HPE Security ArcSight ESM

Software Version: 7.0

ArcSight Administration and ArcSight System Standard Content Guide

April 20, 2018

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notice

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Chapter 1: What is Standard Content?

Standard content is a series of coordinated resources, such as dashboards, active channels, reports, filters, rules, and so on that is designed to give you pre-installed comprehensive correlation, monitoring, reporting, alerting, and case management with minimal configuration. The standard content provides a comprehensive set of tasks that monitor the health of the system.

Standard content is installed using a series of packages (`.arb` files), some of which are installed automatically with the ArcSight Manager to provide essential system health and status operations. The remaining packages are presented as install-time options.

ArcSight Administration content contains several packages that provide statistics about the health and performance of ArcSight products:

- The ArcSight Administration content package is installed automatically with the ArcSight Manager and is essential for managing and tuning the performance of content and components.

- The ArcSight Admin DB CORR content package is installed automatically with the ArcSight Manager for the CORR-Engine (Correlation Optimized Retention and Retrieval) and provides information on the health of the CORR-Engine.

  > **Note:** The ArcSight Admin DB CORR content package is installed automatically when you perform a new ArcSight Manager installation. However package installation is different during upgrade. If you are upgrading your system from a previous version, check to see if the package is installed after upgrade. If the package is not installed, install it from the ArcSight Console.

- The ArcSight Content Management content package is an optional package that shows information about content package synchronization with the ArcSight Content Management feature. The information includes a history of content packages synchronized from a primary source to multiple destinations, and any common issues or errors encountered. You can install this package during ArcSight Manager installation or from the ArcSight Console any time after installation.

- The ArcSight Event Broker Monitoring content package is an optional package that lets you monitor activities with ArcSight Event Broker. If ESM is configured to consume events from Event Broker, you can install and use this package during ArcSight Manager installation or from the ArcSight Console any time after installation.

- The ArcSight ESM HA Monitoring content package is an optional package that lets you monitor systems that use the ESM High Availability Module. You can install this package during ArcSight Manager installation or from the ArcSight Console any time after installation.

- The ArcSight Search Filters content package is installed automatically with the ArcSight Manager. It is used to filter searches performed in the ArcSight Command Center. Note that this applies to a fresh ESM installation. For upgrades from earlier versions, the package in `/All Packages/ArcSight Administration/ArcSight Search Filters` are imported but require installation before you can use them.

ArcSight System content is installed automatically with the ArcSight Manager and consists of three packages: ArcSight Core, ArcSight Groups, and ArcSight Networks. ArcSight Core and ArcSight Groups contain resources required for basic security processing functions, such as threat escalation and priority calculations, as well as basic throughput channels required for ready-to-use functionality. The ArcSight Networks package contains zones, and local and global network resources. Zones are provided for IPv4 and IPv6 addresses.

> **Note:** ArcSight System resources manage core functionality. The resources are **locked** to protect them from unintended change or deletion.

ArcSight Foundation content contains the **Shared Libraries**, which are common resources that provide core functionality for common security scenarios:

- Conditional Variable Filters is a library of filters used by variables in standard content report queries, filters, and rule definitions.
- Global Variables contain a set of variables used to create other resources and to provide event-based fields that cover common event information, asset, host, and user information, and commonly used timestamp formats.
- Network filters contain a set of filters required by ArcSight Administration.

The following resources are packages that you install with the Manager.

> **Note:** The ArcSight Foundation content package is installed automatically when you perform a new ArcSight Manager installation. However package installation is different during upgrade. If you are upgrading your system from a previous version, check to see if the package is installed after upgrade. If the package is not installed, install it from the ArcSight Console.

- The ArcSight ClusterView is for ESM with distributed correlation. This resource group contains all the resources required to monitor the health of ESM distributed correlation cluster(s). The Cluster View dashboard is available on the ArcSight Command Center. This dashboard provides a visual map of your cluster configuration, EPS, available node services, connections, and cluster audit events. The ArcSight Console provides a ClusterView icon that changes color if something is wrong with connections. Users can click on the icon from the Console, which launches the Command Center dashboard. This ClusterView icon on the Console is disabled if you have ESM compact mode.

  On the Console, the ClusterView package is located at `/All Packages/ArcSight Foundation/ArcSight ClusterView`. However, the resources will not be functional in compact mode.

- The ArcSight SocView resource group contains all the resources that provide updated information to the security analysts working for the enterprise's Security Operations Center. Various data monitors displaying information such as Top Attacks, Malicious Activity, destination and source addresses, and so on, are assembled on the SOC Manager dashboard, which is available on the ArcSight Command Center.

  On the Console, the package is located at `/All Packages/ArcSight Foundation/ArcSight SocView`.

Downloads Groups contains folders used by the security use cases, which are separate content packages that address specific security needs, such as VPN Monitoring, Suspicious Outbound Traffic Monitoring, Anomalous Traffic Detection, Brute Force Attack, and Reconnaissance, to name a few. These use cases are available from the ArcSight Marketplace portal.

Note that this applies to a fresh ESM installation. For upgrades from earlier versions, the package in `/All Packages/Downloads` are imported but require installation.

> **Caution:** The resources in the ArcSight Administration, ArcSight DB CORR, Conditional Variable Filters, Global Variables, and Network Filters content packages are not locked even though they manage core functionality; HPE recommends that you do not delete or modify these resources unless you are an advanced user who understands fully the resources and their dependencies.

This document describes how to configure and use the standard content. For detailed information about using ArcSight ESM, see the ArcSight ESM documentation set, available as a unified help system from the ArcSight Console **Help** menu. PDF versions of the documentation set, as well as Security Use Case Guides, Release Notes, and individual SmartConnector Guides are available from Protect 724.

Chapter 2: Installation and Configuration

Standard content is required for basic functionality and is pre-installed on the ArcSight Manager. You do not have to perform any additional installation tasks. However, some basic configuration is recommended to tailor the content for your operating environment.

> **Note: ArcSight Content Management**, **ESM HA Monitoring**, and **Event Broker Monitoring** are *optional* packages provided in the ArcSight Administration package group. You can install either of these packages during ESM installation or from the ArcSight Console any time after installation.
>
> To install after installation, go to the **Packages** tab in the Navigator, open the ArcSight Administration group, right-click the package you want to install and select **Install Package**. After you install the package, the ArcSight Administration group on the Use Cases tab lists the content use cases.

For detailed information about installing ESM, refer to the ArcSight *ESM Installation Guide*.

The list below shows the general tasks you need to complete to configure content with values specific to your environment.

Modeling the Network

A network model keeps track of the network nodes participating in the event traffic. Modeling your network and categorizing critical assets using the standard asset categories is what activates some of the standard content and makes it effective.

There are several ways to model your network. For information about populating the network model, refer to the *ArcSight Console User's Guide*. To learn more about the architecture of the network modeling tools, refer to the *ESM 101 guide*.

Categorizing Assets

After you have populated your network model with assets, apply the standard asset categories to activate standard content that uses these categories.

Asset Category	Description
`/Site Asset Categories/` `Address Spaces/Protected`	Categorize all assets (or the zones to which the assets belong) that are internal to the network with this asset category. Internal Assets are assets inside the company network. Assets that are not categorized as internal to the network are considered to be external. Make sure that you also categorize assets that have public addresses but are controlled by the organization (such as web servers) as *Protected*.
`/System Asset Categories/` `Criticality/High`	Categorize all assets that are considered *critical* to protect (including assets that host proprietary content, financial data, cardholder data, top secret data, or perform functions critical to basic operations) with this asset category. The asset categories most essential to basic event processing are those used by the Priority Formula to calculate the criticality of an event. Asset criticality is one of the four factors used by the Priority Formula to generate an overall event priority rating.
`/System Asset Categories/` `Criticality/Very High`	Same as `/System Asset Categories/` `Criticality/High`

You can assign asset categories to assets, zones, asset groups, or zone groups. If assigned to a group, all resources under that group inherit the categories.

You can assign asset categories individually using the Asset editor or in a batch using the Network Modeling wizard. For information about how to assign asset categories using the ArcSight Console tools, refer to the *ArcSight Console User's Guide*.

For more about the Priority Formula and how it leverages these asset categories to help assign priorities to events, refer to the *ArcSight Console User's Guide* or the *ESM 101 guide*.

Configuring Active Lists

The standard content includes active lists. Certain active lists are populated automatically during run-time by rules. You do not have to add entries to these active lists manually before you use them. Other active lists are designed to be populated *manually* with data specific to your environment. After the lists are populated with values, they are referenced by active channels, filters, rules, reports, and data monitors to provide more information about the assets in your environment.

You can add entries manually to active lists using the following methods. Both methods are described in the *ArcSight Console User's Guide*.

- One by one using the Active List editor in the ArcSight Console.
- In a batch by importing values from a CSV file.

For a list of the ArcSight Administration active lists you need to configure manually, refer to the configuration information for each use case presented in"ArcSight Administration Content" on page 20.

For a list of the ArcSight System active lists you need to configure manually, refer to the configuration information for each resource group presented in "ArcSight System Content" on page 74

Configuring Filters

For a list of the ArcSight Administration filters you need to configure, refer to the configuration information for each use case presented in "ArcSight Administration Content" on page 20.

For a list of the ArcSight System filters you need to configure, refer to the configuration information for each resource group presented in "ArcSight System Content" on page 74.

Enabling Rules

Rules trigger only if they are deployed in the `/All Rules/Real-time Rules` group and are enabled.

- By default, all the **ArcSight System** rules are deployed in the `/All Rules/Real-time Rules` group and are also enabled.

- By default, all the **ArcSight Administration** rules are deployed in the `/All Rules/Real-time rules` group and all rules, are enabled except for all deployed rules under `/Logger/System Health`.

  You can enable the Logger System Health rules if you have a Logger connected to your system. The Logger System Health rules are described in "Logger Overview" on page 27.

- By default, the rules in the optional **Content Management** package under ArcSight Administration, are deployed in the `Real-time Rules` group but are disabled.

- By default, the rules in the optional **ArcSight ESM HA Monitoring** and **Event Broker Monitoring** packages under ArcSight Administration are deployed in the `Real-time Rules` group and are also enabled.

To enable or disable a rule:

1. In the Navigator panel, go to **Rules** and navigate to the Real-time Rules group.
2. Navigate to the rule you want to enable or disable.
3. Right-click the rule and select **Enable Rule** to enable the rule or **Disable Rule** to disable the rule.

Configuring Notifications and Cases

Standard content depends on rules to send notifications and open cases when conditions are met. Notifications and cases are how you can track and resolve the security issues that the content is designed to find.

By default, most notifications and create case actions are disabled in the standard content rules that send notifications about security-related events.

To enable rules to send notifications and open cases, first configure notification destinations (see "Configuring Notification Destinations" below), then enable the notification and case actions in the rules. For more information about working with Rule actions in the Rules Editor, refer to the *ArcSight Console User's Guide*.

Configuring Notification Destinations

Configure notification destinations if you want to be notified when some of the standard content rules are triggered. By default, most notifications are disabled in the standard content rules, so the admin user needs to configure the destinations *and* enable the notification in the rules.

The notification action is enabled by default in the following standard content rules:

- ArcSight Administration/Devices/**Alert - Critical Devices inactive for more than 1 hour**
- ArcSight Administration/ESM/HA Monitoring/**Alert - HA Status Change**
- ArcSight Administration/ESM/System Health/Resources/Domains/**Out of Domain Fields**
- ArcSight Administration/ESM/System Health/Storage/**ASM Database Free Space - Critical**

Make sure you configure notification destinations for the Device Administrators, SOC Operators, and the CERT team groups so that the notifications are received.

Refer to the *ArcSight Console User's Guide* for information on how to configure notification destinations.

Rules with Notifications to the CERT Team

The following rule is configured to send notifications to the **CERT Team** notification destination group.

Rule Name	Rule URI
Out of Domain Fields	ArcSight Administration/ESM/System Health/Resources/Domains/

Note: The notification action for the **Out of Domain Fields** rule is enabled by default. Make sure you configure destinations for the CERT team to receive notifications when this rule triggers.

Rules with Notifications to SOC Operators

The following rules are configured to send notifications to the **SOC Operators** notification destination group.

Rule Name	Rule URI
Connector Dropping Events	ArcSight Administration/Connectors/System Health/
Connector Still Down	ArcSight Administration/Connectors/System Health/
Connector Still Caching	ArcSight Administration/Connectors/System Health/
Excessive Rule Recursion	ArcSight Administration/ESM/System Health/Resources/Rules/
Rule Matching Too Many Events	ArcSight Administration/ESM/System Health/Resources/Rules/
ASM Database Free - Critical	ArcSight Administration/ESM/System Health/Storage/
Alert - HA Status Change	ArcSight Administration/ESM/HA Monitoring

Note: The notification action for the **ASM Database Free Space - Critical** and **Alert - HA Status Change** rules is enabled by default. Make sure you configure destinations for the SOC Operators group to receive notifications when these rules trigger.

Rules with Notifications to the Device Administrators Group

The following rule is configured to send notifications to the **Device Administrators** notification destination group:

Rule Name	Rule URI
Alert - Critical Devices inactive for more than 1 hour	ArcSight Administration/Devices/

Note: The notification action in this rule is enabled by default. Make sure you configure destinations for the Device Administrators group to receive notifications when this rule triggers. See .

Scheduling Reports

You can run reports on demand, automatically on a regular schedule, or both. By default, reports are not scheduled to run automatically.

Evaluate the reports that come with the content, and schedule the reports that are of interest to your organization and business objectives. For instructions about how to schedule reports, refer to the *ArcSight Console User's Guide*.

Configuring Trends

Trends are a type of resource that can gather data over longer periods of time and can then be leveraged for reports. Trends streamline data gathering to the specific pieces of data you want to track over a long range, and breaks the data gathering up into periodic updates. For long-range queries, such as end-of-month summaries, trends greatly reduce the burden on system resources. Trends can also provide a snapshot of which devices report on the network over a series of days.

ArcSight System content does not contain any trends. ArcSight Administration content includes trends, which are enabled by default. Majority of these enabled trends are scheduled to run on an alternating schedule between the hours of midnight and 7:00 a.m., when network traffic is usually less busy than during peak daytime business hours. Exceptions are two `/All Trends/Arcsight Administration/ESM` trends:

- `/Licensing/Storage Licensing Data` is scheduled to run daily at 10:52.22 a.m.
- `/System Health/Storage/ASM Database Free Space` is scheduled to run daily at 2:34 p.m.

You can customize these schedules to suit your needs using the Trend scheduler in the ArcSight Console.

To disable a trend, go to the Navigator panel, right-click the trend you want to disable and select **Disable Trend**.

> **Caution:** To enable a disabled trend, you must first **change the default start date** in the Trend editor.
>
> If the start date is not changed, the trend takes the default start date (derived from when the trend was first installed), and back fills the data from that time. For example, if you enable the trend six months after the first install, these trends try to get all the data for the last six months, which might cause performance problems, overwhelm system resources, or cause the trend to fail if that event data is not available.

For more information about trends, refer to the *ArcSight Console User's Guide*.

ArcSight Administration contains resources that enable you to monitor the performance of your enabled trends. The **Trend Details** dashboard in the **ESM Reporting Resource Monitoring** use case (described on page 63) shows the runtime status for all enabled trends. The trend reports show statistics about trend performance for all enabled trends.

Viewing Use Cases

ArcSight Administration resources are grouped together in the ArcSight Console in use cases. A use case groups a set of resources that help address a specific issue or business requirement.

Note: Currently, ArcSight System content does not contain any use cases. "ArcSight System Content" on page 74 documents System resources by grouping them by function.

To view the resources in a use case:

1. In the Navigator panel, select the **Use Cases** tab.
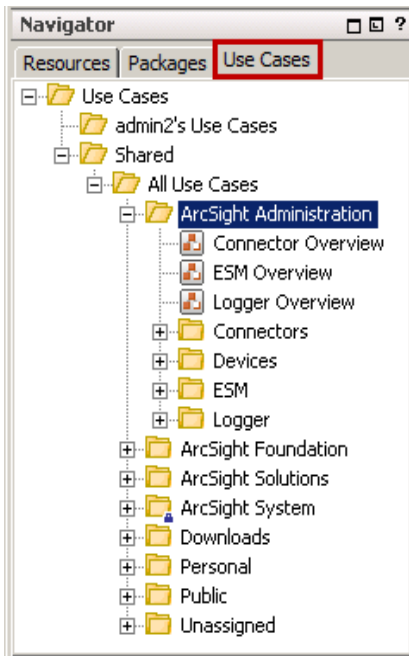
2. Browse for a use case; for example, ArcSight Administration/ESM Overview.

3. Right-click the use case and select **Open Use Case**, or double-click the use case.

The use case with its associated resources displays in the Viewer panel of the ArcSight Console.
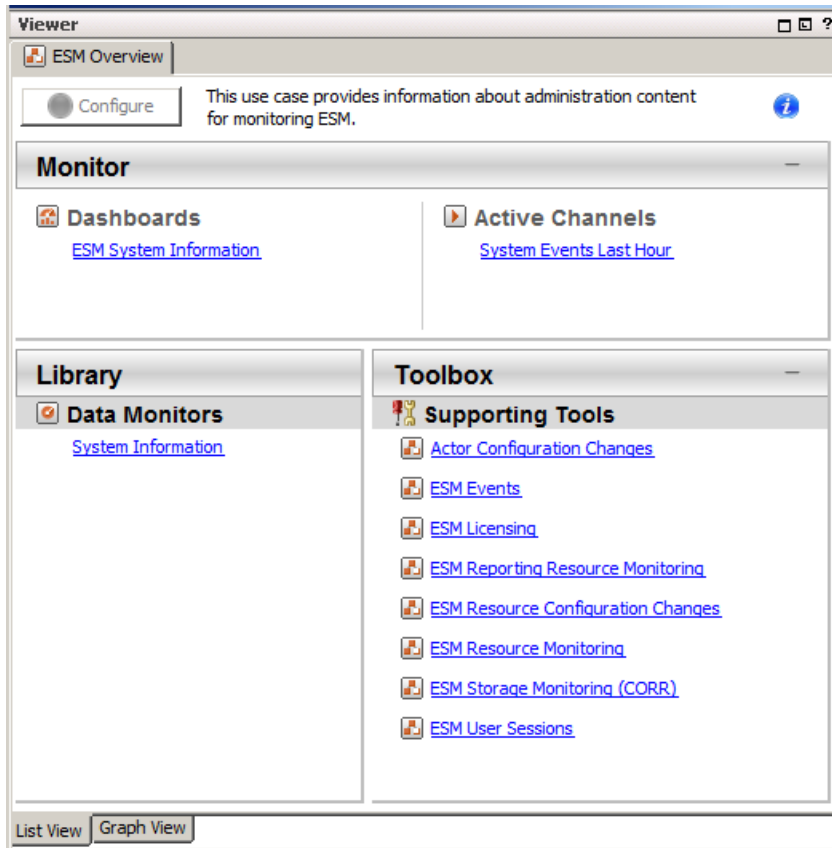
Chapter 3: ArcSight Administration Content

The ArcSight Administration resources provide statistics about the health and performance of the ArcSight system and its components. This content is essential for managing and tuning performance.

The ArcSight Administration use cases are listed in the table below.

> **Note:** ArcSight Administration relies on a series of common resources that provide core functions for common security scenarios. These common resources are located under the `Common` group. You can identify these resources by the URI; for example, `ArcSight Foundation/Common/ Network Filters/`.

Use Case	Purpose
Overview	
"Connector Overview" on page 22	Provides administration content for monitoring connectors and devices.
"ESM Overview" on page 24	Provides administration content for monitoring the system.
"Logger Overview" on page 27	Provides Logger status and statistics.
Connectors	
"Connector Configuration Changes" on page 29	Provides information about configuration changes (such as upgrades) and the versions of the connectors on the system.
"Connector Connection and Cache Status" on page 31	Provides the connection status and caching status of connectors on the system.
Devices	
"ArcSight ESM Device Monitoring" on page 34	Provides resources to help you monitor the status of devices that send events to connectors.
ESM	
"ESM Licensing" on page 41	Provides information about licensing compliance.
"ESM User Sessions" on page 43	Provides information about user access to the system.
ESM - Configuration Changes	
"Actor Configuration Changes" on page 45	Provides information about changes to the actor resources.
"ESM Resource Configuration Changes" on page 47	Provides information about changes to the various resources, such as rules, reports, and so on.
ESM - Content Management	

Use Case	Purpose
"Content Management" on page 49	Provides information about content package synchronization with the Content Management feature, including the history of content packages synchronized from a primary ESM source to multiple ESM destinations, and any common issues or errors encountered during synchronization.
ESM - HA Monitoring	
"High Availability Monitoring" on page 55	Provides resources to help you monitor the status of ESM systems that are using the optional ESM High Availability Module (HA Module). The HA Module provides for a backup ESM machine with automatic failover capability should the primary ESM machine experience any communications or operational problems.
ESM - Event Broker Monitoring	
"Event Broker Monitoring" on page 50	Provides resources to help you monitor the status of connectivity and event consumption between an ArcSight Event Broker deployment and ESM.
ESM - System Health	
"ESM Events" on page 61	Provides statistics on the flow of events through the system.
"ESM Reporting Resource Monitoring" on page 63	Provides performance statistics for reports, trends, and query viewers.
"ESM Resource Monitoring" on page 65	Provides processing statistics for various resources, such as trends, rules, and so on.
"ESM Storage Monitoring (CORR-Engine)" on page 68	Provides information on the health of the CORR- (Correlation Optimized Retention and Retrieval) Engine. This does not apply if you are using ESM with the Oracle database.
Logger	
"Logger Events" on page 70	Provides statistics for events sent through a Logger.
"Logger System Health" on page 71	Provides performance statistics for any Logger connected to the system.

Connector Overview

The Connector Overview use case provides resources to help you monitor connectors and devices.

Configuring the Connector Overview Use Case

The Connector Overview use case uses the following active lists from the Connector Connection and Cache Status use case:

- **Connector Information**
- **Connectors - Caching**
- **Connectors - Down**
- **Connectors - Dropping Events**
- **Connectors - Still Caching**
- **Connectors - Still Down**
- **Black List - Connectors**

For information about configuring these active lists, refer to the configuration section in "Connector Connection and Cache Status" on page 31.

Using the Connector Overview Use Case

The **Connector Overview** use case is located in /All Use Cases/ArcSight Administration on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two dashboards to help you monitor the status of your connectors and see the top devices that are contributing events. The Library section of the use case lists supporting resources.

Viewing the Dashboards

To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel.

- The **Current Event Sources** dashboard shows the top 20 devices that are contributing events. The device vendor and product type are listed.

- The **Connector Connection and Cache Status** dashboard displays the overall status of connectors and provides information about connectors that are down, caching, or dropping events. An example dashboard is shown below.
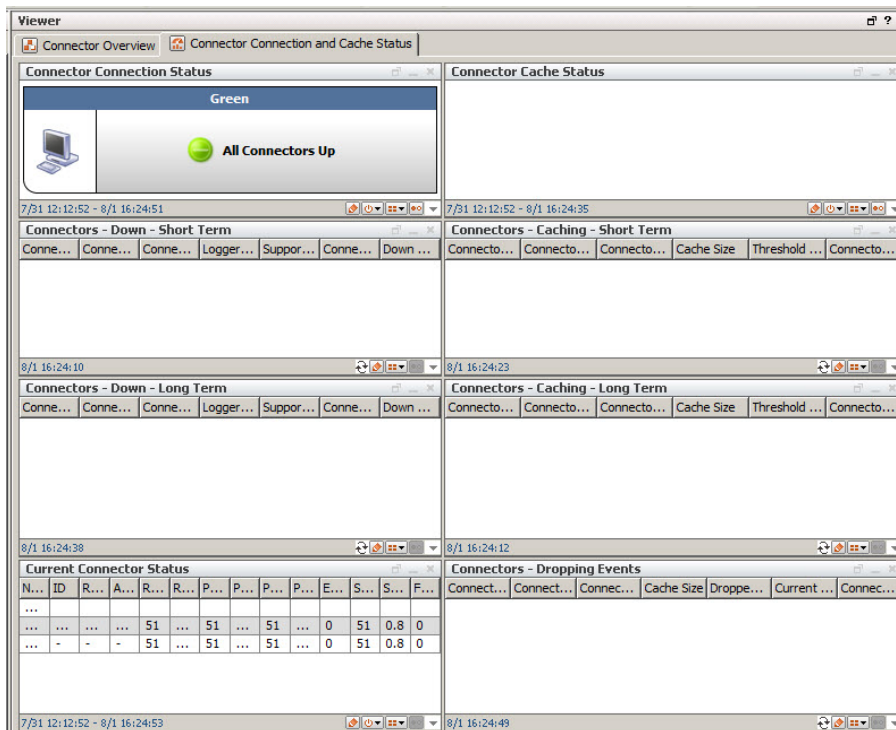
Focus on any yellow or red icons, as they represent connectors that might require attention.

