SINE NOMINE ASSOCIATES

OpenAFS Audit Interface Enhancements

Cheyenne Wills

OpenAFS 2019 Workshop

Overview

SINE NOMINE ASSOCIATES

- **Multiple Interfaces**
- **Multiple Instances of an interface**
- **New FIFO (named pipe) interface**
- **Collecting information from the audit facility**

Multiple Interfaces

SINE NOMINE ASSOCIATES

- **What's New**
  - **Multiple audit logs**
  - **New format for -auditlog**

*interface-name:*filespec*:interface params*

```
-auditlog file:/tmp/auditfile
-auditlog sysvmq:/tmp/mqtok -auditlog /tmp/auditfile
-audit-interface sysvmq -auditlog /tmp/mqtok -auditlog
file:/auditfile
```

Multiple Interfaces

SINE NOMINE ASSOCIATES

- **What changed**
  - **-audit-interface. Sets a default audit interface**
  - **Internally, audit.c uses a list of "active" interfaces and invokes the the "audit_ops" function on each element in the list**

Multiple instances of an interface

SINE NOMINE ASSOCIATES

- **What's New**
  - **Multiple instances of the same interface**

```
-auditlog /tmp/auditlog1 -auditlog /tmp/auditlog2
-audit-interface sysvmq -auditlog /tmp/mq1 -auditlog /tmp/mq2
-auditlog /tmp/a1 -auditlog /tmp/a2 -auditlog sysvmq:/tmp/mq1
```

Multiple instances of an interface

SINE NOMINE ASSOCIATES

- **What changed (internals)**
  - **“Relocated” append_msg from the individual interfaces into audit.c**
  - **Reduce the scope of the audit lock**

pipe audit interface

SINE NOMINE ASSOCIATES

- **New audit interface - pipe**
  - **Creates a new named pipe or reuses an existing named pipe**
  - **Creates a separate thread and buffer to avoid blocking the callers of the audit facility**

pipe audit interface - cont

SINE NOMINE ASSOCIATES

- **Problem: Named pipes will block when a reader process is not connected, or the reader process doesn't consume the data**
- **Solution: A separate thread is used to to handle all operations on the named pipe**

pipe audit interface - cont

SINE NOMINE ASSOCIATES

- **Buffers are used to pass data from the main audit facility into the pipe interface thread**
- **Audit records will be dropped if the buffers fill**
  - **Pipe is not connected to a reader process**
  - **Reader process doesn't consume data "fast" enough**

pipe audit interface - cont

- **Size of the buffer is configurable via a parameter specified in the -auditlog parameters**

```
-auditlog pipe:/tmp/pipe:buf=16M
```

pipe audit interface - cont

SINE NOMINE ASSOCIATES

- **Monitoring dropped audit events**
  - **Audit events produced by the pipe interface are prefixed by a sequence number to assist in tracking dropped event messages.**

```
[18911] Fri May 3 09:00:49 2019 [131] EVENT AFS_SRX_RmFile CODE 0 NAME admin HOST 10.0.0.198 ID
1 FID 536870918:39:7009 STR posix_types.h
```

  - **A new audit event record, AFS_Aud_Pipe_Dropped, reports if audit events have been dropped**

```
[34218] Fri May 3 09:03:14 2019 EVENT AFS_Aud_Pipe_Dropped COUNT 15304 FIRST 1556895649 FIRSTID
18912 LAST 1556895671 LASTID 34217
```

pipe audit interface - cont

SINE NOMINE ASSOCIATES

- **During a performance test, ~200K to ~250K audit messages/sec***

  *** Professional driver on a closed track, your mileage may vary depending on road conditions, etc.**

Interface considerations

SINE NOMINE ASSOCIATES

- **Other than adding support for multiple instances, the file and sysvmq interfaces behave as before**
- **Running multiple file or sysvmq interfaces may have a negative impact on overall performance of the audit facility**

Using the audit facility

SINE NOMINE ASSOCIATES

The OpenAFS services each have their own audit events

Historical list of audit events are documented in the OpenAFS Admin Guide in appendix D - AIX Audit Events

Using the audit facility - cont

SINE NOMINE ASSOCIATES

- **Recording audit events into kafka**
  - `-auditlog pipe:/tmp/kafkapipe`

```
./kafka-console-producer.sh --topic afs_fileserver --broker-list
kafkaserver.example.com :9092 < /tmp/kafkapipe
```

- **Almost replicating the file interface**
  - `-auditlog pipe:/tmp/pipe`

```
cp /tmp/pipe /tmp/auditfile
```

Using the audit facility - cont

SINE NOMINE ASSOCIATES

- **Traditional "auditing"**
  - **When did some "event" happen**
- **Monitoring for volume or file activity**
  - **Inactive objects, usage patterns**

Future

SINE NOMINE ASSOCIATES

- **Currently only the fileserver command line has been updated to support multiple interfaces**
- **Add command line support to remaining services**
- **Internal reviews**
- **Submit to master**