eFT263I

NetEx/eFT™ for OpenVMS on HP Integrity Systems

Release 4.0

Memo To Users

March 31, 2009

6420 Sycamore Lane N #300
Maple Grove, MN 55369

Introduction

This product implements the Network Executive Software eFT263I OpenVMS Integrity software. This product has been tested on OpenVMS Integrity V8.3. For additional prerequisites refer to the Installation section.

Refer to the Update Summary for a list of new additions and fixes provided with this release. Refer also to Documentation Updates for previously undocumented features.

New Features

This is the initial release of this product on the HP Integrity platform.

Previous Release

This is the initial release of this product on the HP Integrity platform.

Service Notes

The following are known problems and/or limitations with this release of OpenVMS Integrity eFT:

- Multiple consecutive failures to login (e.g. 5 in a row) through the Service Initiator (via the "CONNECT" command) will cause a temporary security lockout of all subsequent login attempts made through the Service Initiator for all users.
- Execution of LOCAL or REMOTE commands returning character records exceeding 1024 characters in length can result in an error specifying that the output mailbox is too small for the request. This is working as designed.
- It is typical for users to have commands in their login command files that set up terminal characteristics for interactive logins. Since eFT logins come in as interactive, these commands (such as SET TERM/LOWER,...) are usually executed. The problem is eFT logins are made from a mailbox, not a terminal device. Commands such as SET TERM tend to generate warnings complaining about the device being a mailbox. Users can get around this warning condition by modifying their command procedures to make sure the login device is a terminal prior to executing the SET TERM type commands. The following is an example of this:

  ```
  if f$mode() .eqs. "INTERACTIVE" .and. -
     f$getdvi("sys$output","trm") then -
        $ SET TERM/LOWER/INQUIRE
  ```

  Doing this will eliminate needless warning messages generated during an eFT login.

- Multiple versions of eFT may be installed and run on a single system at the same time. This may be necessary for version testing or to support multiple protocols. The following steps will help in setting up multiple versions:

  Specify different installation directories for the different versions during the install procedure. For example, if you use SYS$SYSDEVICE:[NSC.SICOM] (the default) for one version of eFT, you must specify a different directory when installing the second version.

  The OpenVMS symbols USER, UASERVER, and EFT are defined in the DCL script SYLOGIN.COM in the base directory specified during the install procedure (SYS$SYSDEVICE:[NSC.SICOM], by default). Rerunning the SYLOGIN.COM from the appropriate area will redefine the symbols to use the eFT version installed in that area. An alternative is to use different symbols for the different versions by editing the SYLOGIN.COM of one version and replacing the symbols with alternate symbols. If, for example, a default version of eFT is installed in SYS$SYSDEVICE:[NSC.SICOM] and a test version is installed in SYS$SYSDEVICE:[NSC.SICOM1], you may want to modify the symbol definitions in SYS$SYSDEVICE:[NSC.SICOM1]SYLOGIN.COM as such:

  ```
  $ USER1 :== @'USERDIR'user.com
  $ UASERVER1 :== @'USERDIR'uaserver.com
  ```

  Then by executing the SYLOGIN.COM in both directories, you may use both versions of eFT at the same time. For example, the symbol USER will invoke the eFT client from the default version, while the symbol USER1 will invoke the eFT client from the test version.

  If multiple service initiators are running using the same protocol, they must offer different services. If the same service is being offered by multiple service initiators using the same transport protocol, errors or unpredictable results will occur.

- For this release of eFT263i the user will not be able to use the FTP aliases. These will be added in a subsequent release.

- If the user wishes to change the connect blocksize below 2048 the following error will occur during the connection attempt.

```
Set connect blocksize 2047

Connect <remote host><userid><user password>

BLOCKSIZE of 2047 is out of range (2048-32768) (UA-4102)
```

Installation Notes

Prerequisites

The following are prerequisites for installing eFT263I

- OpenVMS Integrity V8.3 or later.
- The privileges to create directories, load files from magnetic tape, write files in the SYS$LOADABLE_IMAGES directory, edit system startup and system login files, define logical names in the system logical name table, and install executable images using the OpenVMS INSTALL utility. In addition, you must have at least the following privileges to run the Service Initiator: DETACH, EXQUOTA, TMPMBX, WORLD, GROUP, and GRPNAM.
- This product only supports the NetEx/IP as the transport (i.e. TCP/IP is not supported); H267IPI must be installed prior to installing eFT263I

INSTALLATION PROCEDURE

Initial installation and verification of eFT consists of the following steps:

1. Create the distribution directory
2. Load the distribution
3. Install the distribution
4. Start the Service Initiator
5. Verify eFT
6. Make eFT available to other users
7. Automatically starting the Service Initiator

Step 1. Create the Distribution Directory

The eFT release is loaded into a DISTRIBUTION directory and is then installed into a TARGET directory. Existing files in the TARGET directory are replaced with the new release files. Any user-modified control files are automatically preserved. This version of eFT requires no more than 6000 blocks of disk space.

