Integrate IBM AIX

EventTracker Enterprise

Publication Date: April 6, 2016
About this Guide

This guide will facilitate an IBM AIX user to send logs to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise 7.x or later and IBM AIX 6.1 and 7.1.

Audience

Administrators who want to monitor IBM AIX using EventTracker Enterprise.
Table of Contents

About this Guide .................................................................................................................................... 1
   Scope.................................................................................................................................................. 1
   Audience............................................................................................................................................. 1
Introduction ........................................................................................................................................... 3
Pre-requisites........................................................................................................................................ 3
Configuring IBM AIX for Auditing ....................................................................................................... 3
IBM AIX syslog configuration ................................................................................................................ 3
EventTracker Knowledge Pack .............................................................................................................. 4
   Categories .......................................................................................................................................... 4
   Alerts ................................................................................................................................................ 6
   Flex Reports ....................................................................................................................................... 6
Import Knowledge Pack into EventTracker ........................................................................................ 14
   Categories ........................................................................................................................................ 15
   Alerts ................................................................................................................................................ 17
   Token Templates .............................................................................................................................. 18
   Flex Reports ..................................................................................................................................... 19
   Knowledge Object ............................................................................................................................ 20
Verifying IBM AIX knowledge pack in EventTracker ........................................................................ 23
IBMAIX Categories ............................................................................................................................... 23
IBMAIX Alerts ...................................................................................................................................... 23
IBMAIX Token Template ...................................................................................................................... 25
IBMAIX Flex Reports ........................................................................................................................... 25
IBMAIX Knowledge Object .................................................................................................................. 26
Create Flex Dashboards in EventTracker ............................................................................................ 27
   Schedule Reports .......................................................................................................................... 27
   Create Dashlets ............................................................................................................................. 30
Sample Flex Dashboards .................................................................................................................... 33
Integrate IBM AIX

Introduction

AIX (Advanced Interactive eXecutive, pronounced ‘a i ex”) is a series of proprietary UNIX operating system developed and sold by IBM for several of its computer platforms.

Pre-requisites

- EventTracker 7.x or later should be installed.
- User should have administrator privileges to IBM AIX server.

Configuring IBM AIX for Auditing

The audit logger constructs the audit record and appends it to the kernel audit trail. From there, it can be written in one or both of the following modes:

- BIN mode Written in two binary files.
- STREAM mode Written synchronously via an audit pseudo-device

To enable STREAM mode auditing and select audit events:

1. Start:
   streammode = on
   cmds = /etc/security/audit/streamcmds

IBM AIX syslog configuration

1. Login to the IBM AIX Unix machine as root.
2. Open Terminal Window.
3. Open syslog.conf in VI Editor. Vi /etc/syslog.conf.
4. Add the below mentioned line in file syslog.conf at last.

   *.info@IP address of EventTracker Enterprise machine

5. Save the file using :wq
6. Run refresh –s syslogd
Once IBM AIX is configured events are received in EventTracker; Alerts and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support IBM AIX.

Categories

- **IBM AIX: Account management**
  This category provides information related to system accounting, being enabled or disabled by the admin.

- **IBM AIX: Administrator logon activity**
  This category provides information related to successful user logon attempts.

- **IBM AIX: Audit configuration**
  This category provides information when an administrator performs auditing on process control events, security events and privilege required events.

- **IBM AIX: Backup and restore activity**
  This category provides information related to backup, restore and export activity.

- **IBM AIX: Cron activity**
  This category provides information related to cron that tasks running automatically in the background at regular intervals.

- **IBM AIX: Device management**
  This category provides information related to device configuration, device create, delete, remove, start and stop details.

- **IBM AIX: File access control changes**
  This category provides information related to access control list that defines the access rights to the object.

- **IBM AIX: File management**
  This category provides information related to file management that performs read, write, rename, change of mode and ownership.

- **IBM AIX: File system activity**
  This category provides information related to file system that make, remove, change of directory and root.
Integrate IBM AIX

- **IBM AIX: General activity**
  This category provides information related to port locked, port changed, enqueuing request to shared resources and installs, updates and maintenance of the available software products.

- **IBM AIX: Group management**
  This category provides information related to group name, checks the existence of the users that are listed as group administrators in the group database files and also checks for valid admin attribute for each group.

- **IBM AIX: Kernel process activity**
  This category provides information related to the state of each active processes and threads in the system.

- **IBM AIX: Logical volume management activity**
  This category provides information related to logical volume management and locally attached disk drives operations.

