Systems
Lab Services and Training

SECURITY

Security and Compliance Tools for IBM i
Syslog Reporting Manager V2.1

User's Guide

Thomas Barlen
Terry Ford

Version 2021.11.16

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

© Copyright 2018, 2021 IBM Corporation
Licensed Materials - Property of IBM
Private and Confidential - For IBM and customer use only

Syslog Reporting Manager

Table of Contents

1 Introduction....4
2 What's new in V2.1 (6th November 2021)....9
3 Implementation and use....11
3.1 Prerequisites....11
3.2 Authorities required to Install the Tool....11
3.2.1 Authorities required to Run the Tool....11
3.3 Installation....12
3.4 Upgrade information related to V2R1M0 from a previous version....13
2.1 Migration overview....13
2.2 Performing the migration....14
3.5 Granting access to the Syslog Reporting Manager....15
3.5.1 Granting management access to the Journal Extract Tool....15
3.6 Registering the *license key*....15
3.7 Basic setup of the Syslog Reporting Manager tool....19
3.8 Defining the audit journal monitor environment....21
3.9 Defining the IFS stream file change monitor environment....22
3.10 Defining the QHST history log event monitor environment....26
3.11 Sending database change events via Journal Extract Tool integration....30
3.11.1 Preparation....30
3.11.2 Integration overview....30
3.11.3 Configuring the Journal Extract Tool integration....32
3.12 Sending message queue events....44
3.12.1 Configure the global message queue monitoring settings....45
3.12.2 Defining message queues to be monitored....46
3.12.3 Starting the message queue monitor....47
3.12.4 Ending the message queue monitor....47
3.13 Sending custom events....48
3.13.1 Sending custom events with the SNDEVT commands....51
3.13.2 Sending custom events with ILE procedures....53
3.14 Starting and ending the Syslog Reporting Manager....55
3.15 Autostarting the Syslog Reporting Manager at IPL....55
3.16 Exporting and importing configuration settings....56
3.16.1 Exporting the configuration....56
3.16.2 Importing the configuration....58
4 Managing the job environment....61
4.1 Manually starting and stopping event monitor jobs....62
5 Special function settings....63
6 CEF and LEEF key mapping information....64
7 Transport Layer Security (TLS) implementation information....69

7.1 Prerequisites....69
7.2 Enabling TLS encrypted communication....70
7.3 Digital Certificate Manager integration....71
8 Additional information....73
8.1 Working with event statistics....73
8.2 User-type audit journal entries....74
8.3 Deleting the Syslog Reporting Manager....75
9 Change History....76
9.1 Version 1.0 dated May 18th, 2018....76
9.2 Version 1.1 dated August 8th, 2018....76
9.3 Version 1.2 dated May 24th, 2019....76
9.4 Version 1.3 dated Jan. 25th, 2020....77
9.5 Version 1.4 dated Sep. 30th, 2020....80
10 Audit journal entry type support....83
11 IBM Systems Lab Services and Training Security....87

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

1 Introduction

IBM i provides extensive logging and auditing capabilities. System events or file events are typically captured in journals, such as the QAUDJRN system journal. Native IBM i commands exist to analyze collected events.

In recent years more and more companies implement central logging services to collect mostly security related events on a central server. These central servers typically host Security Information and Event Management (SIEM) systems, such as QRADAR, to store events from many systems in an enterprise, analyze the data, and react on monitored events.

A DB2 table function has been introduced in 2017 to query the system audit journal and format entries according to RFC3164 or RFC5424 compliant syslog messages with a payload formatted in the Common Event Format (CEF) as supported by commonly used SIEM solutions. However, audit journal entries are just returned as part of a SQL select statement but not forwarded or logged to a syslog server. The IBM i history log can also be queried via a special table function, but just like the audit journal table function, does not forward returned entries to a syslog server.

Some IBM i customers also expressed interest in monitoring Integrated File System (IFS) stream file changes, message queue events, and database journal changes and report those changes to a central syslog-based logging service.

The Security and Compliance Tools for IBM i - Syslog Reporting Manager (SRM) tool has been created to simplify the monitoring of system audit journal events, history log events, and stream file change events. An administrator can select the events that should be monitored and specify the remote syslog server / SIEM server that should receive the monitored events. All events are sent in either the Common Event Format (CEF) or Log Event Extended Format (LEEF).

Details

The SRM tool is a native IBM i application with the following key characteristics:

- Provides separate monitoring programs for system audit journal events, user audit journal events, QHST history log events, IFS stream file changes, message queue events, and database journal changes (requires additional tool).
- Highly configurable through many custom settings
- Supports RFC3164 and RFC5424 syslog protocol formats
- Entries that are sent to a syslog server can be formatted in either Common Event Format (CEF) or Log Event Extended Format (LEEF).
- Automatic restart capabilities of monitor jobs in case of failures or malicious ending of monitor jobs
- All tool-related programs run as batch programs in a separate subsystem
  - Subsystem name is SLSBS
  - Monitor control job name is SLMONSTR. It is responsible for:
    - for starting event monitor jobs
    - monitoring event monitor job status
    - restarting event monitor jobs
  - >Audit journal monitor job name is SLAUDMON. It is responsible for:
    - retrieving custom set of system audit journal entries. Filters can be applied to limit the number of reported events. The supported filters are user profile names and system-type entry specific data (event type field of entry-specific data).

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

    - providing retrieved entries to the communication jobs that send the events to a network accessible syslog / SIEM server
  - Audit journal monitor job name is SLAUDMONU. It is responsible for:
    - retrieving user-type audit journal entries. Filters can be applied to limit the number of reported events. The supported filters are user profile names.
    - providing retrieved entries to the communication jobs that send the events to a network accessible syslog / SIEM server
  - QHST history log event monitor job name is SLHSTMON. It is responsible for:
    - retrieving history log events based on a customizable set of filter rules. If no filter rules are defined, all history events are reported.
    - providing retrieved entries to the communication jobs that send the events to a network accessible syslog / SIEM server
  - IFS stream file monitor job name is SLIFSMONnn. It is responsible for:
    - retrieving IFS stream file changes for monitored stream files. Files to be monitored are added to a journal. There is a SRM-provided journal named IFSJRN. The user can also files in custom-defined journals.
    - providing retrieved entries to the communication jobs that send the events to a network accessible syslog / SIEM server
  - Message queue monitor job names are SLMSGQMON and SLMSQMONS. They are responsible for:
    - retrieving messages from monitored message queues. Filters can be applied to limit the number of reported events. The supported filters are user profile names, message identifier, message types, and the message severity.
    - providing retrieved entries to the communication jobs that send the events to a network accessible syslog / SIEM server
  - Database journal monitor job name is SLDB2MON and is started at a configured interval by the SLMONSTR job. Note that this function requires another IBM Systems Lab Services asset named Journal Extract Tool. It is responsible for:
    - processing all configured database journals in the Journal Extract Tool and convert the retrieved events into the proper SIEM message format.
    - providing retrieved entries to the communication jobs that send the events to a network accessible syslog / SIEM server
  - Communication job name(s) are SLSNDEVTx. They are responsible for:<
    - retrieving events from monitor jobs.
    - send retrieved entries to a network accessible syslog / SIEM server
  - All programs run under the owner profile QZRDSRMOWN
  - Access to configuration commands is granted via group membership to IBM i group profile QZRDSRMGRP.

The monitor programs receive events from the audit journal, the QHST history log, message queues, database journals (in combination with JET) or a dedicated journal for monitoring stream file changes. Events are sent to a syslog server via the syslog protocol over IP protocol UDP or TCP or TLS-encrypted. The syslog message payload contains the events in CEF format. Following are a few event examples:

Audit journal event of an authority failure (AF) in RFC3164 format:

```
<36>Aug 25 14:52:08 i5osp4 102F5F: CEF:0|IBM|IBM i|7.4|QSYS-
QAUDJRN|T-AF|Medium|reason=Authority failure msg=Not authorized to
object fileType=*PGM cs1Label=objName cs1=QZRDSECSRM/CFGJSCR
suser=THOMAS sproc=722470/THOMAS/QPADEV000P shost=I5OSP4
src=192.168.126.71 spt=36868
```

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

Stream file change event in RFC5424 format:

```
<134>1 2020-08-25T21:55:41.520032+02:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM IFSMON 102F5F - CEF:0|IBM|
IBM i|7.4|IFSMON|IFS File Monitor Journal Entry Type  B-WA|3|
act=B-WA Write, after-image event sproc=722496/BARLEN/QZSHSH
suser=BARLEN shost=I5OSP4 filePath=/home/barlen/ifsmon/weblog2.log
fileType=*STMF cs2Label=changedDataLength cs2=0000000064
cs3Label=changedDataPart cs3=*ONLY cs4Label=changedDataFileOffset
cs4=00000000000000788915 cs1Label=changedData cs1=Unauthorized
access to Web resource accountInfo by user TBARLEN<LF>
```

Audit journal event of a command (CD) entry type in RFC5424 format:

```
<38>1 2020-08-25T17:48:12.936816+02:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM AUDMON 102F5F - CEF:0|IBM|
IBM i|7.4|QSYS-QAUDJRN|T-CD|Low|reason=Command string audit
msg=Command run interactively from a command line or by choosing a
menu option that runs a CL command - CHGENVVAR ENVVAR(test4)
VALUE(77777) LEVEL(*SYS) fileType=*CMD cs1Label=objName
cs1=QSYS/CHGENVVAR suser=BARLEN sproc=721738/BARLEN/QPADEV000Q
shost=I5OSP4 src=192.168.126.71 spt=36888
```

QHST history log event of a job start in RFC5424 format (CEF) with second header:

```
<14>1 2020-08-25T18:59:04.791738+02:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM HSTMON 102F5F - CEF:0|IBM|
IBM i|7.4|QSYS-QHST|CPF1124|Low|reason=CPF1124 msg=Job
722506/QZRDSRMOWN/SLMSQMONS started on 25.08.20 at 18:59:04 in
subsystem SLSBS in QZRDSECSRM. Job entered system on 25.08.20 at
18:59:04. suser=QZRDSRMOWN sproc=722506/QZRDSRMOWN/SLMSQMONS
```

IFS stream file change log event in RFC5424 format where a custom tag of THOMAS5 was specified in LEEF format:

```
<134>1 2020-08-25T15:02:04.006928+02:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM IFSMON THOMAS5 - LEEF:2.0|
IBM|IBM i|7.4|IFSMON|x09|act=B-WA Write, after-image event
sproc=722519/BARLEN/QZSHSH usrName=BARLEN resource=I5OSP4
filePath=/home/barlen/ifsmon/weblog2.log  fileType=*STMF
changedDataLength=0000000055 changedDataPart=*ONLY
changedDataFileOffset=00000000000000788979 changedData=User BARLEN
removed access permission from user THOMAS<LF>
```

Custom generated event in RFC5424 format where a custom tag of P4MON was specified in LEEF format:

```
<14>1 2020-08-25T15:05:12.856000+02:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM CUSEVT P4MON - LEEF:2.0|
IBM|IBM i|7.4|CUSEVT-IBMi|x09|
resource=i5osp4.ai.stgt.spc.ihost.com usrName=MARION
```

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

```
sproc=721736/BARLEN/QPADEV000M cat=Loan application msg=User gave
0% interest rate for account 1294192
```

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

Message queue monitor event in RFC5424 format in CEF format:

```
<11>1 2020-04-30T11:35:29.886549+02:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM MSGMON 102F5F - CEF:0|IBM|
IBM i|7.4|MSGMON|CPF0907|5|cat=MSG Queue Messages rt=2020-04-30-
11.35.29.886549 reason=CPF0907 cs1Label=msgSev cs1=ERROR
cs2Label=msgQueue cs2=QSYS/QSYSOPR cs3Label=pgmName cs3=QWCATARE
msg=Serious storage condition may exist. Press HELP. cs4Label=srdb
cs4=I5OSP4 suser=QSYS sproc=541034/QSYS/QSYSARB5 shost=I5OSP4
```

Database journal monitor event via the Journal Extract Tool in RFC3164 syslog format and SIEM CEF message format:

```
<14>Apr 30 12:11:52 i5osp4 102F5F: CEF:0|IBM|IBM i|7.4|DB2MON|DB2
change monitoring (Journal Extract Tool)|3|act=UPDATE rt=2020-04-
30-12.11.52.265056 sproc=551907/BARLEN/QPADEV000D shost=I5OSP4
suser=BARLEN fname=QZRDSECSRM/SLTHSTENT cs1Label=pgmName
cs1=CFGSLHSTP cs2Label=updatedColumnNames
cs2=EVTUSER1,EVTMSGID1,EVTMSGID2,EVTMSGID3 cs5Label=rowDataBefore
cs5=QJ_JOURNAL_ENTRY_TYPE\="UB" QJ_RECEIVER_NAME\="DETRCV0010"
QJ_SEQUENCE_NUMBER\="22145" EVTUSER1\="BARLEN" EVTMSGID1\
="CPF1122" EVTMSGID2\="CPF9998" EVTMSGID3\="SLS0040"
cs4Label=rowDataAfter cs4=QJ_JOURNAL_ENTRY_TYPE\="UP"
QJ_RECEIVER_NAME\="DETRCV0010" QJ_SEQUENCE_NUMBER\="22146"
EVTUSER1\="BARLEN3" EVTMSGID1\="CPF1129" EVTMSGID2\="CPF9997"
EVTMSGID3\="SLS0042"
```

Information about syslog formats, the Common Event Format, and the Log Event Extended Format can be found at the following Web resources:

- RFC3164 IETF standard
- RFC5424 IETF standard
- Log Event Extended Format

  https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_LEEF_Format_Guide_intro.html

- Common Event Format information

  Using your favorite Internet search engine search for the following string:
  "common event format (cef)"

  There are several PDF documents that point to the same document describing the CEF format and outline.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

2 What's new in V2.1 (6th November 2021)

This section describes the enhancements in this version of the tool including the highlights about introduced changes.
To help you see where technical changes have been made, the following markers are used throughout the document.

- The > mark where new or changed information begins.
- The < mark where new or changed information ends.

>The following list summarizes the enhancements and changes in this version:

- SRM V2.1 is now using license keys to provide access to the tool instead of product access keys. This change has been made to streamline the packaging of IBM Systems Lab Services tools (assets). The advantage is that IBM i administrators can now test-drive the tool within a grace period of 70 days before making a decision to buy the tool. As part of this change, SRM has been changed as follows:
  - The tool library has changed from QZRDSYSLOG to QZRDSECSRM.
  - The owner and group profile has been changed from QZRDSLOWN/QZRDSLGRP to QZRDSRMOWN/QZRDSRMGRP.
  - The license product identifier has changed from 5ZRDPSC (option *BASE and 1) to 5ZRDSRM (option *BASE only).

- The Independent ASP support has been enhanced. V2.1 now supports multiple iASPs for IFS file monitor journals, the Journal Extract Tool integration, and the message queue monitor. Each definition for a message queue, an IFS monitor journal, or a journal that is defined for Journal Extract Tool integration, provides a new parameter to specify an ASP name. The ASP parameter accepts the following values:
  - A name of an ASP
  - The value *SYSTEM which refers to the system ASP (ASP number 1)
  - The value *GLOBAL which refers to the Syslog Reporting Manager global configuration parameter ASPGRP that is defined via the CFGSLENV command.

- The message queue monitoring function has been enhanced to support more selection filter. The new filter criteria, that can be applied on a per message queue level, are:
  - Up to 8 user profile names from which the message was sent. The parameter accepts generic user names.
  - Up to 8 message identifier. The message IDs can also be specified as generic values, i.e. CPI* would only report messages with a message ID that starts with CPI like CPI1E84.
  - Up to 3 message types.

- The audit journal monitor for system-supplied entry types (journal code T) has been enhanced to support additional filter criteria. In particular, the administrator can now select for each journal entry type one or mode entry type codes of the journal entry's entry-specific data. The IBM i Security Reference describes in Appendix F all IBM i issued journal entry types. The first field of the entry-specific data (the data following the entry headers) is a 1 character field. The meaning of the field varies by journal entry type. The filter does not apply to user type journal entries (journal code U). The filter capability allows you to enter one or more of the entry specific codes. Following are two examples:

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

- Example 1: Appendix F lists for the JS (Job Change) journal entry type 18 different entry types, but you are only interested in job hold (H), job release (R), and ENDJOBABN (A) operations. In this case, you would enter `AHR` in the parameter.
- Example 2: Appendix F lists for the PW (Password) journal entry type 12 different entry types, but you are only interested in password not valid (P), user not valid (U), signon failed due to a disabled user (Q), and when a CHKPWD authentication attempt fails (C) operations. In this case, you would enter `CPUQ` in the parameter.

- The IFS file monitor configuration command has been enhanced to allow you to specify directory journal inheritance for new IFS files that are created in the selected directory. Before this change, you could only enter the corresponding option with the STRJRN command. The configuration list also shows which directory has inheritance turned on.

- The IFS file monitor has been enhanced to autodetect the code page for deleted IFS files. In rare situations, a change of a monitored IFS file could be processed by the monitor after the file has been deleted. In this case the monitor cannot retrieve the code page of the file. This could lead to unreadable data in the reported event. In V2.1, the monitor tries to autodetect whether the changed data was stored in ASCII or EBCDIC format and then formats the output in the syslog event accordingly.

- The global configuration for the IFS file monitor has been moved from the CFGSLIFS command to the CFGSLIFSJ command.

- The Syslog Reporting Manager (SRM) has been enhanced to support Transport Layer Security (TLS) encrypted communication to the configured syslog servers. The encrypted session uses the underlying TCP protocol. SRM registers itself as a client application QIBM_5ZRD_SRM in the Digital Certificate Manager (DCM). DCM can then be used to define properties, such as supported TLS protocols, cipher specs, whether Online Certificate Status Protocol (OCSP) should be used to check for revoked certificates, etc.
  The global configuration command CFGSLENV is used to enable TLS-encrypted communication. It also has some new parameters that determine whether additional checks should be performed on the peer certificate's subject distinguished name of the syslog server. More information about the TLS implementation can be found in section 7 Transport Layer Security (TLS) implementation information on page 69.

- SRM also maintains a statistics table SLSTAT in library QZRDSECSRM which keeps the number of events by category that have been processed and sent by SRM. This version has been enhanced with the CFGSLSTAT command to specify the retention period in days for how long SRM will keep the statistics.

- **Statement of direction:** It is planned that V2R1 of the Syslog Reporting Manager will be the last release that supports IBM i V7R2.<

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

3 Implementation and use

The following sections guide you through installation, configuration, and usage if the SRM utility.

3.1 Prerequisites

The tool is an IBM i native ILE application. The following list shows the prerequisites:

- At least IBM i version 7.2.
- The following group PTFs are the minimum levels that are required:
  - IBM i 7.2 SF99702 Level 21
    - and PTF SI67459 or the PTF(s) that supersedes it
    - No support for additional T-journal code audit journal entry types. Only the first initial 30 entry types are supported.
  - IBM i 7.3 - SF99703 Level 22
  - IBM i 7.4 - SF99704 Level 10
    - Refer to chapter 10 Audit journal entry type support on page 83 for a list of supported journal entry types and the PTF prerequisites.

- PTF information for IBM i 7.4.
  - There is a problem when retrieving history log entries with the HISTORY_LOG_INFO table function. The configured EOF delay does not properly work. Install the following PTF or the PTF that supersedes it to correct the problem:
    - SI72062<
- Database change monitoring also requires the IBM Systems Lab Services Journal Extract Tool, which must be purchased separately. Refer to the Journal Extract Tool documentation for all details related to the installation and configuration of the tool. The enhanced configuration support of this tool is described in this document.
- SIEM messages contain information about the system that generated and sent the event. The identifier (host name) is derived from the TCP/IP configuration of your IBM i system. This requires that your TCP/IP setup is correct and meets the following specifications:
  - The TCP/IP domain must contain the hostname and the corresponding IP domain.
    Example:
    ```
    CHGTCPDMN HOSTNAME('i5osp4') DMNNAME('ai.stgt.spc.ihost.com')
    ```
  - The TCP/IP host table must contain an entry that matches the configured fully qualified host name.
    Example:
    ```
    ADDTCPHTE INTNETADR('172.17.17.40')
    HOSTNAME(('i5osp4.ai.stgt.spc.ihost.com'))
    ```

3.2 Authorities required to Install the Tool

The user installing the tool must have *ALLOBJ, *AUDIT, *IOSYSCFG, *JOBCTL and *SECADM special authorities or must be QSECOFR or an equivalent profile.

3.2.1 Authorities required to Run the Tool

Users running the tool must be a member of the group QZRDSRMGRP. No special authorities are required for the user profile.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

3.3 Installation

The tool consists of one component:

1. The IBM Security and Compliance Tools for IBM i Syslog Reporting Manager code
   Save file: `srmbase.savf`

>

Important note when upgrading from a previous version

Previous versions of the Syslog Reporting Manager have been shipped in two components (*BASE and option 1 of the license program 5ZRDPSC). In an effort to streamline IBM Systems Lab Services security assets packaging, the Syslog Reporting Manager needed to undergo several changes as outlined below:

- The product ID has changed from 5ZRDPSC to 5ZRDSRM
- The Syslog Reporting Manager is now packaged in license program option *BASE instead of 1
- The product code library has changed from QZRDSYSLOG to QZRDSECSRM
- The base product library QZRDPSC does not exist anymore
- The product owner profile has changed from QZRDSLOWN to QZRDSRMOWN
- The product administrator group profile has changed from QZRDSLGRP to QZRDSRMGRP.

