

# Integrating security with HP ArcSight

# **Table of contents**

Executive summary	
HP CloudSystem Enterprise overview	
HP CloudSystem Enterprise supply layer	3
HP CloudSystem Enterprise demand and delivery: HP Cloud Service Automation	3
HP CloudSystem Enterprise components	
HP ArcSight overview	
Enterprise Security Manager	
HP ArcSight Logger	5
HP ArcSight Connectors	5
Typical deployment scenarios	6
Sending events in RAW and CEF format to HP ArcSight Logger	6
Sending events to HP ArcSight Logger using Connectors	7
Sending events to HP ArcSight ESM using Connectors	
Devices	9
Grouping devices	9
Forwarding events to HP ArcSight ESM	10
Protecting HP CloudSystem Enterprise components with HP ArcSight	11
Cloud Service Automation 3.1	12
Matrix Operating Environment	13
Server Automation	15
VMware ESXi 5 Host	15
Networking	21
HP TippingPoint Security Management System (SMS) Appliance	22
Protecting CloudSystem Enterprise Services with HP ArcSight	25
HP LAMP solution	25
Working with events	27
Searching the HP ArcSight Logger	27
HP ArcSight ESM – Viewing Events with Active Channels	29
Zones	
Queries	
Rules	
Cloud Security Alliance	
Summary	

Appendix A: ASLinuxAudit.props	
For more information	

## **Executive summary**

Organizations are faced with threats that could disrupt operations and critical IT services. HP CloudSystem Enterprise provides automation to rapidly deliver compute resources to cloud consumers. Security must be a key component to ensure availability of the components that deliver and provision cloud based services. This document is a reference implementation of an HP ArcSight Security Information and Event Management (SIEM) solution and CloudSystem Enterprise. Security is a key concern of organizations deploying resources into private and public cloud environments. In this reference implementation we will explain how to configure HP ArcSight Logger, HP ArcSight Enterprise Security Manager (ESM), and HP ArcSight Connectors to monitor and protect the core components of HP CloudSystem Enterprise. This document will also explain how to configure and protect services provisioned by HP CloudSystem Enterprise with HP ArcSight security products.

**Target audience:** The intended audience of this white paper is system integrators, installers, and administrators of HP CloudSystem Enterprise. The reader should be familiar with CloudSystem Enterprise and HP CloudSystem Matrix.

# **HP CloudSystem Enterprise overview**

With HP CloudSystem Enterprise, an organization can deliver not only laaS, but also anything as a Service (XaaS) directly to line-of-business teams. That is, in addition to delivering virtual servers and storage as services, CloudSystem Enterprise can manage and provision enterprise-grade applications such as Microsoft® Exchange, or even custom developed applications, such as cloud-based services. Figure 1 illustrates the HP CloudSystem Enterprise architecture. HP CloudSystem Enterprise extends the foundation of HP CloudSystem Matrix with the seamless integration of HP Cloud Service Automation (CSA). HP CloudSystem Enterprise manages the entire application-to-infrastructure lifecycle—from provisioning, to managing and monitoring, to releasing resources back to the cloud. The diagram shows how Cloud Service Automation, with its cloud management platform for brokering and managing enterprise grade application and infrastructure cloud services, and HP Matrix Operating Environment are engineered to work together, as well as with additional HP CloudSystem extensions and third-party assets.

### HP CloudSystem Enterprise supply layer

Like the HP CloudSystem Matrix offering, the supply layer in HP CloudSystem Enterprise calls on the Matrix Operating Environment for service delivery of infrastructure elements such as compute, network, storage, and other resources, both physical and virtual. HP CloudSystem Enterprise can also leverage VMware vCloud Director for infrastructure services. Supported infrastructure includes HP BladeSystem servers, HP storage, and HP networking, as well as servers, storage, and networking from third parties.





### HP CloudSystem Enterprise demand and delivery: HP Cloud Service Automation

HP Cloud Service Automation software enables and manages the delivery of application services. It includes user interfaces that allow infrastructure design, specifying what assets will be available, and service design, in which a service designer can add to and manage service catalogs. Cloud Service Automation orchestrates the deployment of compute resources and complex multitier application architectures. It integrates and leverages the strengths of several mature HP management and automation products. And it adds workload management, service design, and a customer portal to create a

comprehensive service automation solution. Cloud Service Automation (CSA) can leverage CloudSystem Matrix infrastructure services, and adds applications to the supply layer. It also expands the system's infrastructure capabilities: for example, with CSA, HP CloudSystem Enterprise can support multiple hypervisors—such as those from VMware, Microsoft, KVM, and Xen—within the supply layer. Cloud Service Automation also provides portal services for the demand layer, where consumers or business users can request services. The software delivers laaS and PaaS in a heterogeneous environment, as well as virtual desktop infrastructure (VDI or "Desktop as a Service") and XaaS. Cloud Service Automation manages the entire cloud service lifecycle, including provisioning the infrastructure, whether by extension to one—or several—Matrix Operating Environment resource pools, or from non-Matrix infrastructure pools. It also handles provisioning, patching, and ensuring compliance of business and custom applications; managing and monitoring the cloud; and releasing resources back to the cloud. Extensions allow adding further service assurance, enhanced security, storage management, and network management.

HP CloudSystem Enterprise users can:

- Broker and manage on-demand application and infrastructure services
- Enforce compliance
- Meet service-level agreements (SLAs) with performance and availability management
- Secure data with multi-tenancy and role-based access
- Deliver comprehensive, unified service lifecycle management

### HP CloudSystem Enterprise components

Besides Cloud Service Automation, components of CloudSystem Enterprise that enable its capabilities include:

### HP Operations Orchestration (00)

00 coordinates communication between integrated products and managed devices.

#### **HP Server Automation (SA)**

SA deploys operating systems and policies to managed devices. It provides lifecycle server management and automated application deployment, and automates tasks such as provisioning, patching, configuration management, and compliance management. This software can also provision operating systems, and can automate the ongoing lifecycle management of a deployed OS or application with policy-based patching and compliance capabilities.

#### HP Database and Middleware Automation (DMA)

DMA provides a content library for database and middleware management. It provisions application architectures onto existing infrastructure, and can also manage those applications, providing pre-packaged workflows for application patching, compliance, and code release. DMA eliminates the need for manual customization.

#### **HP SiteScope**

SiteScope provides agentless monitoring of infrastructure platforms and the key performance indicators (KPIs) of applications. KPIs include CPU, disk, and memory usage, etc.

#### HP Universal Configuration Management Database (UCMDB)

UCMDB maintains accurate, up-to-date information regarding the relationships between infrastructure, applications, and cloud services.

#### **HP Matrix Operating Environment**

Matrix Operating Environment supplies infrastructure services. Cloud Service Automation is thoroughly integrated with the infrastructure services created by the Matrix Operating Environment and through this layer can burst to public cloud services.

### **HP ArcSight overview**

### **Enterprise Security Manager**

HP ArcSight Enterprise Security Manager (ESM) is the premiere security event manager that analyzes and correlates every operational event (login, logoff, file access, database query), or other event in order to support your IT team in every aspect of security event monitoring, from compliance and risk management to security intelligence and operations. The ArcSight ESM event log monitor sifts through millions of log records to find the targeted critical events, and presents them in real time via dashboards, notifications, and reports, so you can accurately prioritize security risks and compliance violations. By adding HP Reputation Security Monitor (RepSM), vetted reputation-based threat intelligence can be correlated with security events to identify threats earlier and to detect and avert even the most sophisticated attacks.

Key Benefits

- A cost-effective solution for all your regulatory compliance needs
- Automated log collection and archiving
- Fraud and Real-time threat detection
- · Forensic analysis capabilities for cyber security
- Detect threats early using timely reputation data with HP RepSM

### **HP ArcSight Logger**

With HP ArcSight Logger you can improve everything from compliance and risk management, security intelligence and IT operations to efforts that prevent insider and advanced persistent threats. This universal log management solution collects machine data from any log-generating source and unifies the data for searching, indexing, reporting, analysis, and retention. And in the age of Bring Your Own Device (BYOD) and mobility, it enables you to comprehensively manage an increasing volume of log data from an increasing number of sources.

Key features

- Collect logs from any log generating source through 300+ connectors from any device and in any format
- Unify data across IT through normalization and categorization, into a common event format (CEF registered)
- · Search through millions of events using a text-based search tool with a simple interface
- Store years' worth of logs and events in a unified format through a high compression ratio at low cost
- Automate analysis, alerting, reporting, intelligence of logs and events for IT security, IT operations, IT Governance Risk Management and Compliance (GRC), and log analytics

### **HP ArcSight Connectors**

HP ArcSight Connectors solve the problem of managing log records in hundreds of different formats. While the HP ArcSight SIEM Platform can collect log records in native formats, HP ArcSight Connectors provide normalization to a common format, which greatly improves reporting and analysis. By normalizing all events into one common event taxonomy, HP ArcSight Connectors decouple analysis from vendor selection. This approach has four significant advantages:

#### Centrally manage 300+ connectors through HP ArcSight Connector Appliance (ConApp)

HP ArcSight Connector appliance manages the ongoing updates, upgrades, configuration changes and administration of a distributed log collection deployment through a simple and centralized web-based interface. ConApp can be deployed both as an appliance and software.

#### **Future proofing**

If a Cisco router is swapped for a Juniper router or if a new SQL database is added to a network that previously only had Oracle, no reporting or rules changes are required and the organization retains continuous visibility into all activity.

#### **Ease of analysis**

The HP ArcSight common event format eliminates the need for end users to be familiar with hundreds of different log syntaxes across products. As a result, non-technical line of business users can easily conduct analysis on their own, reducing the burden on IT.

#### Universal content relevance

With the HP ArcSight normalized format, a report that shows "authentication failures" will cover every system automatically, even though one application may refer to authentication failures with a specific event ID while a database refers to the same as an "unsuccessful login."

This unique architecture is supported across hundreds of commercial products out-of-the-box as well as legacy systems. HP ArcSight Connectors also offer various audit quality controls including secure, reliable transmission and bandwidth controls. In addition to software-based deployments, HP ArcSight Connectors are available in a range of plug-and-play appliances that can cost-effectively scale from small store or branch office locations to large data centers. Connector appliances enable rapid deployment and eliminate delays associated with hardware selection, procurement and testing.

# **Typical deployment scenarios**

Security and log event information is captured at the host and application level. Events can be sent directly to an HP ArcSight Logger or HP ArcSight ESM. HP ArcSight Connectors can be used to normalize the log data into the Common Event Format (CEF). The Common Event Format presents log data from various vendors to the HP ArcSight ESM and HP ArcSight Logger in a standardized format for searching and correlation.

Log information can be sent to the HP ArcSight Logger for aggregation; once the data is collected on the HP ArcSight Logger, filters can be applied to forward specific event information to the ArcSight ESM for further analysis, investigation, and action.