- **IBM AIX: Password changed**
  This category provides information related to change of user’s password, administrator password and verifies the correctness of local authentication information.

- **IBM AIX: Security objects audit**
  This category provides information related to the environment attributes allowing admin to read, write and execute operations on security objects.

- **IBM AIX: Security roles management**
  This category provides information related to role based access control allowing the creation, change and removal of roles for system by administrator.

- **IBM AIX: System resource controller**
  This category provides information related to start and stop of the system resource controller and changes in the subserver and subsystem definition in the object class.

- **IBM AIX: System start and stop**
  This category provides information related to server startup and shutdown.

- **IBM AIX: TCPIP activity**
  This category provides information related to changes in TCP/IP interfaces, routes and system time via network.

- **IBM AIX: User authentication failed**
  This category provides information related to authentication failure for user due to incorrect password or insufficient permission.
• **IBM AIX: User management**
  This category provides information related to user create, change, remove and user access to the shell.

### Alerts

- **IBM AIX: Account disabled**
  This alert is generated when administrator disables the system accounting.

- **IBM AIX: Device removed**
  This alert is generated when administrator removes the device from the server.

- **IBM AIX: Security role changed**
  This alert is generated when administrator create, change and remove the security roles.

- **IBM AIX: System rebooted**
  This alert is generated when administrator reboots the server.

### Flex Reports

- **IBM AIX: Administrator logon activity**
  This report provides information related to user logon activity, that is, whoever has logged in, logged out or exited from the server.

```
<table>
<thead>
<tr>
<th>When</th>
<th>Computer</th>
<th>Who</th>
<th>Command</th>
<th>Action</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 19 13:51:45</td>
<td>AIXSERVER</td>
<td>root</td>
<td>term</td>
<td>USER_Login</td>
<td>user: root tty: /dev/pts/2</td>
</tr>
<tr>
<td>Feb 19 13:52:32</td>
<td>AIXSERVER</td>
<td>root</td>
<td>rlogind</td>
<td>USER_Ext</td>
<td>tty: User root logged out on</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>USER_Logout</td>
<td>/dev/pts/2</td>
</tr>
<tr>
<td>Feb 19 20:52:27</td>
<td>AIXSERVER</td>
<td>root</td>
<td>logout</td>
<td>USER_Logout</td>
<td></td>
</tr>
</tbody>
</table>


**USER_Logout** root  OK  Tue Jan 23 20:52:27 2007 logout /dev/pts/0

```

- **IBM AIX: Audit configuration**
  This report provides the information related to the events and objects, which are audited.
Integrate IBM AIX

<table>
<thead>
<tr>
<th>When</th>
<th>Computer</th>
<th>Who</th>
<th>Command</th>
<th>Action</th>
<th>Status</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 17 15:09:48 2016</td>
<td>AXSERVER2</td>
<td>root</td>
<td>auditat</td>
<td>AUD_Proc</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Jan 17 15:09:48 2016</td>
<td>AXSERVER2</td>
<td>root</td>
<td>auditat</td>
<td>AUD_Bin_Def</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Jan 23 21:27:10 2016</td>
<td>AXSERVER2</td>
<td>root</td>
<td>audit</td>
<td>AUD_Il</td>
<td>OK</td>
<td>cmd: 1 arg: 0</td>
</tr>
<tr>
<td>Jan 31 11:03:27 2016</td>
<td>AXSERVER2</td>
<td>root</td>
<td>vi</td>
<td>AUD_CONFIG_WR</td>
<td>OK</td>
<td>audit object write event detected</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/etc/security/audit/configurevent</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>login status time command</td>
</tr>
</tbody>
</table>

**AUD_CONFIG_WR root OK Wed Jan 31 11:03:27 2007 vi audit object write event detected**

**/etc/security/audit/configevent login status time command**

**AUD_Il root OK Tue Jan 23 21:27:10 2007 audit cmd: 1 arg: 0**

**AUD_Bin_Def root OK Wed Jan 17 15:09:48 2007 auditbin**

**AUD_Proc root OK Wed Jan 17 15:09:48 2007 auditcat**

- **IBM AIX:Cron activity**
  - This report provides information related to scheduling the tasks to be executed at a specified time.