End all monitor jobs by using the ENDSLMON command prior to installing the new version. After the monitor jobs have ended, end the subsystem SLSBS.<

Perform the installation as follows:

Important: Ensure all prerequisite license programs and PTF levels have been installed prior to performing the following steps.

1. FTP the psrmbase.savf file to a library of your choice. The example shows the QGPL library.
   ```
   bin
   quote site nam 1
   put srmbase.savf /QSYS.LIB/QGPL.LIB/SRMBASE.SAVF
   ```
2. Sign on to your IBM i partition with a user profile that has the authority to restore license programs.

3. Restore the IBM Security and Compliance Tools for IBM i Syslog Reporting Manager:

   ```
   RSTLICPGM LICPGM(5ZRDSRM) DEV(*SAVF) SAVF(QGPL/SRMBASE)
   ```

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

The installation process performs the following tasks:

- Creates a user profile QZRDSRMOWN. This profile is used as the owner profile for all objects that belong to the tool. In addition, all monitor jobs run as batch jobs under this profile.
- Creates a group profile QZRDSRMGRP. Membership to this profile grants access to the configuration and management commands of the Syslog Reporting Manager.
- Creates a library QZRDSECSRM. This library contains all QSYS.LIB file system objects of the tool including programs, commands, files, etc.
- In case of a version upgrade, all existing configuration settings will be migrated to the new version when running the RSTLICPGM commands.

Important: The tool requires a license key. The key must be obtained from your IBM Systems Lab Services contact. The key will be entered as part of the setup.

3.4 Upgrade information related to V2R1M0 from a previous version

>Version 2.1 of the Syslog Reporting Manager (SRM) supports a migration path from previous versions 1.3 and 1.4. A migration path from versions prior to version 1.3 is not supported. If you have an older version installed, you need to upgrade first to version 1.3 or 1.4 before performing the migration.

2.1 Migration overview

The migration is performed in multiple steps. The following overview summarizes the migration process:

Important: Migration can only be performed when both, the old version and the new version are installed at the same time.

1. Version 1.3 or 1.4 is installed on the system.
2. Version 2.1 is installed on the system.
3. Stop the Syslog Reporting Manager.
4. Run the migration program phase 1 to migrate all configuration data from your previous configuration in library QZRDSYSLOG to the new library QZRDSECSRM.
5. Delete the old Syslog Reporting Manager.
6. Run the migration program phase 2 to complete the migration.
7. Start the new Syslog Reporting Manager.

The following configuration data can be migrated:

- Global configuration data
- Audit monitor settings
- History log monitor settings
- IFS file monitor configuration, the configured IFS journals (only for V1.4), and the monitored file in the SRM journal QZRDSYSLOG/IFSJRN. For custom journals that have

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

been added to the configuration in V1.4, only the journal definition itself will be migrated. The monitored files are not touched by the migration process as they are not impacted.

- The message queue monitor global configuration and monitored message queues.
- Custom program options that have been modified.
- The global configuration of the Journal Extract Tool (JET) integration.
- All timestamps of previously processed events of the various monitors. It ensures that the new version will not loose any entries and starts after the events that have been processed by the previous version.

iASP Information for SRM V1.4

If you used the Independant ASP (iASP) support from version 1.4, the following migration considerations must be taken into account:

- IFS journal definitions of custom journals (command CFGSLIFSJ) and monitored message queues that are not found during migration will be added with an ASP name of *GLOBAL if an ASP Name was set in the CFGSLENV command. If no ASP name was defined in V1.4 in the CFGSLENV command, the ASP name of the migrated definitions is set to *SYSTEM (system ASP).

2.2 Performing the migration

The following steps guide you through the migration process. It is assumed that you had a working Syslog Reporting Manager version 1.3 or 1.4 (library QZRDSYSLOG) installed and that this version is still installed on the system. It is also assumed that you followed the steps to install the new Syslog Reporting Manager (library QZRDSECSRM).

1. Open a 5250 emulation session and sign on with a user profile that has the *ALLOBJ special authority.
2. Enter the following command to display the jobs in subsystem SLSBS.
   `WRKACTJOB SBS(SLSBS)`
   No jobs should be listed and the subsystem must not be active. If the subsystem is still active, end the Syslog Reporting Manager and its subsystem before continuing with the next step.
3. Enter the following command to start phase 1 of the migration process.
   `QZRDSECSRM/MIGFRMV1 PHASE(1)`
   The process should complete with message *"All configuration migration tasks completed successfully."*
   If you get the completion message "*One or more migration tasks failed. See joblog for more information."* check the joblog for information which migration step did not complete or had a warning.
4. Enter the following command to open the Syslog Reporting Manager main menu.
   `CFGSRM`
5. Check all monitor and global configurations. They should contain your migrated definitions and settings.
6. Check with the following command if user QZRDSLGRP has any members. If yes, remove the group from the listed member profiles.
   `DSPUSRPRF USRPRF(QZRDSLGRP) TYPE(*GRPMBR)`

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

7. Delete the previous version of your Syslog Reporting Manager.
   DLTLICPGM LICPGM(5ZRDPSC) OPTION(*ALL)
8. Complete the migration by running phase 2 of the migration process. This phase will recreate the proxy commands in library QSYS.
   QZRDSECSRM/MIGFRMV1 PHASE(2)
   If you receive a message that phase 2 cannot start because phase 1 issued warnings or errors and you have identified and solved all issues, you can force phase 2 by issueing the command:
   QZRDSECSRM/MIGFRMV1 PHASE(2) FORCE(*YES)
9. Delete the owner user profile of the old version **QZRDSLOWN** with the DLTUSRPRF command.
10. If any members were found in step 6 of the migration and have been removed from the QZRDSLGRP group profile, verify the list of removed users if they are still needed and if yes, add them to QZRDSRMGRP group.

This completes the migration. <

3.5 Granting access to the Syslog Reporting Manager

The SRM tool has been designed to be configured and operated by a user profile without any special authorities. The administrator responsible for managing the SRM tool must be a member of the QZRDSRMGRP group. The group can be added as a primary group or supplemental group profile.

Example of assigning the group as primary group:

```
CHGUSRPRF USRPRF(MYADMIN) GRPPRF(QZRDSRMGRP)
```

Example of assigning the group as a supplemental group:

```
CHGUSRPRF USRPRF(MYADMIN) SUPGRPPRF(QZRDSRMGRP)
```

3.5.1 Granting management access to the Journal Extract Tool

If you have the Journal Extract Tool installed and want the Syslog Reporting Manager administrator to also manage the Journal Extract Tool configuration, you can achieve this in two ways:

1. The administrator user must have the *ALLOBJ special authority
2. The administrator user must be member of the QZRDSRMGRP group profile and you must issue the following command as a user with *ALLOBJ special authority:
   ```
   CALL PGM(QZRDSECSRM/GRTJSACC)
   ```
   This program will grant the object permissions for group QZRDSRMGRP to objects in the QJSCRAPE library.

In case you want to remove access from the QZRDSRMGRP profile at a later time from objects in library QJSCRAPE, you need to run the following command:

```
CALL PGM(QZRDSECSRM/RVKJSACC)
```

3.6 Registering the license key

>After the installation of SRM, you can use the tool for a grace period of 70 days without registering a license key. The grace period starts when SRM is started for the first time. After the grace period has expired, you need to obtain a proper license key for your IBM Power System to continue using the tool. <

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

1. Start a 5250 session and sign on with a user that has *ALLOBJ special authority or as a member of the QZRDSRMGRP group.

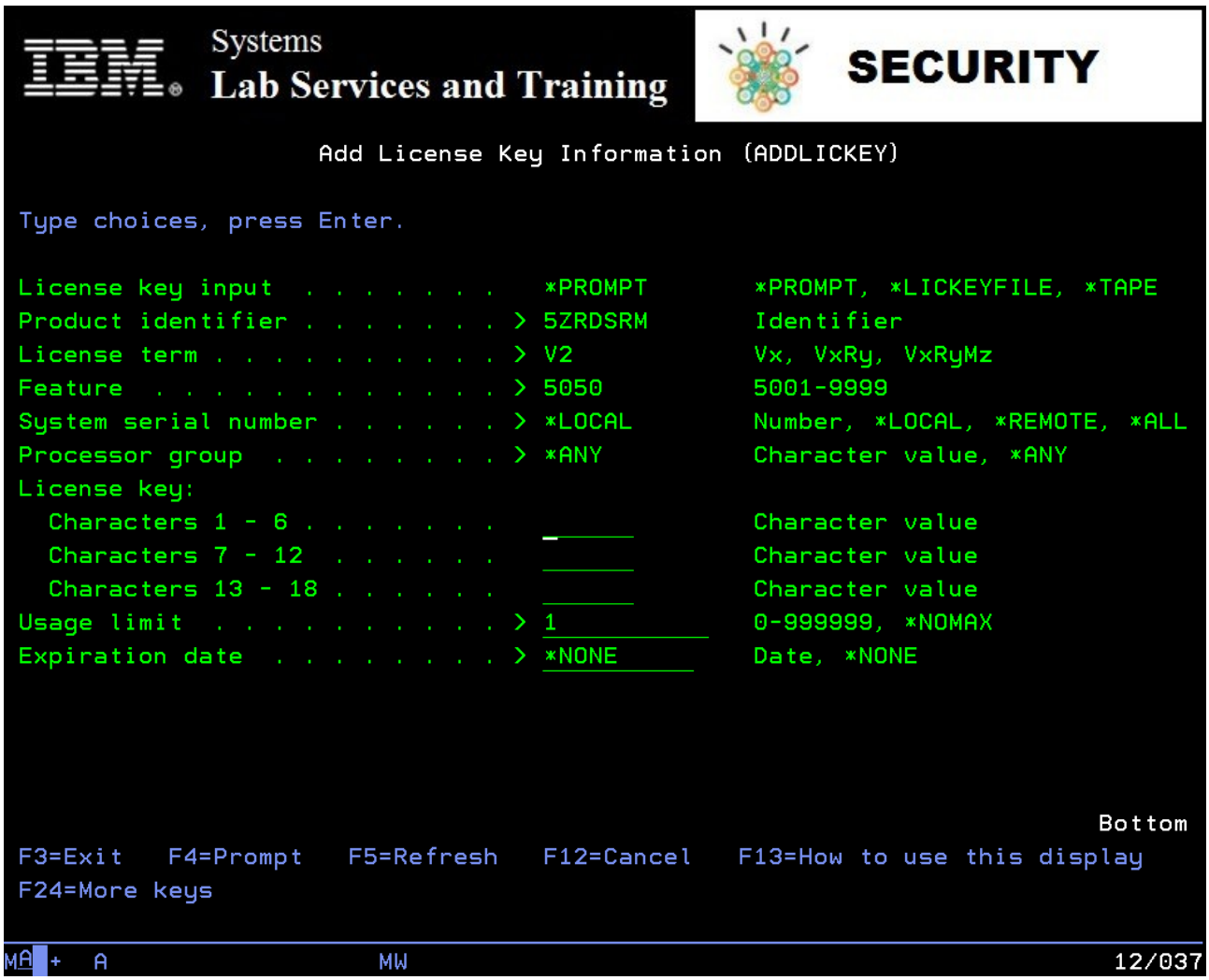
2. Enter the following command to display the Syslog Reporting Manager menu.
   `CFGSRM`

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

```
SLMON                Security and Compliance Tools for IBM i
                                                          System:   I5OSP4
                     Syslog Reporting Manager - Version 2.1.0

Select one of the following:

  Global environment
     1. Add product license key                          ADDLICKEY
     2. Configure global settings                        CFGSLENV
     3. Configure statistics settings                    CFGSLSTAT

  Data Journal Monitor (JET)
     5. Configure Journal Extract Tool                   GO SLJET

  Audit journal monitor
    10. Configure audit monitoring                       CFGSLAUD
    11. Start audit monitor                              STRSLMON *AUDMON
    12. End audit monitor                                ENDSLMON *AUDMON
    13. Work with audit system values                    WRKSYSVAL QAUD*
                                                                    More...
Selection or command
===>
F1=Help   F3=Exit   F6=SLMSGQ MSGs   F7=Active SRM Jobs
(C) Copyright IBM Corporation 2017, 2021  All Rights Reserved.
MA  +  C                                                          22/007
```

3. Take option 1 to enter your license key.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved



4. Enter the following information:
   - License key
   - Usage limit
   - Expiration date

   Note: The information is provided by IBM Systems Lab Services.

5. Press Enter to add your license code.

User configuration recommendation:

It is recommended to create a separate administrator profile and assign the following parameter to the profile:

```
INLMNU(QZRDSECSRM/SLMON)
CURLIB(QZRDSECSRM)
GRPPRF(QZRDSRMGRP)
```

A profile with these user profile settings has full administrative access to the Syslog Reporting Manager.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

3.7 Basic setup of the Syslog Reporting Manager tool

There are a few global properties that need to be set up first.

1. Display the SLMON menu by entering the command.

```
CFGSRM
```

2. Take option 2 (Configure global settings)

```
                    Configure Syslog Report Env (CFGSLENV)

 Type choices, press Enter.

 Hostname of Syslog server  . . . > 'siemhost.internal.local'
                                    'siemhost2.internal.local'
 Hostname backup Syslog server  . >
 Syslog server port number  . . . > 514          1-65535
 Syslog message tag . . . . . . .   *DEFAULT
 Starting journal time stamp  . .   *LASTPROC     *LASTPROC, *FIRST
 Specify Syslog format  . . . . .   RFC5424       RFC3164, RFC5424
 SIEM message format  . . . . . .   *CEF          *CEF, *LEEF
 Maximum message length . . . . .   8192          480-65535
 Send event statistics  . . . . .   *YES          *YES, *NO
 Number of send event jobs  . . .   1            1-9
 iASP group name  . . . . . . . .   *NONE        Character value, *NONE
 Transport protocol . . . . . . . > *TCP          *UDP, *TCP, *TLS
 TCP message transfer method  . .   *LF           *OCTCOUNT, *LF, *CR, *CRLF...

                                                                        Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
 F13=How to use this display        F24=More keys

MA  +  B                  MW                                          07/062
```

Information: Direct access via command: CFGSLENV

3. Provide the global information, such as:
   - Hostname or IP address of primary and backup syslog server that will receive the syslog messages.
   - The port that the syslog server is listening on.
   - An optional syslog header tag.
   - Starting journal time stamp option
   - Time stamp that is used in the syslog header
   - Syslog standard
   - SIEM message format (LEEF or CEF)
   - Maximum message length
   - Event statistics collection and reporting option
   - Number of send event jobs
   - iASP group name
   - <Transport protocol (UDP, TCP, or TLS)>
   - TCP message transfer method

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

- <Certificate path validation
- Peer certificate check for primary syslog server
- Wildcard certificate check for primary syslog server
- Peer certificate check for backup syslog server
- Wildcard certificate check for backup syslog server>
- Number of rows to fetch for the audit journal monitor for T-journal code events
- Number of rows to fetch for the audit journal monitor for U-journal code events
- Number of rows to fetch for the history log monitor

Information: Every command and configuration display provides detailed online help for all parameters via the F1 key.

Important: You have to completely end and start the Syslog Reporting Manager if you change the iASP group name.

To be able to use TLS encryption, you need to meet certain prerequisites. See section Transport Layer Security (TLS) implementation information on page 69 for more details.

4. After all global configuration values have been specified, press Enter to save your changes.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

3.8 Defining the audit journal monitor environment

The settings for the audit journal event monitor specify:

- Whether the audit journal event monitor will automatically start when the subsystem SLSBS starts
- The EOF delay specifies the number of seconds to sleep when all events have been read before trying to retrieve new events.
- Whether audit journals should be processed in all attached audit journal receivers (*CURCHAIN) or only in the currently attached receiver (*CURRENT).
- The audit journal event types that the event monitor job should process.

1. Display the SLMON menu by entering the command.

   `CFGSRM`

2. Take option 10 (Configure audit monitoring)

```
                         Configure Audit Monitor

Autostart Audit monitor . . . . :  *NO        *YES, *NO
EOF Delay after entries are read:  005        5 - 240 seconds
Audit journal receiver selection:  *CURCHAIN

Type options, press Enter.
 2=Edit  4=Delete  5=Display  6=Enable  7=Disable  Filter by entry type. : __
    Jrn                                          Displayed entry source: *ALL
    Ent                                                   Monitor Ent  U E S
Opt Typ Description                                       Enabled Src  F F P
 _  AD  Auditing changes                                  *YES    *SYS
 _  AF  Authority failures                                *YES    *SYS
 _  AP  Obtain adopted authority                          *NO     *SYS
 _  AU  Attribute changes (EIM)                           *NO     *SYS
 _  AX  Row and column access control                      *NO     *SYS
 _  CA  Authority changes                                 *NO     *SYS
 _  CD  Command string audit                              *NO     *SYS
 _  CO  Create object                                     *NO     *SYS
 _  CP  User profile changed, created, or restored        *YES    *SYS
 _  CQ  Change of Change Request Descr. (*CRQD) object    *NO     *SYS
                                                                   More...
F3=Save/Exit F5=Refresh F6=Add F11=Toggle source *SYS F12=Cancel

MA + A                  MW                                          12/003
```

Information: Direct access via command: CFGSLAUD

3. Enable all events that you want to have the event monitor report as syslog messages to the remote syslog server. See the online help for detailed information about each parameter. >With option 2 you can also specify user profile or entry-specific data filters.<

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

Note: The support for several journal entry types depend on the installed IBM i release and partly also on installed PTFs. See appendix 10 Audit journal entry type support on page 83 for the prerequisites for the various journal entry types of the entry source category *SYS.

4. Optionally you can also add U-journal code event types. They are listed as entry source *USR in the list of events. User type journal event types must be unique. They can be deleted or added as needed. System-type (*SYS) journal event types cannot be deleted.

<*Audit event processing information*

Which events the audit journal monitor processes depends on different criteria. The audit monitor processes all entries that are enabled in the configuration and that match the optional filter criteria (user filter and entry type filter). In addition, the following applies:

- When SRM is installed and starts the first time, it starts with the currently attached audit journal receiver and processes entries from the current time minus 24 hours.
- When SRM runs, the audit monitor keeps track of the last event that has been successfully processed and also the journal receiver in which the event was stored.
- When SRM is stopped and started again, the audit monitor checks whether the previously logged journal receiver still exists, if it does, the event selection is done based on the receiver and timestamp of the last event as the starting point. If the receiver does not exist anymore, the audit monitor starts either from the current chain of receivers (*CURCHAIN) or the currently attached receiver (*CURRENT). This is configurable in audit journal receiver selection parameter in the CFGSLAUD command. >

3.9 Defining the IFS stream file change monitor environment

The settings for the IFS file change event monitor specify:

- Select or define journals that monitor for IFS file changes. There is always the default journal QZRDSECSRM/IFSJRN.
- Whether the IFS file change event monitor will automatically start when SRM starts
- The syslog severity that is used for each file change event that is reported via the event monitor. See online help for valid values.
- The syslog facility that is used for each file change event that is reported via the event monitor. See online help for valid values.
- The selection of the data parts of the changed content that will be reported to the remote syslog/SIEM server.

