



Protect 2014

Washington, D.C. September 8-11

HP ArcSight ESM Health Check

Tracy Barella, Chief Services Strategist

HP ArcSight Health Check

Agenda

- What is a Health Check?
- What do we check?
- Where do we find symptoms?
- Items to review before starting a Health Check
- Health Check steps by ArcSight component
 - ESM Manager
 - ESM Database and Storage
- Q & A



Health Check overview



What is a Health Check?

Purpose

The purpose of performing a Health Check is to identify and remove performance bottlenecks to enable top performance of the HP ArcSight implementation. Minor issues can result in major performance degradations over time, impacting system availability and user satisfaction. Performing regular Health Checks will identify issues, allowing them to be remediated quickly and ensuring continued top performance of the HP ArcSight implementation.

In a nutshell...

A Health Check consists of common administrative tasks and verifies that the ArcSight solution is configured and performing optimally.



What do we check?

Performance

- Event Insertion
- Event Retrieval

Logs

- Warnings and errors

Configuration

- Optimal settings and parameters

Content

- Rules and Lists
- Data Monitors
- Trends, Reports, etc.
- Filters and Active Channels

Architecture

- Event volume
- Storage
- Network communication



Where do we find symptoms?

It's just simple plumbing!

- Information gathered during the planning phase
- Support Tickets
- ESM Console, Logger WebUI, and ConnApp WebUI
 - Analysis Tools
 - Logfu
 - Manager: `../manager/bin/arcsight logfu -m -noplots`
 - Connector: `../current/bin/arcsight agent logfu -a`
 - Oracle RDA
- ArcSight System Management Interface
 - <https://<managerhost>:8443>
 - For ESM 6.0c, simply logon to the Management Console home page and add `?advancedadmin=true` to the end of the URL
- Operating System Tools
- Operating System logs and ArcSight logs



Preparing for a Health Check



Items to review before starting a Health Check

Past

- Review the complete history of the ArcSight implementation
- When was ArcSight purchased?
- What was the business driver behind the purchase? Log Management, PCI, SOX, HIPPA, NERC, FISMA, etc.?
- Who sized the architecture? Review the original architecture recommendations
- Was the “initial” ArcSight implementation successful? If not, why?

Present

- What's the current status of the ArcSight solution?
- Is the implementation phase complete?
- Has the ArcSight solution met the original business requirement? If not, why?
- Review the architecture diagram(s) of the ArcSight solution
- Are there any success stories?
- What problems are there in the current ArcSight solution? Are there any open Support tickets?

Future

- What are the plans for the ArcSight solution? New use cases/data sources, monitoring additional business units, etc.
- The Health Check will identify areas needed to scale the architecture for future growth



Health Check steps by ArcSight component

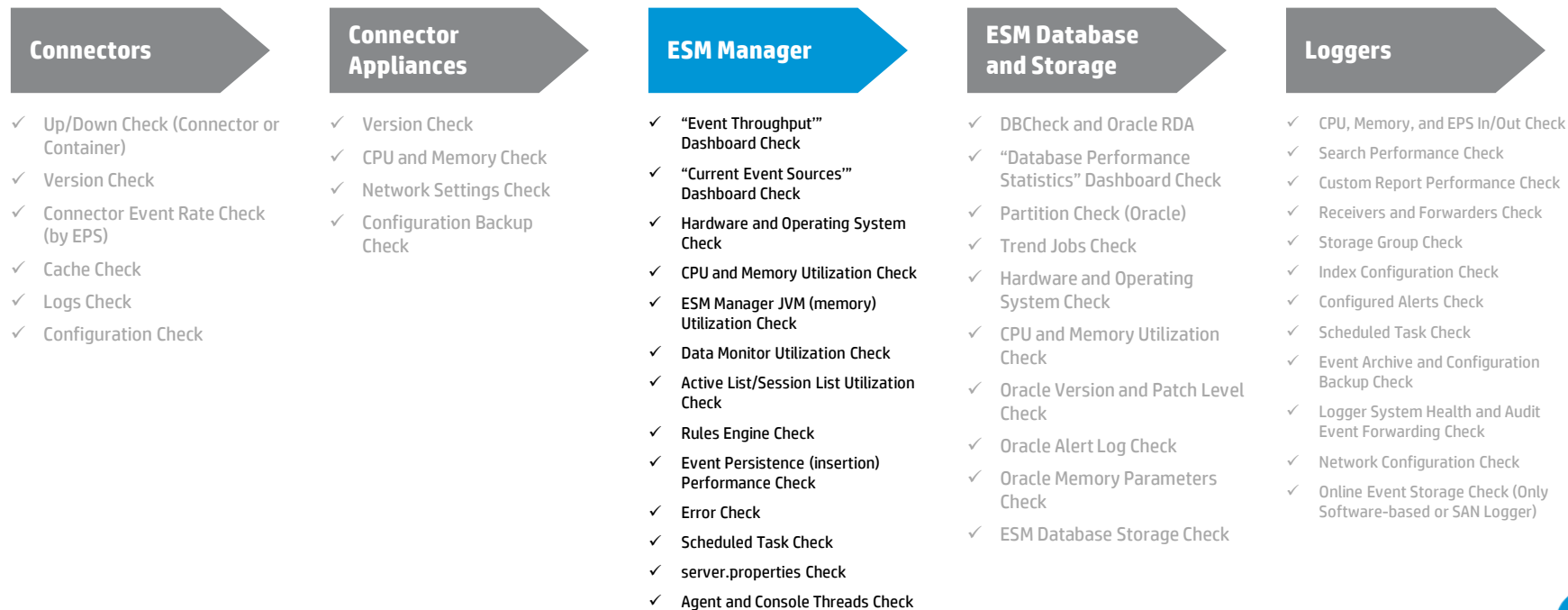
Note: It's impossible to cover every scenario in this presentation, so only the **common** checks will be discussed.



Health Check steps by ArcSight component

ESM Manager

Tip: Check each ArcSight Component by the order of the Event Flow



ESM Manager

“Event Throughput” Dashboard Check

- Compare the “current” event rates (EPS/EPD) with what the architecture was “originally sized” for
- If you’ve exceeded the event rate that you were originally sized for, you’re most likely seeing performance problems. All hope is not lost, so here are a few options:
 - Apply Aggregation and/or Filters to the Connectors to reduce the event rate
 - Re-evaluate the device feeds. Do we need these devices for our security monitoring use cases or are they just noise?
 - Consider proactively expanding the architecture before problems occur

Event Throughput Statistics							
Name	ID	E/s(avg.)	E/s(min)	Events	E/day	Min E/s	Max E/s
	3qfEhOdcBABDBmGZDcoBNOA==	0.7	1.6	794,100	0.1M	0.0	4.7
	3IO8GoCdBABCEBWZDcoBNOA==	0.6	0.6	604,275	0.0M	0.0	2.8
	33r7fnzdBABCU4WZDcoBNOA==	0.4	0.4	429,642	0.0M	0.0	11.4
	3GfwnzdBABDHGZDcoBNOA==	0.9	1.2	914,723	0.1M	0.0	6.2
	3ShwZdcBABCpQWZDcoBNOA==	0.0	0.0	4,658	0.0M	0.0	0.2
	3NwNwGOkBABCNxsVMBgwA==	876.6	1,175.2	932,366,438	75.7M	0.0	6,945.7
	3XV7uWjKBABC-qcPNJL2gwi==	22.7	18.3	24,137,723	2.0M	0.0	2,736.7
	3EO6ZXTgBADO-fCyGpB0ztg==	0.1	0.0	122,636	0.0M	0.0	101.7
	3K-A2eBgBABC-HWdXhBgJug==	1,197.9	1,385.0	1,274,051,233	103.9M	0.0	2,905.0
	3shk4pBABCvImVdYgJug==	27.7	29.4	29,426,996	2.4M	1.7	1,790.0
	3CauJJTgBABDSdVMOvDY2Q==	0.4	0.2	385,615	0.0M	0.0	1.7
	3YQnCwzdBABD9bveYg6XAQ==	0.2	0.0	202,515	0.0M	0.0	1.5
	31XTeWzdBABDVZf6eyg6IAQ==	0.2	0.1	209,183	0.0M	0.0	0.9
	3SbmWzdBABCOV6eyg6IAQ==	0.2	0.0	200,581	0.0M	0.0	1.6
	3WKdQJjdBABDK8Mpz7Ky4Ew==	0.7	0.1	706,856	0.1M	0.0	5.8
	3Z0uJjdBABCPrspz7Ky4Ew==	0.6	0.1	628,432	0.1M	0.0	5.9
	3BGO3UjdBABDS+Mpz7Ky4Ew==	0.5	0.0	528,331	0.0M	0.0	5.1
	3cu20UjdBABDCMpz7Ky4Ew==	0.5	0.0	498,755	0.0M	0.0	5.0
	3OumuJjdBABCc4pz7Ky4Ew==	0.5	0.0	498,252	0.0M	0.0	5.0
	3ymolUjdBABDslpz7Ky4Ew==	0.5	0.0	569,132	0.0M	0.0	5.4
	3CGd7AzkBABCY35xGpB0ztg==	354.4	0.0	376,970,297	30.6M	0.0	6,311.0
Since Last Reset	-	2,545.4	2,665.2	2,707,891,750	219.9M	1.4	9,565.7
Server Lifetime	-	2,545.4	2,665.2	2,707,891,750	219.9M	1.4	9,565.7

9/5 11:04:11 - 9/18 18:34:06



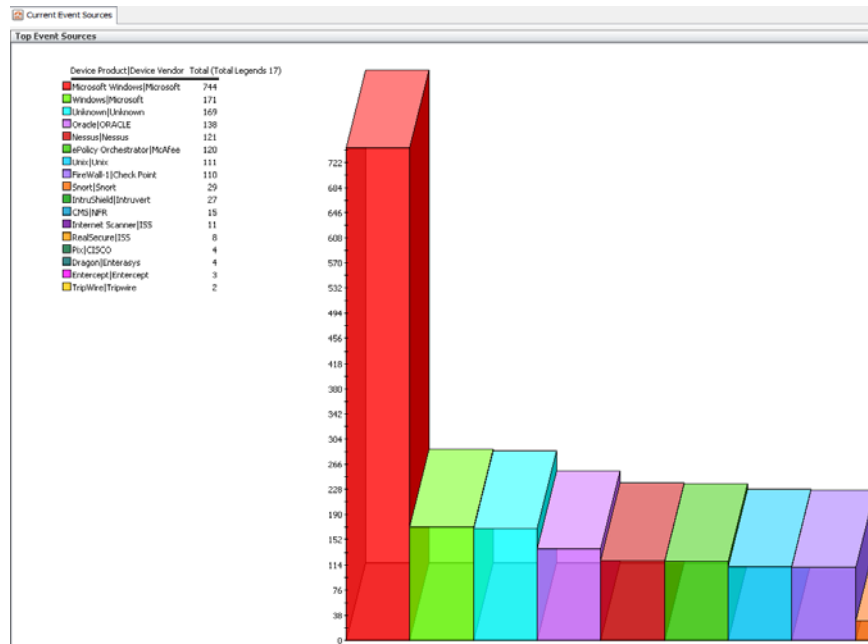
ESM Manager (continued)

“Current Event Sources” Dashboard Check

- Are there any “unknown” vendors/products listed?
 - If yes, maybe there’s a possible parsing problem to investigate
 - Are the “unknown” vendors/products useless devices? (They add no value to the use cases defined in ESM and should be excluded)
- Which vendors/products have the highest EPS?
 - This helps us prioritize which device types or Connectors we should tune first

Tip: I use the information provided in this Dashboard to recommend new use cases to an existing customer. “I see you have Oracle Audit events in ArcSight, have you ever thought about...?” This is where simple device-specific content packs will add immediate value!

