Tips and Best Practices for ESM Performance

Nordine Tbahriti

March 2014

Agenda

After completing this presentation you should be able to understand:

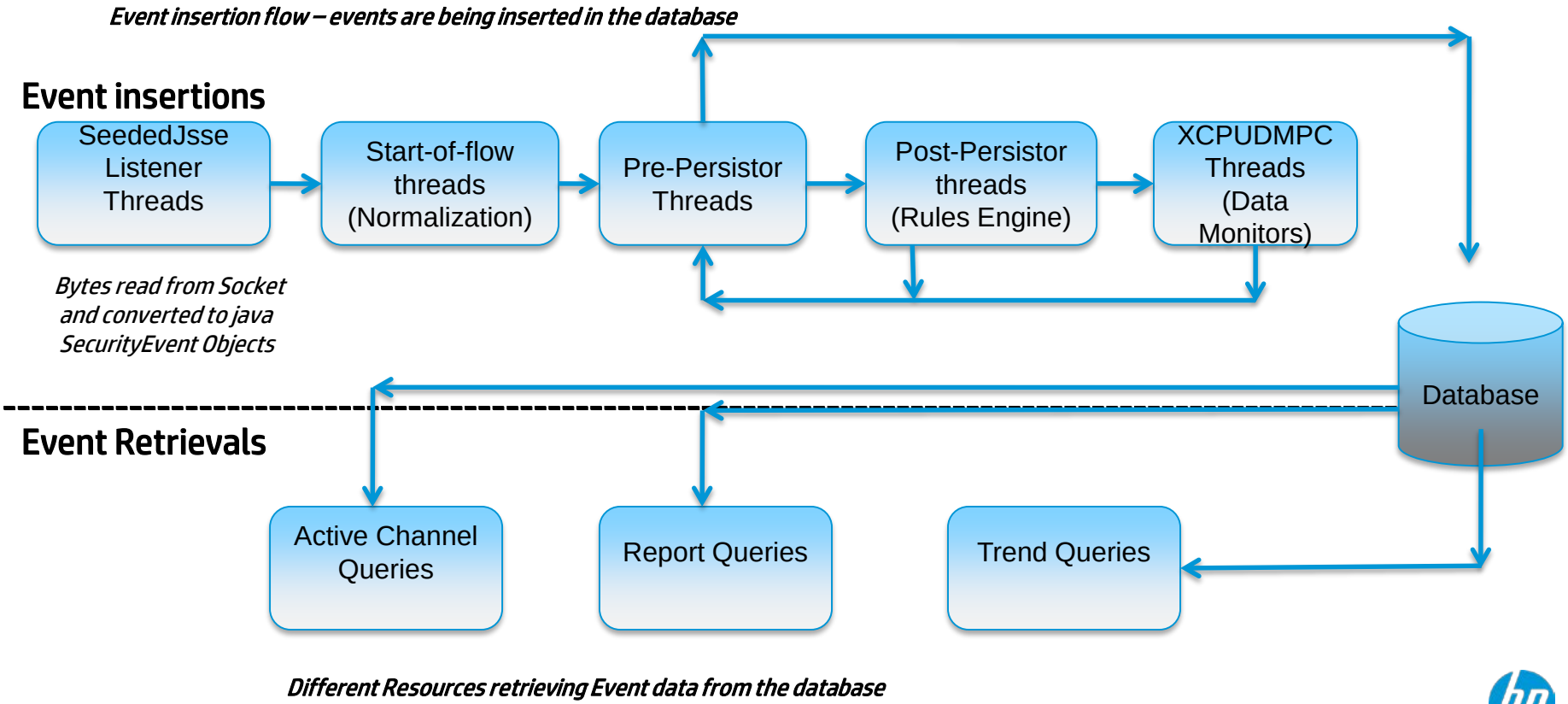
- Data flow
- Symptoms of Performance Issues
- Logs and Data Collection
- Data Analysis
- Monitoring ESM
- Thread dumps
- Best Practices

