Technical white paper

HP CloudSystem Enterprise

Integrating security with HP ArcSight

Table of contents

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.

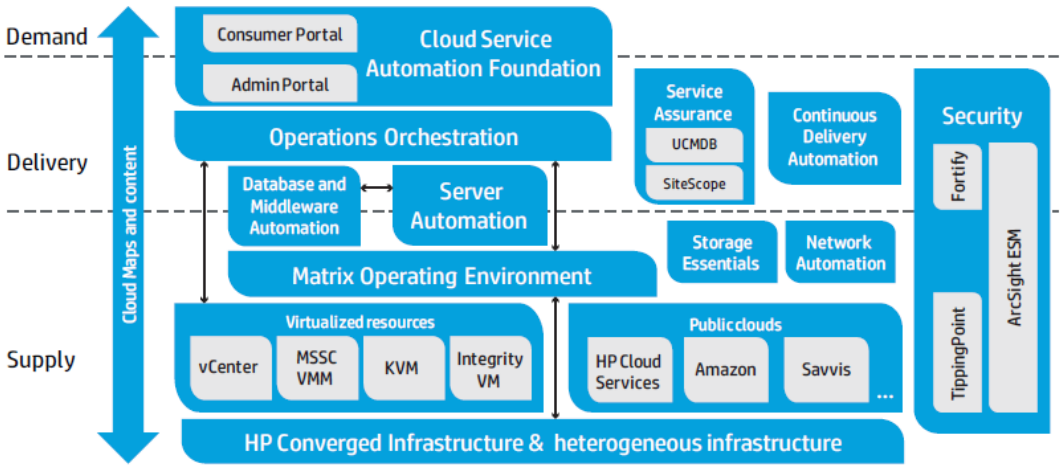
HP CloudSystem Enterprise overview

With HP CloudSystem Enterprise, an organization can deliver not only IaaS, 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.

Figure 1. CloudSystem Enterprise Functional Architecture



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 IaaS 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 (OO)
OO 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.

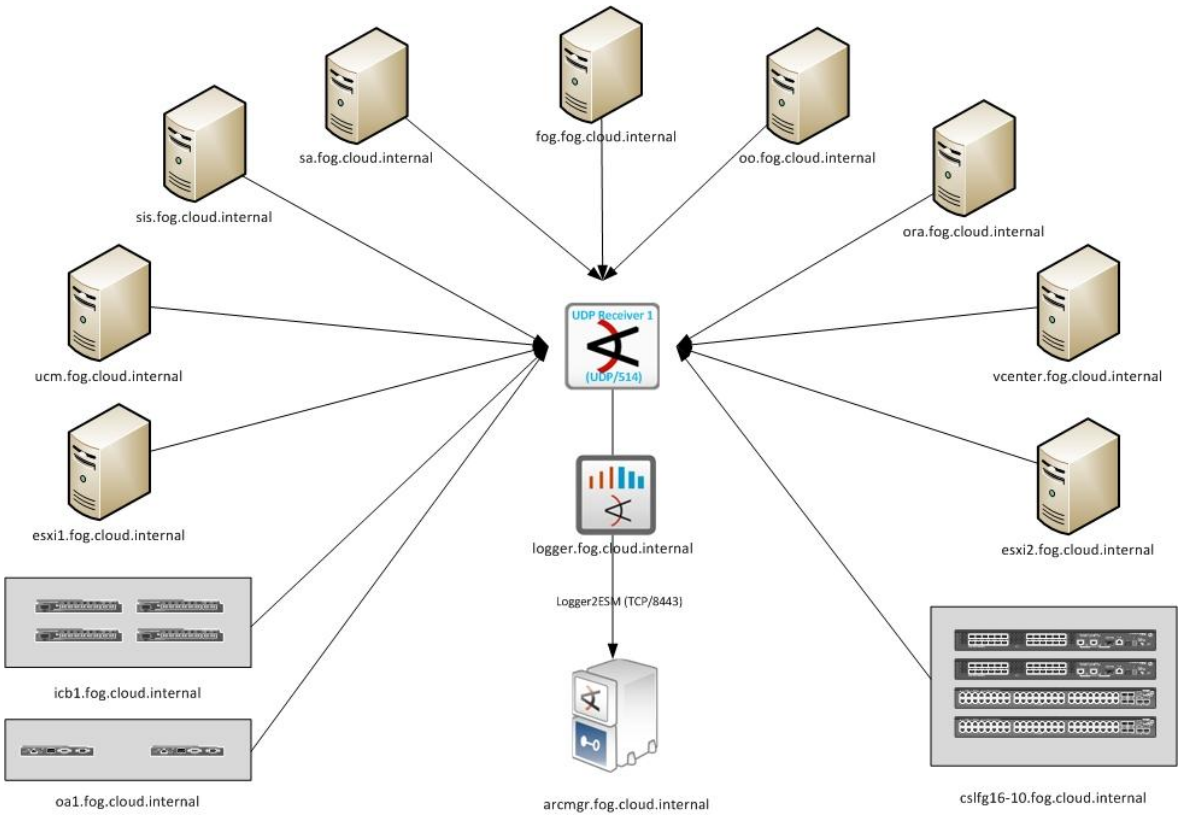
Our reference implementation is comprised of the following servers that are illustrated in Figures 2 – 4:

- 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

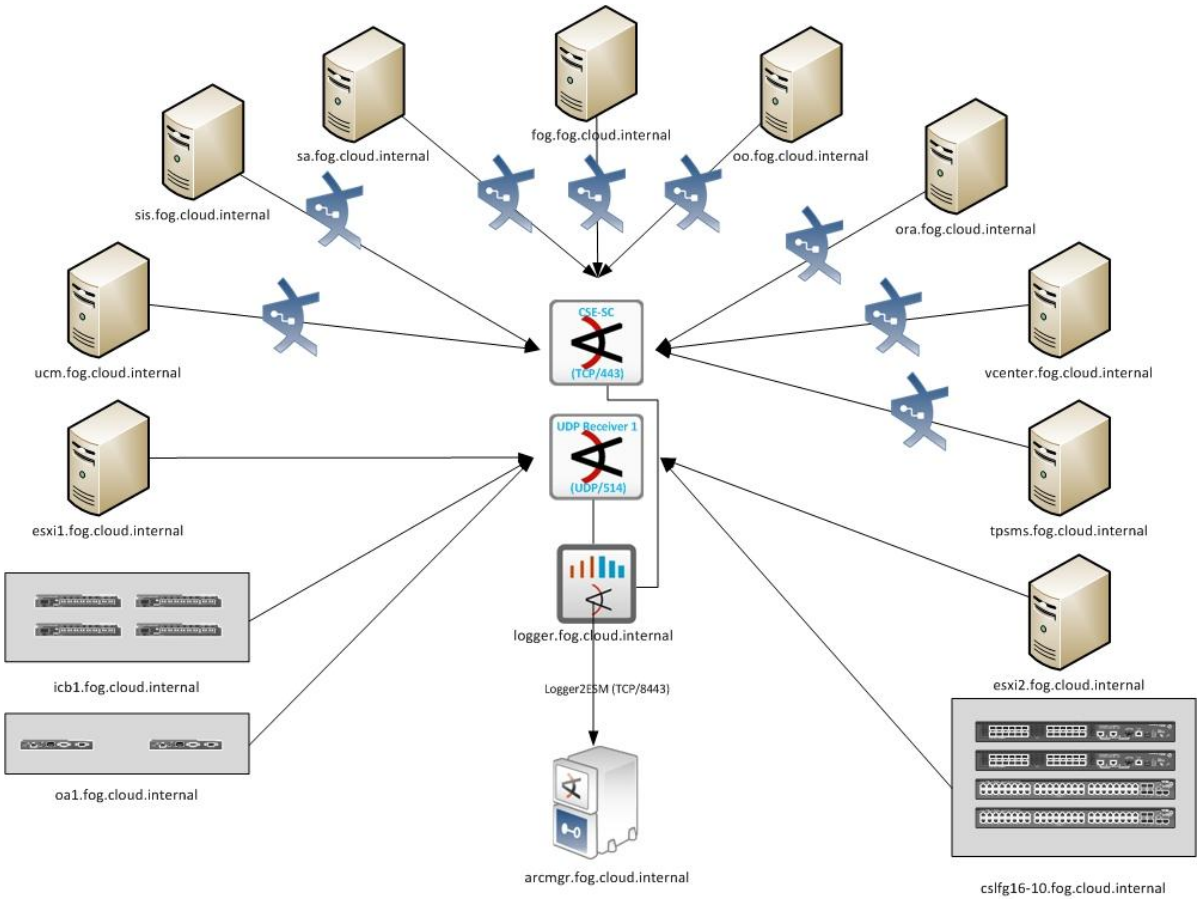


Sending events to HP ArcSight Logger using Connectors

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.

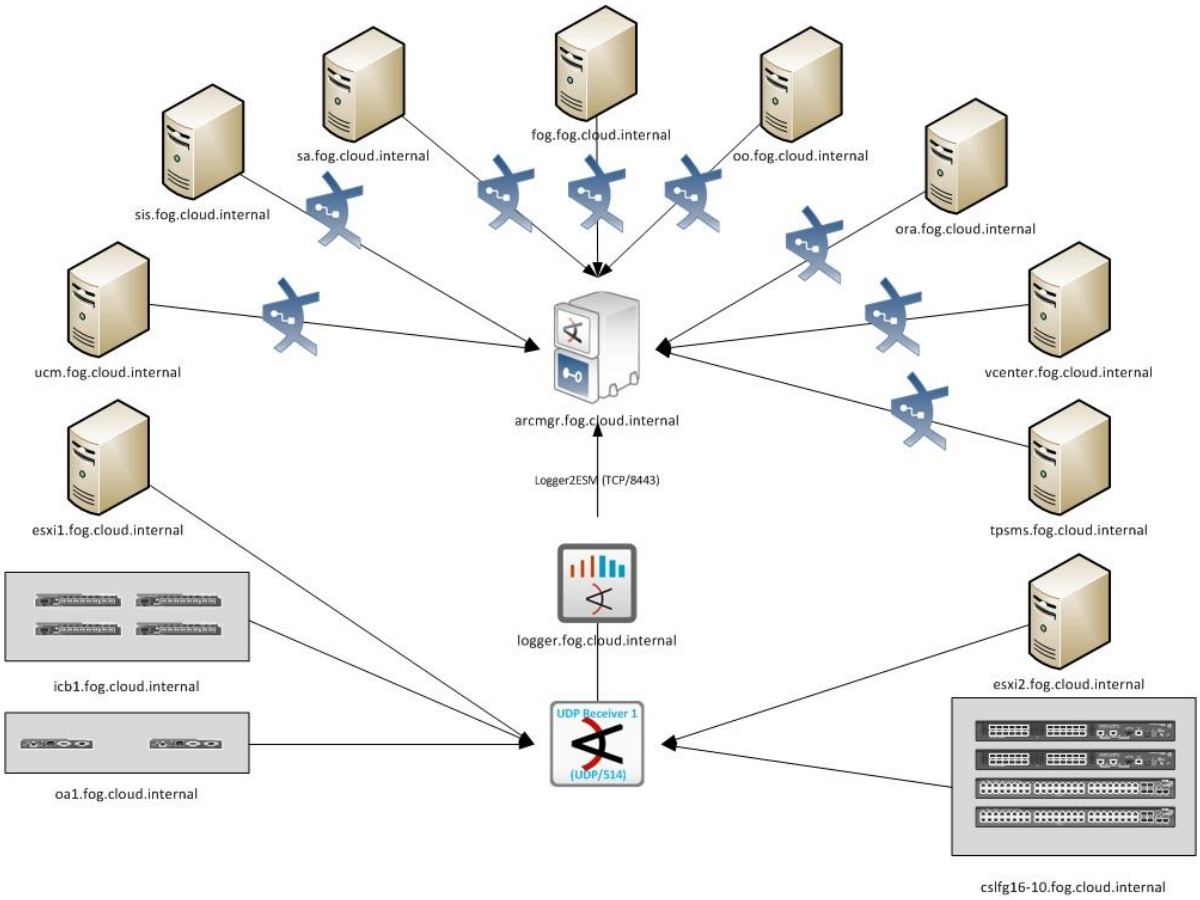
Figure 3. HP ArcSight Connectors and logging to the HP ArcSight Logger



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



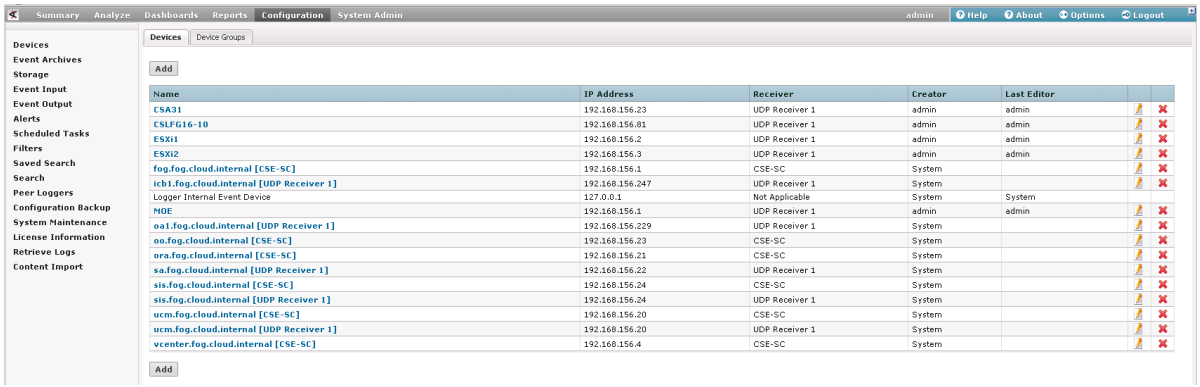
The screen shot below in Figure 5 shows a UDP Receiver and a SmartMessage Receiver created in the HP ArcSight Logger to receive events. The UDP Receiver (UDP Receiver 1) will receive log4j events from the CloudSystem Enterprise applications and other devices on the network (Onboard Administrator (OA), 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.

