IBM Distributed Computing Environment for AIX,
Version 2.2:

Network File System to Distributed File System Authenticating Gateway Guide and Reference

IBM Distributed Computing Environment for AIX,
Version 2.2:

Network File System to Distributed File System Authenticating Gateway Guide and Reference

Note

Before using this information and the product it supports, be sure to read the general information under "Appendix. Notices" on page 29.

First Edition (February 1998)

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

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

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

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

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

Contents

Figures

About This Book

This book provides guide and reference information about the IBM Distributed Computing Environment (DCE) NFS** to DFS Authenticating Gateway for AIX. Throughout this book, the product is called the NFS to DFS Gateway for ease of reading. The book explains how the NFS to DFS Gateway provides a way to associate a Network File System** (NFS) client request to an authenticated DCE principal, which gives NFS clients authenticated access to the Distributed File Service (DFS) filespace.

Who Should Use This Book

This book is intended for DFS users or administrators who need to understand how to provide authenticated access to the DFS filespace for NFS clients. The book assumes that you have a working knowledge of DCE and its requirements.

Purpose of This Book

This book provides information about:

- Understanding the relationship of the NFS to DFS Gateway to DCE and DFS
- Using the NFS to DFS Gateway effectively

How This Book Is Organized

The book is organized as follows:

- Chapter 1. Overview of the NFS to DFS Gateway, introduces you to the NFS to DFS Gateway and describes how it fits into DCE.
- Chapter 2. Planning for the NFS to DFS Gateway, describes information needed for planning and setting up the NFS to DFS Gateway.
- Chapter 3. Installing and Configuring for the NFS to DFS Gateway, explains how to install and configure the NFS to DFS Gateway.
- Chapter 4. Administering the NFS to DFS Gateway, explains how to manage mappings and perform other administrator activities.
- Chapter 5. Using the NFS to DFS Gateway, explains how to work with the translator to register, change, or delete mappings using the **dfsiauth** command.
- Chapter 6. Command and API Reference, contains reference information for the NFS to DFS Gateway.
- Chapter 7. Troubleshooting the NFS to DFS Gateway, describes some problems you may have with the NFS to DFS Gateway and how you can solve them.

This book also has an index.

Related Publications

For information about DCE in general, and DCE administration for AIX in particular, refer to the following publications:

- *IBM DCE for AIX, Version 2.2: Quick Beginnings*
- *IBM DCE for AIX, Version 2.2: Administration Guide—Introduction*
- *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components*

- *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference*
- *IBM DCE for AIX, Version 2.2: Administration Commands Reference*

Conventions Used in This Book

This book uses the following typographic conventions:

Bold **Bold** words or characters represent system elements that you must enter into the system literally, such as commands.

Italic *Italicized* words or characters represent values for variables that you must supply.

`Example Font`
Examples and information displayed by the system are printed using an example font that is a `constant width typeface`.

[ ] Brackets enclose optional items found in format and syntax descriptions are enclosed in brackets.

{ } Braces enclose a list from which you must choose an item found in format and syntax descriptions are enclosed by braces.

| A vertical bar separates items in a list of choices.

< > Angle brackets enclose the name of a key on a keyboard.

... Horizontal ellipsis points indicate that you can repeat the preceding item one or more times. Vertical ellipsis points indicate that you can repeat the preceding item one or more times.

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

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

This publication uses the following keying conventions :

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

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

Entering commands
When instructed to *enter* a command, type the command name and then press the **<Return>** key. For example, the instruction to “Enter the **ls** command” means that you type the **ls** command and then press the **<Return> key**.

Chapter 1. Overview of the NFS to DFS Gateway

The IBM* NFS to DFS Gateway provides Network File System client users authenticated access to the Distributed File Service (DFS) filespace in the Distributed Computing Environment (DCE). The ability of NFS clients to access the DFS filespace from a DFS client is already inherent in DFS. However, NFS client users are limited to unauthenticated access because the authentication information for DFS and NFS is different. The NFS to DFS Gateway provides a bridge between the diverse authentication information and connects an NFS client user with an authenticated DCE principal. This gives NFS client users authenticated access to the DFS filespace and to the features of DFS.

The relationship among the NFS to DFS Gateway, an NFS Client, and a DFS Server is shown in Figure 1.

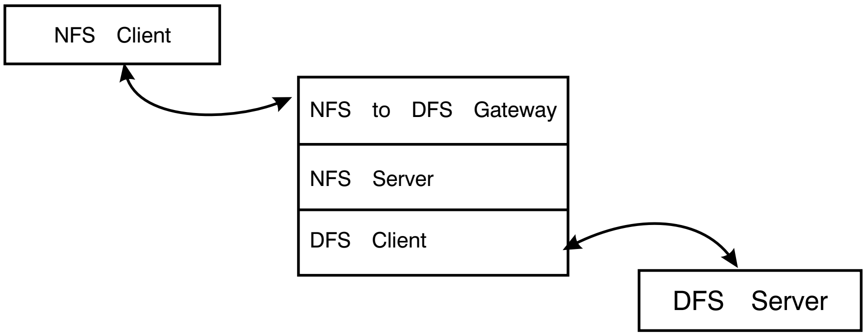

Figure 1. Overview of the NFS to DFS Gateway

Services Provided by the NFS to DFS Gateway

The primary function of the NFS to DFS Gateway is to provide NFS clients with authenticated access to DFS. The NFS client can then view the same file system hierarchy as the DFS client. NFS client users who do not have DFS products for their hardware platforms can participate in DFS file sharing. In addition, the NFS to DFS Gateway provides a migration capability for existing NFS clients to access DFS objects while making the transition to a DFS file sharing environment.

How Does It Work?