The **Connectors - Down - Short Term** and **Connectors - Down - Long Term** query viewers show connectors that have been down for less than 20 minutes (yellow icons) and for more than 20 minutes (red icons). Down time of less than 20 minutes might be acceptable; for example, scheduled maintenance of the host machine on which the connector is installed. However, more than 20 minutes might indicate an issue that requires investigation. Maybe the connector is configured improperly or needs to be restarted; or there is an underlying network, connection, or hardware problem.

You can find more information about each connector in the **Connector Connection Status** and **Connector Cache Status** data monitors. Check the **Failed Connection Attempts** column to see if the connector is repeatedly failing to connect to the ArcSight Manager. (You might need to undock the component to see this column on the far right side.)

The components on the right side of the dashboard show connectors that are caching events instead of sending them to the ArcSight Manager. Short term caching (for less than two hours) is expected behavior when the connector receives bursts of events or when the ArcSight Manager is down. However, investigate long term caching (more than two hours), as it can result in a full cache and the permanent loss of events. Check the **Cache Size** and **Threshold Size** columns to determine if the cache is nearing its maximum capacity. Check to see if events have been dropped. If so, review the connector logs and ArcSight Manager logs for errors, and adjust the connector configuration properties as needed.

For answers to frequently asked questions about caching, see the *ArcSight SmartConnectors User's Guide*. For configuration information about a specific connector, see the configuration guide for that connector. For information about connector caching issues, check the Protect 724 community.

ESM Overview

The ESM Overview use case provides resources that help you monitor the ArcSight system. No configuration is required for this use case.

Using the ESM Overview Use Case

The **ESM Overview** use case is located in /All Use Cases/ArcSight Administration on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides the **ESM System Information** dashboard to help you monitor your ArcSight system and the **System Events Last Hour** active channel to help you investigate generated events. The Library section of the use case lists supporting resources that help compile information in the dashboard and active channel.

Viewing the Dashboard

To view the **ESM System Information** dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel and displays important information about the ArcSight system, such as the version, license, total amount of memory available to the system, and the amount of used memory. System resource availability and statistics, and other important settings are also shown. Following is an example dashboard:

```
ESM System Information                                                         _ □ ▣ ?

  System Information                                                         ⬚ _ ✕

    Arcsight:service=NGServer
    ActiveThreadCount                      283
    ArcSightSystemVersion                  6.11.0.32217.0
    BaseURL                                
    ClusterId                              default
    CrossDomainEnabled                     false
    GlobalDebugEnabled                     false
    HostInformation                        
    ID                                     k5u4iVkBABCAW9qxjyv2mA==
    LastGeneratedThreadDump                null
    LastThreadDump                         null
    Location                               default
    LogLevel                               1
    MaxMemory                              15937M (16711155712 bytes)
    OS                                     Linux (amd64), Version 3.10.0-514.el7.x86_64
    PersistEvents                          true
    ProcessorCount                         24
    Ready                                  true
    ReportLicenseKey                       S000-758-ERX-0000BF002000006-F29D3F2339F7
    RulesCheckpointRecoveryComplete        true
    ServiceSessionTimeout                  900
    SessionCount                           5
    SessionUserInfo                        [Name:        , ID:1dPe2iVkBABCA3GSPu76eKg==, TotalL...
    StartTimestamp                         Wed Jan 11 23:24:09 PST 2017
    TotalMemory                            15937M (16711155712 bytes)
    Uptime                                 182hr 44min 42sec
    UsedMemory                             12632M (13245860336 bytes)
    VersionID                              BE32217_1-10-2017_1:7:24
    XmlRpcDebug                            false


  1/11 23:24:37 - 1/19 14:08:51                                        ⟳ ⏻▼ ▦▼ ▬▼ ▼

  Data last refreshed: 1/19 14:08:54                                              ●
```

Some of the information on this dashboard is for internal system use.

System Information Dashboard

System Information	Meaning
Arcsight:service=NGServer	Standard naming convention for the ESM server
ActiveThreadCount	(For internal system use)
ArcSight SystemVersion	ESM release version number, including build number
BaseURL	The URL to the ESM server
ClusterId	(For internal system use)
CrossDomainEnabled	Whether or not the server is enabled for cross-domain requests
GlobalDebugEnabled	(For internal system use)
Host Information	The ESM host name and IP address
ID	Resource ID for the ESM server system as shown in /All Assets/ArcSight System Administration/Managers/<*ESM server*>
LastGeneratedThreadDump	(For internal system use)
LastThreadDump	(For internal system use)
Location	The physical location of the Manager server, entered during setup (`managersetup` wizard). Shows `default` if nothing was entered.

System Information Dashboard, continued

System Information	Meaning
LogLevel	(For internal system use)
MaxMemory	Returns the maximum amount of memory that the Java virtual machine will attempt to use. If there is no inherent limit then the value java.lang.Long.MAX_VALUE will be returned.
OS	Operating system platform on which the ESM server is installed
PersistEvents	Events are persisted on the database
Processor Count	Number of CPU cores on the system
Ready	System is ready
ReportLicenseKey	Unique license key for the ESM Report Template Designer (InetSoft)
RulesCheckpointRecoveryComplete	Denotes the completion of the rules checkpoint process. See the *ESM Administration Guide* for information on the rules checkpoint process.
ServiceSessionTimeout	(For internal system use)
SessionCount	Number of concurrent sessions to ESM using ArcSight Console, ArcSight Command Center, and ESM Web Services.
SessionUserInfo	Login name of the user viewing this dashboard, including the resource ID corresponding to that ESM user.
StartTimeStamp	Date and time when Manager was last started.
TotalMemory	Returns the total amount of memory in the Java virtual machine. The value returned may vary over time, depending on the host environment.
Uptime	Amount of time the system was up and running
UsedMemory	Current Java memory used by ESM
VersionID	ESM build number; concurs with ArcSightSystemVersion
XmlRpcDebug	(For internal system use)

Viewing the Active Channel

To view the **System Events Last Hour** active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel and shows all events generated by the ArcSight system during the last hour. A filter prevents the active channel from showing events that contributed to a rule triggering, commonly referred to as correlation events. Double-click an event to see details about the event in the Event Inspector.

Logger Overview

The Logger Overview use case provides resources to help you monitor Logger status and statistics.

Configuring the Logger Overview Use Case

If you have a Logger connected to your ArcSight system, follow the steps below to configure the Logger Overview use case:

To configure the Logger Overview use case:

1. Enable the following rules in the `/All Rules/Real-time Rules/ArcSight Administration/Logger/System Health` folder:

   - **Logger Sensor Status**—This rule detects Logger system health events related to hardware sensor status. The rule updates the Logger Status and Logger Sensor Type Status active lists with the Logger address, sensor type, sensor name, and sensor status.

   - **Logger Sensor Type Status**—This rule detects Logger Sensor Status correlation events and triggers only if all the sensor statuses for the same sensor type for a Logger indicate OK.

   - **Logger Status**—This rule detects Logger Sensor Status correlation events and triggers only if all the sensor statuses for a Logger indicate OK.

     For information about enabling rules, refer to .

2. Edit the **My Logger** filter in the `/All Filters/ArcSight Administration/Logger/System Health` folder. On the **Filter** tab, change the **Device Address** in the condition from the default 127.0.0.1. to the IP address of your Logger.

3. Enable the following data monitors.

   - **Logger Hardware Status**

   - **Logger Disk Usage**

   - **Network Usage (Bytes) - Last 10 Minutes**

   - **Disk Usage**

   - **CPU Usage (Percent) - Last 10 Minutes**

   - **EPS Usage (Events per Second) - Last 10 Minutes**

   - **Memory Usage (Mbytes per Second) - Last 10 Minutes**

   - **Disk Read and Write (Kbytes per Second) - Last 10 Minutes**

   - **Sensor Type Status**

> **Note:** These data monitors are disabled by default to avoid increasing the load on environments without a Logger.

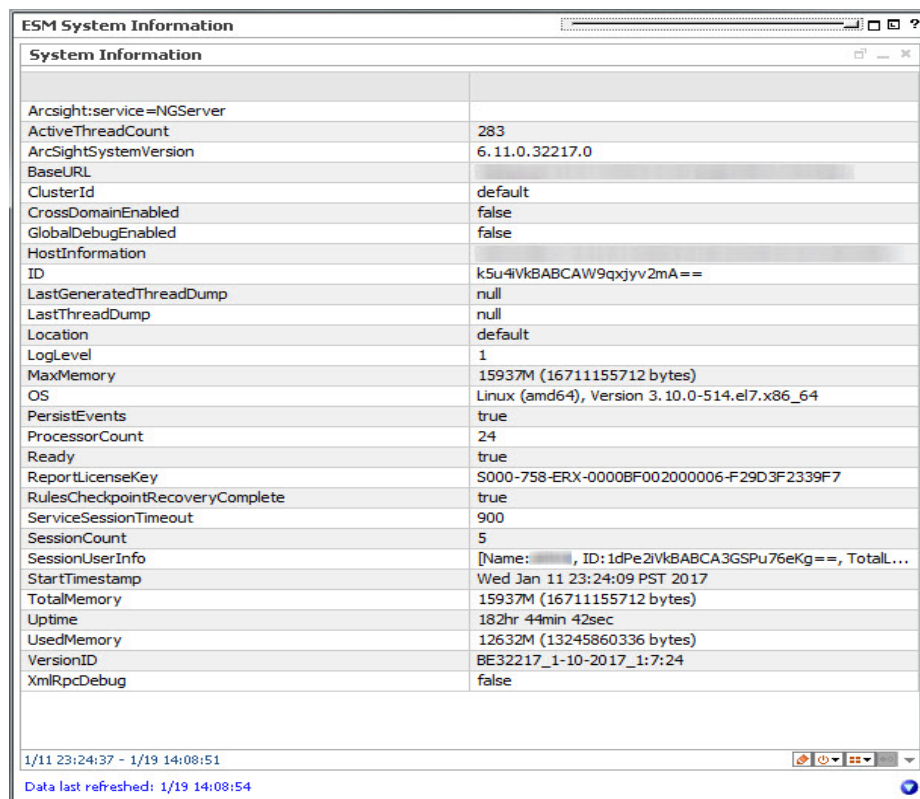For information about data monitors, refer to the *ArcSight Console User's Guide*.

Using the Logger Overview Use Case

The **Logger Overview** use case is located in /All Use Cases/ArcSight Administration on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two dashboards to help you monitor all your ArcSight appliances and the hardware, storage, CPU, memory, network, and EPS usage for a specific Logger. The Library section of the use case lists supporting resources that help compile information in the dashboards.

Viewing the Dashboards

To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below:

- **ArcSight Appliances Overview** - Review the data monitors on this dashboard to check your ArcSight appliances. Focus on any red icons, as they represent appliances that might require attention. Examine the disk status for all appliances; a warning or critical status requires your attention.

- **My Logger Overview** - Review the data monitors on the dashboard to check the hardware, storage, CPU, memory, network, and EPS usage for the Logger defined in the My Logger filter. The information is collected during the last ten minutes.

> **Note:** The data monitors in the **My Logger Overview** and **ArcSight Appliances Overview** dashboards are disabled by default to avoid increasing the load on environments without Logger. Enable these data monitors if you have a Logger in your environment as described in "Configuring the Logger Overview Use Case" on the previous page.

Connector Configuration Changes

The Connector Configuration Changes use case provides information about configuration changes (such as upgrades) and the versions of the connectors on the system. No configuration is required for this use case.

Using the Connector Configuration Changes Use Case

The **Connector Configuration Changes** use case is located in /All Use Cases/ArcSight Administration/Connectors on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides an active channel to help you monitor connector upgrades, and several reports that show the status and historical information about connector upgrades. The Library section of the use case lists supporting resources that help compile information in the active channel and the reports.

Viewing the Active Channel

To view the **Connector Upgrades** active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel and displays all events related to connector upgrades received within the last two hours. The active channel uses the Connector Upgrades field set. Use this active channel as a baseline for your monitoring.

Running Reports

The **Connector Configuration Changes** use case provides several reports that show connector upgrade history. You can provide these historical reports to the stakeholders in your company, when needed.

By default, the reports use data for the last week from the time you run the report. You can change the start and end time of the report for longer- or shorter-term analysis when you run the report.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below.

- The **Connector Upgrades Count** report shows the total count of successful and failed connector upgrades in a pie chart and the counts per day in a table.

- The **Connector Versions** report lists all the connectors with their latest versions, grouped by connector type, connector zone, and connector address.

- The **Connector Versions by Type** report lists all the connectors by connector type, grouped by connector version, connector zone, and connector address.

- The **Failed Connector Upgrades** report lists the connectors with failed upgrades, grouped by connector zone, connector address, connector name, and connector ID. The report also shows the reason for the failure.

- The **Successful Connector Upgrades** report lists the connectors with successful upgrades, sorted chronologically.

- The **Upgrade History by Connector** report shows the upgrade history by connector sorted chronologically. When running this report, use the connector ID located in the connector resource and copy-paste the ID into the ConnectorID field in the Custom Parameters for the report.

- The **Upgrade History by Connector Type** report shows the upgrade history by connector type, grouped by connector zone, connector address, connector name, and connector ID.

- The **Version History by Connector** report shows the version history by connector, sorted chronologically. When running this report, use the connector ID (located in the connector resource) and copy-paste it in to the ConnectorID field in the Custom Parameters for the report.

- The **Version History by Connector Type** report shows the version history by connector type, grouped by connector zone, connector address, connector name, and connector ID.

Connector Connection and Cache Status

The Connector Connection and Cache Status use case provides the connection status and caching status of connectors on the system. Connectors can be connected directly to the ArcSight system or through Loggers.

Configuring the Connector Connection and Cache Status Use Case

The Connector Configuration and Cache Status use case requires the following configuration for your environment:

Customize the following active lists:

- In the **Connectors - Down** active list, adjust the Time to Live (TTL) attribute, if needed.
  By default, the TTL is set to 20 minutes. A connector down for fewer than 20 minutes is considered to be down for a short term. After 20 minutes, the entry for this active list expires and the connector information is moved to the **Connectors - Still Down** active list, unless the connector comes back up before 20 minutes.

- In the **Connectors - Caching** active list, adjust the Time to Live (TTL) attribute, if needed. By default, the TTL is set to two hours. A connector that has been caching for fewer than two hours is considered to be caching for a short term. Connectors caching for up to two hours are not considered to be a problem. After two hours, the entry for this active list expires and the connector information is moved to the **Connectors - Still Caching** active list, unless the connector cache is emptied in fewer than two hours, and it is removed by the Connector Cache Empty rule.

- Populate the **Black List - Connectors** active list with the URI and IP address of each connector you want to exclude from being evaluated by the Connector UP and Connector Down rules. These rules detect connectors that are started and are reporting events, and those that are shut down. These rules can send a notification (if notifications are enabled) when the connectors have been down for a certain period of time. You might want to exclude connectors that you start and stop manually, connectors that are scheduled to run once every week (such as vulnerability scanners), or connectors that you are testing (starting and stopping frequently during the setup process).

- *Optional*: Populate the **Connector Information** active list with the contact information for each connector, if needed. For example, you can add contact information for connectors maintained by other individuals or organizations. Add the contact information in the Support Information field in the format provided (poc= | email= | phone= | dept= | action=).

  The Connector Information active list collects information about connectors that have reported into the system, as well as information from the ArcSight Manager when the connector is first registered.

Do not add information to this active list for connectors that are not already reported into the system and registered.

For information about how to configure an active list, refer to the *ArcSight Console User's Guide*.

Using the Connector Connection and Cache Status Use Case

The **Connector Connection and Cache Status** use case is located in `/All Use Cases/ArcSight Administration/Connectors` on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides a dashboard, two active channels and two reports to help you monitor connector connection and status. The Library section of the use case lists supporting resources that help compile information in the dashboard, active channels, and reports.

Viewing the Dashboard

To view the **Connector Connection and Cache Status** dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel and displays the status of your connectors in real time. You can see which connectors have been down for a short time or a long time, and which connectors are dropping or caching events. Use this dashboard as a baseline for your monitoring. Investigate any connectors that have been down for a long period of time and any connectors that are dropping or caching events.

Viewing the Active Channels

The **Connector Connection and Cache Status** use case provides two active channels. To open an active channel in the Viewer panel, click the link for the active channel in the use case.

- The **Connector Caching Events** active channel shows information about connector *cache* status audit events and correlation events from the related connector monitoring rules.

- The **Connector Connection Status Events** active channel shows information about connector *connection* status audit events and correlation events from the related connector monitoring rules.

Running Reports

The **Connector Connection and Cache Status** use case provides two reports that show connector cache history and connector status. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.

2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below.

- **Cache History by Connectors** shows the cache history by connector, sorted chronologically. By default, the report shows all of the connectors known by the system. You can specify the connector URI (located in the Connector Information active list) in the ConnectorURI field in the custom parameters for the report to narrow down the connector cache histories reported, from groups (such as `/All Connectors/Site Connectors/`) to a specific connector (such as `/All Connectors/Site Connectors/DMZ/WUC-1`). The default time range of this report is the past three to four months.

- **Current Cache Status** lists the connectors that are currently caching and dropping events.

ArcSight ESM Device Monitoring

The ArcSight ESM Device Monitoring use case enables you to monitor the status of ArcSight ESM devices that send events to SmartConnectors (connectors). You can monitor all devices continuously and detect inactive devices promptly with minimum impact on the ArcSight ESM system. For example, you can see which firewall is inactive, which web server is new, and if a critical device is inactive for more than one hour.

A connector can use the Device Status Monitoring (DSM) feature to generate Connector Device Status events periodically reporting the status of each device communicating with it. A device is a unique combination of these five fields: deviceHostName, deviceVendor, deviceProduct, deviceZone, and customer.

When a device is sending base events to the connector and the connector is receiving them, the status of a device is *active*. When a connector receives no events from a device for a set period of time, the status of a device is *inactive*. The inactive status does not provide details about the network status, hardware or software issues on the device or connector.

> **Note:** The ArcSight ESM Device Monitoring content monitors devices that send events to SmartConnectors (connectors that work on security events). The content does not support Model Import connectors.

Understanding Connector Device Status Events

When DSM is enabled, the connector generates a `Connector Device Status` internal event for each device it is tracking. The event contains the information in the following table.

To enable DSM, see "Configuring the ArcSight ESM Device Monitoring Use Case" on the next page.

Connector Device Status Event Fields	Field Value
Event Name	Connector Device Status
Device Event Class ID	agent:043
Device Custom String1	device vendor (from the base events received from the device)
Device Custom String2	device product (from the base event received from the device)
Device Custom Number1	total event count (total number of events for this device since the SmartConnector started)
Device Custom Number2	event count SLC (since last check) (number of events for this device since the last internal event was sent)

Connector Device Status Event Fields	Field Value
Source Address	device address (source device sending base events to the connector)
Source Hostname	device hostname (source device sending base events to connector)
Device Custom Date1	Last Event Received (connector time when the last event was received from the device)
deviceEventCategory	/Agent/Connection/Device/Status
agentSeverity	low
deviceVendor	ArcSight
deviceProduct	ArcSight

When a new device sends the first event to the connector, the connector starts generating the Connector Device Status events for this device. The **All Monitored Devices** rule is configured to trigger when the Connector Device Status events have a non-zero Device Custom Number2 (indicating that the device is active and sending base events to the connector since the last check).

Configuring the ArcSight ESM Device Monitoring Use Case

The ArcSight ESM Device Monitoring use case requires the following configuration for your environment:

1. Enable Device Status Monitoring (DSM) on your connector. When DSM is enabled, a `Connector Device Status` internal event is sent for each device tracked by the connector with the following information: the last time the connector received an event from the device, the total number of events from this device since the connector started, and the number of events sent by this device since the last check.

    a. On the **Resources** tab of the ArcSight Console Navigator panel, go to **Connectors**, right click the connector on which you want to enable DSM, then select **Configure**.

    The **Inspect/Edit** panel for the Connector Editor opens. On the **Connector** tab, the **Name** field is populated automatically with the name assigned during connector installation.

    b. On the **Default** tab, set the **Enable Device Status Monitoring (in millisec)** option.

    By default, DSM is disabled on a connector; the **Enable Device Status Monitoring (in millisec)** option is set to -1. The minimum positive value you can assign is one minute (60000 milliseconds).

    > **Caution:** Enabling DSM can create a heavy load on busy connectors. HPE recommends that you set DSM to ten minutes or more; for example, 600000.

    c. Restart the connector.

2. Populate the **Critical Monitored Devices** active list with the devices that are critical in your

environment. This active list is then updated automatically when the Critical Monitored Devices rule triggers. The **Critical Monitored Devices** dashboard shows only the devices included in this active list.

To add devices that are critical to your environment, you can export the specific devices from the **All Monitored Devices** active list and import them to the **Critical Monitored Devices** active list. If you have a predefined list of critical devices, you can import a csv file containing all your critical devices to the **Critical Devices** active list. When the Critical Monitored Devices rule triggers, the entries from the **Critical Devices** active list are added to the **Critical Monitored Devices** active list.

3. Populate the **Whitelisted Monitored Devices** active list with the devices that you do not want to monitor. For example, include in this active list non-critical devices or devices that only respond once a day. The **Whitelisted Monitored Devices** active list is used in the **All Monitored Devices** rule condition.

4. Configure notification destinations for the Device Administrators group so that the correct administrators are notified when the **Alert - Critical Devices inactive for more than 1 hour** rule triggers. The send notification action in the **Alert - Critical Devices inactive for more than 1 hour** rule is enabled by default. For details on how to configure notification destinations, refer to the *ArcSight Console User's Guide*.

Using the ArcSight ESM Device Monitoring Use Case

The **ArcSight Device Monitoring** use case is located in `/All Use Cases/ArcSight Administration/Devices` on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two dashboards, an active channel, and several reports to help you monitor your ESM devices, including critical assets, and investigate device status events. The Library section of the use case lists supporting resources that help compile information in the dashboards, active channel, and reports.

Viewing the Active Channel

To view the **ArcSight ESM Device Monitoring** active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel and shows all Device Status events received within the last two hours. Double-click an event to see details about the event in the Event Inspector.

Viewing the Dashboards

The **ArcSight Device Monitoring** use case provides two dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

> **Tip:** View the dashboards for short-term activity and inactivity monitoring (for example, 20 minutes to one hour). For longer term activity, run the ArcSight ESM Device Monitoring reports. See "Running Reports" on page 39.

All Monitored Devices Dashboard
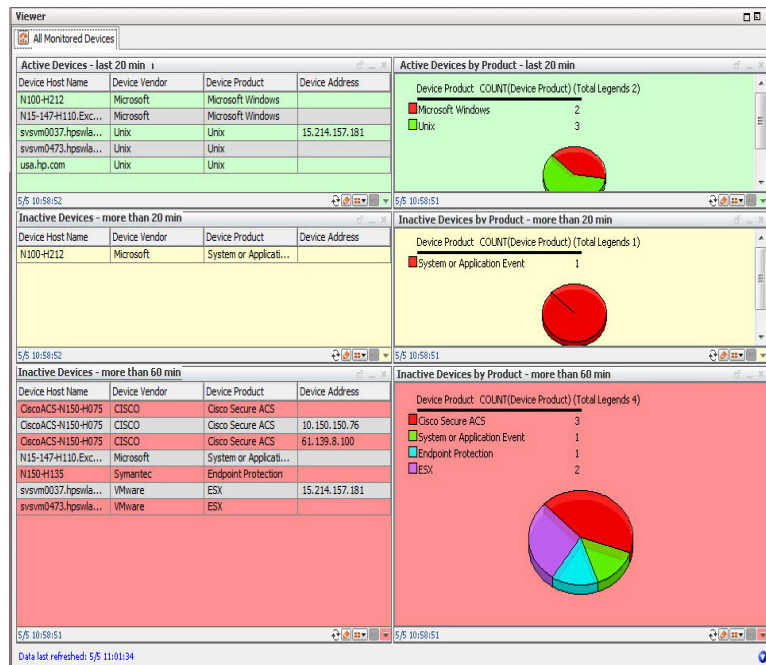
This dashboard provides query viewers that show information about all known devices (all the devices in the **All Monitored Devices** active list). The query viewers are color coded so you can identify problems quickly.