Nothing is modified in the DISTRIBUTION directory during the installation process allowing repeated installations into different TARGET directories, each with different install options. To preserve disk space the DISTRIBUTION directory can be deleted once eFT is fully installed into the TARGET directory.

The installation procedures and examples assume a TARGET directory of [NSC.SICOM] on SYS$SYSDEVICE. However, any valid disk/directory with adequate space can be selected. At this point, you should create your DISTRIBUTION directory:

```
$ CREATE/DIRECTORY eFT_DIR
$ SET DEFAULT eFT_DIR
```

Step 2. Load the Distribution

Distribution media is CD-ROM

1. Logon to a system privileged account.
2. Save any previous configuration files.
3. Create or identify a directory on the OpenVMS system where the installation data set may be loaded into.

   ```
   XXX:[YYY] (ex:eFT_DIR)
   ```

4. The CD is not in VMS format so it must be loaded onto a PC and the data set (eFT263I) should be transferred via FTP from the PC to the selected directory on the OpenVMS system.
5. Once the data set is loaded into the host directory, its file attributes must be modified. Use the following command to change the attributes of the data set.

   ```
   SET FILE/ATTR=(RFM=FIX,LRL=32256) EFT263I.BCK
   ```

6. Run OpenVMS Backup Utility to extract the distribution:

   ```
   $ BACKUP/LOG/NEW_VERSION EFT263I.BCK/SAVE XXX:[YYY]
   ```

Step 3. Install the Distribution

The installation will copy files from the DISTRIBUTION directory to the TARGET directory. Any control files with differences are suffixed with the string "_SAVE." For example, if the file 'SCLIENT.UA' has changed since the previous release, the older version is copied to the file 'SCLIENT.UA_SAVE.'

Change your default directory to XXX:[YYY] and invoke the installation procedure. The installation procedure prompts for the TARGET directory for this release. Below are the commands to install eFT and an example of the installation prompts.

```
$ SET DEFAULT XXX:[YYY]
$ @INSTALL

The installation options are:

  ALL         - full NETEX-eFT install
  DRIVER      - assemble and link NETEX-eFT CA driver
  CLIENT      - install NETEX-eFT client
  SERVER      - install NETEX-eFT server
  ENCRYPT     - install NETEX-eFT encryption utility
  SVCINIT     - install NETEX-eFT Service Initiator
  CONTROL     - install NETEX-eFT Control Utility

Hit RETURN for the default option 'ALL'.

Enter the desired install OPTION: all


Enter the TARGET USER-Access root directory.

Hit RETURN for the default target 'SYS$SYSDEVICE: [NSC.SICOM]'.

Enter the desired TARGET: ___________
```

Step 4. Start the Service Initiator

The Service Initiator is a program that services eFT CONNECT or LOGIN requests from hosts on the network. It runs as a detached process under the name SVCINIT. Before proceeding, make certain that you have all of the privileges listed in "Prerequisites" at the beginning of this document. Also make sure that a previous copy of the Service Initiator is not running. This can be verified by issuing a SHOW SYSTEM command and looking for a process by the name of SVCINIT. If one appears, stop it using STOP/ID=xxx, where xxx is the process id of the SVCINIT process.

To startup a new Service Initiator, issue the following command (remember to replace the directory name below with the directory name you used during the installation):

```
$ @SYS$SYSDEVICE:[NSC.SICOM]STARTUP SI
```

Within a few seconds you should see a VMS message indicating the process successfully started. It should appear similar to:

```
%RUN-S-PROC_ID, identification of created process is 00024B
```

To further verify the Service Initiator is running, type:

```
$ SHOW SYSTEM
```

You should see a process name of SVCINIT in the table. If not, check to make sure the protection on the SICOM root directory and SI subdirectory allow you to have read/write access. Also check the log and input files for errors.

Step 5. Verify eFT

A simple verification command procedure has been supplied as part of the eFT release. This verification procedure prompts you for the local host name, and a valid username and password on this host (for verification purposes, the username and password specified should at least have the privileges you do - specify your username and password to be safe). It attempts to connect back to the host, login, and send and receive several files.

To invoke the verification procedure, type the following (remember to replace the directory name below with the directory name you used during the installation):

```
$ @SYS$SYSDEVICE:[NSC.SICOM.USER]VERIFY
```

You should have several messages printed to your terminal followed by a final "Verification Successful" message. If an error is encountered during the verification, the procedure will terminate and an error message will be printed.

Step 6. Make eFT available to other users

In order to make eFT easily available to other OpenVMS users, you will have to edit your site system login file. To find out the exact name of this file, type:

```
$ SHOW LOG SYS$SYLOGIN
```

You will find a site login file name similar to SYS$MANAGER:SYLOGIN.COM. When you have found the login filename, edit the site login file and add the following lines (remember to replace the directory name below with the directory name you used during the installation):

```
$! Define eFT utilities
$!
$ @SYS$SYSDEVICE:[NSC.SICOM]SYLOGIN
```

Any user that will be using eFT also should have their VMS Page File Quota (PGFLQUO) set to at least 3000. This is needed in order to execute LOCAL and REMOTE commands.

