - IBM DCE Slim Client for Windows NT

Components

DCE for Windows NT is composed of the following components:

IBM DCE Runtime Services for Windows NT

Contains the following components that are necessary to configure your Windows NT system as a full DCE client:

Security client	RPC services
CDS client	Documentation
DTS	Event Management Services (EMS)

IBM DCE Cell Directory Server for Windows NT

Provides the additional DCE components to configure a Cell Directory Server (CDS) on your Windows NT system. The CDS server also includes the Global Directory Agent (GDA), which allows linking multiple CDS namespaces together with either X.500 or the Internet Domain Name Server (DNS).

IBM DCE Security Server for Windows NT

Provides the DCE Security server daemon required to configure a Security server on your Windows NT system.

IBM DCE Application Development Kit for Windows NT

Provides the tools required for developing DCE applications on the Windows NT operating system. The kit includes all DCE application programming interfaces, the IDL compiler, the SAMS compiler, as well as sample programs and example source code.

IBM DCE Slim Client for Windows NT

Provides the same programming environment to RPC-based applications as the full DCE client, but requires fewer resources such as RAM and DASD. It contains the following components: Slim Client, Additional Documentation, and NLV Libraries.

To include client systems running OS/2 Warp or Windows 95 in your DCE for Windows NT network, the following programs are also included:

IBM DCE Client including Distributed File System (DFS) for OS/2 Warp, Version 4

Contains the following components that are necessary to configure your OS/2 Warp system as a DCE client:

DFS client	DTS client
CDS client	RPC services
Security client	Documentation

IBM DCE Runtime Services for Windows 95, Version 2.X

Contains the following components that are necessary to configure your Windows 95 system as a DCE client:

Security client	RPC services
CDS client	Documentation
DTS client	

IBM DCE Application Developer's Kit for Windows 95, Version 2.X

Provides the tools required for developing DCE applications on the

Windows 95 operating system. The Developer's Kit includes all DCE application programming interfaces, the IDL compiler, the SAMS compiler, as well as sample programs and example source code.

Compatibility and Interoperability with Other DCE Systems

DCE for Windows NT complies with applicable OSF DCE Release 1.1, Release 1.2.1, or Release 1.2.2 specifications and interoperates with other IBM Software Servers (such as IBM AIX, IBM OS/2 Warp) and non-IBM DCE implementations (such as HP, Digital, Gradient, and Solaris).

DCE for Windows NT provides source-level runtime compatibility with DCE systems from other vendors for applications that conform to the OSF DCE Application Environment Specification (AES).

For more information on interoperability and compatibility issues, see the *readme.txt* file located in the DCE for Windows NT Program Folder.

Supported Transport Protocols

DCE for Windows NT provides RPC communications over the following transport protocols:

- TCP/IP (**ncacn_ip_tcp**)
- UDP/IP (**ncadg_ip_udp**)

Functions and Enhancements

OSF's DCE is a comprehensive set of servers that support the development, use and maintenance of distributed applications and enable diverse systems to work together cooperatively masking the technical complexities of the network.

DCE for Windows NT provides improvements in the areas of system management, application development support, installation and configuration, performance, and usability. These value-added enhancements and functions include the following:

New OSF DCE Release 1.2.2 Functions

- Kerberos V5 Interoperability

New IBM Functions in DCE for Windows NT, Version 2.2

- Public Key Certificate Login Support
- Slim Client

- CDS Preferencing
- DHCP Support
- Operation in a Multiple Network Interface Card Environment
- Tunable Timeout Values for Configuration
- Tunable Timeout Values for RPC
- RPC Code Set Conversion
- Microsoft Visual C++ v5.0 Support

IBM Functions Available from DCE for Windows NT, Version 2.0

- DCEsetup
- DCE Director
- Visual DCE ACL Editor
- VisualAge C++ Support
- Auto-Start
- Unattended Configuration
- Silent Install
- Integrated Login
- Remote DCE Client Configuration
- Name Service Interface Daemon
- Distributed Time Service (DTS) Providers
- Inline CDS Clerk
- CDS Cache Restructuring
- Credential Cache Cleanup
- Modifications to Internationalization
- Simple Network Management Protocol (SNMP)
- Commercial Data Masking Facility (CDMF)
- Event Management Service (EMS)
- MVS DCE Load Balancing Client Support
- DCE Control Program (dcecp) Extensions
- RPC Event Logger Utility
- IDL Compiler Enhancements
- Additional Example Programs
- Uninstall Procedure
- Enhanced Online Information

New OSF DCE Release 1.2.2 Functions

The following feature is from the OSF DCE Release 1.2.2:

Kerberos V5 Interoperability

The DCE security service includes an implementation of the MIT Kerberos Version 5 (V5) authentication and key distribution service. Prior to DCE 1.2.2 there had been no formal OSF DCE interoperability commitments.

New IBM Functions in DCE for Windows NT, Version 2.2

The following IBM functions and enhancements have been added to the existing functions available in DCE for Windows NT, Version 2.0:

Public Key Certificate Login Support

DCE for Windows NT supports the use of Entrust public key infrastructure to login to DCE. This allows DCE users to login and obtain DCE credentials using their public key certificate and their public-private key pairs that are generated by Entrust.

Users receive DCE credentials that allow them to use current Kerberos-based DCE security mechanisms. The users do not need to present either their traditional DCE secret-key password, or a public-private key pair that is generated by the DCE registry to login to DCE.

The online help file, *DCE Enhancements*, contains a full description of the Public Key Certificate Login.

Slim Client

In general, client systems are more likely to be memory constrained than server systems. In many cases, the configuration of a DCE client results in more DCE daemons being started than are necessary for the client, particularly if the client does not offer DCE services to other systems in a cell. The Slim client option reduces DCE memory consumption on client systems by starting a minimal number of DCE daemons and requires no cell administrator intervention for configuration (configurations are local only).

The Slim client provides the same programming environment to RPC-based applications as the full DCE client, but requires fewer resources such as RAM and DASD.

The online help file, *DCE Enhancements*, contains a full description of the Slim Client.

CDS Preferencing

This enhancement improves performance at CDS clients by providing a ranking to the order in which clearinghouses are contacted by the client for

CDS information. This can be accomplished automatically through the use of defaults associated with the location of CDS clients with respect to CDS servers or by manual overrides made by cell administrators.

The online help file, *DCE Enhancements*, contains a full description of CDS Preferencing.

DHCP Client Support

Dynamic Host Configuration Protocol (DHCP) is a client-server protocol that enables you to centrally locate and dynamically distribute configuration information, including IP addresses.

DHCP is supported for DCE clients only. DCE servers must have IP addresses that remain constant.

Operation in a Multiple Network Interface Card Environment

DCE for Windows NT, Version 2.2 is capable of running on Personal Computers (PCs) that have multiple Network Interface Cards (NICs). An environment variable will determine which network card DCE will use.

The online help file, *DCE Enhancements*, contains a full description of NIC.

Tunable Timeout Values for Configuration

DCE for Windows NT, Version 2.2 allows you to configure certain internal defaults for DCE functions by modifying the **usrstime.tcl** file in the **%DCELOC%\dcelocal\etc** directory. Through these modifications you can define certain default time-outs and intervals for configuration calls.

The online help file, *DCE Enhancements*, contains a full description of these parameters and their use.

Tunable Timeout Values for RPC

DCE for Windows NT, Version 2.2 allows you to configure certain internal defaults for DCE functions through environment variables. With environment variables you can define certain default time-outs for Security Server initialization, TCP connections and calls to CDS.

