OpenVMS Technical Journal V12

Access Restrictions in FTP

Ananth Shenoy

Currently, FTP service (provided by TCP/IP services for OpenVMS) does not provide a method to restrict access of user operations to a directory or set of directories. This has been inconvenient for system administrators and is risky for the system.

An FTP client (non-anonymous) who logs in can read all world-readable files, delete all world-deletable files, etc. A client's operation cannot be restricted to the login directory or a set of pre-defined directories. System administrators can use ACLs (access control lists) to restrict FTP user access, but ACL setup can be a difficult process. Also, ACL-based access restriction can be quite slow and can reduce the performance of other applications on the system. There have been other options to achieve the same goal, such as the use of the concealed logical, but those methods are even more cumbersome.

Keeping all these pain points in mind, a simple method of restricting user access to a particular set of directories was developed and implemented in TCP/IP v5.6 ECO3 and above.

FTP Anonymous Light

FTP Anonymous Light is a simple method for restricting user access to a particular set of directories. A system administrator who wants to restrict an OpenVMS user's FTP access to a particular set of directories should set TCPIP$FTP_ANONYMOUS_LIGHT for that user. Setting this parameter restricts the FTP operations of that user to a particular set of directories pointed to by TCPIP$FTP_ANONYMOUS_DIRECTORIES. For any particular target user, TCPIP$FTP_ANONYMOUS_LIGHT can be defined in LOGIN.COM. If FTP access must be restricted for all users, the parameter can be defined system-wide. FTP Anonymous Light users have to specify the correct password in order to log in. By contrast, when truly anonymous users are prompted to send their identity, any password is accepted.

The system administrator can also optionally set TCPIP$FTP_ANONYMOUS_WELCOME, and a message will be displayed upon successful login.

This example shows how FTP Anonymous Light works:

```
"TCPIP$FTP_ANONYMOUS_DIRECTORY" = "TCPIP$ENETINFO1:[UCX]"
    = "TCPIP$ENETINFO1:[UCX_AXP]"
    = "TCPIP$ECO:"
    = "TCPIP$PATCH:"
    = "COMMON_SYSDISK:[FAL$SERVER]"
    = "TCPIP$INTERNAL:"
"TCPIP$FTP_ANONYMOUS_LIGHT" = "1"
"TCPIP$FTP_ANONYMOUS_LOG" = "SYS$LOGIN:TCPIP$FTP_ANONYMOUS.LOG"
"TCPIP$FTP_ANONYMOUS_WELCOME" = "FTP Anonymous Light demo"
```

Commentary is marked in bold.

```
ftp plane.tcpip.zko.hp.com
220 plane.tcpip.zko.hp.com FTP Server (Version 5.6) Ready.
Connected to plane.zko.hp.com.
Name (plane.zko.hp.com:shenoy):
331 Username shenoy requires a Password
Password:
230-FTP Anonymous Light demo
230 Guest login OK, access restrictions apply.
FTP> cd sys$system
550 insufficient privilege or file protection violation
```

>>> This directory not in TCPIP$FTP_ANONYMOUS_DIRECTORY, hence access is restricted

```
FTP> cd tcpip$eco
250-CWD command successful.
250 New default directory is TCPIP$ENETINFO1:[TCPIP$ENGINEERING_CHANGE_ORDERS]
```

>>> This directory is present in TCPIP$FTP_ANONYMOUS_DIRECTORY, hence access is allowed

```
FTP> cd sys$login
250-CWD command successful.
250 New default directory is WORK4$:[SHENOY]
FTP> bye
221 Goodbye.
```