- The **Active Devices - last 20 min** query viewer displays information about devices that have reported events within the last 20 minutes. The **Active Devices by Product - last 20 min** query viewer displays the number of devices that have reported events within the last 20 minutes, in a pie chart by device product type.

- The **Inactive Devices - more than 20 min** query viewer displays information about devices that have not reported events within the last 20 minutes but have reported events within the last 60 minutes. The **Inactive Critical Devices by Product - more than 20 min** query viewer displays the number of devices that have not reported events within the last 20 minutes but have reported events within the last 60 minutes, in a pie chart by device product type.

- The **Inactive Devices - more than 60 min** query viewer displays information about devices that have not reported events within the last 60 minutes. The **Inactive Devices by Product - more than 60 min** query viewer displays the number of devices that have not reported events within the last 60 minutes, in a pie chart by device product type.

  Focus on the devices in the **Inactive Devices - more than 60 min** query viewers, as these devices might require attention. Not reporting events for more than 60 minutes might be acceptable; for

example, scheduled maintenance of a device. However, this might indicate an issue that requires investigation. Maybe the device is improperly configured or needs to be restarted; or there is an underlying network, connection, or hardware problem.

Drill down to see details about an event on the dashboard, such as the Agent Name, Event Count SLC, Creation Time, and so on:

- If the view in the query viewer is a pie chart, change the view to a table (click the **View as** button on the bottom right of the query viewer).

- Right click an event in the query viewer and select **Drilldown > Show device details for selected Device Product**.

Critical Monitored Devices Dashboard
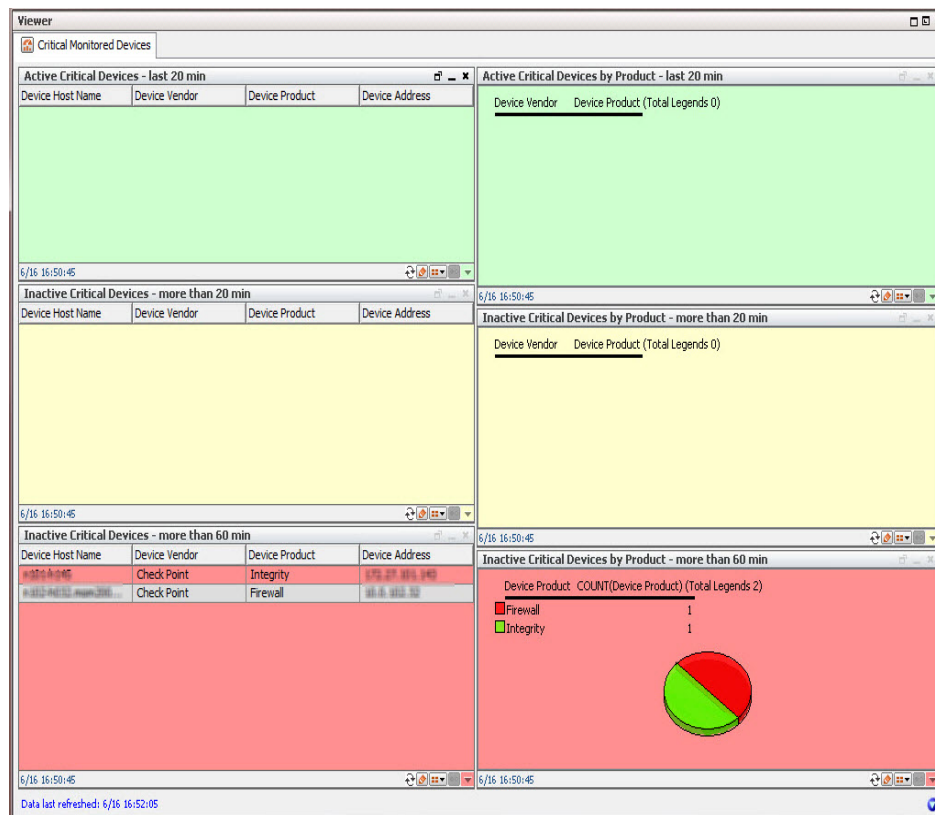
This dashboard provides several query viewers that show an overview of your critical devices (the devices in the **Critical Monitored Devices** active list).

- The **Active Critical Devices - last 20 min** query viewer displays information about critical devices that have reported events within the last 20 minutes. The **Active Critical Devices by Product - last 20 min** query viewer displays the number of critical devices that have reported events within the last 20 minutes, in a pie chart by device product type.

- The **Inactive Critical Devices - more than 20 min** query viewer displays information about critical devices that have not reported events within the last 20 minutes but have reported events within the

last 60 minutes. The **Inactive Critical Devices by Product - more than 20 min** query viewer displays the number of critical devices that have not reported events within the last 20 minutes but have reported events within the last 60 minutes, in a pie chart by device product type.

- The **Inactive Critical Devices - more than 60 min** query viewer displays information about critical devices that have not reported events within the last 60 minutes.

  The **Inactive Critical Devices by Product - more than 60 min** query viewer displays the number of critical devices that have not reported events within the last 60 minutes, in a pie chart by device product type.

  Focus on the devices in the **Inactive Critical Devices - more than 60 min** query viewers, as these devices might require attention. Not reporting events for more than 60 minutes might be acceptable; for example, scheduled maintenance of a device. However, this might indicate an issue that requires investigation. Maybe the device is improperly configured or needs to be restarted; or there is an underlying network, connection, or hardware problem.

Running Reports

The **ArcSight Device Monitoring** use case provides several reports that show historical information about your ESM devices. You can provide these historical reports to the stakeholders in your company, when needed. You can run the following reports for longer-term activity and inactivity monitoring.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.

2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- The **All Devices Detected Inactive - Last 24 Hours** report displays information about all devices that are *inactive* within the last 24 hours.

- The **All Devices Detected Inactive - Last 7 Days** report displays information about all devices that are *inactive* within the last seven days.

- The **All Monitored Devices** report displays information about all known devices (devices listed in the **All Monitored Devices** active list).

- The **Critical Devices Detected Inactive - Last 24 Hours** report displays information about critical devices that are *inactive* within the last 24 hours (critical devices are listed in the **Critical Monitored Devices** active list).

- The **Critical Devices Detected Inactive - Last 7 Days** report displays information about critical devices that are *inactive* within the last seven days.

- The **Critical Monitored Devices** report displays information about all critical devices being monitored.

- The **New Devices Detected - Last 24 Hours** report displays information about the new devices detected within the last 24 hours.

- The **New Devices Detected - Last 7 Days** report displays information about new devices detected within the last seven days.

ESM Licensing

The ESM Licensing use case provides information about licensing compliance. No configuration is required for this use case.

Using the ESM Licensing Use Case

The **ESM Licensing** use case is located in /All Use Cases/ArcSight Administration/ESM on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides several reports that provide a historical view of ESM license compliance. You can provide these reports to the stakeholders in your company, when needed. The Library section of the use case lists supporting resources that help compile information in the reports.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.

2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **Actors Licensing Report** shows the licensing history for actors within the last seven days. A chart shows the current count and the count limit.

- **Assets Licensing Report** shows the licensing history for assets within the last seven days. A chart shows the current count and the count limit.

- **Console Users Licensing Report** shows the licensing history for console users within the last seven days. A chart shows the current count and the count limit.

- **Devices Licensing Report** shows the licensing history for devices within the last seven days. A chart shows the current count and the count limit.

- **Web Users Licensing Report** shows the licensing history for web users (using the ArcSight ESM Command Center) within the last seven days. A chart shows the current count and the count limit.

- **Licensing Report** shows the licensing history for each of the license types within the last seven days. The chart shows the current count and the count limit in a chart.

- **Licensing Report (All)** shows the licensing history for all the license types within the last seven days. A chart shows the current count and the count limit for each of the license types.

- **Storage Licensing Report** shows an overview of the storage used by the system for each day, with a breakdown of the raw event data size sent by each connector and by connector type.

ESM User Sessions

The ESM User Sessions use case provides information about user access to the ArcSight system. No configuration is required for this use case.

Using the ESM User Sessions Use Case

The **ESM User Sessions** use case is located in `/All Use Cases/ArcSight Administration/ESM` on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two dashboards to help you monitor user access to ArcSight ESM (user login and logout activity, including login session and notification information) and several reports that provide a historical view of ArcSight user login and logout activity. The Library section of the use case lists supporting resources that help compile information in the dashboards and reports.

Viewing the Dashboards

To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel.

- **ArcSight User Status** displays information about ArcSight Manager user sessions, including the username, the IP address and zone for the system from which the user is connecting, and the status of the connection (Logged In, Logged Out, or Login Timed Out).

- **ArcSight User Activity** displays information about the users currently logged into the ArcSight ESM system, such as the username, IP address of the system from which the user is connecting, the client type and version, and the last access time. Recent user session information and notification activity generated by ArcSight ESM rules are also provided.

Running Reports

The **ESM User Sessions** use case provides several reports that show information about ESM user sessions. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.

2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **ArcSight User Login Trends** shows a summary of the number of ArcSight user logins for the previous day. A bar chart shows the total number of logins by user and a table shows the number of logins by user per hour.

- **ArcSight User Logins - Last Hour** shows details for all the ArcSight user logins within the past hour. The report contains a table showing the source host, the username, and the login time.

- **User Login Logout Report** shows successful and failed user login events, and logout events.

Actor Configuration Changes

The Actor Configuration Changes use case provides information about changes to the actor resources. No configuration is required for this use case.

Using the Actor Configuration Changes Use Case

The **Actor Configuration Changes** use case is located in `/All Use Cases/ArcSight Administration/ESM/Configuration Changes` on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two dashboards, an active channel, and several reports to help you monitor changes made to the actor resources. The Library section of the use case lists supporting resources that help compile information in the dashboards, active channel, and reports.

Viewing the Dashboards

The **Actor Configuration Changes** use case provides two dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **Actor Administration** displays a list of all the authenticators for actors.
- **Actor Change Log** displays an overview of the actor resource changes (the total number of changes by type within the last hour) and the most recent events related to changes in actors (including creation, deletion, and modification of single-value and multi-value parameters of actor resources).

Viewing the Active Channel

To view the **Actor Audit Events** active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel and displays all events where there are data changes to the actor resources.

Running Reports

The **Actor Configuration Changes** use case provides several reports that give you a historical view of the changes made to the actor resources. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.

2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **Actor Full Name and Email Changes** shows information from actor audit events that result from changes to the Full Name or Email attribute of an actor. The report shows the old and new information.

- **Actor Manager and Department Changes** shows information from actor audit events that result from changes to the Department or Manager attribute of an actor. This report shows the old and the new information.

- **Actor Title and Status Changes** shows information from actor audit events that result from changes to the Title or Status attribute of an actor. The report shows the old and new information.

- **Configuration Changes by Type** shows recent actor configuration changes. A table lists all the changes grouped by type and user, and sorts them chronologically.

- **Configuration Changes by User** shows recent actor configuration changes. A table lists all the changes grouped by user and type, and sorts them chronologically.

- **Created** shows a list of all the actors created the previous day.

- **Deleted** displays audit event information for actors that have been deleted.

- **IDM Deletions of Actors** shows the list of all the actors that have been marked as deleted by the IDM. This is not the same as deleting the actor resource from the ArcSight ESM system.

- **Updated** shows a list of all the actors updated the previous day.

ESM Resource Configuration Changes

The ESM Resource Configuration Changes use case provides information about changes to the ESM resources, such as rules, reports, and so on. No configuration is required for this use case.

Using the ESM Resource Configuration Changes Use Case

The **ESM Resource Configuration Changes** use case is located in `/All Use Cases/ArcSight Administration/ESM/Configuration Changes` on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides a dashboard to help you monitor all changes to content resources and several reports that provide information about recently deleted, created, or updated ESM resources. The Library section of the use case lists supporting resources that help compile information in the dashboard and reports.

Viewing the Dashboard

To view the **Resource Change Log** dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel and displays the total number of ESM resource changes by type within the last hour in a pie chart. Detailed information about logs associated with these changes is also provided.

Running Reports

The **ESM Resource Configuration Changes** use case provides several reports that provide historical information about recently deleted, created, or updated ESM resources. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.

2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **ESM Configuration Changes by Type** shows recent ESM configuration changes. A table lists all the changes grouped by type, sorted chronologically. Use this report to find all the configuration changes of a certain type.

- **ESM Configuration Changes by User** shows recent ESM configuration changes. A table lists all the changes grouped by user, sorted chronologically. Use this report to find all the configuration changes made by a specific user.

- **Resource Created Report** shows a list of all the resources created by ESM users the previous day.

- **Resource Deleted Report** shows a list of all the resources deleted by ESM users the previous day.

- **Resource History Report** shows a list of all the resources that have been created, updated, or deleted by ESM users the previous day.

- **Resource Updated Report** shows a list of all the resources updated by ESM users the previous day.

Content Management

The Content Management use case provides resources that show information about content package synchronization with the ESM Content Management feature. The information includes the history of content packages synchronized from a primary ESM source to multiple ESM destinations, and any common issues or errors encountered during synchronization.

> **Note:** The Content Management use case is available only if you install the optional ArcSight Content Management package located in the ArcSight Administration package group.

For information about the ESM Content Management feature, refer to the *ArcSight Command Center User's Guide*.

Configuring the Content Management Use Case

Enable the **Content Management Data** rule. This rule maintains list information for the ESM Content Management feature. To enable the rule, right-click the rule in the Rules section of the Content Management use case and select **Enable Rule**.

Using the Content Management Use Case

The **Content Management** use case is located in /All Use Cases/ArcSight Administration/ESM/Content Management on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides a dashboard to help you monitor the history of content packages synchronized across peered ArcSight Manager or subscribers. Several reports provide a history of content package synchronization and information about content packages with synchronization errors or subscription errors. The Library section of the use case lists supporting resources that help compile information in the dashboard and reports.

Viewing the Dashboard

To view the **Synchronization Status History** dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel and shows:

- The content packages with the most issues related to either package update delivery or to installation after the package has been delivered.
- The most common issues with delivery or installation of managed packages.
- The subscribers experiencing the most issues with managed package delivery or installation.

Running Reports

The **Content Management** use case provides several reports that provide a historical view of the content package synchronization history and information about content packages with synchronization errors or subscription errors. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.

2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **Top Packages with Synchronization Errors** shows information about the content packages with the most update delivery issues or installation issues after the package has been delivered.

- **Synchronization Status History** shows information about the history of content packages synchronized across peered ArcSight Managers or subscribers.

- **Top Synchronization Errors** shows information about the most common issues experienced by subscribers with managed package delivery or installation.

- **Top Subscribers with Errors** shows information about the subscribers experiencing the most issues with managed package delivery or installation.

Event Broker Monitoring

The Event Broker Monitoring optional package provides resources to help you monitor the status of connectivity and event consumption by ESM from an ArcSight Event Broker deployment.

After Event Broker and connectors are properly configured for connectivity and topic identification, ESM can consume topics from Event Broker.

Prerequisites:

Using the resources from the Event Broker Monitoring package assumes that your environment has a deployment of the ArcSight Event Broker, and Event Broker is set up with one topic specifically for ESM consumption.

See the *HPE Security ArcSight Data Platform Event Broker Administrator's Guide* and the accompanying *Release Notes*.

Event Broker Monitoring Audit Events

The Event Broker Monitoring content uses information from the Event Broker audit events generated by the ArcSight Manager.

The Device Event Class ID and Name fields, with more fields in the audit event are displayed in the Event Broker Audit Events active channel. See .

The following table lists the Event Broker audit events.

Event Broker Audit Events

Device Event Class ID	Audit Event Description
eventbroker:100	Connection to Event Broker is up
eventbroker:101	Connection to Event Broker is down
eventbroker:102	Number of messages remaining in Event Broker
eventbroker:103	Number of events forwarded from Event Broker to ESM

Using the Event Broker Monitoring Use Case

The **Event Broker Monitoring** use case is an optional module installed in /All Use Cases/ArcSight Administration/ESM/Event Broker Monitoring on the **Use Cases** tab of the Navigator.

To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.
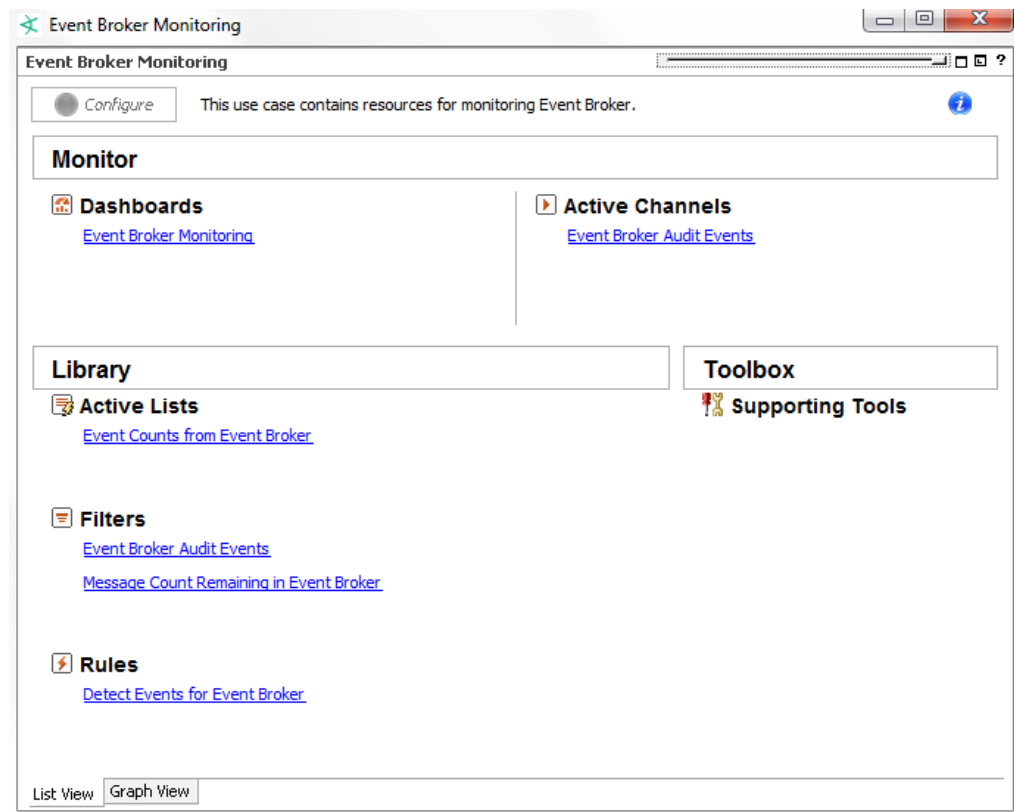
The Monitor section of the use case provides a dashboard and an active channel to help you monitor the status of Event Broker activity in terms of events received by ESM, and status of connectivity between ESM and Event Broker.

The Library section of the use case lists supporting resources that help compile information in the dashboard and active channel.

Viewing the Dashboard

Launch the Event Broker Monitoring dashboard either from the use case, or from the Console's Resources Navigator:

- On the Event Broker Monitoring use case, click the Dashboards link, **Event Broker Monitoring:**

- On the Navigator Resources panel, expand `/All Dashboards/ArcSight Administration/ESM/Event Broker Monitoring`.
  - Right-click **Event Broker Monitoring** and select **Show Dashboard**, or
  - Double-click **Event Broker Monitoring**.

Following is an example of the Event Broker Monitoring dashboard:
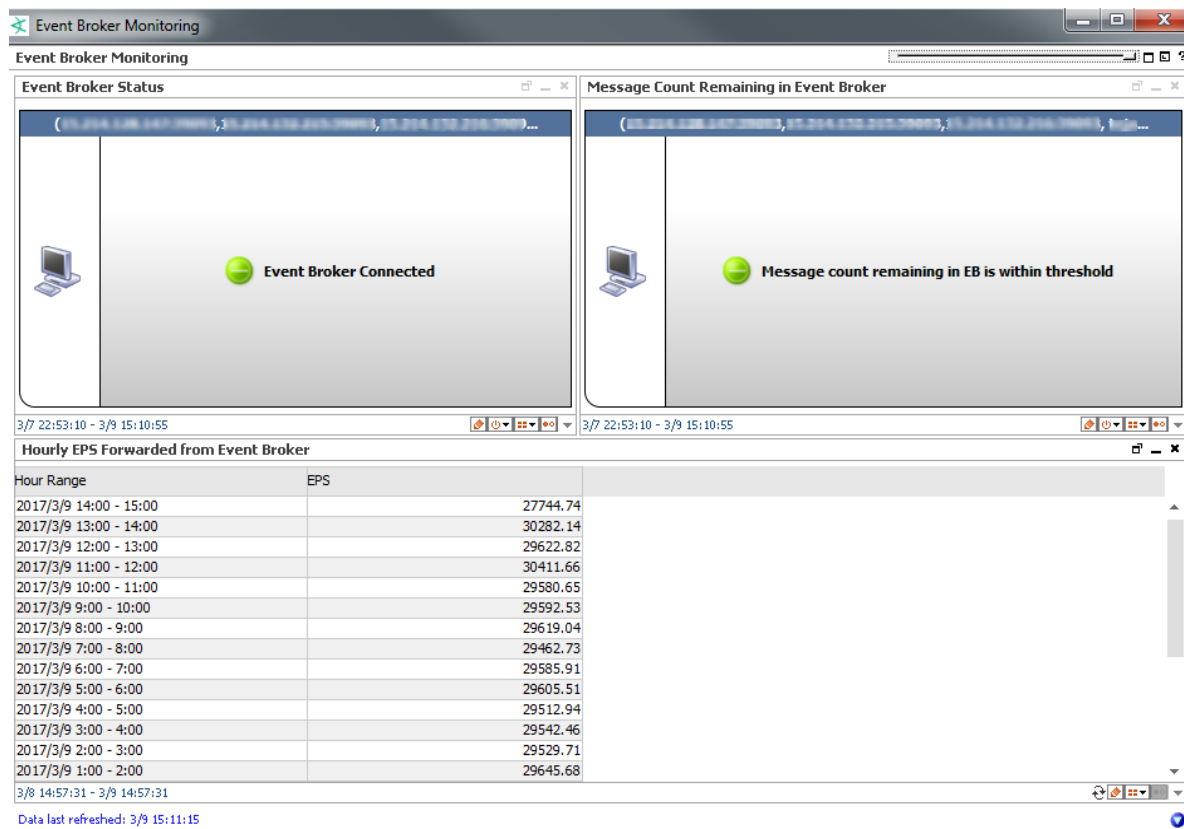
Note: If you change the Event Broker host information in the Manager, it will take 24 hours before the host information is completely updated on the data monitors. Query viewer information on hourly EPS rate is up to date because it is refreshed every 15 minutes.

The dashboard includes:

Data Monitors	• Event Broker Status This is a Last State data monitor. A green circle indicates that ESM is connected to the Event Broker host. If the connection is broken, you should investigate if the Event Broker host itself is up. • Message Count Remaining in Event Broker This is a Last State data monitor. It indicates that there are messages in Event Broker that are yet to be consumed by ESM. If the circle is green, the message count is within acceptable thresholds.
Query Viewer	Hourly EPS Forwarded from Event Broker The query viewer displays the total events per second consumed from Event Broker, every hour. It is refreshed every 15 minutes. If you want to update the data manually, click the **Refresh** button ↻.

Viewing the Active Channel

Launch the Event Broker Audit Events active channel either from the Event Broker Monitoring use case, or from the Console's Resources Navigator:

- On the Event Broker Monitoring use case, click the Active Channels link, **Event Broker Audit Events:**

- On the Navigator Resources panel, expand `/All Active Channels/ArcSight Administration/ESM/Event Broker Audit Monitoring`.
  - Right-click **Event Broker Audit Events** and select **Show Active Channel**, or
  - Double-click **Event Broker Audit Events**.