The online help file, *DCE Enhancements*, contains a full description of these parameters and their use.

RPC Code Set Conversion

The DCE for Windows NT 2.2 support for RPC Code Set Conversion varies in some key ways from the original OSF implementation. The codesets.idl interface has been modified to provide improved cross-platform support. The version number has been increased to 2.0, which is the version supported in other IBM implementations of DCE.

The online help file, *DCE Enhancements*, contains a description of the variations from OSF as well as important programming information and a revised version of the sample RPC program.

Microsoft Visual C++ v5.0 Support

This release supports the Microsoft Visual C++, Version 5.0 compiler.

Functions Available from DCE for Windows NT, Version 2.0

The following functions that were available in DCE for Windows NT, Version 2.0 are still supported in the current release:

DCEsetup

DCEsetup is a Windows-based graphical tool that simplifies configuration and management of DCE clients and servers. Using DCEsetup you can configure your DCE cell.

The online help file, *Configuring with DCEsetup*, contains a full description of DCEsetup.

DCE Director

The DCE Director is a Windows-based graphical tool that makes DCE management easier, including management of foreign cells and multiplatform cells. It allows a DCE user to perform many management tasks generally done by a cell administrator, such as:

- Creating, deleting, modifying, and browsing user accounts, security groups, and directories.
- Viewing and changing access control lists (ACLs) of CDS objects and application objects and determine whether security, CDS, and time servers are running.
- Configuring a remote client system by accessing and using configuration data established by the cell administrator.

The online help file, *Using DCE Director*, contains a full description of DCE Director.

Visual DCE ACL Editor

The Visual DCE ACL Editor is a Windows-based graphical tool that enables you to manage all DCE ACLs. You can set the permissions for all security-relevant objects within DCE, including Registry objects and CDS objects, and it supports inquiries about other users' access, copying ACLs, and modifying multiple ACLs at once.

The online help file, *Using Visual ACL Editor*, contains a full description of Visual DCE ACL Editor.

Silent Install

Silent Install enables automated electronic software distribution. When you use Silent Install it eliminates the need for the user to monitor their installation process or provide input.

The online help file, *DCE Enhancements*, contains a full description of Silent Install.

Unattended Configuration

DCE for Windows NT supports unattended configuration of DCE servers and DCE clients. Unattended configuration enables you to create a response file containing all required input for configuration. Invoking this file from a command line configures a server or client without requiring your continued presence.

The online help file, *DCE Enhancements*, contains a full description of Unattended Configuration.

VisualAge C++ Support

DCE for Windows NT provides continuing support for the VisualAge C++ compiler and adds support for the IBM VisualAge C++ compiler. The DCE for Windows NT Application Development Kit (ADK) works with both the Microsoft and IBM compiler. IBM Visual Age C++ provides a consistent set of tools, compiler technology, and class libraries that enable the portability of C and C++ source code across multiple, heterogeneous environments.

The online help file, *DCE Enhancements*, contains a full description of VisualAge C++.

Auto-Start

DCE for Windows NT provides an auto-start option that automatically starts DCE services during Windows NT startup. When enabled, this feature adds

the DCE Auto-Start Service to the list of services that are started automatically as part of the Windows NT startup procedure. Using Auto-start, you can synchronize the local system time with the cell time.

The auto-start feature is available through DCEsetup. The online help file, *Configuring with DCEsetup*, contains a full description of DCEsetup and its features.

Integrated Login

Integrated login automatically logs you into DCE when you log in to Windows NT. The integrated login feature is available during configuration with DCEsetup.

Also, the integrated login feature automatically updates your DCE password whenever you change your NT password. If you change the password using the Windows NT User Manager utility, the passwords do *not* remain synchronized.

The online help file, *Configuring with DCEsetup*, contains a full description of DCEsetup and its features.

Remote DCE Client Configuration

With DCEsetup Remote Client option, configuration of a client system into a DCE cell is quick and easy. An added benefit to using this configuration method is enhanced security; you can configure client systems without being given access to the cell administrator account. You can then access this configuration information to configure their client systems.

During remote client configuration, the cell administrator can create and store configuration information for DCE client systems in the centrally located DCE CDS namespace. You can then access this configuration information to configure your client systems from a single place.

The online help file, *Configuring with DCEsetup*, contains a full description of DCE setup and its features.

Name Service Interface Daemon

The Name Service Gateway, also known as the Name Service Interface Daemon (nsid), provides access to DCE name services from native Microsoft RPC applications. The nsid runs on one or more DCE systems in the cell and performs the operations of the DCE RPC name service interface (NSI).

The online help file, *DCE Enhancements*, contains a full description of Name Service Interface Daemon.

Distributed Time Service (DTS) Providers

DCE for Windows NT includes DTS time provider applications that work in conjunction with the DTS to provide an accurate time source. When a time provider is started, it becomes the sole time provider for the DTS service.

The online help file, *DCE Enhancements*, contains a description of Distributed Time Service.

Inline CDS Clerk

The CDS clerk runs as a shared library running within the client's address space. This shared library clerk code, known as the inline clerk, eliminates the necessity and overhead of a separate process for every unique user name attempting to use CDS.

CDS Cache Restructuring

The cache is now divided into a shared cache and private caches. These private caches are also known as per-user caches.

The shared cache contains data that is global in nature, and that is accessible to all users, such as CDS clearinghouses. The CDS Advertiser controls the shared cache—creating, updating, and periodically flushing it. User applications can read data in the shared cache, but cannot write data to it.

Per-user caches contain private data, such as CDS objects that can be viewed only by the cache owner. If a per-user cache is populated with all the data that an application needs, that application can run without starting the Advertiser.

When a user application requires CDS information, the per-user cache is searched. If the information is not found, the search is extended to the shared cache. If the information is not located there, the CDS server is contacted.

Credential Cache Cleanup

The credentials cache cleanup feature optimizes disk space. It consists of a thread that runs at regular, settable intervals to clean up the credentials directory. It searches the directory for files belonging to credentials that have expired and deletes those files, which frees disk space.

Modifications to Internationalization

DCE uses the X/Open XPG4 locale programming model for internationalization. Internationalized Windows NT applications can use this model, or they can use the traditional Windows NT country environment model. Although DCE is designed to use the locale model, it accommodates the Windows NT internationalization programming and operating environments. Most existing internationalized Windows NT applications do not need to be changed when running on DCE.

The online help file, *DCE Enhancements*, contains a full description of the modifications to Internationalization.

Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) provides network management support in the TCP/IP environment for monitoring DCE resources and services. System administrators and system management application programmers can use SNMP to easily monitor the DCE environment so that they can focus on making their resources and services more manageable. An SNMP network management system consists of the following:

- One or more network elements (nodes), each containing an SNMP agent
- One or more Network Management Stations (NMS) containing an SNMP manager
- A network management protocol

The online help file, *DCE Enhancements*, contains a full description of SNMP.

Commercial Data Masking Facility

Commercial Data Masking Facility (CDMF) provides data privacy support for customers outside the U.S. and Canada. Like the Data Encryption Standard (DES) provided in OSF DCE, CDMF supports RPC application encryption and GSSAPI message encryption.

CDMF was developed by IBM as an alternative to DES, because distribution of the DES encryption algorithm for data privacy support outside the U.S.A. is regulated by the U.S.A. Government. CDMF has export approval from the U.S. Government and is compatible with DES.

