Open Software Foundation **J. Brezak (HP)**
Request For Comments: 84.0
July 1995

DFS GATEWAY SUPPORT OF @SYS AND @HOST PER NFS CLIENT MAPPINGS

1. INTRODUCTION

The DFS Gateway allows NFS clients to mount the exported DCE DFS namespace (rooted at `/.../`) from an NFS client host, using a secure mechanism for the NFS client to obtain DCE credentials, as described in [MiSo]. When an NFS client accesses the DFS namespace through the DFS client, it uses the DFS client's values for `@sys` and `@host`. The `@sys` and `@host` values should represent the NFS client instead of the DFS client acting as the gateway. This will let NFS clients of differing machine architectures share a single DFS gateway server.

Adding the capability for NFS clients to have unique `@sys` and `@host` values requires that the DFS Gateway components `dfsgw`, `dfsgwd` and `dfs_login` be modified. In addition, the DFS cache-manager (CM) needs to be modified to use the appropriate `@sys` and `@host` values for the correct client — local or remote NFS.

2. TARGET

This capability is for users of the DFS Gateway who wish to have the `@sys` and `@host` expansions match the NFS client system that they are using instead of the DFS Gateway machine.

3. TERMINOLOGY

(a) **@host**

A syntactic token that can exist in a file or directory name that gets expanded to the hostname on lookup.

(b) **@sys**

A syntactic token that can exist in a file or directory name that gets expanded to the sysname on lookup.

(c) **cache manager**

The DFS cache-manager (CM). It implements the client side of the DFS and (usually) resides in the system's OS kernel.

(d) **hostname**

The hostname is (usually) the value returned by `gethostname(2)`. It may be a fully qualified name (contains the domain).

(e) **sysname**

A unique name that describes the machine architecture and OS type.

4. REQUIREMENTS

This change will not affect the existing security model of the DFS Gateway. It will require the revision of the DFSGW login protocol. DCE 1.1 `dfs_login` clients will interoperate with a new `dfsgwd`, however the `@sys` and `@host` values will be defaulted. The new `dfs_login` will interoperate with a DCE 1.1 `dfsgwd`, but the old protocol will be used. This will result in no `@sys` and `@host` assignment.

5. FUNCTIONAL DEFINITION

The components affected by adding this functionality are the DFS Gateway and the DFS cache-manager.

5.1. Constructing a Sysname

The default `@sys` value will be built into the `dfs_login` program for each system port that is done. For systems that support `uname(2)`, it will be used to provide the sysname. The sysname is in the form of *machine-class_os-release*:

(a) The *machine-class* is a constant (e.g., `sun4`), based on the machine's CPU type. On systems that support `uname(2)`, it can be derived from the `utsname.machine` value. Machine model details should not be used unless they are significant to identify a machine for running a class of executable files for that machine type. For example if `utsname.machine` contains `hp725`, the only relevant part would be `hp700`.

(b) The *os-release* is made from the mnemonic name of the OS (e.g., `ux`) and the OS release number. When using `uname(2)`, it can be derived from the `utsname.release` value. Any leading zeros should be removed.

If there are current definitions in DFS, then they should be used instead of this algorithm for consistency.

Here are some *examples* of `@sys` names:

(a) `i386_msdos`

(b) `i386_winnt35`

(c) `mac68k_macos7`

(d) `hp700_ux905`

NOTE: There should be a sysname registry.

5.2. dfs_login Changes

The `dfs_login` command will be modified to specify a sysname corresponding to the machine that it is running from. It will use the `uname` method (as described in the previous section) if available on the machine's operating system. Otherwise an alternative mechanism should be used, such as a compile-time default.

The sysname can be overriden from the default value through the use of an environment variable `DFS_SYSNAME`, or the command option `-S`. The command option will take precedence.

The auth protocol version number will be changed to 2. If the `dfsgwd` that the `dfs_login`/`dfs_logout` is trying to talk to doesn't support the new protocol, a fallback to the version 1 protocol will occur.

5.3. dfsgwd Changes

The `dfsgwd` server will be changed to handle the new protocol. It will also handle old protocol clients, but it will use a default sysname.