Objective

- Maintain and improve ESM performance

Data Flow

Events Insertion versus Events Retrieval



Symptoms of Performance Issues

Symptoms of Performance Issues

Event Data Retrieval

- Channels slow to load
- Channels don't finish loading
  - Channels show *Loading Event ID*
- Reports failing or not running
  - *ORA-01555* or *user cancelled operation*
- Reports based on trends are empty
- Trends failing or not running
- Trends getting disabled

Symptoms of Performance Issues

Event Data Insertion

- Connectors caching continuously
- Connector status shifting between up and down frequently
- Manager logs show one of the following
  - *It appears the database is hung*
  - Rejected threads
- Delayed events (maybe not)

Symptoms of Performance Issues

Post-Aggregation vs Sent Manager EPS

Queues filling caused by

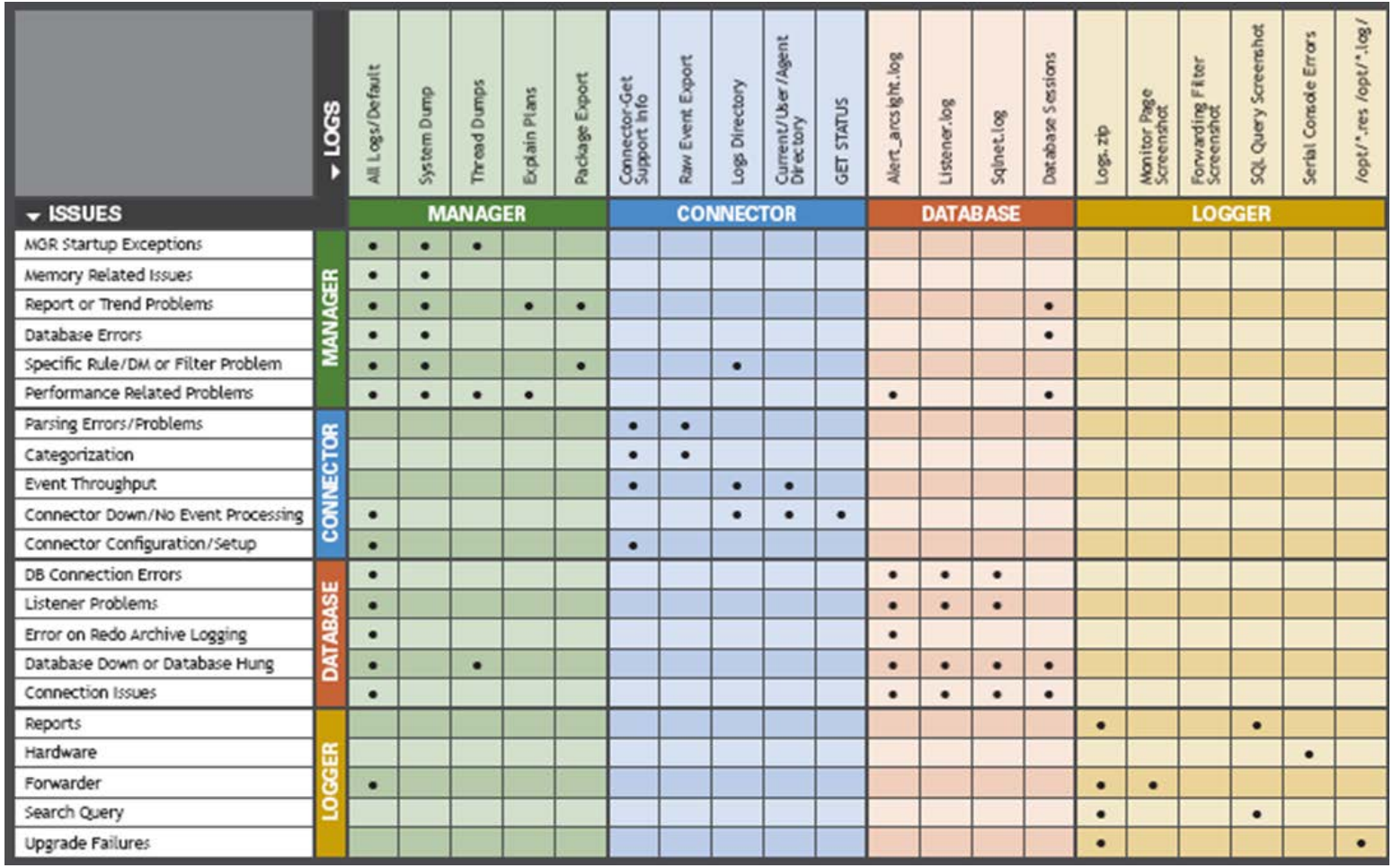
- Database performance
- Disk I/O
- Slow rules engine processing
- Slow data monitor processing