- Microsoft content pack
- Cisco content pack
- Tipping Point content pack
- Etc. etc.



ESM Manager (continued)

Hardware and Operating System check

- Are there sufficient CPU cores and memory to support the event rate and use cases (content)?
- Is there sufficient Disk Space?
- Is the Operating System supported?

CPU and memory utilization check

- Use standard Operating System tools to check for high CPU and memory utilization
 - Linux/Unix: Execute top and review load averages and memory utilization
 - Windows: Use Task Manager or Performance Monitor
- If the utilization is high, is it ArcSight or a third-party process that's causing it?
- Understanding Load Averages in Linux Top:
<http://blog.scoutapp.com/articles/2009/07/31/understanding-load-averages>

```
top - 20:50:16 up 577 days, 12:33, 1 user, load average: 0.00, 0.03, 0.00
Tasks: 284 total, 1 running, 282 sleeping, 0 stopped, 1 zombie
Cpu0  :  0.3%us,  0.0%sy,  0.0%ni, 99.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu1  :  0.0%us,  0.0%sy,  0.0%ni,100.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu2  :  0.0%us,  0.0%sy,  0.0%ni,100.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu3  :  0.3%us,  2.3%sy,  0.0%ni, 97.4%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu4  :  3.0%us,  1.0%sy,  0.0%ni, 96.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu5  :  0.3%us,  0.3%sy,  0.0%ni, 99.3%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu6  :  0.7%us,  0.0%sy,  0.0%ni, 99.3%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu7  :  0.0%us,  0.0%sy,  0.0%ni,100.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu8  :  0.0%us,  0.0%sy,  0.0%ni,100.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu9  :  0.0%us,  0.0%sy,  0.0%ni,100.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu10 :  0.0%us,  0.0%sy,  0.0%ni,100.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu11 :  1.7%us,  0.3%sy,  0.0%ni, 97.7%id,  0.0%wa,  0.0%hi,  0.3%si,  0.0%st
Cpu12 :  0.0%us,  0.0%sy,  0.0%ni,100.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu13 :  0.0%us,  1.3%sy,  0.0%ni, 98.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu14 :  0.3%us,  0.0%sy,  0.0%ni, 99.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu15 :  0.0%us,  0.0%sy,  0.0%ni,100.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:  49302440k total, 38466068k used, 10836372k free, 1680936k buffers
Swap: 2097144k total,      0k used, 2097144k free, 23274944k cached

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
  4695 arcsight  18   0 17.7g 11g   16m  S   9.3   24.4 12579:50 java
  5798 root       34  19    0    0    0   S   1.3    0.0 9121:52 kpmi0
      1 root       15   0 10348 632   532  S   0.0    0.0  0:12.18 init
      2 root       RT  -5    0    0    0   S   0.0    0.0  2:12.63 migration/0
```



ESM Manager (continued)

ESM Manager JVM (memory) Utilization Check

- Review the “ESM System Information” Dashboard for current and max memory
- Review ../manager/logs/default/server.std.log to determine the frequency of Full GCs
 - Healthy JVM = a Full GC once every hour or more
 - Unhealthy JVM = a Full GC once every 5 to 10 minutes or less
 - All processing stops during a Full GC, so if a Full GC occurs every 5 minutes, ArcSight ESM is useless (Connectors caching, Consoles freezing, etc.)
- Review ../manager/logs/default/server.std.log to determine how long each Full GC takes to complete
- Review CAPS Manager in the ArcSight System Management Interface and the Rules Status Dashboard to determine which resources are consuming the most memory
- Open a ticket with Support if you're unable to determine the root cause of memory issues
- How do we determine the optimal heap size for the Manager's JVM?
 - Configure the Manager's JVM heap size to 2 x the average heap usage

See the following 3 slides for examples.



ESM Manager (continued)

ESM Manager JVM (memory) Utilization Check (continued) – healthy example 1

```
Arcsight:service=HqServer
ActiveThreadCount: 220
ArCSightSystemVersion: 5.0.2.6731.1
BaseURL: https://
ClusterID: default
GlobalDebugEnabled: false
HostInformation: Host name:
ID: n3orly8BACaIy5mE84de==
LastGeneratedThreadDump: null
LastThreadDump: null
Location: Kansas City
LogLevel: 1
MainMemory: 16333M (17126195200 bytes)
OS: Linux (amd64), Version 2.6.18-194.3.1.el5
PersistEvents: true
ProcessorCount: 16
Ready: true
ReportLicenseKey: 5000-758-ERX-00000F002000006-F29D3F2339F7
RulesCheckOnRecoverComplete: true
SessionCount: 2
SessionUserInfo: Name: ID: lvpVLLBACuKZLVkygd==, Tole
StartTimeStamp: Wed May 02 11:39:26 CDT 2012
TotalMemory: 16333M (17126195200 bytes)
Uptime: 4017y 2min 55s
UsedMemory: 1240M (12933888 bytes)
ArCSight:10-18-2011_16:5:14
false
```

```
top - 20:50:16 up 577 days, 12:33, 1 user, load average: 0.00, 0.03, 0.00
Tasks: 284 total, 1 running, 282 sleeping, 0 stopped, 1 zombie
Cpu0 : 0.3%us, 0.0%sy, 0.0%ni, 99.7%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu1 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu2 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu3 : 0.3%us, 2.3%sy, 0.0%ni, 97.4%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu4 : 3.0%us, 1.0%sy, 0.0%ni, 96.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu5 : 0.3%us, 0.3%sy, 0.0%ni, 99.3%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu6 : 0.7%us, 0.0%sy, 0.0%ni, 99.3%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu7 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu8 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu9 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu10 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu11 : 1.7%us, 0.3%sy, 0.0%ni, 97.7%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu12 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu13 : 0.0%us, 1.3%sy, 0.0%ni, 98.7%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu14 : 0.3%us, 0.0%sy, 0.0%ni, 99.7%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu15 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 49302440k total, 38466068k used, 10836372k free, 1680936k buffers
Swap: 2097144k total, 0k used, 2097144k free, 23274944k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
4695	arcsight	18	0	17.7g	11g	16m	S	9.3	24.4	12579:50	java
5798	root	34	19	0	0	S	1.3	0.0	9121:52	kpmio1	
1	root	15	0	10348	632	532	S	0.0	0.0	0:12.18	init
2	root	15	0	0	0	S	0.0	0.0	2:12.63	migration0	

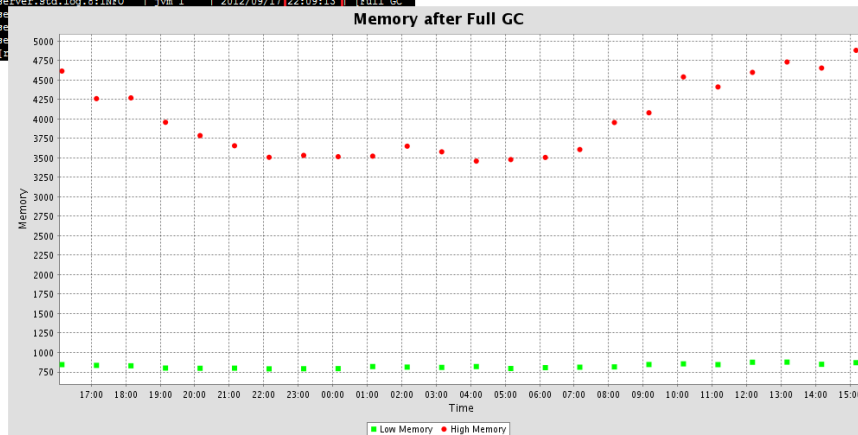
```
[arcsight@arcsight default]$ grep Full server.std.log
server.std.log:INFO jvm 1 | 2012/10/16 19:55:53 | Full GC
server.std.log:1:INFO jvm 1 | 2012/10/16 19:55:52 | [Full GC
server.std.log:1:INFO jvm 1 | 2012/10/16 10:55:25 | [Full GC
server.std.log:1:INFO jvm 1 | 2012/10/16 11:55:28 | [Full GC
server.std.log:1:INFO jvm 1 | 2012/10/16 12:55:31 | [Full GC
server.std.log:1:INFO jvm 1 | 2012/10/16 13:55:34 | [Full GC
server.std.log:1:INFO jvm 1 | 2012/10/16 14:55:37 | [Full GC
server.std.log:1:INFO jvm 1 | 2012/10/16 15:55:41 | [Full GC
server.std.log:1:INFO jvm 1 | 2012/10/16 16:55:44 | [Full GC
server.std.log:1:INFO jvm 1 | 2012/10/16 17:55:47 | [Full GC
server.std.log:1:INFO jvm 1 | 2012/10/16 18:55:50 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/10 13:48:05 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/10 14:48:08 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/10 15:48:11 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/10 16:48:15 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/10 17:48:18 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/10 18:48:21 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/10 19:48:24 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/10 20:48:27 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/10 21:48:30 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/10 22:48:33 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/10 23:48:36 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/11 00:48:40 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/11 01:48:43 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/11 02:48:46 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/11 03:48:49 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/15 17:54:32 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/15 18:54:35 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/15 19:54:38 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/15 20:54:42 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/15 21:54:45 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/15 22:54:48 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/15 23:54:51 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/16 00:54:54 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/16 01:54:57 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/16 02:55:00 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/16 03:55:03 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/16 04:55:06 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/16 05:55:09 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/16 06:55:12 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/16 07:55:15 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/16 08:55:18 | [Full GC
server.std.log:10:INFO jvm 1 | 2012/10/16 09:55:21 | [Full GC
server.std.log:3:INFO jvm 1 | 2012/10/15 03:53:47 | [Full GC
server.std.log:3:INFO jvm 1 | 2012/10/15 04:53:50 | [Full GC
```



ESM Manager (continued)

ESM Manager JVM (memory) Utilization Check (continued) – healthy example 2