<table>
<thead>
<tr>
<th>When</th>
<th>Computer</th>
<th>Who</th>
<th>Command</th>
<th>Action</th>
<th>Status</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 24 03:00:00 2016</td>
<td>AXSERVER</td>
<td>root</td>
<td>cron</td>
<td>CRON_Start</td>
<td>OK</td>
<td>event = start cron job cmd =</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lpp/diagnostics/bin/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>run_ssa_healthcheck 1&gt;/dev/null</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2&gt;/dev/null time = Sun Jul 12 03:00:00 1970</td>
</tr>
<tr>
<td>Feb 24 19:30:00 2016</td>
<td>AXSERVER</td>
<td>root</td>
<td>cron</td>
<td>CRON_Finish</td>
<td>OK</td>
<td>user = root pid = 77854 time = Wed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Feb 24 19:30:00 2016 file name = root</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1169520610.a User = root time = Wed Feb</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>24 20:46:15 2016 file name = Frank</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cooper User = Frank Cooper time = Wed Feb</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>24 21:01:05 2016 file name = Jeff Smith</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>User = Jeff Smith time = Wed Feb 24</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>21:01:18 2016</td>
</tr>
<tr>
<td>Feb 24 20:50:07 2016</td>
<td>AXSERVER</td>
<td>root</td>
<td>at</td>
<td>AT_JobAdd</td>
<td>OK</td>
<td>file name = Frank Cooper User =</td>
</tr>
<tr>
<td>Feb 24 21:01:05 2016</td>
<td>AXSERVER</td>
<td>root</td>
<td>at</td>
<td>AT_JobRemove</td>
<td>OK</td>
<td>Frank Cooper time = Wed Feb 24</td>
</tr>
<tr>
<td>Feb 24 21:01:18 2016</td>
<td>AXSERVER</td>
<td>root</td>
<td>crontab</td>
<td>CRON_JobAdd</td>
<td>OK</td>
<td>file name = Jeff Smith User =</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Jeff Smith time = Wed Feb 24</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>21:01:18 2016</td>
</tr>
</tbody>
</table>

**CRON_JobRemove root OK Mon Jan 22 21:01:18 2016 crontab file name = Frank Cooper User = Frank Cooper**

**time = Mon Jan 22 21:01:18 2016**

**CRON_JobAdd root OK Mon Jan 22 21:01:05 2016 crontab file name = Jeff Smith User = Jeff Smith time =**

**Mon Jan 22 21:01:05 2016**

**CRON_Start root OK Sun Jul 12 03:00:00 1970 cron event = start cron job cmd = /usr/lpp/diagnostics/bin/ run_ssa_healthcheck 1>/dev/null 2>/dev/null time = Sun Jul 12 03:00:00 1970**
Integrate IBM AIX

- **IBM AIX: Device management**
  This report provides the information related to device create, configure and change details.

<table>
<thead>
<tr>
<th>When</th>
<th>Computer</th>
<th>Who</th>
<th>Command</th>
<th>Action</th>
<th>Status</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 24 20:24:25 2016</td>
<td>AIXSERVER</td>
<td>root</td>
<td>mkdev</td>
<td>DEV_Create</td>
<td>FAIL</td>
<td>mode: 1114032461 dev: 87537690 filename 5 Cannot perform the requested function because the parent of the specified device does not exist.</td>
</tr>
</tbody>
</table>

- **IBM AIX: File access control changes**
  This report provides information related to access control list defined to files by the user.

<table>
<thead>
<tr>
<th>When</th>
<th>Computer</th>
<th>Who</th>
<th>Command</th>
<th>Action</th>
<th>Status</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 24 15:09:45 2016</td>
<td>AIXSERVER</td>
<td>root</td>
<td>uncompress</td>
<td>FILE_ReadXacl</td>
<td>OK</td>
<td>foo.z</td>
</tr>
<tr>
<td>Feb 24 15:09:47 2016</td>
<td>AIXSERVER</td>
<td>root</td>
<td>uncompress</td>
<td>FILE_WriteXacl</td>
<td>OK</td>
<td>foo.z</td>
</tr>
<tr>
<td>Feb 24 20:55:27 2016</td>
<td>AIXSERVER</td>
<td>root</td>
<td>vi</td>
<td>FILE_WriteXacl</td>
<td>OK</td>
<td>fd: 4</td>
</tr>
</tbody>
</table>

**FILE_Acl root OK Wed Jan 31 13:51:45 2007 telnetd**
filename: /dev/pts/2, ACL: length: 16, mode: 0, user: 6, group: 6, other: 6

**FILE_Facl root OK Wed Jan 31 13:51:45 2007 rlogind**
fd: 8, ACL: length: 16, mode: 0, user: 0, group: 0, other: 0

**FILE_WriteXacl root OK Wed Jan 17 15:09:47 2007 uncompress foo.z**

**FILE_WriteXacl root OK Wed Jan 31 13:53:24 2007 vi**
fd: 3, ACL: Type = AIXC, length = 16 * * ACL_type AIXC * attributes: base permissions owner(nobody): rw- group(nobody): rw-others: r-- extended permissions disabled
• IBM AIX: File management
  This report provides information related to files that are compressed, uncompressed, changing of ownership and renaming by the user.