Symptom

- Events Cache
- STM eps < P-A eps

Post-Filter Count	Post-Filter EPS	Post-Aggregation Count	Post-Aggregation EPS	Estimated Cache Size	Sent To Manager Count	Sent To Manager EPS
0	0.0	0	0.0	0	0	0.0
25922	312.3	25798	310.8	14000	11800	142.2
25,922	312.3	25,798	310.8	14,000	11,800	142.2

Logs and Data Collection



Application Logs

Manager

- <ARCSIGHT_HOME>/logs/default/*.log*
  - SERVER.LOG
  - SERVER.STD.LOG
  - SERVER.STATUS.LOG
  - SERVER.REPORT.LOG
  - SERVER.SQL.LOG
  - SERVER.LICENSE.LOG
  - PARTITIONMANAGER.LOG
  - PARTITIONARCHIVER.LOG
  - PARTITIONCOMPRESSER.LOG
  - PARTITIONSTATSUPDATER.LOG

Oracle

- <ORACLE_HOME>
  - /admin/arcsight/bdump/ALERT_<LISTENER>.LOG
  - /network/log/LISTENER.LOG
  - /network/log/SQLNET.LOG

CORR-Engine

- /opt/arcsight/logger/current/arcsight/logger/logs/*
- /opt/arcsight/logger/data/mysql/*.log*
- /opt/arcsight/logger/data/pgsql/serverlog*

Data Analysis

Data to Collect (Data Insertion)

99% of time, bottleneck found on Manager

Thread Dumps

- Generate five thread dumps with Session data

Logs

- Manager Logs
- Oracle based Manager
  - Alert Log
  - DB Sessions
- CORR-E based Manager
  - Session Waits
  - mysql.log

System Tables

- If reproduction to be performed

Agent Logs

- If Manager is not identified as the bottleneck
  - Agent stability
  - Network connectivity
  - Network latency
- Save time and collect when generating TDs

Data to Collect (Data Retrieval)

99% of time, bottleneck found on Manager

Logs

- All the Manager logs

Oracle Based Manager

- Partition Info report
- Alert logs
- Explain Plans
- RDA
- CPU/PSU inventory (lsinventory)

CORR-Engine Based Manager

- mysql.log

Database Connectivity

SERVER.STD.LOG

- Connectivity Issues
  - SERVER.STD.LOG
    - SUBSYSTEM STATUS CHANGED
    - Received exception while trying to check connectivity to the database: Communications link failure

- Persistence Rate
  - should take less than 100ms
    - INFO | jvm 2 | 2009/05/07 20:41:58 | (02-Pre-SecurityEventPersistor330) Persisted 100 events in 32 ms.
    - INFO | jvm 1 | 2009/05/08 11:20:53 | (02-Pre-SecurityEventPersistor1) Persisted 100 events in **3,698 ms**

Manager Busy

SERVER.STD.LOG

- Manager stops accepting events
  - INFO | jvm 1 | 2005/04/04 00:42:26 | WARNING: '1' agent requests REJECTED because the limit of '64' agent threads was exceeded.