These new options will be added:

(a) `-sysname` *name*

(b) `-nodomains`

The default sysname will be that of the system that is running this instance of the `dfsgwd`. This can be overridden by starting `dfsgwd` with the `-sysname` *name* argument.

The hostname will be determined by the `dfsgwd` by doing a `gethostbyaddr(3)` on the source IP address in the protocol packet of the request. The `-nodomains` options can be used to prune the domain part from the hostname.

5.4. dfsgw Changes

The `dfsgw` command will be changed to allow manipulation of the sysname and hostname fields in the auth database.

These new command options will be added to the `add` command:

(a) `-sysname` *name*

(b) `-remotehost` *name*

The `dfsgw` command will default the remote host option to that of the networkid specified in the `-id` option. If the networkid is specified in dot-notation, the address will be resolved to a hostname before being used for the remotehost name.

The default for the sysname will be to pass a zero length string in the syscall to perform the add operation. The `at_add` syscall will use the default sysname for the DFS gateway machine in this case.

In addition, the `list` command will be modified to display any `@sys` and `@host` values for each mapping.

5.5. DFS Cache-Manager Changes

The changes to the DFS cache manager require that the `cm_lookup()` operation be changed to query the AT database when either a `@sys` or `@host` component is encountered. If the request is via the DFS Gateway and a mapping is found for the caller's PAG, the appropriate translation is returned. If no mapping is found, then the machine's default (acting as the DFS GW) mappings are used.

6. PROTOCOL CHANGES

Version 2 of the auth request will be:

```
u_char  DFSGW_PROTOCOL_VERSION = 2
u_char  DFSGW_AUTH_PACKET = (1 << 1)
unsigned  :0            /* pad to long boundary */
u_long  dce_username_len
char    dce_username<dce_username_len>
unsigned  :0            /* pad to long boundary */
u_long  networkAddrLen
char    networkAddr<networkAddrLen>
unsigned  :0            /* pad to long boundary */
u_long  unix_uid
unsigned  :0            /* pad to long boundary */
u_long  sysname_len
char    sysname<sysname_len>
unsigned  :0            /* pad to long boundary */
```

7. DATA STRUCTURES

The auth database structure defining the PAG mappings will be modified to include the client sysname and hostname.

```
/*
 * Mapping table entry, used in most AT syscalls.
 */
typedef struct {
        struct sockaddr addr;
        uid_t uid;
        unsigned long pag;
        time_t expiration_time;
        char sysname[CM_MAXSYSNAME];
        char hostname[MAXHOSTNAMELEN];
} at_pag_mapping_t;
```

NOTE: A zero-length string in either the sysname or hostname will mean to use the default for that value.

8. API'S

The AFS_SYSCALL's for `AT_ADD` and `AT_LIST` for the DFS Gateway will now accept the expanded parameter list including the sysname and hostname.

9. REMOTE INTERFACES

There are no changes to remote interfaces.

10. COMPATIBILITY

The old and new versions of the DFS Gateway components will interoperate, but the new functionality will not be present. This is accomplished by using the protocol version. Clients will attempt to use the new version; if the server doesn't support this version an error will be returned. This will cause the client to use the old version of the protocol. The new server will support both the version 1 and (new) version 2 protocols.

If the `dfsgw` server is presented with a request from a client whose protocol version it doesn't support, it will reply with an error code of `DFSGW_REPLY_ERROR_BAD_VERSION` (= 2).

11. STANDARDS

These standards are applicable to this work:

(a) IETF RFC-1510, ''The Kerberos Network Authentication Service (V5)''.

REFERENCES

[MiSo] T. Mistretta, W. Sommerfeld, ''Remote Kerberos Authentication for Distributed File Systems; As Applied to a DCE DFS-to-NFS File System Translator''. [Contact J. Brezak for copies.]

AUTHOR'S ADDRESS

John Brezak
Hewlett-Packard Company
300 Apollo Drive
Chelmsford, MA 01824
USA

Internet email: brezak@apollo.hp.com
Telephone: 1-508-436-4915