```
[root@ ~]# default]# grep Full server.std.log
INFO | jvm 1 | 2012/09/18 14:10:19 | [Full GC
[root@ ~]# default]# date
Tue Sep 18 14:54:33 PDT 2012
[root@ ~]# default]# grep Full server.std.log
server.std.log:INFO | jvm 1 | 2012/09/18 14:10:19 | [Full GC
server.std.log.1:INFO | jvm 1 | 2012/09/18 13:10:14 | [Full GC
server.std.log.10:INFO | jvm 1 | 2012/09/17 16:08:48 | [Full GC
server.std.log.10:INFO | jvm 1 | 2012/09/17 17:08:53 | [Full GC
server.std.log.2:INFO | jvm 1 | 2012/09/18 11:10:05 | [Full GC
server.std.log.2:INFO | jvm 1 | 2012/09/18 12:10:09 | [Full GC
server.std.log.3:INFO | jvm 1 | 2012/09/18 09:09:56 | [Full GC
server.std.log.3:INFO | jvm 1 | 2012/09/18 10:10:01 | [Full GC
server.std.log.4:INFO | jvm 1 | 2012/09/18 07:09:49 | [Full GC
server.std.log.4:INFO | jvm 1 | 2012/09/18 08:09:52 | [Full GC
server.std.log.5:INFO | jvm 1 | 2012/09/18 04:09:37 | [Full GC
server.std.log.5:INFO | jvm 1 | 2012/09/18 05:09:41 | [Full GC
server.std.log.5:INFO | jvm 1 | 2012/09/18 06:09:45 | [Full GC
server.std.log.6:INFO | jvm 1 | 2012/09/18 02:09:30 | [Full GC
server.std.log.6:INFO | jvm 1 | 2012/09/18 03:09:34 | [Full GC
server.std.log.7:INFO | jvm 1 | 2012/09/17 23:09:17 | [Full GC
server.std.log.7:INFO | jvm 1 | 2012/09/18 00:09:22 | [Full GC
server.std.log.7:INFO | jvm 1 | 2012/09/18 01:09:26 | [Full GC
server.std.log.8:INFO | jvm 1 | 2012/09/17 21:09:09 | [Full GC
server.std.log.8:INFO | jvm 1 | 2012/09/17 22:09:13 | [Full GC
```



ESM Manager (continued)

ESM Manager JVM (memory) Utilization Check (continued) – unhealthy example

Arcsight-service=NGServer	
ActiveThreadCount	219
ArcsightSystemVersion	5.0.2.6731.1
BaseURL	https:// @443/
ClusterId	default
GlobalDebugEnabled	false
HostInformation	Host name:
ID	19y8y8Q8ACBAZ6H5SaGwbQ==
LastGeneratedThreadDump	null
LastThreadDump	null
Location	
LogLevel	1
MaxMemory	9165M (9610002432 bytes)
OS	Linux (amd64), Version 2.6.18-238.9.1.el5
PersistEvents	true
ProcessorCount	16
Ready	
ReportLicenseKey	S000-758-ERX-00008F002000006-F290-3F2339F7
RulesCheckponRecoveryComplete	true
SessionCount	29
SessionUserInfo	[Name: , ID:IGUWVWQ8ABCD15d82pJg==, TotalLength:3hr 41min
StartTimeStamp	Fri Sep 21 10:55:36 GMT 2012
TotalMemory	9165M (9610002432 bytes)
Uptime	629hr 50min 15sec
UseMemory	4464M (5074976928 bytes)
	A5731 10-18-2011 16:51:14
	false

```
top - 17:08:41 up 30 days, 21:45, 2 users, load average: 0.37, 0.52, 0.60
Tasks: 325 total, 1 running, 322 sleeping, 0 stopped, 2 zombie
Cpu0 : 0.0%us, 0.0%sy, 0.0%ni, 99.3%id, 0.7%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu1 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu2 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu3 : 0.3%us, 0.3%sy, 0.0%ni, 97.4%id, 2.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu4 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu5 : 0.3%us, 0.0%sy, 0.0%ni, 99.7%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu6 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu7 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu8 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu9 : 0.0%us, 1.7%sy, 0.0%ni, 98.3%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu10 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu11 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu12 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu13 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu14 : 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Cpu15 : 24.1%us, 3.1%sy, 0.0%ni, 63.7%id, 0.0%wa, 2.0%hi, 7.1%si, 0.0%st
Mem: 16279868k total, 13976040k used, 2303828k free, 252664k buffers
Swap: 2097144k total, 0k used, 2097144k free, 1124064k cached

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
1269 arcsight 19 0 10.7g 10g 17m S 29.3 64.4 15160:22 java
```