To provide file access, the NFS client mounts the exported DFS filespace. In DCE, end users are identified by principal names. In NFS, client requests are identified by an IP address and userID pair. Because the NFS to DFS Gateway resides on a separate machine, NFS users must log in to this translation point and issue the **dfsiauth** command. The **dfsiauth** command describes the address of the NFS client user’s machine and the user’s ID (uid) on that machine and authenticates with DCE, declaring a DCE principal and entering the password. When the NFS to DFS Gateway receives an NFS request, it includes the NFS client user’s machine address and the uid of the request. The NFS to DFS Gateway embeds the DCE credential information in the request, which enables DCE authentication.

Note: This authentication mapping is stored in the operating system kernel so that the architecture requires the user to re-authenticate every time the NFS to DFS Gateway system restarts or the DCE credentials expire. The user is not notified of this need to re-authenticate.

NFS client users can use the NFS to DFS Gateway without making changes to their existing software if they use the **dfsiauth** command on the NFS file server. An API library, **libdceiauth.a**, is provided with the NFS to DFS Gateway so that client/server applications can be developed that establish authentication mappings from the native NFS client to the NFS to DFS Gateway system. Such applications eliminate the need for users to log in to the NFS to DFS Gateway machine to establish their mappings. Additionally, PC-NFS clients can establish authentication mappings transparently if their Gateway System is running **rpc.pcnfsd**.

Some Limitations

The NFS to DFS Gateway does not provide complete DCE services from NFS clients. DCE services such as Directory Services, Security Services, and RPC Services are not available to NFS clients. Also, tools to modify Access Control Lists (ACLs) and DFS administrative commands are not available to NFS client users.

The sole purpose of the NFS to DFS Gateway is to provide authenticated access to DFS from NFS clients.

When data is exported from NFS, the NFS to DFS Gateway and the DFS client do not support byte-range file locking. Attempts to use file locking in applications running in this environment receive the ENOLCK error code at the NFS client.

Packaging of the NFS to DFS Gateway

The NFS to DFS Gateway is optional in a DCE cell. The package has one installable fileset: **dce.dfsnfs.rte**. The **dce.dfsnfs.rte** option contains:

- AIX kernel extension for the NFS to DFS Gateway
- **startnfs.dfs** file to start the NFS to DFS Gateway
- **dfsiauth** command to register, list, and delete authentication mappings
- **libdceiauth.a** user library
- **dcedfs/dceiauthapps.h** include file for application development

dce.compat contains all of the System Management Interface Tool (SMIT) screens for NFS to DFS Gateway management. These screens are in the **dce.compat.dfsnfs.smit** fileset. The message catalogs are contained in **dce.msg.en_US.compat.dfsnfs.smit**.

Chapter 2. Planning for the NFS to DFS Gateway

This chapter provides planning information for the NFS to DFS Gateway.

Setup Considerations

The NFS to DFS Gateway should run on a system where the DFS client has been configured and an NFS server can be configured. The number of NFS users accessing the data should be considered when configuring the DFS client. A large DFS cache may be needed, depending on the number of users and the amount of data accessed from a single DFS client.

When exporting DFS directories to NFS, additional considerations for setting ACLs on DFS directories may be necessary. See “Mounting the DFS Filespace from NFS Clients” on page 6 for more information.

Local ID Differences

The NFS to DFS Gateway adds the authentication information to NFS requests before they are passed to DFS. This authentication mechanism allows the NFS requests to become associated with a DCE principal.

All the DFS requests then seem to come from the DCE principal described in the authentication mapping. Access and ownership attributes are evaluated based on the DCE principal. In particular, when a file is created, the owner is the value associated with the DCE principal.

If the DCE value (user ID and group ID values) associated with the principal is different than the ID value of the NFS client user, the difference can lead to unexpected behavior. For example, a file created by some NFS client users can seem to be owned by a different uid. This is a problem, because many NFS clients infer that the access to files is based on the locally-cached versions of the owner and permission, and these may not correctly express the actual access allowed. For this reason, you should map the local or Network Information Service (NIS)-maintained **/etc/passwd** and **/etc/group** files of your client to the DCE registry or the reverse.

The DCE security utilities, **passwd_export** and **passwd_import**, can help keep these user ID spaces consistent. This action ensures that NFS clients using the NFS to DFS Gateway always obtain the proper permissions for DFS filespace objects.

Adding NFS Clients to DCE Security Registry

Before an NFS client user can set up an NFS to DFS Gateway authentication mapping, a valid DCE principal and account must exist in the DCE security registry. For information on how to add principals and accounts to the registry using the **dcecp** command, see the *IBM DCE for AIX, Version 2.2: Administration Guide—Introduction* and the *IBM DCE for AIX, Version 2.2: Administration Guide—Core Components* .

Performance Considerations

For optimal performance, consider NFS client-to-server ratios when deciding the DFS clients that also act as NFS servers and run the NFS to DFS Gateway within a file-sharing environment.

Multiple Gateway Considerations

To achieve proper load balancing if multiple gateway machines are configured in the cell, ensure that the NFS client mounts are divided evenly among the gateway systems. One way to balance the load placed on an environment by NFS client systems is to configure multiple gateway machines in the cell and divide the load among these machines instead of using a single gateway to serve the needs of the entire environment.

Even if multiple gateway machines are not configured, each machine still maintains it own authentication mapping table. The **dfsiauth** commands affect entries in the authentication mapping table only on the machine that the command is issued against.

Chapter 3. Installing and Configuring for the NFS to DFS Gateway

This chapter explains the steps needed to install and configure your system for the NFS to DFS Gateway.

Installing

To install the NFS to DFS Gateway, the **dce.client** package (**dce.client.core.rte** and **dce.client.dfs.rte**) and **bos.net.nfs.server** (version 4.1.0.0) are required. For more information on installing DCE for AIX and the NFS to DFS Gateway, see *IBM DCE for AIX, Version 2.2: Quick Beginnings*.

