Open Software Foundation
Request For Comments: 96.0
April 1996

H. Hashimoto (Hitachi)
T. Ito (Hitachi)
T. Yamaura (Hitachi)

DFA: DISTRIBUTED FILE ACCESS MANAGER — FUNCTIONAL SPECIFICATION

1. INTRODUCTION

1.1. Purpose

Mainframes have been widely considered the most important form of company-wide information processing system for several decades, especially for critical applications. However, due to rapid progress in the areas of hardware and network technology, workstation-based distributed systems have emerged as another means of handling such core operations. OSF DCE, a de facto standard among distributed systems, is one of the most promising environments to offer a distributed system consisting of heterogeneous hardware and operating systems. DCE DFS (Distributed File System), one of the DCE services, allows physically distributed files to be seen and accessed as a single logically-centralized file system.

On the other hand, PCs are often used at department level in companies, and PC network systems, enabling file- and printer-sharing, predominate. Novell's NetWare, with well over 60% of market share, dominates this field.

As a result of this typical division of information resources, a great need has arisen for some way of making sharable the files used by the two kinds of system and allowing inter-department and intra-company file sharing. The Distributed File-Access Manager (hereafter abbreviated as ''DFA'') is designed to meet this need.

DFA provides a gateway function to access DFS files from a NetWare client, using the same operations as in NetWare. This gateway function allows inter-department data sharing via DFS, and access to workstation DCE-based DFS files from PC clients.

1.2. Features

DFA has the following features:

(a) DFS can be accessed with NetWare commands.

DFA offers almost all of the fundamental file operations (such as assigning a DFS sub-directory to a DOS virtual drive, and file copying) using the identical equivalent NetWare commands. In addition, DFA allows users to automatically log into DCE/DFS with NetWare login operations. Users accessing DFS get the same ''look and feel'' as with NetWare. (DFA does not, however, support access in the opposite direction, i.e., from a DFS client to NetWare files.)

(b) DOS/Windows application programs can access DFS.

Since DFA accesses DFS files using the NetWare client API, end users can access DFS files in the same manner as they would use to access NetWare files from DOS/Windows application programs.

(c) Arbitrary portions of DFS can be accessed.

DFA can define any portion of the DFS directory as a single NetWare volume, and this can be redefined as many times as desired. Even if the target DFS is large and complex, a user can easily designate the target file.

(d) Robust security.

DFA has robust security: its authentication mechanism will not allow raw passwords to leak into network communications. DFA employs an encryption key-based security. Access rights to DFS files are checked and compared with users' authentication information. Since DFA accesses DFS files using the access rights established for a user at DCE login, users get the advantage of robust file security via DFS's authorization checking.

(e) High reliability.

DFA is a highly reliable system with an error auditing process for periodic sanity checking, and it provides multiple means of recovery from system failures.

(f) Ease of installation and scalability.

DFA can be easily installed on an existing system without modification to DCE/DFS, the current NetWare file configuration, or the user's environment. DFA is highly scalable and flexible: as a system grows, you simply add additional DFAs to balance the load. (In order to be applied to large scale systems, additional instances of DFA must be multiplied for load balancing.)

1.3. System Configuration

The DFA system consists of PCs and workstations on which the NetWare client, NetWare server, DFS client, and DFSserver are running. DFA's basic components are: a DFA gateway on a NetWare server, an Administration Utility, a DFA agent on a DFS client, and client utilities on a NetWare client.

The DFA gateway is the component which provides most of the gateway functions. Its primary purpose is to convert NetWare API calls into the equivalent DFS API calls. These calls are then directed by the DFS agent to a DFS cache manager; the agent later returns the results of the calls to the DFA gateway. The client utilities are a group of utility commands to concurrently log into DCE/DFS and NetWare. The Administration Utility is a group of utilities which (among other things) performs the initialization of a DFA environment.

1.4. Functional Overview

1.4.1. DFS volume assignment

DFA assigns an arbitrary portion of the DFS directory (hereafter called ''DFS sub-directory'') to a DFS volume created as a NetWare volume on NetWare (hereafter called ''DFA Volume''). The DFS sub-directories can be mapped to multiple DFA volumes, and DFS sub-directories of different DCE cells can be assigned to multiple DFA volumes on a single NetWare server. Actually, the DFA utility assigns and deletes the DFS sub-directories, and keeps track of the assignment/deletion history on the DFA volume table. Prior to the assignment, DFS must have the sub-directory (mount point) assigned.

