Configuring Audit Messages

1 Audit Message

By enabling system and file access events, the AUDIT server will send messages to a program called AUDMSG, which listens to a mailbox device.

Below is a list of selected system events:

1. MSG_AUDIT — System wide change to auditing.
2. MSG_BREAKIN — Break-in attempt detected.
3. MSG_LOGFAIL — Login failure.
4. MSG_NCP — Modification to network configuration database.
5. MSG_OBJ_CREATE — Object creation attempted.
6. MSG_OBJ_DELETE — Object deletion attempted.
7. MSG_PRVAUD — Privilege audit.
8. MSG_RIGHTSDB — Rights database change.
9. MSG_SYSUAF — Modification to system user authorization file (SYSUAF).

By selecting all of the events, the AUDIT server will generate many messages, which could fill the listener mailbox.

The AUDMSG utility will run on every MISER node and will use a binary point for each event type generated by the local system. For each event, AUDMSG will set an alarm for the corresponding point with the time from the audit message. The selected data packets will be used to form a PMM (Point Message Maintenance) message (four lines of sixty characters) linked to binary point. PMM.DAT is a distributed file written by AUDMSG and read by MTKMSG.

The MTKMSG utility will process alarms coming from AUDMSG, read information in related PMM records, and will generate emails. After sending all the emails, the alarm will be reset. Emails will be sent based on the email address files specified in the MTKMAN.DAT file. MTKMAN.DAT is an index file with point acronyms as the key. It has two fields: the email address file and the MTK process. MTKMAN.DAT can be maintained using these tools:

- MTKRP — displays a list of the points currently on the MTK list.
- MTKON — puts a point ON the MTK list.
- MTKOF — takes a point OFF the MTK list
- MTKDIAG — verifies the integrity of the MTK list and address files.

Audit points used by MISER programs are defined as follows:

Acronym	Name	Area	Type	Subtype	Node	ON status	Intermediate status
AUDIT-MVA-AUDI	AUDIT	02	BIN	CALC	ACTMVA	1	49
AUDIT-MVA-BREA	BREAKIN	03	BIN	CALC	ACTMVA	1	49
AUDIT-MVA-CREA	OBJ CREATE	23	BIN	CALC	ACTMVA	1	49
AUDIT-MVA-DELE	OBJ DELETE	24	BIN	CALC	ACTMVA	1	49
AUDIT-MVA-LOGF	LOGFAIL	05	BIN	CALC	ACTMVA	1	49
AUDIT-MVA-NCP	NCP CMD LINE	29	BIN	CALC	ACTMVA	1	49
AUDIT-MVA-PRIV	PRIVILEGE	16	BIN	CALC	ACTMVA	1	49
AUDIT-MVA-RIGH	RIGHTS DB	12	BIN	CALC	ACTMVA	1	49
AUDIT-MVA-SYSU	SYSUAF CHNG	11	BIN	CALC	ACTMVA	1	49

The “Area” field is used to specify the event type.

All audit points have “ON ALARM Y” and “UNDEFINE STATE ALARM Y”.

MISER points will be defined for all nodes: MVA, MV, VS1, and VS2.

OpenVMS commands are used to set the audit server:

```
$ @SYS$SYTEM:STARTUP AUDIT_SERVER
$ SET AUDITNOLISTENER
$ define/system USE_MTKMSG “Y”
```

The AUDMSG program runs as a batch job using the command file, AUDMSG_STARTUP.COM:

```
$ SET AUDIT/NOLISTENER
$ set proc/name=audmsg/prio=8
$ run mnet$exe:audmsg
$ exit
```

The MTKMSG program runs as a batch job using the command file, MTKMSG_STARTUP.COM:

```
$ set proc/name=mtkmsg/prio=7
$run mnet$exe:mtkmsg
$ exit
```

An email sent by MTKMSG will look like below:

From: system@hsq.com [mailto:system@hsq.com]
Sent: Tuesday, September 15, 2020 8:37 AM
To POLISSKY@HSQ.COM
Subject: MTKMSG 2020

Event: LOGFAIL REMOTE
AUDIT_NAME:SECURITY
SYSTEM_NAME:ACTVS1
PROCESS_NAME:_RTA1:
REMOTE_USERNAME:SYSTME
FINAL_STATUS:%LOGIN-F-INVPWD, invalid password
TERMINAL:1869::SYSTEM
FINAL_STAMP:15-SEP-2020 08:36:32.500
USERNAME:SYSTEM