Disk Space Required (in Megabytes)

The DCE options for the NFS to DFS Gateway have the following approximate space requirements:

dce.dfsnfs.rte
.2

dce.compat.dfsnfs.smit
.01

dce.msg.en_US.compat.dfsnfs.smit
.001

Configuring

To provide NFS to DFS Gateway service, you can perform configuration using NFS System Management Interface Tool (SMIT). SMIT uses interactive menus to guide users through configuration and other system management tasks.

As **root**, start SMIT by entering:

```
smit
```

Then, select the following sequence of SMIT menu options:

1. **Communication Applications and Services**
2. **DCE (Distributed Computing Environment)**
3. **NFS to DFS Authenticating Gateway Administration**
4. **Start NFS to DFS Gateway**

To configure NFS to DFS Gateway using the command line interface, you need to:

1. Verify that DCE/DFS and NFS are configured and running on a system.
2. Load the NFS to DFS Gateway kernel extension by running the **startnfs.dfs** command.

   Note: The **startnfs.dfs** command now has an autostart option. From the command line you can run or rerun the **startnfs.dfs** command with the **-autostart yes** option. To turn autostart off, the **startnfs.dfs** command can be run or rerun with the **-autostart no** option.

To support automatic startups as **root**, start SMIT by entering:

```
smit
```

Then, select the following sequence of SMIT menu options:

1. **Communication Applications and Services**
2. **DCE (Distributed Computing Environment)**
3. **Configure DCE/DFS**
4. **DCE/DFS Start Options**
5. From the list of options, select **DCE, DFS, and NFS to DFS Gateway**
6. **Select the DCE/DFS items to start**
7. From the list of options, select **START now, system restart or both**
8. By selecting **system restart or both**, automatic startup begins.

To support automatic startups, experienced system administrators can also modify /**etc**/**inittab** file to include the /**etc**/**dce**/**rc.dfsnfs** startup file. Make this change after DCE/DFS (**rc.dce all**) and NFS (**rc.nfs**) are started within this file.

Exporting the DFS Filespace to NFS

After the DFS client and NFS server are both running on a system, the DFS filespace is made available to NFS clients by exporting the DFS filespace to NFS. For example, the top of the DCE tree is /**...**. Following that is the cell name and the junction point into DFS (/**...**/*cellname*/**fs**). Any portion of this path can be exported to NFS.

By exporting **/...**, NFS clients have access to all cells that the local DCE cell can access through intercell registration. By exporting **/.../***cellname***/fs**, NFS client access is limited to a particular cell. Administrators should consider these options in deciding that part of the DFS filespace that is exported. If using PC-NFS, the full name of **/.../***cellname***/fs** should be used.

In addition, NFS-exporting the DFS filespace exposes it to a decreased level of protection because NFS RPC is less secure than DCE RPC.

Note: Administrators should take precautions against forged NFS requests, replay, and IP address spoofing by exporting to a specific group of machines only and by protecting the NFS protocol.

After considering these alternatives, the DFS filespace can be NFS-exported by adding an entry to the **/etc/exports** file and running the **exportfs** command. You can also use the SMIT screen, *Add a Directory to Exports List*. This action allows NFS client users to have both unauthenticated and authenticated access to the DFS filespace.

Mounting the DFS Filespace from NFS Clients

On the NFS client system, the DFS filespace must be mounted in order for the NFS client to access files and directories. The following steps should be performed:

1. Log on to the NFS client system.
2. Mount the DFS filespace (/... or a leaf node of /...) on the system using the appropriate mount command for the NFS client.
3. Verify that the mount command was successful by using a listing command to view the contents of the DFS filespace from the NFS client.

After the DFS filespace is mounted, NFS clients should see a view similar to what DFS clients see for the DFS filespace. At this point, NFS clients can access the DFS filespace as unauthenticated users. An authentication mapping between the NFS client user and a DCE principal must be established (using the **dfsiauth** command) before authenticated access to the DFS filespace is provided.

Additional steps may be necessary for the NFS client mount to succeed. When the NFS client mounts a file system, the **rpc.mountd** daemon on the NFS server (the gateway system) performs the mount on behalf of the client. Because **rpc.mountd** is not DCE-aware, it may not have the proper DCE credentials to access DFS and successfully perform the mount.

On a DCE client, the local operating system root user and daemons that run as root run with the DCE machine context if an explicit **dce_login** is not done. This is also known as the *self credential* and the DCE principal is of the form, **hosts/<***dce_hostname***>/self**.

The ACL on the root of the fileset where the mount is performed may need to be changed so that the local root user on the Gateway system that is using the machine context can access the directory using the **rpc.mountd** daemon. This gives access to the local root on the gateway only; unauthenticated users will not be able to access protected DFS data.

There are several different ACLs which can be placed on the directory mount point to allow the mount to be performed. In all cases, the minimal permissions needed are **read** and **execute/search** permissions (rx). The ACL can be added or changed by using the **acl_edit** or **dcecp** commands.

- Add the individual self principal to the ACL.
- Create a group in the registry which contains the self principals for each Gateway system. Then add the group to the ACL.
- Change the permissions on the **other_obj** ACL.

If the mount is being performed on a leaf node of **/.../<***cellname***>/fs**, it may be necessary to change the ACLs on parent directories of the mount point also.

If the DFS filespace has been accessed prior to the ACLs being changed, it may be necessary to flush the directory information from the DFS client cache before the cache recognizes the changes. This can be done by executing **cm flush** and **cm flushfileset** commands against the mount point and any parent directories of the mount point.

Chapter 4. Administering the NFS to DFS Gateway

After the NFS to DFS Gateway is started on the DFS client, users can begin setting up authentication mappings and making authenticated requests from NFS clients. This chapter explains the following topics for administering the NFS to DFS Gateway:

- Setting @sys and @host values
- Managing expired authentication mappings
- Considering DFS access for NFS clients
- Understanding NFS anonymous mappings

Examples of these activities are shown in Chapter 5. Using the NFS to DFS Gateway.