To support data privacy with CDMF, a new privacy level for communication between clients and servers is introduced. For GSSAPI message encryption, a new parameter for **gss_seal** and **gss_unseal** is added.

The online help file, *DCE Enhancements*, contains a full description of CDMF.

Event Management Service

The Event Management Service (EMS) manages event services in a DCE cell. EMS supports asynchronous event suppliers (any DCE core service or DCE-based application) and event consumers (any application with an interest in receiving asynchronous events from one or more DCE processes) and sets up an event channel between them to support asynchronous communication. EMS also provides a filtering mechanism to enable administrators and consumers control over which event EMS will send, and it provides integration for DCE clients and servers using the DCE Serviceability (SVC) and Audit interfaces.

EMS consists of:

- The EMS daemon (emsd) includes consumer and supplier registration, event type and filter support, and event forwarding
- Integration with SVC and Audit
- API support for development of supplier and consumers (libems)
- DCE Control Program (dcecp) support for administration of EMS

The online help file, *DCE Enhancements*, contains a full description of EMS.

MVS DCE Load Balancing Client Support

DCE for Windows NT includes support for load balancing in an MVS parallel sysplex environment. This support allows the automatic rerouting of rpc calls from one host to another for load balancing.

With this support, DCE client requests are routed to servers based on the capacity and loads on the MVS parallel sysplex. DCE load balancing enables customers to better use system resources in a parallel sysplex environment on MVS, when that support becomes available in MVS DCE.

The online help file, *DCE Enhancements*, contains a full description of Load Balancing.

DCE Control Program (dcecp) Extensions

DCE for Windows NT product provides extensions to the DCE Control Program (**dcecp**). **dcecp** offers a common command line interface for managing DCE services.

The online help file, *DCE Enhancements*, contains a full description of the **dcecp** extensions.

RPC Event Logger Utility

The RPC Event Logger provides enhanced application debugging support beyond that provided by OSF DCE. The Event Logger records information about operations relating to the running of an RPC application. When enabled, the Event Logger creates a separate log for each client and server process. The application developer can log all events or can specify the type of event to be logged. Events can include those relating to application calls, context handles, logging operations, errors, and miscellaneous events.

The online help file, *DCE Enhancements*, contains a full description of the RPC Event Logger.

IDL Compiler Enhancements

The DCE for Windows NT Interface Definition Language (IDL) compiler includes several enhancements. Some of these enhancements are provided with the OSF DCE Release 1.2.2 IDL compiler, while others offer value-added functionality.

The online help file, *DCE Enhancements*, contains a full description of the IDL Compiler Enhancements.

Additional Example Programs

The DCE for Windows NT Application Development Kit provides a full range of example programs. In addition to the standard OSF example programs, this includes programs designed specifically for use with Windows NT. Also included are programs written in C++ that illustrate the use of distributed objects.

For more information, see “Appendix A. Overview of Example Programs” on page 33.

Uninstall Procedure

DCE for Windows NT provides a procedure for uninstalling that removes all Windows NT Registry entries related to the DCE kit, and then deletes the executable files and directory tree where DCE is installed.

For more information, see “Uninstalling Full DCE or a Slim Client from Windows NT” on page 26.

Enhanced Online Information

The online information has been enhanced to provide the following:

- OSF documentation set, in native Windows Help format
- Important product-specific online information in the form of Troubleshooting and DCE Enhancement help files

The online help file, *DCE Enhancements*, contains a full description of the online enhancements.

Unsupported OSF DCE Features

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

Unsupported Services:

- Security:
 - Transitive Trust in a cell hierarchy
 - The Public Key Certificate Management API
 - The Private Key Storage server
 - User-to-User Authentication
 - Global Groups
- Directory:
 - Hierarchical Cells
 - Global Directory Service (GDS) is not provided in this release. However, GDS can exist in the same cell and be used for intercell communications, if it is provided by another vendor.
- RPC
 - Single-threaded RPC

Unsupported Commands:

- Security:

The **sec_salvage_db**, **rlogin**, **rlogind**, **rsh**, and **rshd** commands supplied by OSF
- Distributed Time Service:

The **dtss-graph** command, which converts synch trace to PostScript

Unsupported Subroutines : The DFS APIs are not supported.

Limitations of Supported Services

There are several limitations for accounts that use Public Key Certificate Login. These include:

- The **kinit** command cannot be used to refresh expired DCE credentials unless the DCE password is provided. Using the Entrust user profile and passphrase for this refresh operation is not supported. If the Entrust user profile name and passphrase are synchronized with the DCE principal name and password, this limitation is transparent to the user.
- When multiple Entrust users are mapped to a single DCE principal, the level of detail of DCE functionality such as auditing and access control is reduced. Only the DCE principal information is available and used in audit records and access control checks.
- If the *pwd_val_type* ERA that requires password strength checking is attached to a DCE principal, these checks are only enforced on the DCE password for that principal. The Entrust PKI establishes a separate set of rules which are enforced on the Entrust passphrase.
- The key management API is used only by applications that use the shared-secret key authentication protocol. Application servers cannot use the public key certificate login protocol.
- When using GSSAPI, the DCE administrator must set up an account in the DCE registry database for the initiator and the acceptor. The acceptor cannot use Public Key Certificate Login. No restrictions apply to the account for the initiator.

OSF DCE 1.2.2 Public Key Login Support has the following limitations:

- The DCE Security Server supports login requests from DCE clients that support the OSF 1.2.2 public key login protocol. The OSF 1.2.2 protocol uses public-private key pairs that are generated by the DCE Security Server itself. This feature is separate from the IBM Public Key Certificate Login feature for DCE that supports login requests based on public key information that is generated by the Entrust public key infrastructure.
- The DCE client does not support the use of the OSF 1.2.2 public key protocol to login to DCE. For compatibility and interoperability purposes, the DCE Security Server supports these login requests from other DCE clients that do use the protocol.

Chapter 2. Planning for DCE for Windows NT

Before you install any software read System Requirements and Disk Space Requirements to ensure that your system satisfies the specified software and hardware requirements. Also, make sure you read the online readme file that is located on the CD in the following directory.

```
x:\language\documentation\readme.txt
```

Where

x is the drive for the CDROM

language is the language in which you want the readme file displayed. For example:

```
g:\English\documentation\readme.txt
```

License Requirement

You must be licensed to install and run the Runtime Services, Application Development Kit, Cell Directory Server, or Security Server options.

System Requirements

To install Distributed Computing Environment for Windows NT, Version 2.2, you need the following:

- **Server:** An Intel-based system at Windows NT 4.0 Server or Workstation with Service Pack 3 or higher installed
- **Client:** An Intel-based system at Windows NT 4.0 Server or Workstation with Service Pack 3 or higher installed
- **Slim Client:** An Intel-based system at Windows NT 4.0 Server or Workstation with Service Pack 3 or higher installed

Hardware Requirements

The following table identifies the memory, and the central processing unit requirements for DCE for Windows NT on a Windows NT system.

Table 1. Memory and CPU Requirements for Server and Client Systems

	Requirements	
	Memory	CPU
SERVER	Minimum: 32MB Recommended: 64MB or higher	Minimum: Pentium 90 Recommended: Pentium 166 or higher
CLIENT (Runtime Services)	Minimum: 16MB Recommended: 32MB	Minimum: 486 Recommended: Pentium 90 or higher
Slim CLIENT (Runtime Services)	Minimum: 8MB Recommended: 16MB	Minimum: 486 Recommended: Pentium 90 or higher

The following table identifies the disk space requirement for each component.