```
INFO | jvm 1 | 2012/10/16 19:48:41 | Memory Status: 7,830.9 MB Used, 9,164.8 MB Max
INFO | jvm 1 | 2012/10/16 19:48:42 | (02-Pre-SecurityEventPersistor100) Persisted 1 e m 1 | 2012/10/17 06:31:54 | [Full GC
INFO | jvm 1 | 2012/10/16 19:48:43 | 8264555K->7990125K(9384768K), 0.0735460 secs] m 1 | 2012/10/17 07:25:02 | [Full GC
INFO | jvm 1 | 2012/10/16 19:48:43 | (02-Pre-SecurityEventPersistor100) Persisted 17 m 1 | 2012/10/17 08:01:12 | [Full GC
INFO | jvm 1 | 2012/10/16 19:48:44 | (02-Pre-SecurityEventPersistor100) Persisted 1 e m 1 | 2012/10/17 08:21:55 | [Full GC
INFO | jvm 1 | 2012/10/16 19:48:44 | HOSTINFO 1350416925039 3.0 1.0 0.0 97.0 2376 109 m 1 | 2012/10/17 08:27:15 | [Full GC
INFO | jvm 1 | 2012/10/16 19:48:45 | (2192009096ms / 8802760200000000ns) Current proce m 1 | 2012/10/17 08:37:39 | [Full GC
INFO | jvm 1 | 2012/10/16 19:48:45 | (02-Pre-SecurityEventPersistor100) Persisted 21 m 1 | 2012/10/17 08:47:52 | [Full GC
INFO | jvm 1 | 2012/10/16 19:48:50 | HOSTINFO 1350416930040 1.0 0.0 0.0 99.0 2375 109 m 1 | 2012/10/17 08:58:18 | [Full GC
INFO | jvm 1 | 2012/10/16 19:48:50 | (02-Pre-SecurityEventPersistor100) Persisted 27 m 1 | 2012/10/17 09:23:57 | [Full GC
INFO | jvm 1 | 2012/10/16 19:48:50 | (2192014098ms / 8802768000000000ns) Current proce m 1 | 2012/10/17 09:34:24 | [Full GC
INFO | jvm 1 | 2012/10/16 19:48:51 | Memory Status: 8,197.9 MB Used, 9,164.8 MB Max m 1 | 2012/10/17 09:39:40 | [Full GC
INFO | jvm 1 | 2012/10/16 19:48:51 | [Full GC m 1 | 2012/10/17 09:44:58 | [Full GC
INFO | jvm 1 | 2012/10/16 19:48:51 | 8409581K->8463410K(9384768K), 0.1292190 secs] m 1 | 2012/10/17 10:05:07 | [Full GC
INFO | jvm 1 | 2012/10/16 19:48:51 | [Full GC m 1 | 2012/10/17 11:13:06 | [Full GC
INFO | jvm 1 | 2012/10/16 19:49:01 | 8463410K->2912124K(9384768K), 10.2280600 secs] m 1 | 2012/10/17 11:25:27 | [Full GC
INFO | jvm 1 | 2012/10/16 19:49:01 | Memory Status: 2,844.0 MB Used, 9,164.8 MB Max m 1 | 2012/10/17 11:37:34 | [Full GC
INFO | jvm 1 | 2012/10/16 19:49:02 | (2192025162ms / 8802879900000000ns) Current proce m 1 | 2012/10/17 12:24:39 | [Full GC
INFO | jvm 1 | 2012/10/16 19:49:02 | HOSTINFO 1350416941967 1.0 0.0 0.0 99.0 2375 109 m 1 | 2012/10/17 12:34:02 | [Full GC
INFO | jvm 1 | 2012/10/16 19:49:02 | server.std.log:INFO | jvm 1 | 2012/10/17 12:39:18 | [Full GC
INFO | jvm 1 | 2012/10/16 19:49:02 | server.std.log:INFO | jvm 1 | 2012/10/17 12:39:18 | [Full GC
```



ESM Manager (continued)

Data Monitor Utilization Check

- Review the Data Monitor section of Caps Manager to reveal which Data Monitors are consuming the most memory
- Disable all unused Data Monitors
- Tune Data Monitors that are currently used in use cases
 - Avoid using “broad” Filters in Data Monitors that may match too many events
 - If possible, adjust the number of buckets (samples) and the seconds for each bucket (sample size) to reduce memory utilization
- Additional details for each Data Monitor can be found in the ProbeStats section of FilterOptimizedXCPUDMPC shown here

ArcSightService=CapsManager;Id=DataMonitor;Caps Manager					
GeographEventGraph: ACME Geo View - IDS and Correlated Events	0	2040	2000 events		2040, 2040, 2040, 2040
EventGraph: Virus Activity	3	1716	1602 events		1716, 1716, 1716, 1715
EventGraph: IDS-IPS Event Graph	3	1310	1204 events		1309, 1309, 1309, 1300
BucketizedTopValueCountsEvent: Top Categories	13	1039	2328 counts, fields [Category Object, Category Beha...		1037, 1034, 1033, 1029
EventGraph: Correlated Event Graph	2	413	434 events		412, 412, 412, 411
BucketizedTopValueCountsEvent: Top Event Sources	1	147	524 counts, fields [Device Product, Device Vendor]		147, 147, 147, 146
BucketizedTopValueCountsEvent: Top 10 Service Events	3	124	562 counts, fields [Name]		123, 123, 122, 121
BucketizedTopValueCountsEvent: Top 10 Firing Rules	1	121	550 counts, fields [Name]		121, 120, 120, 120
BucketizedTopValueCountsEvent: Top 10 Operating System Events	1	84	381 counts, fields [Name]		84, 84, 83, 83
BucketizedTopValueCountsEvent: Events By Priority	0	76	466 counts, fields [Priority]		76, 76, 76, 76
Rest (243 more)		17	2286		2282, 2286, 2285, 2279
Total		44	9386		9377, 9377, 9373, 9358

ArcSight Manager Status for https://h011.ac...									
ArcSightService=CapsManager;Id=DataMonitor;Caps Manager									
Events									
Time: Consumer Name: Resource: Usage:									
LastPill: Sun Jul 07 22:20:45 EDT 2013									
MaxMemoryUsage: 8 MB									
MemoryLimit: Controlled by parent caps manager									
MemoryReductions: Time: Consumer Name: Resource: Usage: Reduction:									
MemoryUsageInfo: Time: Consumer Name: Resource: Usage: Reduction:									
Consumer Name: Priority: Delta: Estimated Usage: UsageInfo: Past 4 Usages (938)									
GeographEventGraph: ACME Geo View - IDS and Correlated Events									
EventGraph: Virus Activity									
EventGraph: IDS-IPS Event Graph									
BucketizedTopValueCountsEvent: Top Categories									
EventGraph: Correlated Event Graph									
BucketizedTopValueCountsEvent: Top 10 Alerts									
BucketizedTopValueCountsEvent: Top 10 Service Events									
BucketizedTopValueCountsEvent: Top 10 Firing Rules									
BucketizedTopValueCountsEvent: Events By Priority									
Rest (243 more)									
Total									

ArcSight Manager Status for https://h011.ac...									
OnEventLastInvocationCount: 0									
OnSingleEventInvocationCount: 40924									
ProblematicEventsPerSecondCount: 884									
ProbeStats: Time: Consumer Name: Resource: Usage: Reduction:									
URI: Invocation Count: Invocation Percent: Type: Filter:									
All Data Monitors/Right Foundation/Intrusion Monitoring/Outback Monitoring/Target/Critical Asset Monitoring/Critical Asset Group Count									
All Data Monitors/Right Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/Top Connectors									



ESM Manager (continued)

Active List/Session List Utilization Check

- Review the Active Lists section of Caps Manager to reveal which Active Lists are consuming the most memory
 - If an Active List is only used for Reports, consider changing the Active List to Partially Loaded to reduce memory consumption
- Review the ActiveCacheInformation section of ActiveList Monitor
 - Fix Active Lists that are at or near 100% capacity
 - The Queries and Changes per Second columns may help determine how heavily the Active Lists are used by other resources (content)
- Review the SessionCacheInformation section of SessionList Monitor
 - Fix Session Lists that are at or near 100% capacity
 - The Queries and Changes per Second columns may help determine how heavily the Session Lists are used by other resources (content)

Consumer Name	Priority	Delta (KB)	Estimated Usage (KB)	Usage Info
ArcsightService=CapsManager;id=ActiveLists Caps Manager				
ActiveList:	3	0	1297920	120000 current entries, sche
ActiveList:	3	0	1230663	402704 current entries, sche
ActiveList:	3	0	57907	4770 current entries, schem
ActiveList:	3	0	56813	4712 current entries, schem
ActiveList:	3	0	47134	4712 current entries, schem
ActiveList:	3	0	23568	7712 current entries, schem
ActiveList:	3	0	6207	994 current entries, schema