Our reference implementation is comprised of the following servers that are illustrated in Figures 2 - 4:

- 00.fog.cloud.internal Operation Orchestration and Cloud Service Automation
- Ora.fog.cloud.internal Oracle Database Server for UCMDB
- Fog.fog.cloud.internal Matrix Operating Environment Central Management Server
- Sis.fog.cloud.internal SiteScope
- UCM.fog.cloud.internal UCMDB server
- vCenter.fog.cloud.internal VMware vCenter
- sa.fog.cloud.internal Server Automation
- tpsms.fog.cloud.internal TippingPoint Security Management System
- esxi1.fog.cloud.internal ESXi Host
- esxi2.fog.cloud.internal ESXi Host

### Sending events in RAW and CEF format to HP ArcSight Logger

In this example the log information is sent directly to the HP ArcSight Logger. Some network devices and systems that have not been configured to convert log data into the standard CEF format will send log data in a raw format. Information collected by the CloudSystem Enterprise applications, CSA, HP Matrix infrastructure orchestration (HPIO), Operations Orchestration, SiteScope, and UCMDB are sent to the HP ArcSight Logger in the CEF format. Log events are sent to a preconfigured receiver on the HP ArcSight Logger, the receivers are described later in this section.

Figure 2. Log Events sent to the HP ArcSight Logger



### Sending events to HP ArcSight Logger using Connectors

HP ArcSight Connectors can be installed on CloudSystem Enterprise host operating systems to collect operating system event information. This information is converted to the standard CEF format at each host by the HP ArcSight Connector. Log events are collected by the HP ArcSight Connectors and sent to a SmartMessage receiver configured on the HP ArcSight Logger.

Figure 3 below illustrates log data being sent from the CloudSystem Enterprise nodes to the UDP and SmartMessage receivers on the ArcSight Logger.

Figure 3. HP ArcSight Connectors and logging to the HP ArcSight Logger



cslfg16-10.fog.cloud.internal

### Sending events to HP ArcSight ESM using Connectors

The HP ArcSight Connectors can also send CEF formatted log data directly to the HP ArcSight ESM as shown in Figure 4 below. This is useful for monitoring high value assets by the HP ArcSight ESM. Connectors can be configured to send log data to multiple locations simultaneously, for example to both the HP ArcSight Logger and HP ArcSight ESM.

Figure 4. HP ArcSight Connectors logging directly to HP ArcSight ESM



cslfg16-10.fog.cloud.internal

The screen shot below in Figure 5 shows a UDP Receiver and a SmartMessage Receiver created in the HP ArcSight Logger to receive events. The UDP Receiver (UDP Receiver 1) will receive log4j events from the CloudSystem Enterprise applications and other devices on the network (Onboard Administrator (OA), Virtual Connect (VC), ESXi, network switches, etc.). The SmartMessage receiver (CSE-SC) will receive event log data from the HP ArcSight Connectors installed on the HP CloudSystem Enterprise host operating systems. HP ArcSight Connectors have been also configured for TippingPoint and vCenter resources in our reference implementation.

rs

🕾 🔹 🕊 ArcSight Logger 🛛 🗙 🧃	finkernet Explorer cannot dis					🏠 • 🖬 • 🗆 🖶	• Page •	Safety •	Tools +
🛠 Summary Analyz	e Dashboards Reports Configuration Sys	em Admin	admin	Help	? About	😳 Options	🗢 Lo	ogout	
Devices	Receivers Source Types Parsers								
Event Archives Storage	Add								
Event Input	Name	Туре		IP Addres	s	Port			
Event Output	Apache URL Access Error Log	Folder Follower Receiver					1	×	0
Alerts	Var Log Messages	Folder Follower Receiver					1	×	0
Scheduled Tasks	CSE-SC	SmartMessage Receiver					1	ж	~
Saved Search	UDP Receiver 1	UDP Receiver		All		514	1	×	*
Search									

### Devices

3

As systems connect to the HP ArcSight Logger, either through the UDP receiver or the SmartMessage receiver, they will automatically be registered and displayed in the Devices section of the HP ArcSight Logger Configuration interface.

Figure 6. Devices registered with the ArcSight Logger

Summary Analyze	Dashboards Reports Configuration System Admin			admin 🛛 🛛 Hel	p 🛛 About 🔹 Options	🗢 Logo	out
evices vent Archives torage	Add						
vent Input	Name	IP Address	Receiver	Creator	Last Editor		
vent Output lerts	CSA31	192.168.156.23	UDP Receiver 1	admin	admin admin	1	×
cheduled Tasks ilters	ESXII	192.168.156.2	UDP Receiver 1	admin	admin	- <u>2</u>	x
aved Search	ESXi2 fog.fog.cloud.internal [CSE-SC]	192.168.156.3 192.168.156.1	UDP Receiver 1 CSE-SC	admin System	admin		×
earch eer Loggers	icb1.fog.cloud.internal [UDP Receiver 1] Logger Internal Event Device	192.168.156.247 127.0.0.1	UDP Receiver 1 Not Applicable	System	System	1	×
onfiguration Backup	MOE	192.168.156.1	UDP Receiver 1	admin	admin	1	×
ystem Maintenance icense Information	oa1.fog.cloud.internal [UDP Receiver 1] oo.fog.cloud.internal [CSE-SC]	Inductinternal [UDP Receiver 1]         192.168.156.229         UDP Receiver 1         System           uud.internal [CSE-SC]         192.168.156.23         CSE-SC         System					××
etrieve Logs ontent Import	ora.fog.cloud.internal [CSE-SC] sa.fog.cloud.internal [UDP Receiver 1]	ra.fog.cloud.internal [CSE-SC] 192.168.156.21 CSE-SC a fog.cloud.internal [UDB Receiver 1] 192.168.156.22 UDB Receiver 1				/	x
	sis.fog.cloud.internal [CSE-SC]	192.168.156.24	CSE-SC	CSE-SC System		2	×
	sis.fog.cloud.internal [UDP Receiver 1] ucm.fog.cloud.internal [CSE-SC]	192.168.156.24 192.168.156.20	UDP Receiver 1 CSE-SC	System System			x
	ucm.fog.cloud.internal [UDP Receiver 1] vcenter.fog.cloud.internal [CSE-SC]	192.168.156.20 192.168.156.4	UDP Receiver 1 CSE-SC	System System		/	××

### **Grouping devices**

Device Groups can be created in the HP ArcSight Logger. In Figure 7 below, we have created a device group named CSE. This device group contains the systems running HP ArcSight Connectors and applications with logging enabled as devices from our CloudSystem Enterprise core components, CSA, Matrix Operating Environment, SiteScope, UCMDB, Operations Orchestration and vCenter.

Figure 7. Creating a Device Group

ArcSight	er	EPS In	EPS Out	CPU	EPS In: 2 EPS Out: 0 CPU Load: 1%	<ul> <li>Help</li> <li>About</li> <li>Options</li> </ul>
Summary Analyze Da	ashboards Reports Configuration System Admin				admin	🔿 Logout
Devices Event Archives Storage Event Input Event Output Alerts Scheduled Tasks Filters Saved Search Search Peer Loggers Configuration Backup System Maintenance License Information	Device         Group           You may assign one or more devices to a device group.           If you wish to add a device which is not yet created, you must first go to the Device Group           To select or deselect devices, ctrl-click each device name.           Name         CSE           Devices         CSA31           fog.fog.doud.internal [CSE-SC]         Sis fog.cloud.internal [CSE-SC]           sis fog.cloud.internal [CDP Receiver 1]         Sis fog.cloud.internal [CDP Receiver 1]	evices page and cre	atə it.			
Content Import	ucm fög cloud internal [UDP Rečeiver 1] vænter fög cloud internal [CSE-SC] Use ctrl-click to select or deselect items	<b>v</b>			Save	ancel

### Forwarding events to HP ArcSight ESM

The HP ArcSight Logger can be used to aggregate events and forward specific events to an HP ArcSight ESM system for further analysis and correlation.

To accomplish this, forwarders are created in the HP ArcSight Logger > Configuration > Event Output interface. The forwarders are configured to send log data to an ESM Destination. The ESM Destination is displayed below in Figure 8; the forwarder configured here will show up as a connector in the ArcSight ESM Console. In our example we have named this connector Logger2ESM to represent events being forwarded from the HP ArcSight Logger to the HP ArcSight ESM.

#### Figure 8. Event Forwarding to an ESM Destination

ArcSight Logger				EPS In	EPS Out CPU EPS EPS CPU L	S In: 3 Out: 0 .oad: 1%	Help About Options	۵
Summary Analyze Day	shboards Reports	Configuration System Admin			a	dmin 🧲	Logout	
Devices Event Archives Storage	Forwarders ESM Desti	nations Certificates						
Event Input	Name	IP/Host	Port	Connector Name	Connector Location	Logger Lo	cation	
Alerte	Logger2ESM	arcmgr.fog.cloud.internal	8443	Logger2ESM	/All Connectors/Houston	Houston		×
Scheduled Tasks Filters Saved Search Search Configuration Backup System Maintenance License Information Retrieve Logs Content Import		Ν						

Once the connector is created it can be used by event Forwarders to forward specific events to the HP ArcSight ESM. In the example below we have created a forwarder based on a regular expression query that will forward all failed login attempts that are captured by the ArcSight Logger.

ArcSight Log	ger			EPS In	EPS Out	CPU	EPS In: 5 EPS Out: 0 CPU Load: 2%
Summary Analyze	Dashboards Rep	oorts Configuratio	n System Admin				admin
Devices	Forwarders	ESM Destinations (	Certificates				
Event Archives Storage	Edit Forwa	irder					
Storinge Event Input Event Output Alerts Scheduled Tasks Filters Saved Search Search Peer Loggers Configuration Backup System Maintenance License Information Retrieve Logs Content Import		Name Query Filters	Windows Logon failures         I cef:0.*categoryBehavior=/Authentication/Verify         I categoryOutcome=/Failure         CSE         Configuration - System Configuration Changes (CEF         Events - CEF         Events - CEF         Logins - All Logins (CEF format)         Logins - All Logins (CEF format)         Logins - Successful Logins (CEF format)         Logins - Unsuccessful Logins (CEF format)	r			
			Filter by time range				
	Conne	ection Retry Timeout	5				
		ESM Destination	Logger2ESM	-			

This forwarder has a query defined where the criteria states that if authentication is verified and the outcome is failure, send all events that match this query to the ArcSight ESM.

Save Cancel

We can also forward events from specific devices or device groups. In our example in Figure 10, we have created a forwarder based on a device group named CSE and a forwarder named CSE Application Events. All events from systems that are part of the device group CSE will be forwarded to the HP ArcSight ESM.

Figure 10. Event Forwarding based on a Device Group

ArcSight Logger				EPS In	EPS Out	CPU	EPS In: 3 EPS Out: 0 CPU Load: 1%	<ul> <li>Help</li> <li>About</li> <li>Options</li> </ul>	
Summary Analyze Da	shboards F	Reports Config	uration System Admin				admin	🗢 Logout	
Devices Event Archives Storage Event Input Event Output Alerts Scheduled Tasks Filters Saved Search Search Peer Loggers Configuration Backup System Naintenance License Information	Forwarders Add Forwa	ESM Destinations arder Name Type Filter Type	Cettficates CSE Events ArcSight ESM (CEF) Forwarder		Next	Cancel			
Content Import									

Below in Figure 11, you can see the two forwarders that were created: CSE Application Events and Windows Logon Failures.

	er			EPS In EPS Out	CPU EPS In: 3 EPS Out: 0 CPU Load: 1%	<ul> <li>Help</li> <li>About</li> <li>Options</li> </ul>					
Summary Analyze Da	ashboards Reports (	Configuration System	n Admin					🔿 Logout			
Devices Event Archives Storage Event Input	Forwarders ESM De Filter by Type All Add	stinations Certificates									
Alerts	Name	Туре	Filter Type	IP/Host	Port	Query					
Scheduled Tasks	CSE Application Events	ArcSight ESM (CEF) Forwarder	🛐 Unified Query			_deviceGroup IN ["CSE"]		1	×	*	11
Filters Saved Search	Windows Logon failures	ArcSight ESM (CEF) Forwarder	Expression			cef:0.*categoryBehavior=/Authe categoryOutcome=/Failure	entication/Verify :AND:	2	ж	*	
Search Deer Loggers											

#### Figure 11. Event Forwarders

# Protecting HP CloudSystem Enterprise components with HP ArcSight

Configuring HP ArcSight to protect HP CloudSystem Enterprise core components involves configuring these component applications to send security information and events from each application to the HP ArcSight ESM or HP ArcSight Logger. In this section we will explain how to configure each CloudSystem Enterprise core component. This includes collecting information from the operating system and application log files. This information can be collected using standard syslog and event log collection or through the use of HP ArcSight Connectors for more detailed application and operating system specific event logging.