The relationships among NFS and DFS clients and servers, and the NFS to DFS Gateway are shown in Figure 2.

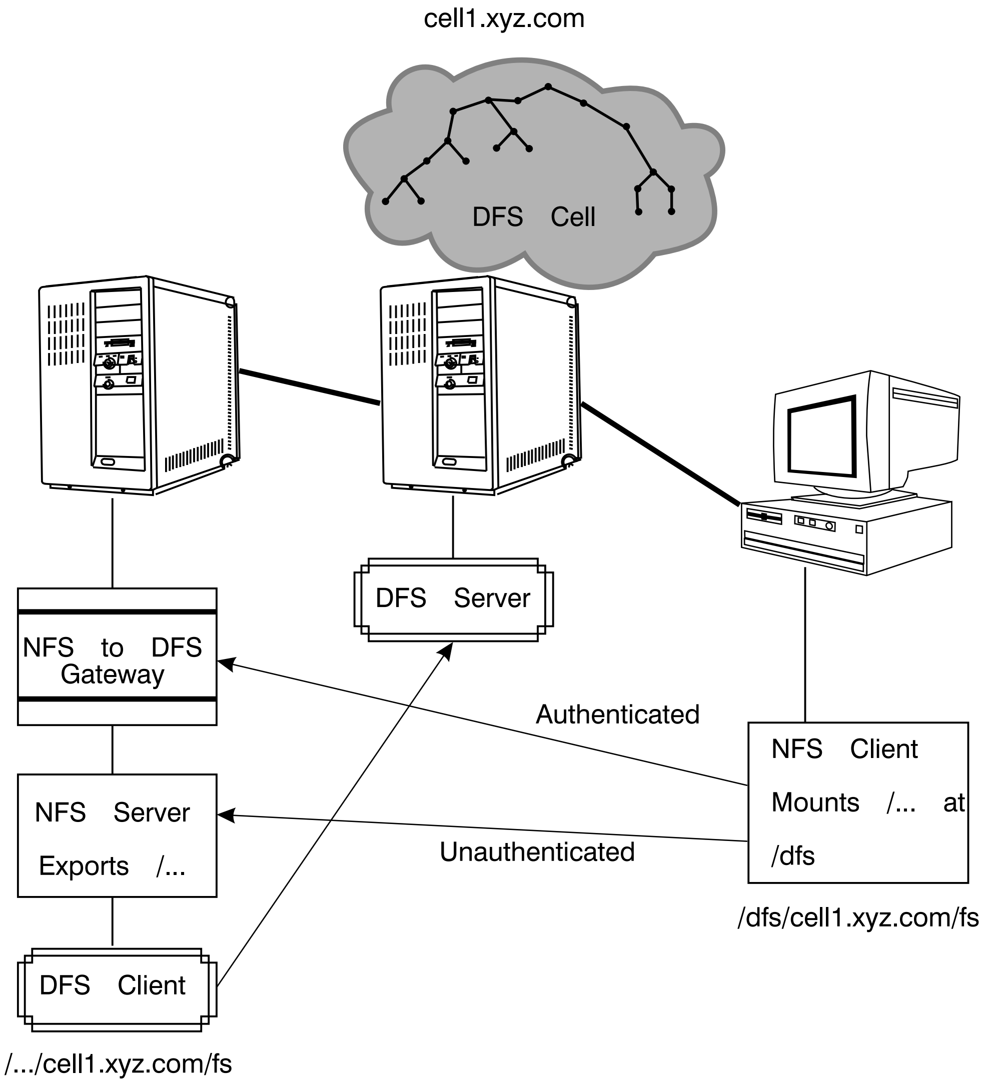

Figure 2. How the NFS to DFS Gateway Works

Setting up @sys and @host Values

DFS uses the @sys and @host values to access operating system-specific and host-specific files and directories if the administrator has set them up. The DFS client expands @sys and @host names that it encounters to a defined system name or hostname.

The NFS to DFS Gateway can make these pathname substitutions if the @sys and @host values are registered for a host-uid pair. To register these values, use the **dfsiauth** command with options for @sys and @host substitution values to be used with the host-uid pair being registered for authentication.

The DFS system administrator must set up the proper symbolic links in the DFS filespace so clients can access system- and host-specific information correctly. Refer to the *IBM DCE for AIX, Version 2.2: DFS Administration Guide and Reference*for information on setting up @sys and @host symbolic links in the DFS filespace.

It is sometimes desirable to allow certain NFS clients unauthenticated access only to the DFS filespace. However, these clients may still need to translate @sys and @host pathnames when accessing the file space.

For example, NFS PC clients may want to access the DOS binaries of an application stored in DFS. These values can be registered by using the **dfsiauth** *-add* command without specifying a principal name. This tells the command to register the @sys and @host values given on the command line only and does not attempt to authenticate as a DCE principal. Because authentication is not attempted, the NFS client host-uid pair does not obtain authenticated access in the DFS filespace.

Because DFS clients have a default @sys value, an NFS client accessing the DFS filespace without an @sys value defined in its authentication mapping can unintentionally pass through an @sys symbolic link and access information of a different machine type. This can cause undesirable behavior on user systems. To avoid this situation, the @sys value should be defined for the NFS client architecture when registering an authentication mapping.

Managing Expired Authentication Mappings

When DCE authentication tickets expire, the NFS client user is not notified. On the NFS client machine, it seems to the user that authenticated access has suddenly been lost. The NFS to DFS Gateway on the DFS client collects the expired authentication mappings and removes them from the authentication mapping table to avoid having the NFS to DFS Gateway overrun with expired mappings. This action occurs when the NFS to DFS Gateway is managing more than 1000 active mappings.

When a user adds another authentication mapping beyond the 1000 active-mapping limit, the NFS to DFS Gateway attempts to remove any expired and unauthenticated mappings. If no expired or unauthenticated mappings exist, the NFS to DFS Gateway still adds the authentication mapping.