<table>
<thead>
<tr>
<th>When</th>
<th>Computer</th>
<th>Who</th>
<th>Command</th>
<th>Command</th>
<th>Action</th>
<th>Status</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 22 13:07:37 2016</td>
<td>AIXSERVER</td>
<td>root</td>
<td>cron</td>
<td>FILE_Fchmod</td>
<td>OK</td>
<td>mode: 444 file descriptor 3</td>
<td></td>
</tr>
<tr>
<td>Feb 22 13:51:45 2016</td>
<td>AIXSERVER</td>
<td>root</td>
<td>rlogind</td>
<td>FILE_FREvoke</td>
<td>OK</td>
<td>fd: 7</td>
<td></td>
</tr>
<tr>
<td>Feb 22 15:00:01 2016</td>
<td>AIXSERVER</td>
<td>root</td>
<td>lsv</td>
<td>FILE_Mknod</td>
<td>OK</td>
<td>mode: 20500 dev: 1 filename /dev/__pv22.1.389300</td>
<td></td>
</tr>
<tr>
<td>Feb 22 15:09:45 2016</td>
<td>AIXSERVER</td>
<td>root</td>
<td>uncompressed</td>
<td>FILE_Read</td>
<td>OK</td>
<td>staff finance</td>
<td></td>
</tr>
<tr>
<td>Feb 22 15:09:47 2016</td>
<td>AIXSERVER</td>
<td>root</td>
<td>uncompressed</td>
<td>FILE_Write</td>
<td>OK</td>
<td>staff finance</td>
<td></td>
</tr>
<tr>
<td>Feb 22 20:33:30 2016</td>
<td>AIXSERVER</td>
<td>root</td>
<td>iqueryvg</td>
<td>FILE_Mknod</td>
<td>FAIL</td>
<td>mode: 20500 dev: 0 filename /dev/__vg10</td>
<td></td>
</tr>
<tr>
<td>Feb 22 20:53:00 2016</td>
<td>AIXSERVER</td>
<td>root</td>
<td>cron</td>
<td>FILE_Fchown</td>
<td>OK</td>
<td>owner: 0 group: 0 file descriptor 1</td>
<td></td>
</tr>
<tr>
<td>Feb 22 21:18:01 2016</td>
<td>AIXSERVER</td>
<td>root</td>
<td>chmod</td>
<td>FILE_Mode</td>
<td>OK</td>
<td>mode: 660 filename /dev/fslv01</td>
<td></td>
</tr>
<tr>
<td>Feb 22 21:19:00 2016</td>
<td>AIXSERVER</td>
<td>root</td>
<td>compress</td>
<td>FILE_Unlink</td>
<td>OK</td>
<td>filename /audit/tempfile.00233620</td>
<td></td>
</tr>
<tr>
<td>FILE_Unlink root OK Tue Aug 18 21:19:00 1970 compress filename /audit/tempfile.00233620</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FILE_Read root OK Wed Jan 17 15:09:45 2007 uncompress</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FILE_Write root OK Wed Jan 17 15:09:47 2007 uncompress</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FILE_Unlink root OK Tue Aug 18 21:19:00 1970 compress filename /audit/tempfile.00233620</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FILE_Mode root OK Tue Jan 23 21:18:01 2007 chmod mode: 660 filename /dev/fslv01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FILE_Fchown root OK Mon Jan 22 20:53:00 2007 cron owner: 0 group: 0 file descriptor 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FILE_Mknod root FAIL Mon Jan 22 15:00:01 2007 lsv mode: 20600 dev: 1 filename /dev/__pv22.1.389300</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FILE_Dupfd root OK Wed Jan 17 15:09:45 2007 sh</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FILE_Utimes root OK Wed Jan 17 15:09:46 2007 uncompress</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FILE_Accessx root OK Wed Jan 17 15:09:45 2007 sh</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
- **IBM AIX: File system activity**
  This report provides information related to files change of current root, make change and remove of directory by the user.