Figure 5. Logger Event Receivers

Devices

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.

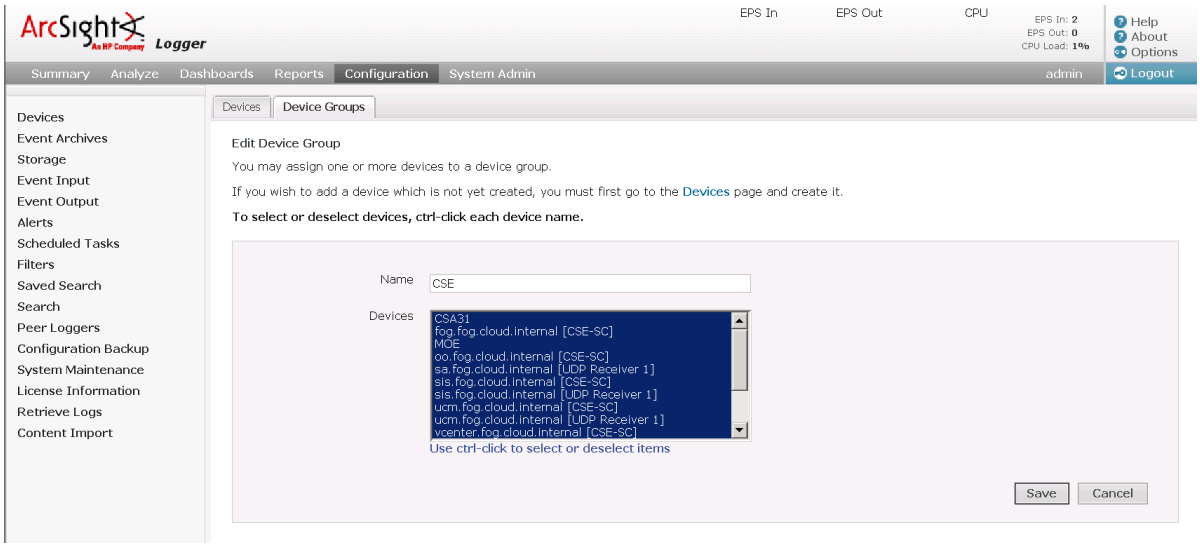
Figure 6. Devices registered with the ArcSight Logger



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

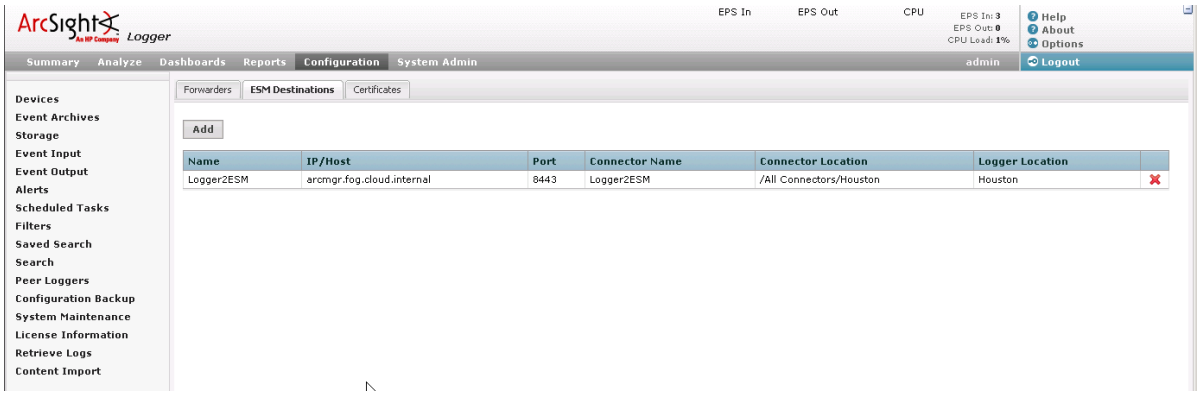


Forwarding events to HP ArcSight ESM

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.

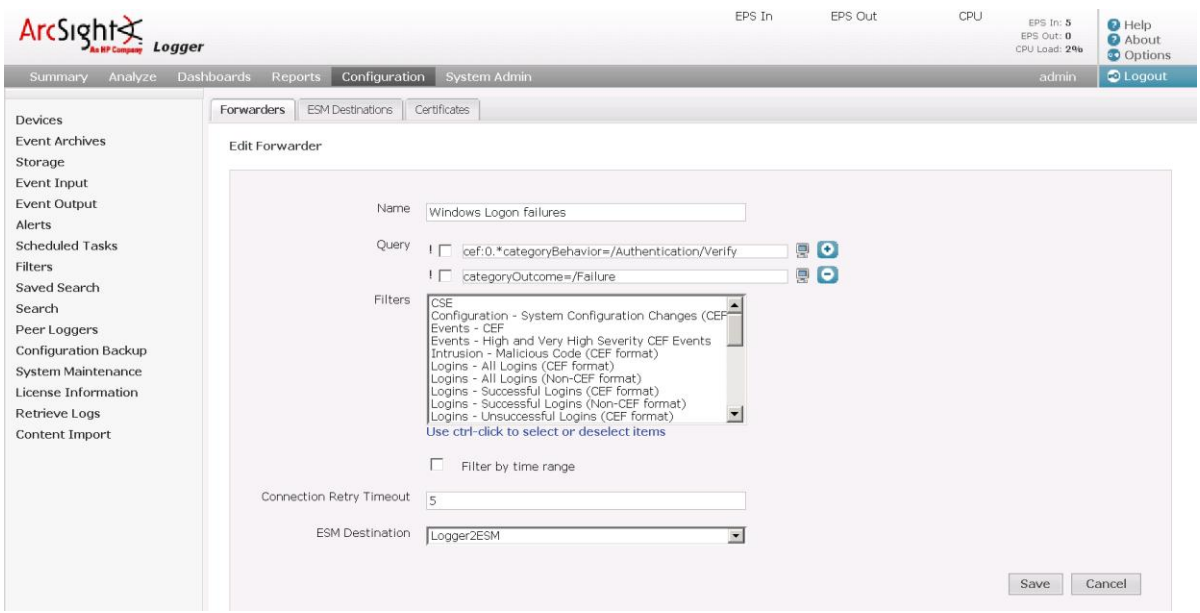
To accomplish this, forwarders are created in the HP ArcSight Logger > Configuration > Event Output interface. The forwarders are configured to send log data to an ESM Destination. The ESM Destination is displayed below in Figure 8; the forwarder configured here will show up as a connector in the ArcSight 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



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.

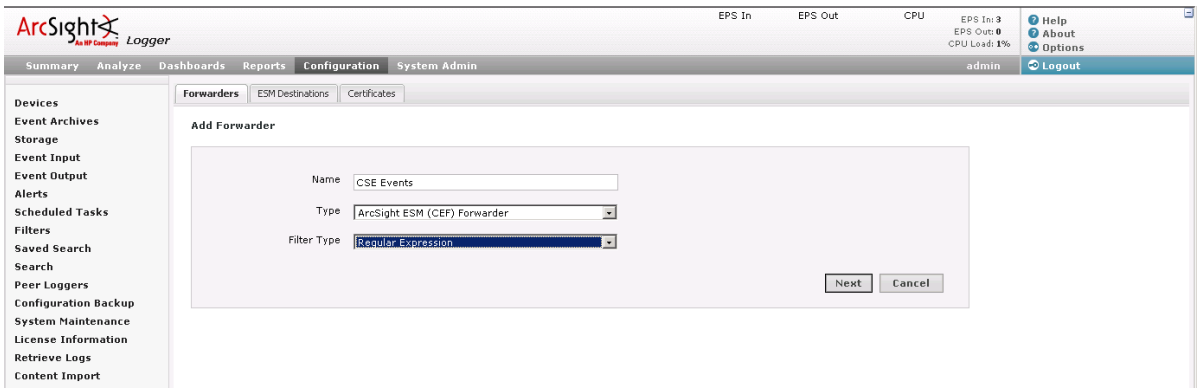
Figure 9. Event Forwarder Logon Failures



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.

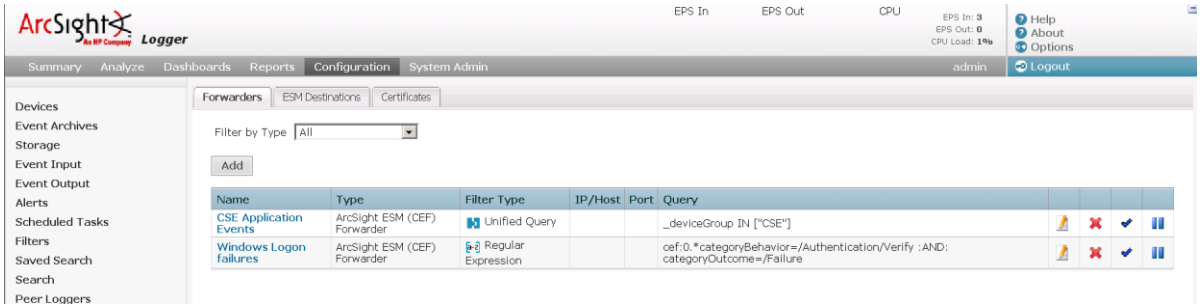
We can also forward events from specific devices or device groups. In our example in Figure 10, we have created a forwarder based on a device group named CSE and a forwarder named CSE Application Events. All events from systems that are part of the device group CSE will be forwarded to the HP ArcSight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