Following is an example (a partial view) of the active channel:
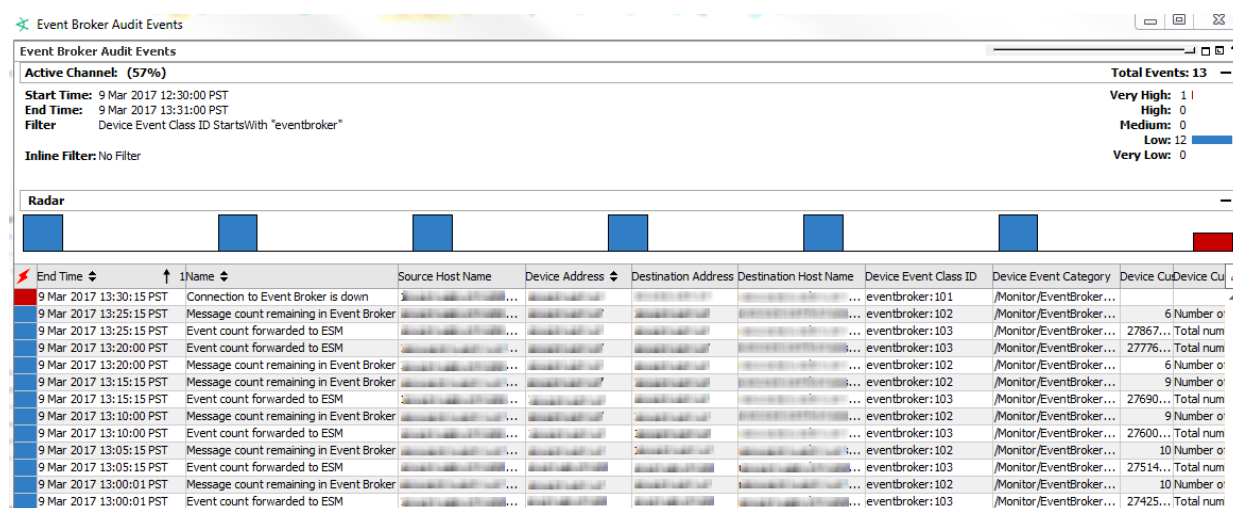
The Device Event Class ID and Name are among the columns of information displayed on this channel. The Source columns (address and hostname) correspond to the Event Broker host, while the Destination columns correspond to the ESM consumer.

> **Tip:** Under Device Event Class ID, look for `eventbroker:101`, which corresponds to the event name `Connection to Event Broker is down`. If not followed by `eventbroker:100`, which corresponds to `Connection to Event Broker is started`, contact your Event Broker administrator to investigate and fix the connection problem.

High Availability Monitoring

The High Availability (HA) Monitoring use case lets you monitor the status of ESM systems that are using the optional ESM High Availability Module (HA Module). The HA Module provides for a backup ESM machine with automatic failover capability should the primary ESM machine experience any communications or operational problems.

The HA Monitoring use case is part of the optional ArcSight ESM HA Monitoring content package. This content package is not installed by default on the ArcSight Manager. If you are using the HA Module, you can opt to install the content package during ArcSight Manager installation or from the ArcSight Console any time after installation (right click the **ArcSight ESM HA Monitoring** package in the ArcSight Administration folder on the **Packages** tab in the Navigator and select **Install Package**).

The HA Monitoring use case provides several resources that help you monitor HA events. You can see the current HA status, the current Primary System, all ESM System status changes within the last 24 hours, and the last ten HA status changes.

The HA Monitoring content shows you general HA status information and alerts you to problems. For more detailed diagnostics and troubleshooting, refer to the *ESM High Availability Module User's Guide*.

> **Note:** The HA Monitoring content displays data only if you have installed the HA Module and you have set up HA according to the *ESM High Availability Module User's Guide*.
>
> **Important:** The HA Monitoring active channel shows historical data (events generated since ArcSight Manager installation). The HA Monitoring dashboard displays the current status (events arriving in real time). If you install the ArcSight ESM HA Monitoring content package after ArcSight Manager installation when the HA link is established and fully in sync, the HA Monitoring dashboard does not display the current OK status if no new HA events are being generated.

HA Monitoring Audit Events

The HA Monitoring content uses information from the HA audit events generated by the ArcSight Manager. The Device Event Class ID, Event Name, and Event Message fields in the audit event are displayed in the **HA Monitoring** active channel and the **ESM HA Status** dashboard. The **ESM HA Status** dashboard provides the current HA status, which is derived from the audit event fields. In most cases, the current HA status and the Event Name field of the HA audit event are identical.

The **HA Monitoring** active channel and the **ESM HA Status** dashboard are described in "Using the HA Monitoring Use Case" on the next page

The following table lists the HA audit events.

Device Event Class ID	Event Name	Event Message
highavailability:100	Primary Manager Started	Manager started up due to HA failover or restart
highavailability:200	HA Status Failed	HA system failure
highavailability:300	DRBD Sync in Progress	Secondary system data syncing in progress **Note**: DRBD is the Distributed Replicated Block Device.
highavailability:400	iPDU status Failed	iPDU failover control function failed: iPDU agent stopped or cannot communicate with iPDU **Note**: iPDU is the Intelligent Power Distribution Unit.
highavailability:500	HA Status OK	HA system restored

Configuring the HA Monitoring Use Case

The HA Monitoring use case includes the **Alert - HA Status Change** rule. This rule triggers when an HA status change event (HA audit event) is generated. After the rule triggers, a notification is sent to the SOC Operators team. Make sure that you have configured notification destinations so that the correct SOC operators are notified when an HA status event is generated. For details on how to configure notification destinations, refer to the *ArcSight Console User's Guide*.

Using the HA Monitoring Use Case

The **HA Monitoring** use case is located in /All Use Cases/ArcSight Administration/ESM/HA Monitoring on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides a dashboard, an active channel and a report to help you monitor the status of ESM systems using the optional ESM HA Module. The Library section of the use case lists supporting resources that help compile information in the dashboard, active channel, and report.

### Viewing the Active Channel

To view the **HA Monitoring** active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel and displays all HA status events received within the last hour, including information such as when the Primary Manager started, when HA failed, and when HA returned to an OK state.

The active channel shows detailed information about the HA audit events generated by the ArcSight Manager, such as the Device Event Class ID, the Event Name, the Event Message, and other information. The IP address and hostname of both the Primary System and Secondary System are also shown. See for a list of the audit events generated by the ArcSight Manager.

An example of the **HA Monitoring** active channel is shown below.
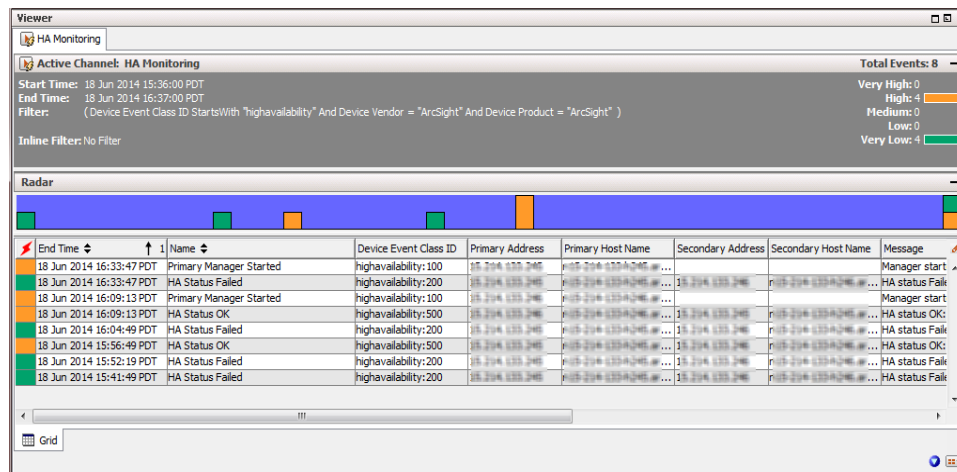
> **Tip:** Double-click an event in the active channel to see details about the event in the Event Inspector.

Viewing the Dashboard

To view the **ESM HA Status** dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel and displays an overview of the ArcSight ESM High Availability (HA) state.
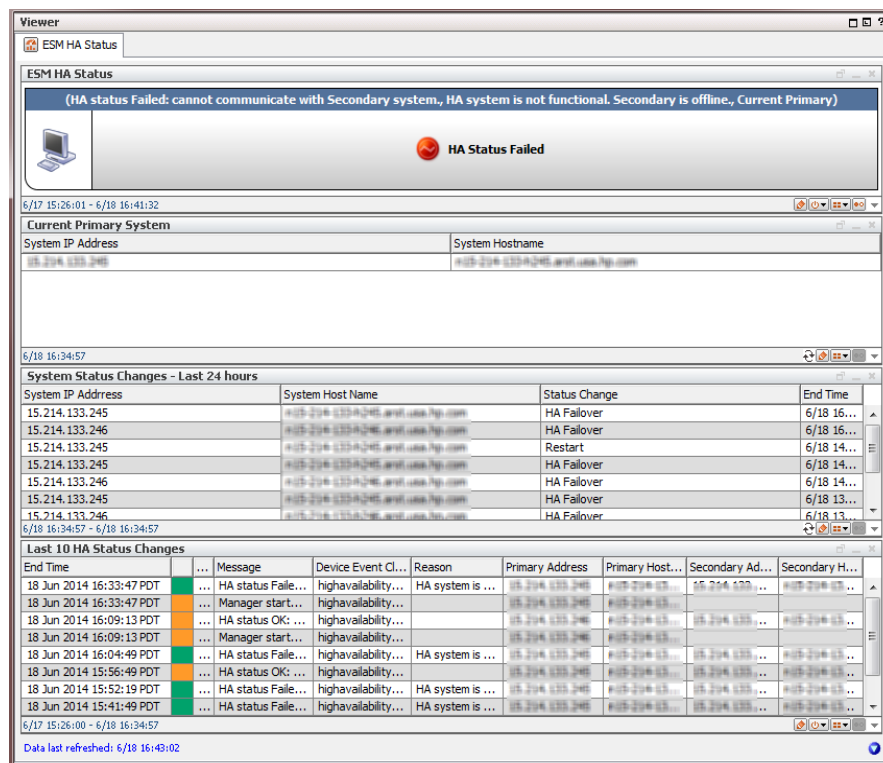
The dashboard data monitors and query viewers are described below.

- The **ESM HA Status** data monitor shows the current HA status (such as HA `Status Failed` or `HA Status OK`). The Event Message and event reason from the latest audit event generated by the ArcSight Manager provide additional details and are also displayed at the top of the data monitor.

  > **Tip:** To find out details about the current Primary System, such as the system hostname, IP address, and start time, click the data monitor heading. When the data monitor heading changes color, right click anywhere in the data monitor and select **Drilldown > Current Primary System**.
  >
  > To generate a report showing all HA status updates within the last seven days, right click anywhere in the data monitor and select **Drilldown > ESM HA Status - last 7 days**.

  The following table describes each HA status alert shown in the middle of the **ESM HA Status** data monitor and provides a description for each, including general troubleshooting tips. "HA Monitoring Audit Events" on page 55 provides a list of the HA Monitoring audit events and includes the Device Event Class ID, Event Name, and Event Message fields for each event. The current HA status is generated from the audit event fields.

ESM HA Status	Description
HA Status Failed	The Secondary System has become unavailable and cannot assume the role of the Primary System. The audit event is generated every five minutes until the Secondary System is restored. Investigate the failure. Possible causes are: • Failure of either network interface card (NIC) • Cross-over cable failure or disconnect • Secondary System failure or shutdown • Secondary System hard drive failure • Secondary System reboot • ArcSight ESM license expired
HA Status OK	The Secondary System has changed from HA Status Failed to HA Status OK. It might take 30 seconds for the audit event to generate after the Secondary System and high-availability service is restored.
HA Status Unknown	There is a failover and the Secondary System has taken over to become the Primary System, or the Primary System has restarted. This status indicates two situations: • The Primary System was restarted but no HA failover occurred. • HA failover occurred and the former Secondary System started up as the Primary System. This status turns into either "HA Status OK" or "HA Status Failed" a few minutes after the Primary System starts up.
DRBD Sync in Progress	The Distributed Replicated Block Device (DRBD) storage system began the process of synchronizing the Primary and Secondary System hard drives, and continues every five minutes until synchronization is complete. Each audit event includes the amount of data between the two systems that has been synchronized as a percentage until it reaches 100 percent. **Note**: This status is typically short. The system detects the HA status as soon as the Primary System starts up.
iPDU status Failed	The Intelligent Power Distribution Unit (iPDU) agent cannot communicate with the iPDU on either the Primary or Secondary System. The audit events are sent once every five minutes until communication is re-established. After the iPDU status returns to UP, you see the status HA Status OK.

- The **Current Primary System** query viewer shows the IP address and hostname of the current Primary System. Right click on the entry in the table and select **Drilldown > System Status Changes** to see all status changes for the System.

- The **System Status changes - Last 24 Hours** query viewer shows System changes, such as restarts and failovers, within the last 24 hours.

- The **Last 10 HA Status Changes** data monitor shows the last ten HA status changes. Right-click on an entry in the table and select **Drilldown > System Status Changes** to see all status changes for the selected System.

Running the Report

The HA Monitoring use case provides the **ESM HA Status Updates - last 7 days** report. Run this report to see all HA status updates within the last seven days. You can provide this historical report to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.

2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

Tip: You can also run the report from the **ESM HA Status** data monitor of the **ESM HA Status** dashboard by right-clicking the data monitor heading and selecting **Drilldown > ESM HA Status - last 7 days**.

ESM Events

The ESM Events use case provides statistics on the flow of events through the ArcSight system. No configuration is required for this use case.

Using the ESM Events Use Case

The **ESM Events** use case is located in `/All Use Cases/ArcSight Administration/ESM/System Health` on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides several dashboards to help you monitor your ArcSight ESM and non-ArcSight ESM events (including event throughput), active channels that show system monitoring events generated by the local ArcSight ESM system and all events generated by ArcSight, and reports that provide historical information about ArcSight events. The Library section of the use case lists supporting resources that help compile information in the dashboards, active channels, and reports.

Viewing the Dashboards

The **ESM Events** use case provides several dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **Event Count History** displays the total number of non-ArcSight ESM events within the last seven days and within the last 30 days.

- **Event Overview** displays an overview of non-ArcSightESM events focusing on event counts, events by connector, by vendor and product, and by device IP address.

- **Event Throughput** displays event throughput information in addition to an overview of the system activity related to connectors.

- **Latest Events By Priority** displays event count distribution by priority. Additional detailed event count distribution for low, high, elevated, and severe priority ratings are also shown.

Viewing the Active Channels

The **ESM Events** use case provides two active channels. To view an active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel.

- **ASM Events** shows ArcSight System Monitoring events generated by the local ArcSightESM system.
- **System Events Last Hour** shows all events generated by ArcSight during the last hour. A filter prevents the active channel from showing events that contributed to a rule triggering, commonly referred to as correlation events.

Running Reports

The **ESM Events** use case provides several reports that show information about ArcSight events. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below.

- **Destination Counts** shows destination details and the sum of event counts for each destination.
- **Event Count by Agent Severity** shows events by agent severity with event counts.
- **Event Count by Source Destination Pairs** shows event counts by source-destination pairs.
- **Event Name Counts** shows event names and their event counts.
- **Events by ArcSight Priority (Summary)** displays a table of all events, grouped by ArcSight priority, showing the count of each event occurrence within that priority. Note: This report shows all ArcSight events; use the `FilterBy` parameter to limit the output to the areas of most interest.
- **Hourly Distribution Chart for Event** shows the hourly distribution of specific events.
- **Hourly Distribution Chart for a Destination Port** shows the hourly distribution of events for destinations with a specific port.
- **Hourly Distribution Chart for a Source Port** shows the hourly distribution of events for sources with a specific port.
- **Hourly Event Counts (Area Chart)** shows the hourly distribution of event counts.
- **Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart)** shows the hourly distribution of events by priority rating.
- **Source Counts by Event Name** shows event names by source address in addition to event counts.
- **Top 10 Events** shows the top events by count.
- **Top 10 Inbound Events** shows the top inbound events by count.
- **Top 10 Outbound Events** shows the top outbound events by count.

ESM Reporting Resource Monitoring

The ESM Reporting Resource Monitoring use case provides performance statistics for reports, trends, and query viewers. No configuration is required for this use case.

Using the ESM Reporting Resource Monitoring Use Case

The **ESM Reporting Resource Monitoring** use case is located in `/All Use Cases/ArcSight Administration/ESM/System Health` on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides dashboards, active channels, and reports to help you monitor, investigate and report on performance statistics for reports, trends, and query viewers. The Library section of the use case lists supporting resources that help compile information in the dashboards, active channels, and reports.

Viewing the Dashboards

The **ESM Reporting Resource Monitoring** use case provides several dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **Query Running Time Overview** shows the top ten longest queries for reports, trends, and query viewers. The dashboard also shows query counts by query type.

- **Query Viewer Details** shows query details for query viewers.

- **Report Details** shows query details for reports.

- **Reporting Subsystem Statistics** shows an overview of the resources and processing time devoted to reports.

- **Trend Details** shows query details for trends.

Viewing the Active Channels

The **ESM Reporting Resource Monitoring** use case provides three active channels. To view an active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel. The active channels are described below.

- **Query Viewer Status** shows all the query viewer-related events received within the last two hours.

- **Reports Status** shows all the report-related events received within the last two hours.

- **Trends Status** shows all the trend-related events within the last two hours. The Trend Name field shows the name of the Trend and the URI. The Trend Infos field shows information on the Trend event.

Running Reports

The **ESM Reporting Resource Monitoring** use case provides several reports that show information about queries. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.

2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below.

- **Failed Queries** shows the failed queries for trends, reports, and query viewers made within the past week.

- **Longest QueryViewer Queries** shows query duration information for query viewers made during the past week. A chart shows the top ten longest queries for a query viewer and a table shows the duration details for query viewers.

- **Longest Report Queries** shows query duration information for reports made during the past week. The chart shows the ten longest report queries and the table shows the duration details for the report queries.

- **Longest Trend Query** shows query duration information for trends made during the past week. A chart shows the ten longest trend queries and a table shows the duration details for trend queries.

- **Query Counts by Type** shows the number of queries made within the past week, grouped by type.

ESM Resource Monitoring

The ESM Resource Monitoring use case provides processing statistics for various resources, such as trends, rules, and so on.

Configuring the ESM Resource Monitoring Use Case

Enable the notification action for the following rules, if appropriate for your organization:

- **Excessive Rule Recursion**
- **Rule Matching Too Many Events**

For information about how to enable notification actions, see the *ArcSight Console User's Guide*.

Using the ESM Resource Monitoring Use Case

The **ESM Resource Monitoring** use case is located in `/All Use Cases/ArcSight Administration/ESM/System Health` on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides dashboards that show statistics about the rules engine, reporting, and the queries used for reports and trends. Reports are provided to show information about the resources being used by your ESM system. The Library section of the use case lists supporting resources that help compile information in the dashboards and reports.

Viewing the Dashboards

The **ESM Resource Monitoring** use case provides several dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **Query Running Time Overview** displays the top ten longest queries for reports, trends, and query viewers. The dashboard also shows query counts by type and query failures during the last 24 hours.

- **Reporting Subsystems Statistics** displays an overview of the resources and processing time devoted to reports.

- **Rules Status** displays information about the rules engine. Detailed information and event count distribution about partial rule matches, top firing rules, recently fired rules, and error logs are shown.

  Note: The Sortable Rules Stats data monitor on the Rules Status dashboard does not include pre-persistence rules.

Running Reports

The **ESM Resource Monitoring** use case provides several reports that show information about the resources being used by your ESM system. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.

2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **Active List Access** shows active list access statistics. A chart shows the number of added, deleted, and updated active list entries the previous day, grouping the counts by ten-minute intervals. A table shows details of the active list access, grouping the number by time interval and active list name.

- **Correlation Events Statistics** shows information about correlation events. A chart shows the number of correlation events within the last hour, grouping them by ten-minute intervals. A table shows details of the number of correlation events, grouping them by rule name and time interval.

- **Data Monitor Evaluations Statistics** shows a chart with the average number of data monitor evaluations per second.

- **Fired Rule Events** shows all events that were triggered by a rule (correlation events) and includes the number of times the rule triggered and the ESM priority of the event.

- **Invalid Resources** shows a list of resources that are invalid. A chart shows the count of invalid resources by resource type. A table lists all the invalid resources grouped by type and sorted by URI.

- **Number of Events Matching Rules** shows the total number of events matching rules within the last hour, grouping them by ten-minute intervals. A chart shows the number of events matching filter rules, join rules, and the total of both rule types.

- **Rules Engine Warning Messages** shows warning messages received from the rules engine during the past 24 hours.

- **Session List Access** shows session list access statistics. A chart shows the number of added, deleted, and updated session list entries in the last hour, grouping the counts by ten-minute intervals. A table shows the details of the session list access, grouping the number by time interval and active list name.

- **Top Accessed Active Lists** shows the top ten accessed active lists. A chart shows the top ten accessed active lists the previous day, grouping the counts by ten-minute intervals. A table shows the details of the active list access, grouping the number by active list name and time interval.

- **Top Accessed Session Lists** shows the top ten accessed session lists. A chart shows the top ten accessed session lists within the last hour, grouping the counts by ten-minute intervals. A table shows details of the session list access, grouping the number by active list name and time interval.

ESM Storage Monitoring (CORR-Engine)

The ESM Storage Monitoring (CORR-Engine) use case provides information on the health of the CORR (Correlation Optimized Retention and Retrieval)- Engine. This does not apply if you are using ESM with the Oracle database.

No configuration is required for this use case.

Using the ESM Storage Monitoring (CORR-Engine) Use Case

The **ESM Storage Monitoring (CORR-Engine)** use case is located in /All Use Cases/ArcSight Administration/ESM/System Health on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides dashboards and reports to help you monitor and report on database performance and the status of the database archive, including critical archive failures and archive task failures. The Library section of the use case lists supporting resources that help compile information in the dashboards and reports.

Viewing the Dashboards

The **ESM Storage Monitoring (CORR-Engine)** use case provides two dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **Active Status** displays database archive information.
- **Database Performance Statistics** displays an overview of database related statistics, such as available space, insert, and retrieval times.

Running Reports

The **ESM Storage Monitoring (CORR-Engine)** use case provides several reports that show information about the ESM Storage Monitoring (CORR) engine. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below.

- **Event Data Free Space - Last 30 Days** shows the free space percentages by day for the ARC_ EVENT_DATA database table space for the last 30 days.

- **System Data Free Space - Last 30 Days** shows the free space percentages by day for the ARC_ SYSTEM_DATA database table space for the last 30 days.

- **ASM Database Free Space** shows the current free space percentages for the ASM database table spaces. The report shows the percentages for the ARC_EVENT_DATA and ARC_SYSTEM_DATA table spaces.

- **ASM Database Free Space - by Day** shows the free space percentages by day for each of the ASM database table spaces. The report has one chart and one table, and has a custom parameter that can be used to choose one of the table spaces (ARC_EVENT_DATA or ARC_SYSTEM_DATA, if this is an Oracle installation, ARC_EVENT_INDEX and ARC_SYSTEM_INDEX are also available).

- **ASM Database Free Space - by Hour** shows the free space percentages by hour for the ASM database table spaces. The report shows the percentages by hour for the ARC_EVENT_DATA and ARC_SYSTEM_DATA table spaces.

- **Archive Processing** shows the archives that take the longest to process and the time it takes to archive information.

- **Archive Status Report** shows the current status of archive and disk space used.

Logger Events

The Logger Events use case provides statistics for events sent through a Logger. No configuration is required for this use case.

Using the Logger Events Use Case

The **Logger Events** use case is located in `/All Use Cases/ArcSight Administration/Logger` on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two active channels to help you investigate Logger application and platform events. The Library section of the use case lists supporting resources that help compile information in the active channels.

Viewing the Active Channels

The **Logger Events** use case provides two active channels. To view an active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel. The active channels are described below.

- **Logger Application Events** shows all the Logger application events received within the last hour. The active channel displays the Logger user and IP address, and the client address (web browser) for each event.

- **Logger Platform Events** shows all the Logger platform events received within the last hour. The active channel displays the Logger user and IP address, and the client address (web browser) for each event.

Logger System Health

The Logger System Health use case provides performance statistics for any Logger connected to the ArcSight system.

Configuring the Logger System Health Use Case

If you have a Logger connected to the ArcSight system, configure the Logger System Health use case for your environment as follows:

1. Enable the following rules in the `/All Rules/Real-time Rules/ArcSight Administration/Logger/System Health` folder:

   - **Logger Sensor Status**—This rule detects Logger system health events related to hardware sensor status. The rule updates the Logger Status and Logger Sensor Type Status active lists with the Logger address, sensor type, sensor name, and sensor status.

   - **Logger Sensor Type Status**—This rule detects Logger Sensor Status correlation events and triggers only if all the sensors statuses for the same sensor type for a Logger indicate OK.