Step 7. Automatically starting the Service Initiator

eFT logical names can be defined, and the Service Initiator can be started automatically at boot time by inserting several lines into your system startup file. At this time you should edit SYS$MANAGER:SYSTARTUP_VMS.COM and add the following lines somewhere after the NETEX startup procedure (depending on the network selected). (Remember to replace SYS$SYSDEVICE:[NSC.SICOM] below with your TARGET directory, as defined in Step 3):

To start the Service Initiator (this is recommended), add the line:

```
$ @SYS$SYSDEVICE:[NSC.SICOM] STARTUP SI
```

At system boot time, the Service Initiator will be started with the process name SVCINIT. Its messages will be logged to the file SYS$SYSDEVICE:[NSC.SICOM.SI)SVCINIT.LOG.

In order to verify your changes to the system startup files, you should reboot your system. This is not a requirement of eFT but strongly recommended to ensure eFT executables get properly installed and the Service Initiator gets started successfully when the system is booted.

This completes the formal installation of eFT on your local host. However, it is important to continue on through this document in order to set up your environment properly.

STOPPING THE SERVICE INITIATOR

The Service Initiator can be stopped by using the Service Initiator Control program SYS$SYSDEVICE:[NSC.SICOM.SI]CONTROL.EXE. First, create a symbol SICTL to reference CONTROL.EXE:

```
$ SICTL:==$SYS$SYSDEVICE:[NSC.SICOM.SI]CONTROL.EXE
```

Now, to stop the Service Initiator, enter:

```
$ SICTL STOP -H host -S service
```

where ‘host’ is the name of the local host and 'service' is the service name being offered by the Service Initiator ("USER" is generally the service name being offered). You need to stop the Service Initiator in order to examine the current log file SYS$SYSDEVICE:[NSC.SICOM.SI]SVCINIT.LOG.

PROVIDING A GUEST LOGIN

The Service Initiator provides for a default (or guest) login when no username or password is provided on the eFT CONNECT command. If you want a guest login for eFT, edit the file SYS$SYSDEVICE:[NSC.SICOM.SI]STARTUP.INP. Remove the comments (#) from the following lines:

```
USER SERVERRUN SYS$SYSDEVICE: [NSC.SICOM.USER]SERVER.EXE
# USERNAME guest
# PASSWORD secret
```

Change the username guest and the password secret to correspond to a valid username/password for your system. In doing so, this username/password account becomes an eFT guest account. Alternatively, add guest to your list of valid accounts (by running AUTHORIZE). The username and password you specify becomes the default if none are given on the CONNECT command.

The Service Initiator must be stopped and restarted for this change to take effect.

SERVICE INITIATOR KEYWORDS

The Service Initiator startup input file, SYS$SYSDEVICE:[NSC.SICOM.SI]STARTUP.INP, contains a list of keywords that can be set to alter the way the Service Initiator operates for a given SERVICE being offered. Below each keyword is listed along with a brief description of the value that can be assigned to it:

LOGTIMEOUT

Specifies the login timeout in seconds. This is used to terminate a login request that for some unknown reason, is hanging around.

MINIMUM

Specifies the minimum session number that will be offered for this service. For example, a MINIMUM value of 5 would result in SERVICE "USER" being offered as "eFT005" up to MAXIMUM (below).

MAXIMUM

Specifies the maximum session number that will be offered for this service. A value of 30 for example would result in the last offer of "USER" being "eFT030," before the offers started over at MINIMUM.

OPERATOR

Specifies a password that is required when issuing commands through the CONTROL program (SICTL used for shutting down the Service Initiator).

PASSWORD

Specifies an optional guest logon password.

SECONDARY

Specifies a secondary password if one is required for the guest logon id.

TRACE

Allows different levels of tracing of the Service Initiator. Refer to the startup file "SYS$SYSDEVICE:[NSC.SICOM.SI]STARTUP.INP" for a description of the different trace levels.

USERNAME

Specifies an optional guest logon userid.

VERBOSE

Specifies whether the LOGON output is displayed back to the connecting user. The LOGON output is the normal banner information that displays when a user logs onto this OpenVMS system.

REINSTALLING eFT

At any time the eFT distribution can be reinstalled into the current TARGET root directory. The distribution contents are required to re-link an executable image. The installation can be run as described in the previous section, INSTALLATION. For example, if the current distribution is located in the directory SYS$SYSDEVICE:[eFT_DIR], the installation script can be run with the following commands, selecting the current TARGET directory as the TARGET:

```
$ SET DEFAULT [eFT_DIR}
$ @INSTALL
```

Update Summary

This is the initial release of this product on the HP Integrity platform.