Monitoring ESM

Whine Messages

System Alerts via E-Mail

Why

- Subsystem Failures
  - Database connection problem
  - Event insertion times high
  - SSL certificate expiration
- Database space shortage
  - Running out of space
  - Usually event space
  - Sometimes system table space
- Partition Manager Failures
  - Get your DBA!!!

Where

- stdout, server.std.log, server.log
- E-mail
- Console pop-up
- Internal Event

Memory Usage

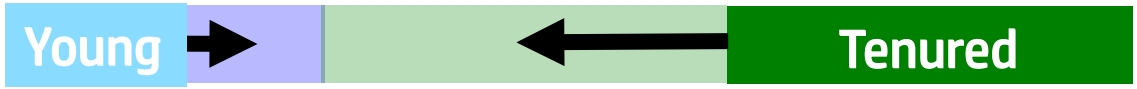
- Manager allocates memory in Java heap
- Server.std.log

```
2006/02/22 23:22:51 | Memory Status: 765.6 MB Used, 1,014.0 MB Max
2006/02/22 23:22:52 | [Full GC
2006/02/22 23:22:58 | 797362K->471587K(1038336K), 5.9847261 secs]
```

- Java heap is garbage collected
  - Server only allocates memory
  - Java VM reclaims unused memory automatically
  - Manager doesn't know how much garbage is in the heap
- Reported memory usage includes garbage

Two Types of Garbage Collection (GC)

Java heap is divided into generations



Minor GC

Only collects young generation

May expand to entire heap, and become a major collection

```
[GC 929899K->838966K(1036928K), 0.0353791 secs]
```

Major GC or Full GC

Collects both young generation and tenured generation

```
[Full GC 932135K->542955K(1036928K), 3.9721866 secs]
```

GC pause

Stop the world GC

When GC is happening, everything else is stopped

Pause Time

```
[Full GC 932135K->542955K(1036928K), 3.9721866 secs]
```

Minor GC pause (“[GC ...]”)

Should be under 1 sec

Major GC pause (“[Full GC ....]”)

Actual time depends on Hardware

Estimate: ~1 sec every 200 MB Heap

Real Memory Usage – The Working Set

Real memory usage is captured in “Full GC” messages

server.std.log

```
2006/02/22 23:22:51 | Memory Status: 765.6 MB Used, 1,014.0 MB Max
2006/02/22 23:22:52 | [Full GC
2006/02/22 23:22:58 | 797362K->471587K(1038336K), 5.9847261 secs]
```

Working Set is defined as the memory that is in actual use and doesn’t have any garbage. Working set of the Manager can be found as above, immediately after a “Full GC”