ActiveList:	3	0	1630	793 current entries, schema
ActiveList:	3	0	1513	214 current entries, schema
ActiveList:	3	0	681	331 current entries, schema
Rest (60 more)			2136435	
Total		0	587201	-

Name	ID	Capacity	Main Entry Count	Context Count	Percent Used	* Temp Entry Count	Temp Entry Capacity	Max Temp ID	Queries/Sec	Changes/Sec
		1000	85	1	8.5%	0	0	null	5.537509173068524E-7	0.0011922577464471
		10000	6118	2	61.18%	6041	6041	Real-time(Recovery)	7.182441970700928E-6	1.8186688940915012
		1000	143	1	14.300000000000004%	0	0	null	0.0	0.0
		2000	62	1	3.1%	0	0	null	3.994901287671834E-7	0.0011919120241980
		10000	202	2	2.02%	153	153	Real-time(Recovery)	1.6835657886116417E-4	0.0037286181781231
		10000	1875	1	18.75%	0	0	null	0.0	0.0
		10000	10000	1	100.0%	0	0	null	0.0	0.0
		10000	129	1	1.29%	0	0	null	1.3133426590792284E-5	1.6099039047914381
		10000	73	1	0.73%	0	0	null	4.0544912947578385E-6	0.0370683699577021
		10000	70	2	0.7000000000000001%	70	70	Real-time(Recovery)	0.0	0.0
		10000	54	2	0.54%	25	25	Real-time(Recovery)	2.309271308211595E-6	2.3092713091310328
		1000	4	1	0.4%	0	0	null	0.0	0.0
		10000	29	1	0.29%	0	0	null	3.198027436721339E-7	0.0096640940169446
		10000	28	2	0.2799999999999997%	12	12	Real-time(Recovery)	6.627047432677152E-5	6.6270474326771528
		10000	28	1	0.2799999999999997%	0	0	null	3.171384711009740E-6	1.0057820083488034
		10000	25	2	0.25%	40	40	Real-time(Recovery)	1.2397987615944121E-5	0.00365159118143951
		10000	14	1	0.1399999999999999%	0	0	null	4.72121512833796E-7	4.7212151283379658
		50000	42	1	0.124%	0	0	null	0.0	0.0
		10000	6	2	0.06%	6	6	Real-time(Recovery)	0.0	0.0
		10000	2	2	0.02%	0	0	Real-time(Recovery)	3.474236151269541E-6	3.4742365978713228
		10000	2	2	0.02%	2	2	Real-time(Recovery)	0.0	0.0
		100000	18	1	0.018000000000000002%	0	0	null	0.0	0.0
		10000	1	1	0.01%	0	0	null	2.7156396842818594E-6	4.3450234948509758
		10000	1	1	0.01%	0	0	null	0.001921589764006815	0.00951709131818436
		10000	1	1	0.01%	0	0	null	0.0	0.0
		10000	1	1	0.01%	0	0	null	6.728123400013605E-7	1.12100740094091611
		10000	1	2	0.01%	0	0	Real-time(Recovery)	0.7601101610101010E-6	0.7601101610101010E-6

Name	Capacity	Main Entry Count	Percent Used	Queries/Sec	Changes/Sec
ArcsightService=SessionListMonitor;type=OracleSession...					
	10000	1	0.01%	0.03818475547070...	0.0
	10000	334	3.34%	0.0	0.22638237615293907
	1000	8	0.8%	0.001300212584757...	0.0
	10000	4	0.04%	0.0	0.002542020876092...
	10000	0	0.0%	0.0	0.0
	10000	300	3.0%	0.0	0.12261805021397477



Rules Engine Check

- Partial Matches per Rule**

Rule Name	Total (Total Legends 21)
Deny Port Scan Base	4950232
Detector Infected Host	4549566
Possible Internal Network Sweep	151156
Possible Outbound Network Sweep	151730
Warm-Outbreak Detected	2072
ASPM Database Status Change - Normal	351
Possible Successful Attack - Execute	34
Audit Account Modifications	49
Trend Query Started	34
Trend Query Ended	34
Reverse Audit Event Detected	6
ASPM Database Status Change - Warning	33
ASPM Database Status Change - Critical	15
Possible Successful Attack - Brute Force	18
Successful User Login	8

Top Firing Rules

Name	Total (Total Legends 10)
Trend Query Ended	6
Reverse Audit Event Detected	6
Trend Query Started	6
Agents updated	4
Possible Outbound Network Sweep	4
Report deleted	2
ASPM Database Status Change - Warning	1
Report inserted	1
ArchiveReport inserted	1
ASPM Database Status Change - Normal	1

Recent Fired Rules

Name	Category Object	Category Behavior	Category Outcome	Category Technique	Device Event Category	Priority	Attacker Zone Name	Attacker Address	Target Zone Name	Target Address
Agents updated	Agents/Update	Execute/Query	Success	Resource/Update	Resource/Update	7				
Agents updated	Host/Application	Execute/Query	Success	Resource/Update	Resource/Update	7				
Agents updated	Host/Application	Execute/Query	Success	Resource/Update	Resource/Update	7				
Agents updated	Host/Application	Execute/Query	Success	Resource/Update	Resource/Update	7				

Rules Engine Internal Stats

Armsight:service=rulesName, type=live, id=real-time	
AggregationEventCount	477
CorrelationEventCount	422
CorrelationEventCount	4269
GenerationEventCount	0
InputBufferLength	7
InputBufferStatus	Accumulating elements ... for 0
LastCheckFunction	133667
LoaderRules	[[Rule ID]Rule Name[Active]StartTimeMatching Events[Correlation Events]Aggregation Sets[Partial Matches, S3RmixQpABCG3H4KcmkHQ==Local Win...
NumEventsInQueue(QPS)	694745527
NumEventsProcessed(QPS)	1397015537
NumEventsInQueue(QPS)	763669590
OutputBufferLength	0
OutputBufferStatus	Accumulating elements ... for 681001
PerformanceTracing	False
RuleEngineInternalStats	[[Rule ID]Rule Name[Total Time (ms)](Memory (bytes))
RuleEngineInternalStats	Live

Rule Error Logs

Time	Name	Device Event Category	Attacker Zone Name	Attacker Address	Target Zone Name	Target Address	Priority
13 Sep 2012 08:08:00 PDT	Deactivating the rule Possible Internal Network Sweep: The number of Correlated alerts created is too high	Rule/Inactive/Deactivate/Unusable					7
14 Sep 2012 13:07:00 PDT	Activating the rule Possible Internal Network Sweep: The rule is under control	Rule/Active					7
14 Sep 2012 13:06:00 PDT	Deactivating the rule Possible Internal Network Sweep: The number of Correlated alerts created is too high	Rule/Inactive/Deactivate/Unusable					7
14 Sep 2012 13:07:00 PDT	Activating the rule Possible Internal Network Sweep: The rule is under control	Rule/Active					7

ESM Manager (continued)

Event Persistence (insertion) Performance Check

- Review ../manager/logs/default/server.std.log for event persistence performance
- Event Insertion performance can be negatively impacted by poorly written content (Rules, Data Monitors, and Lists), network latency to the Database, or Disk I/O contention on the SAN attached to the Database
- ESM on Oracle - Review the persist times in server.std.log or LogFu
 - Benchmark = 1 event in 1 ms
 - Excellent = 100 to 300 events in under 100 ms
 - Average = 100 to 300 events in 300 ms
 - Bad = 100 to 300 events in 500 to 1000+ ms
- ESM on CORRE - Review the persist times in server.std.log or LogFu
 - Benchmark = 1 event in 1 ms
- See the following slide for examples.



Event Persistence (insertion) Performance Check (continued) – healthy example

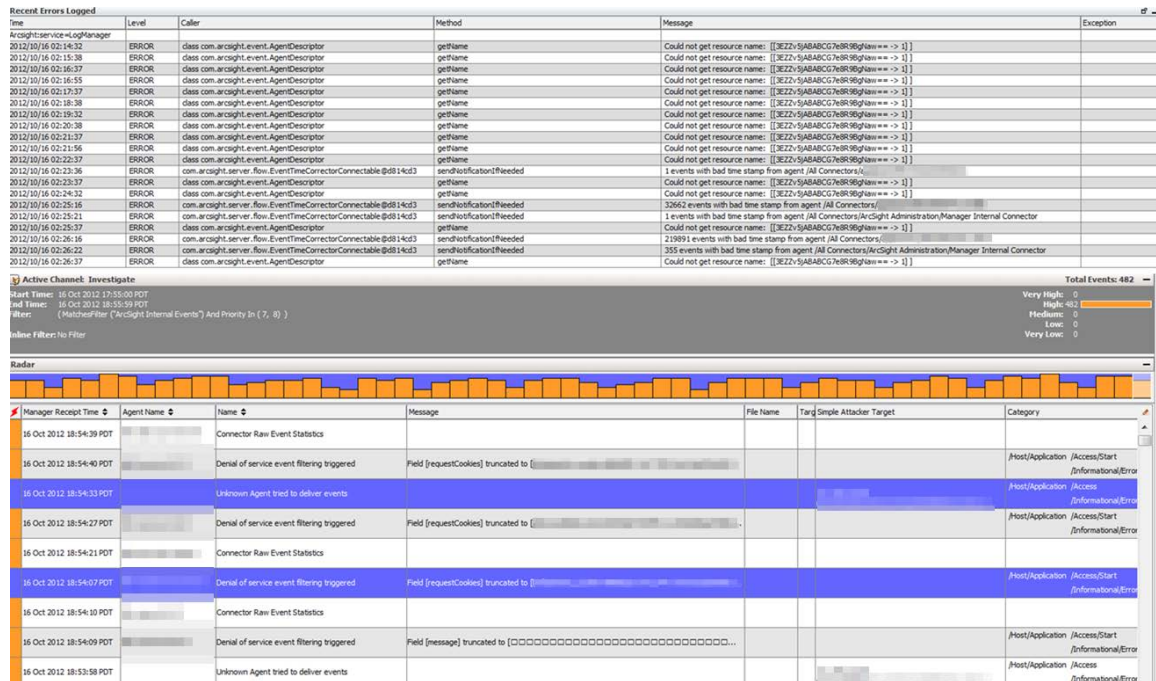


ESM Manager (continued)

Error Check

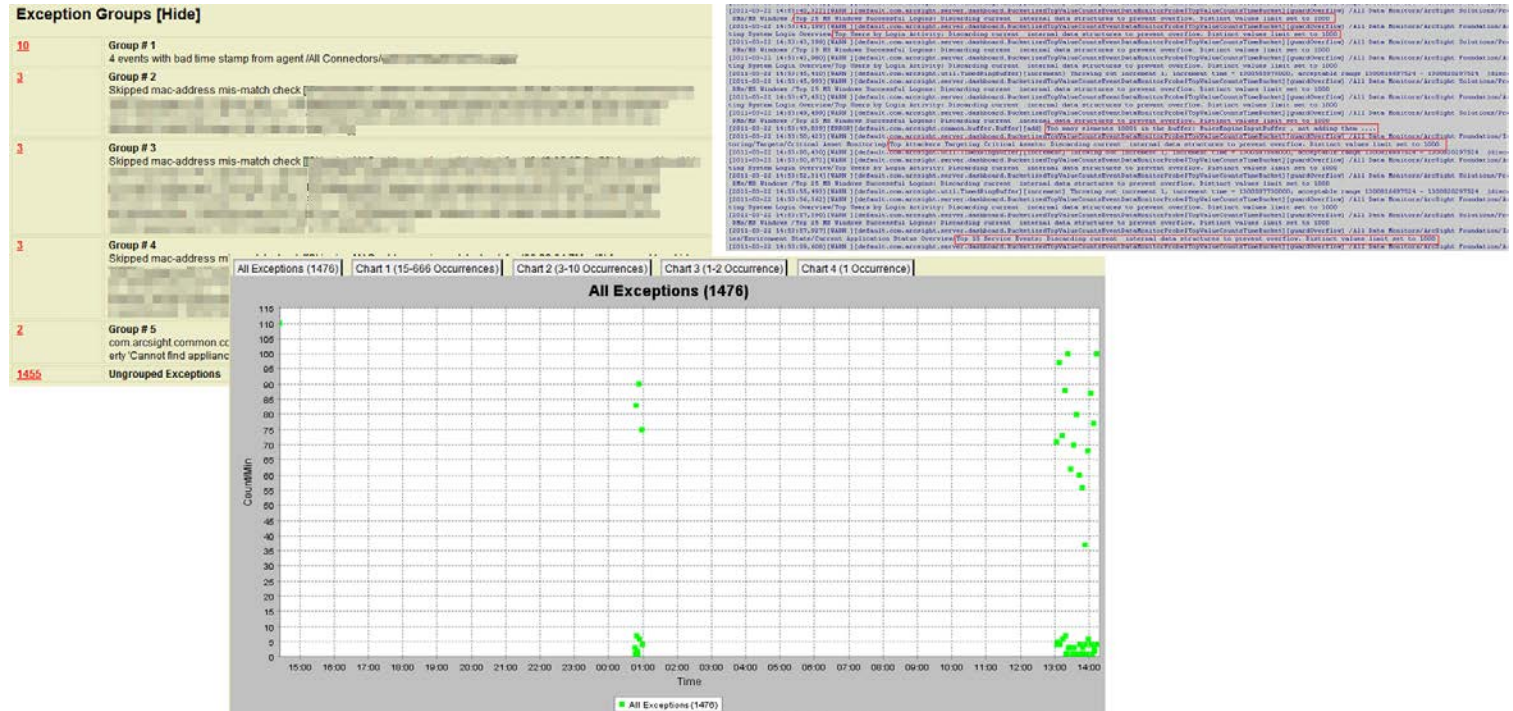
- Review both `../manager/logs/default/server.std.log` and `server.log` for chronic ERROR and WARN messages
 - tail -f server.log | grep -v INFO (exclude INFO messages)
- Review the Exception Report of Manager LogFu: `../manager/bin/arcsight logfu -m -noplots`
- Review the MostRecentErrorLogRecords of LogManager for the Recent Errors Logged
- Utilize the 'arcsight exceptions' command: `<ARCSIGHT_HOME>/bin/arcsight exceptions -n <ARCSIGHT_HOME>/logs/default/*.log*`
- Review the 'System Events' Active Channel for High and Very-High system events

See the following slide for more examples.



ESM Manager (continued)

Error Check (continued)



ESM Manager (continued)

CORRE-specific error

Symptom

- Event flow slows or stops entirely
- server.std.log shows:

```
INFO | jvm 1 | 2013/01/10 19:28:33 | @@@@ raw chunk size 4335504 > 1000000, will retry with smaller event list
INFO | jvm 1 | 2013/01/10 19:28:33 | @@@@ raw chunk size 2162444 > 1000000, will retry with smaller event list
INFO | jvm 1 | 2013/01/10 19:28:33 | @@@@ raw chunk size 1079826 > 1000000, will retry with smaller event list
INFO | jvm 1 | 2013/01/10 19:28:33 | @@@@ raw chunk size 1082634 > 1000000, will retry with smaller event list
INFO | jvm 1 | 2013/01/10 19:28:34 | @@@@ raw chunk size 2173436 > 1000000, will retry with smaller event list
INFO | jvm 1 | 2013/01/10 19:28:34 | @@@@ raw chunk size 1092338 > 1000000, will retry with smaller event list
INFO | jvm 1 | 2013/01/10 19:28:34 | @@@@ raw chunk size 1081106 > 1000000, will retry with smaller event list
```

Root cause

- Large Event size requires smaller batches of events to be written to disk
 - RequestURL, Raw Events, deviceCustomString

Workaround (KM00634332)

- Reduce number of events per batch in server.properties
 - queue.logger.pre-security-event-persistor.batchsize
 - queue.logger.pre-security-event-persistor.threshold



CAUTION: May impact read performance

ESM Manager (continued)

Scheduled Task Check

- Verify that scheduled tasks don't conflict with each other
- Heavy Tasks should be scheduled during off hours
- Are there any failed jobs?

The screenshot displays the ArcSight Manager interface, specifically the Scheduler service status page. The top section shows the service status as 'Running' and provides a link to the service's status page. Below this, there are sections for 'CurrentlyExecutingTasks', 'CurrentlyQueuedTasks', and 'SchedulerThreadPoolSize'. The main part of the interface is a table listing scheduled tasks, including their ID, Name, Next Run, Type, User, and Priority. The table shows a variety of tasks, such as 'Resource Search Index Updater', 'Top Users with Failed Logins per Day', 'AUP Updater', 'PurgeStaleMarkSimilarConfigs', 'Table Status Updater', 'Event Partition Stats Updater', 'Hourly Trend - IDS-IPS Activity', 'Configuration Modifications (Daily)', 'sa Events', 'Top 20', 'Shutdown Events - Daily Trend', 'sa by Hour', 'sa by Port', 'sa by Source', 'sa by Destination', 'sa Login Attempts - Daily Trend', 'sa by Priority', 'sa by Failures', 'sa by EPS', 'sa by Last 7 days', and 'Trends - Hourly'.

ID	Name	Next Run	Type	User	Type	Priority
JUK8jwBARCB3t:BcaX04Q==	Resource Search Index Updater	Mon Jul 08 09:35:00 EDT 2013	Other		ScheduledTask	High
J5F6nRABACAG4WUvB87Bg==	Top Users with Failed Logins per Day	Mon Jul 08 09:40:00 EDT 2013	Daily		Trend	Normal
J000jwBACB39cBcaX04Q==	AUP Updater	Mon Jul 08 09:40:00 EDT 2013	Other		ScheduledTask	High
JR08jwBACB5t:BcaX04Q==	PurgeStaleMarkSimilarConfigs	Mon Jul 08 10:00:00 EDT 2013	Hourly		ScheduledTask	High
J0SEM08BACCCGh010MvYchg==	Table Status Updater	Mon Jul 08 10:00:00 EDT 2013	Hourly		ScheduledTask	High
JSEM08BACCCGh010MvYchg==	Event Partition Stats Updater	Mon Jul 08 10:00:00 EDT 2013	Daily		ScheduledTask	High
Jc9cWjBACCCGh010MvYchg==	Hourly Trend - IDS-IPS Activity	Mon Jul 08 10:00:00 EDT 2013	Hourly	admin	Trend	Normal
	alter	Mon Jul 08 10:10:00 EDT 2013	Hourly		ScheduledTask	High
		Mon Jul 08 13:00:00 EDT 2013	Daily		ScheduledTask	High
		Mon Jul 08 17:24:00 EDT 2013	Daily		Trend	Normal
		Mon Jul 08 23:00:00 EDT 2013	Daily		ScheduledTask	High
		Tue Jul 09 01:00:00 EDT 2013	Daily	admin	Report	Normal
		Tue Jul 09 01:55:00 EDT 2013	Daily		ScheduledTask	High
		Tue Jul 09 03:06:00 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 03:40:00 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 04:03:59 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 04:15:00 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 04:15:09 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 04:20:00 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 04:35:00 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 04:40:00 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 05:20:00 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 05:40:00 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 05:40:34 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 06:07:08 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 06:15:00 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 06:30:00 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 06:33:36 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 06:40:00 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 06:42:45 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 07:20:00 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 07:40:00 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 07:40:04 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 07:42:19 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 07:45:51 EDT 2013	Daily		Trend	Normal
		Tue Jul 09 08:00:00 EDT 2013	Daily		Trend	Normal

Below the table, there is a section for 'Scheduled Runs' for the task 'Accumulate task for trend [id=Jc9cWjBACCCGh010MvYchg=]'. It shows the status of the task as 'Succeeded' and provides details about the job name, resource, and schedule time.

Status	Job Name	Resource	Schedule Time
Succeeded	Accumulate task for trend [id=Jc9cWjBACCCGh010MvYchg=]	[/All Trends/ACME/Connector/System Health/EPSS/Connector Average EPS - Last 7 days]	8 Jul 2013 00:00:00 EDT
Pending	Accumulate task for trend [id=Jc9cWjBACCCGh010MvYchg=]	[/All Trends/ACME/Connector/System Health/EPSS/Connector Average EPS - Last 7 days]	8 Jul 2013 10:00:00 EDT
Pending	Accumulate task for trend [id=Jc9cWjBACCCGh010MvYchg=]	[/All Trends/ACME/Connector/System Health/EPSS/Connector Average EPS - Last 7 days]	8 Jul 2013 11:00:00 EDT



ESM Manager (continued)

server.properties Check

- Review any non-standard settings in ../manager/config/**server.properties**
 - Tip: Look at the ../manager/config/**server.properties** file of a recently installed ArcSight VM to see what's "standard"
- Are there any temporary or legacy parameters that could be removed?
- Is there anything we can 'tweak' to make improvements?

Agent and Console Threads Check

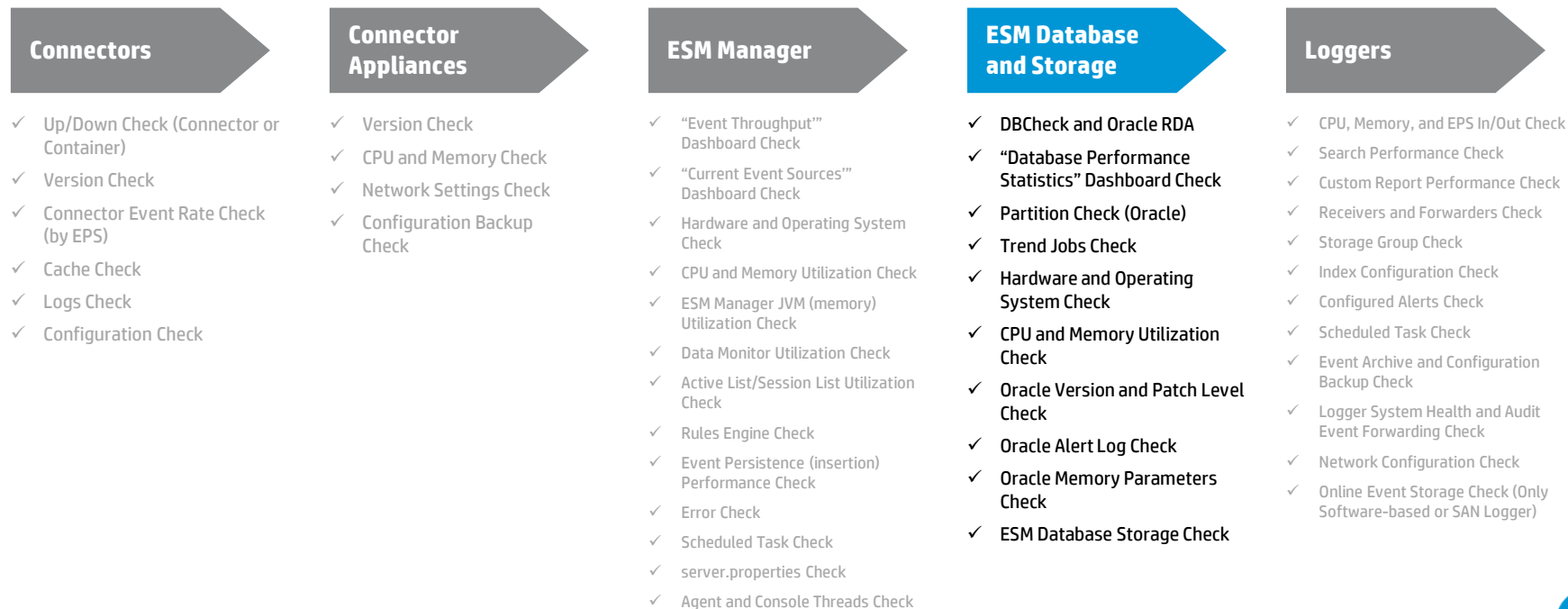
- If there are more than 60+ Connectors registered directly to ESM, increase the threadpool and agent threads in ../manager/config/**server.properties** as needed.
 - servletcontainer.jetty311.threadpool.maximum=
 - The maximum number of threads in the pool. This defines the upper bound of client connections that can be handled simultaneously. Keep in mind that both agents and consoles will share these connections
 - There are 128 total threads allocated to the Thread Pool by default. 64 of those threads are allocated to Console connections.
 - agents.threads.max=
 - Maximum number of concurrent threads to use for agents. If the number is exceeded, all further requests from agents will be rejected up to the point where threads become available again.
 - There are 64 threads allocated to the Agent (Connector) Threads by default



Health Check steps by ArcSight component

ESM Database & Storage

Tip: Check each ArcSight Component by the order of the Event Flow



ESM Database and Storage

Tools to provide immediate insight into database health

- ArcSight DBCheck Tool
 - Can be executed from Manager or DB: `../bin/arcsight dbcheck`
 - DBCheck will generate an html report with findings and recommendations
- Oracle RDA Tool
 - See Support's presentation titled "Reviewing RDAs - for non-DBAs"
 - RDA Tool location:
`$ARCSIGHT_HOME/utilities/database/oracle/common/rda.zip`
 - What to review:
 - Overview – System Settings and Information
 - Performance – Top SQL, ADDM, AWR
 - RDBMS – Database Parameters, Database Files, Log/Trace Files
- Hey, what about CORRE?!
 - Typical settings to tune (we'll cover later in this presentation):