Using NetWare's MAP command, any portion of the DFS sub-directory assigned to the DFA volume can be assigned to a drive in a NetWare client, and then accessed via redirection (see section 1.4.2 for details), using the same API as for NetWare files.

1.4.2. Redirection

After the DFA volume assignment, accesses to the DFA volume are redirected to the assigned DFS sub-directory. The mechanism of redirection is that, on a NetWare server, NetWare file access API calls are hooked and converted into the equivalent DFS access. The conversions are as follows:

(a) Conversion of file/directory names.

DFS file and directory names comply with UNIX naming conventions, which allow much longer names than does DOS. DFA converts DFS file and directory names into DOS form in such a way as to prevent the converted names' matching any already-existing DOS file or directory names.

(b) Conversion of trustees/attributes.

ACLs (Access Control Lists) control access rights to DFS. DFA converts ACLs to NetWare trustees, and sets default values for the NetWare file attributes (DFS does not have ''file attributes'').

(c) Conversion of file locking protocols.

DFA mutually converts the locking protocols of NetWare and DFS. DFA does not, however, support record-level (or lower-level) locking.

1.4.3. Automatic DCE login

The DFA login utility allows automatic and simultaneous login to DCE/DFS whenever a user logs into NetWare. Even though NetWare and DCE/DFS do not have the equivalent user ID and password, a user can simultaneously login to both NetWare and DCE/DFS with a single operation, provided that mapping of user IDs and passwords is enabled.

1.4.4. Multiple DFA agent support

If there are multiple DFA agents, the DFA gateway automatically selects a DFA agent to which to connect. This provides both for resource redundancy in case of system failure, and load balancing.

1.4.5. System error monitoring and recovery

(a) File access error.

Whenever a file access error occurs, DFA retries the access. If the error occurs a second time, DFA terminates the job. To ensure that files in such cases are not left opened and unusable, the file is closed and the connection terminated.

(b) Error auditing.

Both the DFA gateway and the agent audit errors. Whenever an error is detected, DFA issues a report, and initiates error recovery procedures.

(c) DFA agent switching.

As mentioned above in section 1.4.4, to provide seamless operation, DFA will automatically switch from a malfunctioning to a correctly-operating agent.

2. GENERAL CONCEPTS OF DFA

DFA's primary purpose is to allow a PC user to easily take advantage of DCE DFS file access via his or her NetWare environment, and thus transform a mainframe-centered into a company-wide distributed system. In order for users to be able to handle DFS files in the same manner as NetWare files, DFA supports various file sharing and mapping functions.

DFA is highly expandable. NetWare can access DFS files only if a NetWare server and DFS client are equipped with DFA modules, and are connected with TCP/IP. Since DCE authenticates NetWare users with DCE's Kerberos, a NetWare user can access DFS files without diminishing the robustness of DCE security.

Possessing only a NetWare user ID, a user can simultaneously log into NetWare and DCE with a single simple operation. Users are automatically able to access files in both systems, NetWare and DFS, using the same commands and the same programs.

DFA also provides utilities for system error auditing, error analysis, error recovery, and system administration.

2.1. File Sharing and Mapping

2.1.1. Assignment of DFS file to netware volume

DFA enables a PC user connected to a NetWare server to handle the DFS file system (hereafter called DFS) as if those files resided in NetWare. Users can access DFS files with the same operations as they would PC files. Since users on different NetWare servers can share and access the same DFS files, NetWare can be expanded into a company-wide file sharing system.

A DFA administrator can pick as a mount point any arbitrary directory under the DFS junction (`fs`), and assign all the files and directories under the specified mount point (collectively called ‘‘DFS sub-directory’’) to a NetWare volume (see section 2.6 for details; prior to making this assignment, the DFS administrator needs to create the DFS sub-directories). The NetWare volume to which the DFS sub-directory is assigned, is called a ‘‘DFA volume’’. DFA reproduces on the DFA volume the DFS sub-directory's directory structure, using dummy (i.e., zero-length) files to represent on the DFA volume the original DFS sub-directory files. Users access the DFS files by using the DFA volume and file name (i.e., a directory path name).

A DFS sub-directory whose DCE cell is different from the one connected to DFA can also be assigned to a DFA volume. Moreover, DFA administrators for different NetWare servers can independently assign the same DFS sub-directory.

2.1.2. Volume redirection

By designating a DFA volume name, users can access DFS files in the same way as they would a NetWare server volume. If a directory (of the user's choice) in the DFA volume is mapped to the client's virtual disk drive using NetWare MAP commands, the user can create, delete, and rename the files and directories in the DFA volume as well as read and write the files.