   - **Logger Status**—This rule detects Logger Sensor Status correlation events and triggers only if all the sensor statuses for a Logger indicate OK.

     For information about enabling rules, refer to the *ArcSight Console User's Guide*.

2. Edit the **My Logger** filter in the `/All Filters/ArcSight Administration/Logger/System Health` folder. On the **Filter** tab, change the **Device Address** in the condition from the default 127.0.0.1. to the IP address of your Logger.

3. Enable the following data monitors:

   - **Network Usage (Bytes) - Last 10 Minutes**

   - **Network Usage (Bytes) - Last Hour**

   - **EPS Usage (Events per Second) - Last Hour**

   - **CPU Usage (Percent) - Last Hour**

   - **Disk Usage (Percent)**

   - **Memory Usage (Mbytes per Second) - Last 10 Minutes**

   - **EPS Usage (Events per Second) - Last 10 Minutes**

   - **CPU Sensors**

   - **Sensor Type Status**

   - **Disk Read and Write (Kbytes per Second) - Last 10 Minutes**

- **Disk Read and Write (Kbytes per Second) - Last Hour**

- **Memory Usage (Mbytes per Second) - Last Hour**

- **FAN Sensors**

- **Disk Usage**

- **CPU Usage (Percent) - Last 10 Minutes**

- **System Sensors**

For information about data monitors, refer to the *ArcSight Console User's Guide*.

Using the Logger System Health Use Case

The **Logger System Health** use case is located in `/All Use Cases/ArcSight Administration/Logger` on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides dashboards and an active channel to help you monitor and investigate the health of the Logger system defined in the **My Logger** filter. The Library section of the use case lists supporting resources that help compile information in the dashboards and active channel.

Viewing the Dashboards

The **Logger System Health** use case provides several dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **CPU and Memory** shows the CPU and memory usage within the last ten minutes and the last hour for the Logger defined in the **My Logger** filter.

- **Hardware** shows the status for all the hardware sensors on the Logger defined in the My Logger filter. The dashboard includes the CPU Sensors, FAN Sensors, and System Sensors data monitors.

- **My Logger Overview** shows an overview of the hardware, storage, CPU, memory, network, and EPS usage for the Logger defined in the **My Logger** filter.

- **Network** shows the network and EPS usage within the last ten minutes and the last hour for the Logger defined in the **My Logger** filter.

- **Storage** shows the disk usage and the disk read/write speed within the last ten minutes and the last hour for the Logger defined in the **My Logger** filter.

Viewing the Active Channel

The **Logger System Health** use case provides the **Logger System Health Events** active channel, which shows all Logger system health events received within the last hour. To view the active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel.

Chapter 4: ArcSight System Content

The ArcSight System content consists of resources required for basic security processing functions, such as threat escalation and priority calculations, as well as basic throughput channels required for default functionality. Resources that manage core functionality are **locked** to protect them from unintended change or deletion.

In this section, the ArcSight System resources are grouped together based on the functionality they provide. The ArcSight System resource groups are listed in the table below.

Resource Group	Purpose
"Actor Support Resources" on the next page	Includes resources that support the actors feature.
"Priority Formula Resources" on page 76	Includes resources that directly or indirectly affect the Priority Formula.
"System Resources" on page 78	Includes resources that are either required by the system to operate or are customizable so you can adjust the behavior of the system.

Actor Support Resources

The actors feature maps people and their activity to events from applications and network assets by leveraging user attributes defined within identity management systems, and correlating them with user account information from the user authentication systems in your network. Correlating user identifiers from the event traffic that reflects their activity throughout the day makes it possible to ensure that users are doing role-appropriate activity across the assets in your organization, and to detect and track inappropriate access and suspicious activity. For more information on Actors, see the *ArcSight Console User's Guide*.

> **Note:** Actors are a licensed feature; they do not apply to every environment.

Using the Actor Support Resources

The actor support resources consist of several reports located in the `/All Reports/ArcSight System/Core/` folder on the **Resource** tab of the Navigator:

- **Actor Context Report by Target Username** shows activity related to an actor based on the `ActorByTargetUserName` global variable.

- **Actor Context Report by Account ID** shows activity related to an actor based on the `ActorByAccountID` global variable.

- **Actor Context Report by Attacker Username** shows activity related to an actor based on the `ActorByAttackerUserName` global variable.

- **Actor Context Report by Custom Fields** shows activity related to an actor based on the `ActorByCustomFields` global variable.

To run a report:

1. Right-click the report in the Navigator tree on the **Resource** tab and select **Run.**

2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

Priority Formula Resources

The Priority Formula Resources group includes resources that directly or indirectly affect the Priority Formula. The Priority Formula is a series of five criteria against which each event is evaluated to determine its relative importance, or urgency, to your network. The Priority Formula is also referred to as the Threat Level Formula. For more information about the Priority Formula, refer to the *ArcSight Console User's Guide* or the *ESM 101* guide.

There are no monitoring resources for the priority formula. However, there are several rules that detect successful hostile attempts and identify correlation events that originate from other reconnaissance rules. See "Priority Formula Rules" below.

Configuring the Priority Formula Resources Group

Configure the following active lists:

- Populate the **Trusted List** active list with the IP sources on your network that are known to be safe.
- Populate the **Untrusted List** active list with the IP sources on your network that are known to be unsafe.

  For more information about working with active lists, see "Configuring Active Lists" on page 13.

  > **Note:** You can set up rules to add and remove entries from the **Trusted List** and **Untrusted List** active lists dynamically. The information in these active lists is then used in the Priority Formula.

Priority Formula Rules

The Priority Formula resources consist of several rules located in the `/All Rules/ArcSight System/` folder on the **Resource** tab of the Navigator.

- **Reconnaissance - Attackers** identifies correlation events that originate from other reconnaissance rules. The events signify successful reconnaissance events from an attacker. The rule adds the attacker to the Reconnaissance List active list.
- **Reconnaissance - Targets** identifies correlation events that originate from other reconnaissance rules. The events signify successful reconnaissance events targeted by an external attacker to an internal asset. The rule adds the target information into the Scanned List active list.
- **Compromise - Success** detects any successful attempt to compromise a device from a source that is not listed in the Trusted List active list, with either the attacker information (zone and address) or the target information present. The rule triggers whenever an event is categorized as Success and Compromise. On the first event, agent severity is set to high, the attacker address is added to the Hostile List and Infiltrators List active lists, and the target address is added to the Compromised List

and Hit List active lists.

- **Hostile - Attempt** detects any hostile attempt on a device that is not already compromised from a source that is not listed in the Trusted List active list. The rule triggers whenever an event is categorized as Attempt and Hostile, and the target does not belong to a compromised active list.

- **Hostile - Success** detects any successful hostile attempts on a device that is not already compromised from a source not listed in the Trusted List active list. The rule triggers whenever an event is categorized as Success and Hostile, and the target does not belong to a compromised active list. On the first event, the severity is set to medium, the attacker address is added to the Infiltrators List active list, the target address is added to the Compromised List active list, and the target information is removed from Hit List active list.

- **Compromise - Attempt** detects any attempt to compromise a device from a source that is not listed in a trusted active list. The rule triggers whenever an event is categorized as Attempt and Compromise. On the first event, agent severity is set to high, the attacker address is added to the Hostile List active list, and the target address is added to the Hit List active list.

- **Incident Resolved - Remove From List** detects a Resolved message in an ArcSight Data Monitor Value Change event from the Attacked or Compromised Systems data monitor (in the Executive View dashboard), which is sent when a user marks an asset within the data monitor as resolved. This rule only triggers if you have the Intrusion Monitoring package installed from a previous ESM release.

System Resources

The System Resources group includes resources that are either required by the system to operate or are customizable so you can adjust the behavior of the system.

Configuring System Resources

Configure the following filters:

- Modify the **Connector Asset Auto-Creation Controller** filter to specify which assets to exclude from the asset auto creation feature.

  The **Connector Asset Auto Creation Controller** filter directs the creation of an asset for network nodes represented in events received from the connectors present in your environment. By default, the **Connector Asset Auto Creation Controller** filter is configured with the generic condition True, which matches all events. You can exclude connectors from a specific zone, such as a VPN zone, (where the asset already exists, but traffic is coming into the network from an alternate VPN interface). You can also exclude traffic from different types of connectors, such as from a particular device and vendor. For more information about asset auto creation, refer to the *ArcSight Console User's Guide*.

- Modify the **Device Asset Auto-Creation Controller** filter.
  ArcSight creates assets in the asset model automatically for events whose devices are not already modeled either manually or using an asset scanner. Depending on what devices you have reporting to ArcSight and what devices report in to your network, this can cause more individual assets to be added to your asset model than necessary. For example, every time a laptop logs onto the network via a VPN or wireless network, a new asset ID is generated for that device. By default, the Device Asset Auto Creation Controller filter is configured with the generic condition True, which matches all events. Configure this filter to specify traffic from specific devices and device vendors, or event categories, such as Hostile. When you specify an event category, the filter directs the system to only create assets for events with this severity.

- Modify the **SNMP Trap Sender** filter if you have the SNMP Trap Sender enabled to forward events through SNMP to a network management system.
  By default, this filter is configured with the /ArcSight System/Event Types/ArcSight Correlation Events filter. If you leave this default setting and you have SNMP forwarding enabled, all ArcSight correlation events are trapped and forwarded to the network management system.
  To configure this filter to forward certain events as an SNMP trap, change the default condition in the SNMP Trap Sender filter to specify which events are forwarded as traps. You can express this condition directly in the SNMP Trap Forwarding filter, or you can create another filter that expresses these parameters and point to it in the SNMP Trap Sender filter. To enable the SNMP trap sender, refer to the *ArcSight ESM Administrator's Guide*.

Using the System Resources

The System Resources group consists of several active channels that show events received by ArcSight ESM over different periods of time, two reports that are used by the ArcSight console for internal processing, and several integration commands that you can use in ArcSight ESM active channels and dashboards.

Viewing the Active Channels

The System Resources group provides several active channels located in the `/All Active Channels/ArcSight System/` folder on the **Resource** tab of the Navigator. To open an active channel, right-click the active channel in the resource tree and select **Show Active Channel**. The active channels are described below:

- **System Events Last Hour** shows all events generated by ArcSight during the last hour. A filter prevents the active channel from showing events that contributed to a rule triggering, commonly referred to as correlation events.

- **Today** shows all events received today since midnight. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlation events.

- **Last 5 Minutes** in `/All Active Channels/ArcSight System/All Events` shows events received during the last five minutes. The active channel includes a sliding window that always displays the last five minutes of event data.

- **Last Hour** in `/All Active Channels/ArcSight System/All Events` shows events received during the last hour. The active channel includes a sliding window that always displays an hour of event data.

- **Live** in `/All Active Channels/ArcSight System/Core` shows events received during the last two hours. The active channel includes a sliding window that always displays the last two hours of event data. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events.

- **Personal Live** in `/All Active Channels/ArcSight System/Core` shows events received during the last two hours. The active channel includes a sliding window that always displays the last two hours of event data. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlation events. This active channel also hides all the events that have been assigned to the current user.

Reports

The System Resources group consists of two reports located in the `/All Reports/ArcSight System/Core/` folder on the **Resource** tab of the Navigator:

- **Assets having Vulnerabilities** is used by the ArcSight Console for internal processing; do not run this locked report.

- **Selected Case Report** is a basic report template for case management. Refer to the *ArcSight Console User's Guide* topic on "Creating a Report on a Case."

- **Vulnerabilities of an Asset** is used by the ArcSight Console for internal processing; do not run this locked report.

Integration Commands

ArcSight ESM provides several integration commands; a set of tools that make it possible to invoke scripts and utilities directly from the ArcSight Console. You can use these commands directly from dashboards and active channels. You can edit these commands from the `/All Integration Commands/ArcSight System/Tools` folder in the Resource tree of the Navigator panel.

- **Nslookup (Linux)** in `/All Integration Commands/ArcSight System/Tools/Linux` enables you to find details about an IPv4 hostname in the Domain Name System (DNS). Use this command from an ArcSight Console running Linux.

- **Nslookup-IPV6 (Linux)** in `/All Integration Commands/ArcSight System/Tools/Linux` enables you to find details about an IPv6 hostname in the Domain Name System (DNS). Use this command from an ArcSight Console running Linux.

- **Nslookup (Windows) in** `/All Integration Commands/ArcSight System/Tools/Windows` enables you to find details about a Domain Name System (DNS). Use this command from an ArcSight Console running Windows.

- **Ping (Linux)** in `/All Integration Commands/ArcSight System/Tools/Linux` enables you to test whether a particular host is reachable across an IPv4 network. Use this command from an ArcSight Console running Linux.

- **Ping6 (Linux)** in `/All Integration Commands/ArcSight System/Tools/Linux` enables you to test whether a particular host is reachable across an IPv6 network. Use this command from an ArcSight Console running Linux.

- **Ping (Windows)** in `/All Integration Commands/ArcSight System/Tools/Windows` enables you to test whether a particular host is reachable across an IPv4 or IPv6 network. Use this command from an ArcSight Console running Windows.

- **Portinfo (Linux)** in `/All Integration Commands/ArcSight System/Tools/Linux` enables you to find information about the selected port. Use this command from an ArcSight Console running Linux.

- **Portinfo (Windows)** in `/All Integration Commands/ArcSight System/Tools/Windows` enables you to find information about the selected port. Use this command from an ArcSight Console running Windows.

- **Traceroute (Linux)** in `/All Integration Commands/ArcSight System/Tools/Linux` enables you to determine the route taken by packets across an IP network. Use this command from an ArcSight Console running Linux.

- **Traceroute (Windows)** in `/All Integration Commands/ArcSight System/Tools/Windows` enables you to determine the route taken by packets across an IP network. Use this command from an ArcSight Console running Windows.

- **Web Search** enables you to run a search with the selected item, device vendor, and device product in the selected event.

- **Whois (Linux)** `/All Integration Commands/ArcSight System/Tools/Linux` enables you to determine the owner of a domain name or an IP address on the Internet. Use this command from an ArcSight Console running Linux.

- **Whois (Windows)** `/All Integration Commands/ArcSight System/Tools/Windows` enables you to determine the owner of a domain name or an IP address on the Internet. Use this command from an ArcSight Console running Windows.

Appendix A: ArcSight Administration Resources

This appendix lists all the resources by type in the ArcSight Administration packages.

ArcSight Administration Resources By Type

This section lists all the resources by type.

Active Channels

The following table lists all the active channels.

Active Channel Resources

Resource	Description	URI
ASM Events	This active channel shows ArcSight System Monitoring events generated by the local ArcSight ESM system.	/All Active Channels/ArcSight Administration/ESM/System Health/Events/
Actor Audit Events	This active channel displays events in which there are changes to data in the actor resources.	/All Active Channels/ArcSight Administration/ESM/Configuration Changes/Actors/
ArcSight ESM Device Monitoring	This active channel shows device status events.	/All Active Channels/ArcSight Administration/Devices/
Connector Caching Events	This active channel displays information about Connector cache status audit events and correlation events from the related Connector Monitoring rules.	/All Active Channels/ArcSight Administration/Connectors/System Health/
Connector Connection Status Events	This active channel displays information about connector connection status audit events and correlation events from the related Connector Monitoring rules.	/All Active Channels/ArcSight Administration/Connectors/System Health/
Connector Upgrades	This active channel shows all the events related to connector upgrades within the last two hours. The active channel uses the Connector Upgrades field set.	/All Active Channels/ArcSight Administration/Connectors/Configuration Changes/
Distributed Correlation Events	This active channel shows distributed correlation audit events.	/All Active Channels/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Logger Application Events	This active channel shows all the Logger application events within the last hour.	/All Active Channels/ArcSight Administration/Logger/
Logger Platform Events	This active channel shows all the Logger platform events within the last hour.	/ArcSight Administration/Logger/

Active Channel Resources, continued

Resource	Description	URI
Logger System Health Events	This active channel shows all the Logger system health events within the last hour.	/All Active Channels/ArcSight Administration/Logger/
Query Viewers Status	This active channel shows all the query viewer-related events within the last two hours.	/All Active Channels/ArcSight Administration/ESM/System Health/Resources/
Reports Status	This active channel shows all the report-related events within the last two hours.	/All Active Channels/ArcSight Administration/ESM/System Health/Resources/
System Events Last Hour	This active channel shows all events generated by ArcSight during the last hour. A filter prevents the active channel from showing events that contributed to a rule triggering, commonly referred to as correlated events.	/All Active Channels/ArcSight Administration/ and /All Active Channels/ArcSight Administration/ESM/System Health/Events/
Trends Status	This active channel shows all the trend-related events within the last two hours. The Trend Name field shows the name of the Trend and the URI. The Trend Infos field shows information on the Trend event.	/All Active Channels/ArcSight Administration/ESM/System Health/Resources/

Active Lists

The following table lists all the active lists.

Active List Resources

Resource	Description	URI
All Monitored Devices	This active list is populated by the All Monitored Devices rule. The active list stores entries for 365 days and is used by queries to retrieve device activity information by dashboards and reports.	/All Active Lists/ArcSight Administration/Devices/
Average EPS	This active list stores average EPS during last hour.	/All Active Lists/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Black List - Connectors	This active list maintains a list of connectors that are not monitored by the Connector Monitoring rules.	/All Active Lists/ArcSight Administration/Connectors/System Health/Custom/

Active List Resources, continued

Resource	Description	URI
Black List - Reverse Look Up	This active list stores look-up data to enable the rules to update the connector connection and caching status displays when a connector is added to the Black List - Connectors active list. Note: This list should contain all the information that is also included in the Connector Information active list. This active list links the information in the Black List - Connectors active list to the information in the Connector Information active list. The connectors listed in the Black List - Connectors active list are the only ones not processed by the Connector Monitoring rules. Do not edit the entries in this list unless you are sure that an entry is no longer valid (and can be removed).	/All Active Lists/ArcSight Administration/Connectors/System Health/Custom/
Connector Average EPS - Last 7 Days	This active list stores the average EPS for all connectors during the last seven days. The data is from a trend.	/All Active Lists/ArcSight Administration/Connectors/System Health/EPS/
Connector Daily Average EPS	This active list stores the daily average EPS for all connectors. The data is from a trend.	/All Active Lists/ArcSight Administration/Connectors/System Health/EPS/
Connector Information	This active list maintains a list of the available information about connectors, whether they are directly connected to an ESM manager or indirectly through a Logger. Note: Information is derived from connector audit events and some information might be incomplete (blank) until the appropriate audit event arrives and is processed by the Connector Monitoring rules.	/All Active Lists/ArcSight Administration/Connectors/System Health/
Connector Upgrades	This active list stores information related to successful and failed connector upgrades. When an upgrade is successful, the active list stores the Upgrade Time, Connector ID, Connector Name, Connector Version, Connector Type, Connector Address, and Connector Zone. When an upgrade fails, the active list also stores the reason for the failure. The active list is populated by the Connector Upgrade Failed and Connector Upgrade Successful rules.	/All Active Lists/ArcSight Administration/Connectors/Configuration Changes/

Active List Resources, continued

Resource	Description	URI
Connectors - Caching	This active list stores information about the connectors that are currently caching events. A connector is removed from the active list when the cache is empty again or when it has been caching for more than two hours (by default).	/All Active Lists/ArcSight Administration/Connectors/System Health/
Connectors - Down	This active list stores the IDs and names of connectors that are currently down (either a connector shut down or a heartbeat timeout). After the TTL of the active list expires, the connector information is added to the Connectors Still Down active list and a notification is sent to the SOC Operators to inform them that the connector has been down for 20 or more minutes. The connector is removed from the active list when it restarts or reconnects.	/All Active Lists/ArcSight Administration/Connectors/System Health/
Connectors - Dropping Events	This active list stores the connectors that are currently dropping events (for example, when the cache is full). The connector is removed from the active list when the cache is empty again.	/All Active Lists/ArcSight Administration/Connectors/System Health/
Connectors - Still Caching	This active list stores available information about connectors that have been caching for over two hours (by default).	/All Active Lists/ArcSight Administration/Connectors/System Health/
Connectors - Still Down	This active list stores the ID and the name of the connectors that are have been down for 20 minutes or more (either a connector shut down or a heartbeat timeout). After the TTL of the Connectors - Down active list expires, the connector information is added to this list and a notification is sent to the SOC Operators to inform them that the connector has been down for more than 20 minutes. The connector is removed from the active list when it restarts or reconnects.	/All Active Lists/ArcSight Administration/Connectors/System Health/
Counts from Distributed Correlation	No description available.	/All Active Lists/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Counts in Persistor	No description available.	/All Active Lists/ArcSight Administration/ESM/Distributed Correlation Monitoring/

Active List Resources, continued

Resource	Description	URI
Critical Devices	This active list is populated manually and used by the Critical Monitored Devices rule first. If the rule finds a match, it updates the Critical Monitored Devices active list, which in turn is used by queries to retrieve critical device activity information by dashboards and reports.	/All Active Lists/ArcSight Administration/Devices/
Critical Monitored Devices	This active list is populated manually at first and then updated by the Critical Monitored Devices rule. The entries in this active list never expire, and are used by queries to retrieve critical device activity information by dashboards and reports.	/All Active Lists/ArcSight Administration/Devices/
Invalid Resources	This active list stores a list of resources that become invalid. The Resource Became Invalid rule adds an entry to the active list and the Resource Became Valid rule removes the corresponding entry from the active list.	/All Active Lists/ArcSight Administration/ESM/System Health/Resources/
Logger Sensor Type Status	This active list stores the status of the various hardware sensors on the Loggers. The active list stores the Logger address, the sensor type, the sensor name, and the sensor status. The Logger address and the sensor type are the key fields. This active list is used by a set of rules to identify the status of a sensor type for a Logger.	/All Active Lists/ArcSight Administration/Logger/System Health/
Logger Status	This active list stores the status of the various hardware sensors on the Loggers. The active list stores the Logger address, the sensor type, the sensor name, and the sensor status. The Logger address is the key field. This active list is used by a set of rules to identify the overall status of a Logger.	/All Active Lists/ArcSight Administration/Logger/System Health/
Query Running Time	This active list stores query information used to monitor and report the query duration.	/All Active Lists/ArcSight Administration/ESM/System Health/Resources/
Storage Licensing Data by Connector	This active list stores the raw event length reported by the raw event statistics events for each connector.	/All Active Lists/ArcSight Administration/ESM/Licensing/
Whitelisted Monitored Devices	This active list includes non-critical devices that you want to exclude from monitoring. This list is populated manually. The entries never expire.	/All Active Lists/ArcSight Administration/Devices/

Dashboards

The following table lists all the dashboards.

