Setting Up an Auditing System to Monitor Cron Events

Special Notices

Information in this document is correct to the best of our knowledge at the time of this writing. Please send feedback by fax to "AIXServ Information" at (512) 823-4009.

Please use this information with care. IBM will not be responsible for damages of any kind resulting from its use. The use of this information is the sole responsibility of the customer and depends on the customer's ability to evaluate and integrate this information into the customer's operational environment.

> **Note:** The information in this document has **not** been verified for AIX 4.1.

Procedure

This procedure is intended only for configuration of auditing in stream mode and for configuration of tracking of the cron events CRON_Start and CRON_Finish. (In stream mode, the report is written in ASCII.) This procedure applies to AIX 3.2.

Two files in /etc/security/audit must be modified in order to monitor cron events. They are:

/etc/security/audit/config: This ASCII stanza file contains audit system configuration information. It has five stanzas: start, bin, stream, classes, and users.

/etc/security/audit/events: This ASCII stanza file contains information about audit events. It has just one stanza, auditpr, which lists all the audit events in the system. The stanza also contains formatting information that the auditpr command needs to write an audit trail for each event.

1. In the "start" stanza in the /etc/security/audit/config file, "streammode" should be set to "on" and "binmode" should be set to "off".

   The default setting of the bin and stream stanzas are:

```
bin:
          trail = /audit/trail
          bin1 = /audit/bin1
          bin2 = /audit/bin2
          binsize = 10240
          cmds = /etc/security/audit/bincmds

stream:
          cmds = /etc/security/audit/streamcmds
```

2. Group cron audit events into sets of similar items called audit classes. Define these audit classes in the "classes" stanza of the /etc/security/audit/config file. The CRON_Start and CRON_Finish events monitor cron-job start and finish events. Below is the cron audit class with every event that audit can track.

```
cron = AT_JobAdd,AT_JobRemove,CRON_JobAdd,CRON_JobRemove,CRON_Start,CRON_Finish
```

3. To assign audit classes to an individual user, add a line to the users stanza of the /etc/security/audit/config file. Each line is in the form

   ```
   <user> = <audit class>, <audit class>
   ```

   For example, to enable tracking of cron events from root's crontab table, enter:

   ```
   root = cron
   ```

4. From the list in the /etc/security/audit/events file, select and/or add system activities (events) to be audited. Here is an example of the CRON_Start and CRON_Finish events.

   ```
   CRON_Start = printf "event = %s cmd = %s time = %s"
   CRON_Finish = printf "user = %s pid = %s time = %s"
   ```

   The purpose of these formatting instructions is to enable the auditpr command to write customized data in the audit record for the event.

   Note: There was a defect in the documentation related to cron events (IX34755). The names for the cron start and stop events were documented as CRON_start and CRON_finish; they should have been CRON_Start and CRON_Finish.

5. The output file for the cron report is specified in /etc/security/audit/streamcmds. The default setting for streamcmds is:

   ```
   /etc/auditstream | auditpr -v > /audit/stream.out &
   ```

6. After the config and events files have been changed, auditing must be restarted so that it will be reinitialized with the new parameters. To restart auditing, enter these commands:

   ```
   audit shutdown
   audit start
   ```

Reader's Comments

Please fax this form to (512) 823-4009, attention "AIXServ Information". You may also e-mail comments to: elizabet@austin.ibm.com. These comments should include the same customer information requested below.

Use this form to tell us what you think about this document. If you have found errors in it, or if you want to express your opinion about it (such as organization, subject matter, appearance) or make suggestions for improvement, this is the form to use.

If you need technical assistance, contact your local branch office, point of sale, or 1-800-CALL-AIX (for information about support offerings). These services may be billable. Faxes on a variety of subjects may be ordered free of charge from 1-800-IBM-4FAX. Outside the U.S. call 415-855-4329 using a fax machine phone.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Note: If you have a problem report or item number, supplying that number may help us determine why a procedure did or did not work in your specific situation.

Problem Report or Item #: Branch Office or Customer #:

Be sure to print your name and fax number below if you would like a reply:

Name: Fax Number:

11/21/94

END OF DOCUMENT (cron.auditing.cmd, 4FAX# 2226)