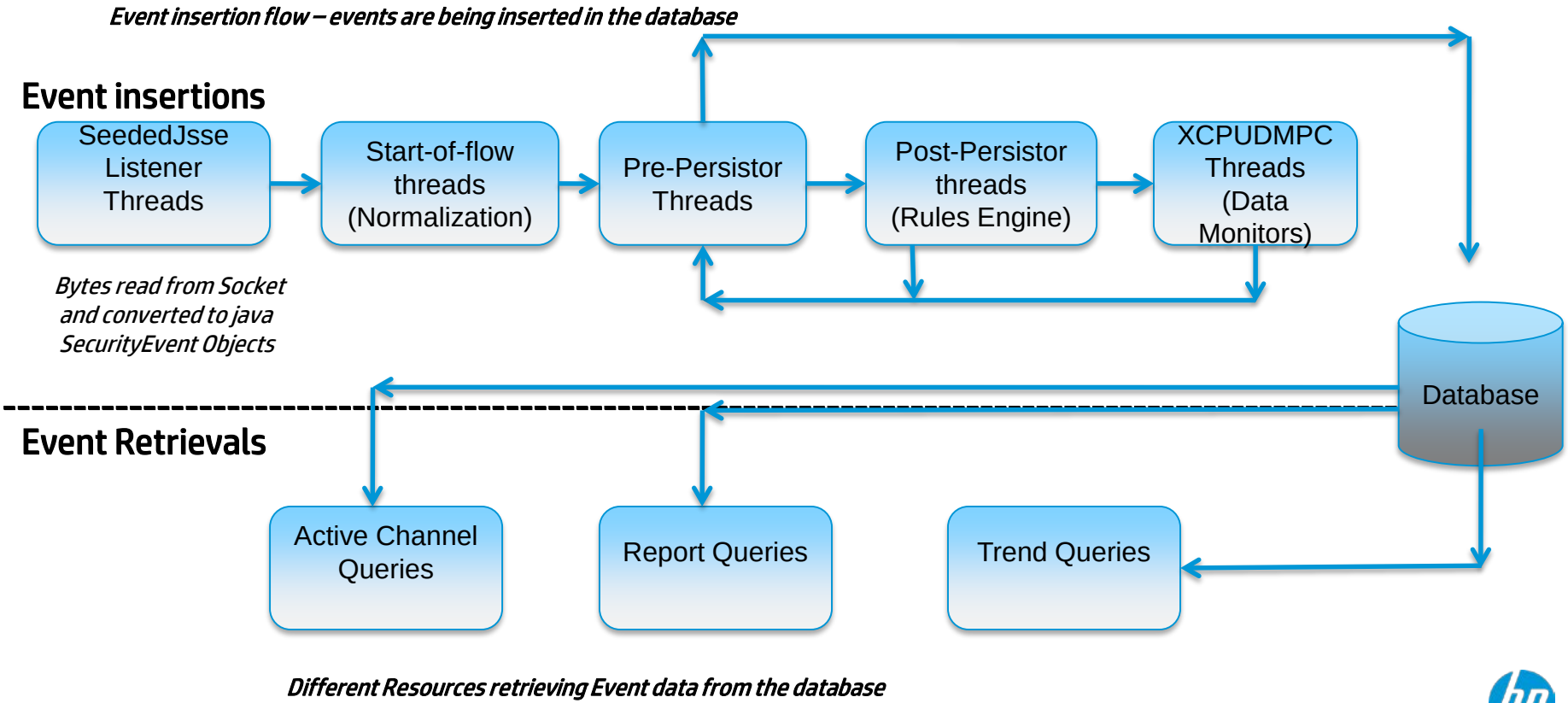
Out of Memory

Server will restart on out of memory errors

- Multiple memory intensive tasks at the same time may *spike* memory
- Memory *leak* usually symptomatic of loose filters
- Increasing heap size only delays the problem
- Memory leak is hard to track down
- Look for hprof files if Out of Memory error occurs and send to Support

Thread Dumps

Insertion issues require Thread Dumps



A Java Snapshot

Don’t restart or reboot before collecting thread dumps!

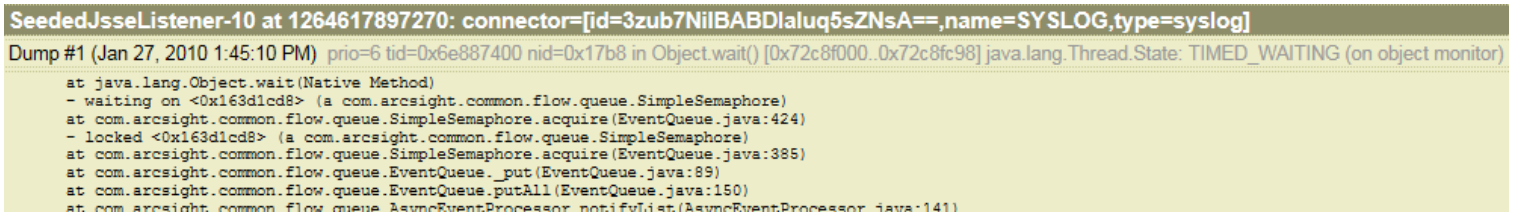
Why Thread Dumps

- Stack trace for each thread in the VM
- Many different threads
- Bottleneck area usually identifiable
  - Session Waits or DB Sessions needed to correlate database activity

Servlet Engine

SeededJsseListener

- Read bytes from network sockets
- Convert read bytes to Java Objects “Security Event Batch”
- Place event batches into queue for Flow 1



