SafeNet/i

IBM QRadar® SIEM and QRadar Log Manager.

Table of Contents

Function Overview

SafeNet/i is introducing new features in this product update.

1. Integration with **IBM** QRadar SIEM and QRadar Log Manager.
   Administrators can now configure SafeNet/i to integrate with IBM's QRADAR family of products
   SafeNet/i can send alerts via the required LEFF compliant log file format and store that log file in the system
   IFS for FTP pickup and processing by the QRADAR Network Anomoly Detection Monitor software.

Prerequisites

1. SafeNet/i minimum of V10.11 installed. See our support website for PTF level required. (PTF10.11)
2. Alert Notifications must be configured and active in SafeNet/i.
3. IBM's QRADAR software must be installed on a separate system.

Integration Process Overview

Listed below are the general setup steps for integration with Qradar.

You must have a SafeNet/i minimum PTF Version 10.11 for this function to operate.

1. On the IBM i, create an IFS Directory to hold the SafeNet/i Qradar alert files.
    Example: /SafeNet/Qradar

2. Setup an IBMi User Profile that QRADAR will use to pick up the alert files by FTP or SFTP.
   Example: QRADARUSER

3. Setup the same user in SafeNet/i, allowing FTP access to the directory created above.
     a. User must have authority to the FTPLogon and FTPServer points
     b. User must have authority to LIST and GET FTP Sub commands.
     c. User must have READ authority to the IFS Path created for the QRADAR alert files.

4. Using the SafeNet/i CHGRDRSET command, verify or enter the following:
     a. Enter a Host name or identifier for this IBM i. This is for QRADAR identification.
     b. Path to directory created above. Must be in the format of '/path1/path2/'

5. Setup Alert Notifications in SafeNet/i with the CHGNOTIFY command. You must use Summarized Alerts.

6. Configure the QRADAR software for your SafeNet/i system as a Log Source.:
     a. Define a log source for this IBM i. (see details below)
     b. Test alert generation and file pickup by Qradar

7. The alert files created in the IFS directory will be named "SN_QRAD_xxxx.txt" where xxxx = a number

CHGRDRSET Command Example

```
                     QRADAR Integration Settings (CHGRDRSET)

 Type choices, press Enter.

 Activate QRADAR Integration? . .    *YES           *YES, *NO
 This Host Identifier . . . . . .    IBMi.yourdomain.com
 IFS Path to QRADAR Alert Files      '/SafeNet/QRadar/'
 _____


                                                                 Bottom
 F3=Exit    F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

Notes:

1. The IFS Path must exist prior to entering it in this command.
2. The Host Name entered here is only for Documentation/Identification of this host to the QRADAR log activity.
3. You must have Alert Notification active in SafeNet/i for QRADAR alerts to be generated.

FTP User Setup Example for QRadar®

The FTP User from QRADAR must have at a minimum LIST and GET authority.

```
 FTPSETD                          SafeNet/i                              3/28/14
 MPA1                   Work With Authorized FTP Statements             15:00:21
                 User-> QRADARUSER QRADAR FTP USER


 Type option, press Enter.
      1=Select
                 Opt      FTP Operation        Associated FTP Command
                  _     Directory/Lib Create    MKDIR, XMKD
                  _     Directory/Lib Delete    RMD, XRMD
                  _     Set Current Dir         LCD,CWD,CDUP,XCWD
                  1     List Files              LIST, NLIST
                  _     File Deletion           DELE
                  1     Receiving Files         GET, MGET
                  _     Sending Of Files        PUT, APPEND, MPUT
                  _     Renaming Files          RNFR, RNTO
                  _     Execute CL Commands     Any CL - SYSCMD



                                                                        Bottom

 F2=Show Defined Users    F3=Exit     F4=Additional Settings   F7=Alt Profiles
 F9 = WRKUSRCMD                 F12 = Cancel         (c) Copyright 1997 MP Assoc.,Inc
```

Then, Press F4 for Additional Parameters

Note the Initial Name Format and Home Directory settings:

```
 FTPSET2D                         SafeNet/i                              3/28/14
                   Maintain Special FTP Settings for Users             15:02:25

  User->  QRADARUSER   QRADAR FTP USER

   Initial Name Format->    *PATH       (*LIB, *PATH)
   Initial List Format->    *UNIX       (*DFT, *UNIX)
   Initial Library----->    *USRPRF      Name, *USRPRF
   Encrypted FTP Connection-->  0 (0=Allowed,1=Not Allowed,2=Required)

   Initial Home Directory Path   Name of Path or *USRPRF
 /SafeNet/Qradar



 _____

   CCSID of Initial Path--->  00000  (0 - 65533) 0=Default




   F3 = Exit
   F12=Return                        HELP        (c) Copyright 2001 MP Assoc.,Inc
```

Finally, Use the WRKUSRPTH command and give the FTP user authority to the IFS path where the QRADAR alerts files will be placed.