Figure 10. Event Forwarding based on a Device Group



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

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® 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, *HP Cloud Service Automation 3.10 Integration with ArcSight Logger* 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=OO Event
```

Notice the line log4j.appender.cef1.eventName=OO Event, this will allow us to search the logger for all events with an event name of OO 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, OO, HPIO, SiteScope, and UCMDB. This is discussed in detail later in the section titled Working with events.

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:

- OO.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

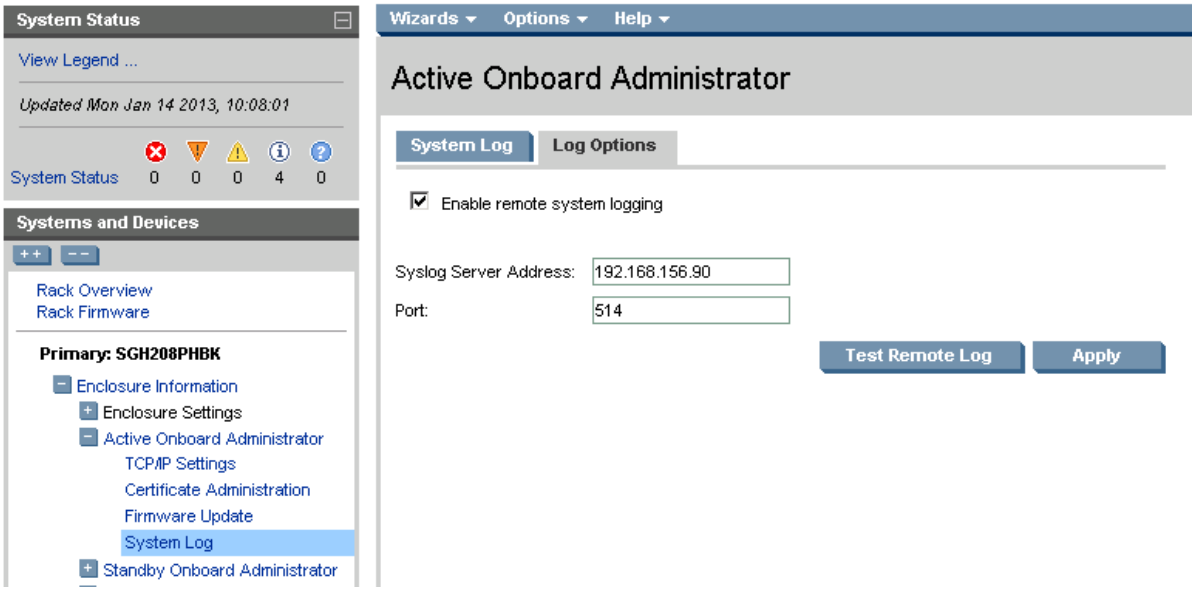
HPIO events have been configured for logging through the procedures described in the Integration with ArcSight document and operating system events are captured by the HP ArcSight Connector. This next section will describe how to configure logging for the c7000 Onboard Administrator and HP Virtual Connect.

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



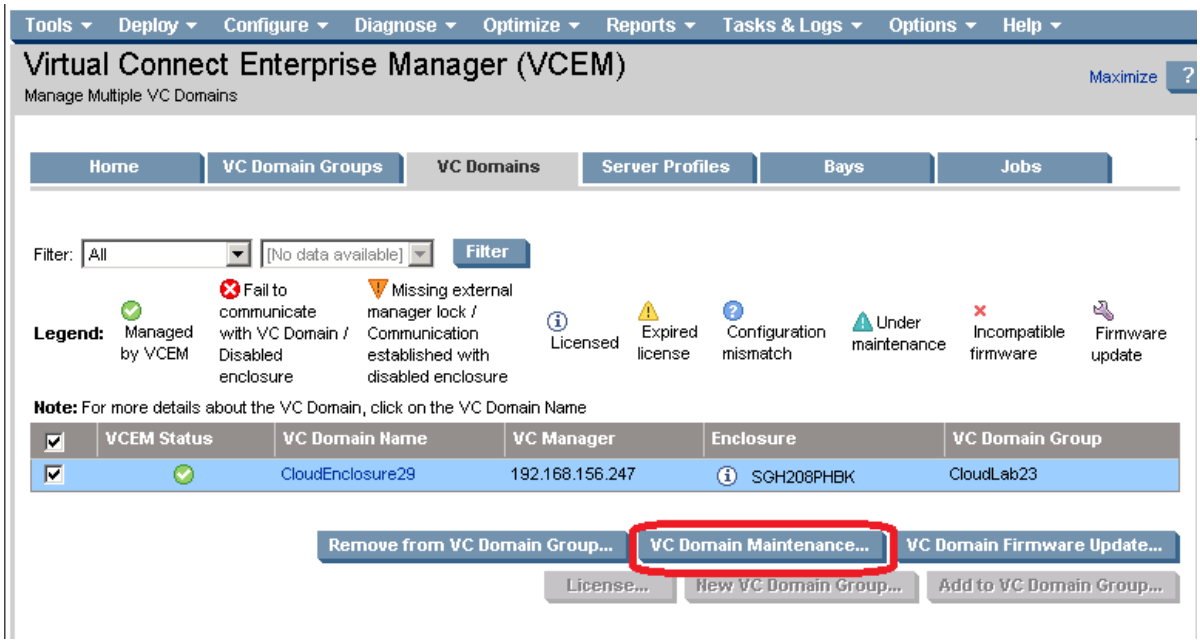
- Select "Apply" to apply the settings.
- Once the screen refreshes, you can select "Test Remote Log". By doing so, a test message is sent to the Logger. If everything is working, you should see the IP or the host name of the HP Onboard Administrator registered in HP ArcSight Logger in the "Configuration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

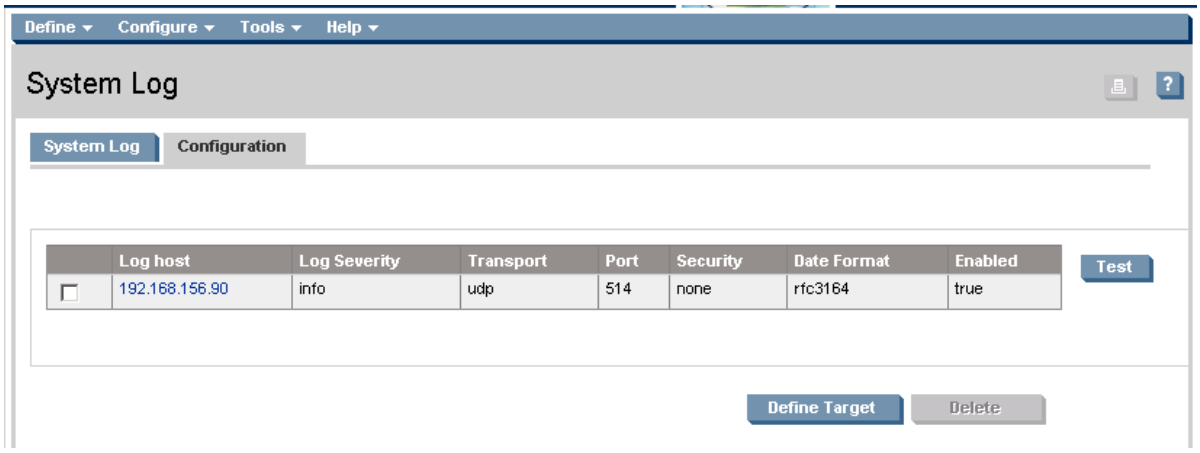
- Log into the HP Matrix Operating Environment Portal and navigate to "Tools -> Integrated Consoles -> Virtual Connect Enterprise Manager (VCEM)..."
- Select the VC domain to be monitored by HP ArcSight from either the "VC Domain Groups" or "VC Domains" tab and select "VC Domain Maintenance..." (Figure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

Figure 13. Virtual Connect Domain Maintenance Mode



- 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



- 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
```

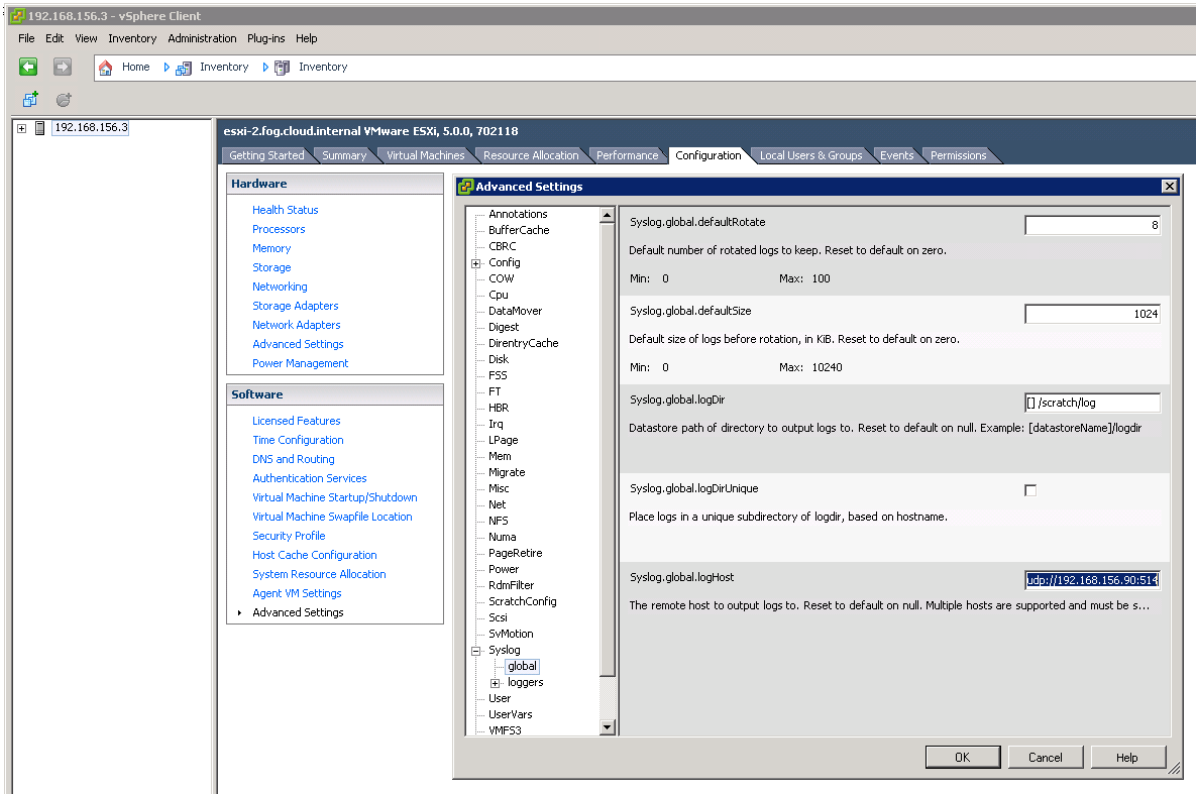
In the example above 192.x.x.x should be replaced with the IP Address of your ArcSight Logger. Restart the syslog daemon and log events will be sent in raw format to the HP ArcSight Logger.

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:

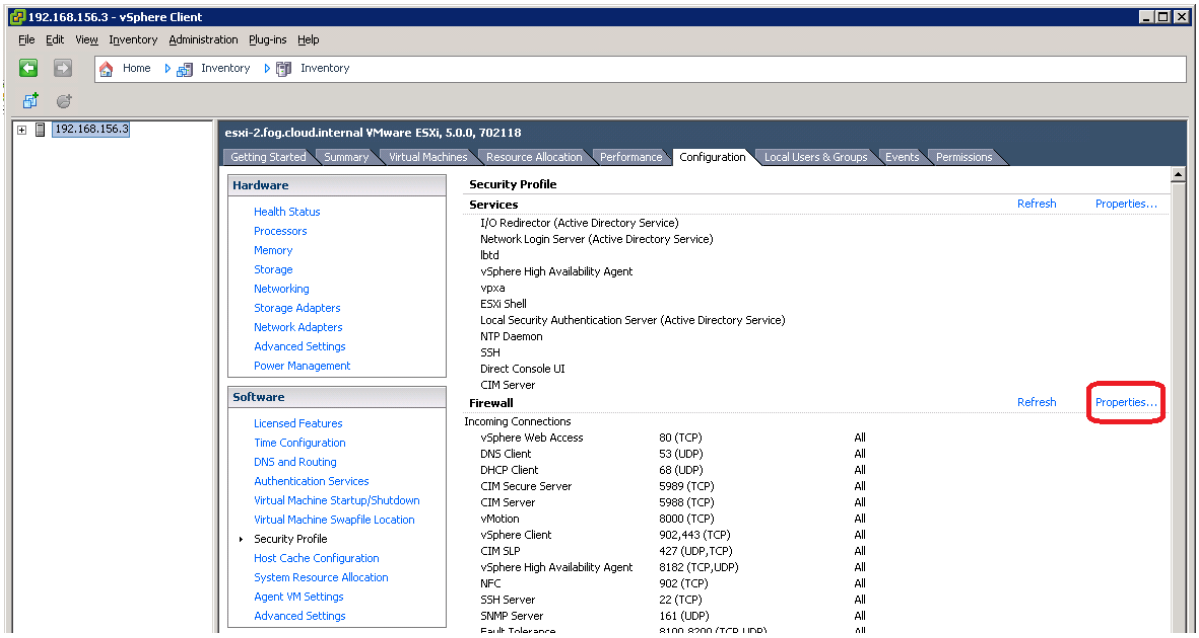
- Log into the host or the VMware vSphere Server using the VMware vSphere Client
  - If connecting to a VMware vSphere Server, navigate to the Host and Clusters view by selecting “Home > Inventory > Host and Clusters” from the View menu.
  - If connecting directly to the host using the VMware vSphere 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