To collect operating system events we will leverage the HP ArcSight Connectors. The HP ArcSight Connectors will be installed on each host running the HP CloudSystem Enterprise applications. These applications include:

- CloudSystem Matrix Central Management Server
- Cloud Service Automation
- Operations Orchestration
- Cloud Service Automation Database server
- SiteScope
- Universal Configuration Management Database Server (UCMDB)

Cloud Service Automation and Operations Orchestration are hosted on the same Microsoft Windows<sup>®</sup> Server 2008 R2 server.

Operating system event logs are directed to the HP ArcSight logger through HP ArcSight Connectors that are specific for each host operating system.

### **Cloud Service Automation 3.1**

Monitoring of events that occur in the core applications that comprise HP CloudSystem Enterprise: CSA, OO, HPIO, UCMDB, and SiteScope, is thoroughly documented in the Cloud Service Automation 3.1 documentation, <u>HP Cloud Service Automation</u> <u>3.10 Integration with ArcSight Logger</u> document ID KM00231339. Access to this document requires an HP Passport account. This document contains detailed instructions on configuring the application event logging to an ArcSight logger. The instructions describe how to configure application event logging in Common Event Format (CEF) for the following applications:

- Cloud Server Automation
- Operations Orchestration RAS
- Operations Orchestration
- SiteScope
- UCMDB
- HPIO

The procedures described in the Integration with ArcSight Logger document involve:

- Editing the log4j.properties file for each application to support CEF logging
- Editing the log4j.properties file for each application to define the IP Address or host name of the HP ArcSight Logger
- Copying the arcsight-cef-library-1.0.0.release.8.jar file to the lib directory of each application. This file is included in the HP Cloud Service Automation 3.1 software distribution.

Below is an example of the modifications made to the log4j.properties file for Operations Orchestration.

```
log4j.appender.cef1=com.hp.esp.arcsight.cef.appender.Log4jAppender
log4j.appender.cef1.deviceVendor=HP
log4j.appender.cef1.deviceProduct=CSA
log4j.appender.cef1.deviceVersion=3.1
log4j.appender.cef1.transportType=SYSLOG
log4j.appender.cef1.hostName=192.x.x.x
log4j.appender.cef1.port=514
log4j.appender.cef1.layout=org.apache.log4j.PatternLayout
log4j.appender.cef1.layout.ConversionPattern=%d [%t] (%F:%L) %-5p - %m%n
log4j.appender.cef1.useCefHeader=true
log4j.appender.cef1.eventName=00 Event
```

Notice the line log4j.appender.cef1.eventName=00 Event, this will allow us to search the logger for all events with an event name of 00 Event. Each of the core products also contains the line log4j.appender.cef1.deviceProduct=CSA, this is another way to search all events that are related to the core products, CSA, 00, HPIO, SiteScope, and UCMDB. This is discussed in detail later in the section titled <u>Working with events</u>.

Once the applications have been configured for ArcSight integration, install the HP ArcSight Connector for each host operating system to capture operating system log and event data. Follow the procedures described in the ArcSight documentation: *User's Guide HP ArcSight SmartConnectors*. Install the HP ArcSight Connector for Windows on each of the operating systems that host the CloudSystem Enterprise core applications. In our example we have the following Windows 2008 R2 hosts:

- 00.fog.cloud.internal Operation Orchestration and Cloud Service Automation
- Ora.fog.cloud.internal Oracle Database Server for UCMDB
- Fog.fog.cloud.internal Matrix Operating Environment Central Management Server
- Sis.fog.cloud.internal SiteScope
- UCM.fog.cloud.internal UCMDB server.
- vCenter.fog.cloud.internal VMware vCenter

The events captured from the log4j application logs will be sent to the HP ArcSight Logger and then select events can be configured and forwarded to the HP ArcSight ESM manager via the Logger2ESM connector described earlier. The "log4j.appender.cef1.hostName=192.x.x.x" line in the log4j.properties file specifies the HP ArcSight Logger IP Address. A corresponding UDP receiver (UDP Receiver 1) was created on the HP ArcSight Logger to receive the events that are sent from each application.

### **Matrix Operating Environment**

HPIO events have been configured for logging through the procedures described in the Integration with ArcSight document and operating system events are captured by the HP ArcSight Connector. This next section will describe how to configure logging for the c7000 Onboard Administrator and HP Virtual Connect.

#### HP BLc7000 Onboard Administrator

To enable a HP BLc7000 Onboard Administrator (OA) to be monitored and viewed in HP ArcSight Logger and ESM, you need to point the internal system log of the OA to the HP ArcSight Logger. To complete this action, perform the following:

- Active Onboard Administrator -> System Log -> Log Options
  - Select "Enable remote system logging"
  - Syslog Server Address: <IP of your HP ArcSight Logger>
  - Port: <Port of Logger's UDP Receiver (default: 514)>

#### Figure 12. Onboard Administrator Logging

System Status 📃	Wizards 👻 Options 👻 Help 👻								
View Legend Updated Mon Jan 14 2013, 10:08:01	Active Onboard Administrator								
System Status 0 0 0 4 0									
Systems and Devices									
Rack Overview Rack Firmware         Primary: SGH208PHBK         Enclosure Information         Enclosure Settings         Active Onboard Administrator TCP/IP Settings Certificate Administration Firmware Update         System Log         Standby Onboard Administrator	Syslog Server Address: 192.168.156.90 Port: 514 Test Remote Log Apply								

- Select "Apply" to apply the settings.
- Once the screen refreshes, you can select "Test Remote Log". By doing so, a test message is sent to the Logger. If
  everything is working, you should see the IP or the host name of the HP Onboard Administrator registered in HP ArcSight
  Logger in the "Configuration -> Devices" page (Figure 6).

### **HP Virtual Connect**

To enable HP Virtual Connect (VC) to be monitored and viewed in HP ArcSight Logger and HP ArcSight ESM, you need to point the internal system log of the VC to the HP ArcSight Logger. To complete this action, perform the following:

- Log into the HP Matrix Operating Environment Portal and navigate to "Tools -> Integrated Consoles -> Virtual Connect Enterprise Manager (VCEM)..."
- Select the VC domain to be monitored by HP ArcSight from either the "VC Domain Groups" or "VC Domains" tab and select "VC Domain Maintenance..." (Figure 13)

Figure 13. Virtual Connect Domain Maintenance Mode

Tools 🔻	Deploy 🔻	Configure 🔻	Diagnose 🔻	Optimize 🔻	Reports 🛪	· Tasks & l	.ogs 👻 Optic	ons 🔻 Help 🔻	
Virtua Manage Mu	I Conne uttiple VC Dom	ct Enterpris ains	se Manag	ger (VCE	EM)				Maximize <b>?</b>
Ho	ome	VC Domain Gro	ups VC	Domains	Server Pro	files	Bays	Jobs	
Filter: All	1	[No data av	ailable] 💌	Filter					
Legend:	⊘ Managed by VCEM	S Fail to communicate with VC Domain / Disabled enclosure	W Missing ex manager lock Communicatio established w disabled enclo	ternal / (i) n Lice /ith osure	ensed License	(2) ⊴ Configurat mismatch	ion 🛕 Under maintenan	x Incompatible ce firmware	الله Firmware update
Note: For	r more details :	about the VC Domai	n, click on the V	/C Domain Nam	e				
	VCEM Status	s VC Dom	ain Name	VC Man	ager	Enclosure		VC Domain Gro	pup
	0	CloudEnc	losure29	192.168.1	156.247	i SGH20	8PHBK	CloudLab23	
		Re	move from V(	C Domain Gro	up VC D icense	omain Mainte New VC Dom	nance VC ain Group	Domain Firmwar Add to VC Doma	e Update in Group

- Type "YES" without the quotation marks when prompted with the Warning IMPORTANT: VCEM has detected you may be using other products.... and select "OK".
- Scroll down on the page and select the button that says "*Make Changes via VC Manager...*" a new window will open up and you will now need to log into the HP Virtual Connect Manager (VCM) interface.
- Once logged in, select "OK" on the informational dialog stating "VC Domain under maintenance by Virtual Connect Enterprise Manager..."
- Select "System Log" on the left Navigation bar and select the "Configuration" tab.
- Select "Define Target" and fill in the following information
  - Log Host: <IP of your HP ArcSight Logger>
  - Log Severity: <Select the entry appropriate to your needs>
  - Transport: <UDP or TCP, depending on how you defined your UDP/TCP Receiver>
  - Port: <Port of you UDP/TCP Receiver>
  - Date Format: RFC 3164
  - Enabled: Yes
- Select "Apply" and you should have a screen similar to Figure 14

Figure 14. Enabling Virtual Connect Remote System Logging

Define 🔻	Configure 👻 Tool	s 🔻 Help 🔻						
System Log								
System	Log Configuratio	n						
	Log host	Log Severity	Transport	Port	Security	Date Format	Enabled	Test
	192.168.156.90	info	udp	514	none	rfc3164	true	
						Nefine Terget	Relata	
					_	benne rarget	Delete	

- Select "Test". By doing so, a test message is sent to the Logger. If everything is working, you should see the IP or the host name of the HP Virtual Connect Manager registered in HP ArcSight Logger in the "Configuration -> Devices" page (Figure 6)
- Once you have validated that your VCM is communicating properly with HP ArcSight Logger, sign out and close the VCM window.
- Back on the VCEM window, select the "Complete VC Domain Maintenance" button on the bottom of the screen.

### **Server Automation**

The Linux host running Server Automation is configured to send syslog log events in raw format to the ArcSight Logger. To accomplish this, edit the */etc/syslog.conf* file and add the following line to the end of the file:

\*.\* @192.x.x.x

In the example above 192.x.x.x should be replaced with the IP Address of your ArcSight Logger. Restart the syslog daemon and log events will be sent in raw format to the HP ArcSight Logger.