1. Display the SLMON menu by entering the command.

```
CFGSRM
```

2. Take option 20 (Configure IFS file monitor)

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

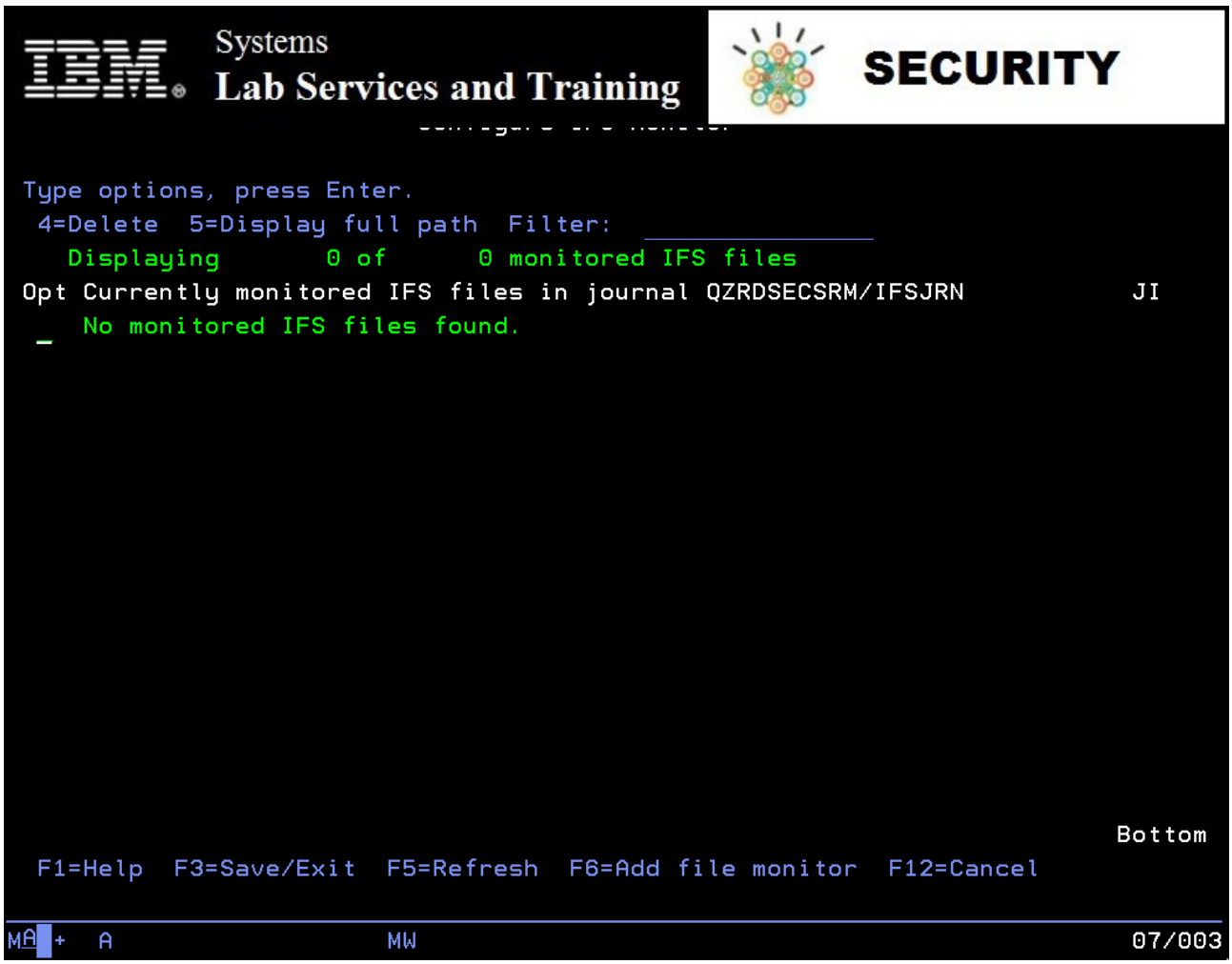
```
                    Configure IFS File Monitor Journals

  Autostart IFS monitor . . . . . :  *NO        *YES, *NO
  Syslog severity . . . . . . . . :  INFO       See help text for values
  Syslog facility . . . . . . . . :  LOCAL0     See help text for values
  Message part selection  . . . . :  *ALLSTR    See help text for values
  Type options, press Enter.
    4=Delete  6=Enable  7=Disable  12=Work with monitored files
  Opt  Jrn Lib.   Jrn Name   ASP Name   Type Enabled
  __   QZRDSECSRM IFSJRN     *SYSTEM    *SRM *YES

                                                                  More...
   F1=Help  F3=Exit  F6=Add journal  F12=Cancel

MA+  K                  MW                                        10/005
```

Information: Direct access via command: CFGSLIFSJ

3. >Work with the journals that monitor IFS file changes. You can add or remove journal names, enable or disable processing of events in a defined journal or work with files that are journaled via a specific journal.
   Specify the autostart, syslog severity, syslog facility, and message part settings. Note that these parameters are valid for all journals.
   Note that you cannot delete the SRM-provided journal QZRDSECSRM/IFSJRN from the list.

   Option 12 lets you work with files that are journaled via the selected journal.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved



Information: Direct access via command: CFGSLIFS

To add a new file to be monitored, press F6.
>The JI column indicates whether a directory has journal inheritance turned on. The meaning the column values are:

- **-**
  The listed item is a stream file and directory journal inheritance does not apply.
- **N**
  The listed item is a directory and journal inheritance for new objects is not turned on.
- **Y**
  The listed item is a directory and journal inheritance for new objects is turned on. In this case all new objects that are created in the directory are automatically added to the journal. <

4. Add IFS files to the list of monitored files. See the online help text for more information.

Alternative method to add or remove IFS files from the monitor list.

- Adding files using the STRJRN command. Example:

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

- `STRJRN OBJ(('/www/prodserver/logs/critlog')) JRN('/QSYS.LIB/QZRDSECSRM.LIB/IFSJRN.JRN')`
- Note that you can also add files generically by using a path such as `www/prodserver/logs/*`
- You can also add an entire directory and all future files that will be created in a directory:

```
STRJRN OBJ(('/www/prodserver/logs/'))
JRN('/QSYS.LIB/QZRDSECSRM.LIB/IFSJRN.JRN') INHERIT(*YES)
```

Important note: The path name length of an IFS file is limited to 350 characters.

- Removing files from the monitor list with the ENDJRN command. Example:
  - Removing a single file

```
ENDJRN OBJ(('/www/prodserver/logs/critlog'))
JRN('/QSYS.LIB/QZRDSECSRM.LIB/IFSJRN.JRN')
```

  - Removing all files

```
ENDJRN OBJ(*ALL) JRN('/QSYS.LIB/QZRDSECSRM.LIB/IFSJRN.JRN')
```

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

3.10 Defining the QHST history log event monitor environment

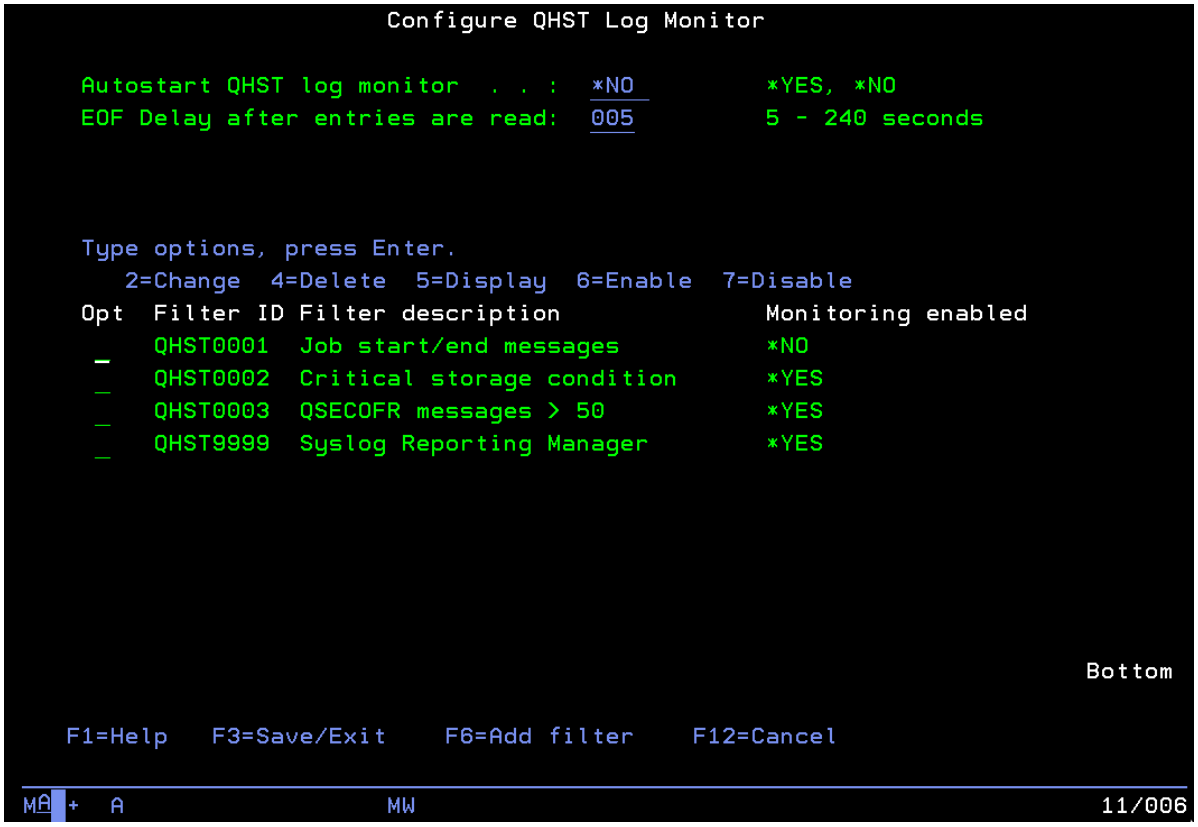
The settings for the QHST history log event monitor specify:

- Whether the history log event monitor will automatically start when the subsystem SLSBS starts
- The EOF delay specifies the number of seconds to sleep when all events have been read before trying to retrieve new events.
- The history selection filter rules that the event monitor job should process.

1. Display the SLMON menu by entering the command.

   ```
   CFGSRM
   ```

2. Take option 30 (Configure history monitoring)



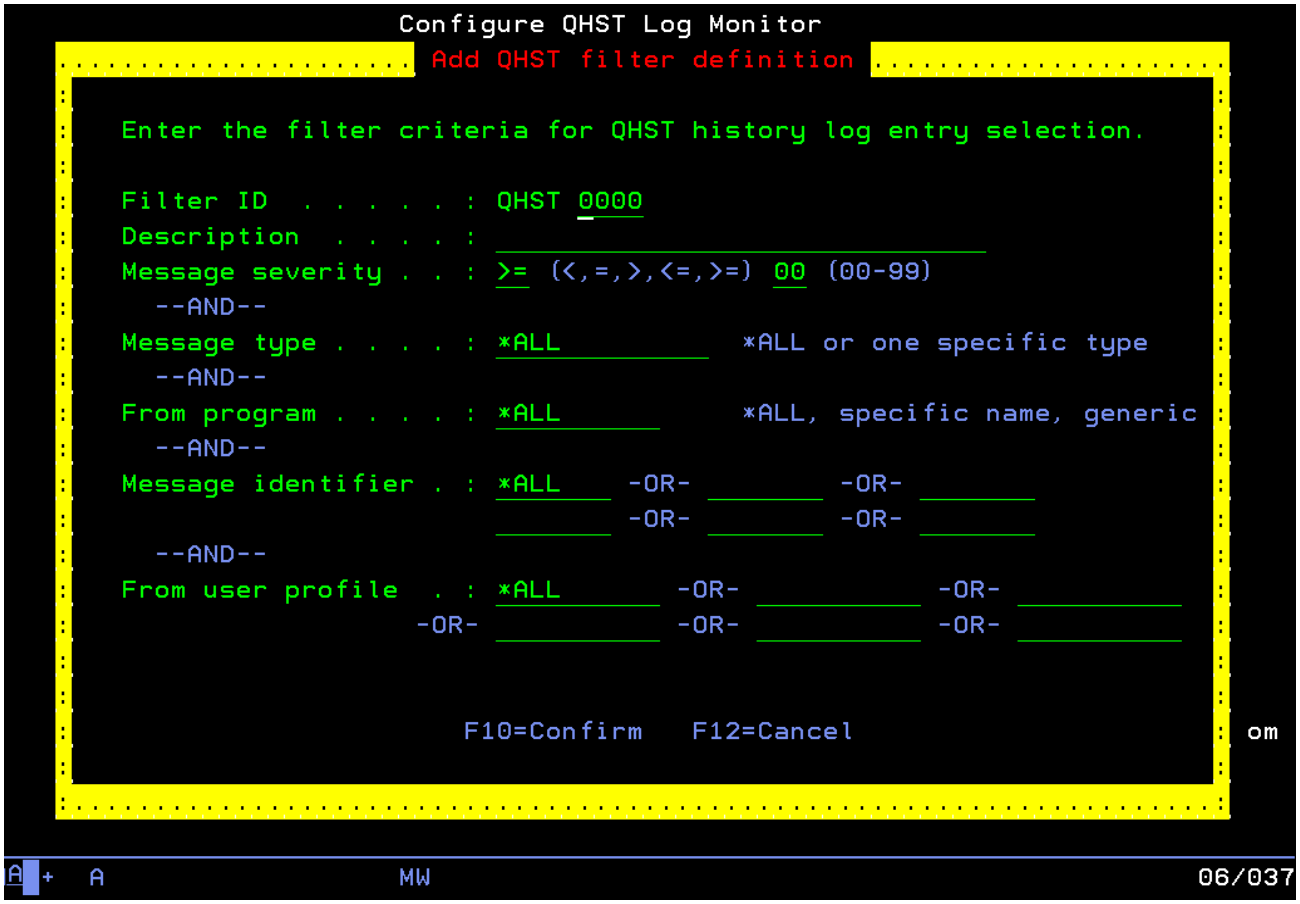
Information: Direct access via command: CFGSLHST

3. Specify the autostart and EOF delay parameter. See the online help for detailed information about each parameter.
4. Define one or more history log selection filter rules. A filter rule specifies one or more criteria for selecting history log entries to be reported by the event monitor to the remote syslog server. Only filter rules that are enabled are processed.

   To define a new filter selection rule, press F6.

   IMPORTANT: If you want to report all history log events to a syslog server, do not define or enable any filter selection rule. As soon as at least one filter rule is enabled for monitoring, only events that match the filter criteria will be reported.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved



Filter ID: A filter ID is the unique identifier for a history selection filter. You must specify a unique number. Note that the prefix cannot be changed.

Description: Provide a meaningful name for the filter so that you can easily determine its purpose on the overview list.

Message Severity: Use the comparator values and severity numeric values if you want to filter for messages that have a certain severity. If you do not want to limit by severity, leave the default of `>= 00`.

Message type: You can specify one of message types, such as `COMPLETION` or `DIAGNOSTIC`. If you do not want to filter by message type, leave the default of `*ALL`.

From Program: You can also specify the program from which the history log entry originated from. The name can be `*ALL` (default for no program filter), a specific program name, or a generic one, such as `QCMD*`.

Message Identifier: You can specify up to 6 message IDs. The filter will meet the selection criteria if one of the messages matches the history log entry. A value >of `*ALL` will not limit the history events by message ID. You can enter

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

complete 7-character message IDs or select message IDs generically, i.e. CPI* for the messages that start with CPI. The wildcard character * can be anywhere in the message ID.<

From User Profile: Enter up to 6 user profile names. You can specify an exact name or enter a generic user profile name.

Examples are:

PAYR*	=	All user profiles that start with PAYR match
SRV	=	All user profiles with a name that has somewhere the string SRV match, i.e. ORDSRV1 or SRVBATCH1

*ALL does not limit the events by user profile name.

NOTE: A filter matches a history log event if ALL of the specified criteria for a selection rule matches. Example: Severity > 30 AND User profile = (abc OR def)

5. Press F10 to save your new filter selection rule.
6. Repeat the previous steps to add all your required filter rules.
7. Enable all events that you want to be reported by the history event monitor.

Option 6 enables a filter and option 7 disables a filter.

```
                    Configure QHST Log Monitor

 Autostart QHST log monitor  . . :  *YES        *YES, *NO
 EOF Delay after entries are read:  005         5 - 240 seconds



 Type options, press Enter.
    2=Change  4=Delete  5=Display  6=Enable  7=Disable
 Opt  Filter ID Filter description              Monitoring enabled
  _   QHST0001  Job start/end messages          *NO
  _   QHST0002  Critical storage condition      *YES
  _   QHST0003  QSECOFR messages > 50           *YES
  _   QHST9999  Syslog Reporting Manager        *YES




                                                                  Bottom

 F1=Help   F3=Save/Exit    F6=Add filter    F12=Cancel

 A +  A                  MW                                      04/040
```

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

8. You can also use option 2 to change existing filter rules or option 4 to delete a rule entirely.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

3.11 Sending database change events via Journal Extract Tool integration

IMPORTANT INFORMATION

The database change event reporting leverages another IBM Systems Lab Services asset (tool) called Journal Extract Tool (JET). This tool is not part of the Syslog Reporting Manager (SRM) and needs to be purchased separately. Once this tool is installed and operable, it can be integrated into SRM. Without JET installed, SRM cannot generate database change events.

3.11.1 Preparation

- Install the Journal Extract Tool
- Perform any basic configuration that the Journal Extract Tool requires. Refer to the tool's users guide for more information.

3.11.2 Integration overview

The Journal Extract Tool uses journal objects to extract database table changes from tables that are journaled. Within the tool, you define the following:

- Journal objects that should be processed
- Table names of database tables whose changes should be reported
- User name tables for user profiles whose changes should be reported for the defined tables

The Syslog Reporting Manager provides user interfaces that list all defined journals, tables, and users of the Journal Extract Tool. The user interfaces let you add, remove, and partly change entries of the Journal Extract Tool configuration. A menu provides access to all Journal Extract Tool commands.

As an extension to the standard Journal Extract Tool, the Syslog Reporting Manager provides the following customization options:

- Specify for each table name in the Journal Extract Tool AUDITOBJ table, whether you want to generate syslog events at all, generate only summary events, or generate detailed events that also contain the column data of a changed table row.
- Specify for each journal in the Journal Extract Tool PROCTRACK table, whether you want the Syslog Reporting Manager process the journal for event generation.

In general, with the configuration options of the Syslog Reporting Manager you can further define whether you want to drop/clear the Journal Extract Tool tables at each journal processing job run and the interval in minutes at which the journal processing job runs.

The journal processing job performs the following tasks:

- Executes the PRCJRNENT command for every journal in the PROCTRACK table that is enabled in the Syslog Reporting Manager.
- After all PRCJRNENT commands have been completed, the GENSUMMARY command is executed to generate the change summary table.
- The summary table entries are now processed in the order of table names within the summary collection. Depending on the configured information level, syslog events will be generated:
  - As a summary entry from the data in the summary file
  - As a detailed entry from the data in the summary file and the corresponding data in the individual data tables that were created by the PRCJRNENT command. The content of the event depends on the database action:
    - INSERT or DELETE – All columns of a deleted or inserted row
    - UPDATE – Depending on whether before and after images are captured by the journals, the event might only include the before or after image of a row or both.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

- All events are sent in either LEEF or CEF format to the configured remote syslog or SIEM server.
- At the end of the journal processing job a summary event is sent to QSYSOPR, QHST (message SLS0050), and a syslog event with CEF/LEEF header info SRMDB2STAT1 containing statistics about the processed events. An example of such an event is:
  ```
  <14>1 2019-12-04T20:32:43.420000+01:00
  i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM IBMSRM 102F5F -
  CEF:0|IBM|IBM i|7.4|IBMSRM|SRMDB2STAT1|5|
  shost=i5osp4.ai.stgt.spc.ihost.com cat=SRM DB monitoring
  msg=Syslog Reporting Manager DB monitoring journal processing
  finished start=2019-12-04-20.31.58.156000 end=2019-12-04-
  20.32.43.353000 cs1Label=numberSummaryEvents cs1=8
  cs2Label=numberDetailEvents cs2=28
  sproc=384161/QZRDSRMOWN/SLDB2MON
  ```

Example of summary events in CEF format using the RFC5424 syslog RFC format:

Entry 1 (INSERT)
```
<181>1 2019-11-29T16:48:33.962144+01:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM DB2MON 102F5F - CEF:0|IBM|
IBM i|7.4|DB2MON|DB2 change monitoring (Journal Extract Tool)|3|
act=INSERT rt=2019-11-29-16.48.33.962144
sproc=379504/BARLEN/QPADEV0002 shost=I5OSP4 suser=BARLEN
fname=QZRDSECSRM/SLTHSTENT cs1Label=pgmName cs1=CFGSLHSTP
cs3Label=memberName cs3=SLTHSTENT
```

Entry 2 (DELETE)
```
<181>1 2019-11-29T16:48:42.567456+01:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM DB2MON 102F5F - CEF:0|IBM|
IBM i|7.4|DB2MON|DB2 change monitoring (Journal Extract Tool)|3|
act=DELETE rt=2019-11-29-16.48.42.567456
sproc=379504/BARLEN/QPADEV0002 shost=I5OSP4 suser=BARLEN
fname=QZRDSECSRM/SLTHSTENT cs1Label=pgmName cs1=CFGSLHSTP
cs3Label=memberName cs3=SLTHSTENT
```

Entry 3 (UPDATE)
```
<181>1 2019-11-29T16:51:40.752096+01:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM DB2MON 102F5F - CEF:0|IBM|
IBM i|7.4|DB2MON|DB2 change monitoring (Journal Extract Tool)|3|
act=UPDATE rt=2019-11-29-16.51.40.752096
sproc=379504/BARLEN/QPADEV0002 shost=I5OSP4 suser=BARLEN
fname=QZRDSECSRM/SLTHSTENT cs1Label=pgmName cs1=CFGSLHSTP
cs2Label=updatedColumnNames cs2=EVTTEXT,EVTPGM,EVTMSGID1
```

Example of detail events in LEEF format using the RFC3164 syslog RFC format:

Entry 1 (INSERT)
```
<181>Nov 29 16:48:33 i5osp4 102F5F: LEEF:2.0|IBM|IBM i|7.4|DB2MON|
x09|act=INSERT devTimeFormat=YYYY-MM-dd-HH.mm.ss.SSSSSS
devTime=2019-11-29-16.48.33.962144 sproc=379504/BARLEN/QPADEV0002
resource=I5OSP4 usrName=BARLEN pgmName=CFGSLHSTP
fname=QZRDSECSRM/SLTHSTENT memberName=SLTHSTENT rowData=EVTID\
="QHST4440" EVTTEXT\="Test filter Thomas Barlen" SEV\="0"
EVTUSER1\="*ALL" EVTUSER2\="" EVTUSER3\="" EVTUSER4\="" EVTUSER5\
```

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

```
="" EVTUSER6\="" EVTPGM\="*ALL" EVTMSGID1\="*ALL" EVTMSGID2\=""
EVTMSGID3\="" EVTMSGID4\="" EVTMSGID5\="" EVTMSGID6\=""
EVTMSGTYPE\="*ALL" SEVCOMP\=">\=" SEL\="*YES"
QJ_JOURNAL_ENTRY_TYPE\="PX" QJ_COUNT_OR_RRN\="6"
QJ_SEQUENCE_NUMBER\="1050" QJ_RECEIVER_NAME\="DETRCV0001"
```

Entry 2 (DELETE)

```
<181>Nov 29 16:48:42 i5osp4 102F5F: LEEF:2.0|IBM|IBM i|7.4|DB2MON|
x09|act=DELETE devTimeFormat=YYYY-MM-dd-HH.mm.ss.SSSSSS
devTime=2019-11-29-16.48.42.567456 sproc=379504/BARLEN/QPADEV0002
resource=I5OSP4 usrName=BARLEN pgmName=CFGSLHSTP
fname=QZRDSECSRM/SLTHSTENT memberName=SLTHSTENT rowData=EVTID\
="QHST4440" EVTTEXT\="Test filter Thomas Barlen" SEV\="0"
EVTUSER1\="*ALL" EVTUSER2\="" EVTUSER3\="" EVTUSER4\="" EVTUSER5\
="" EVTUSER6\="" EVTPGM\="*ALL" EVTMSGID1\="*ALL" EVTMSGID2\=""
EVTMSGID3\="" EVTMSGID4\="" EVTMSGID5\="" EVTMSGID6\=""
EVTMSGTYPE\="*ALL" SEVCOMP\=">\=" SEL\="*YES"
QJ_JOURNAL_ENTRY_TYPE\="DL" QJ_COUNT_OR_RRN\="6"
QJ_SEQUENCE_NUMBER\="1053" QJ_RECEIVER_NAME\="DETRCV0001"
```

Entry 3 (UPDATE with before and after image)

```
<181>Nov 29 16:51:40 i5osp4 102F5F: LEEF:2.0|IBM|IBM i|7.4|DB2MON|
x09|act=UPDATE devTimeFormat=YYYY-MM-dd-HH.mm.ss.SSSSSS
devTime=2019-11-29-16.51.40.752096 sproc=379504/BARLEN/QPADEV0002
resource=I5OSP4 usrName=BARLEN pgmName=CFGSLHSTP
fname=QZRDSECSRM/SLTHSTENT
updatedColumnNames=EVTTEXT,EVTPGM,EVTMSGID1
rowDataBefore=QJ_JOURNAL_ENTRY_TYPE\="UB" QJ_RECEIVER_NAME\
="DETRCV0001" QJ_SEQUENCE_NUMBER\="1059" EVTTEXT\="This is Thomas
Filter" EVTPGM\="*ALL" EVTMSGID1\="CPF4711"
rowDataAfter=QJ_JOURNAL_ENTRY_TYPE\="UP" QJ_RECEIVER_NAME\
="DETRCV0001" QJ_SEQUENCE_NUMBER\="1060" EVTTEXT\="This is Marion
Filter" EVTPGM\="CHKE1" EVTMSGID1\="CPF3333"
```

3.11.3 Configuring the Journal Extract Tool integration

All configuration options are available from the SLMON menu. The configuration of the Journal Extract Tool integration is done via a sub-menu of the SLMON menu.