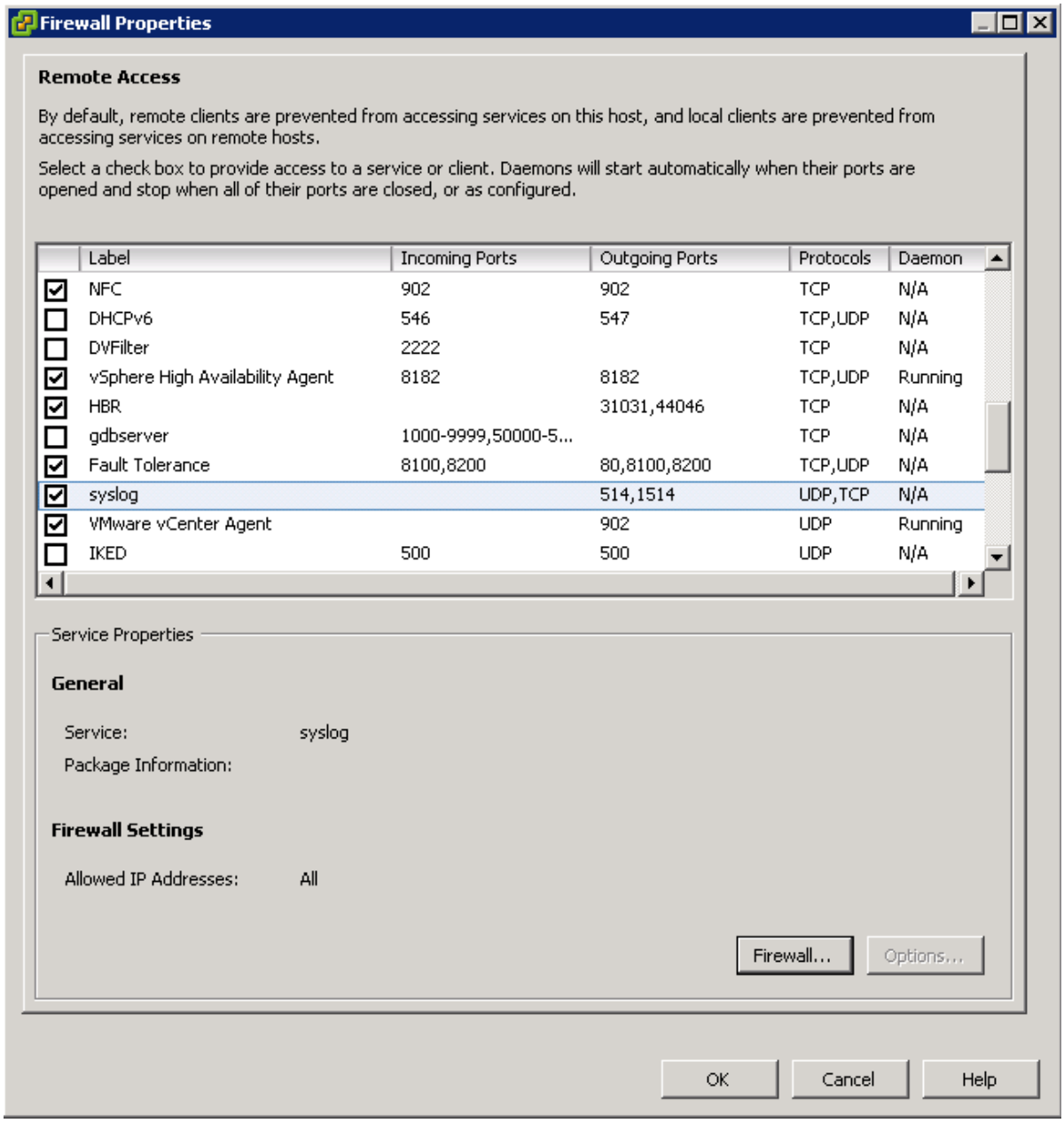
- Select “OK”.
- Select “Security Profile” under the “Software” group box
  - To the right of “Firewall” select “Properties”

Figure 16. ESXi Firewall Select “Properties” to the right of “Firewall”



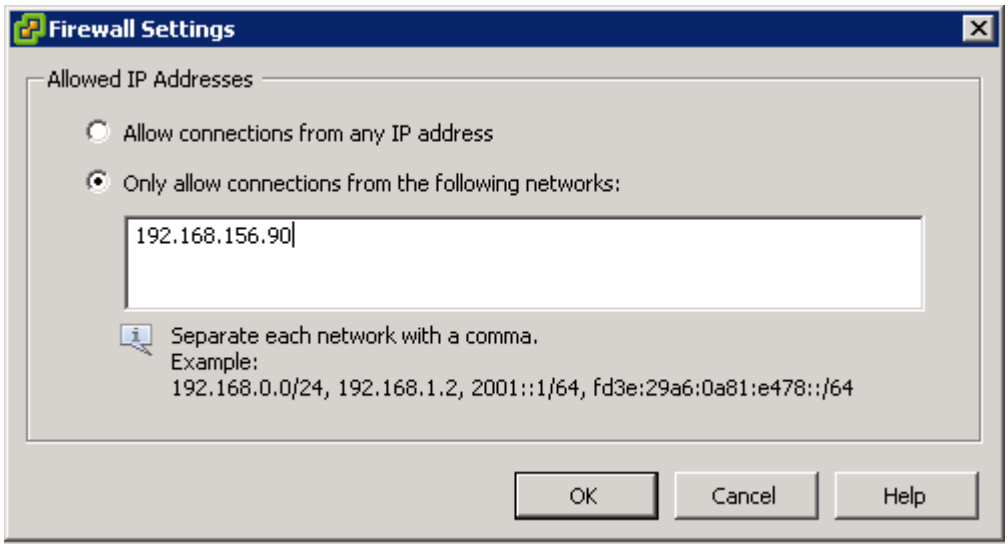
– In the “Firewall Properties” window, scroll down the list until you see “syslog” and select the check box to enable it (Figure 17).

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



– 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



– 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.

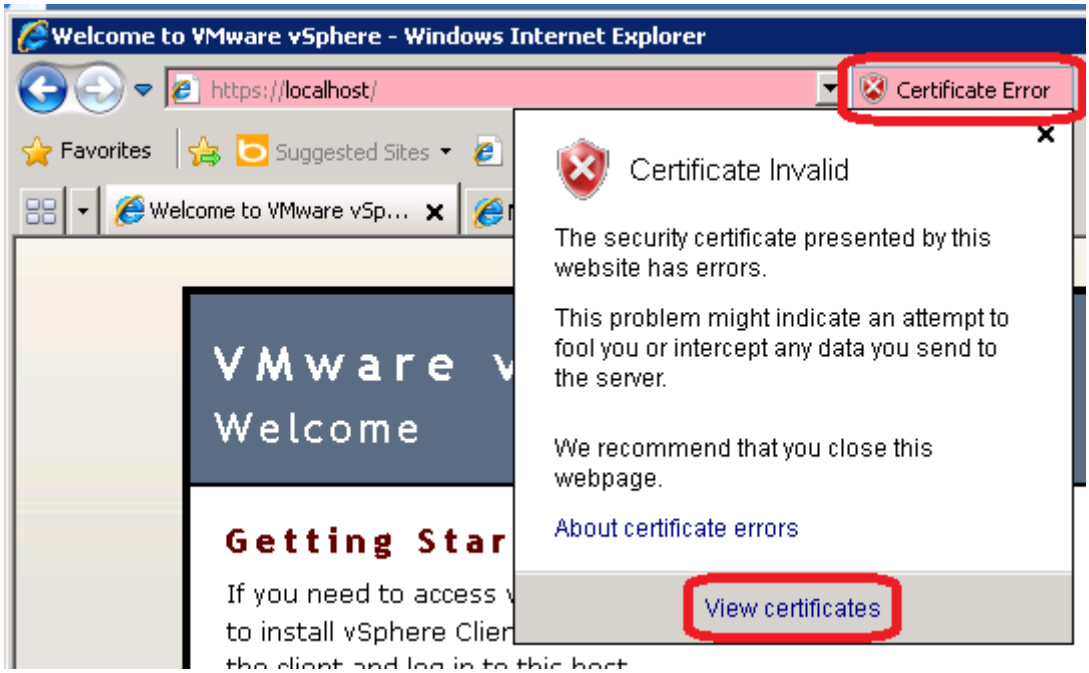
VMware vSphere Web Services

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 https://localhost
  – Next to the address bar, select “Certificate Error” and select “View Certificates” (Figure 19)

Figure 19. Selection of "VMware Web Services"