### VMware ESXi 5 Host

To configure a VMware ESXi Host to be monitored and viewed in HP ArcSight Logger and HP ArcSight ESM, or to a syslog server with the appropriate HP ArcSight Connector installed to talk to an HP ArcSight ESM, you need to point the internal system log of the host to the HP ArcSight Logger or external syslog server. To complete this action, perform the following steps:

- Log into the host or the VMware vSphere Server using the VMware vSphere Client
  - If connecting to a VMware vSphere Server, navigate to the Host and Clusters view by selecting "Home > Inventory > Host and Clusters" from the View menu.
  - If connecting directly to the host using the VMware vSphere Client, navigate to the Inventory view by selecting "Home > Inventory > Inventory" from the View menu.
- Select the host in the left navigation bar and select the Configuration tab.
- In the software group box, select "Advanced Settings".
- In the left navigation tree in the Advanced Settings window select "Syslog > global".
- Set the "Syslog.global.logHost" variable to point to your HP ArcSight Logger or external syslog server with the appropriate HP ArcSight Smart Connector installed. (Figure 15)
  - Example: udp://192.168.156.90:514

Figure 15. Setting the ESXi Syslog.global.logHost variable

2 192.168.156.3 - vSphere Client					
File Edit View Inventory Administr	ration Plug-ins Help				
💽 💽 🏠 Home 🕨 🛃 Inv	ventory 🕨 🎁 Inventory				
at et					
192.166.156.3	essi-2.fog.cloud.internal VMware ESX, f Getting Started Summary Virtual Mach Health Status Processors Memory Storage Networking Storage Adapters Network Adapters Advanced Settings Power Management Software Licensed Features Time Configuration DVS and Routing Authentication Services Virtual Machine Startup/Shutdown Virtual Machine Swapfie Location Security Profile Host Cache Configuration System Resource Allocation Agent VM Settings Advanced Settings	S.O.O, 702118 ins: Resource Allocation Per Annotations BufferCache - GBRC ⊕ Config - COW - CAW - Digest - DirentryCache - Digest - DirentryCache - Digest - DirentryCache - Digest - PorentryCache - Digest - PorentryCache - Digest - PorentryCache - Digest - PorentryCache - Digest - D	Formance         Configuration         Local Lisers & Groups         Events         Permiss           Syslog.global.defaultRotate         Default number of rotated logs to keep. Reset to default on zero.         Min:         0         Max:         100           Syslog.global.defaultSize         Default size of logs before rotation, in KiB. Reset to default on zero.         Min:         0         Max:         102           Default size of logs before rotation, in KiB. Reset to default on zero.         Min:         0         Max:         10240           Syslog.global.logDir         Detastore path of directory to output logs to. Reset to default on null         Syslog.global.logDir         Detastore path of directory of logdir, based on hostname.         Syslog.global.logPirUnique           Place logs in a unique subdirectory of logdir, based on hostname.         Syslog.global.logHost         The remote host to output logs to. Reset to default on null. Multiple for the remote host to output logs to.	In Example: [detastoreName]/logdr	
		ugebul ⊕- loggers User			
		VMF53	1		
			ОК	Cancel Help	

- Select "OK".
- Select "Security Profile" under the "Software" group box
  - To the right of "Firewall" select "Properties"

Figure 16. ESXi Firewall Select "Properties" to the right of "Firewall"

🛃 192.168.156.3 - vSphere Client						_ 🗆 ×
Eile Edit View Inventory Administra	ation Plug-ins Help					
💽 💽 🏠 Home 🕨 🛃 Inv	ventory 🕨 🛐 Inventory					
	esxi-2.fog.cloud.internal ¥Mware ESXi,	, 5.0.0, 702118				
	Getting Started Summary Virtual Mac	hines Resource Allocation Performat	nce Configuration Local L	Isers & Groups Events Permission	ns	
	Hardware	Security Profile				-
	Health Status	Services			Refresh	Properties
	Processors	I/O Redirector (Active Directory Sectors)	ervice)			
	Memory	Network Login Server (Active Dire	ctory Service)			
	Storage	vSphere High Availability Agent				
	Networking	vpxa				
	Storage Adapters	ESXi Shell				
	Network Adapters	Local Security Authentication Serv	er (Active Directory Service)			
	Advanced Settings	SSH				
	Power Management	Direct Console UI				
	Software	CIM Server				
	Joint de	Firewall			Refresh	Properties
	Licensed Features	Incoming Connections	80 (TCP)	All		
	Time Configuration	DNS Client	53 (UDP)	All		
	DNS and Routing	DHCP Client	68 (UDP)	All		
	Authentication Services	CIM Secure Server	5989 (TCP)	All		
	Virtual Machine Scarcup/Shutdown	CIM Server	5988 (TCP) 8000 (TCP)	All		
	Virtual Machine Swapnie Location	vSphere Client	902.443 (TCP)	All		
	Security Profile	CIM SLP	427 (UDP, TCP)	All		
	System Resource Allocation	vSphere High Availability Agent	8182 (TCP,UDP)	All		
	Agent VM Settings	NFC	902 (TCP)	All		
	Advanced Settings	SNMP Server	22 (TCP) 161 (UDP)	All		
		Eault Tolerance	8100 8200 /T/D LIND)	01		

ſ

 In the "Firewall Properties" window, scroll down the list until you see "syslog" and select the check box to enable it (Figure 17).

Figure 17. Proper selection and enablement of syslog in the ESXi firewall

ire	wall Properties						[
em	ote Access						
y de	efault, remote clients are	prevented fr	om accessing services on I	this host, and local cli	ents are prevente	d from	
cces	ssing services on remote h	hosts.					
elec	t a check box to provide -	access to a s	ervice or client. Daemons	will start automaticall	y when their ports	; are	
pen	ed and stop when all or tr	heir ports are	e closed, or as configured.				
	[ ] _k _l				Ductoreals		_
	Label		Incoming Ports	Outgoing Ports	Protocols	Daemon	-
싁	NEC		902	902	TCP	N/A	
	DHCPV6		546	547	TCP,UDP	N/A	
	DVFilter		2222		TCP	N/A	
⊻	vSphere High Availability	y Agent	8182	8182	TCP,UDP	Running	
⊻	HBR			31031,44046	TCP	N/A	
	gdbserver		1000-9999,50000-5		TCP	N/A	
~	Fault Tolerance		8100,8200	80,8100,8200	TCP,UDP	N/A	
~	syslog			514,1514	UDP,TCP	N/A	_
~	VMware vCenter Agent			902	UDP	Running	
	IKED		500	500	UDP	N/A	-
•							·
Ser	vice Properties						
Gei	neral						
Se	ervice:	syslog					
Pa	ackage Information:						
Fire	ewall Settings						
		- 11					
AI	llowed IP Addresses:	All					
				[	Firewall	Options	1
				L		opcionaria	
				OF	Capital		lala
				OK			ieip

 Optionally, you can select the "Firewall..." button, select the "Only allow connections from the following networks" radio button, and specify your HP ArcSight Logger server or external syslog server for added security. (Figure 18)

Figure 18. Restricting outbound syslog traffic from the VMware ESXi Host to HP ArcSight Logger

🛃 Firewall Settings	×
Allowed IP Addresses	
O Allow connections from any IP address	
Only allow connections from the following networks:	
192.168.156.90	
Separate each network with a comma. Example: 192.168.0.0/24, 192.168.1.2, 2001::1/64, fd3e:29a6:0a81:e478::/64	
OK Cancel Help	

- Select "OK" on the "Firewall Settings" and/or "Firewall Properties" windows.

 It might take a few minutes for the VMware ESXi Host to send its first event to the HP ArcSight Logger, but you should see the IP or hostname of the host registered in HP ArcSight Logger in the "Configuration -> Devices" page (Figure 6). You will need to repeat these steps for all of your VMware ESXi Hosts.

#### **VMware vSphere Web Services**

The VMware vSphere Web service is a programming interface that exposes the functionality of VMware vSphere to customer-written or third party applications. The vSphere Web service is part of vSphere. It is distributed and installed along with the rest of vSphere and there is no additional cost or licensing required

With HP ArcSight SmartConnector for Windows, you are able to monitor VMware vSphere Web Services. You will first need to install the SmartConnector as described in the ArcSight documentation – *User's Guide HP ArcSight SmartConnectors*. Once you are at the "Select the connector to configure" window, close the HP ArcSight Connector Setup window and perform the following steps to complete the setup.

- You first need to obtain the certificate from VMware vSphere vCenter Server and import it so that the connector can see it. To do so, open Internet Explorer on your vCenter host and browse to your vCenter Server instance, for example <u>https://localhost</u>
  - Next to the address bar, select "Certificate Error" and select "View Certificates" (Figure 19)

Figure 19. Selection of "VMware Web Services"



- Select the "Details" tab and select "Copy to File..."
  - Select "Next >" on the Welcome screen
  - Select "Base-64 encoded X.509 (.CER)" and select "Next >"
  - Select "Browse" and save the file to a location on your local disk and select "Next >"
  - Select "Finish"
- Now open a command window. If you are not logged in as Administrator you will need to run the command window with "Run as administrator". If you do not "Run as administrator" you may get access denied messages when importing the certificate.
  - Start -> All Programs -> Accessories -> (Right Click) Command Prompt -> Select "Run as administrator"
- Change directory to the %ARCSIGHTSMARTCONNECTORS\_HOME%\current\bin
  - By default that is C:\Program Files (x86)\ArcSightSmartConnectors\current\bin
- Run the following command, setting the parameter after "-file" with the location of your saved certificate.

```
C:\Program Files (x86)\ArcSightSmartConnectors\current\bin>arcsight agent
keytool -import -trustcacerts -alias vmware -file c:\vcenter-cert.cer -store
clientcerts
```

- Type "yes" when asked "Trust this certificate?"
- Rerun the connector setup by entering in that same command prompt window "runagentsetup"
- Select "Add a Connector"
- Select "VMware Web Services" as the connector "Type" (Figure 20 and select "Next >"

Figure 20. Selection of "VMware Web Services" Connector

Connector Setup		_ 🗆 🗙
Configure	Select the connector to configure	
	Type VMware Web Services	
····		
ArcSight		
	< Previous Ca	ncel

- Select "true" for the "ValidateCert" option, then select "Next >"
- Select "Add" on the "Enter the device details" window and enter the following:
  - Host Host name or IP address of the VMware Web Services device.
  - User User name for accessing VMware Web Services. It is strongly recommended for security reasons to use or create a user in vCenter that only has Read-Only permissions to what you want monitored. You could grant that user permissions to the entire vSphere Server instance, or just particular Data Centers, Clusters, Host, VMs, etc.
  - Password Password for the VMware Web Services user.
  - Select "Next >"

Connector Setup			
Configure	Enter the device details		
	Host	User	Password
	localhost	lfoa domain\ReadOnlvUser	*****
1°0,et			
· · ·			
du under			
Archabt			
Arcsignis	Add	Remove Import	Export
- As in cariping			
		< Previous	Next > Cancel

Figure 21. Example of completed Connector VMware Web Services device details

- NOTE: If you get an information dialog box stating the Connector table parameters did not pass the verification with error[0:Unable to open a connection to[localhost]], then your certificate was not imported correctly or was the wrong certificate. You need to re-run the keytool and possibly export the certificate again to rectify the issue before continuing.
- On the "Enter the type of destination" select "ArcSight Manager (encrypted)"
- From this point on, refer to the ArcSight documentation *User's Guide HP ArcSight SmartConnectors* for completion of the Connector installation.
- Upon completion of the installation, ensure the service is started, and you should see the Connector registered in the HP ArcSight ESM Console.