Dashboard Resources

Resource	Description	URI
Actor Administration	This dashboard shows the Actor Authenticators query viewer.	`/All Dashbords/ArcSight Administration/ESM/Configuration Changes/Actors/`
Actor Change Log	This dashboard shows an overview of actor resource changes.	`/All Dashbords/ArcSight Administration/ESM/Configuration Changes/Actors/`
All Monitored Devices	This dashboard shows an overview of all ESM devices. The green panel shows monitored devices that have been active for the last 20 minutes. The yellow panel shows monitored devices that have been inactive for more than 20 minutes but less than 60 minutes. The red panel shows monitored devices that have been inactive for more than 60 minutes.	`/All Dashbords/ArcSight Administration/Devices/`
ArcSight Appliances Overview	This dashboard shows an overview of all the ArcSight appliances. The dashboard includes the Logger Hardware Status, Logger Disk Usage, Connector Appliance Status, and Connector Appliance Disk Usage data monitors.	`/All Dashbords/ArcSight Administration/Logger/`
ArcSight User Activity	This dashboard shows login session information and notification activity for ArcSight ESM users.	`/All Dashboards/ArcSight Administration/ESM/User Access/User Sessions/`
ArcSight User Status	This dashboard displays the ArcSight User Sessions data monitor, showing recent login/logout activity for users, the remote terminal and zone, and current status.	`/All Dashboards/ArcSight Administration/ESM/User Access/User Sessions/`
CPU and Memory	This dashboard shows the CPU and memory usage for the Logger defined in the My Logger filter within the last ten minutes and the last hour.	`/All Dashboards/ArcSight Administration/Logger/My Logger/`
Connector Connection and Cache Status	This dashboard displays the overall status of connectors and information on connectors that are down, caching, or dropping events.	`/All Dashboards/ArcSight Administration/Connectors/System Health/`

Dashboard Resources, continued

Resource	Description	URI
Critical Monitored Devices	This dashboard shows an overview of the critical devices. The green panel shows monitored devices that have been active for the last 20 minutes. The yellow panel shows monitored devices that have been inactive for more than 20 minutes but less than 60 minutes. The red panel shows monitored devices that have been inactive for more than 60 minutes.	/All Dashboards/ArcSight Administration/Devices/
Current Event Sources	This dashboard displays information about the status of your connectors, as well as the top devices (vendor and product) that are contributing events.	/All Dashboards/ArcSight Administration/Connectors/System Health/
ESM System Information	This dashboard displays the System Information data monitor, which provides version, licensing, system resources availability and statistics, and other important settings and status.	/All Dashboards/ArcSight Administration/ESM/System Health/
Event Count History	This dashboard displays the total number of non-ArcSight events within the last seven days and the last 30 days.	/All Dashboards/ArcSight Administration/ESM/Event Analysis Overview/
Event Overview	This dashboard displays an overview of non-ArcSight events focusing on Events Counts, Events by Connector, Events by Vendor and Product, and Events by Device Address.	/All Dashboards/ArcSight Administration/ESM/Event Analysis Overview/
Event Throughput	This dashboard displays the Event Throughput and Event Throughput Statistics data monitors, providing an overview of the system activity related to connectors.	/All Dashboards/ArcSight Administration/ESM/System Health/Events/
Hardware	This dashboard shows the status for all the hardware sensors on the Logger defined in the My Logger filter. The dashboard includes the CPU Sensors, FAN Sensors, and System Sensors data monitors.	/All Dashboards/ArcSight Administration/Logger/My Logger/
Latest Events By Priority	This dashboard shows event count distribution ordered by priority. Additional detailed event count distribution for low, high, elevated, and severe priority ratings are also shown.	/All Dashboards/ArcSight Administration/ESM/System Health/Events/
My Logger Overview	This dashboard shows an overview of the hardware, storage, CPU, memory, network, and EPS usage for the Logger defined in the My Logger filter.	/All Dashboards/ArcSight Administration/Logger/My Logger/
Network	This dashboard shows the network and EPS usage for the Logger defined in the My Logger filter within the last ten minutes and the last hour.	/All Dashboards/ArcSight Administration/Logger/My Logger/
Query Running Time Overview	This dashboard shows the top ten longest queries for report, trend, and query viewers. The dashboard also shows query counts by type of queries.	/All Dashboards/ArcSight Administration/ESM/System Health/Resources/Reporting/

Dashboard Resources, continued

Resource	Description	URI
Query Viewer Details	This dashboard shows query details for query viewers.	/All Dashboards/ArcSight Administration/ESM/System Health/Resources/Reporting/
Report Details	This dashboard shows query details for reports.	/All Dashboards/ArcSight Administration/ESM/System Health/Resources/Reporting/
Reporting Subsystem Statistics	This dashboard displays the ArcSight Reporting Statistics, Currently Running Reports, and Report Statistics data monitors, providing an overview of the resources and processing time devoted to reports.	/All Dashboards/ArcSight Administration/ESM/System Health/Resources/Reporting/
Resource Change Log	This dashboard shows the changes (add, update, delete) to content resources and detailed information about logs associated with those actions.	/All Dashboards/ArcSight Administration/ESM/Configuration Changes/Resources/
Rules Status	This dashboard shows status about the rules engine. Detailed information and event count distribution about partial rule matches, top firing rules, recently fired rules, Sortable Rule Stats, and error logs are shown.	/All Dashboards/ArcSight Administration/ESM/System Health/Resources/Rules/
Storage	This dashboard shows the disk usage and the disk read/write speed for the Logger defined in the My Logger filter within the last ten minutes and the last hour.	/All Dashboards/ArcSight Administration/Logger/My Logger/
Trend Details	This dashboard shows query details for trends.	/All Dashboards/ArcSight Administration/ESM/System Health/Resources/Reporting/

Data Monitors

The following table lists all the data monitors.

Data Monitor Resources

Resource	Description	URI
Actor Change Log	This data monitor displays the most recent events related to changes in actors. These changes include creation, deletion, and modification of single-valued and multi-valued parameters of actor resources. Note: This data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/ESM/Configuration Changes/Actors/Actor Change Log/
Actor Change Overview	This data monitor shows an overview of the actor resource changes. The data monitor shows the total number of changes by type within the last hour.	/All Data Monitors/ArcSight Administration/ESM/Configuration Changes/Actors/Actor Change Log/
ArcSight Reporting Statistics	This data monitor shows report statistics for the last 15 minutes. Report statistics include the number of running reports, the number of reports querying the database, and the number of reports rendering. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Reporting/Reporting Subsystem Statistics/
ArcSight User Sessions	This data monitor shows the status of the ArcSight user sessions to the ArcSight Manager. The data monitor shows the username, the IP address of the machine from which the user is connecting, and the status of the connection. The status of the connection can be: Logged in, Logged out, or Login Timed Out.	/All Data Monitors/ArcSight Administration/ESM/User Access/User Sessions/ArcSight User Status/
CPU Sensors	This data monitor shows the status for all the CPU sensors on the Logger defined in the My Logger filter. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/Hardware/
CPU Usage (Percent) - Last 10 Minutes	This data monitor shows the CPU usage for the Logger defined in the My Logger filter within the last ten minutes. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/CPU and Memory/

Data Monitor Resources, continued

Resource	Description	URI
CPU Usage (Percent) - Last Hour	This data monitor shows the CPU usage for the Logger defined in the My Logger filter for the last hour. This Data Monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/CPU and Memory/
Connector Cache Status	This data monitor shows the current status of caching across all connectors. If one or more connectors has been caching for longer than two hours (by default), the status is yellow (long-term caching). If one or more connectors is dropping events, the status is red.	/All Data Monitors/ArcSight Administration/Connectors/System Health/Connector Connection and Cache Status/
Connector Connection Status	This data monitor shows the current status of the connector connections across all connectors. If one or more connectors is down for less than 20 minutes (by default), the status is yellow (short-term outage). If one or more connectors is down for longer than 20 minutes, the status is red (long-term outage).	/All Data Monitors/ArcSight Administration/Connectors/System Health/Connector Connection and Cache Status/
Current Connector Status	This data monitor displays information about the connectors that are registered with the system and reporting events.	/All Data Monitors/ArcSight Administration/Connectors/System Health/Current Event Sources/
Current Users Logged In	This data monitor shows information about the users currently logged into the ArcSight ESM system.	/All Data Monitors/ArcSight Administration/ESM/User Access/User Sessions/Console and ArcSight Web Status/
Currently Running Reports	This data monitor shows report statistics for currently running reports.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Reporting/Reporting Subsystem Statistics/
Database Transaction Volume	This data monitor shows transaction settings and detailed information about database transactions.	/All Data Monitors/ArcSight Administration/ESM/System Health/Storage/
Disk Read and Write (Kbytes per Second) - Last 10 Minutes	This data monitor shows the disk read/write speed for the Logger defined in the My Logger filter for the last 10 minutes. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/My Logger Overview/

Data Monitor Resources, continued

Resource	Description	URI
Disk Read and Write (Kbytes per Second) - Last Hour	This data monitor shows the disk read/write speed for the Logger defined in the My Logger filter within the last hour. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/Storage/
Disk Usage	This data monitor shows the disk status for the Logger defined in the My Logger filter. The state can be normal, warning, or critical, based on the disk free space. This Data Monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/My Logger Overview/
Disk Usage (Percent)	This data monitor shows the disk free space for the Logger defined in the My Logger filter. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/Storage/
EPS Usage (Events per Second) - Last 10 Minutes	This data monitor shows the EPS usage for the Logger defined in the My Logger filter within the last ten minutes. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/My Logger Overview/
EPS Usage (Events per Second) - Last Hour	This data monitor shows the EPS usage for the Logger defined in the My Logger filter within the last hour. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/Network/
Event Counts	This data monitor shows all non-ArcSight events	/All Data Monitors/ArcSight Administration/ESM/Event Analysis Overview/Event Overview/
Event Throughput	This data monitor shows the average EPS (events per second) for all the events within the last hour. The sampling interval is five minutes.	/All Data Monitors/ArcSight Administration/ESM/System Health/Events/Event Throughput/
Event Throughput Statistics	This data monitor shows event throughput from various connectors sending events to this ArcSight ESM.	/All Data Monitors/ArcSight Administration/ESM/System Health/Events/Event Throughput/
Events By Priority	This data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/

Data Monitor Resources, continued

Resource	Description	URI
Events by Connector	This data monitor shows the total number of non-ArcSight events by connector.	/All Data Monitors/ArcSight Administration/ESM/Event Analysis Overview/Event Overview/
Events by Device Address	This data monitor shows all non-ArcSight events by device address.	/All Data Monitors/ArcSight Administration/ESM/Event Analysis Overview/Event Overview/
Events by Vendor and Product	This data monitor shows all non-ArcSight events by vendor and product.	/All Data Monitors/ArcSight Administration/ESM/Event Analysis Overview/Event Overview/
FAN Sensors	This data monitor shows the status for all the FAN sensors on the Logger defined in the My Logger filter. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/Hardware/
Last 10 Trend Queries Returning No Results	This data monitor shows the last ten trend queries that return no results.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Trends/
Latest Elevated Threat Events	This data monitor shows the list of critical devices that are currently down. A device is down if it has not reported for a certain period of time (30 minutes by default).	/All Data Monitors/ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/
Latest Guarded Threat Events	This data monitor shows detailed information about the latest threat events with a priority level of 3 or 4.	/All Data Monitors/ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/
Latest High Threat Events	This data monitor shows detailed information about the latest threat events with a priority level of 7 or 8.	/All Data Monitors/ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/
Latest Low Threat Events	This data monitor shows detailed information about the latest threat events with a priority level less than or equal to 2.	/All Data Monitors/ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/
Latest Severe Threat Events	This data monitor shows detailed information about the latest threat events with a priority level greater than 8.	/All Data Monitors/ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/
Logger Disk Usage	This data monitor shows the disk status for all Loggers. The state can be normal, warning, or critical, based on the disk free space. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/ArcSight Appliances Overview/

Data Monitor Resources, continued

Resource	Description	URI
Logger Hardware Status	This data monitor shows the overall hardware status for all Loggers. The state is green (OK) if all the hardware sensors for a Logger are OK, red (NOT OK) if any of the sensors are not OK. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/ArcSight Appliances Overview/
Memory Usage (Mbytes per Second) - Last 10 Minutes	This data monitor shows the memory usage (JVM, Platform) for the Logger defined in the My Logger filter within the last ten minutes. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/CPU and Memory/
Memory Usage (Mbytes per Second) - Last Hour	This data monitor shows the memory usage (JVM, Platform) for the Logger defined in the My Logger filter for the last hour. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/CPU and Memory/
Network Usage (Bytes) - Last 10 Minutes	This data monitor shows the network usage for the Logger defined in the My Logger filter within the last ten minutes. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/My Logger Overview/
Network Usage (Bytes) - Last Hour	This data monitor shows the network usage for the Logger defined in the My Logger filter within the last hour. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/Network/
Notification Log	This data monitor shows notification activity generated by ArcSight ESM rules. The data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/ESM/User Access/User Sessions/Console and ArcSight Web Status/
Partial Matches per Rule	This data monitor shows event counts for partial rule matches.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/
Recent Fired Rules	This data monitor shows detailed information about the most recently fired rules.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/

Data Monitor Resources, continued

Resource	Description	URI
Recent System Resource Deletes	This data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/ESM/Configuration Changes/Resources/
Recent System Resource Inserts	This data monitor does not populate all values when running in Turbo Mode Fastest.	/ArcSight Administration/ESM/Configuration Changes/Resources/
Recent System Resource Updates	This data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/ESM/Configuration Changes/Resources/
Report Statistics	This data monitor shows reporting statistics related to runtimes for currently running and past run reports.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Reporting/Reporting Subsystem Statistics/
Resource Change Log	This data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/ESM/Configuration Changes/Resources/Resource Change Log/
Resource Change Overview	This data monitor shows an overview of the ArcSight resource changes (the total number of changes by type within the last hour).	/All Data Monitors/ArcSight Administration/ESM/Configuration Changes/Resources/Resource Change Log/
Rule Error Logs	This data monitor shows the most recent errors received from the rules engine.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/
Sensor Type Status	This data monitor shows the hardware status by sensor type for the Logger defined in the My Logger filter. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/My Logger Overview/
Sortable Rule Stats	This data monitor shows statistics for rule performance, such as partial matches, matching events, correlation events, time to execute, and memory used by each rule. You can sort the information in each column by clicking the column title. Note: Lightweight rules do not use in-memory operations or data field aggregation, and do not generate correlation events. Therefore, Matching Events, Correlation Events, and Aggregation Sets are always zero for lightweight rules.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/

Data Monitor Resources, continued

Resource	Description	URI
System Information	This data monitor shows detailed system information about this ArcSight ESM.	/All Data Monitors/ArcSight Administration/ESM/System Health/ESM System Information/
System Sensors	This data monitor shows the status for all the hardware sensors that are not CPUs or FANs on the Logger defined in the My Logger filter. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/Hardware/
Top Event Sources	This data monitor shows the most common event generating products and displays a listing of the top 20.	/All Data Monitors/ArcSight Administration/Connectors/System Health/Current Event Sources/
Top Firing Rules	This data monitor shows detailed information about the top firing rules.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/
User Access Log	This data monitor shows recent user session data events. The data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/ESM/User Access/User Sessions/Console and ArcSight Web Status/

Fields

The following table lists all the fields.

Field Resources

Resource	Description	URI
Service Message	This variable returns service message for distributed correlation audit events.	/All Fields/ArcSight Foundation/ArcSight ClusterView/
serviceNameAndId	This variable returns name and ID for distributed correlation audit events.	/All Fields/ArcSight Foundation/ArcSight ClusterView/

Field Sets

The following table lists all the field sets.

Field Set Resources

Resource	Description	URI
ASM Events	This field set contains fields of interest for monitoring ASM events.	/All Field Sets/ArcSight Administration/ESM/
Actor Audit Field Set	This field set contains fields of interest for monitoring changes to actor resources.	/All Field Sets/ArcSight Administration/ESM/Actor/
ArcSight ESM Device Monitoring	This field set contains fields used to examine device status events.	/All Field Sets/ArcSight Administration/Devices/
Connector Monitoring Events	This field set contains fields used to examine connector monitoring events, such as specific connector audit events and correlation events resulting from rules in the Connector Monitoring use cases.	/All Field Sets/ArcSight Administration/Connector/
Connector Upgrades	This field set is used by the Connector Upgrades active channel. The selected fields are: Manager Receipt Time, End Time, Name, Device Event Category, Agent Name, Agent Version, Agent Address, and Agent Zone Name.	/All Field Sets/ArcSight Administration/Connector/
Distributed Correlation Events	This field set is for distributed correlation monitoring.	/All Field Sets/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Logger Application Events	This field set is used by the Logger Application Events active channel. The field set identifies the end time, event name, Logger user, client address (browser), and Logger address.	/All Field Sets/ArcSight Administration/Logger/

Field Set Resources, continued

Resource	Description	URI
Logger Platform Events	This field set is used by the Logger Platform Events active channel. The field set selects the end time, event name, Logger user, client address (browser), and Logger address.	/All Field Sets/ArcSight Administration/Logger/
Logger System Health Events	This field set is used by the Logger System Health Events active channel. The field set identifies the end time, the Logger address, the device event category, the value, unit, time frame, and status of the system health events.	/ArcSight Administration/Logger/
Query Status	This field set displays detailed information about queries.	/All Field Sets/ArcSight Administration/ESM/

Filters

The following table lists all the filters.

Filter Resources

Resource	Description	URI
Aggregator Audit Events	This filter selects audit events for aggregator.	/All Filters/ArcSight Administration/ESM/Distributed Correlation Monitoring/
ASM Asset Resolution Timings	This filter detects ArcSight Status Monitor events that contain asset resolution timing information. The asset resolution average time is the average time in milliseconds taken to resolve an end-point in an event to an asset.	/All Filters/ArcSight Administration/ESM/System Health/Resources/Assets/
ASM CPU Load	This filter identifies ArcSight ESM monitoring events related to CPU load.	/All Filters/ArcSight Administration/ESM/System Health/Resources/
ASM Database Load Statistics	This filter identifies events related to ArcSight ESM database load.	/All Filters/ArcSight Administration/ESM/System Health/Storage/
ASM Database Statistics	This filter identifies events related to ArcSight ESM database statistics (such as insertion/retrieval).	/All Filters/ArcSight Administration/ESM/System Health/Storage/
ASM Event Evaluation	This filter identifies ArcSight ESM events based on rule insert event rates, data monitor evaluations per second, and filter evaluation counts.	/All Filters/All Filters/ArcSight Administration/ESM/System Health/Resources/
ASM Event Flow	This filter captures events that identify the ESM load through flow levels of events.	/All Filters/ArcSight Administration/ESM/System Health/Events/

Filter Resources, continued

Resource	Description	URI
ASM Flow Load	This filter identifies ArcSight ESM monitoring events related to event flow.	/All Filters/ArcSight Administration/ESM/System Health/Resources/
ASM Load Overview	This filter captures events that identify the load associated with the ArcSight ESM system through various parameters such as CPU, database, flow levels, memory, and resources.	/All Filters/ArcSight Administration/ESM/System Health/
ASM Reports Statistics	This filter detects Status Monitor events containing report statistics information. These events provide statistics about the current number of reports querying the database or being rendered.	/All Filters/ArcSight Administration/ESM/System Health/Resources/Reporting/
ASM Resource and Memory Load	This filter identifies ArcSight ESM monitoring events related to resource and memory load.	/All Filters/ArcSight Administration/ESM/System Health/Resources/
ASM Sidetable Cache Hit Rates	This filter detects ArcSight System Monitor events that contain side table cache hit rate information. Side tables are tables held in memory and in the database to retain common and relatively static information, such as geographical information, categorization information, connector information, device information, and labels for custom strings and numbers. The cache hit rate identifies how many successful attempts were made to find entries within the past two hours.	/All Filters/ArcSight Administration/ESM/System Health/Storage/
ASM Sidetable Sizes	This filter identifies ArcSight System Monitor events that contain side table size information. Side tables are tables held in-memory and in the database to retain common and relatively static information, such as geographical information, categorization information, connector information, device information, and labels for custom strings and numbers. The side table size identifies how many entries are currently in the cache.	/All Filters/ArcSight Administration/ESM/System Health/Storage/
ASM Standing Load	This filter identifies currently active, data monitor, rules, and active channel related events.	/All Filters/ArcSight Administration/ESM/System Health/Resources/
ASM Total Asset Count	This filter detects ArcSight System Monitor events that contain the current total number of assets.	/All Filters/ArcSight Administration/ESM/System Health/Resources/Assets/
Actor Changes	This filter detects actor resource audit events.	/All Filters/ArcSight Administration/ESM/Configuration Changes/Actor Update Tracking/

Filter Resources, continued

Resource	Description	URI
Actor Deletes	This filter detects deleted actor resources. Note: This filter only detects deleted actor events and ignores deleted entries for multi-value parameters.	`/All Filters/ArcSight Administration/ESM/Configuration Changes/Actor Update Tracking/`
Actor Inserts	This filter detects new actor resources. Note: This filter searches for new actors only and ignores new entries for multi-value parameters.	`/All Filters/ArcSight Administration/ESM/Configuration Changes/Actor Update Tracking/`
Actor Name or UUID	This filter detects actor audit events in which the file name is a UUID. If the file name is a UUID, an actor is returned and the full name is available. Otherwise, the field is either not a UUID or the actor resource is not in the system.	`/All Filters/ArcSight Administration/ESM/Configuration Changes/Actor Update Tracking/`
Actor Updates	This filter detects changes to the actor resources. Note: Actors can have three types of updates: an update to a single value parameter, and an addition or deletion of multi-value parameters.	`/All Filters/ArcSight Administration/ESM/Configuration Changes/Actor Update Tracking/`
ArcSight Audit Events	This filter captures ArcSight ESM audit events.	`/All Filters/ArcSight Administration/ESM/System Health/Events/Audit/`
ArcSight Login Events	This filter selects events that are associated with logins to the ArcSight ESM system.	`/All Filters/ArcSight Administration/ESM/User Access/User Sessions/`
ArcSight Login Rule Firings	This filter identifies events that contain ArcSight login rule triggering information. The deviceEventCategory used in this filter is generated by the ArcSight User Login rule. The filter is used by a trend that tracks hourly login statistics.	`/All Filters/ArcSight Administration/ESM/User Access/User Sessions/`
ArcSight Login Tracking	This filter identifies events that contain ArcSight login and logout information. The device event class IDs used in this filter are generated by the ArcSight auditing system.	`/All Filters/ArcSight Administration/ESM/User Access/User Sessions/`
ArcSight Rules	This filter identifies ArcSight ESM correlation events generated by rules.	`/All Filters/ArcSight Administration/ESM/System Health/Resources/Rules/`
ArcSight Status Monitoring Events	This filter selects ArcSight Status Monitoring events generated by the local ArcSight ESM system.	`/All Filters/ArcSight Administration/ESM/System Health/`
Correlator Audit Events	This filter selects audit events for correlator.	`/All Filters/ArcSight Administration/ESM/Distributed Correlation Monitoring/`

Filter Resources, continued

Resource	Description	URI
CPU Sensors	This filter identifies ArcSight correlation events that are generated by the Logger Sensor Status rule and where the sensor type (device custom string 4) is CPU for the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/Hardware/Sensors/
CPU Usage	This filter identifies Logger system health events related to CPU usage that originate from the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/CPU and Memory/
Connector Cache Status	This filter detects correlation events from the Update Connector Caching Status rule.	/All Filters/ArcSight Administration/Connectors/System Health/
Connector Caching Event	This filter detects connector caching events.	/All Filters/ArcSight Administration/Connectors/System Health/Conditional Variable Filters/
Connector Connection Status	This filter detects correlation events related to connector connection status.	/All Filters/ArcSight Administration/Connectors/System Health/
Connector Registered or Heartbeat Event	This filter detects events for connector timeouts because the connector information is not complete in Device Custom String2.	/All Filters/ArcSight Administration/Connectors/System Health/Conditional Variable Filters/
Database Insert Time Statistics	This filter identifies ArcSight system events where the Device Event Category is /Monitor/EventBroker/InsertTime.	/All Filters/ArcSight Administration/ESM/System Health/Storage/
Database Retrieval Time Statistics	This filter identifies ArcSight system events where the Device Event Category is /Monitor/EventBroker/RetrievalTime.	/All Filters/ArcSight Administration/ESM/System Health/Storage/
Disk Read and Write	This filter identifies Logger system health events related to disk read/write speed that originate from the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/Storage/
Disk Usage	This filter identifies Logger system health events related to disk usage that originate from the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/Storage/
Distributed Cache Audit Events	This filter selects audit events for distributed cache.	/All Filters/ArcSight Administration/ESM/Distributed Correlation Monitoring/

Filter Resources, continued

Resource	Description	URI
Distributed Correlation Audit Events	This filter selects audit events for distributed correlation.	/All Filters/ArcSight Administration/ESM/Distributed Correlation Monitoring/
EPS Usage	This filter identifies Logger system health events related to EPS usage that originate from the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/Network/
Elevated Threat Condition	This filter identifies events with a Priority level rating of 5 or 6.	/All Filters/ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
FAN Sensors	This filter identifies ArcSight correlation events that are generated by the Logger Sensor Status rule and where the sensor type (device custom string 4) is FAN for the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/Hardware/Sensors/
Green Threshold	This filter selects that event remaining count in message bus is less than certain time events, by default, it is 10 minutes.	/All Filters/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Guarded Threat Condition	This filter identifies events with a Priority level rating of 3 or 4.	/All Filters/ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
High Threat Condition	This filter identifies events with a Priority level rating of 7 or 8.	/All Filters/ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
Hour less than 10	This filter is used by a Conditional DV. The condition in the filter is Hour(EndTime) is less than 10.	/All Filters/ArcSight Administration/ESM/System Health/Resources/Trends/Conditional Variable Filters/
Logger Application Events	This filter identifies Logger application events.	/All Filters/ArcSight Administration/Logger/Event Types/
Logger Disk Usage	This filter detects Logger system health events related to remaining disk space.	/All Filters/ArcSight Administration/Logger/ArcSight Appliances Overview/
Logger Events	This filter identifies Logger events.	/All Filters/ArcSight Administration/Logger/Event Types/