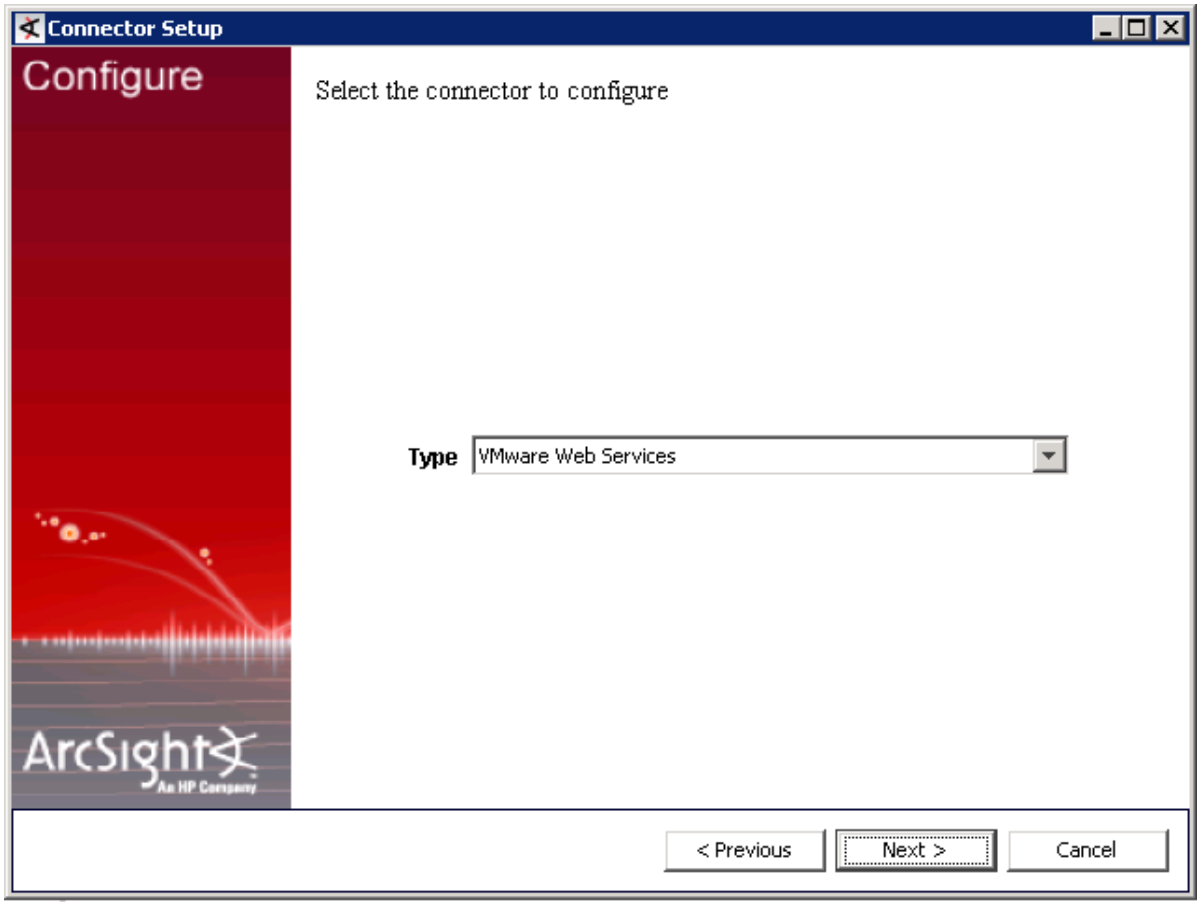


- Select the "Details" tab and select "Copy to File…"
  - Select "Next >" on the Welcome screen
  - Select "Base-64 encoded X.509 (.CER)" and select "Next >"
  - Select "Browse" and save the file to a location on your local disk and select "Next >"
  - Select "Finish"
- Now open a command window. If 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
```

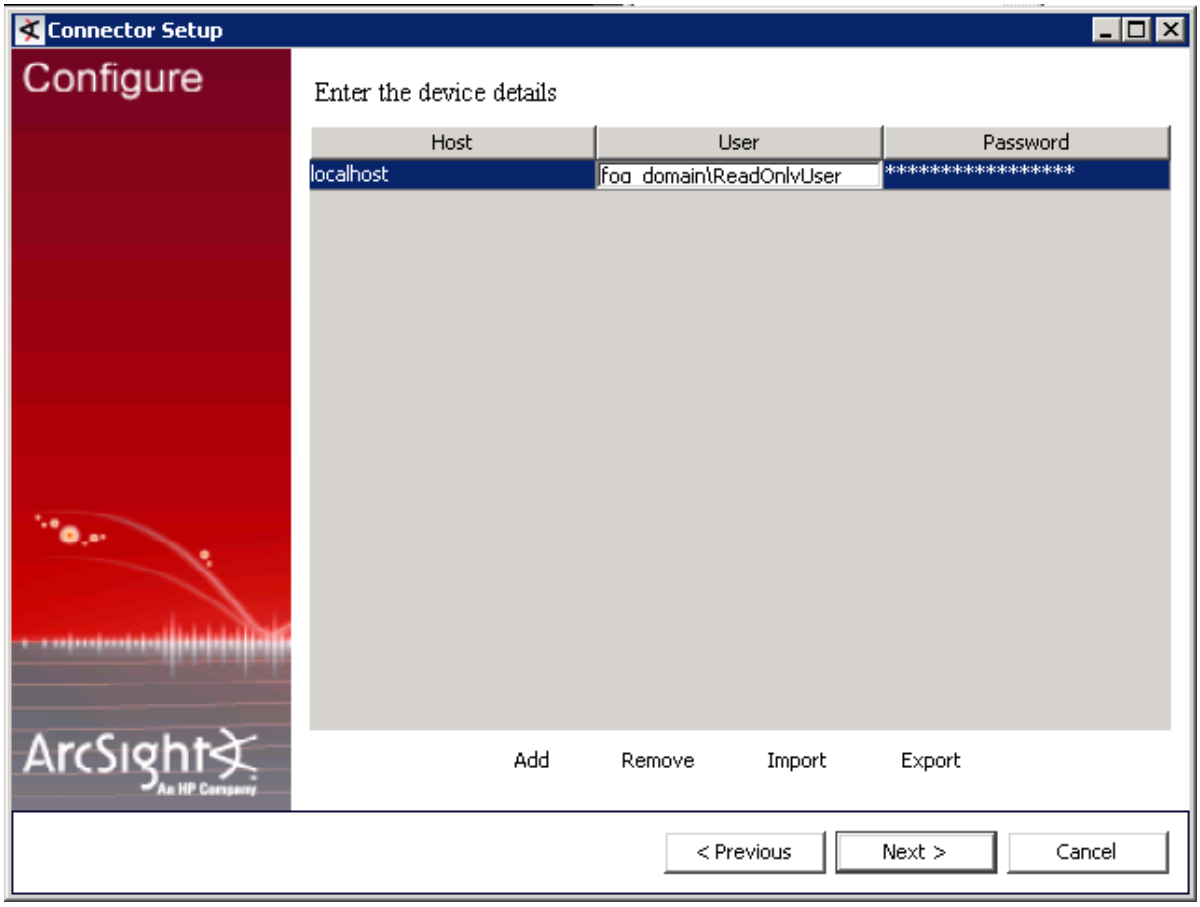
  - Type "yes" when asked "Trust this certificate?"
- Rerun the connector setup by entering in that same command prompt window "runagentsetup"
- Select "Add a Connector"
- Select "VMware Web Services" as the connector "Type" (Figure 20 and select "Next >"

Figure 20. Selection of "VMware Web Services" Connector



- 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 >"

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).

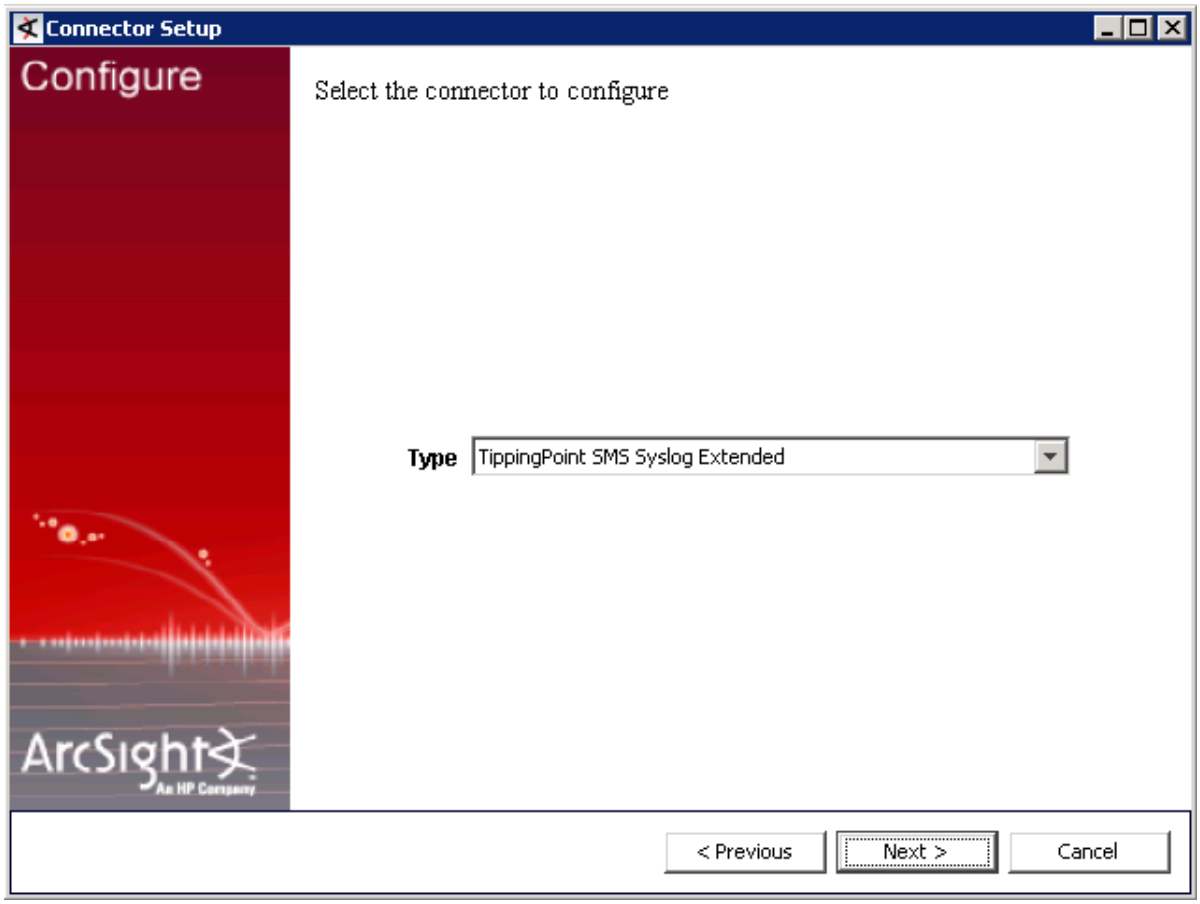
HP TippingPoint Security Management System (SMS) Appliance

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 >"

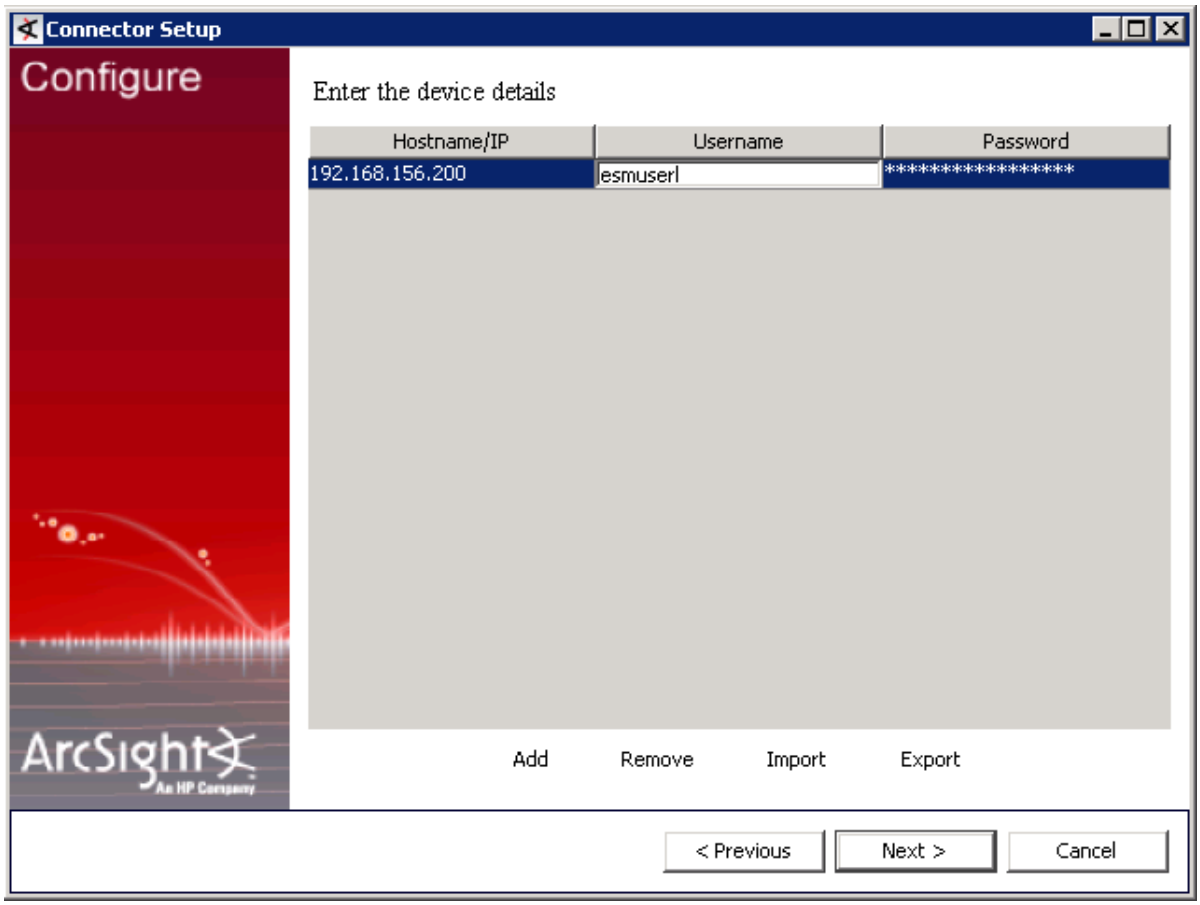
Figure 22. Selecting the "TippingPoint SMS Syslog Extended" Connector



- 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 >”

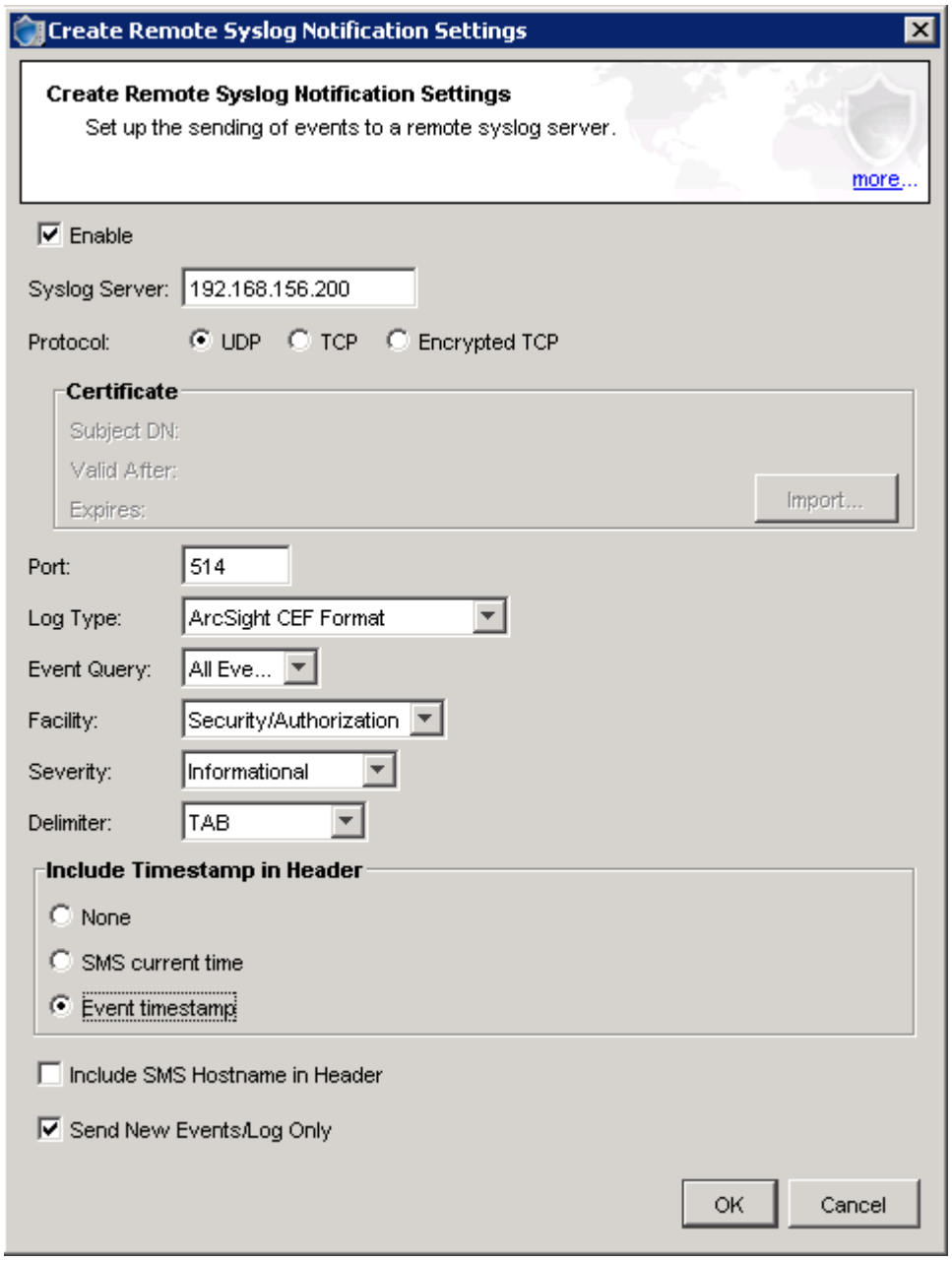
Figure 23. TippingPoint SMS Syslog Extended Connector device details



- 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



- 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

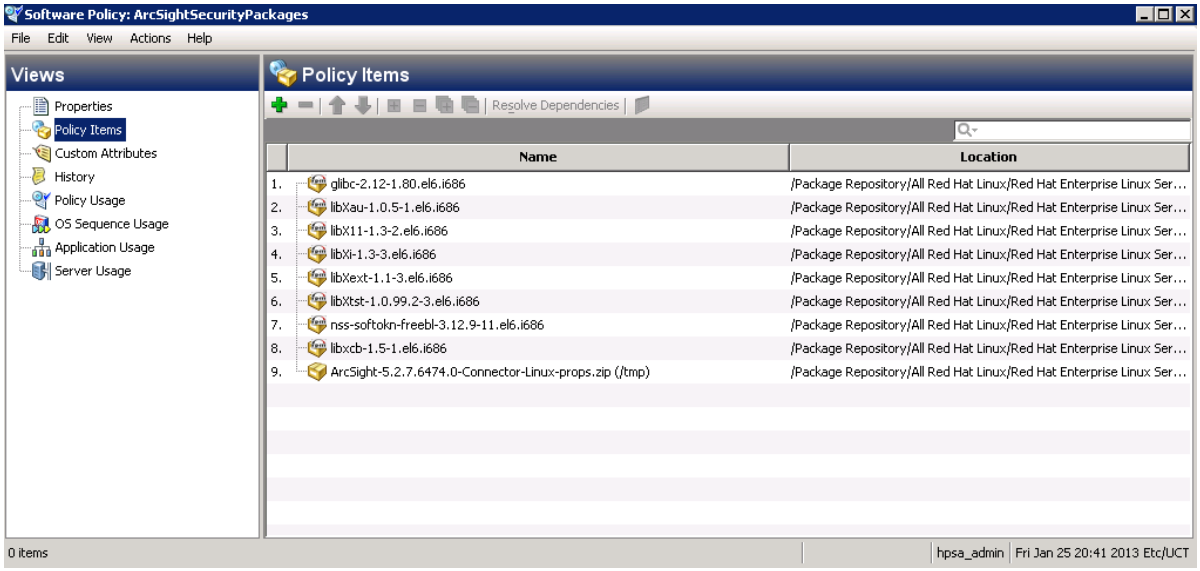
In addition to protecting the HP CloudSystem Enterprise core components that are responsible for supply and delivery of cloud services, the cloud services should also be protected upon provisioning. In this section we will demonstrate how to integrate the HP ArcSight Connector installation and configuration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

