SOFTWARE DIVERSIFIED SERVICES sds

1322 - 81st Ave. NE
Spring Lake Park, MN 55432-2116
Phone: 763.571.9000
Fax: 763-572.1721
www.sdsusa.com

2011

RACF and VFTP: Secure FTP Like Other Resources

VitalSigns for FTP, from Software Diversified Services, Collaborates with RACF

Here is a description of the inherent issues with standard RACF rules as they pertain to FTP and how VFTP from SDS provides additional security while working hand and hand with RACF.

FTP with traditional RACF dataset protection allows data that was once resident on the mainframe to be transferred off and easily distributed anywhere in the world. And FTP allows a whole new class of users to access the mainframe. FTP creates a totally new dimension for malicious behavior to those entities where read authority is granted.

Traditional RACF rules such as dataset access are used to determine if a user can 'read' a dataset. These rules date from days when access to mainframe datasets was controlled by the application (such as CICS) or was limited to a relatively small group of trusted TSO users. But with the advent of FTP on the mainframe, if the user can read the file; they can copy it to their PC. The original intention of 'read' access with RACF was to allow access to pieces of information related to the transaction at hand. It does not take into consideration that the 'read' access now will allow an FTP session to offload the whole file to be used for anything the user wishes, such as emailing it anywhere in the world with ease, or simply writing it to a flash drive and walking home with it. Although there is some protection using RACF, it falls short of what is needed when FTP is added to the mix.

Another concern is that FTP can be used to do many things beyond transferring data. Using a standard FTP session, a hacker can 'snoop' around the system, looking for information that might not be appropriate for everyone's consumption. An example of this might be a user logs on to FTP, does a "cd" (change directory) to /u (the directory that often houses user's workspaces) and lists the contents including several userIDs (directory names associated with the user). Traditional mainframe users include a small number of "trusted" (and audited) TSO users and folks like CICS and IMS users, whose activities are controlled and limited by the applications. With FTP, almost anyone with a user ID can get on the mainframe, snoop around, and retrieve files that would be better left on the mainframe. Although there are some basic protection mechanisms in place with RACF, they don't stand up to what is needed for a true enterprise-class secure protocol.

The SITE command also allows for many dangerous commands. An example of this would be the FILETYPE=JES command. Once the FTP client issues this command, jobs can be submitted to the JES queue and reports could be pulled from the queue. The SITE

command also allows for many dangerous operations. For example, with the FILETYPE=JES, an FTP client can submit jobs to, and pull reports from, the JES queue. SITE can also be used to change permission bits for a file, or to list detailed information about your storage devices.

For all of these reasons, FTP functions need to be treated as protectable resources, just like datasets.