### Networking

### HP 58x0 and 59x0 Series Switching

To enable the HP 58x0 and 59x0 Series Switches to be monitored and viewed in HP ArcSight Logger and HP ArcSight ESM, you need to point the internal system log of the switch to the HP ArcSight Logger. To complete this action, perform the following steps:

• Log into the switch and enter system view

```
    Enter in the following commands
        <switch> system-view
        [switch] info-center loghost 192.168.156.90 port 514
        [switch] info-center enable
        [switch] save
```

• Upon completion of the save command, you should see the IP or hostname of the switch registered in HP ArcSight Logger in the "Configuration -> Devices" page (Figure 6).

### HP TippingPoint Security Management System (SMS) Appliance

The TippingPoint product has two types of devices, sensors and SMS devices, that act as the management console and central logging point. The SMS provides a separate syslog output format option that works with third-party network security devices and host applications. ArcSight currently supports only events sent to the Connector from the SMS console, not the events sent directly to the Connector from the sensor devices, as the two devices log in slightly different formats.

To enable the HP TippingPoint Security Management System (SMS) Appliance to be monitored and viewed in HP ArcSight ESM, you need to point the internal system log of the SMS to the HP ArcSight ESM. The HP ArcSight Connector cannot be installed directly on the SMS system, another system (Linux or Windows) will need to be leveraged to point the SMS to, and that system will require the Connector to be installed to talk to the HP ArcSight ESM or HP ArcSight Logger. To complete this action, perform the following steps:

With the HP ArcSight Connector for Windows, you are able to monitor TippingPoint SMS syslog information. You will first
need to install the HP ArcSight Connector as described in the ArcSight documentation – User's Guide HP ArcSight
SmartConnectors. Once you are at the "Select the connector to configure" window select "TippingPoint SMS Syslog
Extended" (Figure 22). Select "Next >"

🛠 Connector Setup		
Configure	Select the connector to configure	
	Type         TippingPoint SMS Syslog Extended	
······································		
•••••••••••••		
ArcSight		
	< Previous Next > Ca	ancel

Figure 22. Selecting the "TippingPoint SMS Syslog Extended" Connector

• On the "Enter the connector details" window, fill in the appropriate information for your environment. You do not need to specify a username and password. Select "Next >"

- Select "Add" on the "Enter the device details" window and enter the following:
  - Host Host name or IP address of the HP TippingPoint SMS
  - User User name for accessing HP TippingPoint SMS. It is strongly recommended for security reasons to use or create a user in HP TippingPoint SMS that only has Read-Only permissions to what you want monitored. You could grant that user permissions to the entire HP TippingPoint SMS or just particular devices, segment groups, profiles, etc.
  - Password Password for the HP TippingPoint SMS user
  - Select "Next >"

Figure 23. TippingPoint SMS Syslog Extended Connector device details

≮ Connector Setup			
Configure	Enter the device details		
	Hostname/IP	Username	Password
	192.168.156.200	lesmuserl	****
100 m			
1			
ArcSight	bba	Remove Import	Export
Company	had	inport	Eddan a
		< Previous	Next > Cancel

- On the "Enter the type of destination" select "ArcSight Manager (encrypted)"
- From this point on, refer to the ArcSight documentation, *User's Guide HP ArcSight SmartConnectors*, to complete the SmartConnector installation

- Log into the HP TippingPoint SMS and navigate to "Admin > Server Properties > Syslog"
  - Select the "New..." button and fill in the information for the system you just installed the HP TippingPoint SMS connector on. You can set up multiple Facilities and Severity levels as needed for your configuration. An example is given in Figure 24.

Figure 24. TippingPoint Remote Syslog Setting Window

🎯 Create Ren	note Syslog Notification Settings
Create Rem Set up th	note Syslog Notification Settings e sending of events to a remote syslog server. more
🔽 Enable	
Syslog Server:	192.168.156.200
Protocol:	UDP C TCP C Encrypted TCP
Certificate	e
Subject DN	d:
Valid After	1 Import
Expires:	
Port:	514
Log Type:	ArcSight CEF Format
Event Query:	All Eve
Facility:	Security/Authorization
Severity:	Informational
Delimiter:	TAB
Include Tim	estamp in Header
O None	
C SMS curr	ent time
Event time	estamp
Include SM	IS Hostname in Header
Send New	Events/Log Only
	OK Cancel

• Upon completion of the installation, use the Windows Services applet to ensure the HP Connector service is started. Once started you should see the Connector registered in HP ArcSight ESM.

# **Protecting CloudSystem Enterprise Services with HP ArcSight**

In addition to protecting the HP CloudSystem Enterprise core components that are responsible for supply and delivery of cloud services, the cloud services should also be protected upon provisioning. In this section we will demonstrate how to integrate the HP ArcSight Connector installation and configuration to dynamically connect to the HP ArcSight ESM and HP ArcSight Logger.

### **HP LAMP solution**

The <u>HP LAMP and WordPress Reference Implementation for CloudSystem Enterprise</u> can be enhanced to include ArcSight Connector for the deployed physical or virtual machines. HP ArcSight Connector for Linux can be automatically deployed using Server Automation policies.

Create the Server Automation software policy ArcSightSecurityPackages. Figure 25 shows the required Linux packages that were needed to deploy the ArcSight Smart connector on a Red Hat Enterprise Linux 6.3 virtual machine.



Software Policy: ArcSightSecu	rityPackages	
Views	🇞 Policy Items	
Properties	💠 🗕   🛧 🦊   🗷 🔳 🔁 🔁   Re <u>s</u> olve Dependencies   📁	Q.
Custom Attributes	Name	Location
Policy Usage     Sequence Usage     Application Usage     Server Usage	1.         Image: Control (Control (Contro) (Contro) (Control (Contro) (Control (Contro) (Control (Contro)	Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Ser  Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Ser  Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Ser  Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Ser  Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Ser  Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Ser  Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Ser  Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Ser  Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Ser  Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Ser  Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Ser
	<ol> <li>How Ibxcb-1.5-1.el6.i686</li> <li>ArcSight-5.2.7.6474.0-Connector-Linux-props.zip (/tmp)</li> </ol>	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Ser /Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Ser
0 items		hpsa_admin Fri Jan 25 20:41 2013 Etc/UCT

The ArcSight zip file shown in the figure above was created by zipping up the Linux smart connector .bin file and the properties file used for silent installation. The contents of the zip file are shown in Figure 26.

Figure	26.	Package	Contents
--------	-----	---------	----------

SPackage: ArcSight-5.2.7.6474.0-Cor	nnector-Linux-props.zip	_ 🗆 🗵
File Edit View Actions Help		
Views	Solution Contents	
Properties	Files Scripts	
Software Policy Usage	ASLinuxAudit.props ArcSight-5.2.7.6474.0-Connector-Linux.bin	
Server Usage		
	hpsa_admin Fri Jan 25 21:13 20	13 Etc/UCT

The zip file is then imported into Server Automation. Add a Post-Install script as seen in Figure 27 to run the silent installer and start the service after deployment.

#### Figure 27. Policy Properties

Package: Arc5ight-5.2.7.6474.0-Connector-Linux-props	s.zip
File Edit View Actions Help	
Views 📕 Propertie	S
Properties General	* ×
Vame:	ArcSight-5.2.7.6474.0-Connector-Linux-props.zip
Software Policy Usage Description:	
Application Usage	
Type:	ZIP Archive
O5:	Red Hat Enterprise Linux Server 6 X86_64
Location:	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 6 X86_64 Select
Default Install Pat	th: Jtmp
Last Modified:	Thu Jan 24 21:40:17 2013
Last Modified By:	hpsa_admin
Created:	Wed Jan 23 22:56:44 2013
Created By:	hpsa_admin
File Name:	ArcSight-5.2.7.6474.0-Connector-Linux-props.zip
File Version:	
File Size:	179.93 MB
Checksum:	578da8aaf1033dc7b6501fb2e12b2e59461ce169
Object ID:	81990001
Archived Script	s 😵
Install Parame	v V
Install Scripts	*
Pre-Install Scrip	Post-Install Script
cd /tmp chmod +× Arc5 ./Arc5ight-5.2. service arc_lini	Sight*i,bin 7.6474.0-Connector-Linux.bin -i silent -f /tmp/ASLinuxAudit.props .x_auditd start
12	hpsa_admin Fri Jan 25 20:47 2013 Etc/UC

The response file ASLinuxAudit.props was created by manually deploying the ArcSight Smart connector for Linux and issuing the command **runagentsetup.sh**—**i** recorderui and specifying a response file name. The complete response file is found in <u>Appendix A</u>.

The LAMP + WordPress reference implementation defines two Server Automation policies to deploy the required packages to the database and web servers. The Server Automation policies defined are ApacheWordPress-RHEL6 and MariaDB-RHEL6. These policies are modified to include deployment of the ArcSightSecurityPackages policy as seen in Figure 28.

#### Figure 28. Policy Items

ws	🍫 Policy Items	
Properties	💠 🖛   🛧 🦊   🖩 🖷 🕀 🐂   Resolve Dependencies   💋	1
Policy Items		Q-
Custom Attributes	Name	Location
History	1. Syget_rmt_srvr_ip.zip (/tmp)	, Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 6 X86
Policy Usage	2 🧐 epel-release-6-8.noarch	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 5 X86
OS Sequence Usage	3 🧐 apr-1.3.9-3.el6_1.2.x86_64	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 6 X86
Application Usage	4. 🧠 🧐 apr-util-1.3.9-3.el6_0.1.x86_64	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 6 X86
Server Usage	5. i 🧐 apr-util-ldap-1.3.9-3.el6_0.1.x86_64	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 6 X86
	6. i 😌 libtool-ltdl-2.2.6-15.5.el6.x86_64	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 5 X86
	7 😌 httpd-tools-2.2.23-1.el6.x86_64	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 6 X86
	8 🧐 httpd-2.2.23-1.el6.x86_64	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 6 X86
	9 🧐 php-5.3.3-3.el6_2.8.x86_64	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 6 X86
	10 🧐 php-cli-5.3.3-3.el6_2.8.x86_64	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 6 X86
	11 🧐 php-common-5.3.3-3.el6_2.8.x86_64	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 5 X86
	12 🧐 php-Idap-5.3.3-3.el6_2.8.x86_64	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 6 X86
	13 🧐 php-mysql-5.3.3-3.el6_2.8.x86_64	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 6 X86
	14 🧐 php-pdo-5.3.3-3.el6_2.8.x86_64	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 5 X86
	15. ig wordpress-3.5.zip (/usr/local/wordpress)	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 6 X86
	16. 🥰 OPSWagent_tools_unix-45.0.19256.0.zip (/opt/opswa	re/agent_tools) /Opsware/Tools/Python Opsware API Access
	17. 🗄 💜 ArcSightSecurityPackages	/Package Repository/All Red Hat Linux/Red Hat Enterprise Linux Server 6 X86

Including the ArcSightSecurityPackages policy into the MariaDB-RHEL6 and ApacheWordPress-RHEL6 policies will automatically deploy the ArcSight Smart Connector for Linux audit logger to the database and web servers and start logging events to ArcSight Logger. The linux\_auditd events are visible from the summary page of the ArcSight Logger under Agent Type and the nodes will be displayed in the Configuration > Devices section of the HP ArcSight Logger.