1. Start a 5250 session and sign on with a user that has *ALLOBJ special authority or as a member of the QZRDSRMGRP group.

2. Add the library QZRDSECSRM to the job's library list.

   ```
   ADDLIBLE QZRDSECSRM
   ```

3. It is recommended to permanently assign the library to the administrator's user profile. Enter the following command to display the Syslog Reporting Manager menu.
   >

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

CFGSRM

<

```
SLMON                Security and Compliance Tools for IBM i
                                                          System:    I5OSP4
                     Syslog Reporting Manager - Version 2.1.0

Select one of the following:

  Global environment
     1. Add product license key                          ADDLICKEY
     2. Configure global settings                        CFGSLENV
     3. Configure statistics settings                    CFGSLSTAT

  Data Journal Monitor (JET)
     5. Configure Journal Extract Tool                   GO SLJET

  Audit journal monitor
    10. Configure audit monitoring                       CFGSLAUD
    11. Start audit monitor                              STRSLMON *AUDMON
    12. End audit monitor                                ENDSLMON *AUDMON
    13. Work with audit system values                    WRKSYSVAL QAUD*
                                                                   More...
Selection or command
===>
F1=Help   F3=Exit   F6=SLMSGQ MSGs   F7=Active SRM Jobs
(C) Copyright IBM Corporation 2017, 2021  All Rights Reserved.
MA  +  B                                                          22/007
```

4. Enter option 5 Configure Journal Extract Tool to open the Journal Extract Tool integration menu.
   Note: You need the Journal Extract Tool to be installed on the system to be able to open the menu. Otherwise you will not see the menu option.

```
SLJET                Syslog Reporting Manager - Version 2.1.0
                                                          System:    I5OSP4
                        Journal Extract Tool Integration

Select one of the following:

  Journal Extract Tool commands
     1. Configure audit users                          CFGJSUSR
     2. Configure audit objects                        CFGJSOBJ
     3. Configure journals to be processed             CFGJSPRC

    10. Change the logging value                       QJSCRAPE/CHGLOG

    20. Process journal entries                        QJSCRAPE/PRCJRNENT
    21. Generate a summary report                      QJSCRAPE/GENSUMMARY
    22. Display journal report                         QJSCRAPE/DSPJRNRPT

  Syslog Reporting Manager integration
    30. Configure journal extract tool integration     CFGJSGLB
                                                                    Bottom
Selection or command
===>
F1=Help   F3=Exit   F7=Active SRM Jobs
(C) Copyright IBM Corporation 2017, 2021  All Rights Reserved.
MA +  B                  MW                                        22/007
```

Journal Extract Tool tasks

Before the Syslog Reporting Manager can report database change events, the Journal Extract Tool has to be properly set up. Refer to the documentation of the Journal Extract Tool for detailed information.

The Syslog Reporting Manager integration provides some additional features that are only available via the SLJSCR menu. The features are:

- You can specify the level of detail that should be included
- You can enable individual journals to be processed when the Syslog Reporting Manager reports database change events.

The Journal Extract Tool uses journals to capture database changes. The analysis of the captured data is further filtered by the tables that are registered with the tool and the users who performed the database changes within the registered tables.

Note that the Journal Extract Tool commands are all listed on the Syslog Reporting Manager integration menu, but only the customized configuration is covered in this section of the user's guide. For all details regarding menu options 10, 20, 21, and 22 refer to the documentation of the Journal Extract Tool.

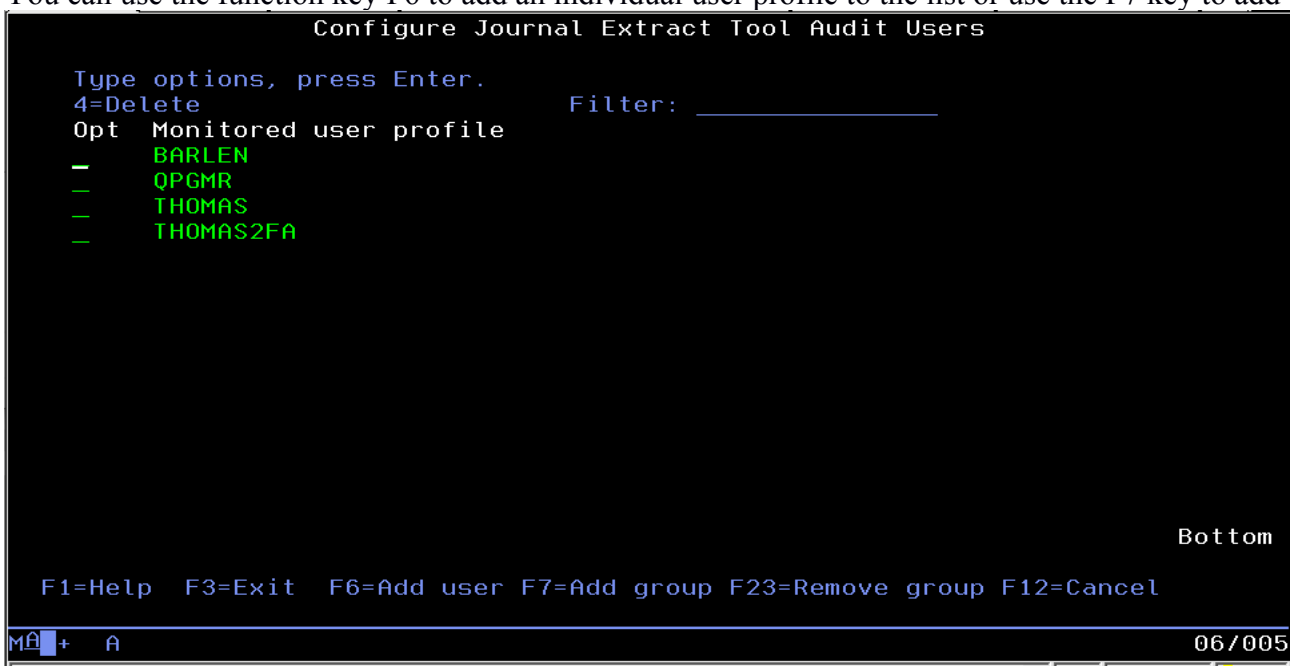
Define users whose database changes are reported

The Journal Extract Tool uses the AUDITUSERS table in the QJSCRAPE library to define all user profile names whose changes are reported for the database tables that are defined in the AUDITOBJ table. The Syslog Reporting Manager lets you view and manage the registered user profiles via the SLJSCR menu.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

Take option 1 to view currently registered user profiles and manage them.

You can use the function key F6 to add an individual user profile to the list or use the F7 key to add



all users that are member of a specific group to the list. F23 lets you remove all users of a specific group from the list.

Note: If you select F23 to remove users who are member of the specified group, all members are removed even though the user might be a member of another group that you also added with the F7 key.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

Define database table objects whose changes are reported

The Journal Extract Tool uses the AUDITOBJ table in the QJSCRAPE library to define all database tables whose changes are reported. The Syslog Reporting Manager lets you view and manage the registered tables via the SLJSCR menu.

```
SLJET                Syslog Reporting Manager - Version 2.1.0
                                                          System:    I5OSP4
                        Journal Extract Tool Integration

Select one of the following:

  Journal Extract Tool commands
     1. Configure audit users                              CFGJSUSR
     2. Configure audit objects                            CFGJSOBJ
     3. Configure journals to be processed                 CFGJSPRC

    10. Change the logging value                           QJSCRAPE/CHGLOG

    20. Process journal entries                            QJSCRAPE/PRCJRNENT
    21. Generate a summary report                          QJSCRAPE/GENSUMMARY
    22. Display journal report                             QJSCRAPE/DSPJRNRPT

  Syslog Reporting Manager integration
    30. Configure journal extract tool integration         CFGJSGLB
                                                                        Bottom
Selection or command
===> ____________________________________________________________________________
F1=Help   F3=Exit   F7=Active SRM Jobs
(C) Copyright IBM Corporation 2017, 2021  All Rights Reserved.
MA + B                  MW                                          22/007
```

Take option 2 to view currently registered tables and manage them.

```
                Configure Journal Extract Tool Audit Objects
   Type options, press Enter.
              ----- Journal Process Options ----
   4=Delete  6=Global 7=Detail 8=Summary 9=None  Filter: _______________
   Opt  Library    Object     Process option
   _    QZRDSYSLOG AUDCFG     *DETAIL
   _    QZRDSYSLOG SLTHSTENT  *DETAIL

                                                                        Bottom
 F1=Help  F3=Exit  F5=Refresh  F6=Add object  F12=Cancel
MA + A                                                                  06/005
```

When adding a new table to the AUDITOBJ table, processing option of *GLOBAL is selected. The following process options can be used:

- *GLOBAL
  When this value is set, the syslog information level as defined in the global Syslog Reporting Manager integration configuration is used.
- *SUMMARY
  When this value is set, the event that is generated by the Syslog Reporting Manager consists of data stored in the Journal Extract Tool summary file (QJSCRAPE/JSUMMARY). Details about the actual data values that got changed are not included.
- *DETAIL
  When this value is set, the event that is generated by the Syslog Reporting Manager consists of the data in the summary file and the corresponding data in the individual data tables that were created by the PRCJRNENT command. The content of the event depends on the database action:
  - INSERT or DELETE – All columns of a deleted or inserted row
  - UPDATE – Depending on whether before and after images are captured by the journals, the event might only include the before or after image of a row or both.

Define journals that contains database changes that are reported

All the analysis and data extraction that is performed by the Journal Extract Tool is based on database changes that are captured in data journals. You have to register existing data journals to the Journal Extract Tool's PROCTRACK table.

The Syslog Reporting Manager lets you view and manage the registered journals via the SLJSCR menu.

```
SLJET                Syslog Reporting Manager - Version 2.1.0
                                                          System:   I5OSP4
                        Journal Extract Tool Integration

Select one of the following:

  Journal Extract Tool commands
     1. Configure audit users                          CFGJSUSR
     2. Configure audit objects                        CFGJSOBJ
     3. Configure journals to be processed             CFGJSPRC

    10. Change the logging value                       QJSCRAPE/CHGLOG

    20. Process journal entries                        QJSCRAPE/PRCJRNENT
    21. Generate a summary report                      QJSCRAPE/GENSUMMARY
    22. Display journal report                         QJSCRAPE/DSPJRNRPT

  Syslog Reporting Manager integration
    30. Configure journal extract tool integration     CFGJSGLB
                                                                    Bottom
Selection or command
===> ____________________________________________________________________
F1=Help   F3=Exit   F7=Active SRM Jobs
(C) Copyright IBM Corporation 2017, 2021  All Rights Reserved.
MA + B                  MW                                          22/007
```

Take option 3 to view currently registered database journals and manage them.

```
                 Configure Journal Extract Tool Process Journal Objects

Type options, press Enter.
2=Change  4=Delete  5=Display  6=Enable  7=Disable  Filter:
Opt  Library    Object     Last Starttime             Jrn rcv    Status    ASP
     LIBJRN14   JRN14A     0001-01-01-00.00.00.000000 *CURRENT   *ENABLED   S
     LIBJRN14   JRN14B     0001-01-01-00.00.00.000000 RCV1400214 *ENABLED   S

                                                                      Bottom

 F1=Help  F3=Exit  F5=Refresh  F6=Add process jrn  F12=Cancel

MA    D                                                              06/002
```

The configuration lets you add and remove journals from the PROCTRACK table. In addition, you can select whether the journal extraction analysis will process a journal.

- *ENABLED
  The status *ENABLED indicates that journal processing that is started with the PRCJRNENT command will also process the database changes of the given journal.
- *DISABLED
  When the status of journal is *DISABLED, the journal processing will ignore the journal and database changes in this journal will not be reported.

>The ASP column indicates the ASP in which the journal objects resides. The following values can be shown:

- S = *SYSTEM ASP
- G = *GLOBAL is the ASP group name that is specified in the CFGSLENV command.
- O = Other ASP. An ASP name has been specified and you can change the name with option 2 or display its name using option 5. <

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

Configure the Syslog Reporting Manager integration

The configuration covered in this section describes the various settings that affect the integration, processing, and reporting of the information provided by the Journal Extract Tool.
The Syslog Reporting Manager lets you view and manage the database change event processing via the SLJSCR menu.

```
SLJET                Syslog Reporting Manager - Version 2.1.0
                                                          System:    I5OSP4
                        Journal Extract Tool Integration

Select one of the following:

  Journal Extract Tool commands
     1. Configure audit users                              CFGJSUSR
     2. Configure audit objects                            CFGJSOBJ
     3. Configure journals to be processed                 CFGJSPRC

    10. Change the logging value                           QJSCRAPE/CHGLOG

    20. Process journal entries                            QJSCRAPE/PRCJRNENT
    21. Generate a summary report                          QJSCRAPE/GENSUMMARY
    22. Display journal report                             QJSCRAPE/DSPJRNRPT

  Syslog Reporting Manager integration
    30. Configure journal extract tool integration         CFGJSGLB
                                                                        Bottom
Selection or command
===> ____________________________________________________________________
F1=Help   F3=Exit   F7=Active SRM Jobs
(C) Copyright IBM Corporation 2017, 2021  All Rights Reserved.
MA + B                  MW                                          22/007
```

Take option 30 to configure the integration options.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

The configuration options are as follows:

- Enable DB event processing
  The parameter specifies whether the database monitor and reporting job will process events generated by the Journal Extract Tool at the interval specified at the Journal processing interval parameter. The events will be processed and send by the Syslog Reporting Manager.
  - ***YES**
    The database change monitor job will be started when the IBM i Syslog Reporting Manager tool starts and runs at the specified interval as defined in the Journal processing interval parameter.
  - ***NO**
    The database change monitor job will not start when the the IBM i Syslog Reporting Manager tool starts. The job needs to be started manually.
- Syslog severity
  The parameter specifies the Syslog severity that will be used by the monitor job to report events via the syslog protocol to the Syslog server. See the online help for detailed information about each parameter.
- Syslog facility
  The parameter specifies the Syslog facility name that will be used by the monitor job to report events via the syslog protocol to the Syslog server. See the online help for detailed information about each parameter.
- Global syslog information level
  You can also select a processing option for journal processing and the level of details that you want to send to the Security Information and Event Management (SIEM) system or remote syslog server. This is the global settings for the level of detail. If a file that is defined

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

in the AUDITOBJ table via the Syslog Reporting Manager interface, you can override the detail level on a per file basis. Only files that are defined with a information level of *GLOBAL will use the settings in this parameter. The following options can be selected:

- ***DETAIL**
  When this option is selected, the information from the Journal Extract Tool summary report and the detailed information for the specified file is sent to the SIEM server. This includes the before and after information of the changed data, assuming that both images are captured in the journal.
- ***SUMMARY**
  With this option selected, only the information in the Journal Extract Tool summary report are processed for the selected file.

- Journal processing interval
  The Syslog Reporting Manager (SRM) runs a journal processing job that analyzes each enabled journal of the Journal Extract Tool. The interval determines how often this job runs. Depending on the number of journals to be processed and the files that are journaled, the processing time of the job varies. SRM runs only one instance of the journal processing job at a time. If you monitor a large number of files and the journal processing takes longer than the interval specified, you may not get the job processed as often as you want. Therefore, you should start with a higher interval and then take a look at the processing job information section. You will see when the job started and ended. This gives you an indication on how to set the interval. Important to know is that the specified number of minutes are used to calculate the next processing time after the previous processing job ended.
  - number of minutes
    The interval is specified in minutes. The minimum value is 1 minute and the maximum value 1440 minutes (1 day).
- Drop tables before processing
  The Syslog Reporting Mananger uses the Journal Extract Tool command PRCJRNENT command to analyze the data journals and to create the tables with the changes. The DROPTBL parameter of the PRCJRNENT command determines if all data tables that are created by the PRCJRNENT command are removed from the QJSCRAPE library. If *YES is specified, then ALL existing QJSCRxxxxx tables are removed, not just those tables associated with the journal name specified. The following options can be selected:
  - ***NO**
    No QJSCRxxxxx tables in library QJSCRAPE will be removed when running the PRCJRNENT command.
  - ***YES**
    The Journal Extract Tool removes ALL existing QJSCRxxxxx tables, not just those tables associated with the journal name specified. *YES causes all QJSCRxxxxx tables to be deleted for each journal that is enabled for processing.
- Clear data tables before processing
  The Syslog Reporting Mananger uses the Journal Extract Tool command PRCJRNENT command to analyze the data journals and to create the tables with the changes. The CLRDATA parameter of the PRCJRNENT command determines if all data tables that are created by the PRCJRNENT command are cleared in the QJSCRAPE library. If *YES is specified, then ALL existing QJSCRxxxxx tables are cleared, not just those tables associated with the journal name specified. The following options can be selected:
  - ***NO**
    No QJSCRxxxxx tables in library QJSCRAPE will be cleared when running the PRCJRNENT command.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

- ***YES**
  The Journal Extract Tool clears ALL existing QJSCRxxxxx tables, not just those tables associated with the journal name specified.
  IMPORTANT: Set this parameter only to *YES for a single run of the database change analysis process. *YES causes all QJSCRxxxxx tables to be cleared for each journal that is enabled for processing.

- Clean up non-existing objects
  The default behavior of the Journal Extract Tool is that you can add objects to the AUDITOBJ table that do not have to exist on the system. However, if you run the PRCJRNENT command or run the equivalent journal processing job within the Syslog Reporting Manager, objects that are defined in the AUDITOBJ file but do not exist on the system, can cause problems. Therefore, the Syslog Reporting Manager contains a function that can be enabled via this parameter to check that every object in the AUDITOBJ and PROCTRACK tables actually exist on the system. If automatic cleanup is enabled, entries in those two tables will be removed if the specified object does not exist on the IBM i partition. >This includes objects that reside in ASP that is not varied on or otherwise not available on the system.< Note that the automatic cleanup process could have an impact on the performance of the journal processing job. This heavily depends on the number of rows in the AUDITOBJ and PROCTRACK tables. The following options can be selected:
  - ***YES**
    When this option is selected, the journal processing job will check that all objects within the AUDITOBJ and PROCTRACK files exist on the system. If not, the corresponding entries are removed from the AUDITOBJ and PROCTRACK files. The check also verifies the existence on configured ASPs.
  - ***NO**
    With this option selected, the journal processing job will not check that all objects within the AUDITOBJ and PROCTRACK files exist on the system. Objects that might not exist could cause problems when running the journal processing job.