Filter Resources, continued

Resource	Description	URI
Logger Hardware Status	This filter identifies ArcSight correlation events that are generated by the Logger Status rule or by the Logger Sensor Status rule and where the sensor status (device custom string 3) is not OK.	`/All Filters/ArcSight Administration/Logger/ArcSight Appliances Overview/`
Logger Platform Events	This filter identifies Logger platform events.	`/All Filters/ArcSight Administration/Logger/Event Types/`
Logger System Health Events	This filter identifies Logger system health events.	`/ArcSight Administration/Logger/Event Types/`
Low Threat Condition	This filter identifies events with a Priority level rating less than or equal to 2.	`/All Filters/ArcSight Administration/ESM/System Health/Events/Event Priority Filters/`
Memory Usage	This filter identifies Logger system health events related to memory usage that originate from the Logger defined in the My Logger filter.	`/All Filters/ArcSight Administration/Logger/System Health/CPU and Memory/`
Message Bus Status Events	This filter selects status audit events for message bus.	`/All Filters/ArcSight Administration/ESM/Distributed Correlation Monitoring/`
Message Count Remaining in Message Bus	This filter selects audit events for messages remaining in message bus.	`/All Filters/ArcSight Administration/ESM/Distributed Correlation Monitoring/`
Minute less than 10	This filter is used by a Conditional DV. The condition in the filter is Minute(EndTime) is less than 10.	`/All Filters/ArcSight Administration/ESM/System Health/Resources/Trends/Conditional Variable Filters/`
My Logger	This filter is used by all the My Logger dashboards and data monitors. The filter defines conditions to select one Logger to be used by these dashboards and data monitors. The default value is 127.0.0.1. Edit the IP address to match your Logger. Note: Only monitor one Logger at a time.	`/All Filters/ArcSight Administration/Logger/System Health/`
Network Usage	This filter identifies Logger system health events related to network usage that originate from the Logger defined in the My Logger filter.	`/All Filters/ArcSight Administration/Logger/System Health/Network/`

Filter Resources, continued

Resource	Description	URI
Notification Actions	This filter selects events that are related to notifications generated by a rule in the ArcSight ESM system.	/All Filters/ArcSight Administration/ESM/System Health/Events/Event Flow/
Red Threshold	This filter selects that event remaining count in message bus exceeds certain time events, by default, it is one hour.	/All Filters/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Resource Changes	This filter detects resource change audit events.	/All Filters/ArcSight Administration/ESM/Configuration Changes/Resource Update Tracking/
Resource Deletes	This filter detects deleted resources.	/All Filters/ArcSight Administration/ESM/Configuration Changes/Resource Update Tracking/
Resource Inserts	This filter detects new resources.	/All Filters/ArcSight Administration/ESM/Configuration Changes/Resource Update Tracking/
Resource Updates	This filter detects updates to resources.	/All Filters/ArcSight Administration/ESM/Configuration Changes/Resource Update Tracking/
Rules Engine Internal Events	This filter identifies internal ArcSight ESM rules engine base events.	/All Filters/ArcSight Administration/ESM/System Health/Resources/Rules/
Sensor Type Update	This filter identifies ArcSight correlation events that are generated by the Logger Sensor Type Status rule or by the Logger Sensor Status rule and where the sensor status (device custom string 3) is not OK for the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/Hardware/
Severe Threat Condition	This filter identifies events with Priority level rating greater than 8.	/All Filters/ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
System Sensors	This filter identifies ArcSight correlation events that are generated by the Logger Sensor Status rule and where the sensor type (device custom string 4) is not CPU or FAN for the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/Hardware/Sensors/

Filter Resources, continued

Resource	Description	URI
Threshold - Critical	This filter is used in the ASM Database Free Space - Critical rule. The filter identifies events in which the free space is less than two percent. The audit event uses Device Custom Number1 to report the database free space.	/All Filters/ArcSight Administration/ESM/System Health/Storage/Custom/
Threshold - Warning	This filter is used in the ASM Database Free Space - Warning rule. The filter captures events where the free space is less than or equal to five percent, but more than two percent. The audit event uses Device Custom Number1 to report the database free space.	/All Filters/ArcSight Administration/ESM/System Health/Storage/Custom/
Trend Query Returning No Results	This filter detects successful trend query events that return no results.	/All Filters/ArcSight Administration/ESM/System Health/Resources/Trends/

Global Variables

The following table lists all the global variables.

Global Variable Resources

Resource	Description	URI
Actor	This field returns the actor name.	/All Global Variables/ArcSight Administration/ESM/Actor/
ActorFromFileName	This global variable selects the actor based on the value in the file name and is used with actor audit events.	/All Global Variables/ArcSight Administration/ESM/Actor/
All Receivers and Forwarders	This field shows the EPS from all connector and forwarder agents connected to this ArcSight ESM.	/All Global Variables/ArcSight Administration/Logger/
CPU Name	The field returns the name of the CPU currently used.	/All Global Variables/ArcSight Administration/Logger/
Change Source	This field returns the source of the change that modified the actor resource.	/All Global Variables/ArcSight Administration/ESM/Actor/
ConnectorID	This variable returns the Resource ID of the connector.	/All Global Variables/ArcSight Administration/ESM/Licensing/

Global Variable Resources, continued

Resource	Description	URI
ConnectorName	This variable returns the name of the connector.	/All Global Variables/ArcSight Administration/ESM/Licensing/
ConnectorNameFromID	This variable returns the name of the Connector by looking up the Connector ID in the Connector Information Active List.	/All Global Variables/ArcSight Administration/ESM/Licensing/
ConnectorType	This variable returns the type of connector.	/All Global Variables/ArcSight Administration/ESM/Licensing/
DN New Value	This global variable extracts the new value for DN (Distinguished Name) in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
DN Old Value	This global variable extracts the old value for DN (Distinguished Name) in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Department New Value	This global variable extracts the new value for Department in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Department Old Value	This global variable extracts the old value for Department in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Disk Name	This field returns the name of the disk currently being used.	/All Global Variables/ArcSight Administration/Logger/
Disk Usage	This field returns the disk usage status whether it is normal or nearing critical usage (less than ten percent).	/All Global Variables/ArcSight Administration/Logger/
DiskUsageCritical	This field returns a value of Critical if the disk usage is determined to be less than five percent. If not, a value of Warning is returned.	/All Global Variables/ArcSight Administration/Logger/
Email Address New Value	This global variable extracts the new value for Email Address in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Email Address Old Value	This global variable extracts the old value for Email Address in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Employee Type New Value	This global variable extracts the new value for the Employee Type in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/

Global Variable Resources, continued

Resource	Description	URI
Employee Type Old Value	This global variable extracts the old value for Employee Type in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Field Status	This field is an alias field for Device Custom String3.	/All Global Variables/ArcSight Administration/Logger/
Field Value	This field is an alias field for Device Custom Number1.	/All Global Variables/ArcSight Administration/Logger/
Free Space	This field is an alias field for Device Custom Number1.	/All Global Variables/ArcSight Administration/Logger/
Full Name New Value	This global variable extracts the new value for Full Name in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Full Name Old Value	This global variable extracts the old value for Full Name in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Inbound and Outbound	This field returns a value of Inbound or Outbound via a filter that determines whether an event is an inbound or an outbound event.	/All Global Variables/ArcSight Administration/Logger/
IndexOfUsage	This field returns the index position of the string /Usage within the Device Event Category field.	/All Global Variables/ArcSight Administration/Logger/
Location New Value	This global variable extracts the new value for Location in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Location Old Value	This global variable extracts the old value for Location in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Logger Address	This field is an alias to the Device Address field.	/All Global Variables/ArcSight Administration/Logger/
Logger IP	This field is an alias to Destination Translated Address.	/All Global Variables/ArcSight Administration/Logger/
Manager New Value	This global variable extracts the new value for Manager in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/

Global Variable Resources, continued

Resource	Description	URI
Manager Old Value	This global variable extracts the old value for Manager in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Memory Name	This field returns a memory related value located within the Device Event Category field.	/All Global Variables/ArcSight Administration/Logger/
Org New Value	This global variable extracts the new value for Org in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Org Old Value	This global variable extracts the old value for Org in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
ReadOrWrite	This field returns whether the logger event is a read or write event.	/All Global Variables/ArcSight Administration/Logger/
Sensor Name	This field is an alias for Device Custom String5.	/All Global Variables/ArcSight Administration/Logger/
Sensor Status	This field is an alias for Device Custom String3.	/All Global Variables/ArcSight Administration/Logger/
Sensor Type	This field is an alias for Device Custom String4.	/All Global Variables/ArcSight Administration/Logger/
Status New Value	This global variable extracts the new value for Status in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Status Old Value	This global variable extracts the old value for Status in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Timeframe	This field is an alias for Device Custom String2.	/All Global Variables/ArcSight Administration/Logger/

Global Variable Resources, continued

Resource	Description	URI
Title New Value	This global variable extracts the new value for Title in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Title Old Value	This global variable extracts the old value for Title in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Unit	This field is an alias for Device Custom String1.	/All Global Variables/ArcSight Administration/Logger/

Integration Commands

The following table lists all the integration commands.

Integration Command Resources

Resource	Description	URI
By Destination	This integration command enables you to run a search by destination address on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours.	/All Integration Commands/ArcSight Administration/Logger/
By Event Name	This integration command enables you to run a search by event name on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours.	/All Integration Commands/ArcSight Administration/Logger/
By Source	This integration command enables you to run a search by source address on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours.	/All Integration Commands/ArcSight Administration/Logger/
By Source and Destination	This integration command enables you to run a search by source and destination address on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours.	/All Integration Commands/ArcSight Administration/Logger/
By User	This integration command enables you to run a search by user on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours.	All Integration Commands/ArcSight Administration/Logger/
By Vendor and Product	This integration command enables you to run a search by device vendor and product on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours.	/All Integration Commands/ArcSight Administration/Logger/
Logger Quick Search	This integration command enables you to run a search on an ArcSight Logger appliance. The search takes the selected field type and value as parameters, and returns all the events matching the condition within the last two hours.	/All Integration Commands/ArcSight Administration/Logger/

Integration Configurations

The following table lists all the integration configurations.

Integration Configuration Resources

Resource	Description	URI
ArcSight Investigate Search	This integration configuration is used to configure the ArcSight Investigate search commands.	/All Integration Configurations/ArcSight Administration/ArcSight Investigate/
Logger Quick Search	This integration configuration is used to configure the Logger Quick Search command.	/All Integration Configurations/ArcSight Administration/Logger/
Logger Search	This integration configuration is used to configure the Logger Search command.	/All Integration Configurations/ArcSight Administration/Logger/

Integration Targets

The following table lists all the integration targets.

Integration Target Resources

Resource	Description	URI
ArcSight Investigate 1	This integration target stores the hostname and port number of an ArcSight Investigate. This target is used by the set of integration commands for ArcSight Investigate search.	/All Integration Targets/ArcSight Administration/ArcSight Investigate/
Logger Appliance 1	This integration target stores the IP address of an ArcSight Logger appliance. This target is used by the set of integration commands for Logger.	/All Integration Targets/ArcSight Administration/Logger/
Logger Appliance 2	This integration target stores the IP address of an ArcSight Logger appliance. This target is used by the set of integration commands for Logger.	/All Integration Targets/ArcSight Administration/Logger/

Queries

The following table lists all the queries.

Query Resources

Resource	Description	URI
ASM Database Free Space	This query looks for internal events showing free space percentage for ASM database table spaces. The query returns the table spaces and free space percentages. The query is used by the ASM Database Free Space trend.	/All Queries/ArcSight Administration/ESM/System Health/Storage/Event Queries/
ASM Database Free Space (current)	This query looks for internal events showing free space percentage for ASM database table spaces. The query returns one table space and its free space percentage using the device event category field as a parameter.	/All Queries/ArcSight Administration/ESM/System Health/Storage/
ASM Database Free Space - by Day	This query on the ASM Database Free Space trend returns the day and minimum free space percentage for one of the ASM database table spaces using the TableName variable as a parameter.	/All Queries/ArcSight Administration/ESM/System Health/Storage/Trend Queries/
ASM Database Free Space - by Hour	This query on the ASM Database Free Space trend returns the hour and free space percentage for one of the ASM database table spaces using the TableName variable as a parameter.	/All Queries/ArcSight Administration/ESM/System Health/Storage/Trend Queries/
Active List Access	This query retrieves the number of times active lists are accessed (addition, deletion, and update of active list entries) in ten minute intervals for the last hour.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Active Lists/
Active List Access (Details)	This query retrieves details about the active lists that are accessed (addition, deletion, and update of active list entries) per active list by ten minute intervals for the last hour.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Active Lists/
Actor Authenticators	This query identifies all the authenticators for actors.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/
Actor Configuration Changes	This query identifies all configuration change audit events made to actor resources. Note: This query does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/

Query Resources, continued

Resource	Description	URI
Actor Full Name and Email Changes	This query identifies information from actor audit events that result from changes to the Full Name or Email attribute of an actor. This query shows the old and the new information.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/
Actor Manager and Department Changes	This query identifies information from actor audit events that result from changes to the Department or Manager attribute of an actor. This query shows the old and the new information.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/
Actor Title and Status Changes	This query identifies information from actor audit events that result from changes to the Title or Status attribute of an actor. This query shows the old and the new information.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/
Actors Created	This query identifies audit events for actors that have been created. Note: This query does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/
Actors Deleted	This query identifies audit events for actors that have been deleted. Note: This query does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/
Actors Updated	This query identifies audit events for actors that have been updated. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/
All Devices Detected Inactive - Last 24 Hours	This query retrieves devices detected as inactive within the last 24 hours.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Devices Detected Inactive - Last 7 Days	This query retrieves devices detected as inactive within the last seven days.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices	This query retrieves devices from the All Monitored Devices active list.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices - Green	This query retrieves devices detected as active within the last 20 minutes.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/

Query Resources, continued

Resource	Description	URI
All Monitored Devices - Green Counter	This query retrieves devices detected as active within the last 20 minutes and sorts them by device product.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices - Red	This query retrieves devices detected as inactive for more than 60 minutes.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices - Red Counter	This query retrieves devices detected as inactive for more than 60 minutes and sorts them by device product.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices - Yellow	This query retrieves devices detected as inactive for more than 20 minutes but less than 60 minutes.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices - Yellow Counter	This query retrieves devices detected as inactive for more than 20 minutes but less than 60 minutes and sorts them by device product.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
ArcSight User Hourly Login Trends	This query on the ArcSight User Login Trends - Hourly trend selects the Target User Name, Attacker Zone, Attacker Address, and the Hour of each Console login for the ArcSight User Login Trends report.	/All Queries/ArcSight Administration/ESM/User Access/User Sessions/
ArcSight User Logins - Last Hour	This query selects events matching the ArcSight Login Rule Firings filter, collecting the Attacker Address, Attacker Asset Name, Attacker Zone, Device Event Category, End Time, Target User Name, and the LoginHour (a variable based on the End Time). This query is used to populate the ArcSight User Login Trends - Hourly trend.	/All Queries/ArcSight Administration/ESM/User Access/User Sessions/
Average Data Monitor Evaluations Per Second	This query identifies the average number of data monitor evaluations per second in ten minute intervals for the last hour.	ArcSight Administration/ESM/System Health/Resources/Data Monitors/
Breakdown by Device Address From Connector	This query selects the top 20 devices within the last 24 hours by connector.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/by Device Address/
Breakdown by Device Address From Vendor and Product	This query selects the top 20 devices within the last 24 hours by the vendor and product.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/by Device Address/

Query Resources, continued

Resource	Description	URI
Breakdown by Event Names From Connector	This query selects the top 20 event names within the last 24 hours by connector.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/by Event Name/
Breakdown by Event Names From Device	This query selects the top 20 event names within the last 24 hours by device.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/by Event Name/
Breakdown by Event Names From Vendor and Product	This query selects the top 20 event names within the last 24 hours by the vendor and product.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/by Event Name/
Breakdown by Event Priority From Connector	This query selects the event priority within the last 24 hours by connector.	ArcSight Administration/ESM/Event Analysis Overview/by Priority/
Breakdown by Event Priority From Device	This query selects the event priority within the last 24 hours by device.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/by Priority/
Breakdown by Event Priority From Vendor and Product	This query selects the events priority within the last 24 hours by vendor and product.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/by Priority/
Cache History by Connectors	This query identifies the cache history for one connector (using a parameter) in the Connector - Caches session list.	/All Queries/ArcSight Administration/Connectors/System Health/Cache/
Connector Average EPS - Last 7 Days	This query identifies the average EPS for all connectors during the last seven days from a trend.	/All Queries/ArcSight Administration/Connectors/System Health/EPS/
Connector Daily Average EPS	This query identifies the daily average EPS for all connectors from a trend. It is used to build a trend-on-trend.	/All Queries/ArcSight Administration/Connectors/System Health/EPS/
Connector Monitor Event	This query identifies the total number of events that connectors forward to the ArcSight Manager per hour.	/All Queries/ArcSight Administration/Connectors/System Health/EPS/
Connector Severity Hourly Stacked Chart	This query replaces the Agent Severity Hourly Stacked Chart Query.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/

Query Resources, continued

Resource	Description	URI
Connector Upgrades Count	This query identifies the count of successful and failed connector upgrades per day in the Connector Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Connector Upgrades Count (Total)	This query identifies the total count of successful and failed connector upgrades in the Connector Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Connector Versions	This query identifies all the connectors with their latest versions in the Connector Versions session list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Versions/
Connector Versions by Type	This query identifies all the connectors with their latest versions by connector type in the Connector Versions session list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Versions/
Connectors - Caching - Long Term	This query identifies data on connectors that have been caching for more than two hours (by default). The query is used on an active list that is maintained by the Connector Monitoring content (rules).	/All Queries/ArcSight Administration/Connectors/System Health/Cache/
Connectors - Caching - Short Term	This query identifies data on connectors that have been caching for under two hours (by default). The query is used on an active list that is maintained by the Connector Monitoring content (rules).	/All Queries/ArcSight Administration/Connectors/System Health/Cache/
Connectors - Down	This query identifies data on connectors that have been down for under 20 minutes (by default). The queries are used on an active list that is maintained by the Connector Monitoring content (rules).	/All Queries/ArcSight Administration/Connectors/System Health/Connector Monitoring/
Connectors - Dropping Events	This query identifies data on connectors that have filled their caches to the point that they are dropping events. The query is used on an active list that is maintained by the Connector Monitoring content (rules).	/All Queries/ArcSight Administration/Connectors/System Health/Cache/
Connectors - Still Down	This query identifies data on connectors that have been down for longer than 20 minutes (by default). The query is used on an active list that is maintained by the Connector Monitoring content (rules).	/All Queries/ArcSight Administration/Connectors/System Health/Connector Monitoring/
Correlation Events Count	This query retrieves the total number of correlation events within the last hour, grouping them by ten minute intervals.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Rules/

Query Resources, continued

Resource	Description	URI
Correlation Events Count (Details)	This query retrieves the number of correlation events per rule within the last hour, grouping them by ten minute intervals.	`/All Queries/ArcSight Administration/ESM/System Health/Resources/Rules/`
Critical Devices Detected Inactive - Last 24 Hours	This query retrieves critical devices detected as inactive within the last 24 hours.	`/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/`
Critical Devices Detected Inactive - Last 7 Days	This query retrieves critical devices detected as inactive within the last seven days.	`/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/`
Critical Monitored Devices	This query retrieves critical devices from the Critical Monitored Devices active list.	`/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/`
Critical Monitored Devices - Green	This query retrieves critical devices detected as active within the last 20 minutes.	`/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/`
Critical Monitored Devices - Green Counter	This query retrieves critical devices detected as active within the last 20 minutes and sorts them by product.	`/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/`
Critical Monitored Devices - Red	This query retrieves critical devices detected as inactive for more than 60 minutes.	`/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/`
Critical Monitored Devices - Red Counter	This query retrieves critical devices detected as inactive for more than 60 minutes and sorts them by device product.	`/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/`
Critical Monitored Devices - Yellow	This query retrieves critical devices detected as inactive for more than 20 minutes but less than 60 minutes.	`/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/`
Critical Monitored Devices - Yellow Counter	This query retrieves critical devices detected as inactive for more than 20 minutes but less than 60 minutes and sorts them by device product.	`/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/`

Query Resources, continued

Resource	Description	URI
Current Cache Status - Caching Events	This query identifies the connectors in the Connectors - Caching session list.	/All Queries/ArcSight Administration/Connectors/System Health/Cache/
Current Cache Status - Dropping Events	This query identifies the connectors in the Connectors - Dropping Events active list.	/All Queries/ArcSight Administration/Connectors/System Health/Cache/
Destination Counts	This query retrieves destination details and the sum of event counts for each destination.	/All Queries/ArcSight Administration/ESM/System Health/Events/
Destination Counts by Connector Type	This query identifies the Agent Type (Connector), Target Zone Name and Target Address, and a count of these events, sorted by Agent Type. The events are not restricted by any filtering conditions.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/
ESM Configuration Changes	This query identifies all the successful configuration changes made to ArcSight ESM. The query identifies the name, the user, the device, and the time the change was made.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Resources/
EPS Received in Correlator	This query retrieves EPS count for events received in correlator.	/All Queries/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Event Count by Agent Severity	This query retrieves events by agent severity with event counts.	/All Queries/ArcSight Administration/ESM/System Health/Events/
Event Count by Source Destination Pairs	This query retrieves event counts ordered by source-destination pairs.	/All Queries/ArcSight Administration/ESM/System Health/Events/
Event Details	This query selects the End Time, Name, Attacker Address, Target Address, Device Address, Device Product, Device Vendor, Priority, Event ID, Device Zone Name, and the local variables Device Information, Vendor and Product, Connector Information.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/
Event Distribution Chart for a Connector Type	This query retrieves the hourly distribution of events for a specific connector type.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/

Query Resources, continued

Resource	Description	URI
Event Name Counts	This query retrieves the event names and their event counts.	/All Queries/ArcSight Administration/ESM/System Health/Events/
Events Count	This query selects the sum of the Aggregated Event Count for non-ArcSight events. The query is used by the Events Count trend.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/
Events Count Last 30 Days	This query on the Events Count trend selects the total number of non-ArcSight events within the last 30 days.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/
Events Count Last 7 Days	This query on the Events Count trend selects the total number of non-ArcSight events and the time stamp within the last seven days.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/
Events by ArcSight Priority (Summary)	This query identifies the ArcSight Priority, event Name, and the sum of the Aggregated Event Count for all events used in the Events by ArcSight Priority (Summary) report.	/All Queries/ArcSight Administration/ESM/System Health/Events/
Events by Connector Type (Summary)	This query retrieves details about various connectors and event counts for each connector.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/
Events by Device (Summary)	This query retrieves the various devices and event counts for each device.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/
Events by Selected Connector Type	This query retrieves events and their counts for a specific connector type.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/
Events for a Destination by Connector Type	This query identifies the Priority, End Time, Agent Type, Attacker Zone Name, Attacker Address, event Name, and the sum of the Aggregated Event Count, ordered by descending priority and by time (hour). The events selected are from the Target Zone and Target Address fields, which default to RFC1918: 192.168.0.0-192.168.255.255 and 192.168.10.10. You can change these default values, either in the Parameters tab of the report or manually when running the report. The Attacker and Target fields are used instead of Source and Destination fields. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/

Query Resources, continued

Resource	Description	URI
Events from a Source by Connector Type	This query identifies the Priority, End Time, Agent Type, Target Zone Name, Target Address, event Name, and the sum of the Aggregated Event Count, ordered by descending priority and by time. The events selected are from the Attacker Zone and Attacker Address fields, which default to RFC1918: 192.168.0.0-192.168.255.255 and 192.168.10.10. You can change these default values either in the Parameters tab of the report or manually when running the report. The Attacker and Target fields are used instead of Source and Destination fields.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/
Failed Connector Upgrades	This query identifies the connectors with failed upgrades (and the reason for the failure) in the Connector Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Failed Queries	This query identifies failed queries for reports, trends, and query viewers. The query is used to build a trend and a query viewer.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Queries/
Failed Queries - Trend	This query retrieves failed queries for reports, trends, and query viewers from a trend.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Queries/
Fired Rule Events	This report does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Rules/
High Volume Connector EPS - By Day	This query identifies the daily average EPS for high volume connectors from a trend.	/All Queries/ArcSight Administration/Connectors/System Health/EPS/
High Volume Connector EPS - Hourly	This query identifies the hourly average EPS for high volume connectors from a trend.	/All Queries/ArcSight Administration/Connectors/System Health/EPS/
Hourly Distribution Chart for Event	This query retrieves the hourly distribution of specific events.	/All Queries/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Hourly Distribution Chart for a Destination Port	This query retrieves the hourly distribution of events for destinations with a specific port.	/All Queries/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/