# **Working with events**

### Searching the HP ArcSight Logger

Figure 29. Logger MOEevent

					EPS In	EPS Out	CPU	EPS In: 3 EPS Out: 0 CPU Load: 2%	<ul> <li>Help</li> <li>About</li> <li>Options</li> </ul>	
Summary Analyze Dashboar	ds Rep	orts Configuration Syste	m Admin					admin	🔿 Logout	
💕 🛃 🗙 🔆 🔽 Fiel	ld Summar	y 🗌 Discover Fields 🛛 Last 12	hours							
Search: MOEevent							₩ Go	o!		
Advanced Search										
Figure All Fields	<b>a</b> 🖻	Auto Lindato: 5 min 💌		<b>2.783</b>	227.978	00:01.069	Export Resi	ults		
Fields: All Fields		Mato opdate.		2//00	Q 221/5/10	0 001011005	Enportread	arcarri		
									1 bar = 1	0 minute 🔺 📖
Field Summary (5)	. K. E	vents								
Sort By Name		Page1 of 28	Show RAW	L All None						
	•	i ugo i orzo i i	- 010111011	. All NUTE			Disp	aying 1 - 100 of 27	83 Events per	page: 100 🗸
Selected Fields (5)	•	Time (Event Time)	Device Log	gger deviceVendor	deviceProduct	deviceVersion	Disp	name ba	83 Events per	page: 100 🗸
Selected Fields (5) deviceEventClassId	2	Time (Event Time)           24         2013/01/27 20:20:57 CST	Device Log MOE Log	gger deviceVendor	deviceProduct	deviceVersion 7.1	Disp deviceEventClassId Signature_ID	name ba	83 Events per seEventCou	page: 100 V destinationAddre:
Selected Fields (5) deviceEventClassId deviceProduct	2 = 2	Time (Event Time)           24         2013/01/27 20:20:57 CST	Device Log MOE Loc	ager deviceVendor	deviceProduct	deviceVersion 7.1	Disp deviceEventClassid Signature_ID	Naying 1 - 100 of 27 name ba MOEEvent 1	83 Events per seEventCou	page: 100 V destinationAddre:
Selected Fields (5) deviceEventClassId deviceProduct deviceVendor	2 = 2 2	Time (Event Time)           24         2013/01/27 20:20:57 CST	Device Log MOE Loc	gger deviceVendor	deviceProduct	deviceVersion 7.1	Disp deviceEventClassId Signature_ID	Naving 1 - 100 of 27	83 Events per	page: 100 V destinationAddre:
Selected Fields (5) deviceEventClassId deviceProduct deviceVendor deviceVersion	2 = 2 2 2	Time (Event Time)           24         2013/01/27 20:20:57 CST	Device Log MOE Loc	gger deviceVendor	deviceProduct	deviceVersion 7.1	Disp deviceEventClassId Signature_ID	Naying 1 - 100 of 27 name ba MOEEvent 1	83 Events per	page: 100 V destinationAddre:
Selected Fields (5) deviceEventClassId deviceProduct deviceVendor deviceVersion name	2 = 2 2 2 2 2 2	Time (Event Time)           24         2013/01/27 20:20:57 CST           RAW         CEF:0 HP HPI0 7.11Sig	Device Log MOE Loc	gger deviceVendor	deviceProduct HPIO 27 20:04:43,408 [	deviceVersion 7.1 Thread-14858 -]	Disp deviceEventClassId Signature_ID	Maying 1 - 100 of 27 name ba MOEEvent 1 controller.manag	83   Events per seEventCou   ger.resource.1	page: 100 V destinationAddre:
Selected Fields (5) deviceEventClassId deviceProduct deviceVendor deviceVersion name	2 = 2 2 2 2	Time (Event Time)           24         2013/01/27 20:20:57 CST           RAW         CEF:0 HP HPI0[7,1]Sig           25         2013/01/27 20:20:57 CST	MOE Loc MOE Loc MOE Loc	gger deviceVendor al HP	deviceProduct HPIO 27 20:04:43,408 [ HPIO	deviceVersion 7.1 Thread-14858 -] 7.1	Disp deviceEventClassId Signature_ID INFO com.hp.hpio.cc Signature_ID	Maying 1 - 100 of 27 name ba MOEEvent 1 controller.manag MOEEvent 1	83   Events per seEventCou ger.resource.1	page: 100 V destinationAddre:
Selected Fields (5) deviceEventClassId deviceProduct deviceVendor deviceVersion name	2 = 2 2 2 2	Time (Event Time)           24         2013/01/27 20:20:57 CST           RAW         CEF:0(IHP)IHP2017.1[51g           25         2013/01/27 20:20:57 CST	MOE Loc MOE Loc MOE Loc	ial HP	deviceProduct HPIO 27 20:04:43,408 [ HPIO	deviceVersion 7.1 Thread-14858 -] 7.1	Disp deviceEventClassId Signature_ID INFO com.hp.hpio.c Signature_ID	MOREVEN 1 MOREVEN 1	183 Events per seEventCou ger.resource.1	page: 100 v destinationAddre: mp1.Resource

In the screen shot above (Figure 29) we searched for MOEevent. This will return all events with the name MOEevent that are sent to the HP ArcSight Logger by the HPIO logging function. The MOEevent is defined in the Matrix infrastructure orchestration log4j properties file as defined in the CSA 3.1 documentation for ArcSight Integration titled <u>HP Cloud Service</u> <u>Automation 3.10 Integration with ArcSight Logger</u> (HP Passport account required). An excerpt from that document is shown below.

#### 27

- log4j.appender.cef1=com.hp.esp.arcsight.cef.appender.Log4jAppender
- log4j.appender.cef1.deviceVendor=HP
- log4j.appender.cef1.deviceProduct=CSA
- log4j.appender.cef1.deviceVersion=3.1
- log4j.appender.cef1.transportType=SYSLOG
- log4j.appender.cef1.hostName=192.x.x.x
- log4j.appender.cef1.port=514
- log4j.appender.cef1.layout=org.apache.log4j.PatternLayout
- log4j.appender.cef1.layout.ConversionPattern=%d [%-18t -%x] %-5p %C.%M %m%n
- log4j.appender.cef1.useCefHeader=true

#### log4j.appender.cef1.eventName=MOEEvent

Similar event types are defined for the other applications that comprise CloudSystem Enterprise including:

- Cloud Service Automation CSAEvent
  - Note this event is not added as part of the CSA 3.1 installation. This was added by modifying the CSA server log4j.properties file with the addition of the following line:
    - log4j.appender.cef1.eventName=CSAEvent
  - C:\Program Files\Hewlett-Packard\CSA\jboss-as-7.1.1.Final\standalone\deployments\csa.war\WEB-INF\classes\log4j.properties
- OOEvent Operations Orchestration
- OORASEvent Operations Orchestration RAS
- SiteScope Event SiteScope
- UCMDBEvent UCMDB

The ArcSight documentation, *User's Guide HP ArcSight SmartConnectors*, explains how to configure an HP ArcSight Connector on each of the Windows operating systems that comprise CloudSystem Enterprise. In the screen shot below we are searching on *failed logon*. Just prior to this search we attempted to login to oo.fog.cloud.internal, this server hosts our Cloud Service Automation and Operations Orchestration applications. As you can see in Figure 30 below, the failed logon attempts are captured and reported in the HP ArcSight Logger.

Figure 30. Logger Failed Logon Event

ArcSight Logger		EPS In EPS Out	CPU EPS In: 3 EPS Out: 0 CPU Load: 2%	<ul> <li>Help</li> <li>About</li> <li>Options</li> </ul>
Summary Analyze Dashboards	Reports Configuration System Admin		admin	🔊 Logout
💕 🛃 🗙 🦊 🛛 🖬 Field Sur	nmary 🗌 Discover Fields 🛛 Last 5 minutes 🖃			
Search: failed logon			Gol	
Advanced Search				
Fields: All Fields	Auto Update: Smin 💌 🔚 4	Q 999 🕚 00:01.344 📃	Export Results	1 bar = 1 second 🔺 🛄
Sort By Name	🕅 4   Page1 of 1   🕨 🕅 😂   Show RAW: All N	one	Displaying 1 - 4 of 4	4 Events per page: 100 🗸
Selected Fields (4)	Time (Event Time) Device	Logger deviceVendor	deviceProduct	deviceVersion
deviceEventClassId 1 deviceProduct 1 deviceVendor 1 name 1	RAW CEF:0 Hicrosoft Hicrosoft Windows  Microsoft- local system which requested the logon. This is most 2 2013/01/28 08:22:50 CST oo fog.cloud.internal[CSE:S	Vindows-Security-Auditing:46251An account 1018 commonly a service such as the Server service C] Local Microsoft	to log on. [Medium] eventīdm , or a local process such as w MicrosoftWindows	▲ 2293 externalId=4625 msg_ finlogon.exe or Services.

Looking at the Logger Analyze screen in Figure 30, we can see that the search criteria was failed logon in the Last 5 minutes. Out of 999 events that were logged during the five minute reporting period, four of these events were failed logons.

### HP ArcSight ESM – Viewing Events with Active Channels

Events can be viewed in the ESM using an Active Channel. To view events forwarded to the HP ArcSight ESM from the ArcSight Logger, right click on the logger connector and set as current filter. This will display all current events as shown in Figure 31.



Figure 31. ArcSight EMS Manager Logger 2ESM Connector

To test our failed login forwarder created earlier, we will attempt to login to oo.fog.cloud.internal. This server hosts our Cloud Service Automation and Operation Orchestration applications. By setting our Active Channel filter to the Logger2ESM Connector we can see in Figure 32 that the failed logon attempts are reported (forwarded) to the HP ArcSight ESM.

Figure 32. ESM view of Failed Logons

🛠 ArcSight Console 5.2.0.6847.0 [arcmgr.fog.cloud.internal:admin.a	t] Internal license, used for development and QA. Customer: ArcSight Internal License Key, Expiration date: 2013/02/28	
File Edit View Window Tools System Help		
- 🗁 🖶 🖳 🐰 隆 🛍 🗶 🔍 144 44 💷 🕨 🕪	₩ <	
Navigator 🖬 ? 🗙	Viewer	d'? ×
Resources Packages Use Cases	🕑 Untitled Active Channel 😼 Logger Platform Events 🔯 Last 5 Minutes 😼 Last Hour	
🔗 Connectors Ctrl+Alt+E 🔻	🙀 Active Channel: Last Hour [Modified]	Total Events: 3 🗕
Connectors	Start Time: 29 Jan 2013 09:29:00 CST End Time: 29 Jan 2013 09:29:00 CST Filter: Agent ID = "Logger/ESM" Inline Filter: No Filter Radar	Very High: 0 High: 0 Medium: 3 Low: 0 Very Low: 0
SREScope(down) T 19 MS(vunning) UCMBS/v(down) CuCMBS/v(down) B 10 Ste Connectors B 10 Unassigned	Image: Section 2013 04:16:12 CST     An account failed to log on.     OO.fog.doud.internal     Microsoft     Microsoft Windows       29 Jan 2013 04:16:12 CST     An account failed to log on.     OO.fog.doud.internal     S     Microsoft     Microsoft Windows       29 Jan 2013 04:16:12 CST     An account failed to log on.     OO.fog.doud.internal     S     Microsoft     Microsoft Windows       29 Jan 2013 04:16:12 CST     An account failed to log on.     OO.fog.doud.internal     S     Microsoft     Microsoft Windows	

You can customize this view by selecting more or less columns of event information to be displayed. Figure 33 shows the failed logon events that were forwarded to the HP ArcSight ESM and the event information includes the event Name, Attacker User Name, Attacker Address, Target Address, Priority, and Device Vendor.