A sample log file looks like this:

```
type SYS$LOGIN:TCPIP$FTP_ANONYMOUS.LOG
20-JUN-2008 05:21:45.64 Anonymous Light User:shenoy from Host:16.116.92.100
20-JUN-2008 05:22:39.61 Anonymous Light User:shenoy status:00010001 CWD
dir:TCPIP$ENETINFO1:[TCPIP$ENGINEERING_CHANGE_ORDERS]
20-JUN-2008 05:23:13.49 Anonymous Light User:shenoy status:00010001 CWD
dir:WORK4$:[SHENOY]
20-JUN-2008 05:23:19.15 Anonymous Light User:shenoy status:00000000 RETR
file:WORK4$:[SHENOY]A.TXT;30
20-JUN-2008 05:23:26.07 Anonymous Light User:shenoy logged out
```

Even if the system administrator does not specify it, SYS$LOGIN will always be added to TCPIP$FTP_ANONYMOUS_DIRECTORY. This means that Anonymous Light users will always have access to their SYS$LOGIN.

In some instances, the system administrator may not want a user to access his or her SYS$LOGIN. To set this up, the system administrator should define TCPIP$FTP_ANONYMOUS_NOSYSLOGIN for that particular user. This parameter is particularly useful when a user has changed their directory in LOGIN.COM and the system administrator does not want to allow access to SYS$LOGIN.

Access restrictions by FTP Operations

The FTP Anonymous Light feature restricts user access to a particular set of directories. To further increase the system administrator's flexibility, a new set of parameters can be defined to restrict user operations.

The FTP server will check for the existence of four parameters. If each is defined, the FTP server will reject all:

TCPIP$FTPD_NOLIST - LIST and NLST commands

TCPIP$FTPD_NOREAD - RETR commands

TCPIP$FTPD_NOWRITE - STOR, STOU, APPE, RNFR, RNTO, DELE, MKD, and RMD commands

TCPIP$FTPD_NODELETE - DELE and RMD commands

These new access restrictions will apply in addition to any restrictions implied by the protections of the underlying files, directories, volumes, and devices.

If TCPIP$FTPD_NOLIST is defined, the use of wildcards will not be allowed in FTP operations. This is necessary in order to prevent FTP users from obtaining a list of the files in the directory simply by attempting to retrieve or delete all the files.

Below is a table of FTP client commands and the parameters used to control their operation:

Client command	**FTP Logical**
directory	TCPIP$FTPD_NOLIST
view	TCPIP$FTPD_NOREAD
put	TCPIP$FTPD_NOWRITE
get	TCPIP$FTPD_NOREAD
append	TCPIP$FTPD_NOWRITE
rename	TCPIP$FTPD_NOWRITE
create	TCPIP$FTPD_NOWRITE
delete	TCPIP$FTPD_NOWRITE, TCPIP$FTPD_NODELETE

So, for example, if a system administrator does not want a user to be able to delete files through FTP, TCPIP$FTPD_NODELETE can be set for that user.

This is a simple illustration of the usage of the above parameters:

```
 "TCPIP$FTPD_NODELETE" = "1"
 "TCPIP$FTPD_NOLIST" = "1"

$ ftp plane.tcpip.zko.hp.com
220 plane.tcpip.zko.hp.com FTP Server (Version 5.6) Ready.
Connected to plane.zko.hp.com.
Name (plane.zko.hp.com:shenoy): shenoy
331 Username shenoy requires a Password
Password:
230-FTP Anonymous Light demo
230 Guest login OK, access restrictions apply.
FTP> dir *
200 PORT command successful.
550 Cannot execute LIST command, Access denied.
```

>>> Here dir command is not allowed, because of wildcard present in command and TCPIP$FTPD_NOLIST is defined

```
%TCPIP-E-FTP_NOSUCHFILE, no such file *
FTP> del a.txt
550 Cannot execute DEL command, Access denied.
```

>>> Here del command is not allowed, because of logical TCPIP$FTPD_NODELETE is set

```
FTP> bye
221 Goodbye.
```

These parameters can be used in conjunction with FTP Anonymous Light to restrict user access via FTP, helping to mitigate a risk to the system that has been problematic for system administrators.