Table 2. Disk Space Requirements for Each Component

Component	Disk Space Requirements
DCE Runtime Services (Client)	29.5MB
DCE Application Development Kit	6.7MB
DCE Security Server	4.1MB
DCE Cell Directory Server	0.9MB
Event Management System (EMS)	1.0MB
Simple Network Management Protocol (SNMP)	2.0MB
Service Files	20.2MB
Online Documentation	14.3MB
Slim Client	4.8MB

Notes:

1. Memory requirements for user applications and data are not included.
2. Server memory requirements vary with the size and usage of the Security Services registry and the CDS directory.
3. Disk space consists of installation requirements only. It does not include the following:
 - paging file
 - log files, security credential files, or other DCE data files
 - Server Security Services registry or CDS server directory

Prerequisite Software Requirements

DCE for Windows NT has the following prerequisite software requirements:

- Service Pack 3 installed on Windows NT 4.0 (see note)
- DCE Runtime Services for Windows NT installed before installing and using DCE ADK for Windows NT, DCE Cell Directory Server for Windows NT, and DCE Security Server for Windows NT
- A DCE cell with at least one DCE Cell Directory Server and at least one DCE Security Server for clients
- Suitable compilers and linkers must be installed on your system before you can use the DCE for Windows NT ADK. On Intel platforms, Microsoft Visual C++ Version 4.0 or higher provides a compatible environment

Note: Service Pack updates are automatically sent to Microsoft Developer Network (MSDN) Level 2 members. If you are not an MSDN Level 2 member, you can obtain the appropriate Service Pack by accessing the Microsoft FTP server directly from the Internet (**ftp ftp.microsoft.com**) or from a World-Wide web browser (**ftp://ftp.microsoft.com**).

If you cannot obtain the prerequisite Service Pack as described above, call Microsoft to order a CD or 3.5" diskette version.

Chapter 3. Installing DCE for Windows NT

The Runtime Services, the Application Development Kit, the Security Server, and the CDS server are packaged on one CD-ROM. To ensure your system meets all the hardware and software requirements, before you begin the installation process read “System Requirements” on page 19, “Hardware Requirements” on page 20, and “Prerequisite Software Requirements” on page 21. Specifically:

- Make sure the appropriate Microsoft Service Pack is installed. For Windows NT Version 4.0, Service Pack 3 is required.
- Make sure that **TCP/IP Protocol** is enabled.
- Make sure that **NetBIOS Services** is enabled. (This is required in order for DCE for Windows NT to obtain a system’s hardware address.)
- Make sure that any installed DCE is not running.

The installation setup program does the following:

- Expands the product files (which are shipped as compressed files) and copies them to the appropriate directories
- Provides the NT registry with necessary information about the DCE software.
- Creates required environment variables
- Creates the appropriate DCE folders on your system’s desktop

Installing

To install DCE for Windows NT, do the following:

1. Insert the CD-ROM in your CD-ROM drive. After a few moments, the **Choose Setup Language** window is displayed.
2. Select the language that you want for the installation.

Note: The language that you select for the installation will also be the language of the DCE icons on your desktop.

3. After reading the information in the **Welcome** window, click **Next** to continue.
4. In the **Question** dialog box for antivirus software, indicate **Yes** or **No**
5. In the **Select Component** window, click on the components you want to install.

Note: DCE Runtime Services must be selected and is a prerequisite for installing any other components.

6. The default installation directory is c:\program files\dce. To change to a different drive or a different directory, click on **Browse**. Click **Next** to continue.
7. In the **DCE Translations** dialog box, select the translation of DCE that you want to install. This selection determines the language for the DCE messages.

Note: English is always installed.

8. In the **Cultural Conventions** window, select a preferred cultural convention. Click **Next** to continue.
9. In the Start Copying Files window, review the installation information. If you want to change any settings, click **Back** to make the changes. Otherwise, click **Next** to start the process of copying files to your hard drive.
10. The Setup window appears showing the progress indicator. When the installation completes the IBM Software Registration Tool window appears. Click **Next** to complete the software registration.
11. After completing the software registration, a question appears asking whether you want to view the online readme file. Click **Yes** to view the readme; otherwise, click **No**.

Note: Viewing the online readme file is optional. Since it contains last minute product changes that are not documented elsewhere, we recommend you read it.

12. After you view the online readme file (or if you choose not to view it), the Installation Complete window appears. You are asked whether you want to restart your system. Make your choice and then click **Finish**.

Note: DCE for Windows NT modifies the system configuration. If you choose not to restart your system at this time, you must restart it later for the DCE changes to take effect.

Configuring DCE for Windows NT

After completing the installation procedure, you must configure DCE services on your system. To configure DCE services on Windows NT:

1. To configure DCE Services on Windows NT Version 4.0, click **Start**, point to **Program**, click **DCE for Windows NT**, and then click the **DCEsetup** icon.
2. Click the **Configure** menu, and then click on one of the configuration options.

Note: For more information on how to configure DCE for Windows NT, see “Appendix B. DCE Configuration” on page 37 or the DCESetup online help file.

Configuring a Slim Client for DCE for Windows NT

After completing the installation procedure, the Slim Client configuration panel is displayed.

Note: If you have already installed DCE for Windows NT and you want to configure a Slim Client, click on the **DCE Slim Client** icon to access the configuration panel.

To configure a Slim Client on Windows NT:

1. Enter the host name of the Security server in the **Security Server hostname:** field.
2. Enter the host name of the CDS server in the **Directory Server hostname:** field.
3. The **Cell name:** field can be left blank. The configuration tool will locate the cell for you.
4. Click the **Configure** button.

Unconfiguring a Slim Client for DCE for Windows NT

You must unconfigure the Slim Client from your system before you can uninstall it. To unconfigure a slim client on Windows NT:

1. Double click on the **DCE Slim Client** icon.
2. Click the **Unconfigure** button.

Unconfiguring DCE for Windows NT

Before uninstalling DCE, you must unconfigure the DCE services on your system. To unconfigure the DCE services on Windows NT:

1. Click **Start**, point to **Program**, click **DCE for Windows NT**, and then click the **DCEsetup** icon.
2. Click the **Configure** menu, and then click on the **Unconfigure** option.

Uninstalling Full DCE or a Slim Client from Windows NT

To uninstall DCE for Windows NT, do the following:

1. Double-click the My Computer icon.
2. Double-click the Control Panel icon.
3. Double-click the Add/Remove Programs icon.
4. Click on **DCE for Windows NT V2.2**, and then click **Add/Remove**.

Migrating to DCE for Windows NT, Version 2.2

Because DCE for Windows NT, Version 2.2 is dependent upon Windows NT Version 4.0 with Service Pack 3 or higher, this version must be installed on your machines to migrate from either the IBM DCE for Windows NT Version 1.1c or Version 2.0. You can do this migration without a reconfiguration of your existing DCE cell by using the following procedures. You are not required to migrate your machines in a specific order, but please pay close attention to the limitations on DCE Security Server functionality as described in Step 3 on page 27, **Migrating DCE Security Replicas**. Read this entire section before beginning the migration procedure.

1. Before Migrating:

- a. In DCE for Windows NT, each workstation in a DCE cell keeps configuration information about the DCE clients and servers running on the local machine. This information is stored locally in the **dced** server configuration database.