### Figure 33. View of Failed Logons with additional fields

- Mouston CMS-Svr(running) CSA-00(running)	Ini Ve	ine Filter: No Filter rified Rules: No Rule						¥e	ry Low: 0	
CSADB(running)	Ra	ədər								-
ESM-WIN(running) Logger2ESM(running) SIS-Svr(running)										
TP SMS(running)	1	Manager Receipt Time 🕇 1	End Time 🗢	Name \$	Attacker User Name	Attacker Address 🖨	Target Address 🖨	Priority 🗢	Device Vendor	,
UCM-Svr(running)		29 Jan 2013 11:52:46 CST	29 Jan 2013 11:52:01 CST	An account failed to log on.	Administrator	192.168.156.51	10.119.109.70	5	Microsoft	*
Venterwebservices(running)		29 Jan 2013 11:52:46 CST	29 Jan 2013 11:52:05 CST	An account failed to log on.	Administrator	192.168.156.51	10.119.109.70	5	Microsoft	
Site Connectors		29 Jan 2013 11:52:46 CST	29 Jan 2013 11:52:14 CST	An account failed to log on.	administrator	192.168.156.51	10.119.109.70	5	Microsoft	
±- 🛄 Unassigned		29 Jan 2013 11:52:46 CST	29 Jan 2013 11:52:19 CST	An account failed to log on.	administrator	192.168.156.51	10.119.109.70	5	Microsoft	
		29 Jan 2013 11:38:56 CST	29 Jan 2013 11:37:47 CST	An account failed to log on.	administrator	192.168.156.51	10.119.109.72	5	Microsoft	
		29 Jan 2013 11:38:56 CST	29 Jan 2013 11:37:51 CST	An account failed to log on.	administrator	192.168.156.51	10.119.109.72	5	Microsoft	

Click on the event to view the event details. Looking at the details we can see details of the failed logon attempt. The Figure below (Figure 34) shows some of the possible event information that is collected by the Connector when the Failed Logon event is triggered, any of the fields in the event details can be used as search criteria for queries and rules described later in this document.

Figure 34. Failed Logon Event Details

Event Details Anno	tations Payload
	Event Inspector
12 Name	Value
Event	
Name	An account failed to log on.
Message	Network: A user or computer logged on to this computer from the network.
Туре	Base
End Time	29 Jan 2013 04:16:23 CST
Aggregated Event C	1
Correlated Event Co	0
Category	
Category Significance	/Informational/Warning
Category Behavior	/Authentication/Verify
Category Device Group	/Operating System
Category Outcome	/Failure
Category Object	/Host/Operating System
Threat	
Model Confidence	4
Severity	0
Relevance	10
Asset Criticality	0
Priority	5
Agent	
Agent Severity	Medium
Agent Host Name	192.168.156.90
Agent Address	192.168.156.90
Agent Zone Resource	CloudSystem Enterprise
Agent Asset ID	4f14rIDwBABCSK3jAYtw8ug==
Agent Version	5.2.4.6344.0
Agent Time Zone	America/Chicago
Agent ID	3dhDqJDwBABDBUnjAYtw8ug==
Agent Type	logger
Agent Name	Logger2ESM

### Zones

High value assets can be grouped into Zones. A Zone is based on a range of IP Addresses which can be used as a filter to search and view log activity.

Figure 35. ArcSight ESM Manager Zones

	Active Channel: Asset Channel 1						T	otal Assets : 5
Fil	t <b>er:</b> Device Zone ID = "Cloud Syste	m Enterprise (Public)						
Ini	ine Filter: No Filter							
Ra	adar							
	Name 🖨	Address 🖨	Mac Address 🖨	Host Name 🗢 🛛 🗍 1	Location 🖨 De	Device Zone Name 🖨	Device Zone Start Addr	Device Zone End 4
₽	ARCMGR	10.119.100.10	00:00:00:00:00:00	ARCMGR		Cloud System Enterprise	10.0.0.0	10.255.255.255
₽	00_0	10.119.109.66	00:00:00:00:00:00	00		Cloud System Enterprise	10.0.0.0	10.255.255.255
₽	ORA_0	10.119.109.70	00:00:00:00:00:00	ORA		Cloud System Enterprise	10.0.0.0	10.255.255.255
₽	SIS	10.119.100.3	00:00:00:00:00:00	SIS		Cloud System Enterprise	10.0.0.0	10.255.255.255
₽	ucm	10.119.109.72	00:00:00:00:00:00	ucm		Cloud System Enterprise	10.0.0.0	10.255.255.255
	Active Channel: Asset Channel						Т	otal Assets : 3
Filt	er: Device Zone ID = "CloudSyster	n Enterprise"						
Inli	ine Filter: No Filter							
Ra	ıdar							1
	Name 🖨	Address 🖨	Mac Address 🖨	Host Name 🖨 🛛 🗍 1	Location 🖨 De	Device Zone Name 🖨	Device Zone Start Addre	Device Zone End #
₽	csa-oo	192.168.156.23	00:00:00:00:00:00	00		CloudSystem Enterprise	192.168.156.1	192.168.156.254
	Fog-CMS	192.168.156.1	00:00:00:00:00:00	fog		CloudSystem Enterprise	192.168.156.1	192.168.156.254
	vcenter	192.168.156.4	00:00:00:00:00:00	vcenter		CloudSystem Enterprise	192.168.156.1	192.168.156.254

Grouping of machines by zones allows the ArcSight administrator to monitor the high value assets; we have grouped the CloudSystem Enterprise server nodes in the Zone named CloudSystem Enterprise.

#### Figure 36. Zone Properties

2	Zone:CloudSystem Enterprise					
At	Attributes Assets Categories Notes					
E	Zone					
	* Name	CloudSystem Enterprise				
	🗰 Start Address	192.168.156.1				
	💥 End Address	192.168.156.254				
	Dynamic Addressing					
	Location	Select a Location				
	Network	Local				

### Queries

Queries can be created and executed against the ArcSight ESM data; a query is created and then executed by the query viewer. We'll use our failed logon example to demonstrate how to create and execute a query.

Launch the New Query pane and provide a Name for your query, in Figure 37 we've used Failed Login as the name for our query. Next we'll select the Fields tab to configure the fields that will be returned by the Query.

Figure 37. ESM Query Failed Logon – General

E	a Query Viewer:Failed Logons 🛛 🛱 Query Editor				
Ge	Seneral Fields Conditions Local Variables Notes				
-	Query				
	* Name	Failed Logon			
	* Query On	Event			
	🛪 Start Time	\$Now - 1d			
	* End Time	\$Now			
	💥 Use as Timestamp	End Time			
	* Row Limit	10000			
	Distinct Rows				
	Database Hint				

In the Fields tab we can select which event fields we want to return and display when the Query is executed. Using the failed logon event we'll display the Category Outcome, Category Behavior, Target Address, Target Host Name and Attacker User Name, as illustrated in Figure 38.

Figure 38. ESM Query Failed Logon – Fields



Next we'll select the conditions that must be met to satisfy our Query. In this section we'll select the Category Behavior equal to /Authentication/Verify and Category Outcome = False.

Figure 39. ESM Query Failed Logon – Conditions

🟹 Query Viewer:Failed Logons 🛛 🗮 Query Editor
General Fields Conditions Local Variables Notes
Field Conditions Group Conditions
🚯 & 🔢 💻 📽 Filters 🕮 Assets 🔯 Vulnerabilities 📑 Active Lists
Edit Summary
Event conditions
Eres AND
Category Defravior = /Failure

Our Failed Logon Query is now ready to display all events that contain these conditions.

Next we'll create a query viewer that will be used to execute our Failed Logon Query. We've named this Query Viewer "Failed Logons" and selected our Failed Logon Query in the Query field.

Figure 40. ESM Query Viewer Failed Logon – Attributes

_						
Query Viewer:Failed Logons						
Attributes Fields Local Variables Drilldowns Notes						
-	Query Viewer	<u>ـ</u>				
	* Name	Failed Logons				
	* Query	Failed Logon				
	Refresh Data After	15 minute(s)				
	Query Time Out	None				
	* Default View	Table				

By default the Query data will be refreshed every 15 minutes.

When we execute our Failed Logon Query using the Failed Logon Query Viewer all events that meet our query criteria are displayed. Below we can see the fields that were selected in the Failed Logon Query.

- Category Outcome
- Category Behavior
- Target Address
- Target Host Name
- Attacker User Name

The Category Outcome must equal "Failure" and the Category Behavior must equal "Authentication / Verify" to meet the criteria of the query and return events in the Query viewer table.

Figure 41. HP ArcSight ESM Query Viewer Results – Failed Logon

ArcSight Console 5.2.0.6047.0 [arcmgr.fog.cloud.internakadmin.ast] Internal license, used for development and QA. Eustomer: ArcSight Internal License Key, Expiration date: 2013/02/28							
File Edit Wew Window Tools System Help							
🗔 - 🗁 🖽 🕵 🕺 🐜 🛍 🗙 🔍 144 44 🔟 🕨 💷 ÞÞ	De 🛛 🖉 🖻 🔸 🧐 🖡	3 G. (P) 🐛 🕼 🔌 📓 🔛 🤋	à - 🔍				
Navigator d' ? ×	Viewer				5° X		
Resources Packages Use Cases Dubited Active Channel 1 Asset Channel 1 Asset Channel 1 Asset Channel 2							
Query Viewers Ctrl+Alt+Q -	💽 Asset Channel 4 🛛 🗮 Fa	iled Logons: Table 📄 Asset Ch	annel 5 📔 🔊 Asset Channel 6	Asset Channel 7 Asset Ch	nannel 8 📄 Untitled Active Channel 1		
Cuery Viewers	Query: Failed Logon				23 shown		
admin's Query Viewers	Start Time: 1/28 11:55:02	tart Time: 1/28.11:55:02					
Ealed Logons	End Time: 1/29 11:55:02						
E-77 Shared	Last Update: 29 Jan 2013 11:55:0	Last Update: 29 Jan 2013 11:55:03 CST					
All Ouery Viewers	Filter: No Filter						
ArcSight Administration	Category Outcome	Category Behavior	Target Address	Target Host Name	Attacker User Name		
ArcSight Foundation	/Failure	/Authentication/Verify	10.119.100.10	arcmgr.fog.cloud.internal			
ArcSight Solutions	/Failure	/Authentication/Verify	10.119.109.66	OO.fog.cloud.internal	Administrator		
🕀 🫅 JumpStart	/Failure	/Authentication/Verify	10.119.109.66	OO.fog.cloud.internal	Administrator		
🕀 🔂 Personal	/Failure	/Authentication/Verify	10.119.109.66	OO.fog.cloud.internal	Administrator		
🔅 🫅 Public	/Failure	/Authentication/Verify	10.119.109.66	OO.fog.cloud.internal	Administrator		
🗄 🛅 Unassigned	/Failure	/Authentication/Verify	10.119.109.66	OO.fog.cloud.internal	Administrator		
	/Failure	/Authentication/Verify	10.119.109.66	OO.fog.cloud.internal	Administrator		
	/Failure	/Authentication/Verify	10.119.109.66	OO.fog.cloud.internal	Administrator		
	/Failure	/Authentication/Verify	10.119.109.66	OO.fog.cloud.internal	Administrator		
	/Failure	/Authentication/Verify	10.119.100.10	arcmgr.fog.cloud.internal			
	/Failure	/Authentication/Verify	10.119.109.72	ucm.fog.cloud.internal	administrator		
	/Failure	/Authentication/Verify	10.119.109.72	ucm.fog.cloud.internal	administrator		
	/Failure	/Authentication/Verify	10.119.109.72	ucm.fog.cloud.internal	administrator		
	/Failure	/Authentication/Verify	10.119.109.72	ucm.fog.cloud.internal	administrator		
	/Failure	/Authentication/Verify	10.119.109.72	ucm.fog.cloud.internal	administrator		
	/Failure	/Authentication/Verify	10.119.109.70	ORA.fog.cloud.internal	Administrator		
	/Failure	/Authentication/Verify	10.119.109.70	ORA.fog.cloud.internal	Administrator		
	/Failure	/Authentication/Verify	10.119.109.70	ORA.fog.cloud.internal	Administrator		
	/Failure	/Authentication/Verify	10.119.109.70	ORA.fog.cloud.internal	Administrator		
	/Failure	/Authentication/Verify	10.119.109.70	ORA.fog.cloud.internal	administrator		
	/Failure	/Authentication/Verify	10.119.109.70	ORA.fog.cloud.internal	administrator		
	/Failure	/Authentication/Verify	10.119.109.70	ORA.fog.cloud.internal	administrator		
	/Failure	/Authentication/Verify	10.119.109.70	ORA.fog.cloud.internal	administrator		