A system administrator who wants to remove expired mappings more frequently can use the **dfsiauth** *-flush* command. By issuing this command, expired mappings, including unauthenticated mappings, are removed immediately from the NFS to DFS Gateway.

Example

The following example shows the local root user flushing expired mappings from the NFS to DFS Gateway system:

```
# dfsiauth -flush
dfsiauth:  flush operation successful
```

Accessing DFS from NFS Clients

Unauthenticated access is provided to users who access DFS without first authenticating to DCE. Unauthenticated users receive the following permissions for objects (files and directories) in the DFS filespace:

- For objects in JFS filesets — the permissions granted by the *other* mode bits of the object

- For objects in DCE LFS filesets — the permissions granted by the *any_other* entry, if it exists, on the ACL of the object. The *mask_obj* entry filters permissions granted through the *any_other* entry.

Authenticated access is available to users who have accounts in the DCE cell. When an authenticated user accesses an object in the DFS filespace, the user receives the permissions associated with that DCE identity. When the user creates an object, the object is owned by the user and the user's primary group.

Understanding NFS Anonymous Mappings

By default, the NFS server maps root requests (uid=0) and unauthenticated requests in the case of Data Encryption Standard (DES)-authenticated NFS, to the nobody user ID (uid=-2). The *-anon* option is provided in the **/etc/exports** file to specify that these requests be mapped to a specific user ID. You can also use the SMIT screen, *Change/Show Attributes of an Exported Directory*. The intermediate authentication process of the NFS to DFS Gateway is performed after this mapping has occurred.

Example

The following example shows how to set up an anonymous mapping for the NFS client, *blue.ibm.com*, to access the DFS filespace as root. The local ID, *dceguest*, which has a uid of *200*, is used.

On the NFS to DFS Gateway system, add the *-anon=200* option to the **/...** line in the **/etc/exports** files. Then set up an authentication mapping for the NFS client using the local id, *200*, with the **dfsiauth** command. For example:

```
$ dfsiauth -add -r blue.ibm.com -i 200 -u peter
Enter Password:
dfsiauth: <blue.ibm.com, 200> mapping added
DCE principal: peter
```

If the user is logged in as the local root user on the NFS client, the DFS filespace can be accessed.

Using the PC-NFS Daemon with the NFS to DFS Gateway

If the AIX v.4 NFS **rpc.pcnfsd** daemon is running on the gateway system, it supports the transparent registration of DCE authentication mappings with the NFS to DFS Gateway. When a PC-NFS client user mounts a filesystem on the Gateway system, the user authenticates with both the AIX system and the NFS to DFS Gateway. The DCE authentication mapping is set up successfully only if the user's local AIX identity (username and password) matches the user's DCE registry identity.

If the local AIX identity and the DCE registry identity for a user do not match, an NFS to DFS Gateway authentication mapping cannot be established through **rpc.pcnfsd**. In this instance, the mapping should be set up by logging into the Gateway system locally or remotely using the telnet or **rlogin** facilities and entering the **dfsiauth** command.

The environment variable, DFSIAUTH_PCNFSD_ATSYS, is also provided and it allows the DFS Gateway administrator to set the **-s** (@sys) value for PC-NFS client users to use when obtaining their authentication mappings through **rpc.pcnfsd**.

This value should be set on the Gateway system before **rpc.pcnfsd** is started. If the environment variable is not set, an @sys value is not defined for PC-NFS users that register through **rpc.pcnfsd**.

The following example and system response sets the environment variable to intel_bin before starting **rpc.pcnfsd** on the Gateway system. It then shows the result of a listing command after the user 'jimmy' has authenticated through his PC-NFS client.

```
# export DFSIAUTH_PCNFSD_ATSYS=intel_bin
# /user/sbin/rpc.pcnfsd
# dfsiauth -list
Host                Uid    Principal   @sys         @host        Expiration
----                ---    ---------   ----         -----        -----------
elvis.com           103    jimmy       intel_bin                 3/31/1996 13:44
```

Chapter 5. Using the NFS to DFS Gateway

This chapter describes how a NFS to DFS Gateway user performs the following tasks:

- Use the **dfsiauth** command
- Register authentication mappings
- Set @sys and @host values within a mapping
- Change authentication mappings
- Display existing authentication mappings
- Delete authentication mappings
- Manage expired mapping information

Using the dfsiauth Command

To use the NFS to DFS Gateway, you must log in to the NFS to DFS Gateway system locally or log in remotely using telnet or rlogin facilities. After logging in to this system, you can enter the **dfsiauth** command to set up the authentication mapping for the NFS to DFS Gateway. Alternatively, the system administrator for the NFS to DFS Gateway can set up the mappings for NFS to DFS Gateway users.

Before entering **dfsiauth**, you must have an account in the DCE security registry with a password. You must enter the remote host and remote uid pair of the NFS client requesting access along with the name of the DCE principal for authentication on the command line. The command prompts for the DCE principal password if it is not included on the command line. It is not necessary to use **dce_login** before entering the **dfsiauth** command.

The **dfsiauth** command with syntax, options, usage notes, and examples can be found in Chapter 6. Command and API Reference.

Registering Authentication Mappings

For an NFS client user to have authenticated access to DFS, an authentication mapping must exist that maps the NFS client machine host ID and remote user ID to a DCE principal that has the proper access to DFS. If this authentication mapping does not exist, DFS determines that the NFS client request for data is unauthenticated. This is equivalent to a DFS user who has not entered a **dce_login** to the DCE cell.

Users register their authentication mappings to the NFS to DFS Gateway by using the **dfsiauth** *-add* command. This command verifies the authentication information of the given DCE principal and then registers an authentication mapping of a host-uid pair to that principal. This command also allows you to specify how to interpret @sys and @host values in pathname substitutions.

