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 -noplot`
    - Connector: `../current/bin/arcsight agent logfu -a`
  - Oracle RDA
- ArcSight System Management Interface
  - [https://<managerhost>:8443](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

<table>
<thead>
<tr>
<th>Connectors</th>
<th>Connector Appliances</th>
<th>ESM Manager</th>
<th>ESM Database and Storage</th>
<th>Loggers</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓ Up/Down Check (Connector or Container)</td>
<td>✓ Version Check</td>
<td>✓ “Event Throughput!” Dashboard Check</td>
<td>✓ DBCheck and Oracle RDA</td>
<td>✓ CPU, Memory, and EPS In/Out Check</td>
</tr>
<tr>
<td>✓ Version Check</td>
<td>✓ CPU and Memory Check</td>
<td>✓ “Current Event Sources” Dashboard Check</td>
<td>✓ “Database Performance Statistics” Dashboard Check</td>
<td>✓ Search Performance Check</td>
</tr>
<tr>
<td>✓ Connector Event Rate Check (by EPS)</td>
<td>✓ Network Settings Check</td>
<td>✓ Hardware and Operating System Check</td>
<td>✓ Partition Check (Oracle)</td>
<td>✓ Custom Report Performance Check</td>
</tr>
<tr>
<td>✓ Cache Check</td>
<td>✓ Configuration Backup Check</td>
<td>✓ CPU and Memory Utilization Check</td>
<td>✓ Trend Jobs Check</td>
<td>✓ Receivers and Forwarders Check</td>
</tr>
<tr>
<td>✓ Logs Check</td>
<td>✓ ESM Manager JVM (memory) Utilization Check</td>
<td>✓ ESM Manager JVM (memory) Utilization Check</td>
<td>✓ Hardware and Operating System Check</td>
<td>✓ Storage Group Check</td>
</tr>
<tr>
<td>✓ Configuration Check</td>
<td>✓ Data Monitor Utilization Check</td>
<td>✓ Partition Check (Oracle)</td>
<td>✓ CPU and Memory Utilization Check</td>
<td>✓ Index Configuration Check</td>
</tr>
<tr>
<td></td>
<td>✓ Active List/Session List Utilization Check</td>
<td>✓ Trend Jobs Check</td>
<td>✓ Oracle Version and Patch Level Check</td>
<td>✓ Configured Alerts Check</td>
</tr>
<tr>
<td></td>
<td>✓ Rules Engine Check</td>
<td>✓ Hardware and Operating System Check</td>
<td>✓ Oracle Alert Log Check</td>
<td>✓ Scheduled Task Check</td>
</tr>
<tr>
<td></td>
<td>✓ Event Persistence (insertion) Performance Check</td>
<td>✓ CPU and Memory Utilization Check</td>
<td>✓ Oracle Memory Parameters Check</td>
<td>✓ Event Archive and Configuration Backup Check</td>
</tr>
<tr>
<td></td>
<td>✓ Error Check</td>
<td>✓ Oracle Version and Patch Level Check</td>
<td>✓ ESM Database Storage Check</td>
<td>✓ Logger System Health and Audit Event Forwarding Check</td>
</tr>
<tr>
<td></td>
<td>✓ Scheduled Task Check</td>
<td>✓ Oracle Alert Log Check</td>
<td></td>
<td>✓ Network Configuration Check</td>
</tr>
<tr>
<td></td>
<td>✓ server.properties Check</td>
<td>✓ Oracle Memory Parameters Check</td>
<td></td>
<td>✓ Online Event Storage Check (Only Software-based or SAN Logger)</td>
</tr>
<tr>
<td></td>
<td>✓ Agent and Console Threads Check</td>
<td>✓ ESM Database Storage Check</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
“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
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
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
ESM Manager (continued)

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

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

Rules Engine Check

- Review the Rules Status Dashboard
  - Tune or disable Rules with excessive partial matches
  - Fix Rules with errors, loops, auto disabled Rules, etc.
  - Review the “Top Firing Rules” Data Monitor for excessive Rule fires and tune or disable as needed
- Tip: Utility Rules (i.e. Dedicated Rules for Active List entry imports, user logon tracking, etc.) should be configured as Lightweight Rules to prevent unnecessary Rule fires. This strategy will reduce the Correlation event count and memory overhead
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.
ESM Manager (continued)

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 noplot`
  - 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.theshold`

⚠️ **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?
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

Connectors
- Up/Down Check (Connector or Container)
- Version Check
- Connector Event Rate Check (by EPS)
- Cache Check
- Logs Check
- Configuration Check

Connector Appliances
- Version Check
- CPU and Memory Check
- Network Settings Check
- Configuration Backup Check

ESM Manager
- "Event Throughput!" Dashboard Check
- "Current Event Sources" Dashboard Check
- Hardware and Operating System Check
- CPU and Memory Utilization Check
- ESM Manager JVM (memory) Utilization Check
- Data Monitor Utilization Check
- Active List/Session List Utilization Check
- Rules Engine Check
- Event Persistence (insertion) Performance Check
- Error Check
- Scheduled Task Check
- server.properties Check
- Agent and Console Threads Check

ESM Database and Storage
- DBCheck and Oracle RDA
- "Database Performance Statistics" Dashboard Check
- Partition Check (Oracle)
- Trend Jobs Check
- Hardware and Operating System Check
- CPU and Memory Utilization Check
- Oracle Version and Patch Level Check
- Oracle Alert Log Check
- Oracle Memory Parameters Check
- ESM Database Storage Check

Loggers
- CPU, Memory, and EPS In/Out Check
- Search Performance Check
- Custom Report Performance Check
- Receivers and Forwarders Check
- Storage Group Check
- Index Configuration Check
- Configured Alerts Check
- Scheduled Task Check
- Event Archive and Configuration Backup Check
- Logger System Health and Audit Event Forwarding Check
- Network Configuration Check
- Online Event Storage Check (Only Software-based or SAN Logger)
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’)

---

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
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
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
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]$ OPatchU $/opatch lsinventory
Invoking OPatchU
Oracle Interim Patch Installer version 11.2.0.1.1
Copyright (c) 2009, Oracle Corporation. All rights reserved.

Oracle Home : /opt/oracle/Oracle11g
Control Inventory : /opt/oracle/oraInventory
from : /etc/oraInst.loc
OPatch version : 11.2.0.1.1
CPU version : 11.2.0.2.1
CPU location : /opt/oracle/Oracle11g/cpu
Log file location : /opt/oracle/Oracle11g/bug/OPatch112012-09-15_16-51-51PM.log
Patch history file: /opt/oracle/Oracle11g/cfgtoollogs/opatch/opatch_history.txt

Inventory Output file location : /opt/oracle/Oracle11g/cfgtoollogs/opatch/lsinventory112012-09-15_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.
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
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)...

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
ESM Database and Storage (continued)

ESM Database Storage Check (continued)

<table>
<thead>
<tr>
<th>Good</th>
<th>Bad</th>
<th>Ugly</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Table Content" /></td>
<td><img src="image" alt="Table Content" /></td>
<td><img src="image" alt="Table Content" /></td>
</tr>
</tbody>
</table>

39 © Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
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
HP

Make it matter.