Flow 1: Start

Start-Of-Flow

- Vulnerability Scanner Reports
- Place event batches into queue for Flow 2

01-Start-Of-Flow0

Dump #1 (Jan 15, 2010 5:18:15 PM) daemon prio=6 tid=0x0000000009fb0c00 nid=0x117c in Object.wait() [0x000000000fdde000..0x000000000fddf860] java.lang.Thread.State: TIMED_WAITING (on object monitor)
Dump #2 (Jan 15, 2010 5:18:39 PM) daemon prio=6 tid=0x0000000009fb0c00 nid=0x117c in Object.wait() [0x000000000fdde000..0x000000000fddf860] java.lang.Thread.State: TIMED_WAITING (on object monitor)
Dump #3 (Jan 15, 2010 5:20:17 PM) daemon prio=6 tid=0x0000000009fb0c00 nid=0x117c in Object.wait() [0x000000000fdde000..0x000000000fddf860] java.lang.Thread.State: TIMED_WAITING (on object monitor)
Dump #4 (Jan 15, 2010 5:21:08 PM) daemon prio=6 tid=0x0000000009fb0c00 nid=0x117c in Object.wait() [0x000000000fdde000..0x000000000fddf860] java.lang.Thread.State: TIMED_WAITING (on object monitor)
Dump #5 (Jan 15, 2010 5:22:17 PM) daemon prio=6 tid=0x0000000009fb0c00 nid=0x117c in Object.wait() [0x000000000fdde000..0x000000000fddf860] java.lang.Thread.State: TIMED_WAITING (on object monitor)
Dump #6 (Jan 15, 2010 5:23:35 PM) daemon prio=6 tid=0x0000000009fb0c00 nid=0x117c in Object.wait() [0x000000000fdde000..0x000000000fddf860] java.lang.Thread.State: TIMED_WAITING (on object monitor)

```
at java.lang.Object.wait(Native Method)
- waiting on <0x00000000a8cf4fb8> (a com.arcsight.common.flow.queue.SimpleSemaphore)
at com.arcsight.common.flow.queue.SimpleSemaphore.acquire(EventQueue.java:424)
- locked <0x00000000a8cf4fb8> (a com.arcsight.common.flow.queue.SimpleSemaphore)
at com.arcsight.common.flow.queue.SimpleSemaphore.acquire(EventQueue.java:385)
at com.arcsight.common.flow.queue.EventQueue._put(EventQueue.java:89)
at com.arcsight.common.flow.queue.EventQueue.putAll(EventQueue.java:150)
at com.arcsight.common.flow.queue.AsyncEventProcessor.notifyList(AsyncEventProcessor.java:140)
```

Flow 2: Pre Persistor

Pre-SecurityEventPersistor

- Remove event from batch from queue
- Initialize and normalize event fields
- Write to database
- Put event batch in to queue for Flow 3