<table>
<thead>
<tr>
<th>When</th>
<th>Computer</th>
<th>Who</th>
<th>Command</th>
<th>Action</th>
<th>Status</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 24 17:12:202016</td>
<td>AXSERVER</td>
<td>root</td>
<td>mount</td>
<td>FS_Umount</td>
<td>OK</td>
<td>umount: object /dev/fslv00 stub /nvoll</td>
</tr>
<tr>
<td>Feb 24 17:20:402016</td>
<td>AXSERVER</td>
<td>root</td>
<td>chfs64</td>
<td>FS_Extend</td>
<td>OK</td>
<td>vfs: 20, cmd: 5</td>
</tr>
<tr>
<td>Feb 24 17:30:142016</td>
<td>AXSERVER</td>
<td>root</td>
<td>find</td>
<td>FS_Fchdir</td>
<td>OK</td>
<td>manual clients proposals .perm - 0600 /usrbin pwd</td>
</tr>
<tr>
<td>Feb 24 17:32:192016</td>
<td>AXSERVER</td>
<td>root</td>
<td>chroot</td>
<td>FS_Chroot</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Feb 24 17:35:302016</td>
<td>AXSERVER</td>
<td>root</td>
<td>rmfs</td>
<td>FS_Rmdir</td>
<td>OK</td>
<td>remove of directory: /test4</td>
</tr>
<tr>
<td>Feb 24 17:40:122016</td>
<td>AXSERVER</td>
<td>root</td>
<td>snmpdv3ne</td>
<td>FS_Mkdir</td>
<td>OK</td>
<td>mode: 755 dir: /tmp/aaaDBakqa</td>
</tr>
</tbody>
</table>

- **IBM AIX: Group management**
  This report provides information related to group changed, created and removed by the user.

<table>
<thead>
<tr>
<th>When</th>
<th>Computer</th>
<th>Who</th>
<th>Command</th>
<th>Action</th>
<th>Status</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 22 20:15:22 2016</td>
<td>AXSERVER</td>
<td>root</td>
<td>chgroup</td>
<td>GROUP_Change</td>
<td>OK</td>
<td>emp users=Chris Meyer</td>
</tr>
<tr>
<td>Feb 22 21:02:57 2016</td>
<td>AXSERVER</td>
<td>root</td>
<td>mkgroup</td>
<td>GROUP_Create</td>
<td>OK</td>
<td>emp</td>
</tr>
<tr>
<td>Feb 22 21:02:57 2016</td>
<td>AXSERVER</td>
<td>root</td>
<td>rmgroup</td>
<td>GROUP_Remove</td>
<td>OK</td>
<td>emp</td>
</tr>
</tbody>
</table>

- **FS_Mount root OK Tue Jan 23 20:46:14 2007 mount mount: object /dev/fslv00 stub /nvoll**
- **FS_Extend root OK Mon Jan 22 20:33:30 2007 chfs64 vfs: 20, cmd: 5**
- **FS_Umount root OK Tue Jan 23 20:46:45 2007 mount umount: object /dev/fslv00 stub /nvoll**
- **FS_Chdir root OK Tue Aug 18 21:30:00 1970 cron change current directory to: /**
- **FS_Fchdir root OK Wed Jan 17 14:49:55 2007 find**
- **FS_Rmdir root OK Wed Jan 31 13:36:01 2007 rmfs remove of directory: /test4**
- **FILE_Utimes root OK Wed Jan 17 15:09:46 2007 uncompress**
- **GROUP_Change root OK Mon Jan 22 20:15:22 2016 chgroup emp users=Chris Meyer**
- **GROUP_Create root OK Tue Jan 23 21:02:57 2016 mkgroup emp**
- **GROUP_Remove root OK Mon Jan 22 20:18:48 2016 rmgroup emp**
**IBM AIX: Kernel process activity**
This report provides information related to the list of kernel processes running on the server.

