an IBM Company

ServiceAssure™ Release 3.1.3 Patch SA3.1.3.8.18 Auditor Log Utility User Manual

System Release: 3.1.3

19th September 2008

Vallent,
an IBM Company
5300 Cork Airport Business Park,
Kinsale Road, Cork
Ireland

Doc. Name: Patch SA3.1.3.8.18 Auditor Log Utility User Manual

Doc. Version: Version 1.0
Release Date: 19th Sep 2008

Abstract

This User Manual details Instructions on using Audit Log Utility

Document Control

REVISION HISTORY

Date	Version	Description of changes
19th Secptember 2008	1.0	Initial Version

TRADEMARKS

Audit Log Utility

The TNSQM audit manager logs a record of each instance of an entity type created/deleted/updated to a syslog format log file provided that the audit manager has been configured to audit that particular entity type. For example, if the audit manager is configured to audit entity type RESOURCE then each instance of a resource created/deleted/updated will be logged to a syslog format file.[1] The files are ascii files and can be viewed using an appropriate editor (for example vi on UNIX).

A set of syslog format log files will exist for each TNSQM entity type being audited. The set of files includes the following:

- current file being written to. The format of the filename is 'TNSQM_Audit_<entitytype>.syslog', for example 'TNSQM_Audit_KqiModel.syslog'.
- rolled over log files. The syslog log files roll over on a daily basis or when a file has reached a maximum configurable size limit. The format of a rolled over filename is 'TNSQM_Audit_<entitytype>.syslog. YYYYMMDD.<current time in milliseconds>.
  For example TNSQM_Audit_KqiModel.syslog.20080917.1221664299514.

A compress tool can be used for archiving rolled over syslog files. The archiving type is ZIP. The directory into which archive files are stored is configurable. A cron entry is used to enable archiving of syslog files. To enable archiving add the following entry to saserver's crontab file:

```
0 1 * * * --WMCROOT--/bin/zipper_util
```

This will result in the syslog files being archived at 1.00am every day.

NOTE: The auditom process needs to be running in order for the syslog files to be produced. Ensure that the process is running by executing the command 'sap disp auditom' and verify that it's state is STARTED.

1 Note that for each entity type audited the audit manager also logs creates/deletes/updates for instances of that entity type to a binary log file. The entries in these binary log files are displayed in the audit manager UI. Also, the OM server which is responsible for management of an entity type needs to be at state STARTED. The state can be determined by running 'sap disp <om service>'.

Configuration of Syslog Files

Configuration of the syslog files is controlled by property settings in the file $WMCROOT/conf/service/dom/extension.properties. The following property settings are relevant for syslog file configuration.

com.comnitel.audit.syslog.enabled=true

This property determines whether syslog reporting is enabled. By default syslogging is enabled. To disable syslogging set the property to 'false'.

com.comnitel.audit.syslog.path =${SALOGDIR}/syslog

The directory in which the syslog files will be created. Note that a subdirectory will be created for each TNSQM entity type being audited. The value for SALOGDIR is configured in the file $WMCROOT/conf/environment/default.properties. The default value for com.comnitel.audit.syslog.path is ${SALOGDIR}/syslog. For example if the audit manager is configured to audit KqiModels and Resources then the directory specified by com.comnitel.audit.syslog.path will contain two directories, namely kqimodel and resources.

com.comnitel.audit.syslog.archive.path=${SALOGDIR}/syslog

The directory into which archived syslog files are stored. By default these files are stored in ${SALOGDIR}/syslog.

com.comnitel.audit.logsize=30KB

The maximum size allowed for a syslog file. Files are rolled over if either this limit is reached or at midnight.

com.comnitel.audit.logpattern=

This property is not used for syslog file configuration.

NOTE: Rollover is triggered by receipt of a new record to be written to a file. On writing to a file the system determines if the file is older than 24 hours or has reached the maximum size and if either of these conditions is true the file is rolled over. If the current file described above is not written to for a number of days then this file will remain current until a new record needs to be written. This means that a log file may not exist for each subsequent day in the log directory.

Content Format of Syslog Files

The format of each syslog message is as follows:

<date> <time> <host> TNSQM_audit: entityname=<value>, entitytype=<value>, operationtype=<value>, username=<value>, addinfo=<value>

where

date is the date the create/delete/update operation occurred on. The format of date is yyyy.mm.dd

time is the time the create/delete/update operation occurred at. The format of time is HH:mm:ss (24 hour format).

An example of a syslog entry is as follows:

2008.08.22 14:20:45 sherkinz1.cork.ie.ibm.com TNSQM_audit: entityname=Int_SASM_Site_MMS_P2P_Failures_Count, entitytype=KqiModel, operationtype=Create, username=saserver, addinfo=