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

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

You can verify this by running the following command:

```
dcecp -c acl show /./hosts/dce_hostname/config/svrconf
```

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

The output of this command should resemble this:

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

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

If an entry does not exist for the self account:

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

If an entry does exist but is not complete:

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

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

```
%DCELOC%\dcelocal\var\dce
%DCELOC%\dcelocal\var\krb5
%DCELOC%\dcelocal\var\etc\dce
```

- c. All prerequisites are listed in “Chapter 2. Planning for DCE for Windows NT” on page 19. Select **Migrate** during the DCE for Windows NT, Version 2.2 installation.

2. Migrating DCE Clients:

- a. Stop DCE.
- b. Install DCE for Windows NT, Version 2.2. Choose the same components that you had installed for your previous level of DCE for Windows NT on this machine.
- c. Start DCE by running **dcecp start.dce** from a command line or through **DCESetup**. Starting DCE will invoke the migration process of all DCE configuration data to the DCE for Windows NT, Version 2.2 format.

3. Migrating DCE Security Replicas:

DCE Security Replica Servers can be migrated using the steps documented in Step 2, *Migrating DCE Clients*. We recommend that you migrate all Security Replicas in your cell prior to enabling DCE for Windows NT 2.2 function on your Master Security Server. When planning your migration, keep the following limitations in mind:

- a. If Security Replicas are migrated prior to the migration of the Master Security Server, they will run with only your previous level of DCE

function enabled. When the DCE for Windows NT 2.2 function is enabled on the security master using the **dcecp** command (given in Step 5.c under *Migrating the DCE Security Master*), these Security Replica Servers will also enable the DCE for Windows NT 2.2 function.

- b. If the DCE for Windows NT, Version 2.2 function is enabled on the Master Security Server prior to the migration of all Security Replicas, any replicas which are running a previous level of DCE will be shut down. These Security Replicas cannot support DCE for Windows NT, Version 2.2 function.

4. Migrating DCE CDS Servers:

- a. Ensure that all CDS Master directory replicas located on this machine are replicated on at least one other CDS server machine in the cell. If you wish to support updates to these CDS directories during the migration process, move these master directory replicas to another CDS server.
- b. Perform the tasks in Step 2 on page 27, *Migrating DCE Clients*.

5. Migrating the DCE Security Master:

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

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

- b. Perform the tasks documented in Step 2 on page 27, *Migrating DCE Clients*.

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

- c. Enable DCE for Windows NT, Version 2.2 function, by executing the following command:

```
dcecp -c registry modify -version secd.dce.1.2.2
                                or
dcecp -c registry modify -version secd.dce.1.2.2a
```

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

Note: IBM DCE for Windows NT, Version 2.2 supports two security versions greater than DCE for Windows NT, Version 2.0 or Version 1.1c. These security versions are **secd.dce.1.2.2** and **secd.dce.1.2.2a**. The **secd.dce.1.2.2** version supports all previous function and introduces OSF Version 1.2.2 function including RFC 68.3 Public Key Server support. The **secd.dce.1.2.2a** version supports all previous function including **secd.dce.1.2.2** function, and introduces IBM's Public Key Certificate Login (PKC) support, based on OSF RFC 68.4. This version is also supported in IBM DCE for AIX, Version 2.2 with the appropriate PTF set.

d.

After you have migrated the Master Security Server, you need to validate any intercell accounts that exist in the DCE registry. Vendor implementations of DCE at the OSF 1.2.2 level generally implement a new restriction for accessing foreign cells. For a DCE client to access a foreign cell, the intercell surrogate account for the foreign cell in the local registry must have its **acctvalid** flag set to **yes**. Otherwise, access to the foreign cell will be denied.

Although DCE for Windows NT, Version 2.2 is at the OSF 1.2.2 level, it does not enforce this restriction. However, other vendor's implementations of OSF DCE 1.2.2 may enforce it. To allow intercell access, the cell administrator can use the following **dcecp** command to change the **acctvalid** flag to **yes** for an existing intercell surrogate account:

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

Where *cell_name* is the name of the foreign cell.

6. Migrating DTS Servers

To correctly migrate DTS servers, follow the tasks described in 2 on page 27, *Migrating DCE Clients*. Note that any time providers in use on the system will not be recognized by the migration tool. To continue using a time provider, it may be necessary to manually reconfigure it after the migration is completed.

Chapter 4. Obtaining Additional Information

This chapter describes the sources for information that can be useful when you are using DCE for Windows NT.

Books

The DCE for Windows NT library contains a hardcopy and an online version of this book. All other supporting product documentation is provided only in online format and on the CD.

Online Information

Extensive online documentation is shipped as part of the DCE for Windows NT product. Both online OSF DCE books and the DCE for Windows NT product documentation are provided as Windows Help files.

Online Documents

Extensive online documentation is part of the DCE for Windows NT product set. The following DCE books are available online:

- *Introduction to OSF DCE*
- *OSF DCE Command Reference*
- *OSF DCE Administration Guide - Introduction*
- *OSF DCE Administration Guide - Core Components*
- *OSF DCE Application Development Guide - Introduction and Style Guide*
- *OSF DCE Application Development Guide - Core Components*
- *OSF DCE Application Development Guide - Directory Services*
- *OSF DCE Application Development Guide - Reference*
- *DCE Problem Determination Guide*
- *Guide to DECthreads*
- *DCE Enhancements*
- *Troubleshooting*

Online Help Files

As part of Runtime Services, this product provides the following value-added files in Windows Help file format.

- *Using DCEsetup*

- *Using Visual ACL Editor*
- *Using DCE Director*

Viewing HTML Books

This book and the *DCE Problem Determination Guide* are also supplied in Hypertext Markup Language (HTML) softcopy format. Softcopy format enables you to search or browse the information more easily, using hypertext links for related information. It also makes it easier to share the library across your site.

To view the HTML book, you can use any browser that supports some version of Windows NT.

Appendix A. Overview of Example Programs

The DCE for Windows NT Application Development Kit (ADK) provides a full range of example programs, including those designed specifically for a Windows NT environment. Also included are programs written in C++ that illustrate use of distributed objects.

Several example programs are supplied with the DCE for Windows NT ADK. These programs are located in directories under `%DCELOC%\dcelocal\examples`. In addition to the information provided here, each example program includes an online README file located in the same directory as the program. The following table shows the different features for each example program.

Table 3. Example Programs

Example Program	Description
RPC Test Program #1	Makes minimal use of DCE services. Server does not register endpoints; binding information not exported to namespace.
RPC Test Program #2	Makes minimal use of DCE services. Server registers endpoints; binding information exported to namespace; uses security.
RPC Test Program #3	Makes minimal use of DCE services. Server registers endpoints; binding information not exported to namespace.
Book Program	Contains a distributed calendar program. Server registers endpoints; binding information is exported to namespace; uses mutex locks and security.
Bank Program	Simulates an automated teller machine. Uses all DCE services, including security.
Timop Program	Calculates the span of time it takes a server to perform an operation. Uses all DCE services, including security and threads.
PC Phone book Program	Looks up employee contact information that resides with the <code>phnbk</code> server. Uses Microsoft RPC and the name service.
Mandelbrot Set Program	Uses multiple DCE RPC servers per client and the name service.

