HP Enterprise Security Products

Advanced Logger Forwarder Tuning

Best Practices and Recommendations

Feb 4, 2014

Contents

General information

Logger Forwarder - Introduction

Forwarders send all events, or events which match a particular filter, on to a particular host. The ability to define a different filter for each forwarder allows Logger to divide traffic among several destinations. For example, because Logger can handle much higher event rates than ArcSight Manager, Logger might be used to forward events to a number of ArcSight Managers. Forwarder filters make it possible to split the flow between the Managers, using one forwarder for each Manager. Additionally, forwarding enables you to send a subset of events to other destinations for further processing while maintaining all events on Logger for long-term storage.

The forwarding filter is a query that searches for matching events, optionally within a time range. You can create two types of forwarder filters—continuous and time-range bound.

A continuous filter constantly evaluates the incoming events and forwards the matching ones to the specified destination.

A time-range bound filter uses a time range in addition to the specified condition to determine whether an event should be forwarded to the destination. If the event falls within the specified time range and matches the specified condition, it is forwarded; otherwise, it is not. The Logger receipt time of an event is used to determine whether an event will be forwarded to a destination when a forwarder filter specifies a time range by which events are evaluated for forwarding. Once a forwarder has forwarded all events within a time range, it does not forward any more events.

A forwarder only forwards events from the Logger that it is configured on; it cannot forward events from peer Loggers.

A forwarder's operation can be paused and resumed at any point in time. When a forwarder resumes operation, forwarding resumes from the last checkpoint that was established before the forwarding operation was paused.

You can also disable and re-enable a forwarder. When you re-enable a forwarder, all previously established checkpoints are removed and forwarding starts over again as per the forwarder configuration-forwarders with continuous filters start from the current time, while forwarders with time-range bound filters start from beginning of the configured time range.

Forwarder types include UDP Forwarder, TCP Forwarder, Connector Forwarder, and ArcSight ESM Forwarder:

UDP: UDP forwarders forward events by using the User Datagram Protocol.

TCP: TCP forwarders forward events by using the Transmission Control Protocol.

Connector Forwarder: Connector forwarders send events to the Logger Streaming Connector.

ArcSight ESM: ArcSight ESM forwarders send Common Event Format (CEF) events to an ESM Destination. The built-in connector on Logger is used to forward these events to ESM.

Prior to Logger 5.2, you could only specify a regular expression query for the filter. However, starting with 5.2, you can also specify indexed search queries (known as Unified Queries). Doing so enables you to take advantage of the indexing technology to quickly and efficiently search for events to forward.

Note: Unified query-based forwarders forward events once they have been indexed. Therefore, these forwarders can exhibit “bursty” behavior because indexing occurs in batches on Logger. You might notice the bursty behavior in the EPS out gauge (on top of the Logger interface screen)—the gauge will display high EPS level as a burst of data is forwarded and then drop back to normal level.

HP Enterprise Security Products Global Services

Organization Overview

HP Enterprise Security Products (ESP) Global Services enables customer success by providing world class Education and Consulting Services tailored to meet customer needs. Whether you're just starting to plan your security strategy, beginning a compliance monitoring program, or you are enhancing an existing security program, HP ESP provides the customized training, tools, and expertise needed. Through our work with companies of all sizes in a wide range of industries, we have accumulated the experience and credibility needed to make your project a success. HP ESP Global Services is comprised of the following practices:

HP ESP Education: HP ESP Education offers of range of learning options for HP ESP customers and partners. Services include:

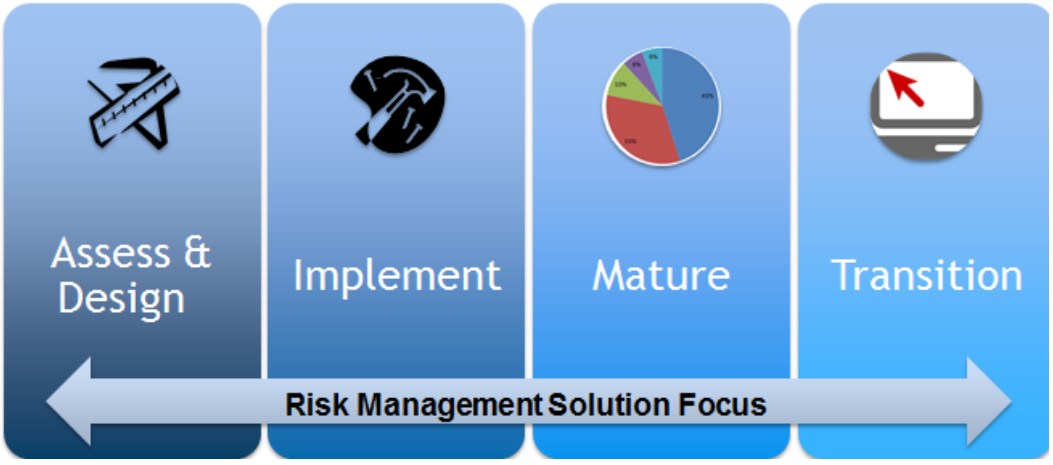
- *Instructor-led training at HP ESP and customer facilities*
- *Computer-based and self-study training*
- *Certification programs and tracks*