<table>
<thead>
<tr>
<th>When</th>
<th>Computer</th>
<th>Who</th>
<th>Process Name</th>
<th>Action</th>
<th>Status</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 24 11:30:00</td>
<td>AXSERVER</td>
<td>root</td>
<td>cron</td>
<td>PROC_Privilege</td>
<td>OK</td>
<td>cmd: 30004 privset: 0:0</td>
</tr>
<tr>
<td>Feb 24 13:07:36</td>
<td>AXSERVER</td>
<td>root</td>
<td>srcmstr</td>
<td>PROC_Environ</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Feb 24 13:52:32</td>
<td>AXSERVER</td>
<td>root</td>
<td>bash</td>
<td>PROC_Kill</td>
<td>OK</td>
<td>pid: 465524, sig: 1</td>
</tr>
<tr>
<td>Feb 24 15:00:01</td>
<td>AXSERVER</td>
<td>root</td>
<td>lslv</td>
<td>PROC_Sysconfig</td>
<td>OK</td>
<td>3</td>
</tr>
<tr>
<td>Feb 24 15:11:25</td>
<td>AXSERVER</td>
<td>root</td>
<td>bash</td>
<td>PROC_Setpgid</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Feb 24 16:11:52</td>
<td>AXSERVER</td>
<td>root</td>
<td>init</td>
<td>PROC_Limits</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Feb 24 16:15:51</td>
<td>AXSERVER</td>
<td>root</td>
<td>init</td>
<td>PROC_SetUserIDs</td>
<td>OK</td>
<td>effect: 0, real: 0, saved: 0, login: 0</td>
</tr>
<tr>
<td>Feb 24 16:16:51</td>
<td>AXSERVER</td>
<td>root</td>
<td>init</td>
<td>PROC_SetGroups</td>
<td>OK</td>
<td>group set: system,bin,sys,security,cron,audit,lp</td>
</tr>
<tr>
<td>Feb 24 16:18:51</td>
<td>AXSERVER</td>
<td>root</td>
<td>init</td>
<td>PROC_ReaIGD</td>
<td>OK</td>
<td>old rgid: 0, new gid: 0, which: rgnoregid: gid new priority: 2</td>
</tr>
<tr>
<td>Feb 24 20:58:30</td>
<td>AXSERVER</td>
<td>root</td>
<td>cron</td>
<td>PROC_SetPri</td>
<td>OK</td>
<td></td>
</tr>
</tbody>
</table>

**IBM AIX: Logical volume management activity**
This report provides information related to creation and deletion of logical volume.

**PROC_Sysconfig root OK Mon Jan 22 15:00:01 2007 lslv 3**

**PROC_Environ root OK Wed Jan 31 13:07:36 2007 srcmstr**

**PROC_Limits root OK Fri Jan 19 16:11:52 2007 init**

**PROC_SetPri root OK Mon Jan 22 20:58:00 2007 cron new priority: 2**

**PROC_Privilege root OK Thu Jan 18 11:30:00 2007 cron cmd: 30004 privset: 0:0**


**PROC_Setpgid root OK Wed Jan 17 15:11:29 2007 bash**

**PROC_SetGroups root OK Fri Jan 19 16:18:51 2007 init group set: system,bin,sys,security,cron,audit,lp**

**LVM_CreateLV root OK Tue Jan 23 21:18:02 2007 lcreatelv Logical Volume Name =fslv01 Mirror Write Consistency = 1 Stripe Width = 0**
**IBM AIX: Password changed**
This report provides information related to password changed, that user root has changed the password for the users specified in the message details.

<table>
<thead>
<tr>
<th>When</th>
<th>Computer</th>
<th>Who</th>
<th>Command</th>
<th>Command</th>
<th>Action</th>
<th>Status</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 22 20:20:20 2016</td>
<td>AIXSERVER</td>
<td>root</td>
<td>passwd</td>
<td></td>
<td>PASSWORD_Change</td>
<td>OK</td>
<td>William</td>
</tr>
<tr>
<td>Jan 22 20:20:20 2016</td>
<td>AIXSERVER</td>
<td>root</td>
<td>passwd</td>
<td></td>
<td>PASSWORD_Change</td>
<td>OK</td>
<td>Ellen</td>
</tr>
</tbody>
</table>

**PASSWORD_Change root OK Mon Jan 22 20:20:20 2007 passwd William**

**PASSWORD_Change root OK Mon Jan 22 20:20:20 2007 passwd Ellen**

**IBM AIX: Security objects audit**
This report provides information audit being performed on the security objects by the user.