When a DFA agent redirects access to a DFS file, DFA preserves compatibility between DOS and DFS file access by doing the following:

(a) NetWare file API calls are translated into DFS file API calls.

(b) NetWare names are converted into DFS file names.

(c) NetWare trustees are converted into DFS file access rights.

(d) DFS file locking is performed.

(e) DFS files are cached on a NetWare server.

2.1.3. API conversion

Conversion of NetWare file API calls into DFS API calls allows users to manipulate DFS files and directories in the same manner as they would NetWare files and directories.

DFA hooks (via a machine's operating system) into the NetWare file I/O operations. Whenever a requested operation is on a DFS file or directory, DFA converts the operation request into the equivalent DFS file access call, and sends the converted DFS call to the DFA gateway, which in turn sends it on to DFS.

When the operation completes, the DFA agent sends back to the DFA gateway the operation's (DFS file access) return code, having first converted the code into its NetWare equivalent.

Note that the API conversion process does not include automatic conversion of text, such as DOS and UNIX linefeed codes.

2.1.4. File name conversion

Basically, a DFA user creates a DOS file on a DFA volume. A NetWare user can access all files in the assigned DFS sub-directory, whether they were created after the assignment or were already present when the assignment to a DFA volume was made. If a given DFS file name does not comply with DOS's file naming rules (i.e., 8 or fewer characters followed optionally by a dot and 3 extension characters), DFA converts the DFS file name into a DOS-like name. It does this using a set of rules which conform to the X/Open PC Internetworking PC-NFS Specification, appending keys so that the converted names remain distinct.

Re-conversion from the converted DOS file name back to the original DFS file name proceeds by: (1) selecting the DFS file names likeliest to have been the original; (2) converting these into DOS names and comparing the conversions with the DOS file name to be reconverted; and (3) matching one of these with the candidate for reconversion

2.1.5. File access mapping between netware and DFS

Using only the rights acquired by logging into NetWare, a user can access DFS files without having to login to DCE. DFA maintains a table which maps user names registered to NetWare to those registered to DCE, and uses this (and the DFS ACLs) to check users' access rights to DFS files. NetWare users can acquire the access rights that belong to the DCE group to which their corresponding DCE user name belongs. If, however, a user has the access rights both of a DCE user and of a DCE group, the latter is ignored.

DFA makes no conversion between NetWare and DFS groups. Thus, a NetWare group access right cannot be applied to DFS files and directories. See Section 2.6.1 for information on administering user names and group names.

A user, using DFA utilities, can set and reference access rights values for DFS files and directories in the DFA volume with the same commands as used for the corresponding NetWare operations.

DFA converts ACL values (i.e., access rights to DFS) to and from trustee (NetWare) values. NetWare files also have attributes such as ‘‘read only’’ and ‘‘purge’’. However, since such attributes cannot be mapped to DFS files, DFA does not convert them. Instead, DFA displays default values when the attribute of a DFS file is requested by a NetWare user.

The conversion between ACL and trustee values is such that, from the user's (or rather, application program's) point of view, NetWare and DFS have virtually equivalent access rights for files and directories. Since NetWare supports ''inherited right masks'' but DFS does not, DFA does not map the masks.

2.1.6. File locking

In order to permit users connected to different servers to share files, DFA can lock the shared files in DFS. DFA, however, only supports implicit file locking. In other words, DFA will lock a DFS file if an application opened the file in ''write mode'', and releases the lock when the file is closed.

There are two ways to lock a DFS file: mandatory locking and advisory locking. DFA uses mandatory locking. This is because NetWare itself supports only mandatory locking, and a file locked by a NetWare user should be locked from access by a DFS user. If, however, the DFS server operating system does not support mandatory locking, DFA is able to employ advisory locking instead.

2.1.7. File caching

By caching a DFS file onto a NetWare server, DFA's DFS file access speed can be made to approach that of file access on a NetWare server. In particular, a user can take advantage of this feature when a DFA gateway is sited far from the DFA agent.

2.2. Expandability

DFA provides the following expandability to allow users to build a company-wide network by expanding existing NetWare servers:

(a) Adding NetWare users.

A DFA agent on a DFS client can handle multiple DFA gateways. Thus, the number of NetWare users that can concurrently access DFS files can be increased by adding NetWare servers that have DFA gateways. Each NetWare server has the maximum number of login users, and the number of the total DCE users is determined by each DCE.