Table 3. Example Programs (continued)

acl_server Program	Shows how a basic ACL manager can be written for an application server.
DTSS Program	Contains time provider services that work in conjunction with a DTSS service to provide an accurate time source.
GSSAPI Program	Shows how a distributed application can make itself secure by using the GSSAPI.
Stock Quote Program	Uses two DCE RPC servers distributing data to multiple clients and the name service.
Tic-Tac-Toe Program	Uses two DCE RPC clients interoperating through a server and the name service.
Virtual Whiteboard Program	Uses multiple DCE RPC clients exchanging large amounts of data in real-time through a server and the name service.
Account Program	Tests inheritance, binding to an object using another interface, binding to an object with an unsupported interface, and the reflexive, symmetric, and transitive relation properties of the bind() API.
Accountc Program	Tests the same properties as the account program, but uses the C interfaces for all the APIs.
Card Program	Tests the passing of C++ objects as parameters using the [cxx_delegate] attribute and the polymorphism property of the base class.
Stack Program	Tests the passing of C++ objects as parameters using the [cxx_delegate] attribute and a user-defined Stack class.
Serviceability Programs	Show how to use DCE, messaging, and serviceability APIs.
EMS Consumer and Supplier Programs	Shows how basic consumer and supplier programs can be written to work in conjunction with EMS for simple event transmission.

You should copy the example program files to a private area before you attempt to build them.

To build the example programs, do the following:

1. Use the File Manager or a command such as **xcopy** to copy the files in `%dceloc%\dcelocal\examples\program_directory*` to your own directory. For example, type:
C:\> **cd \mydir**
C:\MYDIR> **xcopy /s %DCELOC%\dcelocal\examples\rpc\test1**
2. Build the test program using the provided makefile. For example, type:
C:\MYDIR> **nmake -f test1.mak**

Appendix B. DCE Configuration

DCEsetup allows you to configure your system as a full DCE client or as a DCE server. You can create a configuration that joins an existing cell or you can create a new cell.

This appendix provides additional information for the following topics:

- “DCE Cells”
- “Configuring Your System as a DCE Client” on page 39
- “Configuring Your System a DCE Server” on page 41
- “Enabling or Disabling Integrated Login” on page 44
- “Automatically Starting DCE at Boot Time” on page 45
- “Unconfiguring” on page 45
- “Clobbering” on page 47
- “Viewing Log Files” on page 47

Configuring DCE for Windows NT

Using DCEsetup

After completing the installation procedure, you must configure DCE services on your system. To configure DCE services on Windows NT, click **Start**, point to **Program**, click **DCE for Windows NT**, and then click the **DCEsetup** icon.

To exit DCEsetup, pull down the File menu and choose Exit. There is no need to explicitly save any data before exiting. Your configuration is saved automatically.

For more information on how to configure DCE for Windows NT, see the DCEsetup online help file.

DCE Cells

DCEsetup lets you configure your system as a DCE client or a DCE server. You can create a configuration that will join an existing cell or you can create a new cell.

For configuration purposes, a cell must contain one Master CDS server and one Master Security server. You can choose to install both the CDS server and

the Security server on one system in the cell or you can split the two servers and put them on different systems in the cell.

When you use the Distributed Time Service (DTS), it is recommended that you configure a minimum of three local time servers in the cell. If the cell is a Windows NT only cell, you should also run on the null time providers or the NTP time provider. For more information on time providers, see the DCE Enhancements help file.

If there are no other systems in your network already providing DCE services, you must create a new DCE cell to use the DCE services on your system.

If there are other systems in your network already providing or using DCE services and you are configuring your system as a DCE client, there may be an existing cell that your system can join.

Creating a DCE Cell

A cell must exist before you can use DCE services. If you are not joining an existing DCE cell, you must use DCEsetup to create a new DCE cell with a CDS server and a Security server.

You need to define a name for your new DCE cell that is unique in your global network and is the same on all systems that participate in this cell.

Defining a Hostname

All DCE configurations require you to provide a name for your system that is unique within your DCE cell. In most cases, you should use the default hostname. The default hostname is the fully qualified Internet hostname.

To perform DCE configurations, you might be required to provide DCEsetup with a principal name and password.

For most client system configurations, the principal name you provide must have privileges to perform cell administration operations. The exception is local client configurations (see "Configuring a Local Client" on page 40), which do not require cell administration privileges.

For server system configurations, the principal name you provide will be created in the Security registry with the necessary cell administration privileges.

Joining an Existing DCE Cell

Once a CDS server and a Security server have been configured to create a cell, you can configure other systems that join the cell.

You need the following information to configure your Windows NT system to join an existing DCE cell:

- Local hostname
- Cell name
- Security principal name and password authorized to perform cell administration operations. (Not needed if you are performing a local client configuration)
- Additionally, if a CDS server for your cell is not within broadcast range or if you are performing a WAN configuration, you will need:
 - The hostname or IP address of the Master Security server
 - The hostname or IP address of a CDS server.

Note: For any hostname that is not currently defined in the TCP/IP hosts database, you must provide the IP address instead of the IP hostname.

Configuring Your System as a DCE Client

DCEsetup allows you to choose between two types of client configurations:

- Local DCE client configuration, which uses configuration information previously supplied and stored by a user with cell administrator privileges.
- Full DCE client configuration, which requires you to supply additional information. This option requires cell administrator privileges.

Both options automatically configure your system as a CDS client and a Security client.

Configuration Wizards make it easy to perform client configurations. If you click the Cancel button at any time during configuration, the configuration will be aborted and the existing configuration will remain in effect. A new configuration will take effect only when you run through all screens of the wizard and click Finish on the last screen. Once you click Finish, DCEsetup performs the appropriate Unconfigure operation and then configures the system according to the options you selected.

Configuring Your System as a Security and CDS Client

All DCE configuration options, both client and server, enable the DCE Security client runtime services and the CDS client directory services.

You must provide the following information to configure the Security client services:

- Cell administrator principal name
- Password for the cell administrator principal
- Hostname or IP address where the Security server resides (if the CDS server is not within broadcast range)

To complete configuration of the CDS client services, you must provide the following information:

- Hostname or IP address where the CDS server resides. (If the CDS master server is not within broadcast range.)

In addition, if the cell uses multiple LANs, you must provide the following:

- LAN Profile name for your LAN.

Configuring a Local Client

The local client configuration option uses existing configuration information stored in the CDS namespace and Security registry to configure a client system. Because much of the required information is already available, this type of configuration is straightforward and requires minimal additional information. Moreover, this option does not require access to the cell administrator account.

Before a local client configuration can occur, a user with cell administrator privileges must create and store required information using the Remote Client option on the Administration menu.

To perform a local client configuration, pull down the Configuration menu and choose Create>Local Client...

Configuring a Full Client

The full client configuration option allows you to configure your system as a DCE client. Unless you change the default settings, this configuration also enables your system as a DTS client (clerk) and turns on the Integrated Login, Automatic Startup, and Automatic Time Sync features.

Once the full client configuration is complete, DCEsetup remembers the options you have selected and the information you entered. If you later choose to modify this configuration, DCEsetup will provide the current settings as defaults that you can either accept or change.

Full client configuration requires knowledge of the cell administrator password.

To perform a full client configuration, pull down the Configuration menu and choose Create>Full Client...

Configuring Your System a DCE Server

DCEsetup allows you to define a new cell configuration on your Windows NT system. This option automatically enables the runtime Security and CDS client services and allows you to easily choose from the following DCE services, if installed:

- Security server
- CDS server
- Distributed Time Service (DTS)
- Global Directory Agent (GDA)
- Password Strength Server
- Identification Mapping Server (IDMS)
- Auditing
- NSI Gateway

If you are not configuring your system as the Master Security server in the cell, you must provide the following:

- Hostname or IP address of the Master Security server.