<table>
<thead>
<tr>
<th>When</th>
<th>Computer</th>
<th>Who</th>
<th>Command</th>
<th>Command</th>
<th>Action</th>
<th>Status</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 11 19:30:33 2016</td>
<td>AIXSERVER</td>
<td>william</td>
<td>su</td>
<td></td>
<td>S_PASSWD_READ</td>
<td>OK</td>
<td>audit object read event detected /etc/security/passwd</td>
</tr>
<tr>
<td>Jul 12 14:00:00 2016</td>
<td>AIXSERVER</td>
<td>william</td>
<td>cron</td>
<td></td>
<td>S_ENVIRON_WRITE</td>
<td>FAIL</td>
<td>audit object write event detected /etc/security/environ</td>
</tr>
<tr>
<td>Jul 12 14:00:00 2016</td>
<td>AIXSERVER</td>
<td>william</td>
<td>cron</td>
<td></td>
<td>S_USER_WRITE</td>
<td>FAIL</td>
<td>audit object write event detected /etc/security/user</td>
</tr>
</tbody>
</table>

**S_PASSWD_READ william OK Sat Jul 11 19:30:33 1970 su audit object read event detected /etc/security/passwd**

**S_USER_WRITE william FAIL Sun Jul 12 14:00:00 1970 cron audit object write event detected /etc/security/user**

**S_ENVIRON_WRITE william FAIL Sun Jul 12 14:00:00 1970 cron audit object write event detected /etc/security/environ**

**IBM AIX: System resource controller**
This report provides the information related to subroutines and subsystem on the server.
Integrate IBM AIX

SRC_Start root OK Tue Jan 30 16:56:29 2007 srcmstr biod

SRC_Stop root OK Tue Jan 30 17:19:10 2007 srcmstr qdaemon

SRC_Addssys root OK Tue Jan 30 17:23:13 2007 mkssys IBM.CSMAgentRM subsysname=IBM.CSMAgentRM synonym= cmdargs= path=/usr/sbin/rsct/bin/IBM.CSMAgentRMd uid=0 auditid=0 standin=/dev/console standout=/dev/console standerr=/var/ct/IBM.CSMAgentRM.stderr action=1 multi=0 contact=3 svrkey=0 svrmtype=0 priority=20 signorm=0 sigforce=0 display=1 waittime=20 grpname=rsct_rm

SRC_Chssys root OK Tue Jan 30 17:10:50 2007 chssys rpc.statd

SRC_Delssys root OK Tue Jan 30 17:23:13 2007 rmssys IBM.AuditRM

IBM AIX: User authentication failed
This report provides information related to user authentication failed logins.

USER_Login root FAIL_AUTH Mon Jan 07 10:47:52 2013 tsm user: joesmith tty: /dev/pts/33

USER_Login root FAIL_AUTH Mon Jan 07 10:47:52 2013 tsm user: william tty: /dev/pts/2

IBM AIX: User management
This report provides information related to user created, removed and changed details.
Integrate IBM AIX

<table>
<thead>
<tr>
<th>When</th>
<th>Computer</th>
<th>Who</th>
<th>Command</th>
<th>Action</th>
<th>Status</th>
<th>Target Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 22 15:11:16</td>
<td>AIKSERVER2</td>
<td>root</td>
<td>muser</td>
<td>USER_Create</td>
<td>OK</td>
<td>Ellen Adams</td>
</tr>
<tr>
<td>Feb 22 15:34:46</td>
<td>AIKSERVER2</td>
<td>root</td>
<td>rmuser</td>
<td>USER_Remove</td>
<td>OK</td>
<td>Allen Brewer</td>
</tr>
<tr>
<td>Feb 22 17:29:57</td>
<td>AIKSERVER2</td>
<td>root</td>
<td>reboot</td>
<td>USER_Reboot</td>
<td>OK</td>
<td>root login status time command</td>
</tr>
<tr>
<td>Feb 22 20:45:27</td>
<td>AIKSERVER2</td>
<td>root</td>
<td>chuser</td>
<td>USER_Change</td>
<td>OK</td>
<td>Lisa Andrews admin=true</td>
</tr>
<tr>
<td>Feb 22 20:53:55</td>
<td>AIKSERVER2</td>
<td>root</td>
<td>su</td>
<td>USER_SU</td>
<td>OK</td>
<td>Ellen Adams</td>
</tr>
<tr>
<td>Feb 22 21:03:45</td>
<td>AIKSERVER2</td>
<td>root</td>
<td>setgroups</td>
<td>USER_SetGroups</td>
<td>FAIL</td>
<td>staff finance</td>
</tr>
</tbody>
</table>

**USER_Change root OK Mon Jan 22 20:45:27 2007 chuser Lisa Andrews admin=true**

**USER_Remove root OK Wed Jan 17 15:34:46 2007 rmuser Allen Brewer**

**USER_Create root OK Wed Jan 17 15:11:16 2007 mkuser Ellen Adams**

**USER_SU root OK Tue Jan 23 20:53:55 2007 su Ellen Adams**

Import Knowledge Pack into EventTracker

**NOTE**: Import knowledge pack items in the following sequence

- Categories
- Alerts
- Token Templates
- Flex Reports
- Knowledge Object

1. Launch **EventTracker Control Panel**.

2. Double click **Export/Import Utility**, and then click the **Import** tab.
Import Categories, Alerts, Flex Reports and Knowledge Objects as given below.