HP ESP Consulting: HP ESP Consultants assist customers throughout the project lifecycle including strategy and planning sessions, requirements gathering, design and architecture, implementation, and operations. System functionality will be verified, performance testing conducted and benchmarks for the system documented. Customers will learn how to create and manage the power of HP ESP. The end result is a solution that has been tailored to your unique business needs and ensures that you leverage the full power of HP enterprise security products.

Security Operations: HP ESP's Security Operations consultants assist customers in the development of an internal security monitoring and response capability. Delivered as an HP ESP global services engagement, our consultants will gather your organization's business and technical requirements to develop and implement security operations that address the needs of your business. Our consultants accelerate your HP ESP product implementation, help you meet your business objectives and requirements in a timely fashion, and shorten the learning curve for customer personnel. Ultimately, the solution can provide cost savings due to the operational efficiencies gained by mature security operations founded on the ArcSight ESM infrastructure.

Project Phases

HP ESP executes a four-phase project strategy for the establishment of a **Universal Log Management** capability as outlined in the following sections on the next page.



Phase I: Assess & Design: This phase of the methodology is designed to gain an in-depth understanding of the customer's environment. Business drivers are defined**,** stakeholders identified, and requirements (i.e. use cases) derived. From the information gathered, a solution is designed and architected to satisfy the specified requirements. Resource requirements are communicated and tasks prioritized according to the customer's need.

Phase II: Implement: This phase of the methodology involves implementation and integration of the various technologies required to satisfy the requirements. Installation and configuration of ESM, Logger, Connector Appliance, and NSP are typical activities for this phase.

Phase III: Mature: This phase involves technology optimization & tuning as well as performing health checks. The phase also involves identifying additional use cases and incorporating them into the existing solution to extend capabilities of the solution.

Phase IV: Transition: This phase involves the knowledge transfer in the area of intrusion analysis, incident response, and escalation procedures to ensure the customer can successfully respond to identified incidents leveraging the implemented solution and defined process and procedures.

HP ESP Deployments using the phases above

The following chart depicts how a typical deployment maps to the methodology.

Align Solution with Business Requirements	Technical Implementation	Refine solution and optimize	Results: Production

• Define business drivers
• Identify Stakeholders
• Understand customers environment and requirements
• Design and architect solution to meet requirements
• Document in Project Plan & Prioritized Use Case list
	• ArcSight implementations
	  - Database
	  - ESM Manager
	  - Logger
	  - Connector Appliance
	  - Network Synergy Platform
	• Advanced Integrations
	  - Authentication
	  - High Availability
	  - ESM/Logger/CA/ NSP
	• Automate Reporting
	• Document configuration
		• Technology Optimization and tuning
		• Perform health checks on the solution
		• Document solutions details
		• Develop advanced use cases
		• User Feedback and refinement
			• Conduct end user Training
			• Complete knowledge transfer
			• Define career paths of analysts
			• Transfer process improvement framework
			• Collect user feedback
			• Engagement close-out

Tuning Recommendations

Best Practices - Summary

We recommend no more than 3-4 forwarders max. If the customer can use a single forwarder to forward events to a destination, we recommend using a single forwarder. Peak output is on average 3000 EPS total for Logger, NOT 300 EPS for each forwarder. Use one forwarder and apply a filter-out filter on the connector resource in ESM to exclude data that you do not want to forward. Avoid multiple forwarders at all costs

Do not use basic aggregation for Logger's built-in SmartConnector because it is resource intensive. (Basic aggregation is set using the Enable Aggregation (in seconds) field from the ArcSight Console.)

The Logger should be able to forward events to a maximum of 1-2 ESM destinations using 5-10 forwarders for the average customer's environment (EPS In around 2-5K). If the forwarders use more complex filters and the "EPS In" is a 5-10K or more we can start seeing the Logger server's JVM running out of memory, in which case it is normally recommended to reduce the number of forwarders. Regardless, we recommend reducing the amount of forwarders as much as possible.

Please consider having a fewer number of forwarders when forwarding events to the same ESM destination. Instead you can logically separate the events into several active channels once they arrive to the ESM (e.g from one forwarder). In other words usually there is no need to create several forwarders to send events to the same destination.

