AIX

Background

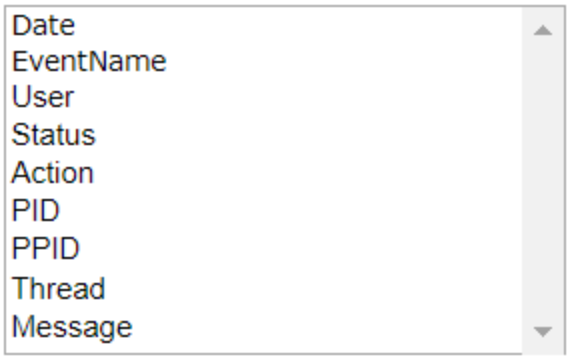
The AIX Servers logs analysis App automatically Collect - Read - Parse - Analyzes - Reports all machine generated log data of the server and presents a comprehensive set of graphs and reports to analyze machine generated data. Use a predefined set of dashboards and gadgets to visualize and address the system software, code written, and infrastructure during development, testing, and production. This AIX logs analysis App helps measure, troubleshoot, and optimize your servers integrity, stability and quality with the several visualization and investigation dashboards.

Steps:

1. The Aix App is running on the audit standard log.
   When adding/editing the logs to XpoLog it is mandatory to apply the correct log type(s) to each of the log.
   a. **aix** - all logs that the application will analyze must have **aix** as a log type.
   b. **audit**- only the audit logs must also be configured to have **audit** as a log type.
   c. **basic** - only the basic audit logs must also be configured to have **basic** as a log type.
   d. **advanced** - only the advanced audit logs must also be configured to have **advanced** as a log type.

2. Once the required information is set, on each log click next and edit the log pattern, this step is crucial to the accuracy and deployment of the Linux App. Use the following patterns for each of the logs:
   a. basic audit log:
   {regexp:Date,refName=Message;columnType=date;dateFormat=EEE MMM dd HH:mm:ss yyyy,(\w\w\w \w\w\w \d\d \d\d:\d\d:\d\d \d\d\d\d)}{regexp:EventName,ftype=eventName;refName=Message,(^\S*)}{regexp:Status,ftype=status;refName=Message,\w+\s+\w+\s+([^\S]\w+\s+)\s}{regexp:User1,refName=Message,\w+\s+(.*)}{regexp:User,ftype=username;refName=User1,(^\S*)}{regexp:Action,ftype=message;refName=Message,\d\d\d\d\s(.*)}{string:Message}
   Then, edit the log->customize->layout and set the right layout table as follows:

   b. advanced audit log:
   first pattern:
   {regexp:Date,refName=Message;columnType=date;dateFormat=EEE MMM dd HH:mm:ss yyyy,(\w\w\w \w\w\w \d\d \d\d:\d\d:\d\d \d\d\d\d)}{regexp:EventName,ftype=eventName;refName=Message,(^\S*)}{regexp:user1,refName=Message,\w+\s+(.*)}{regexp:User,ftype=username;refName=user1,(^\S*)}{regexp:Action,ftype=Message;refName=Message,\d\d\d\d\s([^\s]\w+)}{regexp:PID,ftype=auditid=refName=Message,\d\d\d\d\s\w+\s+\w+\s+(\d+)}{regexp:PPID,refName=Message,\d\d\d\d\s\w+\s+\w+\s+\d+\s+(\d+)}{regexp:Thread,refName=Message,\d\d\d\d\s\w+\s+\w+\s+\d+\s+\d+\s+(\d+)}{regexp:status1,refName=Message,\w+\s+\w+\w\s+(.*)}{regexp:Status,ftype=status;refName=status1,(^\S*)}{string:Message} <{text:text}>
   second pattern:
   {regexp:Date,refName=Message;columnType=date;dateFormat=EEE MMM dd HH:mm:ss yyyy,(\w\w\w \w\w\w \d\d \d\d:\d\d:\d\d \d\d\d\d)}{regexp:EventName,ftype=eventName;refName=Message,(^\S*)}{regexp:user1,refName=Message,\w+\s+(.*)}{regexp:User,ftype=username;refName=user1,(^\S*)}{regexp:Action,ftype=Message;refName=Message,\d\d\d\d\s([^\s]\w+)}{regexp:PID,ftype=auditid;refName=Message,\d\d\d\d\s\w+\s+\w+\s+(\d+)}{regexp:PPID,refName=Message,\d\d\d\d\s\w+\s+\w+\s+\d+\s+(\d+)}{regexp:Thread,refName=Message,\d\d\d\d\s\w+\s+\w+\s+\d+\s+\d+\s+(\d+)}{regexp:status1,refName=Message,\w+\s+\w+\w\s+(.*)}{regexp:Status,ftype=status;refName=status1,(^\S*)}{string:Message}{eol}{text:text}
   Then, edit the log->customize->layout and set the right layout table as follows:


Date
EventName
User
Status
Action
PID
PPID
Thread
Message