 - `sort_temp_limit`
 - `innodb_buffer_pool_size`
 - Although not supported, you may research various settings to tune MySQL in CORRE (search for 'Mysqltuner.pl' or 'Tuning-primer.sh')

DIRECTORY	CONTENT
/SAN02/oradata/arcsight	ARC_SYSTEM_DATA Tablespace
/SAN02/oradata/arcsight	ARC_EVENT_DATA Tablespace
/SAN02/oradata/arcsight	SYSAUX Tablespace
/SAN02/oradata/arcsight	ARC_EVENT_INDEX Tablespace
/SAN02/oradata/arcsight	SYSTEM Tablespace
/SAN02/oradata/arcsight	UNDOTBS1 Tablespace
/SAN02/oradata/arcsight	ARC_UNDO Tablespace
/SAN02/oradata/arcsight	ARC_SYSTEM_INDEX Tablespace

Error: Oracle Redo Logs are on the file system '/SAN02' that is shared by

1. UNDOTBS1 Tablespace
2. USERS Tablespace
3. SYSAUX Tablespace
4. ARC_SYSTEM_DATA Tablespace
5. ARC_UNDO Tablespace
6. ARC_EVENT_DATA Tablespace
7. ARC_SYSTEM_INDEX Tablespace
8. ARC_EVENT_INDEX Tablespace
9. SYSTEM Tablespace
10. ARC_TEMP Tablespace
11. Oracle Redo Log
12. TEMP Tablespace
13. PATROL_DATA Tablespace

This can severely impact the database performance. If ever possible, please move the redo logs to a dedicated volume on separate spindles!!!

Partition Manager Errors

NAME	CREATION STATUS	STATS_UPDATE STATUS
20110224	CREATION FAILED [ARC_SLD_7101SR]	SUCCESS

Partition Compressor Errors

ARC_PARTITION_NAME	ORA_PARTITION_NAME	EXCHANGETABLE	CREATED	INDEXES_CREATED	TABLE
20110319	ARC_EVENT_20110319	YES		YES	NO
20110320	ARC_EVENT_20110320	YES		YES	NO

Partition Archiver Errors (Recorded by the Partition Archive Agent)

NAME	ACTIVE	ARCHIVED	ARCHIVE_TIME	ARCHIVE_TYPE	ARCHIVE_DIRECTORY	ARCHIVE_STATUS	ARCHIVE_SIGNATURE	REACTIVATION_STATUS	DEACTIVATION_S
------	--------	----------	--------------	--------------	-------------------	----------------	-------------------	---------------------	----------------

Partition Archiver Errors (As Seen by the ArcSight Manager)

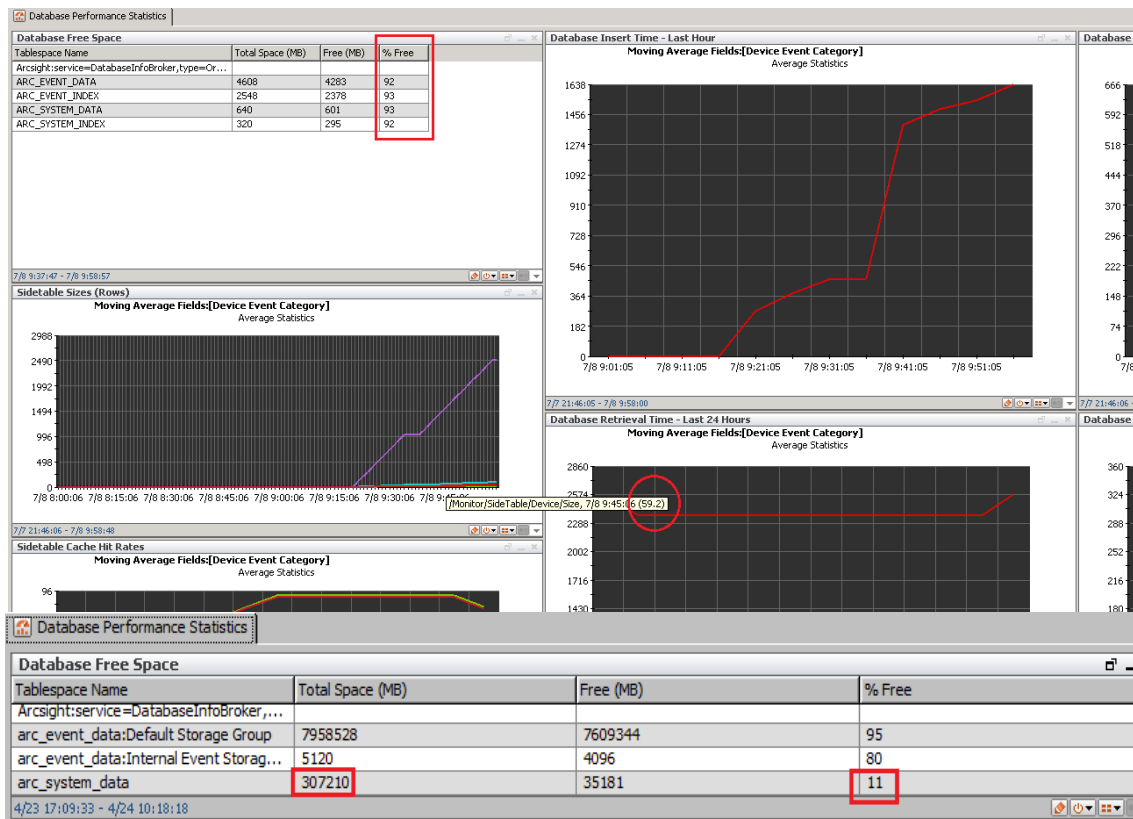
NAME	ACTIVE	ARCHIVED	ARCHIVE_TIME	ARCHIVE_TYPE	ARCHIVE_DIRECTORY	ARCHIVE_STATUS	ARCHIVE_SIGNATURE	REACTIVATION_STATUS	DEACTIVATION_S
------	--------	----------	--------------	--------------	-------------------	----------------	-------------------	---------------------	----------------



ESM Database and Storage

“Database Performance Statistics” Dashboard Check

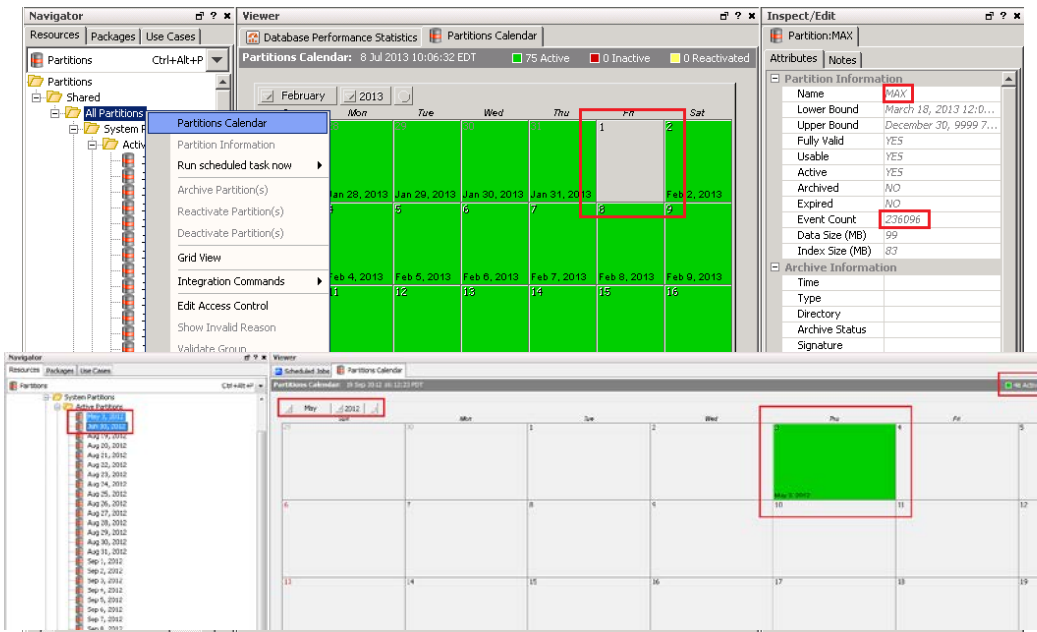
- Database Free Space
 - If the Event Data Free Space is low (below 10% free), there are three ways to fix this situation:
 - Increase the “online” event storage size and extend the database
 - Reduce the “online” retention period
 - Reduce the event volume
- Sidetable Sizes – Rows (Oracle)
 - Common problem:
 - The number of rows in the Device Descriptor Side Table is high (above 50,000 entries). This is usually caused by a parsing problem in the Connector, however in some cases there really are thousands of unique Device Addresses. Execute ‘SideTableStats.sql’ on the database to reveal what’s causing this problem.



ESM Database and Storage (continued)

Partition Check (Oracle)

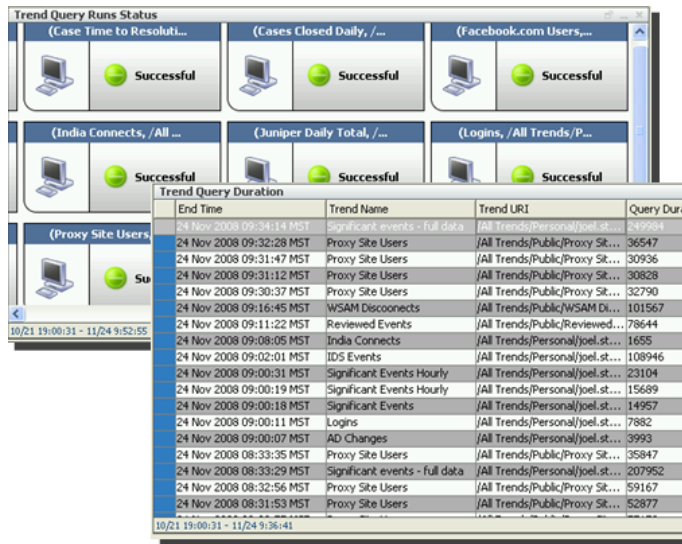
- Check the Partitions in the ArcSight Console for the following:
 - Are there any “orphan” partitions? (Partitions that are outside of the retention period)
 - Are there re-activated archived partitions that are no longer in use?
 - Are there any events in the MAX partition?
- Check the following logs for errors in Partition Jobs
 - ../manager/logs/default/**partitionmanager.log**
 - ../manager/logs/default/**partitionstatsupdater.log**
 - ../manager/logs/default/**partitioncompressor.log**
 - ../manager/logs/default/**partitionarchiver.log** (if archiving is enabled)



ESM Database and Storage (continued)

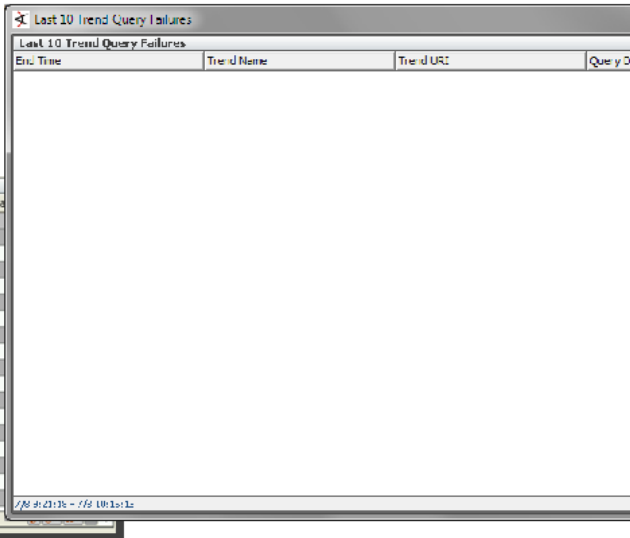
Trend Jobs Check

- Check the “Trends Status” Dashboard
 - Failed Trend Runs
 - Trends that appear to take longer than others to complete
 - Are problems caused by poorly written Trends or pre-existing Database performance problems?
- Check the “Task Manager” in the ArcSight Console to ensure Trend jobs are scheduled properly (i.e. staggered, off hours, etc.) to prevent them from conflicting with each other (and analysts using Active Channels) over database resources



The screenshot shows the 'Trend Query Runs Status' dashboard. At the top, there are three status cards: '(Case Time to Resoluti...', '(Cases Closed Daily, /...', and '(Facebook.com Users,...', all showing a green 'Successful' status. Below these are three more cards: '(India Connects, /All ...', '(Juniper Daily Total, /...', and '(Logins, /All Trends/P...', also showing 'Successful'. At the bottom left is a card for '(Proxy Site Users' with a green status. To the right of these cards is a table titled 'Trend Query Duration'.

End Time	Trend Name	Trend URI	Query Duration
24 Nov 2008 09:34:14 MST	Significant events - full data	/All Trends/Personal/joel.st...	849984
24 Nov 2008 09:32:28 MST	Proxy Site Users	/All Trends/Public/Proxy Sit...	36547
24 Nov 2008 09:31:47 MST	Proxy Site Users	/All Trends/Public/Proxy Sit...	30936
24 Nov 2008 09:31:12 MST	Proxy Site Users	/All Trends/Public/Proxy Sit...	30828
24 Nov 2008 09:30:37 MST	Proxy Site Users	/All Trends/Public/Proxy Sit...	32790
24 Nov 2008 09:16:45 MST	WSAM Disconnects	/All Trends/Public/WSAM DI...	101567
24 Nov 2008 09:11:22 MST	Reviewed Events	/All Trends/Public/Reviewed...	78644
24 Nov 2008 09:08:05 MST	India Connects	/All Trends/Personal/joel.st...	1655
24 Nov 2008 09:02:01 MST	IDS Events	/All Trends/Personal/joel.st...	108946
24 Nov 2008 09:00:31 MST	Significant Events Hourly	/All Trends/Personal/joel.st...	23104
24 Nov 2008 09:00:19 MST	Significant Events Hourly	/All Trends/Personal/joel.st...	15689
24 Nov 2008 09:00:18 MST	Significant Events	/All Trends/Personal/joel.st...	14957
24 Nov 2008 09:00:11 MST	Logins	/All Trends/Personal/joel.st...	7882
24 Nov 2008 09:00:07 MST	AD Changes	/All Trends/Personal/joel.st...	3993
24 Nov 2008 08:33:35 MST	Proxy Site Users	/All Trends/Public/Proxy Sit...	35847
24 Nov 2008 08:33:29 MST	Significant events - full data	/All Trends/Personal/joel.st...	207952
24 Nov 2008 08:32:56 MST	Proxy Site Users	/All Trends/Public/Proxy Sit...	59167
24 Nov 2008 08:31:53 MST	Proxy Site Users	/All Trends/Public/Proxy Sit...	52877



The screenshot shows the 'Last 10 Trend Query Failures' window. It contains a table with columns: 'Err. Time', 'Trend Name', 'Trend URI', and 'Query Duration'. The table is currently empty.

Err. Time	Trend Name	Trend URI	Query Duration
-----------	------------	-----------	----------------

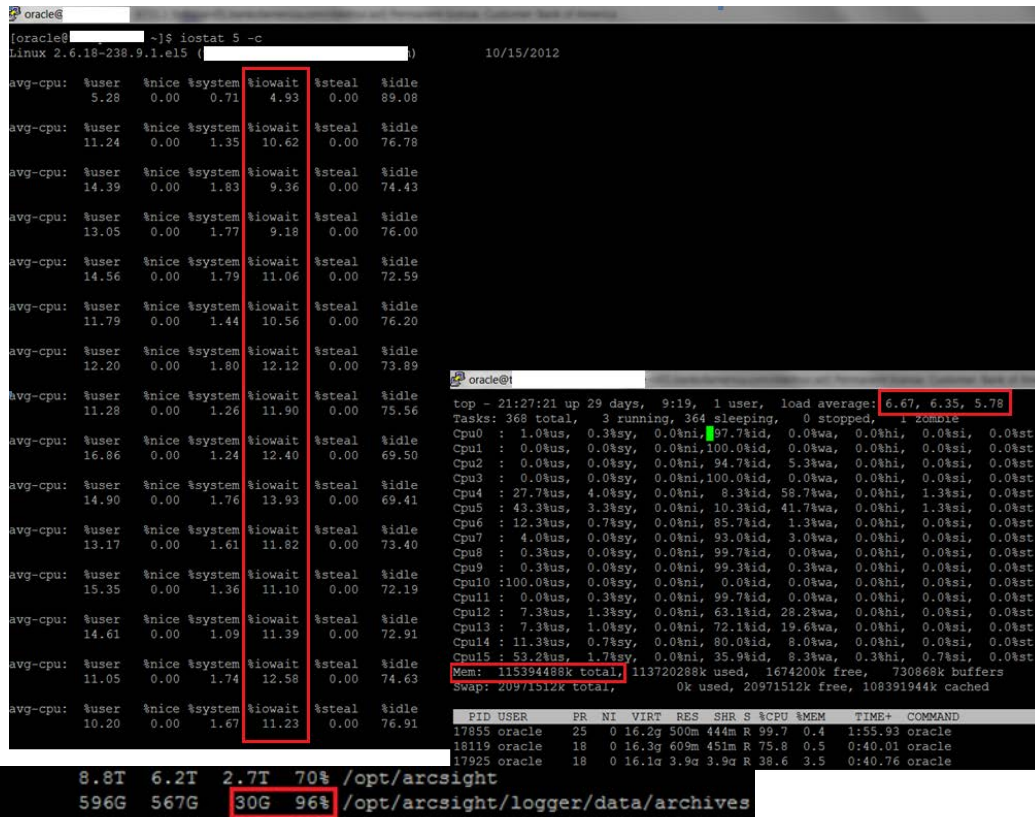
ESM Database and Storage (continued)

Hardware and Operating System Check

- Is there sufficient CPU Cores and Memory to support the event rate and use cases (content)?
- Is there sufficient free Disk Space to extend the 'online' database if needed?
- Is there sufficient free Disk Space for the offline archives?
- Is the Operating System supported?

CPU and Memory Utilization Check

- Use standard Operating System tools to check for high CPU and Memory utilization
- If the utilization is high, is it ArcSight or a third-party process that's causing it?
- Understanding Load Averages in Linux Top:
<http://blog.scoutapp.com/articles/2009/07/31/understanding-load-averages>



/dev/md0	8.8T	6.2T	2.7T	70%	/opt/arcSight
/dev/md1	596G	567G	30G	96%	/opt/arcSight/logger/data/archives



ESM Database and Storage (continued)

Oracle version and patch level check

- Verify that Oracle is on the correct version that's certified for the current version of ESM (see Product Lifecycle Doc or Release Notes)
 - Oracle 10g or 11g
 - Oracle CPU/PSU Patch
 - Many performance issues have been alleviated by applying the Oracle PSU certified with that version of ArcSight
 - If you are not sure that your system has an Oracle PSU or CPU, refer to Knowledge Base Article KM1270280