(b) Adding NetWare servers.

There is no limit to the number of NetWare servers that can be connected to a DFS client. If performance deterioration occurs (such as can happen when, for example, a single DFS client handles too many NetWare servers), a user has only to add a DFS client, and connect some of the NetWare servers to the new client. Bottlenecks can be easily eliminated without changing the current environment.

(c) Adding DFA volumes.

The total number of NetWare and DFA volumes per NetWare server must be 64 or less. However, there is no limit to the number of DFS sub-directories that can be assigned to a DFA volume. Thus, by adding a NetWare server equipped with a DFA gateway to a LAN, a user can virtually augment the effective number of DFA volumes.

(d) NetWare interoperability.

DFA uses the standard NetWare functions. To the extent that new versions of NetWare maintain backward compatibility, DFA will continue to run the new versions.

(e) DFS interoperability.

DFA uses the standard DFS functions. To the extent that new versions of DFS maintain backward compatibility, DFA will continue to run on new versions.

2.3. Security

DFA offers two types of security mechanism: authentication, which ensures that only properly-qualified users can log into DCE; and file access rights, which control DFS file access based on a set of access rights granted to a user. This section describes authentication (see also ''access right control'').

In order to access DFS files via DFA, a user needs to log into (1) a NetWare server equipped with a DFA gateway (in order to access a DFA gateway), and (2) DCE (in order to access DFS). DFA enables a user to login to both with a single operation, and without having to enter a DCE password, greatly simplifying the login operation.

DFA has a login utility for both the DOS and the Windows environment, and this utility provides a login environment at the same level as the NetWare login. At login time, users can select whether or not they will also login simultaneously to DCE. (A user who has chosen to login only to NetWare can subsequently elect to log into DCE by invoking the login utility.)

On a NetWare client, when the login utility receives a user's login request, it first accomplishes the login to NetWare, then (if specified) proceeds to do a DCE login via a DFA gateway. With this method, the user has to specify the NetWare server on which the DFA gateway is running. When a user logs into DCE, the login utility (in fact a DFA gateway) searches the bindery information on the NetWare server, and selects the DCE user name that corresponds to the NetWare user name.

A NetWare password can be different from the DCE password. A DFA administrator can set the DCE password to the NetWare bindery beforehand. See Section 2.6.1 for information on how DCE user names and passwords are registered.

In order for DCE to retain its security level with DFA in operation, it is necessary to make sure there is no password leakage (especially via wire tapping), and also that the DFA gateway is authorized to be connected to DCE.

To prevent illegal access by unauthorized clients, DFA gateways and agents communicate with each other using Kerberos. DFA agents have the full functionality of a Kerberos client, and DFA gateways also have a subset of Kerberos capability. When authentication occurs between a DFA agent and client, no ''raw passwords'' are sent over the wire. NetWare servers store DCE passwords in their bindery, and raw DCE passwords are not transmitted when users login.

2.4. Compatibility

In order to make it as easy as possible to use, DFA inherits PC operations such as displaying file contents, and copying/searching files. In addition, DFA allows use of DOS/Windows application programs, enabling users to smoothly migrate to a DFA-based company-wide network.

DFA's goal is to allow PC application programs to manipulate DFS files in the same manner as local (PC) files. In this sense, DFA guarantees the compatibility of NetWare commands with DFS file operations; however, it should be borne in mind that not all of NetWare's original utility commands will necessarily work with DFS. The following list specifies the kinds and degrees of cross-compatibility that can and cannot be expected from DFA.

(a) Interface compatibility.

DFA compatibility is guaranteed for the following interfaces:

(i) The file access APIs provided by DOS and Windows.

(ii) Operation interfaces provided by Windows utilities that use the above interfaces.

(b) Interface non-compatibility.

DFA compatibility is not guaranteed for the following interfaces:

(i) NetWare client and NLM file access APIs.

(ii) Operation interfaces provided by utilities that use the above interfaces.

Compatibility is accomplished in the following manner (see Section 3.2.2 for details): requests for file access and trustee access via the DOS/Windows API are handled by the corresponding routines of a NetWare server; a DFA gateway hooks into these routines, and translates them into the appropriate DFS file access requests.

2.5. Error Handling

2.5.1. Error detection

This functionality detects DFA errors, allowing users to take the proper action to recover from the error condition. When critical errors occur in a DFA agent or DFA gateway (for example, a DFA agent crash), DFA displays an error message at the consoles of the agent's and gateway's host machines.