HP LAMP solution

The HP LAMP and WordPress Reference Implementation for CloudSystem Enterprise 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.

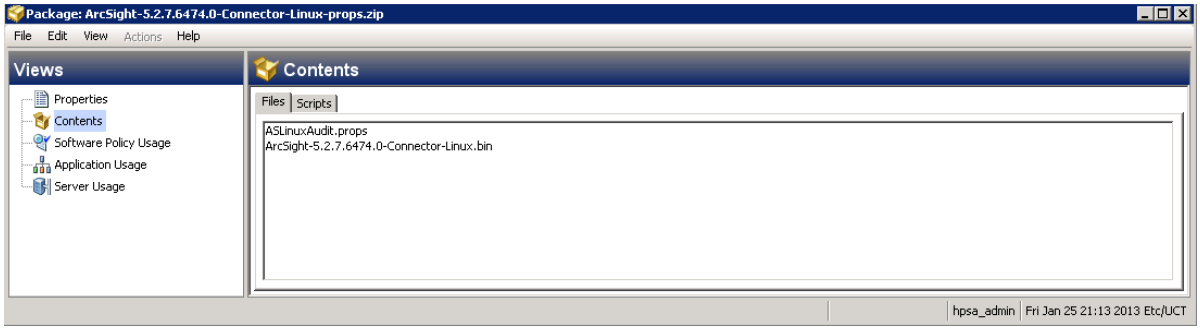
Create the Server Automation software policy ArcSightSecurityPackages. Figure 25 shows the required Linux packages that were needed to deploy the ArcSight Smart connector on a Red Hat Enterprise Linux 6.3 virtual machine.

Figure 25, Required Packages



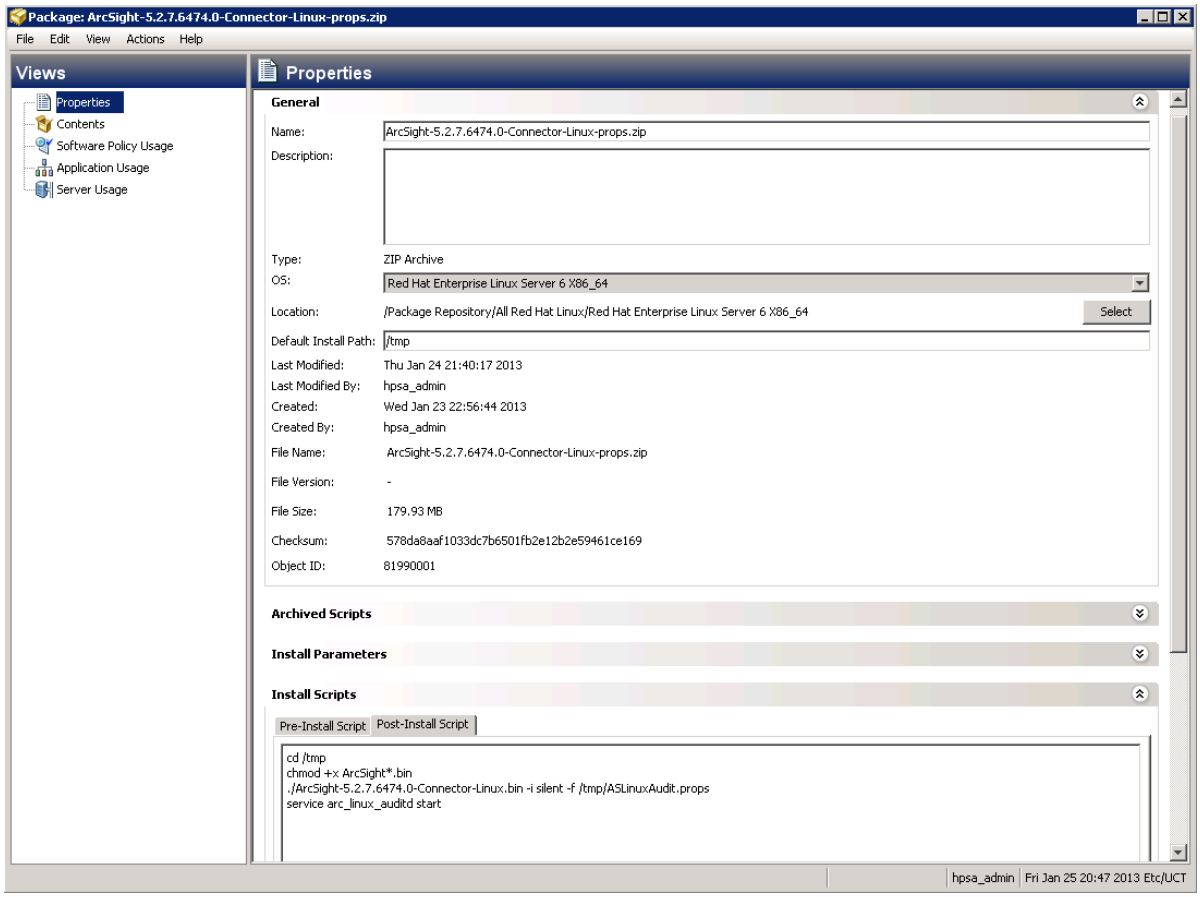
The ArcSight zip file shown in the figure above was created by zipping up the Linux smart connector `.bin` file and the properties file used for silent installation. The contents of the zip file are shown in Figure 26.

Figure 26. Package Contents



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.

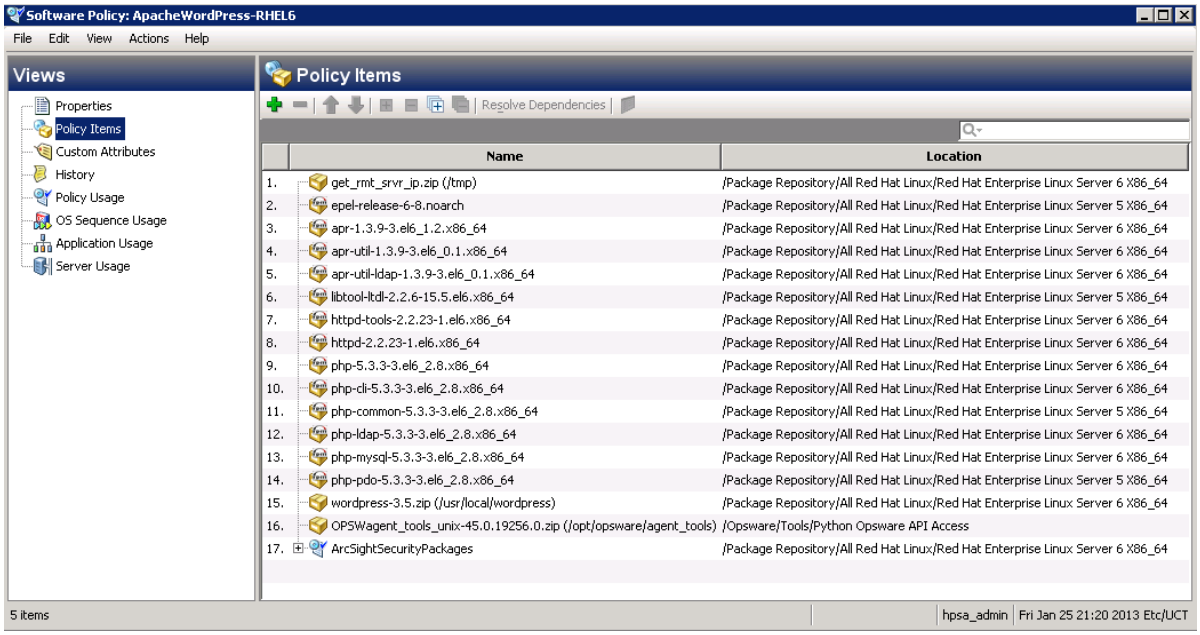
Figure 27. Policy Properties



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 Appendix A.

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

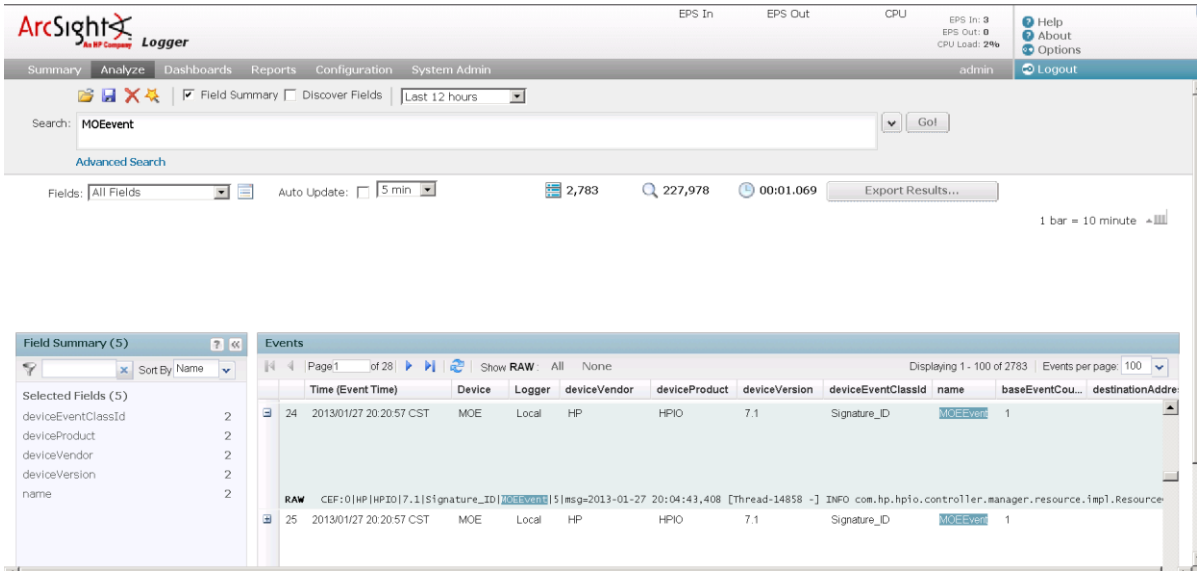


Including the ArcSightSecurityPackages policy into the MariaDB-RHEL6 and ApacheWordPress-RHEL6 policies will automatically deploy the ArcSight Smart Connector for Linux audit logger to the database and web servers and start logging events to ArcSight Logger. The linux_auditd events are visible from the 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



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 HP Cloud Service Automation 3.10 Integration with ArcSight Logger (HP Passport account required). An excerpt from that document is shown below.