- Database monitoring event processing job information
  The information section gives you details about the journal processing job.
  - Job status - The status gives you an indication whether the journal processing is active. The status INACTIVE indicates that the job is neither running nor currently in a job queue. The status SUBMITTED indicates that the SRM control job has submitted the journal processing job, but it has not started yet. ACTIVE indicates that the job is currently running in the SLSBS subsystem.
  - Start timestamp - Is the date and time when the journal processing job started the last time.
  - End timestamp - Is the date and time when the journal processing job finished the last time.
  - Jobname - This is the fully qualied jobname of the most recent journal processing job.
  - Next scheduled submission time - Is calculated by adding the processing interval to the last end timestamp.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

3.12 Sending message queue events

The Syslog Reporting Manager can also monitor message queues within IBM i. Messages that appear in a monitored message queue are reported at a predefined interval.
Following is an example of a raw syslog message in syslog RFC5424 format and SIEM format *LEEF:

```
<11>1 2020-01-13T12:58:01.422426+01:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM MSGMON 102F5F - LEEF:2.0|
IBM|IBM i|7.4|MSGMON-CPF9898|x09|cat=MSG Queue Messages
devTimeFormat=YYYY-MM-dd-HH.mm.ss.SSSSSS devTime=2020-01-13-
12.58.01.422426 reason=CPF9898 msgSev=ERROR
msgQueue=QUSRSYS/BARLEN pgmName=CVTDBTOM msg=Database conversion
job ended in an error.
```

The Syslog Reporting Manager configuration menu provides options 40 – 43 that let you define and control the message queue monitoring and reporting.

```
SLMON                Security and Compliance Tools for IBM i
                                                          System:    I5OSP4
                     Syslog Reporting Manager - Version 2.1.0

Select one of the following:

  IFS file monitor
    20. Configure IFS file monitor                        CFGSLIFSJ
    21. Manage monitored IFS files by journal             CFGSLIFS
    22. Start IFS file monitor                            STRSLMON *IFSMON
    23. End IFS file monitor                              ENDSLMON *IFSMON

  History monitor
    30. Configure history monitoring                      CFGSLHST
    31. Start history monitor                             STRSLMON *HSTMON
    32. End history monitor                               ENDSLMON *HSTMON

  Message queue monitor
    40. Configure message queue monitor                   CFGSLMQM
                                                                      More...
Selection or command
===> ____________________________________________________________________
F1=Help   F3=Exit   F6=SLMSGQ MSGs   F7=Active SRM Jobs

MA + B                MW                                          22/007
```

```
SLMON                Security and Compliance Tools for IBM i
                                                          System:    I5OSP4
                     Syslog Reporting Manager - Version 2.1.0

Select one of the following:

    41. Manage monitored message queues                   WRKMQMM
    42. Start message queue monitor job                   STRSLMON *MSGMON
    43. End message queue monitor job                     ENDSLMON *MSGMON
```

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

3.12.1 Configure the global message queue monitoring settings

The Configure MSG Queue Monitor command sets the global parameter for the message queue monitor. You can monitor different message queues and if a message meets the monitoring criteria (severity, message queue name, enabled status), an event is generated and send to the configured syslog server.

The syslog facility and severity of message events are as follows:

- Facility is always USER
- Severity depends on the IBM i message severity itself.
  - Message severity 00 is sent with syslog severity INFO
  - Message severity 10 is sent with syslog severity NOTICE
  - Message severity 20 is sent with syslog severity WARNING
  - Message severity greater equal 30 is sent with syslog severity ERROR

```
                    Configure MSG Queue Monitor   (CFGSLMQM)

 Type choices, press Enter.

 MSGQ Monitoring On/Off . . . . .   Y             Y=On, N=Off
 Monitor Interval . . . . . . . .   180           180-7200 Seconds
 Message Retention Days . . . . .   2             0-9 Days
 Monitor Messages MSGQ  . . . . .   SLMSGQ        MSGQ Name
   Library  . . . . . . . . . . .     QZRDSYSLOG  Library (not *LIBL,*CURLIB)

                                                                        Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
MA+   A                                                                 06/037
```

The configuration parameter for the global settings are as follows:

- MSGQ Monitoring On/Off
  This parameter specifies whether the message queue monitor starts when the subsystem SLSBS starts. If the parameter is set to *YES and the job has not been started yet, the SLMSGQMON job is started in the SLSBS subsystem.
  - **Y**
    The Y specifies that the message message queue monitor is started if it is not already running and will be started again when the subsystem starts the next time.
  - **N**
    The value N specifies that the message queue monitor ends after the next processing interval and will not be restarted when the subsystem SLSBS will be started again.
- Monitor Interval
  This parameter specifies the interval in number of seconds how often the monitored message queues are analyzed for new messages.
  - number
    Specify the number of seconds for the monitor interval. The range of valid values are between 180 and 7200 seconds.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

- Message Retention Days
  This parameter specifies the number of days that messages that are retrieved from monitored message queues are kept in a database table.
  - number
    Number of days how long processed messages are kept in the Syslog Reporting Manager tool. The range of valid values are 0 to 9 days. 0 indicates that messages that are retrieved from monitored messages queues are removed after they have been processed and sent to the configured syslog server.
- Monitor Messages MSGQ
  This parameter specifies the message queue library and name of a message queue that receives messages related to jobs and messages that are processed by the message queue monitoring function.
  - QZRDSECSRM/SLMSGQ
    The default is the SLMSGQ message queue.
  - name
    You can also specify a different message queue that will receive message related to the message queue monitoring process.

  Information: Direct access via command: CFGSLMQM

3.12.2 Defining message queues to be monitored

Option 41 lets you manage the message queues that you want the Syslog Reporting Manager to monitor.

```
26.02.21                    Work with MSGQs to Monitor                    10:55:57

Position to  . . .    __________   ( MSGQ Name )

Type options, press Enter.
 2=Edit  4=Delete  5=Display  9=Send MSGs Status Toggle
                                                                  MIN  Send
Opt MSGQ Name  Library    ASP Name   UF MF TF                     SEV  MSG's
 _  BARLEN     QUSRSYS    *SYSTEM     *     *                      10  *YES
 _  SLMSGQ     QZRDSECSRM *SYSTEM     *  *  *                      40  *YES

                                                                     Bottom

F1=Help  F3=Exit  F5=Refresh  F6=Add MSGQ  F8=Turn ALL On/Off

MA +  B                  MW                                          09/003
```

The Work with MSGQs to monitor command lets you define all message queues that you want to monitor. All enabled message queues that meet the minimum severity level, <the configured user profile filter, message identifier filter, and message type filter> are monitored and an event is generated.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

The list contains all message queues that you want to monitor. If a message is received on a monitored message queue that meets the configured filter criteria and is set as *YES for the Send MSGQ option, a syslog event is generated and sent to the configured syslog server. Note that the F8 function key will toggle between *YES and *NO for the Send MSGQs option for all listed message queues.

<The filter type columns indicate whether certain filters have been defined for the listed message queue:

- UF – A user profile filter has been defined when a * is displayed
- MF – A message identifer filter has been defined when a * is displayed
- TF – A message type filter has been defined when a * is displayed>

Information: Direct access via command: WRKMQMM

3.12.3 Starting the message queue monitor

You can start the message queue monitor with option 42 of the SLMON menu.

Information: Direct access via command: STRSLMON MONJOB(*MSGMON)

3.12.4 Ending the message queue monitor

You can end the message queue monitor with option 43 of the SLMON menu.

Information: Direct access via command: ENDSLMON MONJOB(*MSGMON)

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

3.13 Sending custom events

Custom events are events that are generated by user applications and not the operating system or the Syslog Reporting Manager itself. Examples could be:

- You have created your own monitor tool for a message queue and want to forward specific messages as a SIEM event to the remote SIEM server.
- You want to send specific events that occurred in your business application to the SIEM server.

Permissions required:

To be able to use the SNDEVT command, the user should be granted *USE access to the following two objects:

QZRDSECSRM/SNDEVT *CMD

QZRDSECSRM/SNDEVTP *PGM

Two different methods can be used to send custom events:

1. There is a `SNDEVT` CL command to send a custom event.
2. You can use the `sendCustomEvent` or `sendCustomFmtEvent` procedures in your ILE program to send custom events.

The following two sections describe more details about each method.

The CL command as well as the procedures can also be used in different ways. The major difference is that one method requires you to specify more information about the source (sending) job and user and the command/procedure will format the SIEM message completely for you or the second method, which gives you the freedom to create your own key-value pairs as expected by the SIEM server. In the latter case you are fully responsible to use the correct key names and also format the values according to the CEF or LEEF specifications.

Custom messages are sent as follows:

<u>Method 1: Proving source user and qualified job name</u>

The following information must be provided in the CL command or procedure sendCustomEvent:

- Syslog facility (used in the syslog header)
  Valid values are: `KERNEL, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CLOCK, AUTHPRIV, LOGAUDIT, LOGALERT, CRON, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7`
  For more information regarding syslog facilities, refer to the specifications of RFC3164 or RFC5424.
- Syslog severity (used in the syslog header)
  Valid values are: `EMERG, ALERT, CRIT, ERROR, WARNING, NOTICE, INFO, DEBUG`
  For more information regarding syslog severities, refer to the specifications of RFC3164 or RFC5424.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

- Timestamp information for the event (can be either the value *CURTIME in which case the syslog header timestamp is the date/time of when the command/procedure was run or it can be a custom provided timestamp in ISO format YYYY-MM-DD-HH.MM.SS.mmmmmm.
- A SIEM header value that will be added to the SIEM header. Depending on the chosen SIEM format, the value is placed as follows:
  - CEF – value added in the NAME field of CEF header
  - LEEF – value added in the EventID field of the LEEF header after the valued CUSEVT-
- Source user profile name
  This is the IBM i user profile name of the user that will be sent as the origin of the event. The user profile name can also be *CURUSER in which case the source user is the user who performs the SNDEVT command or calls the corresponding procedure.
  SIEM payload key:
  CEF: suser
  LEEF: usrName
- Qualified source job name
  A custom provided job name in the format JOBNUMBER/JOBUSER/JOBNAME (i.e. 329701/BARLEN/QPADEV0002) that identifies the job that triggered the event or the special value *CURJOB which uses the job name of the job that performs the SNDEVT command or calls the corresponding procedure.
  SIEM payload key:
  CEF: sproc
  LEEF: sproc
- Event category
  Sources of SIEM evens are often grouped in categories. This parameter lets you specify a category value for your custom event.
  SIEM payload key:
  CEF: cat
  LEEF: cat
- Event text
  This is the actual event message text you want to send.
  SIEM payload key:
  CEF: msg
  LEEF: msg
- Note: your source host will automatically be added by the custom send function. This is not a parameter you can specifiy:
  SIEM payload key:
  CEF: shost
  LEEF: resource

Method 2: Format the custom event payload yourself

The following information must be provided in the CL command or procedure sendCustomEvent:

- Syslog facility (used in the syslog header)
  Valid values are: `KERNEL, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CLOCK, AUTHPRIV, LOGAUDIT, LOGALERT, CRON, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6,`

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

`LOCAL7`

For more information regarding syslog facilities, refer to the specifications of RFC3164 or RFC5424.

- Syslog severity (used in the syslog header)
  Valid values are: `EMERG, ALERT, CRIT, ERROR, WARNING, NOTICE, INFO, DEBUG`

  For more information regarding syslog severities, refer to the specifications of RFC3164 or RFC5424.
- Timestamp information for the event (can be either the value *CURTIME in which case the syslog header timestamp is the date/time of when the command/procedure was run or it can be a custom provided timestamp in ISO format YYYY-MM-DD-HH.MM.SS.mmmmmm.
- A SIEM header value that will be added to the SIEM header. Depending on the chosen SIEM format, the value is placed as follows:
  - CEF – value added in the NAME field of CEF header
  - LEEF – value added in the EventID field of the LEEF header after the valued CUSEVT-
- Note: if your source your source host has not been added by yourself, it will automatically be added by the custom send function :
  SIEM payload key:
  CEF: shost
  LEEF: resource
- Event text
  This parameter contains all the key-value pairs that you provide. It is the responsibility of the user to specify all required keys and their values as expected by the SIEM server. The custom send event function does not perform any syntax checking or escaping of reserved characters.
  SIEM payload key:
  CEF: does not apply, provided by user
  LEEF: does not apply, provided by user

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

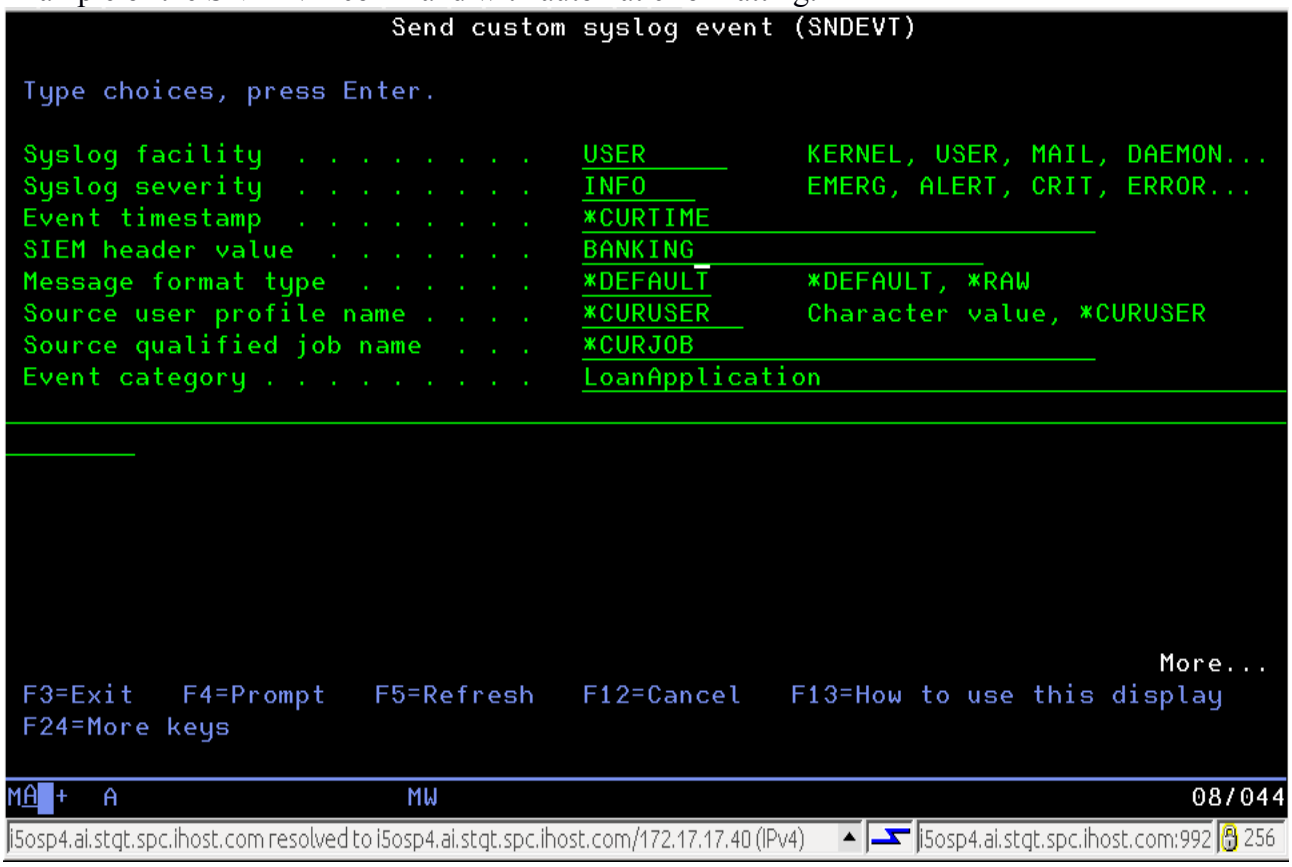
3.13.1 Sending custom events with the SNDEVT commands

If you need to send custom events occasionally, the Send Event (SNDEVT) command has been created for that.

You can use the command in the two ways described in the previous section. Which way you use is selected in the Message format type (MSGTYPE) parameter:

- *DEFAULT – automatic formatting is done and the event text is sent with the msg key-value
- *RAW – own formatting. All key-value pairs for the SIEM payload need to be provided by the user.

Example of the SNDEVT command with automatic formatting:



© Copyright 2018, 2021 IBM Corp. All Rights Reserved

Second page of command:

```
                    Send custom syslog event (SNDEVT)

 Type choices, press Enter.

 Event text . . . . . . . . . . .   Primary account 123334 deleted by user JDOE.
                                                                          ...

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

MA+  A                  MW                                              05/037
i5osp4.ai.stqt.spc.ihost.com resolved to i5osp4.ai.stqt.spc.ihost.com/172.17.17.40 (IPv4)  i5osp4.ai.stqt.spc.ihost.com:992  256
```

Example of the command with own formatting:

```
                    Send custom syslog event (SNDEVT)

 Type choices, press Enter.

 Syslog facility  . . . . . . . .   USER        KERNEL, USER, MAIL, DAEMON...
 Syslog severity  . . . . . . . .   INFO        EMERG, ALERT, CRIT, ERROR...
 Event timestamp  . . . . . . . .   *CURTIME
 SIEM header value  . . . . . . . > BANKING
 Message format type  . . . . . . > *RAW        *DEFAULT, *RAW
 Event text . . . . . . . . . . . > cat=Loan application suser=BLC11 sproc=21213
3/BLC11/ACCTMGT msg=Primry account 123334 deleted by user JDOE. src=172.1.4.22 c
s1Label=ACCTNO cs1=123334
                                                                          ...

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

MA+  A                  MW                                              12/026
i5osp4.ai.stqt.spc.ihost.com resolved to i5osp4.ai.stqt.spc.ihost.com/172.17.17.40 (IPv4)  i5osp4.ai.stqt.spc.ihost.com:992  256
```

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

3.13.2 Sending custom events with ILE procedures

The send custom event ILE procedures that are provided with the Syslog Reporting Manager have the following parameter structures:

Parameter	Type	Used in sendCustomEvent procedure	Used in sendCustomFmtEvent procedure
Syslog Facility	CHAR(9) IN	YES	YES
Syslog Severity	CHAR(7) IN	YES	YES
Timestamp value	CHAR(26) IN	YES	YES
SIEM header	CHAR(20) IN	YES	YES
Source user	CHAR(10) IN	YES	NO
Source job	CHAR(28) IN	YES	NO
Event category	CHAR(100) IN	YES	NO
Event text *1	CHAR(2048) IN	YES	YES
Reserved (*2)	CHAR(33) IN	NO	NO
Return code from proc	INT(5)	YES	YES

*1 = See the description of the parameter in the introduction of this chapter. For the sendCustomFmtEvent procedure, the parameter contains all key-value pairs that are provided by the programmer.
*2 = Parameter can be omitted

Procedure prototypes:

```
//-----------------------------------------------------------------------
//Declarations and prototypes for sending a custom event where the
//provided parameter are sent as follows:
//evtHdrSuffix - in the LEEF or CEF header (see intro)
//evtSrcUser - send as suser (CEF) or usrName (LEEF) attribute in the
//             payload
//evtSrcJob  - send as the sproc key in the payload
//evtCategory - send as the cat key in the payload
//evtText    - send as the msg key in the payload
//Formatted means that all key value pairs in the payload of a CEF or
//LEEF message must be set by the caller of the procedure.
//-----------------------------------------------------------------------
 dcl-pr   sendCustomEvent  int(5);
    syslogFacility     char(9) value; //Facility (see intro section)
    syslogSeverity     char(7) value; //Severity (see intro section)
    evtTimestamp       char(26) value;//Event timestamp(see intro section
    evtHdrSuffix       char(20) value;//SIEM header suffix (see intro)
    evtSrcUser         char(10) value;//Source user profile of event
    evtSrcJob          char(28) value;//Qualified job name of sending job
    evtCategory        char(100) value;//event category (see intro)
    evtText            char(2048) value;//Event data (see intro)
    evtSpc             char(33) options(*nopass); //Reserved
 end-pr;
```

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

```
//-----------------------------------------------------------------------
//Declarations and prototypes for sending a formatted event text
//Formatted means that all key value pairs in the payload of a CEF or
//LEEF message must be set by the caller of the procedure.
//-----------------------------------------------------------------------
 dcl-pr   sendCustomFmtEvent  int(5);
    syslogFacility     char(9) value; //Facility (see intro section)
    syslogSeverity     char(7) value; //Severity (see intro section)
    evtTimestamp       char(26) value;//Event timestamp(see intro section
    evtHdrSuffix       char(20) value;//SIEM header suffix (see intro)
    evtText            char(2048) value;//Event data (see intro)
    evtSpc             char(33) options(*nopass); //Reserved

 end-pr;
```

Coding and compilation information

The library QZRDSECSRM contains the following objects that you need when using the custom procedures.

QZRDSECSRM/SRMBND *BNDDIR

The following source file contains a program with an example on how to call the send custom event procedures.

QZRDSECSRM/SOURCES *FILE
Member: SNDEVT *RPGLE

After you created the module for your program, use the following command to create the program itself:

```
CRTPGM PGM(MYLIB/SNDMYEVT) BNDDIR(QZRDSECSRM/SRMBND)
```

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

3.14 Starting and ending the Syslog Reporting Manager

The tool can be started with the Start Syslog Reporting Manager (STRSRM) command. The command performs the following tasks:

- Check if the Syslog Reporting Manager is already active, if it is check also that the control job is running. If the subsystem is running, but the control job is missing, the start process will restart the subsystem.
- Start the subsystem SLSBS.