2.5.2. Error analysis

This functionality analyzes the causes of hardware errors, program errors and user errors, so that users can avoid repeating the errors.

2.5.3. Error recovery

This functionality assists quick and easy recovery from system faults caused by errors. If a DFA gateway is connected to multiple DFA agents, and one of the DFA agents communicating with the DFA gateway fails, this function automatically connects the DFA gateway to a different DFA agent so that a user can continue the current jobs. Note, however, that DFA does not support automatic recovery of file that was open on a failed gateway.

DFA provides for automatic restart of DFA agents by registering them with a DFS ''overseer'' process (BOS Server).

2.6. DFA Administration

The DFA-specific administrative task is called DFA administration. In order to distinguish a DFS administrator from a NetWare administrator, the person who administers DFA is called a DFA administrator. A DFA administrator and a NetWare administrator can be the same person. The DFA administrator performs DFA administrative tasks from the console of a NetWare server. NetWare supervisor mode is required. Using NetWare's remote console, a DFA administrator can also perform DFA administrative tasks from a NetWare client PC. The details of DFA administration are as follows:

2.6.1. User information administration

DFA maps between NetWare and DCE user names so that NetWare users can access DFS files.

A utility program appends DCE information (e.g., DCE password, DCE user ID) to the NetWare user object, which thus holds information about the DCE properties of the user's DCE user ID. A ''DFA user'' is defined as a user who has such a NetWare/DCE user name mapping. DFA also provides a utility program that displays the NetWare and DCE user name mappings.

However, DFA does not support simultaneous user name registration to DCE and NetWare, nor does it support simultaneous password change in DCE and NetWare.

DFA has a utility program that groups DFA users into a DCE user group. This allows users to set the same access rights for multiple users. The following groups exist:

(a) EVERYONE group.

(b) User group.

The EVERYONE group includes all the DFA user names in the same NetWare server. A User group is a group of DCE users who are eligible to access the same certain DFS directories and files. A User group can be specified, and access rights set for it, in NetWare form.

DFA does not map between already-existing NetWare groups and DCE groups. This is because both groups contain non-DFA users, and it makes no sense to map between them.

DFA registers a DFA user's DCE password with the bindery on a NetWare server, but it does nothing with the DFA user's NetWare password.

2.6.2. Volume administration

The DFA administrator, using a NetWare utility, can create a DFA volume and assign a DFS sub-directory to the DFA volume. DFA displays a directory listing of the DFS file system so that the administrator can easily assign the DFS volume. The ''original'' files in a DFA volume, unlike original NetWare files, reside in a sub-directory of DFS. Since DFS cannot administer the space of a DFS sub-directory, and multiple NetWare administrators can independently assign DFS sub-directories, DFA does not administer the DFA volume space.

If necessary, a DFA administrator can ''un-assign'' the DFA volume from the DFS sub-directory, and, using a NetWare utility, delete the DFA volume.

To use the DFA volume, a user needs to mount the volume onto NetWare using NetWare's mount command, and start DFA. When a user terminates DFA, the DFA volume can be released from NetWare using NetWare's dismount command. NetWare's batch file function enables users to execute such series of operations with a single command.

The DFA utility displays the following volume information:

(a) Volume names.

(b) Names of DFS sub-directories assigned to the volumes.

The DFA administrator, using the DFS back-up utility, can backup the DFS sub-directories onto DFS. The back-up size is by DFS file set (which corresponds to a UNIX file partition). The DFS backup utility does not support the remote execution of DFS backup from a NetWare client, or backup of DFS files onto NetWare.

2.6.3. DCE connection and disconnection

The DFS administrator starts a DFA agent (as a daemon) on the same UNIX machine as the DFS client when starting up the system. The DFA administrator registers a DFA agent's IP address and hostname to the `SYS:ETC$B%H(BOST` file in NetWare. The DFA gateway specifies the IP address of the DFA agent, and has a connection with it. A DFA gateway can connect and disconnect to a DFA agent while DFS is running.

2.6.4. Auditing

DFA administrators can use audit functions provided by both DFS and NetWare. DFA, however, does not provide any new functionality to integrate the two auditing functions.

2.6.5. Accounting

Although DFA does not provide an accounting utility, NetWare's accounting utility (which reports server connect time, number of blocks read, number of blocks written, etc.) can be used on a DFA volume. However, the utility cannot report on disk utilization of DFA sub-directories.