```
[oracle@ ██████████ OPatch]$ ./opatch lsinventory
Invoking OPatch 11.2.0.1.1

Oracle Interim Patch Installer version 11.2.0.1.1
Copyright (c) 2009, Oracle Corporation. All rights reserved.


Oracle Home      : /opt/oracle/OraHome11g
Central Inventory : /opt/oracle/oraInventory
   from           : /etc/oraInst.loc
OPatch version   : 11.2.0.1.1
OUI version      : 11.2.0.2.0
OUI location     : /opt/oracle/OraHome11g/oui
Log file location : /opt/oracle/OraHome11g/cfgtoollogs/opatch/opatch2012-09-18_16-51-51PM.log


Patch history file: /opt/oracle/OraHome11g/cfgtoollogs/opatch/opatch_history.txt
Lsinventory Output file location : /opt/oracle/OraHome11g/cfgtoollogs/opatch/lsinv/lsinventory2012-09-18_16-51-51PM.txt


-----
Installed Top-level Products (1):

Oracle Database 11g                               11.2.0.2.0
There are 1 products installed in this Oracle Home.

There are no Interim patches installed in this Oracle Home.

-----

OPatch succeeded.
[oracle@ ██████████ OPatch]$ pwd
/opt/oracle/OraHome11g/OPatch
[oracle@ ██████████ OPatch]$
```



ESM Database and Storage (continued)

Oracle alert log check

- Check for any ORA- errors that have occurred over the last 10 days or so
 - Connectivity timeouts
 - Data file corruption
 - ORA-01555 snapshot too old
- Make sure the Redo logs are not switching too often
 - No more than 3-4 times an hour
 - If the redo logs are switching too often, increase the size of the Redo logs. If they are 4GB each, then increase them to 8GB each
 - See Knowledge Base Article KM1270172 to increase the size of the Redo logs

```

[oracle@rac1 ~]$ psd
/opt/oracle/OracleHome10g/admin/arcshg/bdump
[oracle@rac1 ~]$ ls *.trc | wc -l
6466
[oracle@rac1 ~]$ bdump]$
[oracle@rac1 ~]$ tail -1000 alert_arcshg.log | grep ORA-
ORA-12012: error on auto execute of job 8177775
ORA-04063: ORA-04063: package body "ORACLE_OCM.MGMT_DB_LL_METRICS" has errors
ORA-06508: PL/SQL: could not find program unit being called: "ORACLE_OCM.MGMT_DB_LL_METRICS"
ORA-06512: at line 1
ORA-12012: error on auto execute of job 8188259
ORA-04063: ORA-04063: package body "ORACLE_OCM.MGMT_DB_LL_METRICS" has errors
ORA-06508: PL/SQL: could not find program unit being called: "ORACLE_OCM.MGMT_DB_LL_METRICS"
ORA-06512: at line 1
ORA-12012: error on auto execute of job 8191428
ORA-04063: ORA-04063: package body "ORACLE_OCM.MGMT_DB_LL_METRICS" has errors
ORA-06508: PL/SQL: could not find program unit being called: "ORACLE_OCM.MGMT_DB_LL_METRICS"
ORA-06512: at line 1
[oracle@rac1 ~]$ bdump]$

```



ESM Database and Storage (continued)

Oracle parameters check

- Verify that Oracle is configured to use no more than 70% of the memory on the server
 - Example: If there's 100GB of physical memory, then configure Oracle's memory_target to 70GB
 - See Knowledge Base Article KM1272826 – for configuring larger memory_target for Oracle
- Verify the log_buffer parameter is set to 14M
- Verify the filesystemio_options parameter is set to SETALL



ESM Database and Storage (continued)

CORRE parameters check

Symptom

- Trend or report fails to run
- Logs show *“temporary sort space limit exceeded”* or *“total number of locks exceeds the lock table size”*

Root cause = sort space

- The query is producing a large number of distinct rows and exceeding the allocated temporary space

Workaround

- Refine query to reduce results
- Adjust timing of queries to limit overlap of queries based on temp space needs
- Increase **sort_temp_limit** in my.cnf
- (TIP: use query viewer to test query to find minimum value)

Root cause = locks

- Buffer size insufficient to handle result set

Workaround

- Refine query to reduce results
- Edit /opt/arcsight/logger/data/mysql/my.cnf
- Increase **innodb_buffer_pool_size**



ESM Database and Storage (continued)

ESM Database Storage Check

- Check for I/O contention
 - Linux/Unix: Execute iostat and look for high I/O Waits
 - Windows: Use Performance Monitor and check for high Disk Queue Length
- Check with the Storage Admin to validate the SAN storage is configured properly for ArcSight
 - If possible, ask the Storage Admin to run diagnostics using tools supplied by the SAN vendor
 - How many IOPS does the current SAN configuration support?
 - Are there enough IOPS to support the current & forecasted event rates?
 - Validate the following configuration with the Storage Admin:
 - RAID 1+0
 - Dedicated spindles (disks) for ArcSight, not shared with other applications
 - Fibre attached storage
 - Verify that Data Files and Redo Logs are on separate Disk Groups and separate LUNs (Oracle only)
- Are the data files sized according to ArcSight's best practices? (I.E. create the least number of data files to represent the tablespace)
- Is there sufficient free Disk Space to extend the "online" database if needed?
- If event archiving is enabled, is there sufficient free Disk Space for the offline archives?

See the following slide for examples of Disk I/O performance (at least what the Operating System will tell us)...



ESM Database and Storage (continued)

ESM Database Storage Check (continued)

Good

```
[oracle@ ~]$ iostat 5 -c
Linux 2.6.18-194.3.1.el5 ( ) 10/16/2012
```

	avg-cpu:	%user	%nice	%system	%iowait	%steal	%idle
		1.73	0.00	0.43	2.64	0.00	95.20
		0.72	0.00	0.15	0.25	0.00	98.88
		0.61	0.00	0.22	0.20	0.00	98.96
		0.85	0.00	0.26	0.20	0.00	98.69
		4.86	0.00	0.65	0.24	0.00	94.25
		10.27	0.00	0.94	0.26	0.00	88.53
		4.18	0.00	0.31	0.41	0.00	95.10
		1.05	0.00	0.21	0.19	0.00	98.55
		0.65	0.00	0.22	0.34	0.00	98.79
		0.81	0.00	0.29	0.29	0.00	98.61
		0.80	0.00	0.29	0.36	0.00	98.55
		0.61	0.00	0.19	0.12	0.00	99.08
		0.83	0.00	0.21	0.24	0.00	98.72
		0.74	0.00	0.19	0.20	0.00	98.88
		0.55	0.00	0.16	0.18	0.00	99.11

Bad

```
avg-cpu:  %user   %nice %system %iowait  %steal   %idle
            8.12    0.00    2.29    7.31    0.00   82.28
```

	avg-cpu:	%user	%nice	%system	%iowait	%steal	%idle
		8.94	0.00	2.44	7.06	0.00	81.56
		9.14	0.00	2.63	6.62	0.00	81.60
		8.18	0.00	2.96	6.78	0.00	82.08
		8.07	0.00	3.38	6.81	0.00	81.74
		7.65	0.00	2.92	7.47	0.00	81.96
		7.83	0.00	2.89	6.34	0.00	82.94
		8.08	0.00	2.18	6.44	0.00	83.30
		6.33	0.00	2.34	7.53	0.00	83.80
		5.70	0.00	2.63	6.71	0.00	84.96
		5.34	0.00	2.61	6.22	0.00	85.83
		6.04	0.00	2.76	6.75	0.00	84.44
		6.39	0.00	3.03	6.11	0.00	84.46
		7.00	0.00	2.82	6.13	0.00	84.05
		6.98	0.00	2.77	6.12	0.00	84.14
		6.21	0.00	2.76	5.43	0.00	85.60

Ugly

```
[oracle@ ~]$ iostat 5 -c
Linux 2.6.18-238.9.1.el5 ( )
```

	avg-cpu:	%user	%nice	%system	%iowait	%steal	%idle
		5.28	0.00	0.71	4.93	0.00	89.08
		11.24	0.00	1.35	10.62	0.00	76.78
		14.39	0.00	1.83	9.36	0.00	74.43
		13.05	0.00	1.77	9.18	0.00	76.00
		14.56	0.00	1.79	11.06	0.00	72.59
		11.79	0.00	1.44	10.56	0.00	76.20
		12.20	0.00	1.80	12.12	0.00	73.89
		11.28	0.00	1.26	11.90	0.00	75.56
		16.86	0.00	1.24	12.40	0.00	69.50
		14.90	0.00	1.76	13.93	0.00	69.41
		13.17	0.00	1.61	11.82	0.00	73.40
		15.35	0.00	1.36	11.10	0.00	72.19
		14.61	0.00	1.09	11.39	0.00	72.91
		11.05	0.00	1.74	12.58	0.00	74.63
		10.20	0.00	1.67	11.23	0.00	76.91



Additional resources



My favorite resources for keeping ArcSight healthy

1. Any HP Protect presentation on ArcSight best practices or troubleshooting:
<https://protect724.arcsight.com>
2. KB Articles on the HP Support Site
3. Solutions listed in previous Support Tickets
4. HP ArcSight University
5. HP ArcSight product documentation



Please give me your feedback

Session TB3259

Speaker Tracy Barella

Please fill out a survey.

Hand it to the door monitor on your way out.

Thank you for providing your feedback, which helps us enhance content for future events.



Thank you





Make it matter.