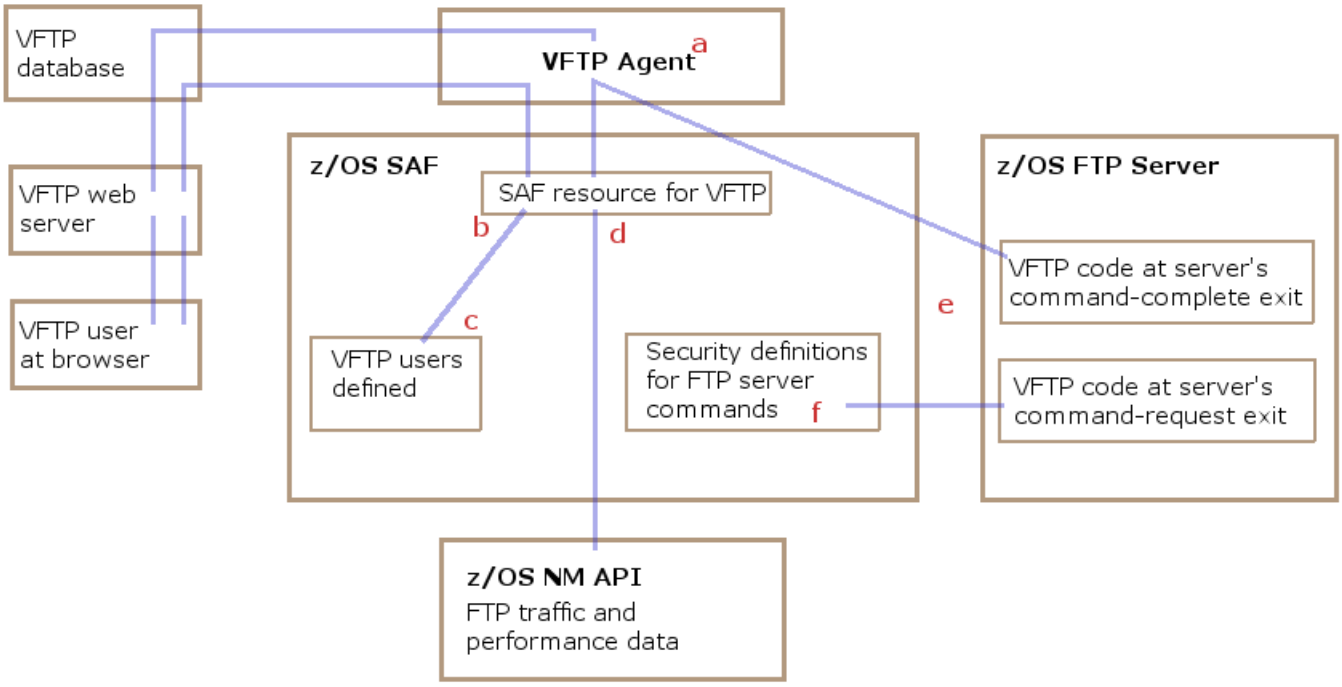
An emerging technique to enable the FTP technology while still maintaining secure control is to use software, such as VFTP, that wraps the FTP functionality into a protective shell.

VFTP can extend the SAF, or RACF, security facilities to include FTP functions. And further, VFTP can provide the management and audit reporting at all levels to provide the oversight necessary for data security. VFTP allows the security administrator to add rules to RACF to protect these resources. Access can be as global or as granular as the administrator deems appropriate.

In addition to what VFTP does to extend traditional RACF rules for FTP sessions, VFTP takes advantage of RACF for authentication to our user interface. The same userid and password used for accessing applications such as TSO or CICS on the mainframe can be used to access our browser interface. The security administrator can decide who should access the monitoring/auditing tool, and determine the role they can play. Through the use of RACF resources defined for VFTP access, a user might be limited to viewing only transfers related to their userid. The help desk or system programmer might need global access to be able to help identify problems end-users are having. Finally, users that can administer how VFTP is to work can be defined, all using RACF as the conduit.

Here is a diagram depicting the VFTP, FTP and RACF installation/implementation. (Please see next page.)

VFTP, FTP, & z/OS Security



VFTP installation involves 6 tasks in SAF
a. Configure the Security Class for VFTP
b. Permit VFTP Agents to Validate VFTP Web Users
c. Permit Users to Access VFTP
d. Permit VFTP to Read the NM API
e. Define FTP Server Exits to SAF
f. Configure VFTP Security for z/OS FTP Server

VFTP Agents validate VFTP user IDs by passing them to z/OS SAF security, RACF and returning the reply to the VFTP Database.

VFTP Agents help secure VFTP servers on z/OS by working with server program exits to verify server-users' FTP commands against RACF security.

Installing a VFTP Agent includes installing a VFTP FTP Client. The VFTP Client provides a wrapper for the z/OS FTP client. That allows VFTP to configure and monitor the z/OS client.

Here are some examples of how VFTP using security definitions managed by RACF.

- Prevent user1 from logging onto the FTP server.
- Prevent users from submitting jobs through the FTP server.
- Prevent user2 from changing out of his home directory.
- Prevent users from listing the contents of SYS1.MACLIB.
- Prevent users from requesting automount of file systems.
- Prevent users from using FTP to list volume information.
- Prevent users from retrieving the contents of sys1 datasets and/or make an exception for user sysprg1.