If you are not configuring your system as the Master CDS server in the cell and the Master CDS server is not reachable on the LAN, you must provide the following:

- Hostname where the Master CDS server resides

In addition, if the cell uses multiple LANs, you must provide the following:

- LAN profile name for your host.

You can also choose to enable additional options such as Integrated Login and Automatic Startup.

To perform a server configuration, pull down the Configuration menu and choose Create>Server...

Once the initial configuration is complete, DCEsetup remembers the options you have selected and the information you entered. For subsequent configurations, DCEsetup will provide relevant remembered information as defaults that you can either accept or change.

A Configuration Wizard makes it easy to perform a server configuration. If at any time during configuration, you click the Cancel button, the configuration will be aborted and the existing configuration will remain in effect. A new

configuration will take effect only when you run through all screens of the wizard and click Finish on the last screen. Once you click Finish, DCEsetup performs an Unconfigure operation and then configures the system according to the options you selected.

Configuring Your System as the Master Security Server

When you create a new cell, you need to configure a Master Security server and supply the following information:

- Cell administrator principal name
- Password for the cell administrator principal
- Confirmation of the password

If you are configuring a Master Security server on this system and a Master CDS server on another system, you are performing a split server installation.

Configuring Your System as a Replica Security Server

To configure a replica Security server, supply the following information:

- Security replica name, which must be unique for the cell
- Cell administrator principal name
- Password for the cell administrator principal

To successfully configure a replica Security server, a Master Security server must already be configured in the cell.

Configuring Your System as Master CDS Server

Every CDS server has a database called a clearinghouse in which it stores directory replicas. Directories are the units by which you distribute and replicate names throughout the namespace. You can have only one writable replica, called the master replica, in the cell. Other replicas of the cell are read-only.

If you are configuring a CDS server as a Master CDS server, you must supply the following information:

- LAN profile name for your host, if the cell uses multiple LANs

If you are installing a CDS server as part of creating a new cell using CDS, the first CDS server in a cell is the Master CDS server. All other CDS servers in the cell will be replica servers.

Configuring Your System as a Replica CDS Server

To configure a replica CDS server, supply the following information:

- Replica clearinghouse name, which must be unique for the cell
- LAN profile name, if your cell uses multiple LANs

If you are installing a CDS server as part of creating a new cell using CDS, the first CDS server in a cell is the master server. All other CDS servers in the cell will be replica servers.

Configuring a Split Server

A configuration that has the Master Security server and the Master CDS server on different systems is known as a split server configuration.

When configuring a split server cell, you must always begin the configuration process on the host where the Master Security registry will reside. Once that system is partially configured, the configuration process pauses, instructing you to begin the configuration of the host where the Master CDS server will reside. When this configuration is complete, DCEsetup instructs you to complete the configuration process on the Security server system.

Notes:

1. If you need to delete a split server configuration using Unconfigure, you must first unconfigure the CDS server and then the Security server on the respective systems. You cannot unconfigure the CDS side of a split server and then reconfigure into the same cell, without first unconfiguring the Security side.
2. If you want to delete a split server configuration using Clobber, you must clobber the CDS server first, then clobber the Security server.

To configure a split server::

1. Run DCEsetup on the system you want to configure as a Security server. If this is your Windows NT system:
 - Pull down the Configuration menu and choose Server...
 - Enter the name for the new cell. (The DCE hostname should be provided for you.)
 - Choose Master Security server and any other desired DCE components. Supply the hostname of the Master CDS server and any other required information. When you are done, click Finish. A dialog box appears, asking you to move to the system where the CDS server is to reside.
2. Run DCEsetup on the system you want to configure as a Master CDS server. If this is your Windows NT system:
 - Pull down the Configuration menu and choose Server...

- Enter the cell name for this system. (The DCE hostname should be provided for you.) The cell name must be the same as that of the first system.
 - Choose Master CDS server and any other desired DCE components, then click Finish.
 - Pull down the Administration menu and choose Test.
3. Return to the first system and click OK to dismiss the dialog box. Pull down the Administration menu and choose Test.

Note: To delete a split server configuration using Unconfigure, first run the DCEsetup procedure on the system that is running the CDS server and select the "Unconfigure" option. Then run DCEsetup on the system that is running the Security server and select the "Unconfigure" option.

Configuring Your System to Use the Distributed Time Service (DTS)

The Distributed Time Service (DTS) synchronizes the different time clocks of the systems within a cell.

Choose this option if you want to accept time from DCE DTS time servers. Click the appropriate DTS button in the Configuration dialog box to configure your system as a DTS clerk, a DTS local server, or a DTS global server.

By default, the courier role is set to backup courier.

Enabling or Disabling Integrated Login

DCE for Windows NT provides an integrated login feature. When enabled (which is the default setting), this feature attempts a dce_login whenever a user logs in to Windows NT.

The integrated login feature uses the Windows NT user name and password for the dce_login. This requires that the user's Windows NT user name and password remain synchronized with the DCE registry in the cell.

This feature automatically attempts to change the DCE principal's password whenever the Windows NT user changes his or her password with the Change Password... button in the Windows NT Login and Security dialog boxes.

To enable or disable integrated login during configuration (or later, through the Configuration>Modify... option), enable or disable **Integrated Login**.

Automatically Starting DCE at Boot Time

DCE for Windows NT provides an Auto Start option that automatically starts DCE services during Windows NT startup. When enabled (which is the default setting), this feature adds the DCE Auto Start Service to the list of services that will be started automatically as part of the Windows NT startup procedure.

If you choose this option, you do not have to remember to restart DCE services whenever your system is rebooted.

You can specify that a DCE Clean operation should be done before auto-starting DCE by checking the **Clean before automatically starting** checkbox in DCEsetup or by entering `—autostart_clean yes` on the `config.dce` command line. The Clean operation removes any temporary files, including credentials that may have expired while the system was down.

To enable or disable DCE automatic startup through DCEsetup

During configuration (or later, through the Configuration>Modify... option), set the checkbox to either enable or disable **Automatically start DCE services during system startup**.

If you choose not to configure for Auto Start at this time, the DCE Auto Start Service is set to manual mode in the Control Panel. Later, if you decide to reconfigure for Auto Start, you can do so with the Configuration>Modify... option. You can also do it through the Control Panel.

To enable DCE automatic startup through the Control Panel

1. In the Control Panel, select Services.
2. Double-click the Auto Start Service. On the popup dialog box that appears, click Automatic.

Unconfiguring

The Unconfigure option stops all active DCE daemons and deletes all temporary and permanent local databases associated with the DCE daemons on your system.

For a client configuration, Unconfigure removes all references to the client from the cell database. This includes objects in the CDS namespace and all security account information in the Security registry. It will also delete local configuration files. In short, Unconfigure does additional cleanup work at the cell.

For both client and server configurations, use the Unconfigure option to delete the configuration. If the Unconfigure operation fails for any reason, use the Clobber option.

During an Unconfigure operation, the actions that occur in order to delete the permanent configuration data are logged in the %DCELOC%\dcelocal\etc\cfgdce.log file.

If, after executing this command, you want to use DCE daemons, you must reconfigure the system.

Note: If you need to delete a split server configuration using Unconfigure, you must first unconfigure the CDS server and then the Security server on the respective systems. You cannot unconfigure the CDS side of a split server and then reconfigure into the same cell, without first unconfiguring the Security server side.