Example

The following example and system response adds an authentication mapping for user ID *100* on the NFS client system, *purple.ibm.com*, which is authenticated as DCE principal *peter*:

```
# dfsiauth -add -r purple.ibm.com -i 100 -u peter
Enter Password:
dfsiauth: <purple.ibm.com, 100> mapping added
DCE principal: peter
```

In addition to registering authentication mappings with the NFS to DFS Gateway, it is possible to register @sys and @host values for unauthenticated NFS users only. You can use the **dfsiauth***-add* command without specifying a DCE principal (*-u*) to add.

Example

The following example and system response adds an unauthenticated mapping for user ID *120*, on NFS client *yellow.ibm.com*, and sets up an @sys value of *intel_dos* and an @host value of *yellow* for the unauthenticated user.

```
# dfsiauth -add -r yellow.ibm.com -i 120 -s intel_dos -h yellow
dfisauth: <yellow.ibm.com, 120> mapping added
DCE principal:
@sys Type: intel_dos, @host Type: yellow
```

Setting @sys and @host Values within a Mapping

The NFS to DFS Gateway can make pathname substitutions if the @sys and @host values are registered for a host-uid pair. This can be done by using the **dfsiauth** command and providing the @sys and @host substitution values to be used with the host-uid pair being registered for authentication.

NFS to DFS Gateway users should verify with their system administrators the correct @sys and @host values to use when registering authentication mappings.

Because DFS clients have a default @sys value, an NFS client user accessing the DFS filespace who does not have an @sys value defined in the authentication mapping can unintentionally pass through an @sys symbolic link and access information of a different machine type. You should be aware of this possibility because it may cause undesirable behavior on your systems. To avoid this situation, the @sys value should be defined for the architecture of the NFS client system when registering an authentication mapping.

Changing Authentication Mappings

If you want to change the *@sys* and *@host* definitions in the authentication mapping that is currently registered, you can use the *-overwrite* option of the **dfsiauth** command. For example, you may want to change the defined *@sys* value which is currently *rs_aix41*, to the value of *rs_aix42*. The *-overwrite* option is the equivalent of deleting the current mapping and adding it again using corrected information. You must authenticate as the DCE principal who originally set up the mapping in order to change the information.

Example

The following example and system response shows changing the authentication mapping for user id `100`, at NFS client system `purple.ibm.com`, which is authenticated as DCE principal, `peter`:

```
# dfsiauth -add -overwrite -r purple.ibm.com -i 100 -u peter -s rs_aix42
Enter password:
dfsiauth: <purple.ibm.com, 100> mapping changed
```

Displaying Authentication Mappings

Authentication mappings that are registered with the NFS to DFS Gateway can be displayed by using the **dfsiauth**-*list* command. You must provide a DCE principal and password in order to display a mapping. The listing displays the current mapping and one of the following:

- Date the mapping expires
- Whether the mapping has expired
- Whether the mapping is unauthenticated

The local root user has authority to view all the registered mappings when using the list option.

Example

The following example and system response shows DCE principal, *peter*, displaying the authentication mappings that are currently registered to it:

```
# dfsiauth -list -u peter
Host                Uid    Principal    @sys     @host     Expiration
----                ---    ---------    ----     ----      ----------
purple.ibm.com      100    peter        rs_aix32           5/21/1995 14:55
```

Deleting Authentication Mappings

When an authentication mapping is no longer needed, you can remove it by using the *-delete* option of the **dfsiauth** command. This command removes a host-uid pair from the NFS to DFS Gateway mapping table. Authentication mappings are also removed when the mapping has expired. It is not necessary to provide the @sys and @host values when deleting an authentication mapping.

Example

The following example and system response shows deleting the authentication mapping for DCE principal, *peter*, which is registered for NFS client, *purple.ibm.com*, as userid *100*.

```
# dfsiauth -delete -r purple.ibm.com -i 100 -u peter
Enter Password:
dfsiauth: <purple.ibm.com, 100> mapping deleted
DCE principal: peter
```

Managing Expired Mapping Information

When you register an authentication mapping, you also authenticate to DCE to obtain DCE credentials. In the DCE environment, you can renew expired credentials using the **kinit** command. However, because the NFS to DFS Gateway authentication mapping does not have a current process associated with it on the NFS to DFS Gateway system, **kinit** cannot be used to renew the credentials of an authentication mapping.

From the NFS user's point of view, it seems the user has lost authenticated access when the user's credentials expire on the NFS to DFS Gateway. To become re-authenticated, the user must reregister the authentication mapping with the NFS to DFS Gateway. If the expired mapping has not been removed by the system administrator, it may still exist at the NFS to DFS Gateway. In this situation, the user should use the **dfsiauth** *-add -overwrite* options to re-establish authenticated access.

Using the NFS to DFS Gateway from Non-UNIX Clients

Because of differences in operating system design, function, and NFS implementations, the following should be considered when using the NFS to DFS Gateway from non-UNIX clients:

- To mount the DFS filespace, OS/2 clients may need a login ID and password or may need to set the UID of the client machine by using: `SET UNIX.UID` and `SET UNIX.GID`.
- If a symbolic link cannot be resolved because the file or directory it points to does not exist, errors may result. The listing command may stop when it attempts to list the symbolic link and may not display any directory entries after the symbolic link.
- AIX and other UNIX operating systems support case sensitivity for file and directory names. OS/2 and other PC operating systems are not case-sensitive. This can cause confusing results when accessing data from the NFS client.

Chapter 6. Command and API Reference

This chapter contains command and API reference information for the NFS to DFS Gateway.

dfsiauth

Purpose

Performs operations against the NFS to DFS Gateway to authenticate a DCE principal; to register, unregister, or list host-uid pairs for translation; and optionally, to associate @sys and @host values for path substitution.