Forwarders with Filters - Guidelines:

1. Forwarder with no filters: Limit is about 2500 to 3500 EPS to the ESM destination (mostly depending on the event size). So if the incoming rate (EPS in) of the events (all **to be** forwarded) is higher than that, the forwarder will not be sending all the incoming events in real time.
2. Forwarder with regex filters: Limit (EPS Out) will decrease depending on the complexity of the regex filter (i.e. it will be lower than the limit in the example #1). For example with rather complex regex having multiple OR boolean operators the limit can drop to a few hundreds EPS Out.

Recommended Remediation:

To increase the limit in the example #1. Adding the second logical ESM destination is known to help increase the limit to 20-30% with some performance impact on the Logger.

To increase the limit in the example #2. One way is to move the filtering from the logger's forwarder upstream to the source connectors and devices. If the customer does not want to filter out events coming in to the Logger then another suggestion is to separate the events sent by the source connectors by the 2 streams, each of them going to a dedicated receiver. One of these streams will have the events that should be forwarded to the ESM and another one will have the rest (i.e. the events not to be forwarded). That way the forwarder will only

point to the right receiver without any need to have regex filters. Therefore its limit will not be decreased by the filters, i.e. will match the limit of the example #1.

Alternate Forwarding Method:

Sending events via CEF to a Syslog destination from Logger can increase the outbound EPS rate up to 5000 to 6000 EPS. All other encrypted destinations have the 3000 EPS limit.

Misc Tuning Recommendations:

- Disable events aggregation (from ESM console).
- Make sure the “preserve raw events” is turned off for the connector (Logger's Forwarder connector in ESM). This is also set at the ESM destination.
- Reduce EPS in (into the receivers) through filtering and aggregation.
- Disable the real time alerts on the Logger, and use rules/alerts within ESM instead.
- Complex queries slow the event feed, use simple queries. Simplify the regex filter at the forwarders
- Filter the Forwarding connector on ESM side for better performance
- Do not stack multiple Forwarders
- Disable DNS lookup on Forwarder connector to ESM
- Increase cache for forwarding connector from 1GB up to 50GB to prevent dropped events.
- Convert RegEx filters to Unified filters.

Defragment Logger Database:

Performance issues in receiver and forwarder operations may indicate the need for a database defragmentation. Please refer to the “Database Defragmentation” steps on page 326 of the Logger Administrator’s Guide (5.3 SP1).

Defragment Global Summary Persistence:

Disk space issues or performance issues in receiver, forwarder, or peering operations may indicate the need for a Global Summary Persistence defragmentation. Please refer to the “Global Summary Persistence Defragmentation” steps on page 331 of the Logger Administrator’s Guide (5.3 SP1).

Advanced Tuning:

NOTE: It is strongly recommended that you engage HP Professional Services to perform and evaluate the results of any advanced tuning steps, as they may result in reduced performance.

When the forwarding connector is registered to ESM you can modify the batching settings:

Increase the batch size and decrease the interval. This will cause more events per batch and more frequent batches getting sent. This is the easiest change as it can be made via the ESM console.

From an SSH connection you can make some additional tweaks:

1. **Modify the memory available for the forwarding connector.**

   If the Forwarding Connector is trying to move a lot of data it can get into yellow/red zone and stop processing events.

   To tweak this you can perform the following:

   ```
   vi /opt/arcsight/connector/current/user/agent/agent.wrapper.conf
   ```

   Modify and then save the file with the following configuration:

   ```
   wrapper.java.initmemory=512 (default is 256)
   wrapper.java.maxmemory=512 (default is 256)
   ```

   Note: Don't add too much memory as the Logger has a fixed amount. If you allocate too much here you can impact something else. You must restart the forwarding connector (or the logger) for this to take effect

2. **Increase the number of HTTP transport threads.**

   It is possible to increase the number of HTTP transport threads available for log transfer.

   ```
   vi /opt/arcsight/connector/current/user/agent/agent.properties
   ```

   Add the following line to this file:

   ```
   http.transport.threadcount=2
   ```

   Note: You must restart the forwarding connector (or the logger) for this to take effect

Support Information

If any issues arise, or if you have any questions, please visit our Software Support Online website.

HP Software Support Online (http://www.hp.com/go/hpsoftwaresupport) is available to you around the clock, 24x7, enabling you to:

- Search the technical knowledge base for known problems, technical documents, manuals and patches
- Log, track and update support incidents electronically through a secured environment
- Review, revise, and renew an HP Software Support Contract
- Register to receive e-mail notifications and access to electronic download of many HP software products
- Download the latest software patches for HP software products

Contact Information:

To contact support by phone, please use this link to select your regional contact number.
http://support.openview.hp.com/contact_list.jsp

Additional Support Information can be found in the Support Handbook.
http://support.openview.hp.com/pdf/HP_Software_Customer_Support_Handbook.pdf