The tool can be ended with the End Syslog Reporting Manager (ENDSRM) command. The command performs the following tasks:

- Ends the automatic restart process of the control job.
- Ends all monitor jobs
- Ends all send event jobs
- Ends the SLSBS subsystem

3.15 Autostarting the Syslog Reporting Manager at IPL

All jobs related to the Syslog Reporting Manager run in the SLSBS subsystem. This subsystem has an autostart job which will automatically start all event monitor jobs that have been set to autostart *YES.

To start the Syslog Reporting Manager job environment at IPL, add the following command to your IBM i startup program that is defined in system value QSTRUPPGM.

```
QZRDSECSRM/STRSRM
```

Also grant the user who runs the startup program, usually QPGMR, *USE access to the command and command program. Example:

```
GRTOBJAUT OBJ(QZRDSECSRM/STRSRMP) OBJTYPE(*PGM) USER(QPGMR) AUT(*USE)
GRTOBJAUT OBJ(QZRDSECSRM/STRSRM) OBJTYPE(*CMD) USER(QPGMR) AUT(*USE)
```

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

3.16 Exporting and importing configuration settings

The Syslog Reporting Manager provides export and import functions to save your configuration settings and restore them when needed. The export function can be used to create a backup of your SRM configuration. The saved configuration can also be used to import the configuration on a different system. That way, you only need to create the configuration once and can then distribute it to other systems you want to monitor.

3.16.1 Exporting the configuration

The export operation saves the following configuration:

- The global configuration:
  - Hostname or IP address of the primary and backup syslog server
  - Port number of remote syslog server
  - Syslog message tag
  - Starting journal time stamp
  - Syslog format (RFC3164 or RFC5424)
  - Transport protocol (TCP or UDP)
  - Maximum message length
  - SIEM message format (CEF or LEEF)
  - Autostart options for event monitor jobs
  - EOF delays for history and audit monitoring
  - Syslog severity used for all IFS file change events
  - Syslog facility used for all IFS file change event messages
  - Event statistics and reporting option
  - TCP message transfer method
  - Number of send event job
  - >Certificate path validation
  - Peer certificate check for primary syslog server
  - Wildcard certificate check for primary syslog server
  - Peer certificate check for backup syslog server
  - Wildcard certificate check for backup syslog server<
- Audit journal monitor specific configuration
  - Audit journal entry type monitoring status
- History log monitor specific configuration
  - History filter selection definitions
- IFS file monitor specific configuration
  - A list of all IFS files that are currently monitored
- Message queue monitor configuration
  - List of message queues to be monitored
- Database change monitor configuration for the Journal Extract Tool integration
  - Global settings related to the interval and processing options for processing Journal Extract Tool tasks
  - Reporting levels related to tables registered in the Journal Extract Tool
  - Processing status of the journals that are registered in the Journal Extract Tool
- Special configuration settings

Perform the following steps to export the configuration:

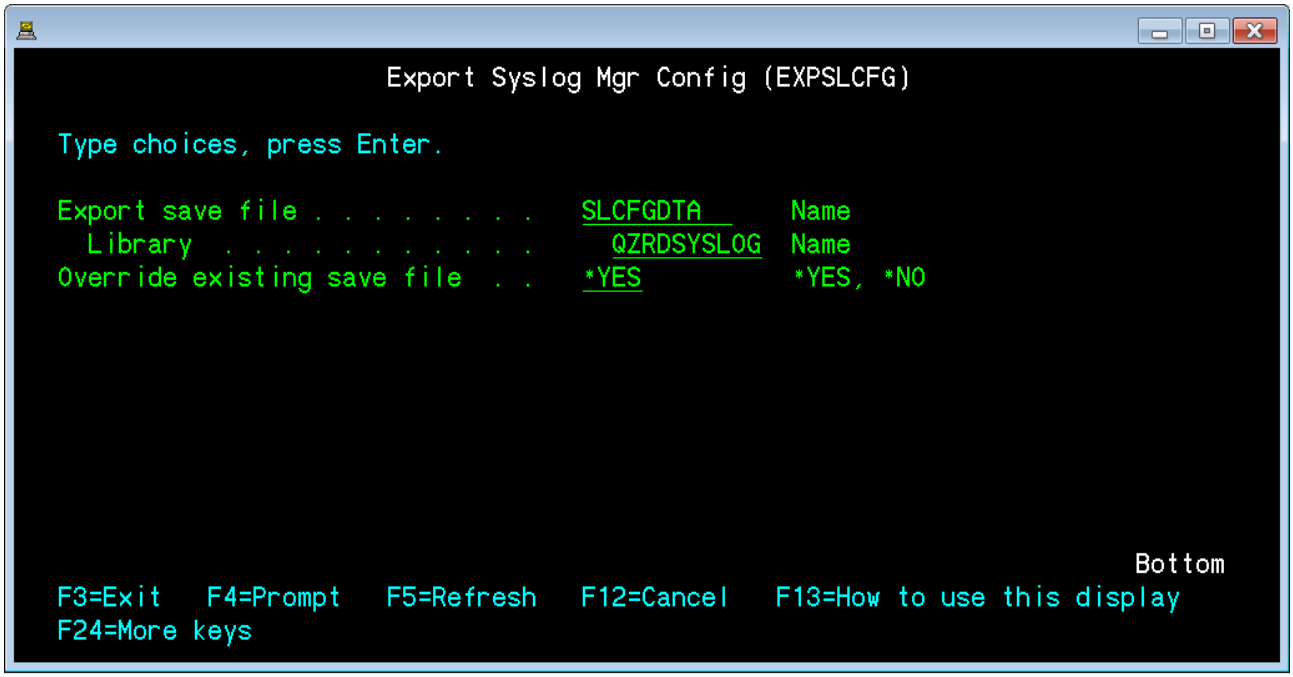
© Copyright 2018, 2021 IBM Corp. All Rights Reserved

1. Sign on with the SRM administrator and make sure library QZRDSECSRM has been added to the library list.

2. Open the SLMON menu (CFGSRM) and use option 70 (Export configuration) to start the export process.

   Information: Direct access via command: EXPSLCFG

   The exported configuration is saved into a save file. By default, the save file is QZRDSECSRM/SLCFGDTA.



   If you previously exported the configuration and the save file already contains data, you can leave the override parameter at *YES. This will clear the save file before saving the configuration data.

3. Press **Enter** to export the configuration.

You can now keep the save file as a backup of your configuration or transfer the save file to another system to be used for an import operation.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

3.16.2 Importing the configuration

The import configuration process requires that you have the save file that was created by the export configuration process. Perform the following to import the SRM configuration:

1. Sign on with the SRM administrator and make sure library QZRDSECSRM has been added to the library list.
2. Open the SLMON menu (CFGSRM) and use option 71 (Import configuration) to start the import process.

   Information: Direct access via command: IMPSLCFG

```
                        Import Syslog Mgr Config (IMPSLCFG)

 Type choices, press Enter.

 Import save file . . . . . . . .   SLCFGDTA      Name
   Library  . . . . . . . . . . .     QZRDSYSLOG  Name
 Backup old configuration . . . .   *YES          *YES, *NO
 Global configuration . . . . . .   *IMPORT       *IMPORT, *NONE
 Audit journal monitor config . .   *IMPORT       *IMPORT, *NONE
 IFS file monitor config  . . . .   *IMPORT       *IMPORT, *NONE
 History log monitor config . . .   *IMPORT       *IMPORT, *NONE, *APPEND
 MSG queue monitor config . . . .   *IMPORT       *IMPORT, *NONE
 DB change monitor config . . . .   *IMPORT       *IMPORT, *NONE

                              Additional Parameters

 Restore special settings . . . .   *NONE         *IMPORT, *NONE


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

MA+   B                                                              05/037
```

Important information for Journal Extract Tool configuration data:

The import process adds all exported table and process journal entries to the corresponding Syslog Reporting Manager tables. However, if the actual tables or journals are not defined in the AUDITOBJ or PROCTRACK tables of the Journal Extract Tool, the entries get deleted from the Syslog Reporting Manager integration tables.

- Specify the library and name of the save file that has been created by the export configuration process.
- By default, the import process will save the current configuration prior to importing the new configuration. The configuration is saved into save file QZRDSECSRM/IMPBACKUP.
- Specify whether you want to import (`*IMPORT`) the following configuration values:
  - Hostname or IP address of the primary and backup syslog server
  - Port number of remote syslog server
  - Syslog message tag
  - Starting journal time stamp
  - Syslog format (RFC3164 or RFC5424)
  - >Transport protocol (TCP, UDP, or TLS)<

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

- Maximum message length
- SIEM message format (CEF or LEEF)
- Autostart options for event monitor jobs
- EOF delays for history and audit monitoring
- Syslog severity used for all IFS file change events
- Syslog facility used for all IFS file change event messages
- Status whether you want statistical events to be sent
- TCP message transfer method
- Number of send event jobs
- >Certificate path validation
- Peer certificate check for primary syslog server
- Wildcard certificate check for primary syslog server
- Peer certificate check for backup syslog server
- Wildcard certificate check for backup syslog server<

NOTE: The `*IMPORT` option will override all existing values.

- Specify whether you want to import (`*IMPORT`) the following audit journal event configuration values:

  - Audit journal entry type monitoring status. The monitoring status determines what journal entry types will be monitored.

  NOTE: The `*IMPORT` option will override all existing values.

- Specify whether you want to import (`*IMPORT`) the IFS file names that have been actively monitored on the system where the export operation was performed:

  - For IFS files that have been monitored on the system where the export was performed, the import process will try to add all IFS file names to the monitor list. In fact, the files will be added to be journaled by the IFSJRN journal. If a file is already monitored or the file does not exist, the IFS file is skipped.

- >Specify whether you want to import (`*IMPORT`) the following message queue monitoring configuration values:

  - Global configuration values about the collection and reporting interval, the number of days that messages are kept on the system, and the message queue that the message queue monitor process used.
  - The list of message queues that are monitored by the message queue monitoring process.

  NOTE: The `*IMPORT` option will override all existing values.

- Specify whether you want to import (`*IMPORT`) the following database change monitoring configuration values:

  - Global configuration values:
    - Enable DB event processing

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

        - Global syslog information level
        - Journal processing interval
        - Drop tables before processing
        - Clear data tables before processing
        - Clean up non-existing objects
    - The list of tables that have been defined for database journal processing
      Note: If a journal has not been added to the AUDITOBJ Journal Extract Tool table prior to running the import, the entries are not imported.
    - The list of journals that will be processed
      Note: If a journal has not been added to the PROCTRACK Journal Extract Tool table prior to running the import, the entries are not imported.

      NOTE: The `*IMPORT` option will override all existing values.<

- Specify the import operation for special function settings. Besides not importing values (option `*NONE`) you can specify the following additional option:

    - **`*IMPORT`**

      The value specifies that the special function configuration will be imported. All existing function settings will be overridden.

3. Press **Enter** to start the import process.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

4 Managing the job environment

As previously stated, it is recommended to automatically start the subsystem QZRDSECSRM/SLSBS at IPL time via the system startup program. During the subsystem start, the control monitor job will start all event monitor jobs that have specified *YES for the autostart parameter.

If all jobs are running, the WRKACTJOB SBS(SLSBS) command output looks like the following:

```
                              Work with Active Jobs                        COMEUR1
                                                          25.09.20  15:18:14 CEST
CPU %:       .8      Elapsed time:    06:27:49      Active jobs:    207

Type options, press Enter.
  2=Change    3=Hold    4=End    5=Work with    6=Release    7=Display message
  8=Work with spooled files    13=Disconnect ...
                      Current
Opt  Subsystem/Job    User         Type   CPU %   Function         Status
__   SLSBS            QSYS         SBS       .0                     DEQW
__     SLAUDMON       QZRDSLOWN    BCH       .0   PGM-SYSLOGAUD     TIMW
__     SLAUDMONU      QZRDSLOWN    BCH       .0   PGM-SYSLOGAUDU    TIMW
__     SLHSTMON       QZRDSLOWN    BCH       .0   PGM-SYSLOGHST     SIGW
__     SLIFSMON01     QZRDSLOWN    BCH       .0   PGM-SYSLOGIFSC    TIMW
__     SLMONSTR       QZRDSLOWN    ASJ       .0                     DEQW
__     SLMSGQMON      QZRDSLOWN    ASJ       .0   DLY-120           DLYW
__     SLSNDEVT1      QZRDSLOWN    BCH       .0   PGM-SNDSYSL       DEQA
__     SLSNDEVT2      QZRDSLOWN    BCH       .0   PGM-SNDSYSL       DEQA
                                                                          More...
Parameters or command
===>
F3=Exit    F5=Refresh        F7=Find       F10=Restart statistics
F11=Display elapsed data    F12=Cancel    F23=More options    F24=More keys

MA    G                                                                  10/002
```

The purpose of each job is:

Job name	Description
SLAUDMON	Audit journal event monitor job. It retrieves all operating system provided audit journal entry types (journal code T) that have been enabled with the CFGSLAUD command and sends the CEF- or LEEF-formatted syslog messages to the specified syslog server.
>SLAUDMONU	Audit journal event monitor job. It retrieves all user generated audit journal entry types (journal code U) that have been enabled with the CFGSLAUD command and sends the CEF- or LEEF-formatted syslog messages to the specified syslog server. If no event types of source event category *USR have been enabled, the monitor job automatically ends and needs to be manually restarted when user type entries are added and enabled for processing. Note: There are two different underlying programs that handle user type entries. In IBM i 7.2 the program SYSLOGAU2U is used and starting from IBM i 7.3 the program SYSLOGAUDU is used. <
SLHSTMON	QHST history log event monitor job. It retrieves all history log entries that have been enabled with the CFGSLHST command and sends the CEF- or LEEF-formatted syslog messages to the specified syslog server. If no history log selection rule is enabled, all received history log events are processed.
>SLIFSMONnn	IFS file change monitor job. The IFS file change monitoring is using the configured and enabled journals to feed the monitor job. Every IFS file that needs to be monitored for changes, are added to be journaled via one of the configured ournals. The command to configure the IFS file monitoring is CFGSLIFSJ (managing journals) and CFGSLIFS (managing monitored files for a selected journal).

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

	A separate job is started for each configured and enabled journal.<
SLMONSTR	This is the control monitor job that is auto-started when the subsystem SLSBS starts or by using the STRSRM command. It submits the event monitor jobs at startup for event monitor jobs that have specified autostart *YES. It also monitors all started jobs and if one event monitor job fails, it will restart the event monitor job. If an event monitor job is ended with the ENDSLMON command, job monitoring ends and no new event monitor job is submitted. The control monitor job also contains detailed messages about all event monitor job activities, such as restarting an event monitor job.
>SLSNDEVT1-9	This job is the communication job that processes events that were reported by the various monitor jobs. It establishes a communication via UDP/IP or TCP/IP or TLS (over TCP) to a configured syslog or SIEM server and sends the events to the remote host. There can be 1 to 9 of these send event jobs in subsystem SLSBS. The number of started send event jobs can be configured with the CFGSLENV command.<
SLMSGQMON	The SLMSGQMON job is the scheduling job of the message queue monitor part of the tool. It runs the analysis of the monitored message queues at the interval that is configured with the CFGSLMQM command. The analysis job name is SLMSQMONS and is also active in the SLSBS subsystem as long as the analysis lasts.
SLDB2MON	This job is started by the control monitor job at the interval defined in the CFGJSGLB command. It processes the database journal change events that have been collected by the Journal Extract Tool. This job is only active as long as the analysis lasts.

If a configuration command, such as CFGSLAUD command is used to change a configuration, the event monitor job is restarted to pick up the changed configuration.

4.1 Manually starting and stopping event monitor jobs

There are two commands that are used to manually start and stop event monitor jobs. Each command has three valid parameter values:

- ***AUDMON** Monitor job for audit journal event processing
- ***HSTMON** Monitor job for history log event processing
- ***IFSMON** Monitor job for IFS file change event processing
- ***MSGMON** Monitor job for message queue event processing
- >***SNDEVT** Restarts any missing send event jobs. The number of missing send event jobs is determined by actual number or active SLSNDEVTn jobs and the number of configured send event jobs.<

Starting

```
STRSLMON    MONJOB(*AUDMON)
```

Stopping

```
ENDSLMON    MONJOB(*AUDMON)
```

Note that the start and end process can take a while due to current processing activities or delays. All start and end requests are passed to the control monitor job and handled by this job.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

5 Special function settings

Starting with SRM V1R1M2, special function settings are supported. These settings are not configurable via regular configuration commands as they can have a significant impact on base functions of the tool. Wrong usage of such functions might cause the tool to not function properly. Currently, the following special functions are implemented:

- Disable ICMP connectivity check to the configured remote syslog/SIEM server.
- Adjust the maximum number of automatic job restart attempts for monitor jobs that fail.
- Sending the event timestamp in the syslog header and as part of the message payload opposed to the default behavior from SRM 1.2.0 that only sends the event timestamp as part of the syslog header and not the payload.
- Adjust the idle timeout value for TCP connections.
- Change the default delimiter character of key-value pairs in a LEEF message. The default is ASCII HEX 09 (TAB character) as defined in the LEEF specifications.
- Enabling debugging.
- Changing the timestamp of the last processed event for the various monitor jobs.
- Changing the time between job recovery attempts.
- >Changing the Digital Certificate Manager default client application name<

Contact your IBM Systems Lab Services contact to get instructions on how to change the listed properties.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

6 CEF and LEEF key mapping information

The following table shows the key names that are used for the various information units in a SIEM message in the Common Event Format (CEF) and Log Event Extended Format (LEEF). It also provides a short description of each element.
The information in the table lists the standard elements that are used by SRM audit, history, and IFS monitoring. The custom event message as used by the SNDEVT CL command or the sndevent* procedures might also use the keys but their use is up to the programmer who uses the command or procedures.

CEF key	LEEF key	Usage in Monitor	Description
act	act	IFS DB2	IFS: Device action that was carried out. This is a B_WA Write action. DB2: Contains the action that was performed on a database table (INSERT, DELETE, UPDATE)
cat	cat	CUS / MSG	CUS: Event category as provided in the raw message format of the custom event or the CAT parameter of the SNDEVT command. MSG: The message queue monitoring category "MSG Queue Messages".
cs1Label= changedData cs1=value	changedData	IFS	IFS: The actual data that has been changed in the monitored IFS file. Depending on the maximum message size that is allowed to be sent, the data in this value can be truncated. If truncation occurs, a corresponding text is added at the end of the value.
cs2Label= changedDataLength cs2=value	changedDataLength	IFS	IFS: Length in bytes of the data that was changed
cs3Label= changedDataPart cs3=value	changedDataPart	IFS	IFS: Depending on the size of the changed data in the monitored IFS file, the change can span one or more IFS journal entries. If it spans across multiple entries, the changedDataPart indicates if it is the first (*FIRST) packet of a change that spans multiple entries, if is is a part in the middle (*MIDDLE) of a change that spans multiple entries, if it is the last (*LAST) part of a change that spans multiple entries, or if is the only (*ONLY) part indicating that the entire change is provided in a single journal entry.
cs4Label= changedDataFileOffset cs4=value	changedDataFileOffset	IFS	IFS: Offset within the changed IFS file where the changed data start in the length as identified in changedDataLength.
deviceExternalId	deviceExternalId	AUD	AUD: Device name (extracted from ENTRY_DATA column)

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

CEF key	LEEF key	Usage in Monitor	Description
dloName	dloName	AUD	AUD: Document Library Object name (DLO_NAME column)
dloPath	dloPath	AUD	AUD: Document Library Object folder path (FOLDER_PATH column)
dproc	dproc	AUD	AUD: Destination job (process) name (extracted from ENTRY_DATA column)
duser	duser	AUD	AUD: Destination user name (extracted from ENTRY_DATA column)
filePath	filePath	AUD / IFS	AUD: IFS stream file path (PATH_NAME column) IFS: IFS stream file path of the file that has been changed.
fileType	fileType	AUD / IFS	AUD: Object type (OBJECT_TYPE column) IFS: Object type of IFS file path.
fname	fname	AUD DB2	AUD: IFS stream file name (OBJECT_FILE_NAME column) DB2: DB2 table name as monitored by the Journal Extract Tool.
msg	msg	HST / AUD / MSG	AUD: Additional information from the audit record not included in other keys (extracted from ENTRY_DATA column) HST: The message text (MESSAGE_TEXT column) from the history log message MSG: The message as received from the monitored message queue
cs1Label= objName & cs1=values	objName	AUD	AUD: Object name (OBJECT column)
oldDloName	oldDloName	AUD	AUD: Document Library Object name (before rename) (extracted from ENTRY_DATA column)
oldDloPath	oldDloPath	AUD	AUD: Document Library Object folder path (before rename) (extracted from ENTRY_DATA column)
oldFileName	oldFileName	AUD	AUD: FS stream file name (before rename) (extracted from ENTRY_DATA column)
oldFilePath	oldFilePath	AUD	AUD: IFS stream file path (before rename) (extracted from ENTRY_DATA column)
cs2Label= oldObjName	oldObjName	AUD	AUD: Object name (before rename) (extracted from ENTRY_DATA column)