Synopsis

```
dfsiauth –add [–overwrite] | –delete –r remote_host –i remote_uid [–u principal][–p password]
[–s sysname] [–h hostname]
```

```
dfsiauth –list [–u principal] [–p password] | –flush
```

Options

–r remote_host
: Specifies the hostname of the machine requesting authenticated access.

–i remote_uid
: Specifies the uid of the user requesting authenticated access.

–u principal
: Specifies the DCE principal to authenticate as.

–p password
: Specifies the password of the DCE principal.

–s sysname
: Associates the parameter sysname with the @sys value for the input host/uid pair.

–h hostname
: Associates the parameter hostname with the @host value for the input host/uid pair.

–add Adds the specified mapping information.

–delete
: Deletes the specified mapping information.

–overwrite
: Changes information about an existing mapping. This option is only valid with the *–add* option.

–list Lists the registered authentication mappings.

–flush Removes expired authentication mappings.

Description

The **dfsiauth** command performs operations against the NFS to DFS Gateway for a remote host and remote uid with an existing DCE principal. It is issued on the machine that performs NFS to DFS translation. The DCE principal password must be included. The password can be included on the command line (*-p password*). When the password is not included, the command prompts for the password.

Options such as *–add* and *–delete* can be abbreviated on the command line to *–a*, *–d*, or other shortened forms of the option. Specific option information includes:

- The *–add* option is used to register a hostname-uid pair to a DCE principal. Along with performing an association for NFS service, the command can also be used to associate an @sys and @host name for path element substitution. If a principal is not specified, an unauthenticated mapping is assumed and only @sys and @host values are registered. No attempt is made to validate the selected values of @sys and @host.
- The *–overwrite* option is used with the *–add* option only to overwrite an existing authentication mapping. This option is useful if the @sys value needs to be changed because of a software upgrade. To overwrite existing information, the principal that initially set up the mapping must also be given as the principal requesting to overwrite the information.
- The *–delete* option is used to remove an authentication mapping from the NFS to DFS Gateway. The principal that added the mapping must be the same as the principal attempting to delete the mapping. This information is checked before the deletion is attempted. If the principals do not match, an error is returned. The principal is not checked when an attempt is made to remove unauthenticated mappings, for example @sys and @host mappings. Also, a mapping cannot be deleted if the principal has been removed from the DCE registry.
- The *–list* option displays the hostname-uid pairs that are registered with the NFS to DFS Gateway. A user must provide the DCE principal and password before the registered mappings can be displayed. Only the user’s mappings are displayed. The local root user can issue this command to view all mappings registered with the NFS to DFS Gateway. The mapping information fields displayed can be truncated to display the output within the screen format.
- The NFS to DFS Gateway periodically performs automatic removal of expired mappings. However, the **dfsiauth –***flush* option can also be used to manually remove all expired and unauthenticated authentication mappings from the NFS to DFS Gateway. Only the local root user can issue this command.

Options

This program runs as a setuid program. The issuer must be the local root user to run the **–flush** option.

Examples

- Adding a Mapping with the Password on a Command Line

  The following command and system response authenticates to DCE as the principal, *dawn*, and registers the remote host, *sunlight*, and remote uid, *1065*. The sysname, *rs_aix32*, is also associated with this authentication mapping.

  ```
  $ dfsiauth -add -r sunlight -i 1065 -u dawn -p -dce- -s rs_aix32
  dfsiauth: <sunlight, 1065> mapping added
  DCE principal: dawn
  System Type (@sys) rs_aix32
  ```

- Adding a Mapping when Prompted for a Password

  The following example and system response shows the authentication mapping for remote host, *spooky.austin.ibm.com*, and uid, *654*, where the command prompts for the password.

  ```
  $ dfsiauth -add -r spooky.austin.ibm.com -i 654 -u ghost
  Password: boo
  dfsiauth: <spooky.austin.ibm.com,654> mapping added
  DCE principal: ghost
  ```

- Adding a Mapping with @sys and @host Values

The following example and system response shows setting the @sys value, *intel_os2*, and @host value, *mystic*, to be associated with the remote host, *mystic*, and remote uid, *1022*. This mapping sets up @sys and @host values for an unauthenticated DFS user.

```
$ dfsiauth -add -r mystic -i 1022 -s intel_os2 -h mystic
dfsiauth: <mystic,1022> mapping added
System Type (@sys) intel_os2, Host Type (@host) mystic
```

- Changing an Existing Mapping

  The following example and system response overwrites the existing mapping of remote host, *sunlight*, and remote uid, *1065*, by changing the current rs_aix32 @sys value to the new value, *sun*. This mapping was previously registered using the DCE principal, *dawn*.

```
$ dfsiauth -add -overwrite -r sunlight -i 1065 -u dawn -p -dce- -s sun
dfsiauth: <sunlight,1065> mapping changed
DCE principal: dawn
System Type (@sys) sun
```

- Deleting an Existing Mapping

  The following example and system response shows deletion of the authentication mapping for the remote host, *spooky.austin.ibm.com*, and remote uid, *654*, associated with DCE principal, *ghost*.

```
$ dfsiauth -delete -r spooky.austin.ibm.com -i 654 -u ghost -p boo
dfsiauth: <spooky.austin.ibm.com, 654> mapping deleted
DCE principal: ghost
```

- Displaying Existing Mappings for All Users

  The following example and system response shows listing the registered authentication mappings. The user is logged in as the local root user.

```
# dfsiauth -list
Host                     Uid     Principal      @sys        @host         Expiration
----                     ---     ---------      ----        -----         ----------
sunlight.austin          1065    dawn           sun                       2/27/1995 12:00
mystic                   1022    -              intel_os2   mystic        [Unauthenticated]
```

- Displaying Existing Mappings for One User

  The following example and system response shows listing the registered authentication mappings. The user is logged in as a local non-root user.

```
$ dfsiauth -list -u dawn -p -dce-
Host                     Uid     Principal      @sys        @host     Expiration
----                     ---     ---------      ----        -----    ----------
sunlight.austin          1065    dawn           sun                  2/27/1995 12:00
```

dceiauthcall

Purpose

Authenticates a DCE principal and performs operations against the NFS to DFS Gateway to register or unregister a host-uid pair for translation, and associate @sys and @host values for path substitution.