**Categories**

1. Click **Category** option, and then click the browse button.
2. Locate All IBM AIX categories.iscat file, and then click the Open button.

3. To import categories, click the Import button.

   EventTracker displays success message.

4. Click OK, and then click the Close button.
Integrate IBM AIX

Alerts

1. Click **Alert** option, and then click the **browse** button.

![Figure 4](image)

2. Locate **All IBM AIX alerts.isalt** file, and then click the **Open** button.

3. To import alerts, click the **Import** button.

EventTracker displays success message.
Integrate IBM AIX

5. Click OK, and then click the Close button.

Token Templates

1. Click the Admin menu, and then click Parsing rule.

2. Select Template tab, and then click on ‘Import’ option.

3. Click on Browse button.
4. Locate **All IBM AIX token template.ettd** file, and then click the **Open** button

5. Now select the check box and then click on **Import** option. EventTracker displays success message.

6. Click on **OK** button.

**Flex Reports**

1. Click **Report** option, and then click the browse button.
Integrate IBM AIX

2. Locate the **All IBM AIX flex reports.issch** file, and then click the **Open** button.
3. Click the **Import** button to import the scheduled reports, EventTracker displays success message.

Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on **Import** option.
3. In **IMPORT** pane click on **Browse** button.

4. Locate **All IBM AIX knowledge object.etko** file, and then click the **UPLOAD** button.
5. Now select the check box and then click on 'OVERWRITE' option. EventTracker displays success message.

6. Click on OK button.
Integrate IBM AIX

Verifying IBM AIX knowledge pack in EventTracker

IBM AIX Categories

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Categories.
3. In Category Tree to view imported categories, scroll down and expand IBM AIX group folder to view the imported categories.

![Figure 18](image)

IBM AIX Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In Search field, type 'IBM AIX', and then click the Go button.

Alert Management page will display all the imported IBM AIX alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

![Message Box](image)

**Figure 20**

5. Click **OK**, and then click the **Activate Now** button.

**NOTE:**
You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.
IBM AIX Token Template

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Parsing Rules.

![IBM AIX Token Template](image)

IBM AIX Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then select Configuration.
3. In Reports Configuration pane, select Defined option.
   
   EventTracker displays Defined page.

4. In search box enter 'IBM AIX', and then click the Search button.
   
   EventTracker displays Flex reports of IBM AIX
IBM AIX Knowledge Object

1. Click the Admin menu, and then click Knowledge Objects
2. Scroll down and select IBM AIX in Objects pane. Imported IBM AIX object details are shown.
Create Flex Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.

2. Navigate to Reports>Configuration.
3. Select **IBM AIX** in report groups. Check **defined** dialog box.

4. Click on 'schedule' to plan a report for later execution.
5. Choose appropriate time for report execution and in **Step 8** check **Persist data in Eventvault explorer** box.

![REPORT WIZARD](image)

6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
7. Proceed to next step and click **Schedule** button.
8. Wait for scheduled time or generate report manually.
Create Dashlets

1. **EventTracker 8** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.

3. Navigate to **Dashboard>Flex**. Flex Dashboard pane is shown.

4. Fill suitable title and description and click **Save** button.
5. Click 🔄 to configure a new flex dashlet. Widget configuration pane is shown.

![Widget Configuration](image)

**Figure 30**

6. Locate earlier scheduled report in **Data Source** dropdown.
7. Select **Chart Type** from dropdown.
8. Select extent of data to be displayed in **Duration** dropdown.
9. Select computation type in **Value Field Setting** dropdown.
10. Select evaluation duration in **As Of** dropdown.
11. Select comparable values in **X Axis** with suitable label.
12. Select numeric values in **Y Axis** with suitable label.
13. Select comparable sequence in **Legend**.
14. Click **Test** button to evaluate. Evaluated chart is shown.
15. If satisfied, Click **Configure** button.

16. Click ‘customize’ to locate and choose created dashlet.
17. Click **+** to add dashlet to earlier created dashboard.
Sample Flex Dashboards

1. IBM AIX-Administrator logon activity

Figure 33
2. IBM AIX-User authentication failed

![Figure 34](image)

3. IBM AIX-Security objects audit

![Figure 35](image)