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

CEF key	LEEF key	Usage in Monitor	Description
& cs2=values			
>cs7Label= attrName & cs7=value	attrName	AUD	AUD: Attribute name of the value that is changed. Used in the system audit entry types AU, EV, and IP.
cs8Label= attrValue & cs8=value	attrValue	AUD	AUD: Value of the attribute that is listed in the cs7Label=attrName/attrName keys. This key is used with system audit entry types AU and EV.
cs9Label= oldAttrValue & cs9=value	oldAttrValue	AUD	AUD: Contains the old value before the change of the attribute that is listed in the cs7Label=attrName/attrName keys. This key is used with system audit entry type AU.<
reason	reason	AUD / HST / CUS / MSG	AUD: Text description of the audit journal entry HST: Text description of the history log message CUS: In a custom event, reason contains the entire event text to be sent. MSG: The message ID of the monitored message.
rt (receiptTime)	devTimeFormat=YYYY-MM-dd-HH.mm.ss.SSSSSS devTime=	DB2 MSG	DB2: The timestamp of the time when the database change has occurred. The timestamp of the message in the monitored message queue.
shost	resource	AUD / IFS / DB2 / MSG	AUD: Source system (host) name (SYSTEM_NAME column) IFS: Source system (host) name DB2: Source system (host) name MSG: The hostname of the system where the monitored message was created. Note: The reported host name is the one as define with CHGNETA parameter SYSNAME.
sproc	sproc	AUD / HST / IFS / DB2 / MSG / CUS	AUD: Source job (process) name (JOB_NAME, JOB_USER, JOB_NUMBER columns) HST: The qualified job name (FROM_JOB column) from the history log message IFS: The qualified job name of the job that performed the IFS file change.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

CEF key	LEEF key	Usage in Monitor	Description
			DB2: The qualified job name of the job that performed the database table change. MSG: The qualified job name of the job that sent the message to the monitored message queue. CUS: If source job *CURJOB, the value contains the qualified job name of the job sending the event.
spt	srcPort	AUD	AUD: Source port number (REMOTE_PORT column)
src	src	AUD	AUD: Source IP address (REMOTE_ADDRESS column)
suser	usrName	AUD / HST / IFS / DB2 / MSG / CUS	AUD: Source user name (CURRENT_USER column) HST: Current user name (FROM_USER column) from the history log message IFS: Current user name from the user that performed the IFS file change. DB2: Current user name from the user that performed the database table change. MSG: The user profile name of the user who sent the message to the monitored message queue. CUS: If source user *CURUSER, the value contains the user profile name of the current user sending the event.
cs1Label=pgmName & cs1=value	pgmName	DB2	DB2: The name of the program that was used to perform the change in the monitored database table.
cs2Label=updatedColumnNames & cs2=values	updatedColumnNames	DB2	When an UPDATE action was performed on a monitored database table, the key value contains the names of the columns that have been updated.
cs3Label=memberName & cs3=values	memberName	DB2	When an INSERT or DELETE action was performed on a monitored database table, the key value contains the name of the database table member name that has been changed.
cs4Label=rowData & cs4=values	rowData	DB2	The key value contains all columns and their values including the Journal Extract Tool columns that identify the used journal receiver, sequence number, etc. of the rows that are added

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

CEF key	LEEF key	Usage in Monitor	Description
			(INSERT), deleted (DELETE), or for updates (UPDATE) where only the before or after image is captured.
cs4Label=rowDataAfter & cs4=values	rowDataAfter	DB2	The key value contains only the columns and their values of the data after the data has been changed for updates (UPDATE) where both the before and after image is captured.
cs5Label=rowDataBefore & cs5=values	rowDataBefore	DB2	The key value contains only the columns and their values of the data before the data has been changed for updates (UPDATE) where both the before and after image is captured.
cs1Label= msgSev & cs1=value	msgSev	MSG	The message severity text representation of the severity. The IBM i message severity is reported as follows: - Severity 0 as INFO - Severity 10 as NOTICE - Severity 20 as WARNING - Severity 30 and higher as ERROR
cs2Label= msgQueue & cs2=value	msgQueue	MSG	Library and name of the monitored message queue that contains the reported event.
cs3Label= pgmName & cs3=value	pgmName	MSG	The program that sent the message to the monitored message queue.
cs4Label= srdb & cs4=value	srdb	MSG	The relational database name of the system where the monitored message queue exists.

The "Usage in Monitor" column values specify:
AUD = Events that are monitored by the QAUDJRN audit journal
HST = Events that are monitored by the history log monitor
IFS = Events that are monitored by the IFS file change monitor
DB2 = Events that are generated by the DB2 Journal Extract Tool integration
MSG = Message queue monitoring events

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

7 Transport Layer Security (TLS) implementation information

>Since the reporting of syslog/SIEM events can also contain confidential and senstive information, the communication from the IBM i partition to the configured syslog server can be encrypted. If enabled, the communication is encrypted via the Transport Layer Security (TLS) protocol (see RFC5425).

7.1 Prerequisites

TLS encrypted communication is only working when the following prerequisites are met:

- The remote syslog server is configured to accept TLS-encrypted communication. The default port for TLS-encrypted traffic is 6514.
- The *SYSTEM certificate store must be created on the IBM i partition. See the IBM Docs (Knowledge Base) under Security→Digital Certificate Manager for information on how to set up and work with DCM.
- The Certificate Authority (CA) certificate(s) of the CA that issued the server certificate of the syslog/SIEM server must be imported into the *SYSTEM certificate store. The administrator of the syslog/SIEM server should be able to provide the CA certificates.
- The supported TLS protocols and cipher suites should be reviewed in the QSSLPCL and QSSLCSL system values. If necessary adjust the values. Note that the system values must contain a protocol, i.e. TLSV1.2 and a cipher suite, i.e. *RSA_AES_256_GCM_SHA384, that the remote syslog/SIEM server also supports. A TLS session can only be established when both sides support at least one common protocol and cipher suite.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

7.2 Enabling TLS encrypted communication

```
                    Configure Syslog Report Env (CFGSLENV)

 Type choices, press Enter.

 Hostname of Syslog server  . . .   'localhost'
 Hostname backup Syslog server  .   'centos.ai.stgt.SPC.ihost.com'
 Syslog server port number  . . .   6514          1-65535
 Syslog message tag . . . . . . .   *DEFAULT
 Starting journal time stamp  . .   *LASTPROC     *LASTPROC, *FIRST
 Specify Syslog format  . . . . .   RFC5424       RFC3164, RFC5424
 SIEM message format  . . . . . .   *CEF          *CEF, *LEEF
 Maximum message length . . . . .   8192          480-65535
 Send event statistics  . . . . .   *YES          *YES, *NO
 Number of send event jobs  . . .   1             1-9
 iASP group name  . . . . . . . .   *NONE         Character value, *NONE
 Transport protocol . . . . . . .   *TLS          *UDP, *TCP, *TLS
 TCP message transfer method  . .   *LF           *OCTCOUNT, *LF, *CR, *CRLF...
 Certificate path validation  . .   *YES          *YES, *NO
                                                                        More...
 F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
 F13=How to use this display        F24=More keys

MA  +   B                  MW                                          19/037
```

Encrypted communication is defined via the CFGSLENV command.

```
                    Configure Syslog Report Env (CFGSLENV)

 Type choices, press Enter.

 Peer certificate check prim. . .   'L=Ehningen,ST=Baden-Wuerttemberg,C=DE'
 Wildcard name primary  . . . . .   *HOSTDMN
 Peer certificate check bkup. . .   *WILDCARD
 Wildcard name backup . . . . . .   *HOSTDMN
```

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

First you need to specify *TLS in the Transport protocol (COMMTYPE) parameter. This triggers the SRM application QIBM_5ZRD_SRM application to be registered in the Digital Certificate Manager (DCM). It also switches to a secure encrypted channel. In addition, you can define the following TLS encryption related configuration parameter:

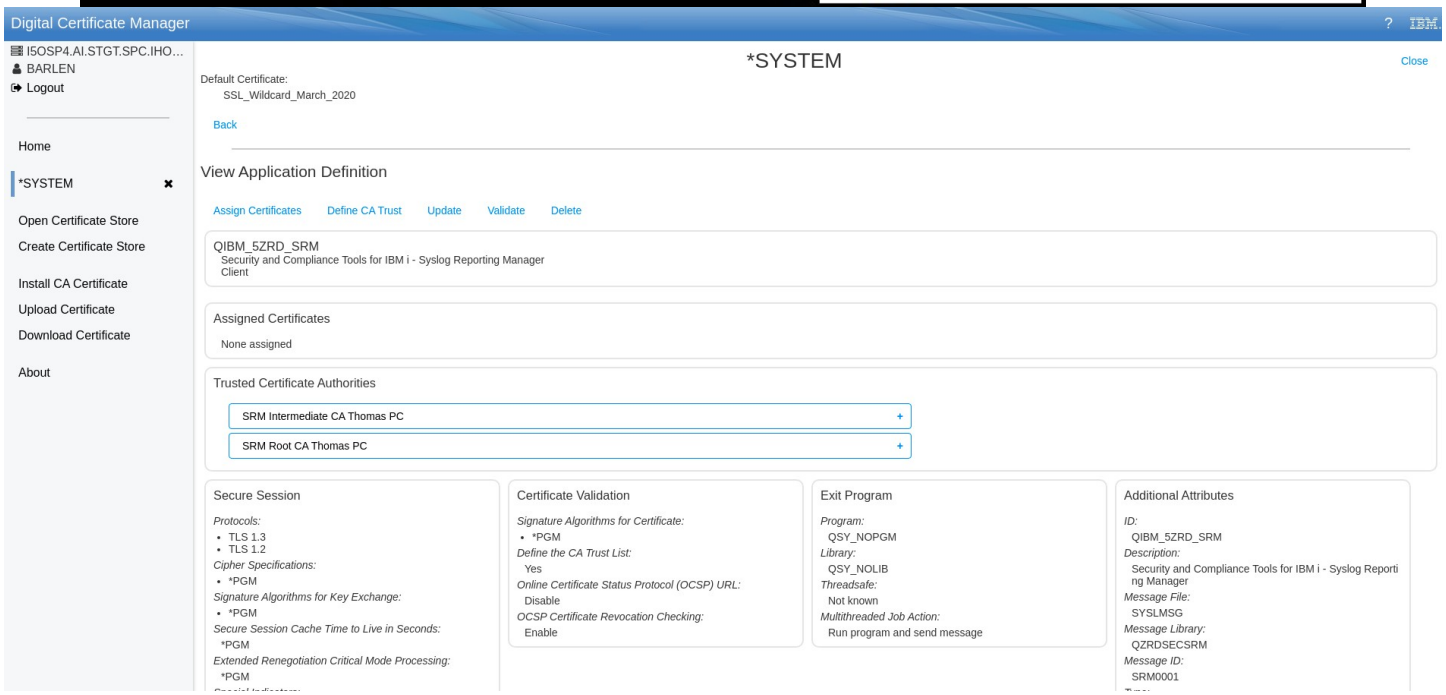
- Certificate path validation (CERTVLD)
  - This parameter specifies whether the certificate that is presented by the peer syslog server during a TLS handshake must succeed the following checks for a successful session initiation.
    - The peer certificate must be issued by a Certificate Authority (CA) that is trusted by the Syslog Reporting Manager (SRM) DCM application. If no application CA Trust List is configured, the issuer CA certificates must be in the DCM *SYSTEM store and must be enabled. If a CA Trust List is enabled in the SRM DCM application QIBM_5ZRD_SRM, the issuer CA certificate or certificate chain must be in the DCM application CA Trust List.
    - The certificate must not be expired.
  - For debugging purposes you can disable the previously listed checks. For added security, it is strongly recommended to enable this check.
- Peer certificate check for the primary and backup syslog server
  - This parameter specifies criteria to be used when checking the subject distinguished name (DN) of the peer X509 certificate that is presented by the syslog server when establishing a TLS-encrypted session. The check is optional. If value *ANY is used, no check is performed. If another value is used and the certificate's subject DN content does not match the configured criteria, the connection request is rejected and no connection is established.
- Wildcard name check for the primary and backup syslog server
  - This parameter specifies criteria to be used when checking the subject distinguished name (DN) of the peer X509 certificate when the certificate uses a wildcard common name (CN). A wildcard name example is *.mydomain.local. Such a certificate could be used by several servers that belong to the same TCP/IP domain.

Note that the online help of the CFGSLENV command provides detailed information about each configuration option.

7.3 Digital Certificate Manager integration

The Syslog Reporting Manager (SRM) tightly integrates with the Digital Certificate Manager (DCM). SRM is registered as a client application QIBM_5ZRD_SRM in DCM.
Note that DCM administration is outside the scope of this document. Consult the official IBM Knowledge Base / IBM Docs for your release to get more information about using DCM.
Note that the following screen capture shows the new DCM interface that was introduced in 2020.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved



When opening the *SYSTEM certificate store and selecting the option Manage Application Defintions, you find the application QIBM_5ZRD_SRM. You can then use DCM to configure the following options:

- CA Trust List
- Supported protocols
- Supported cipher specifications
- OCSP checking properties
- Timeout values <

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

8 Additional information

8.1 Working with event statistics

>The Syslog Reporting Manager has an option to collect information about the number of events that have been sent for the different monitor categories. You turn this option on by specifying *YES in the statistics configuration CFGSLSTAT EVTSTAT(*YES).

When statistics are turned on, you will get the following information:

- Every 24 hours you get a message in the QSYSOPR message queue, the history log, and an event sent to the configured remote syslog server about the number of events that have been sent for categories:
  - Audit journal entries (AUD)
  - History log events (HST)
  - IFS file changes (IFS)
  - Message queue monitor events (MSG)
  - Database journal events using the Journal Extract Tool (DB2)
  - Custom events (CUS)
  - Special events (SPC)
  - Syslog Reporting Manager tool events (SRM)
  - Number of total events sent (TotalCount)

  Example:

  ```
  <14>1 2020-04-30T08:02:08.674000+02:00 i5osp4.ai.stgt.spc.ihost.com
  IBMiPSCSRM  IBMSRM 102F5F - LEEF:2.0|IBM|IBM i|7.4|IBMSRM-SRMEVENTSTAT|
  x09|resource=i5osp4.ai.stgt.spc.ihost.com cat=SRM statistics msg=Syslog
  Reporting Manager processing statistics for sent events
  eventStatisticsDate=2020-04-29 AUD=988 HST=2961 IFS=21 MSG=127 DB2=0 CUS=0
  SPC=0 SRM=168 TotalCount=4265
  ```

  The statistics are kept in the tool by default for 7 days. You can change the number of days that SRM keeps the statistical data by using the CFGSLSTAT command.

  The following example shows how to change the number of days to 14 days:

  ```
  CFGSLSTAT RETDAYS(14)
  ```

  You can use SQL query the statistics. The following example is a SELECT statement that displays the sum for each event monitor category grouped by the send event job name:

  ```
  SELECT
  SOURCEJOB,SUM(STATAUD),SUM(STATHST),SUM(STATIFS),SUM(STATMSG)
  ,SUM(STATDB2),SUM(STATCUS),SUM(STATSPC),SUM(STATSRM),
  SUM(STATTOTAL)FROM slstat GROUP BY sourcejob ORDER BY
  sourcejob
  ```

Source job name	SUM (STATAUD)	SUM (STATHST)	SUM (STATIFS)	SUM (STATMSG)
SLSNDEVT1	289	1,209	27	32
SLSNDEVT2	251	1,223	31	25
SLSNDEVT3	223	1,230	33	31
SLSNDEVT4	219	1,290	55	25
SLSNDEVT5	237	1,237	43	21
SLSNDEVT6	218	1,292	22	17

  Note: The previous output shows only a part of the output for readability.

- A statistics event for database journal events using the Journal Extract Tool every time monitored journals have been processed. The event contains the number of summary and detailed events that have been processed and sent.

  Example:

  ```
  <14>1 2020-02-07T08:50:39.233000+01:00
  i5osp5.ai.stgt.spc.ihost.com IBMiPSCSRM IBMSRM 102F5F -
  ```

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

```
CEF:0|IBM|IBM i|7.3|IBMSRM|SRMDB2STAT1|5|
shost=i5osp5.ai.stgt.spc.ihost.com cat=SRM DB monitoring
msg=Syslog Reporting Manager DB monitoring journal processing
finished start=2020-05-01-08.50.35.670000 end=2020-05-01-
08.50.39.199000 cs1Label=numberSummaryEvents cs1=192772
cs2Label=numberDetailEvents cs2=82314
sproc=237125/QZRDSRMOWN/SLDB2MON
```

<

8.2 User-type audit journal entries

< IBM i sends events as entry code T entries to the system audit journal (QAUDJRN). User applications can also send their own events to the audit journal using the SNDJRNE command or equivalent Send Journal Entry (QJOSJRNE) API. These entries are marked with journal code U in the audit journal. Also IBM Systems Lab Services assets (tools) send audit events to the audit journal. The following tables list the events that Lab Services tools generate along with their layout.

Syslog Reporting Manager
Entry type: SL
Model output file: QZRDSECSRM/SRMAUDFMT

Offset Type 5	Field	Format	Description
1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" in the IBM i Security Reference for the format details.
608	SLSOURCE	CHAR(10)	User event source ID. For the Syslog Reporting Manager the value is always IBMLSSRM
618	SLRESULT Result	CHAR(10)	Result code from the operation reported by the Syslog Reporting Manager facility. The valid result codes are SUCCESS, ERROR, or INFO.
628	SLPROC Command	CHAR(10)	The command or facility name that generated the journal entry.
638	SLUSER User	CHAR(10)	The user profile name of the user who ran the command or facility reported in the Command column.
648	Reserved	CHAR(10)	Reserved area
658	Entry data	CHAR(2800)	Entry specific data. This is a free format text describing the event.

Network Firewall (Exit Point Security)

The Network Firewall is also a tool from IBM Systems Lab Services that can control access from remote clients via exit point programs. The tool also generated a series of user type audit journal events. The event types are pre-populated into the Syslog Reporting Manager and the description of the entries start with *IBM LS XPT*. If you use the tool, you can use the CFGSLAUD command to

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

enable the reporting of the individual event types. For a complete description of the event types, refer to the documentation of the Network Firewall tool.

8.3 Deleting the Syslog Reporting Manager

The Syslog Reporting Manager has been installed with the Restore Licence Program (RSTLICPGM) command. Likewise, when you want to delete the license program, you need to use the DLTLICPGM command. The following steps describe the tasks that need to be performed to completely remove SRM from the system.

1. End SRM with the **ENDSRM** command.
2. Verify that the subsystem SLSBS has ended with the **WRKACTJOB SBS(SLSBS)** command. The subsystem must be ended before proceeding with the next steps.
3. Check if group profile QZRDSRMGRP has any members.
   DSPUSRPRF USRPRF(QZRDSRMGRP) TYPE(*GRPMBR)
   If it does, remove all members.
4. Delete the license program.
   DLTLICPGM LICPGM(5ZRDSRM)
5. Delete the owner user profile **QZRDSRMOWN** with the DLTUSRPRF command.

<

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

9 Change History

This section describes the changes and enhancements of previous versions of the Syslog Reporting Manager.

9.1 Version 1.0 dated May 18th, 2018

Initial version of the tool.

9.2 Version 1.1 dated August 8th, 2018

Changes:

- Added option for IFS file changes that are greater than 32 KB. The administrator can now select whether data changes should be reported from the beginning of the changed content or from the end. In addition, if the change spans across multiple captured journal entries, the administrator can select if only the first entry, the last entry, or all entries are sent via syslog messages.
- The control monitor job in subsystem SLSBS has been changed to restrict the number of automatic restart operations for the audit, IFS file, and history log monitor jobs. An automatic restart usually occurs if a monitor job fails. The maximum number of automatic restarts for a failing monitor job is 10.
- The export and import configuration processes have been enhanced to backup and restore special configuration settings.
- The install process has been updated to migrate existing configuration data during an upgrade to a new version of the SRM tool.
- Various bug fixes.
- More extended help text.