Options

NFS to DFS Gateway Library (libdceiauth.a)

Synopsis

```
#include <dcedfs/dceiauthapps.h>

int dceiauthcall (char * remoteHost, char * remoteUid, char * user, char * passwd, char * sys,
char * host, int * pag, int flags, char * buffer, int * buflen)
```

Arguments

- Input

  remoteHost
  Specifies the hostname of the system requesting authenticated access.

  remoteUid
  Specifies the remote user ID.

  user
  Specifies the principal for authentication.

  passwd
  Specifies the password of the DCE principal in the DCE registry.

  sys
  Specifies the value to be used for @sys pathname substitutions.

  host
  Specifies the value to be used for @host pathname substitutions.

  flags
  Specifies the operation to perform against the NFS to DFS Gateway. Valid flags are listed 23. The parameter value is constructed by logically ORing the specified flags.

- Output

  pag
  Specifies the page ID that has been registered in the call.

  buffer
  Specifies the buffer to return query information. This function is not supported at this time.

- Input/Output

  buflen
  Specifies the length of the buffer being passed. This function is not supported at this time.

- Flags

IAUTH_ADD
Adds the authentication mapping specified.

IAUTH_DELETE
Removes the authentication mapping from the NFS to DFS Gateway.

IAUTH_OVERWRITE
Overwrites an existing mapping with new information. This flag has no effect if specified with the IAUTH_DELETE flag.

Description

The **dceiauthcall** is used by applications to perform operations against the NFS to DFS Gateway. The supported operations allow remote host-remote uid pairs to be registered or unregistered to an existing DCE principal. Values for @sys and @host substitution can also be passed in as parameters. This API calls the proper DCE security routines to verify the authentication and obtain DCE credentials before making the appropriate NFS to DFS Gateway system call to perform the operation. The overwrite flag, IAUTH_OVERWRITE, can be used with the IAUTH_ADD flag to change information about an existing authentication mapping. If the IAUTH_OVERWRITE is used with a nonexistent entry, IAUTH_OVERWRITE is ignored and the entry is added.

Options

On success, a *0* is returned. If the call fails, a negative value is returned, and the *errno* is set as follows:

Options

EPERM
The caller does not have super user privilege or attempted to remove an entry other than its own.

EEXIST
The entry already exists. The IAUTH_OVERWRITE flag should be used to overwrite an existing entry.

ENOMEM
Memory is not available to add the new entry.

EINVAL
A parameter that is not valid was passed into the call.

ENOENT
The entry does not exist for the host-uid pair.

EBUSY
The entry is currently in use and cannot be removed.

startnfs.dfs

Purpose

Starts the NFS to DFS Authenticating Gateway.

Synopsis

startnfs.dfs [**-autostart** {**yes** | **no**}] [**usage**] [**-?**] [**help**] [**operations**]

Options

-autostart {yes | no}]
Specifies that the NFS to DFS Authenticating Gateway should be started at the machine start. (An **rc.dfsnfs** entry is placed in **/etc/inittab** file.)

usage Displays a usage message.

-? Displays a help message.

help Displays a brief description of the options.

operations
Lists all the options.

Description

The **startnfs.dfs** command starts the NFS to DFS Authentication Gateway. If **-autostart** is specified, then the NFS to DFS Authenticating Gateway will be started on a system restart.

Chapter 7. Troubleshooting the NFS to DFS Gateway

This chapter describes some problems you may encounter with the NFS to DFS Gateway, and explains how to solve them.

Unable to Start the NFS to DFS Gateway

If the NFS to DFS Gateway does not start, verify that DCE, DFS, and NFS have been started before starting the NFS to DFS Gateway.

Unable to Access Data from NFS Client

The following items should be checked and corrected before re-attempting to access data. Some items should be checked on the NFS to DFS Gateway system because they may be related to DCE functions.

Verify that the network is operational.

Verify that DCE with DFS, NFS, and the NFS to DFS Gateway is running on the NFS to DFS Gateway system.

Verify that a valid, unexpired authentication mapping exists for the user by entering **dfsiauth** *-list*.

If multiple Gateway systems are configured, verify that the NFS client is mounting to the Gateway system where the authentication mapping has been established.

Verify that the user has the correct Access Control List (ACL) permissions.

Verify that the user's local UNIX ID (uid) or group ID (gid) matches the DCE principal ID or DCE group ID.

System Reboot of Client or System

For a system reboot on the client machine the following items should be checked on startup:

Verify that the network is operational.

Verify that the NFS client is running.

Verify that the DFS filespace has been mounted.

For a system reboot on the NFS to DFS Gateway machine, the following items should be checked on startup:

Verify that the network is operational.

Verify that DCE with DFS, NFS, and the NFS to DFS Gateway are running.

Verify that the DFS filespace is exported.

Verify that the clients have re-added their authentication mappings.

Unable to Add, List, or Delete a Mapping

The following items should be checked and corrected:

If adding a mapping, verify that a mapping does not already exist using **dfsiauth** *-list*. If it does, verify that it has not expired.

If deleting a mapping, verify that a mapping exists using **dfsiauth** *-list*.

Verify that the NFS to DFS Gateway is running.
Verify that DCE security is operational.
Verify that the DCE principal is valid in the Security Registry.
Verify that the password is correct.

Appendix. Notices

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

IBM may have patents or pending patent applications covering subject matter 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 the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594, USA.

This publication may contain examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples may include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

AIX
IBM

Network File System and NFS are registered trademarks of Sun Microsystems, Inc.

DFS is a trademark of the Transarc Corporation.

Index

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