2.7. System and Software Configuration

DFA consists of the following components:

(a) DFA gateway (NLM on NetWare server).

(b) DFA administration utility (NLM on NetWare server).

(c) DFA agent (an application program on a DFS client machine).

(d) Client utility (an application program on a NetWare client machine).

The following table shows the software required to run DFA (in its reference implementation — other ports are beyond the scope of this RFC):

Hardware	Software	Versions
NetWare Client: PC/AT Compatible	DOS Windows (Windows NT) NetWare Shell	5.0 (or later) 3.1 (or later) 3.12
NetWare Server: PC/AT Compatible	DOS NetWare Admin Utility	5.0 (or later) 5.12 1.0
DFS Client: UNIX Machine or PC/AT Compatible	UNIX DCE/DFS	HP-UX 9.02 (or later) AIX 3.25 (or later) Solaris 2.1 (or later) 1.1 (or later)
DFS Server	UNIX DCE/DFS	HP-UX 9.02 (or later) AIX 3.25 (or later) Solaris 2.1 (or later) 1.1 (or later)

Table 1. Prerequisite Software

In order to reduce its size on a NetWare server machine, DFA is split into two parts: a DFA gateway sited on a NetWare server machine, and a DFA agent located on a DFA client machine. Although this method requires that the DFS file access requests re-directed by a DFA gateway be sent to a DFA agent through the communication channel between a NetWare server and DFA client, the NetWare server machine has only to carry a conversion program between NetWare and DFS in order to reduce the load on the server machine.

Another alternative is to embed the functions of the DFS client on the NetWare server machine. The advantage of this method is that the DFS side does not need additional software. However, since the software required to outfit the NetWare server machine is huge, DFA does not employ this method.

2.7.1. Login utility

A NetWare client machine contains the client utilities, including a login utility which logs into NetWare and DCE. This section describes how the login utility is implemented.

DFA DCE login requires the following two steps:

(a) The login request is issued from a NetWare client to a DFA gateway on a NetWare server.

There are two ways to implement this first step: (1) a server catches the login request sent from a client; or (2) a NetWare client provides a different login utility to send the login request to a DFA gateway. Since NetWare does not currently provide the detection means necessary for implementing (1), the method (2) is employed.

(b) The DFA gateway logs into DCE.

This second step can be implemented if the NetWare server machine has a client portion of the DCE security service installed (i.e., Kerberos authentication). This method, however, as was mentioned above, increases the load on the NetWare server. Instead therefore, in DFA the client functionality of the DCE security service is split and embedded in the DFA agent and DFA gateway.

Similarly to NLM on a NetWare server machine, DFA provides the following administration utilities:

(a) Volume assignment (assigning a DFS sub-directory to a DFA volume).

(b) User management (mapping NetWare and DCE user names).

(c) Access rights management (mapping file access rights between NetWare and DFS).

2.8. Internationalization

DFA, using NetWare's enabling service, provides internationalization. For the following items, DFA refers to the ''locale,'' to provide the locally correct value:

(a) Character code.

(b) Numeric.

(c) Dates.

(d) Time.

The localized messages are supplied in a message file, separate from the DFA source code. DFA is shipped with the message file appropriate to the destination's locale.

REFERENCES

[APPL 1.1] OSF, OSF DCE Application Development Reference Revision 1.1, 1994.

[CORE 1.1] OSF, OSF DCE Administration Guide — Core Components Revision 1.1, 1994

[DFS 1.1] OSF, OSF DCE DFS Administration Guide and Reference, Revision 1.1, 1994.

[SDK VOL4] Software Developer's Kits Vol. 4, Novell, 1994.

AUTHOR'S ADDRESSES

Hisashi Hashimoto
Hitachi Limited, SDC
TYG - 11th Building
16-1 Nakamachi 3-CHOME
ATSUGI - SHI, JAPAN
ZIP 243
Internet email: hashimoh@soft.hitachi.co.jp
Telephone: 81-462-25-9271

Toshiya Ito
Hitachi Limited, SDC
TYG - 11th Building
16-1 Nakamachi 3-CHOME
ATSUGI - SHI, JAPAN
ZIP 243
Internet email: itoshiya@soft.hitachi.co.jp
Telephone: 81-462-25-9257

Tsuneo Yamaura
Hitachi Limited, SDC
TYG - 11th Building
16-1 Nakamachi 3-CHOME
ATSUGI - SHI, JAPAN
ZIP 243
Internet email: yamaur_t@soft.hitachi.co.jp
Telephone: 81-462-25-9270