9.3 Version 1.2 dated May 24th, 2019

Changes:

- Created a new communication module that acts as a central function to process all events that are generated by all monitoring jobs (i.e. SLAUDMON, SLIFSMON, SLHSTMON). All monitor jobs use now a data queue to store events to be processed. This new functionality increases performance and reliability. The new module has been developed from scratch as a native IBM i module. It eliminates the dependency on Java.
- The Syslog Message Tag (TAG) parameter in the CFGSLENV command has been changed to allow a special value of *DEFAULT. When the new value is used, the syslog header contains the following values according to the used RFC type:
  - RFC3164
    Tag: IBMiPSCSRM
  - RFC5424
    APP-NAME: IBMiPSCSRM
    PROCID: IFSMON or AUDMON or HSTMON or CUSEVT
    MSGID: IBMiEvent
- A new SIEM message format (MSGFMT) parameter as been added to the CFGSLMON command (SLMON menu option 2) that lets you select the syslog message payload format. It can be either *CEF (Common Event Format) or *LEEF (Log Event Extended Format).
- A new Maximum message length (MAXMSGLEN) parameter as been added to the CFGSLMON command (SLMON menu option 2) that lets you define the maximum length of a syslog message as sent over the network. Some syslog servers have restrictions on the maximum size of messages that they can process. The new parameter allows you to customize the message size according to the used syslog / SIEM server.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

  - Since the maximum message size is now flexible, the Truncate parameter for the RFC5424 RFC has been removed. During upgrade of to the new version, the MAXMSGLEN is set to 1024.
- A new Transport protocol (COMMTYPE) parameter as been added to the CFGSLMON command (SLMON menu option 2) that lets you select the IP protocol that is used when sending events to the syslog server. Initially, all messages had been sent over the User Datagram Protocol (UDP). You have now the choice to also select the Transmission Control Protocol (TCP).
- A new Hostname for backup syslog server (SERVER2) parameter as been added to the CFGSLMON command (SLMON menu option 2) that lets you specify a hostname or IP address of a backup syslog server if the primary server is not available.
- All events can now be formatted in Log Event Extended Format (LEEF) as supported as the standard format for the IBM QRADAR product.
- The first version of the Syslog Reporting Manager (SRM) appended the event to be sent to a regular syslog header. That means, the syslog server showed the syslog header plus another RFC-type specific header plus the CEF event data. In version 1.2.0 of SRM, the default behavior has been changed to be more in line with other products. The header that is generated, i.e. via the DISPLAY_JOURNAL function is actually used as the syslog header and the syslog server shows as the payload (message) just the CEF / LEEF data. Note if you select *SYSTIME as the Syslog Timestamp type in the CFGSLENV command, the syslog header contains the time when the event was sent and the payload still contains a timestamp of the time the event was originally be generated. If you depend on the old behavior, contact your IBM Systems Lab Services representative (or via the contact form at) who can help you sending events in the old format.
- A new function has been added to generate custom events. This feature can be used, for example, in an application to use the Syslog Reporting Manager framework to send events to the configured SIEM server. You can either use a CL command SNDEVT or use a provided service program and call procedures in ILE programs to send custom events.

9.4 Version 1.3 dated Jan. 25th, 2020

Changes:

- Added a value *SYSSRLNBR to the Syslog message tag (TAG) parameter of the CFGSLENV command. When specified, the serial number (DSPSYSVAL QSRLNBR) is added as a tag to the syslog header.
- Added a new parameter EVTSTAT to the CFGSLENV command. This parameter specifies whether the event send function will collect statistical counters for each type event that is sent to the remote syslog server. The statistics are also reported via message SLS0040 to the control message queue that is defined in the CFGSLMQM command. If turned on (*YES), the Syslog Reporting Manager sends a summary event after midnight or latest after 24 hours. The event has the following format:

```
cat=SRM statistics msg=Syslog Reporting Manager processing
statistics for sent events statStartTime=2019-09-25-
14.05.05.000000 statEndTime=2019-09-25-14.12.18.000000 AUD=10
HST=0 IFS=0 MSG=0 DB2=0 CUS=0 SRM=1 TotalCount=11
```

  The key-value pairs are as follows:
  - AUD – Number of audit journal events
  - HST – Number of history log events
  - IFS – Number of IFS file change events
  - MSG – Number of message queue monitoring events

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

  - DB2 – Number of database events captured by the IBM Systems Lab Services asset Journal Extract Tool.
  - SRM – Number of events generated by the Syslog Reporting Manager tool itself.
  - CUS – Number of custom events generated from user applications using the `sendCustomFmtEvent` or `sendCustomEvent` procedures or the `SNDEVT` CL command.
  - Total count of events sent during the reported timeframe.
  - The start timestamp of when the statistic starts.
  - The end timestamp of when the statistic ends.
- Important status messages from the Syslog Reporting Manager are also sent to the IBM i QHST history log. The following messages are sent to QHST:
  - SLS0009 - Monitoring for job &1 started.
  - SLE0019 - Syslog Reporting Manager control job has reached maximum job restart count for monitor job &2.
  - SLS0040 - Syslog Reporting Manager event statistics.
    Daily statistics about number of events sent for each category.
  - SLS0050 - Database change monitoring process completed. Second level text contains job statistics.
  - SLS0051 - Syslog Reporting Manager job &1 will be restarted.
    This message indicates when a monitor job gets restarted for cleanup purposes after 24 hours. The variable contains the job name that was restarted.

  The messages are listed in history filter QHST9999. If enabled, those messages are monitored by the SLHSTMON job and reported to the remote syslog/SIEM server.
  Note: The history filter QHST9999 is only added to new installations. It will not be added when upgrading from a previous version.

- All monitor jobs (SLAUDMON, SLIFSMON, SLHSTMON) and the event send job SLSNDEVT are now restarted every 12 hours to perform some job environment cleanup tasks.

- The default logging level in the SLJOBD job description has been changed to LOG(0 00 *SECLVL) . Therefore no messages are logged in any of the Syslog Reporting Manager jobs anymore.

- IBM Systems Lab Services also offers an asset (tool) called Journal Extract Tool. This tool can be used to monitor database table changes. By default, the tool creates tables with the reported changes of the monitored database tables. The Syslog Reporting Manager (SRM) has been enhanced to analyze the data that is generated by the Journal Extract Tool and send the database changes as Syslog messages (in either CEF or LEEF format) to the configured remote Syslog/SIEM server. The enhancements also provide more convenient configuration interfaces to set up and operate the Journal Extract Tool. All configuration options can be accessed from the SLMON menu.
  Note: To be able to use this new enhancement, you need to purchase the Syslog Reporting Manager and the Journal Extract Tool. These are two independent tools. For more information contact IBM Systems Lab Services at:
  https://www-03.ibm.com/systems/campaignmail/services/labservices/contact.html

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

- Another enhancement of this Syslog Reporting Manager (SRM) version is the ability to monitor message queues. You can configure the SRM to monitor one more message queues and report the messages to the configured remote Syslog/SIEM server.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

9.5 Version 1.4 dated Sep. 30th, 2020

Changes:

- New commands STRSRM and ENDSRM have been added to start and end the Syslog Reporting Manager in a controlled manner.
- A new command CFGSRM has been added to open the main configuration menu.
- The control job SLMONSTR has been enhanced to better handle errors in the send event jobs (SLSNDEVT). Especially in situations where a communication could not be established with a configured syslog / SIEM server, the control job tried 10 times to restart the job. When the connection could still not be established, no events would be sent and the Syslog Reporting Manager would not retry the send process. With this version, the control job will to restart the send event communication jobs after 10 minutes.
  In addition, if the control job SLMONSTR itself fails, it will automatically be restarted along with all monitor jobs to ensure a consistent state of the tool.
- If the audit monitor, history log monitor, or IFS file monitor ended abnormally or a user has ended the job with the ENDJOB command, the SLMONSTR control job tried 10 times (default) to restart the job. If the restart attempts were not successful, the control job stopped restarting the missing monitor jobs. With this version, the control job pauses for 10 minutes and then tries to restart the missing job again for another 10 times. This enhancements ensures that the Syslog Reporting Manager tries to keep all related jobs active unless an administrators ends the tool itself or individual monitor jobs.
- In previous versions of the tool, there has been one communication job SLSNDEVT. This job is in charge of processing all events that the monitor jobs retrieved. The job establishes a communication with the configured syslog / SIEM server and sends the events to the remote host. The Syslog Reporting Manager has been enhanced to support up to 9 send event jobs in this version. In case you observe delays in receiving entries on the remote syslog server, you can start additional send event jobs to increase the throughput of the send process. The started job names are SLSNDEVT1 to SLSNDEVT9. The number of send jobs is configured with the CFGSLENV command.
- The STRSLMON command has been enhanced to provide an additional parameter *SNDEVT. When the command is executed with the *SNDEVT parameter, the control job will check that all configured send event jobs are active. If not, the control job restarts the missing jobs. For example, if you configured to use 4 send event jobs and only job 1,2 and 4 are active, the STRSLMON *SNDEVT would cause number 3 to be started again. Running jobs are not affected.
- Initially introduced in V1.2, events could also be sent via the TCP protocol besides the UDP protocol. The advantage of a TCP session is the reliability and also the option to send multiple events through a single established TCP connection. To differentiate the different events within a single TCP session, V1.2 supported a transfer mode called octect counting as defined in RFC6587. With this method, an event in a TCP session is identified by the message length. The octet count of the length of the entire message is added as a prefix to the syslog message. Based on the length, the receiver knows when an event message ends and the next event starts. This is the newer message transfer mode that is considered more reliable than the second option called non-transparent-framing. Since many SIEM solutions only support the older method, TCP caused a problem when sending events to these SIEM hosts. Version 1.4 has been enhanced to also support the non-transparent-framing transfer mode. It uses a trailer character to indicate the end of a message. The supported trailer characters are LF, CR, CRLF, and NULL. The transfer mode s configured with the CFGSLENV command.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

- The startup performance and behavior of the audit monitor job has changed. In previous versions, when the audit monitor job started, the entire chain of journal receivers were examined starting at the last processed timestamp. Since some clients keep a large number of audit journal receivers on the system, the startup of the audit monitor job could have taken hours. The enhancement in this version does not only keep track of the last processed entry but also of the journal receiver the event was in. When the audit monitor starts, it starts processing entries from the previous timestamp in the journal receiver that the entry was in. If the journal receiver does not exist anymore when the monitor job starts, the currently attached receiver only or the entire current chain of receivers will be examined. This depends on the setting in the CFGSLAUD command's *Audit journal receiver selection* parameter value. If the Syslog Reporting Manager has been installed the first time on a system and the audit monitor job is started only the currently attached journal receiver is examined starting from the time of the installation minus 1 hour.
- On systems that generate a large amount of history log or audit journal entries, the performance of the monitor jobs can be degraded due to the way the monitor jobs process the retrieved entries. Prior to this version, only one entry was read at a time from the log source. In this version, an administrator can decide to increase the number of events that are retrieved in a single SQL FETCH command (read multiple rows). The default is still one row at a time, but you can define between 1 and 200 rows to be fetched at a time for the history monitor and the audit journal monitor. The values are configured with the CFGSLENV command (advanced parameter).
  Important: If the number of entries that your filter selection produce is small and the number of rows to be fetched is large, there will be a delay in sending the events. Read the online help of the CFGSLENV command for further information.
- The audit journal monitor configuration supports now a user profile filter. You can specify up to 9 user profiles per audit journal event type. Wildcards are supported as part of the user profile name. Following are a few examples using the user profile filter:
  - Example 1: QSECOFR filter for entries from QSECOFR only
  - Example 2 : Q* filter for entries from all user profiles that start with Q
  - Example 3: *SRV* filter for entries where the sending user profile name contains somewhere the string SRV like WEBSRV1 or, APPSRVPRF
  - Example 4: *OWN filter for entries where the sending user profile name ends with OWN, such as QZRDSRMOWN, APP1OWN, or APP2OWN
  - The audit journal monitor now supports additional T journal code journal entry types. Following is the list of additional entry types. Note that these entry types are only supported on IBM i releases 7.3 and higher. Certain PTF prerequisites must be met.
    - AP, AU, CQ, CU, CV, CY, DI, EV, IM, IP, IR, IS, JD, JS, KF, ML, M0 (7.4 only), M6 (7.4 only), M7 (7.4 only), M8 (7.4 only), M9 (7.4 only), NA, ND, NE, O1, O2, O3, PF, PO, PS, PU, RQ, SD, SF, SG, SK, SM, VO, VP, XD, X0, X1, X2, YC, and YR.
    - Check section Audit journal entry type support on page 83 for more details about the supported entry types, the minimum release level, and the prerequisite PTF numbers.
  - This version also supports processing of user type audit journal entries that have been produced with the SNDJRNE command or equivalent API. These entries are report under the journal code U in the audit journal. The journal event type depends on the source of the event.
    - The Syslog Reporting Manager generates user type entries of event type SL.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

- Another major enhancements that required changes in many parts of the tool is the support of independent ASPs. You can now specify via the CFGSLENV command the ASP group name of an iASP that contains:
  - Journals that log IFS file changes
  - Journals that log database changes to be processed by the optional Journal Extract Tool (JET) from Lab Services.
- The IFS file change monitoring supports the monitoring of IFS files that are defined in the Syslog Reporting Manager standard journal IFSJRN. In this version, you can also add custom journals where IFS file changes get logged. This supports journals in an iASP or in the system ASP. The IFS journals are configured via command CFGSLIFSJ.
- All Syslog Reporting Manager commands are now available as proxy commands in the QSYS library.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

10 Audit journal entry type support

The Syslog Reporting Manager was first supported with IBM i release 7.2 and specific group PTF levels. Initially only 30 audit journal entry types were supported. Throughout the years IBM development has added support for more journal entry types. Therefore, certain prerequisites have to be met to be able to leverage all journal entry types.
The following table contains a list of journal entry types including the minimum release level and possible PTF dependencies.

Entry type	Min. Release	PTF prerequsites
AD	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
AF	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
AP	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
AU	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
AX	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
CA	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
CD	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
CO	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
CP	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
CQ	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
CU	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
CV	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
CY	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
DI	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
DO	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
DS	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
EV	7.3	7.3: SF99703 Level 18

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

Entry type	Min. Release	PTF prerequsites
		7.4: SF99704 Level 7
GR	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
GS	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
IM	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
IP	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
IR	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
IS	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
JD	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
JS	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
KF	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
LD	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
ML	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
M0	7.4	7.4: SF99704 Level 7
M6	7.4	7.4: SI99704 Level 9
M7	7.4	7.4: SI99704 Level 9
M8	7.4	7.4: SI99704 Level 9
M9	7.4	7.4: SF99704 Level 7
NA	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
ND	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
NE	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
OM	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
OR	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

Entry type	Min. Release	PTF prerequsites
OW	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
O1	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
O2	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
O3	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
PA	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
PF	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
PG	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
PO	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
PS	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
PU	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
PW	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
RA	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
RJ	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
RO	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
RP	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
RQ	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
RU	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
RZ	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
SD	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
SE	7.2	7.2: SF99702 Level 21 and PTF SI67459

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

Entry type	Min. Release	PTF prerequsites
		7.3: SF99703 Level 10 and PTF SI67460
SF	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
SG	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
SK	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7 7.3: SI74230 (provides additional cipher and protocol information) 7.4: SI74229 (provides additional cipher and protocol information)
SM	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
SO	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
ST	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
SV	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
VO	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
VP	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
XD	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
X0	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
X1	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
X2	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
YC	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
YR	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
ZC	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
ZR	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
Note: The listed PTFs represent the PTF number / level where the support was added. There might be newer PTFs available that supersede the listed numbers.		

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

11 IBM Systems Lab Services and Training Security

Privacy and data protection are the responsibility of all. In a world where data is easily acquired, shared and stored (and potential data misuse is a concern) everyone must do their part to handle information in compliance with their company's requirements and values. IBM research indicates security expenses are growing three times faster than IT budgets. Mounting regulatory and compliance mandates carry stiff government penalties and fines if ignored; every-growing volumes of data tax infrastructures and control capabilities; customer records disappear with alarming frequency; and security breaches cost an average of $6.6 million per incident.

With the added pressure of a challenging economy, to compete effectively a business cannot tolerate any security exposures. From a minor breach like exposing one's password to a peer or major failure like the disclosure of client data, neither are unacceptable and can result in new administrative procedures, a failed audit or lost business. Some circumstances could even lead to a lawsuit.

Engage the experts of IBM Systems Lab Services and Training to help uphold your company's commitment to privacy and data security. Our team has developed a multitude of offerings to address your specific security concerns. From help implementing a security feature to additional resources to supplement your staff, our Consulting and Implementation Services provide general and custom consulting. Services include password elimination and single sign-on, data and tape encryption, system auditing setup and analysis, security assessments, breach analysis and penetration testing and IBM® WebSphere® Application Server health checks.

Security Tools

Complementing our security offerings are tools that we have developed over the years to assist us in the delivery of our services. These tools have been written with customers in mind to aid them in the tasks of administrating security and in response to requirements to fill product gaps. They range from easy–to–install tools and utilities to more complex solutions; the latter often includes a services component intended to provide technical training and implementation services so clients and business partners can acquire and maintain mission critical skills. The tools listed below are our most requested. Others exist as well. Perhaps we can build something for you?

IBM i Security Diagnostics Tool (iSAT)

The IBM i Security Diagnostics Tool (iSAT) is an exhaustive security collection tool that is often used during a security assessment to help discover and document security vulnerabilities. More than statistical information found in the Quick Security Check Tool, the iSAT tool drills deep to analyze object authorities, elevated privileges, etc. to enable a holistic methodical approach towards security hardening. It can also be purchased separately for customers wishing to enhance their security reporting capability.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

Compliance Assessment and Reporting Tool (includes Event Monitoring)

The Compliance Monitoring Tool is a centralized security and systems information Data Mart. The tool utilizes DB2 Web Query to provide a web-based interface for easy monitoring of compliance on any or all systems in an enterprise. The GUI includes color coding which highlights deviations from policy, unexpected differences of policy settings between systems, and security attributes that do not adhere to corporate security objectives. Additional capabilities provided by the tool also include:

- An ability to quantify and act upon several aspects of security as statistical measurable components as well as compliance to corporate defined objectives for configuration consistency
- A scoring mechanism (seeded with Best Practices) for prioritization of policy items by High, Medium and Low risk that is customizable by customer objectives
- Built in extensibility to add user-defined items for monitoring inventory, auditing, status, etc. with incorporated scoring mechanisms provided by the tool. These items can be customer defined and written or services obtained for enhancements.
- A federated repository of IBM i user profiles that provide cross system observability of profile administration. This repository could be utilized in the development of administrative tools to reduce helpdesk costs associated with user administration.
- An ability to monitor events as they happen - providing near "real time" monitoring of more than 180 of the most common security events. Additional messages and events can be monitored through a customization utility. These events can be made "actionable" through a provided utility that forwards these events to a customer defined message queue for further action, ie., send to email, cell phone or SMS.

Single Sign On (SSO) / Enterprise Identity Mapping (EIM) Populator Tool

The need for multiple user registries, an issue most enterprises face, creates a large administrative challenge. EIM for the IBM i platform offers administrators and application developers an inexpensive solution for easier management of multiple user registries and user identities. EIM creates a system of identity mappings, called associations, between various user identities in various user registries. It provides a common interface across platforms to look up relationships between user identities.

One of the more time-consuming tasks in implementing a single sign-on solution is registering users to the EIM repository. The EPT is a Java-based desktop GUI application that allows an administrator to easily import information from a comma–separated value text file. With EPT, take a spreadsheet of known user IDs and/or names and create identifiers and mappings for each user. Java 1.4 or higher is required.

Certificate Expiration Manager (CEM)

The Certificate Expiration Manager (CEM) is a Java-based tool for simplifying the management of certificate expiration (cross-platform). CEM maintains a log of all expiration activities and can send notifications vial email. An easy to use configuration GUI is included for managing the XML settings. The tool only runs on platforms that support Java.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

Single Sign On (SSO) / Enterprise Identity Mapping (EIM) Management Tool

The EIM Management Tool is a Java-based desktop GUI application that allows an administrator to easily manage the information within an EIM repository, via a more user-friendly layout than what is provided in iSeries Navigator. Identifiers, aliases, descriptions, associations, and user registries can be created, deleted, and renamed, all from the same screen. The tool also includes a tree view of the EIM repository, domain management functions to create/delete EIM domains, save/restore of the data in an EIM domain to/from a local XML file, as well as a password synchronization view to manipulate EIM data that pertains to the network password synchronization tool (NPST). Java 1.4 or higher is required.

MS Windows Active Directory to IBM i User Synchronization Tool

The Microsoft Windows Active Directory to IBM i user synchronization tool is a lightweight Java tool that offers a programmatic way to create and change IBM i user profiles when changes are detected on the MS Active Directory. All changes on the IBM i are triggered from actions on the MS Active Directory.

Note: IBM i user profile changes do not trigger changes on the MS Active Directory - all tool actions should be considered “one way” going from the MS Active Directory to the IBM i.

Security Exit Points

The Security Exit Point Tool simplifies the managing of Exit Point definitions for users on an IBM i. Currently, the tool includes programs for managing the Exit Points for CLI, DRDA/DDM, FTP, IFS, ODBC, JDBC, File Transfer, REXEC, RMTCMD, Host Server Signon, and others. Additional Exit Point Programs will be added in the future. The tool provides the Security Administrator with an interface to define which users are allowed to use the defined Exit Point. An Audit Journal record is created whenever a user accesses the defined Exit Points.

Password Validation

Despite warnings, one-in-five users choose a non-compliant password to protect their identity. We’ve developed a program that validates and ensures passwords meets company and industry recommended rules and guidelines. The tool also allows the security administrator to establish a dictionary of excluded terms, to further tighten password security.

Password Synchronization

Studies show that corporate users tend to repeat passwords on the various systems they use. The Password synchronization tool makes it easier for end users to remember these passwords and simplify their access to multiple partitions. This is accomplished by reducing the number of passwords that an end user needs to remember, making it less likely for them to write them down, resulting in fewer calls to the corporate Help Desk and less opportunity for others to gain improper access. In addition to password synchronization, this tool supplements the IBM i Operating System supplied password rules to strengthen your security posture.

© Copyright 2018, 2021 IBM Corp. All Rights Reserved

For more information about IBM Systems Lab Services Security Offerings . . .

Terry Ford, Team Leader
Security Services Delivery
507-253-7241

Carol Ward, Opportunity Manager
224-465-2909

Claude Roustan, Opportunity Manager
+33 492072077 office
+33 684635310 mobile

Or visit our website at:

© Copyright 2018, 2021 IBM Corp. All Rights Reserved