In Figure 41 we can see that we have recorded failed logon attempts against the following servers:

- oo.fog.cloud.internal Operations Orchestration and Cloud Service Automation host)
- arcmgr.fog.cloud.internal HP ArcSight ESM Manager and Console
- ucm.fog.cloud.internal Universal Configuration Management Server
- ORA.fog.cloud.internal Oracle Database server for UCMDB

### Rules

Rules are used to trigger an Action when a specific event or event(s) occur. Keeping with our Failed Logon example we are going to create a Rule named Failed Logon Notify that will trigger an email when three failed logons occur on the same host within two minutes.

The Rules configuration is similar to the Query configuration. Use the Rule Editor to define the Conditions. We are going to use the same condition that was specified in out Failed Logon Query to identify failed logon events by specifying the Category Behavior equal to /Authentication/Verify and Category Outcome = /Failure as shown in Figure 42.

**Figure 42.** HP ArcSight ESM Rule Editor – Conditions



Next we'll configure the Aggregation tab, in this section we configure the rule to execute after a defined number of events occur within a specified time period on a single host, three times in two minutes, on the same Target Host Name. The fields of the events can be matched if they are the same or unique. In this example we have selected the Target Host Name field to be the same for three events during a two minute span. Other event fields could be added, for example Attacker User Name or Attacker Address. Once configured the Rule Aggregation Summary will display the following:

• Aggregate if at least 3 matching conditions are found within 2 Minutes AND these event fields are the same (event1.Target Zone Resource, event1.Target Host Name)

The Actions tab specifies the action to take when the conditions of a Rule are met. We can configure actions to occur as specified in the Actions tab. We have chosen to trigger the Send Notification action On Every Event. Selecting Send Notification will prompt you to specify a destination and a brief message for the email body.

📝 Rule Editor 🛛 🚟 Query:Failed Logon 📄									
Attributes Conditions Aggregation Actions Local Variables Notes									
🔚 Add , 🐣 Edit  🗙 Remove 🔺 Move Up 🔻 Move Down  🖹 Hide Empty Triggers									
<ul> <li>On First Event [ Active ]</li> <li>On Subsequent Events</li> <li>On Every Event [ Active ]</li> <li>Send Notification</li> <li>AckRequired: Yes</li> <li>NotificationMessage: Failed Logons occured Resource: /All Destinations/SOC Operators/</li> <li>On First Threshold</li> <li>On Subsequent Thresholds</li> <li>On Every Threshold</li> <li>On Time Unit</li> <li>On Time Window Expiration - Cumulative Rule Chain Is Off</li> </ul>									

Figure 43. HP ArcSight ESM Rule Editor – Actions Summary

In our example we have chosen to send a message to the SOC Operators group and with a message Failed Logons occurred.

# **Cloud Security Alliance**

The Cloud Security Alliance is a not-for-profit-organization that provides guidance, education, and promotes best practices for security in cloud computing. The Cloud Security Alliance's mission statement is:

"To promote the use of best practices for providing security assurance within cloud computing, and provide education on the uses of cloud computing to help secure all other forms of computing."

In accordance with their mission statement, the Cloud Security Alliance publishes security guidance and a cloud controls matrix to address security concerns in cloud computing.

The HP ArcSight products address several areas that are outlined in the security guidance document.

The Cloud Security Alliance guidance document, Security Guidance for Critical Areas of Focus in Cloud Computing, defines 14 domains for operating in a cloud environment and provides recommendations on how to securely operate in those domains. Each domain addresses a specific area of concern with respect to security and cloud computing. The HP ArcSight products address areas of concern in the Cloud Security Alliance Domains listed below:

#### **Domain 5– Information Management and Data Security**

5.4.1 Locations and Access

5.6.5 Database and File Activity Monitoring

#### **Domain 6 – Interoperability and Portability**

6.3.2 Portability Recommendations (logging)

6.3.3 Recommendations for Different Cloud Models - log traces

### Domain 9 – Incident Response

9.3.2 Detection and Analysis

9.3.3 Data Sources

9.3.4 Forensic and Other Investigative Support for Incident Analysis

9.3.5 Containment, Eradication, and Recovery

#### **Domain 10 – Application Security**

10.2 Authentication, Authorization, and Compliance – Application Security Architecture in the Cloud

10.3 Identity Management

10.5 Monitoring Applications in the Cloud

10.5.1 Application Monitoring in the Cloud

10.6.3 Architecture Recommendations

#### Domain 14 – Security As A Service

14.4.7 Security Information & Event Management (SIEM)

14.7.7 SIEM SECaaS Requirements

SECASS Category 7 – Security Information and Event Management Implementation Guidance

https://cloudsecurityalliance.org/research/secaas/

The Cloud Security Alliance Security Control Matrix contains a list of controls that identify and describe security controls that are applicable to cloud computing. The security controls in Table 1 can be addressed with the HP ArcSight solution.

### Table 1. Security controls

Control	Number	Description	HP ArcSight
Information Security – User Access Reviews	IS-10	All levels of user access shall be reviewed by management at planned intervals and documented. For access violations identified, remediation must follow documented access control policies and procedures.	HP ArcSight ESM
Information Security – Incident Management	IS-24	Policies and procedures shall be established to triage security related events and ensure timely and thorough incident management.	HP ArcSight ESM
Information Security – Audit Tools Access	IS-29	Access to, and use of, audit tools that interact with the organizations information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	HP ArcSight ESM
Information Security – Incident Response Metrics	IS-30	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	HP ArcSight ESM
Security Architecture – Audit Logging / Intrusion Detection	SA-14	Audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events shall be retained, complying with applicable policies and regulations. Audit logs shall be reviewed at least daily and file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents. Physical and logical user access to audit logs shall be restricted to authorized personnel.	HP ArcSight ESM

### Summary

In this document we have shown how to use HP ArcSight Logger and HP ArcSight ESM to enhance security for CloudSystem Enterprise environments. Using HP ArcSight Logger as a central repository for security and event logging, organizations can use HP ArcSight ESM to monitor and react to security related events. Monitoring both application and operating system events provides organizations with a comprehensive view of the CloudSystem environment. We also discussed using the HP ArcSight Logger to aggregate events and forward specific events to the HP ArcSight ESM for further analysis, investigation, and action.

## Appendix A: ASLinuxAudit.props

The ASLinuxAudit.props file in the Server Automation Package ArcSight-5.2.7.6474.0-Connector-Linux-props.zip (Figure 26) used for automated deployment of the ArcSight smart connector for Linux audit logger is shown below. This file was generated by running **runagentsetup.sh** -i **recorderui** to capture user input. This Smart Connector installation response file is configured to send events to the ArcSight Logger with a Smart Connector configured with the name "Smart".

```
#
  What would you like to do?
# Please select one of the following options :
  0 - Add a Connector (addconnector)
#
#
  1 - Enable FIPS mode (setfipsmode)
#
containeroperation=addconnector
# ______
# Panel 'connectortype'
# ______
  Select the connector to configure
#
# Type
connectortype.connectortype=linux auditd
# ______
# Panel 'connectorparameter'
# ______
#
 Enter the connector details
#
# Log File Name
connectorparameter.logfilename=/var/log/audit/audit.log
# ______
# Panel 'connectordestinationtypes'
# ______
#
  Enter the type of destination
# Please select one of the following options :
  0 - ArcSight Manager (encrypted) (http)
#
  1 - ArcSight Logger SmartMessage (encrypted) (loggersecure)
#
#
  2 - NSP Device Poll Listener(nsp)
#
  3 - CEF File(ceffile)
#
  4 - CEF Syslog(cefsyslog)
#
  5 - CEF Encrypted Syslog (UDP) (encryptedcefsyslog)
#
  6 - CSV File(file)
#
  7 - Raw Syslog(simplesyslog)
connectordestinationtypes=loggersecure
# Panel 'connectordestinationnew'
# ______
#
  Enter the destination parameters
#
# Host Name/IP
connectordestinationnew.host=192.168.153.159
# Port
connectordestinationnew.port=443
# Receiver Name
connectordestinationnew.rcvrname=Smart
# Compression Mode
# Possible values: [Disabled | Enabled]
```

connectordestinationnew.compression=Enabled

```
# _____
# Panel 'connectordetails'
# ______
#
 Enter the connector details
#
# Name
connectordetails.name=LinuxAudit
# Location
connectordetails.location=Houston
# DeviceLocation
connectordetails.devicelocation=Houston
# Comment
connectordetails.comment=Linux Audit file logging
# Panel 'serviceselection'
# ______
#
 The Smart Connector is currently installed as a standalone application
#
# Please select one of the following options :
#
  0 - Install as a service(installService)
#
  1 - Leave as a standalone application(continueorexit)
serviceselection=installService
# ______
# Panel 'servicedetails'
# ______
 Specify the service parameters
#
# Service Internal Name
servicedetails.internalname=linux auditd
# Service Display Name
servicedetails.displayName=Linux Audit File
# Start the service automatically
# Possible values: [true | false]
servicedetails.auto=true
# _____
# Panel 'continueorexit'
# ______
 Would you like to continue or exit?
#
#
# Please select one of the following options :
#
  0 - Continue(continue)
#
  1 - Exit(exit)
continueorexit=exit
```

# For more information

Learn more at <u>hpenterprisesecurity.com/products</u>

To read more about CloudSystem Enterprise go to <u>hp.com/qo/cloudsystementerprise</u>

Understanding the HP CloudSystem reference architecture <u>http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA3-4548ENW</u>

For more information about the Cloud Security Alliance <u>https://cloudsecurityalliance.org/</u>

To help us improve our documents, please provide feedback at hp.com/solutions/feedback.

# Sign up for updates hp.com/go/getupdated

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.



Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation. Oracle is a registered trademark of Oracle and/or its affiliates.