```
 SND0100                          SafeNet/i                              3/28/14
 MPA1                        Maintain Path Names                        15:04:18
                   User-> QRADARUSER QRADAR FTP USER

Type option, press Enter.
  2=Edit,4=Delete

Opt. Path Names...                                             R W D O/M
  _    /SafeNet/Qradar/*                                       X _ _ _




                                                                        Bottom


 F2 = Show Defined SafeNet Users          F3 = Exit      F6 = Add
 F12 = Return  HELP                               (c) Copyright 1997 MP Assoc.,Inc
```

Setting Up a Log Source in QRadar®.

1. From the main menu of QRadar, select ADMIN, then LOG SOURCES
2. Click on "Add" top add a new log source.
3. Define the IBM i as a log source in Qradar as follows

Log Source Parameter Values:

Log Source Type	IBM AS/400 iSeries ←Must Be Selected
Protocol Configuration	LOG FILE ←Must Be Selected
Service Type	FTP ←Must Select FTP or SFTP
Remote IP or Hostname	IBMiHostIP ←Enter the ACTUAL IP or Host name of IBM i
Remote Port	21 ←For FTP use 21.
Remote User	IBMiUser ←Use the ID you created on the IBMi
Remote Directory	(leaveblank) ←No need to enter if setup in SafeNet/i correctly.
FTP File Pattern	.* ← Use .* for all files to be picked up (a dot and asterisk)
FTP Transfer Mode	Binary ←Must Be BINARY
Recurrence	15M ←15 minutes minimum allowed (customer choice)
Processor	NONE ←Must be NONE
Event Generator	LINEBYLINE ←Must be LINEBYLINE
File Encoding	US-ASCII ←Must be US-ASCII

QRadar Log Manage ×

← → C ⌂ ⓧ https://184.75.122.50/console/qradar/jsp/QRadar.jsp

Apps ☐ New Tab ☐ Imported From IE 🔖 SafeNet/i Web... ☐ Think400.dk - iS... 🔢 Getting Started ...

IBM Security QRadar SIEM

admin ▾   Preferences ▾   Help ▾   Messages ▮▾   IBM.

Dashboard   Log Activity   Reports   Admin

System Time: 9:18 AM

Admin

▶ System Configuration

▶ Data Sources

Log Sources - Google Chrome

ⓧ https://184.75.122.50/console/do/sem/maintainSensorDevice?dispatch=edit&appName=eventviewer&pageId=SensorDeviceList&hasSearched=false&id=70&columnSorting=true

Edit a log source

Field	Value
Log Source Name	SafeNet-i
Log Source Description	SafeNet-i
Log Source Type	IBM AS/400 iSeries
Protocol Configuration	Log File ▾
Log Source Identifier	MPA1
Service Type	FTP ▾
Remote IP or Hostname	www.mpawest.net
Remote Port	21
Remote User	IBM2
Remote Password	••••••••••••••••••••
Confirm Password	••••••••••••••••••••
Remote Directory	
Recursive	☐
FTP File Pattern	*
FTP Transfer Mode	BINARY ▾
Start Time	12:00 AM ▾
Recurrence	15M
Run On Save	☑
EPS Throttle	100
Processor	NONE ▾
Ignore Previously Processed File(s)	☑
Change Local Directory?	☐
Event Generator	LINEBYLINE ▾
File Encoding	US-ASCII ▾
Folder Separator	/
Enabled	☑
Credibility	5 ▾
Target Event Collector	eventcollector0 :: mpa-qradar ▾
Coalescing Events	☑
Store Event Payload	☑

Please select any groups you would like this log source to be a member of:

Save   Cancel

Ⓠ Radar

Testing the Initial Configuration

SafeNet/i Verification:

After the initial setup in SafeNet/i, perform the following to verify proper Setup.

1. Make sure the FTP user can connect and logon, then is able to LIST and GET files from the directory.
2. Make sure Alert Notifications are active in SafeNet/i (See CHGNOTIFY)
3. Manually cause an alert to be generated by SafeNet/i.
    a. Using FTP, connect to the IBMi and enter an invalid user id. That will cause a rejection.
4. After the normal Alert wait interval (see CHGNOTIFY), check for the SN_QRAD_xxxx.txt file in the IFS directory.
5. If the file is NOT found, re-check the configuration and the joblog for the ALERTWATCH job.

This finishes the verification of SafeNet/i alert processing.

QRADAR should be verified next,

1. Define the Log source in the QRADAR application.
2. Activate the Log Source.
3. Check Status of Log Source in QRadar.
4. Check the SafeNet/i transaction file for FTP entries from the QRADAR system. You can select records based on the User Id assigned to the Qradar install. This will allow you to verify if QRadar successfully retrieved the alert files from the IBMi IFS.

Additional References

See the SafeNet/i Reference guide at www.safeneti.com

See QRADAR software guides at www.ibm.com