02-Pre-SecurityEventPersistor1

Dump #1 (Jan 15, 2010 5:18:15 PM) daemon prio=6 tid=0x0000000011869800 nid=0x1594 in Object.wait() [0x0000000016b9f000..0x0000000016b9fa60] java.lang.Thread.State: TIMED_WAITING (on object monitor)
Dump #2 (Jan 15, 2010 5:18:39 PM) daemon prio=6 tid=0x0000000011869800 nid=0x1594 in Object.wait() [0x0000000016b9f000..0x0000000016b9fa60] java.lang.Thread.State: TIMED_WAITING (on object monitor)
Dump #3 (Jan 15, 2010 5:20:17 PM) daemon prio=6 tid=0x0000000011869800 nid=0x1594 in Object.wait() [0x0000000016b9f000..0x0000000016b9fa60] java.lang.Thread.State: TIMED_WAITING (on object monitor)
Dump #4 (Jan 15, 2010 5:21:08 PM) daemon prio=6 tid=0x0000000011869800 nid=0x1594 in Object.wait() [0x0000000016b9f000..0x0000000016b9fa60] java.lang.Thread.State: TIMED_WAITING (on object monitor)
Dump #5 (Jan 15, 2010 5:22:17 PM) daemon prio=6 tid=0x0000000011869800 nid=0x1594 in Object.wait() [0x0000000016b9f000..0x0000000016b9fa60] java.lang.Thread.State: TIMED_WAITING (on object monitor)
Dump #6 (Jan 15, 2010 5:23:35 PM) daemon prio=6 tid=0x0000000011869800 nid=0x1594 in Object.wait() [0x0000000016b9f000..0x0000000016b9fa60] java.lang.Thread.State: TIMED_WAITING (on object monitor)

```
    at java.lang.Object.wait(Native Method)
    - waiting on <0x00000000a8e3c618> (a com.arcsight.common.flow.queue.SimpleSemaphore)
    at com.arcsight.common.flow.queue.SimpleSemaphore.acquire(EventQueue.java:424)
    - locked <0x00000000a8e3c618> (a com.arcsight.common.flow.queue.SimpleSemaphore)
    at com.arcsight.common.flow.queue.SimpleSemaphore.acquire(EventQueue.java:385)
    at com.arcsight.common.flow.queue.EventQueue._put(EventQueue.java:89)
    at com.arcsight.common.flow.queue.EventQueue.putAll(EventQueue.java:150)
    at com.arcsight.common.flow.queue.AsyncEventProcessor.notifyList(AsyncEventProcessor.java:140)
```

Flow 3: Post Persistor

Post-SecurityEventPersistor

- Remove event from batch from queue
- Evaluate events against rules
- Generate Correlation events
- Put event batch in to queue for Dashboards

03-Post-SecurityEventPersistor0

Dump #1 (Jan 22, 2010 2:22:14 PM) daemon prio=6 tid=0x6e361400 nid=0x5e0 in Object.wait() [0x6fd0f000..0x6fd0fd98] java.lang.Thread.State: WAITING (on object monitor)

```
at java.lang.Object.wait(Native Method)
- waiting on <0x1112d530> (a com.arcsight.common.flow.queue.SimpleSemaphore)
at java.lang.Object.wait(Object.java:485)
at com.arcsight.common.flow.queue.SimpleSemaphore.acquire(EventQueue.java:425)
- locked <0x1112d530> (a com.arcsight.common.flow.queue.SimpleSemaphore)
at com.arcsight.common.flow.queue.EventQueue.take(EventQueue.java:299)
at com.arcsight.common.flow.queue.AsyncEventProcessor$ProcessorThread.run(AsyncEventProcessor.java:257)
```

Dump #3 (Jan 13, 2010 4:13:36 PM) daemon prio=6 tid=0x783fc800 nid=0x12a4 waiting for monitor entry [0x733cf000..0x733cfd98] java.lang.Thread.State: BLOCKED (on object monitor)

Dump #4 (Jan 13, 2010 4:13:43 PM) daemon prio=6 tid=0x783fc800 nid=0x12a4 waiting for monitor entry [0x733cf000..0x733cfd98] java.lang.Thread.State: BLOCKED (on object monitor)

```
at com.arcsight.server.dashboard.FilterOptimizedMultiCPUCapableDataMonitorProbeConnectable.onSingleEvent(FilterOptimizedMultiCPUCapableDataMonitorProbeConnectable.java:834)
- waiting to lock <0x23f479e0> (a java.util.ArrayList)
at com.arcsight.common.flow.InputConnector.notifyListener(InputConnector.java:119)
```

Content: Dashboards

XCPUDMPC-Thread

- Remove event from batch from queue
- Evaluate events against Data Monitors
- Generate Correlation events
- Put event batch in to queue for garbage collection