To delete your configuration from the host and the cell using Unconfigure

1. Pull down the Configuration menu and choose Unconfigure.... A dialog box appears, asking you to confirm this action. You must also enter a principal name with cell administrator privileges and associated password.
2. Click Yes to unconfigure the system, deleting the configuration from both the host and cell.

Notes:

1. To delete a split server configuration using Unconfigure, first run the DCEsetup procedure on the system that is running the CDS server and select the "Unconfigure" option. Then run DCEsetup on the system that is running the Security server and select the "Unconfigure" option.
2. Use the Modify option on the Configuration menu to change your configuration. Changes such as adding or deleting components do not require you to unconfigure your entire configuration.

Unconfigure Local All

This option, available from the Administration menu, allows you to delete a local configuration created with the Create>Local Client... or the Create>Full Client... options on the Configuration menu. Use this option to remove local information at the host system.

If you want to reconfigure a local client into the same cell after using this option, you must also use the Remote Client>Delete... option to delete the remote client portion of the configuration.

To delete a configuration created with Create Local Client:

1. Pull down the Administration menu and choose Unconfig Local All.... A dialog box appears asking you to confirm this action.
2. Click Yes to delete the configuration.

Clobbering

The Clobber option stops all active DCE daemons and deletes all temporary and permanent local databases associated with the DCE daemons on your system, including the DCE system configuration files.

The Clobber operation attempts to perform a full Unconfigure operation, removing remnants of the host from both CDS and the Security registry. It also performs a dcecp scrape.dce operation to remove entries in the endpoint map.

To delete your configuration from the host using Clobber

1. Pull down the Administration menu and choose Clobber.... A dialog box appears, asking you to confirm this action.
2. Click Yes to delete the configuration.

Note: To delete a split server configuration using Clobber, first run the DCEsetup procedure on the system that is running the CDS server and select the "Clobber" option. Then run DCEsetup on the system that is running the Security server and select the "Clobber" option.

Viewing Log Files

DCEsetup provides a scrollable window for viewing a log of the events that have occurred during a configuration session. These events are logged in a file every time you run DCEsetup. The log file window appears to the left of the status window.

The file location for the current log file is:

```
%DCELOC%\dcelocal\etc\dcesetup.log
```

The DCELOC environment variable points to the root where DCE was installed.

Events are logged only for the session in which you are using DCEsetup. When you exit DCEsetup, the log file is closed. The next time you run DCEsetup, the file is reopened and logging resumes. DCEsetup appends information to the existing log file. Once the file reaches a size of approximately 62K, the file is renamed dcesetup.bak, and a new dcesetup.log is started.

A second log file, called `cfgdce.log`, contains an additional level of detail on configuration events, including the particular `dcecp` commands executed and their status values. This file is particularly useful for helping determine the cause of configuration failures. The location for this file is:

```
%DCELOC%\dce\local\etc\cfgdce.log
```

This information is also available in the DCEsetup online help file.

Appendix C. Slim Client Limitations

The following commands are supported:

acl_edit	dce_login	kinit
cadump	getcellname	kdestroy
catraverse	getipaddr	rgy_edit
cdscp	klist	rpccp
dcecp		

Note: The same restrictions that apply to a full DCE client apply to a Slim Client.

The following functions are not supported:

define a cached server	show a cached clearinghouse	clear a cached server
show a cached server	show a clerk	disable a server
show a server	clear a clearinghouse	disable a clerk
create a clearinghouse	delete a clerainghouse	

The online help file, *DCE Enhancements*, contains a full description of the Slim Client.

Appendix D. Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make them available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Subject to IBM's valid intellectual property or other legally protectable rights, any functionally equivalent product, program, or service may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

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

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
USA

Asia-Pacific users can inquire, in writing, to the IBM Director of Intellectual Property and Licensing, IBM World Trade Asia Corporation, 2-31 Roppongi 3-chome, Minato-ku, Tokyo 106, Japan.

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

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
USA

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

Trademarks

The following are trademarks of International Business Machines Corporation in the United States, or other countries or both:

AIX
IBM

OS/2
VisualAge

Digital is a trademark of Compaq Corporation.

Microsoft, Windows, Windows NT and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

Entrust is a registered trademark of Entrust Technologies Limited.

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

Index

A

Auto-start 10

B

books 31

C

CDMF 13

CDS cache restructuring 12

CDS preferencing 7

client

slim 7

Commercial Data Masking Facility 13

compatibility with other DCE systems 5

compiler

Microsoft visual C++ v5.0 9

configuration

DCE 24

slim client 25

timeout values 8

configuration, unattended 10

configuration protocol

dynamic host 8

Credential cache cleanup 12

D

DCE

features 2

more about 2

DCE Control Program 14

DCE director 9

DCE for Windows NT

benefits 2

compatibility with other DCE systems 5

interoperability with other DCE systems 5

planning 19

product content 3

supported transport protocols 5

DCEsetup 9

DFS APIs unsupported 16

DHCP 8

disk space requirements 20

Distributed Time Service 12

Dynamic Host Configuration

Protocol (DHCP) 8

E

EMS 14

enhancements to OSF DCE Release

1.2.1

additional sample programs 15

Auto-start 10

CDS Cache Restructuring 12

Commercial Data Masking

Facility 13

Credential Cache Cleanup 12

DCE control program extensions

14

DCE deinstallation procedure 15

DCE Director 9

DCEsetup 9

enhanced online information 16

Event Management Service 14

IDL compiler enhancements 15

Inline CDS Clerk 12

Integrated Login 11

modifications to

Internationalization 13

MVS DCE Load Balancing client

support 14

Name Service Interface Daemon

11

Remote DCE Client

Configuration 11

RPC event logger utility 15

Simple Network Management

Protocol 13

Visual DCE ACL Editor 10

VisualAge C++ 10

Event Management Service 14

F

functions

IBM 5

OSF 1.2.2 5

Windows NT v2.0 6

H

help files, online 31

I

IDL compiler enhancements 15

Inline CDS clerk 12

installing 23

Integrated login 11

interface cards

network

multiple 8

internationalization, modifications to

13

interoperability

kerberos v5 7

interoperability with other DCE

systems 5

introduction 1

K

Kerberos v5 interoperability 7

L

license requirements 19

M

Microsoft visual C++

v5.0 compiler 9

migrating

before 26

permissions 26

multiple network interface cards

(NICs) 8

MVS DCE Load Balancing client

support 14

N

name service interface daemon 11

O

online information

DCE for Windows NT 31

help files 31

OSF 31

online information, enhanced 16

OSF online information 31

P

planning 19

preferencing

CDS 7

prerequisite software 21

product contents 3

R

Remote DCE client configuration 11

requirements

disk space 20

license 19

- requirements (*continued*)
 - software 21
 - system 19
- RPC Event Logger utility 15

S

- sample programs, additional 15
- silent install 10
- Simple Network Management
 - Protocol 13
- slim client 7
 - configuring 25
 - unconfiguring 25
- SNMP 13
- software, prerequisite 21
- system requirements 19

T

- timeout values
 - tunable
 - Configuration 8
 - rpc 8
- transport protocols, supported 5

U

- unattended configuration 10
- unconfiguration
 - DCE 25
 - slim client 25
- uninstall procedure 15
- unsupported OSF features
 - commands
 - dtss-graph 16
 - sec_salvage_db 16
 - Security 16
 - user commands 16
- unsupported subroutines (DFS APIs)
 - 16

V

- Visual DCE ACL editor 10
- VisualAge C++ 10



Part Number: CT75LNA



Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SCT7-5LNA-00



CT75LNA