```
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
```

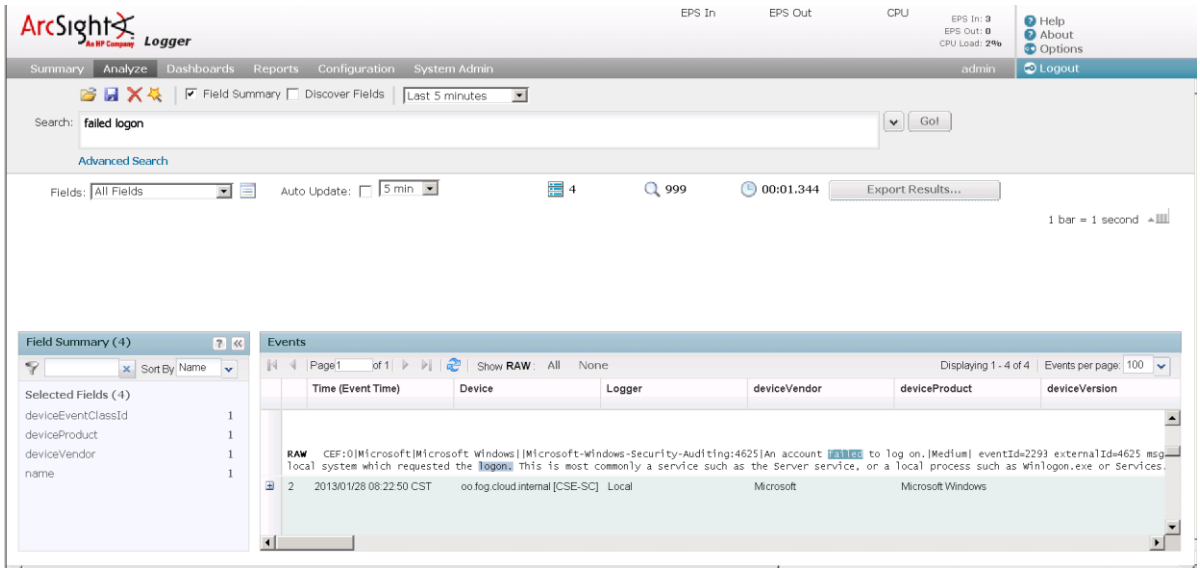
Similar event types are defined for the other applications that comprise CloudSystem Enterprise including:

- 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

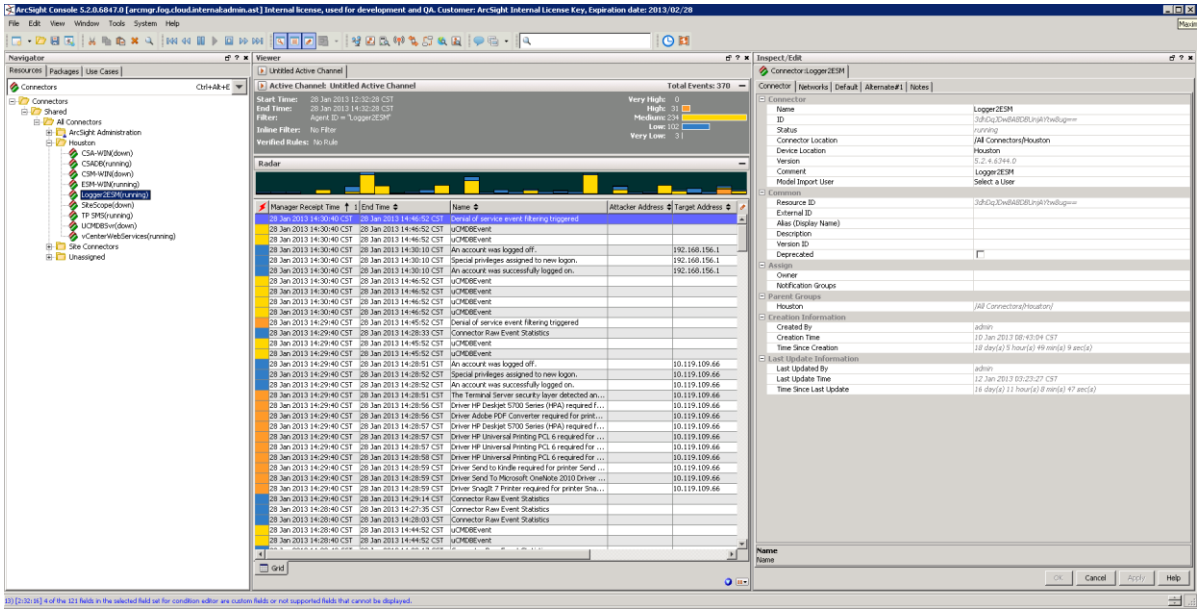


Looking at the Logger Analyze screen in Figure 30, we can see that the search criteria was failed logon in the Last 5 minutes. Out of 999 events that were logged during the five minute reporting period, four of these events were failed logons.

HP ArcSight ESM – Viewing Events with Active Channels

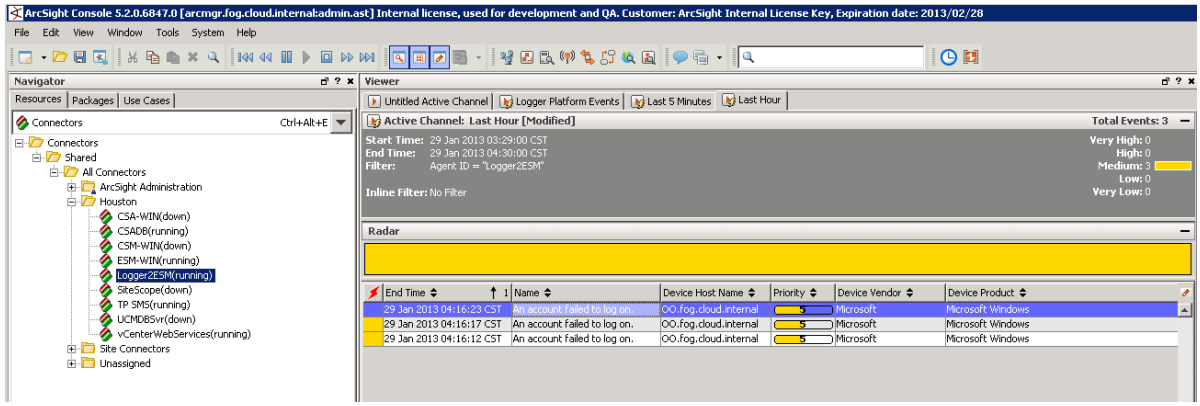
Events can be viewed in the ESM using an Active Channel. To view events forwarded to the HP ArcSight ESM from the ArcSight Logger, right click on the logger connector and set as current filter. This will display all current events as shown in Figure 31.

Figure 31. ArcSight EMS Manager Logger2ESM Connector



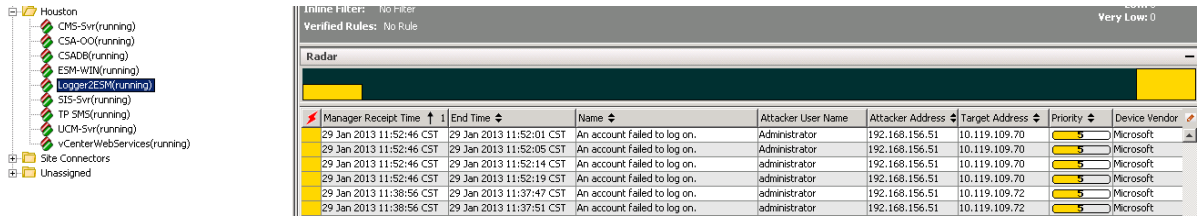
To test our failed login forwarder created earlier, we will attempt to login to oo.fog.cloud.internal. This server hosts our Cloud Service Automation and Operation Orchestration applications. By setting our Active Channel filter to the Logger2ESM Connector we can see in Figure 32 that the failed logon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

Figure 32. ESM view of Failed Logons



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



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 | Annotations | Payload

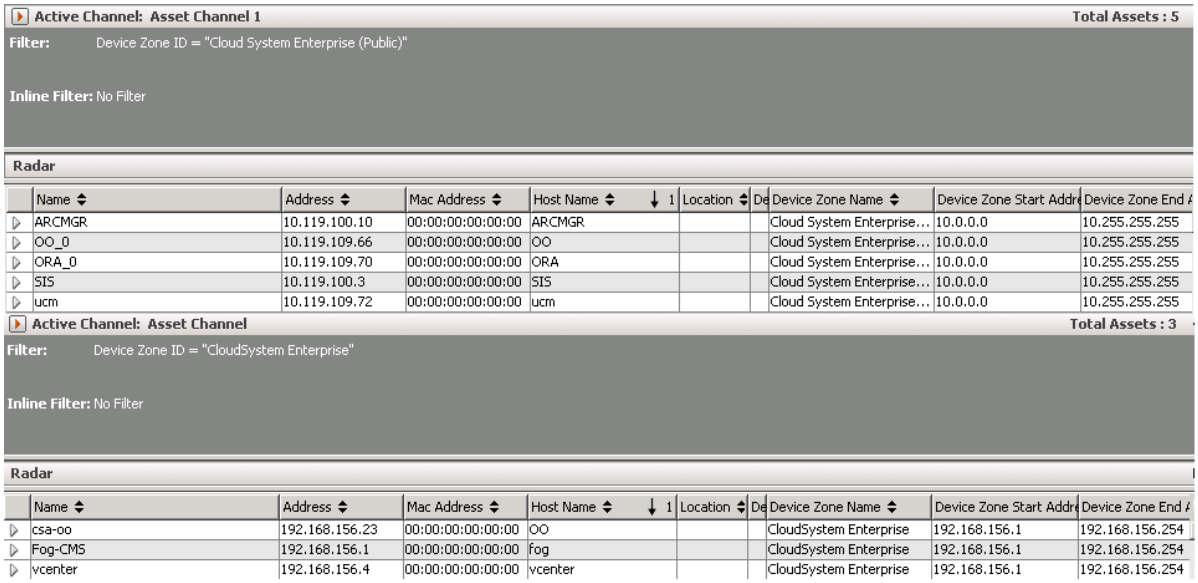
Event Inspector

Name	Value
Event	
Name	An account failed to log on.
Message	Network: A user or computer logged on to this computer from the network.
Type	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

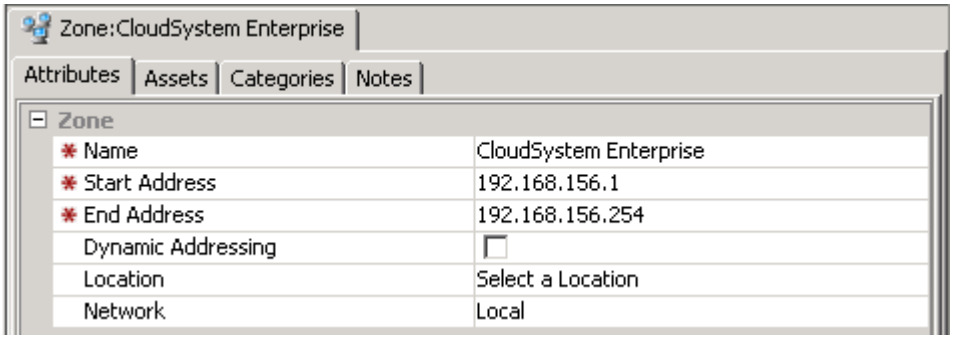
High value assets can be grouped into Zones. A Zone is based on a range of IP Addresses which can be used as a filter to search and view log activity.

Figure 35. ArcSight ESM Manager Zones



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

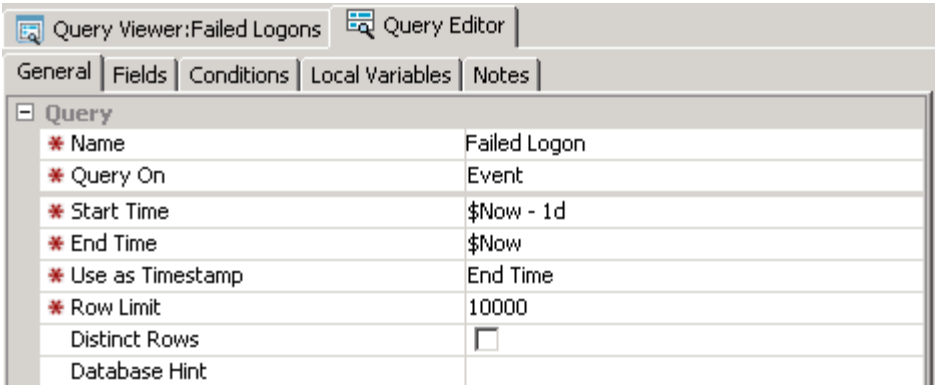


Queries

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.

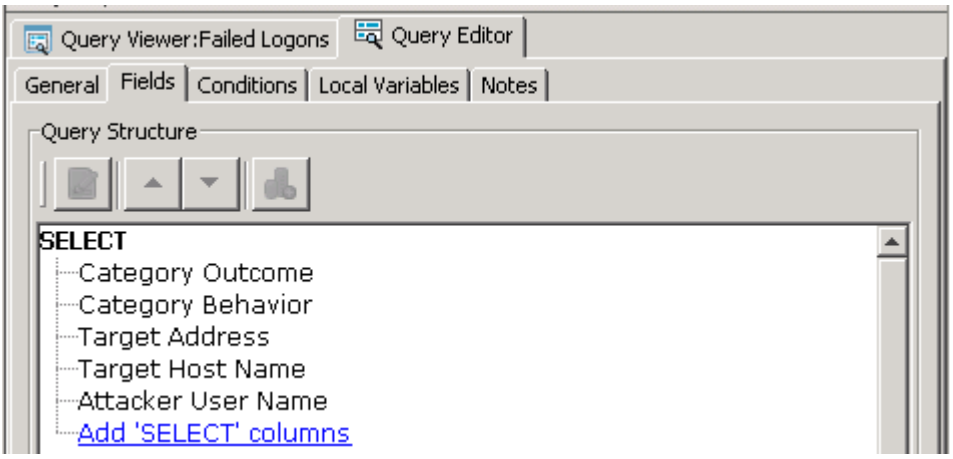
Launch the New Query pane and provide a Name for your query, in Figure 37 we've used Failed Login as the name for our query. Next we'll select the Fields tab to configure the fields that will be returned by the Query.

Figure 37. ESM Query Failed Logon – General



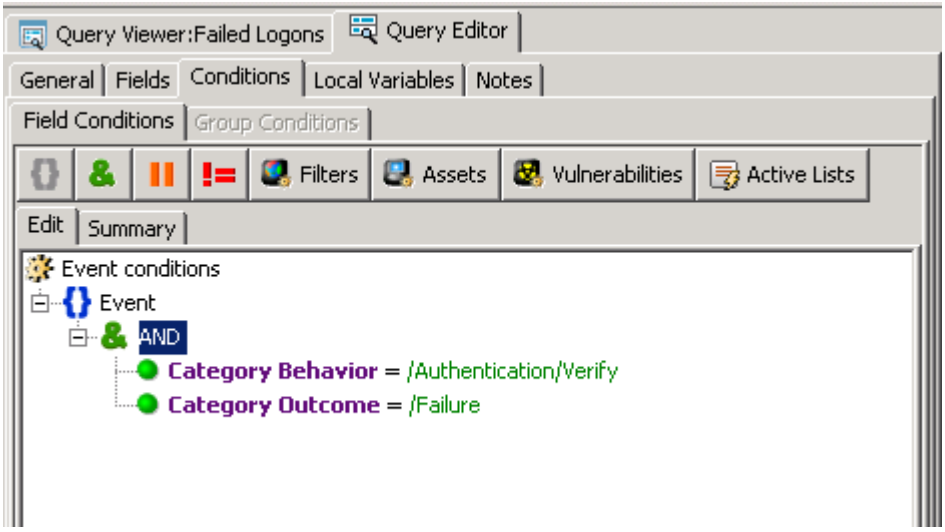
In the Fields tab we can select which event fields we want to return and display when the Query is executed. Using the failed logon event we'll display the Category Outcome, Category Behavior, Target Address, Target Host Name and Attacker User Name, as illustrated in Figure 38.