XCPUDMPC-Thread-1

Dump #1 (Jan 22, 2010 2:22:14 PM) daemon prio=6 tid=0x73269c00 nid=0xaa8 in Object.wait() [0x7107f000..0x7107fd18] java.lang.Thread.State: TIMED_WAITING (on object monitor)
Dump #2 (Jan 22, 2010 2:23:08 PM) daemon prio=6 tid=0x73269c00 nid=0xaa8 in Object.wait() [0x7107f000..0x7107fd18] java.lang.Thread.State: TIMED_WAITING (on object monitor)
Dump #3 (Jan 22, 2010 2:24:51 PM) daemon prio=6 tid=0x73269c00 nid=0xaa8 in Object.wait() [0x7107f000..0x7107fd18] java.lang.Thread.State: TIMED_WAITING (on object monitor)
Dump #4 (Jan 22, 2010 2:25:26 PM) daemon prio=6 tid=0x73269c00 nid=0xaa8 in Object.wait() [0x7107f000..0x7107fd18] java.lang.Thread.State: TIMED_WAITING (on object monitor)

```
at java.lang.Object.wait(Native Method)
- waiting on <0x12082f58> (a EDU.oswego.cs.dl.util.concurrent.BoundedBuffer)
at EDU.oswego.cs.dl.util.concurrent.BoundedBuffer.poll(BoundedBuffer.java:170)
- locked <0x12082f58> (a EDU.oswego.cs.dl.util.concurrent.BoundedBuffer)
at com.arcsight.server.dashboard.FilterOptimizedMultiCPUCapableDataMonitorProbeConnectable$Worker.run(FilterOptimizedMultiCPUCapableDataMonitorProbeConnectable.java:1570)
```

Best Practices

Again and Again

When Seeing Caches :

- Do Not Restart ESM
- Generate Thread Dumps
- Logs, Logs, Logs

Have a Good Back Up

System Tables

- /opt/arcsight/manager/bin/export_system_tables <user> <pw> <db>

Configuration Files

- /opt/arcsight/manager/il8n/common/
- /opt/arcsight/manager/config/
- /opt/arcsight/jre/lib/security/cacerts/
- /opt/arcsight/manager/config/notification

MySQL

- /opt/arcsight/logger/data/mysql/mysql/
- /opt/arcsight/logger/data/mysql/arcsight/

Know Your Hardware

Symptom

- Event flow slows or stops entirely
- Cpu waits, iowaits shows delay bottleneck with disk

```
top - 17:53:53 up  6:23,  1 user,  load average: 14.09, 15.20, 16.10
Tasks: 629 total,   1 running, 628 sleeping,   0 stopped,   0 zombie
Cpu(s): 56.4%us,  5.1%sy,  0.0%ni, 29.0%id,  9.3%wa,  0.0%hi,  0.2%si,  0.0%st
```

Root Cause

- CORR-Engine requires disk speeds of at least 15,000RPM to keep up with writes

Workaround

- Upgrade hardware

Limit use of Group By

Symptom

- Trend or report fails to run
- Large temporary files generated by query
- Logs may show "*temporary sort space limit exceeded*"

Root Cause

- Excessive grouping of data; e.g. five levels or more is extremely resource intensive

Workaround

- Expect increased overhead with each level of Group By; use minimally
- Use substring to truncate long fields (TIP: try trimming Geo Country Codes)
- Try setting **event.query.charset.conversion** to 1 or 2 in server.properties

Memory Heap Size

Recommendation for heap size is 2 x Working Set

Symptom

Too small

- Frequent full GC
- Bad performance
- Manager could die on OutOfMemoryError

Too large

- Peak performance is good, but ..
- Full GC takes long time to finish
- Manager could get killed by Wrapper for being hung for a long time

Workaround

Adjust heap size through Management Console, or by running ‘managersetup’

Tune Rules

Symptom

- Excessive rules firing
- High partial rules matching

Root Cause

- Aggregation window
- Order of variables

Workaround

- Reduce aggregation windows
- Re-order variables (simple first)

Summary

Topics:

- Data flow
- Symptoms of Performance Issues
- Logs and Data Collection
- Data Analysis
- Monitoring ESM
- Thread dumps
- Best Practices

Let’s

- Maintain and improve ESM performance

Q&A

Thank you