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.

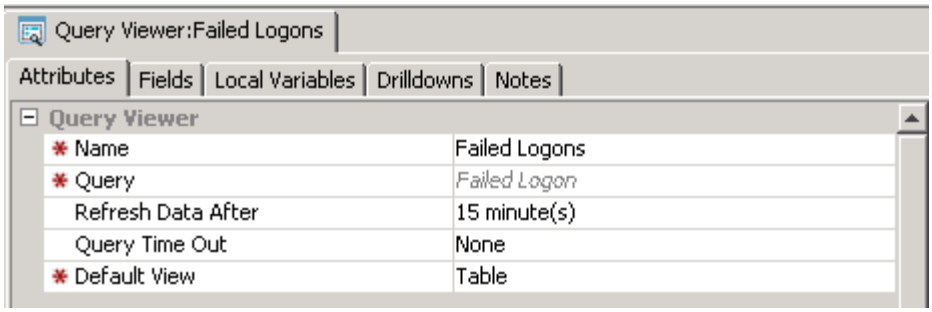
Figure 39. ESM Query Failed Logon – Conditions



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



* Name	Failed Logons
* Query	Failed Logon
Refresh Data After	15 minute(s)
Query Time Out	None
* Default View	Table

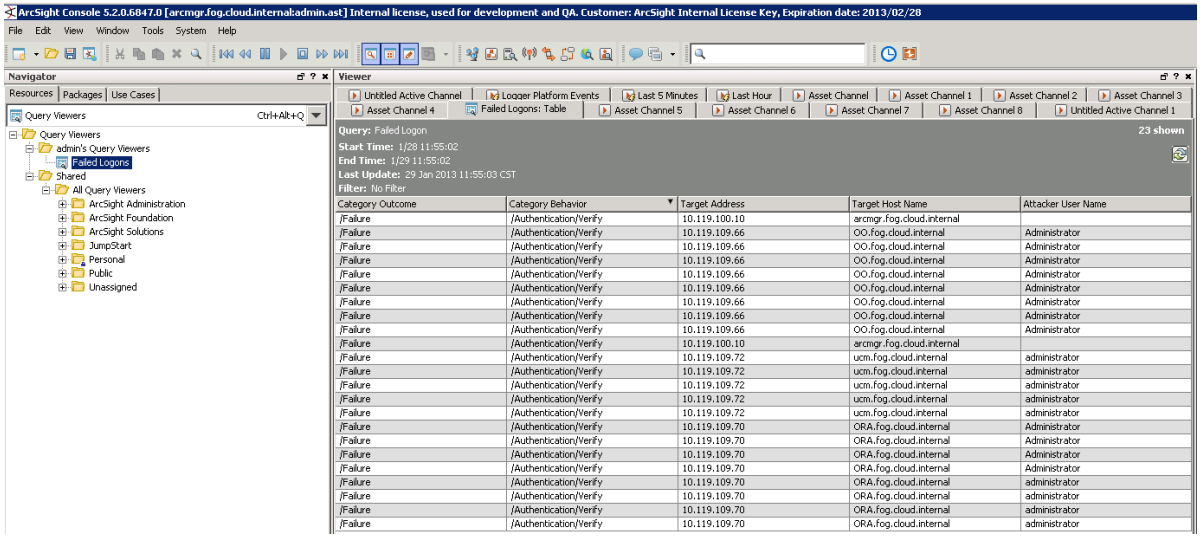
By default the Query data will be refreshed every 15 minutes.

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 5.2.0.6847.0 [arcmgr.fog.cloud.internal:admin.ast] Internal license, used for development and QA. Customer: ArcSight Internal License Key, Expiration date: 2013/02/28

Query: Failed Logon
Start Time: 1/28 11:55:02
End Time: 1/29 11:55:02
Last Update: 29 Jan 2013 11:55:03 CST
Filter: No Filter

23 shown

Category Outcome	Category Behavior	Target Address	Target Host Name	Attacker User Name
/Failure	/Authentication/Verify	10.119.100.10	arcmgr.fog.cloud.internal	
/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	10.119.109.66	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:

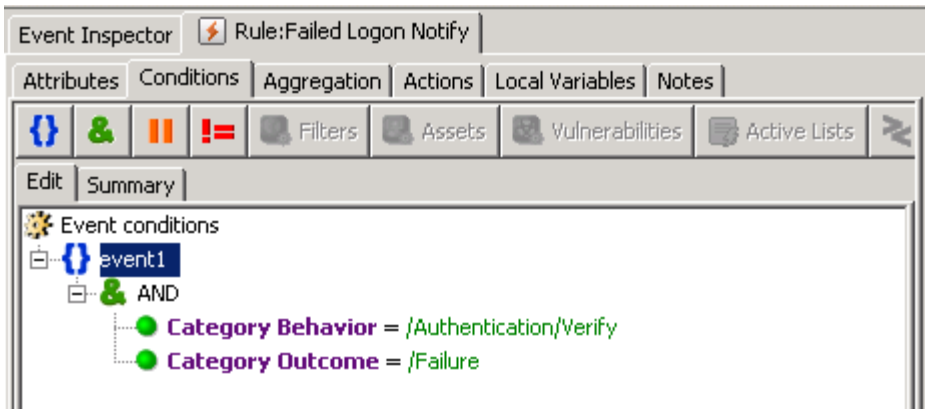
- oo.fog.cloud.internal - Operations Orchestration and Cloud Service Automation host)
- arcmgr.fog.cloud.internal – HP ArcSight ESM Manager and Console
- ucm.fog.cloud.internal – Universal Configuration Management Server
- ORA.fog.cloud.internal – Oracle Database server for UCMDB

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

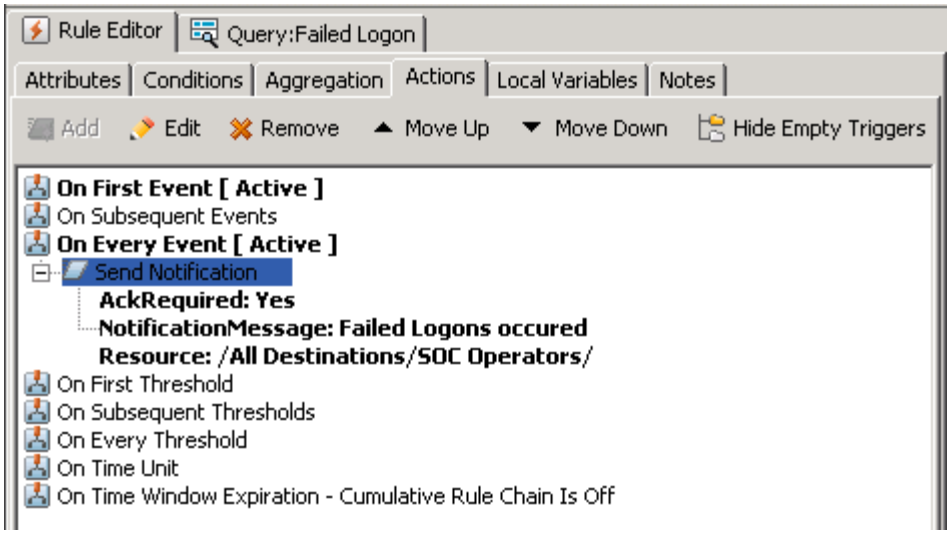


Next we'll configure the Aggregation tab, in this section we configure the rule to execute after a defined number of events occur within a specified time period on a single host, three times in two minutes, on the same Target Host Name. The fields of the events can be matched if they are the same or 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.

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".

```
#
# Arcsight's Silent Properties File
#
# Please edit this file to set the desired values
#
# Automatically generated on Thu Jan 24 13:02:52 EST 2013
#
#
# InstallAnywhere Installer Properties:
#
INSTALLER_UI=SILENT
USER_INSTALL_DIR=/root/ArcSightSmartConnectors
ARCSIGHT_AGENTSETUP_PROPERTIES=/tmp/ASLinuxAudit.props
# ============================================================
# Panel 'containeroperation'
# ============================================================
```

```
#   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
hpenterprisesecurity.com/products

To read more about CloudSystem Enterprise go to
hp.com/go/cloudsystementerprise

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

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

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

Sign up for updates
hp.com/go/getupdated

4AA4-5836ENW, March 2013