Query Resources, continued

Resource	Description	URI
Hourly Distribution Chart for a Source Port	This query retrieves the hourly distribution of events for sources with a specific port.	/All Queries/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Hourly EPS in Persistor	This query selects hourly EPS in persistor.	/All Queries/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Hourly Event Counts (Area Chart)	This query retrieves the hourly distribution of event counts.	/All Queries/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart)	This query retrieves the hourly distribution of events by priority rating.	/All Queries/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
IDM Deletions of Actors	This query identifies information about actors that have been marked as deleted by the IDM. This is not the same as deleting the actor resource from the ArcSight ESM system.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/
Invalid Resources	This query retrieves a list of invalid resources from the Invalid Resources active list.	/All Queries/ArcSight Administration/ESM/System Health/Resources/
Invalid Resources (Chart)	This query retrieves the count of invalid resources by resource type from the Invalid Resources active list.	/All Queries/ArcSight Administration/ESM/System Health/Resources/
Last 10 QueryViewer Queries	This query retrieves query duration information for query viewers, ordered by end time.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/QueryViewers/
Last 10 Report Queries	This query retrieves report query duration information, ordered by end time.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Last 10 Trend Queries	This query retrieves trend query duration information, ordered by end time.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Licensing Query	This query retrieves the licensing history for the various license types taken from the License History session list.	/All Queries/ArcSight Administration/ESM/Licensing/

Query Resources, continued

Resource	Description	URI
Longest QueryViewer Queries	This query retrieves query duration information for query viewers, ordered by duration.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/QueryViewers/
Longest QueryViewer Queries - Trend	This query retrieves query viewer query duration information from trends, ordered by duration.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/QueryViewers/
Longest Report Queries	This query retrieves report query duration information, ordered by duration.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Longest Report Queries - Trend	This query retrieves report query duration information from trends, ordered by duration.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Longest Trend Queries	This query retrieves trend query duration information, ordered by duration.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Longest Trend Queries - Trend	This query retrieves trend query duration information from a trend, ordered by duration.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Low Volume Connector EPS - By Day	This query defines the daily average EPS for low volume connectors from a trend.	/All Queries/ArcSight Administration/Connectors/System Health/EPS/
Low Volume Connector EPS - Hourly	This query defines the hourly average EPS for low volume connectors from a trend.	/All Queries/ArcSight Administration/Connectors/System Health/EPS/
MPS Received in Aggregator	This query retrieves messages per second (MPS) count for events received in aggregator.	/All Queries/ArcSight Administration/ESM/Distributed Correlation Monitoring/
New Devices Detected - Last 24 Hours	This query retrieves all new devices detected within the last 24 hours.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
New Devices Detected - Last 7 Days	This query retrieves all new devices detected within the last seven days.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Number of Events matching Rules	This query retrieves the total number of events matching rules (events matching filter rules, join rules, and the total of both types of rules) within the last hour grouping them by ten minute intervals.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Rules/

Query Resources, continued

Resource	Description	URI
Query Counts During Last 24 hr	This query identifies the resource type and its counts from the Query Running Time active list.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Queries/
Query Counts During Last Week	This query retrieves resource types and their counts from the Query Running Time active list.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Queries/
QueryViewer Failures	This query retrieves query duration information for failed query viewers.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/QueryViewers/
QueryViewer Queries	This query retrieves query duration information for query viewers used to build a trend.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/QueryViewers/
Report Queries	This query retrieves report query duration information used to build a trend.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Report Query Failures	This query retrieves failed query duration information for reports.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Resource Created Report	This query identifies all the resources that have been created by ArcSight users. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Resources/
Resource Deleted Report	This query identifies all the resources that have been deleted by ArcSight users. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Resources/
Resource History Report	This query identifies all the resources that have been created, updated, or deleted by ArcSight users. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Resources/
Resource Updated Report	This query identifies all the resources that have been updated by ArcSight users. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Resources/
Rules Engine Warning Messages	This query retrieves warning messages received from the rules engine.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Rules/
Running Report Queries	This query retrieves currently running report queries.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/

Query Resources, continued

Resource	Description	URI
Running Trend Queries	This query retrieves running trend query duration information.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Session List Access	This query retrieves the number of times session lists are accessed (addition, deletion, and update of session list entries) in ten minute intervals for the last hour.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Session Lists/
Session List Access (Details)	This query retrieves details of session list access (addition, deletion, and update of active list entries) per session list in ten minute intervals for the last hour.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Session Lists/
Source Counts by Connector Type	This query identifies the Agent Type (Connector), Attacker Zone Name and Attacker Address, and a count of these events, sorted by Agent Type. The events are not restricted by any filtering conditions.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/
Source Counts by Event Name	This query retrieves event names by source address in addition to event counts.	/All Queries/ArcSight Administration/ESM/System Health/Events/
Storage Licensing Data	This query selects the raw event length for each day for all the connectors from an active list.	/All Queries/ArcSight Administration/ESM/Licensing/
Storage Licensing Data - trend	This query selects the raw event length for each day for all the connectors from a trend.	/All Queries/ArcSight Administration/ESM/Licensing/
Storage Licensing Data by Connector Name - trend	This query selects the raw event length by connector name for each day from a trend.	/All Queries/ArcSight Administration/ESM/Licensing/
Storage Licensing Data by Connector Type - trend	This query selects the raw event length by connector type for each day from a trend.	/All Queries/ArcSight Administration/ESM/Licensing/
Successful Connector Upgrades	This query identifies the connectors with successful upgrades (and the new connector version) in the Connectors Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/

Query Resources, continued

Resource	Description	URI
Top 10 Events	This query retrieves the top events ordered by their counts.	/All Queries/ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Top 10 Inbound Events	This query retrieves the top inbound events ordered by their counts.	/All Queries/ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Top 10 Outbound Events	This query retrieves the top outbound events ordered by their counts.	/All Queries/ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Top Accessed Active Lists	This query retrieves the most accessed active lists (addition, deletion, and update of active list entries) within the last hour and orders them by most accessed.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Active Lists/
Top Accessed Session Lists	This query retrieves the most accessed session lists (addition, deletion, and update of session list entries) with in the last hour and orders them by most accessed.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Session Lists/
Top Connector Types Chart	This query retrieves connector details with event counts for each connector type.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/
Trend Query	This query retrieves trend query duration information used to build a trend.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Trend Query Failures	This query retrieves failed trend query duration information.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Upgrade History by Connector	This query identifies all the connector upgrades (successful and failed) by connector in the Connector Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Upgrade History by Connector Type	This query identifies all the connector upgrades (successful and failed) by connector type in the Connector Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/

Query Resources, continued

Resource	Description	URI
User Login Logout Report	This query retrieves user login (success/fail) and logout events.	/All Queries/ArcSight Administration/ESM/User Access/User Sessions/
Version History by Connector	This query identifies all the connector versions by connector in the Connector Versions session list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Versions/
Version History by Connector Type	This query identifies all the connectors and connector versions by connector type in the Connector Versions session list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Versions/

Query Viewers

The following table lists all the query viewers.

Query Viewer Resources

Resource	Description	URI
Active Critical Devices - last 20 min	This query viewer displays details for the critical devices detected as active for the last 20 minutes.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Active Critical Devices by Product - last 20 min	This query viewer displays details for the critical devices detected as active for the last 20 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Active Devices - last 20 min	This query viewer displays details for the devices detected as active for the last 20 minutes.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Active Devices by Product - last 20 min	This query viewer displays details for the devices detected as active within the last 20 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Actor Authenticators	This query viewer displays a list of all the authenticators for actors.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/
Actor Configuration Changes	This query viewer displays all audit events that result from changes to actor resources. Note: This query viewer does not populate all values when running in Turbo Mode Fastest.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/

Query Viewer Resources, continued

Resource	Description	URI
Actor Full Name and Email Changes	This query viewer displays information from actor audit events that result from changes to the Full Name or Email attribute of an actor. This query viewer shows the old and the new information.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/
Actor Manager and Department Changes	This query viewer displays information from actor audit events that result from changes to the Department or Manager attribute of an actor. This query viewer shows the old and the new information.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/
Actor Title and Status Changes	This query viewer displays information from actor audit events that result from changes to the Title or Status attribute of an actor. This query viewer shows the old and the new information.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/
Actors Created	This query viewer displays all the audit events for actors that have been created. Note: This query viewer does not populate all values when running in Turbo Mode Fastest.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/
Actors Deleted	This query viewer displays audit events for actors that have been deleted. Note: This query viewer does not populate all values when running in Turbo Mode Fastest.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/
Actors Updated	This query viewer displays audit events for actors that have been updated. Note: This query viewer does not populate all values when running in Turbo Mode Fastest.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/
All Monitored Devices	This query viewer displays details for the devices detected within the last 365 days.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Breakdown by Device Address From Connector	This query viewer shows the top 20 devices within the last 24 hours by connector.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/by Device Address/
Breakdown by Device Address From Vendor and Product	This query viewer shows the top 20 devices within the last 24 hours by vendor and product.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/by Device Address/
Breakdown by Event Names From Connector	This query viewer shows the top 20 event names within the last 24 hours by connector.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/by Name/

Query Viewer Resources, continued

Resource	Description	URI
Breakdown by Event Names From Device	This query viewer shows the top 20 event names within the last 24 hours by device.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/by Name/
Breakdown by Event Names From Vendor and Product	This query viewer shows the top 20 event names within the last 24 hours by vendor and product.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/by Name/
Breakdown by Event Priority From Connector	This query viewer shows the event priority within the last 24 hours by connector.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/by Priority/
Breakdown by Event Priority From Device	This query viewer shows the event priority within the last 24 hours by device.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/by Priority/
Breakdown by Event Priority From Vendor and Product	This query viewer shows the event priority within the last 24 hours by vendor and product.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/by Priority/
Connectors - Caching - Long Term	This query viewer displays data on connectors that have been caching for more than two hours (by default). This query viewer queries on an active list that is maintained by the Connector Monitoring content (rules), so it can update every minute.	/All Query Viewers/ArcSight Administration/Connectors/System Health/
Connectors - Caching - Short Term	This query viewer displays data on connectors that have been caching for under two hours (by default). This query viewer queries on an active list that is maintained by the Connector Monitoring content (rules), so it can update every minute.	/All Query Viewers/ArcSight Administration/Connectors/System Health/
Connectors - Down - Long Term	This query viewer displays data on connectors that have been down for longer than 20 minutes (by default). This query viewer queries on an active list that is maintained by the Connector Monitoring content (rules), so it can update every minute.	/All Query Viewers/ArcSight Administration/Connectors/System Health/
Connectors - Down - Short Term	This query viewer displays data on connectors that have been down for under 20 minutes (by default). This query viewer queries on an active list that is maintained by the Connector Monitoring content (rules), so it can update every minute.	/All Query Viewers/ArcSight Administration/Connectors/System Health/

Query Viewer Resources, continued

Resource	Description	URI
Connectors - Dropping Events	This query viewer displays data on connectors that have filled their caches to the point that they are dropping events. This query viewer queries on an active list that is maintained by the Connector Monitoring content (rules), so it can update every minute.	/All Query Viewers/ArcSight Administration/Connectors/System Health/
Critical Monitored Devices	This query viewer displays details for all critical devices.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Event Details	This query viewer shows the event details.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/
Events Count Last 30 Days	This query viewer shows the total number of non-ArcSight events within the last 30 days.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/
Events Count Last 7 Days	This query viewer shows the total number of non-ArcSight events each day for the last seven days.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/
Hourly EPS Received in Correlator	This query viewer displays hourly EPS reveived in correlator.	/All Query Viewers/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Hourly Messages Per Second Received in Aggregator	This query viewer displays hourly messages per second received in aggregator.	/All Query Viewers/ArcSight Administration/ESM/Distributed Correlation Monitoring/
IDM Deletions of Actors	This query viewer displays information about actors that have been marked as deleted by the IDM. This is not the same as deleting the actor resource from the ArcSight ESM system. Note: This query viewer does not populate all values when running in Turbo Mode Fastest.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/
Inactive Critical Devices - more than 20 min	This query viewer displays details for the critical devices detected as inactive for more than 20 minutes but less than 60 minutes.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Inactive Critical Devices - more than 60 min	This query viewer displays details for the critical devices detected as inactive for more than 60 minutes.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/

Query Viewer Resources, continued

Resource	Description	URI
Inactive Critical Devices by Product - more than 20 min	This query viewer displays details for the critical devices detected as inactive for more than 20 minutes but less than 60 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Inactive Critical Devices by Product - more than 60 min	This query viewer displays details for the critical devices detected as inactive for more than 60 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Inactive Devices - more than 20 min	This query viewer displays details for the devices detected as inactive for more than 20 minutes but less than 60 minutes.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Inactive Devices - more than 60 min	This query viewer displays details for the devices detected as inactive for more than 60 minutes.	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Inactive Devices by Product - more than 20 min	This query viewer displays details for the devices detected as inactive for more than 20 minutes but less than 60 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Inactive Devices by Product - more than 60 min	This query viewer displays details for the devices detected as inactive for more than 60 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Last 10 Query Viewer Queries	This query viewer shows the last ten query viewer query duration information.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Query Viewers/
Last 10 Report Queries	This query viewer shows the duration information for the last ten report queries.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Last 10 Trend Queries	This query viewer shows the duration information for the last ten trend queries.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Query Counts During Last 24 hr	This query viewer shows the query and its counts during the last 24 hours.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/
Query Failures During Last 24 hr	This query viewer displays failed queries for reports, trends, and query viewers.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/

Query Viewer Resources, continued

Resource	Description	URI
Query Viewer Failures During Last 24 hr	This query viewer shows the failed query viewers during the last 24 hours.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Query Viewers/
Report Query Failures During Last 24 hr	This query viewer shows the duration information for failed report queries during the last 24 hours.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Running Report Queries	This query viewer shows the currently running report queries.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Running Trend Queries	This query viewer shows the currently running trend queries.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Top 10 Longest Query Viewer Queries During Last 24 hr	This query viewer shows the duration information for the top ten longest query viewers during the last 24 hours.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Query Viewers/
Top 10 Longest Report Queries During Last 24 hr	This query viewer shows the duration information for the top ten longest report queries during the last 24 hours.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Top 10 longest Trend Queries During Last 24 hr	This query viewer shows the duration information for the top ten longest trend queries during the last 24 hours.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Trend Queries Failures During Last 24 hr	This query viewer shows the duration information for failed trend queries during the last 24 hours.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/

Reports

The following table lists all the reports.

Report Resources

Resource	Description	URI
Active List Access	This report shows active list access statistics. A chart shows the number of added, deleted, and updated active list entries within the previous day, grouping the counts by ten minute intervals. A table shows the details of the active list access, grouping the number by time interval and active list name.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Active Lists/
Actor Full Name and Email Changes	This report shows information from actor audit events that result from changes to the Full Name or Email attribute of an actor. The report shows the old and new information.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/
Actor Manager and Department Changes	This report shows information from actor audit events that result from changes to the Department or Manager attribute of an actor. This report shows the old and the new information.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/
Actor Title and Status Changes	This report shows information from actor audit events that result from changes to the Title or Status attribute of an actor. The report shows the old and new information.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/
All Devices Detected Inactive - Last 24 Hours	This report shows all devices detected as inactive within the last 24 hours.	/All Reports/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Devices Detected Inactive - Last 7 Days	This report shows all devices detected as inactive within the last seven days.	/All Reports/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices	This report shows all devices detected within the last 365 days.	/All Reports/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
ArcSight User Login Trends	This report shows a summary of the number of ArcSight user logins within the previous day. A bar chart shows the total number of logins by user and a table shows the number of logins by user per hour.	/All Reports/ArcSight Administration/ESM/User Access/User Sessions/

Report Resources, continued

Resource	Description	URI
ArcSight User Logins - Last Hour	This report shows details for all the ArcSight user logins within the past hour. The report contains a table showing the source host, the username, and the login time.	/All Reports/ArcSight Administration/ESM/User Access/User Sessions/
Cache History by Connectors	This report shows the cache history by connector (within the last 24 hours by default) sorted chronologically. Notes: When running this report, you can specify the Connector URI (located in the connector resource navigator or the Connector Information active list) in the ConnectorURI field in the custom parameters for the report. By default, the report shows all of the connectors known by the system. You can further specify the ConnectorURI parameter to narrow down the connector cache histories reported, from groups (such as /All Connectors/Site Connectors/) down to a specific connector (such as /All Connectors/Site Connectors/DMZ/WUC-1). The default time range of this report is the past three to four months.	/All Reports/ArcSight Administration/Connectors/System Health/Cache/
Configuration Changes by Type	This report shows recent actor configuration changes. A table lists all the changes grouped by type and user, and sorts them chronologically.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/
Configuration Changes by User	This report shows recent actor configuration changes. A table lists all the changes grouped by user and type, and sorts them chronologically.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/
Connector Severity Hourly Stacked Chart	This report shows hourly event count data ordered by severity in a stacked chart.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Connector Upgrades Count	This report shows the total count of successful and failed connector upgrades in a pie chart, and the counts per day in a table (within the last seven days by default).	/All Reports/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Connector Versions	This report lists all the connectors with their latest versions (within the last seven days by default). The list is grouped by connector type, connector zone, and connector address.	/All Reports/ArcSight Administration/Connectors/Configuration Changes/Versions/

Report Resources, continued

Resource	Description	URI
Connector Versions by Type	This report lists all the connectors with their latest versions (within the last seven days by default). The list is grouped by connector version, connector zone, and connector address.	/All Reports/ArcSight Administration/Connectors/Configuration Changes/Versions/
Correlation Events Statistics	This report shows correlation event statistics. A chart shows the number of correlation events within the last hour, grouping them by ten minute intervals. A table shows details of the number of correlation events, grouping them by rule name and time interval.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Rules/
Created	This report shows a list of all the actors created on the previous day. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/
Critical Devices Detected Inactive - Last 24 Hours	This report shows critical devices detected as inactive within the last 24 hours.	/All Reports/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Critical Devices Detected Inactive - Last 7 Days	This report shows critical devices detected as inactive within the last seven days.	/All Reports/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Critical Monitored Devices	This report shows all critical devices currently being monitored.	/All Reports/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Current Cache Status	This report lists the connectors that are currently caching and dropping events. The first table shows the connectors that are dropping events. The second table shows the connectors that are caching.	/All Reports/ArcSight Administration/Connectors/System Health/Cache/
Data Monitor Evaluations Statistics	This report shows a chart with the average number of data monitor evaluations per second.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Data Monitors/
Deleted	This report displays audit event information for actors that have been deleted. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/

Report Resources, continued

Resource	Description	URI
Destination Counts	This report shows destination details and the sum of event counts for each destination.	/All Reports/ArcSight Administration/ESM/System Health/Events/
Destination Counts by Connector Type	This report displays a table showing the connector type, the destination zones and addresses, and the count from each source. Make sure you select a filter parameter other than the default of All Events. You can also adjust the Start and End times of the report to reduce the number of events selected.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
ESM Configuration Changes by Type	This report shows recent ArcSight ESM configuration changes. A table lists all the changes, grouped by type and user, and sorts them chronologically. This report enables you to find all the configuration changes of a certain type quickly.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Resources/
ESM Configuration Changes by User	This report shows recent ArcSight ESM configuration changes. A table lists all the changes, grouped by user and type, and sorts them chronologically. This report enables you to find all the configuration changes made by a specific user.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Resources/
Event Count by Agent Severity	This report shows events by agent severity with event counts.	/All Reports/ArcSight Administration/ESM/System Health/Events/
Event Count by Source Destination Pairs	This report shows event counts ordered by source-destination pairs.	/All Reports/ArcSight Administration/ESM/System Health/Events/
Event Distribution Chart for a Connector Type	This report shows the hourly distribution of events for a specific connector type.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Event Name Counts	This report shows event names and their event counts.	/All Reports/ArcSight Administration/ESM/System Health/Events/

Report Resources, continued

Resource	Description	URI
Events by ArcSight Priority (Summary)	This report displays a table of all events, grouped by ArcSight Priority, showing the count of each event occurrence within that priority. Note: This report shows all ArcSight events; use the FilterBy parameter to limit the output to the areas of most interest.	/All Reports/ArcSight Administration/ESM/System Health/Events/
Events by Connector Type (Summary)	This report shows events by connector type and the event counts for each connector type.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Events by Device (Summary)	This report shows various devices and event counts for each device.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Events by Selected Connector Type	This report shows events and their counts for a specific connector type.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Events for a Destination by Connector Type	This report displays a table of all events showing time, source, and connector information based on the Target Zone and Target Address fields. These fields are used as the event destinations, and default to RFC1918: 192.168.0.0-192.168.255.255 and 192.168.10.10. You can change these default values either in the Parameters tab of the report or manually when running the report. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Events from a Source by Connector Type	This report displays a table of all events showing time, destination, and connector information based on the Attacker Zone and Attacker Address fields. These fields are used as the source of the events, and default to RFC1918: 192.168.0.0-192.168.255.255 and 192.168.10.10. You can be change these default values either in the Parameters tab of the report or manually when running the report.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Failed Connector Upgrades	This report lists the connectors with failed upgrades (within the last seven days by default). The list is grouped by connector zone, connector address, connector name, and connector ID, and shows the reason for the failure.	/All Reports/ArcSight Administration/Connectors/Configuration Changes/Upgrades/

Report Resources, continued

Resource	Description	URI
Failed Queries	This report shows the failed queries for trend, report, and query viewers. The default time frame is one week.	`/All Reports/ArcSight Administration/ESM/System Health/Resources/Reporting/`
Fired Rule Events	This report does not populate all values when running in Turbo Mode Fastest.	`/All Reports/ArcSight Administration/ESM/System Health/Resources/Rules/`
High Volume Connector EPS - Daily	This report shows the hourly average EPS for high volume connectors. The default time frame is yesterday. By default, a connector with a daily average EPS greater than or equal to 100 is considered a high volume connector.	`/All Reports/ArcSight Administration/Connectors/System Health/EPS/`
High Volume Connector EPS - Weekly	This report shows the daily average EPS for high volume connectors. The default time frame is one week. By default, a connector with a daily average EPS greater than or equal to 100 is considered a high volume connector.	`/All Reports/ArcSight Administration/Connectors/System Health/EPS/`
Hourly Distribution Chart for Event	This report shows the hourly distribution of specific events.	`/All Reports/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/`
Hourly Distribution Chart for a Destination Port	This report shows the hourly distribution of events for destinations with a specific port.	`/All Reports/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/`
Hourly Distribution Chart for a Source Port	This report shows the hourly distribution of events for sources with a specific port.	`/All Reports/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/`
Hourly Event Counts (Area Chart)	This report shows the hourly distribution of event counts.	`/All Reports/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/`
Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart)	This report shows the hourly distribution of events by priority rating.	`/All Reports/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/`

Report Resources, continued

Resource	Description	URI
IDM Deletions of Actors	This report shows the list of all the actors that have been marked as deleted by the IDM. This is not the same as deleting the actor resource from the ArcSight ESM system. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/
Invalid Resources	This report shows a list of resources that are invalid. A chart shows the count of invalid resources by resource type. A table lists all the invalid resources grouped by type and sorted by URI.	/All Reports/ArcSight Administration/ESM/System Health/Resources/
Licensing Report	This report shows the licensing history for one of the license types. The chart shows the current count and the count limit in a chart. By default, the licensing history is over the last seven days.	/All Reports/ArcSight Administration/ESM/Licensing/
Licensing Report (All)	This report shows the licensing history for all the license types. The charts show the current count and the count limit for each of the license types. By default, the licensing history is over the last seven days.	/All Reports/ArcSight Administration/ESM/Licensing/
Longest QueryViewer Queries	This report shows query duration information for query viewers. A chart shows the top ten longest queries for a query viewer and a table shows the duration details for query viewers. The default time frame is one week.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Reporting/
Longest Report Queries	This report shows query duration information for reports. The chart shows the top ten longest report queries and the table shows the duration details for the report queries. The default time frame is one week.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Reporting/
Longest Trend Query	This report shows query duration information for trends. A chart shows the top ten longest trend queries and a table shows the duration details for trend queries. The default time frame is one week.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Reporting/
Low Volume Connector EPS - Daily	This report shows the hourly average EPS for low volume connectors. The default time frame is yesterday. By default, a connector with a daily average EPS less than 100 is considered a low volume connector.	/All Reports/ArcSight Administration/Connectors/System Health/EPS/

Report Resources, continued

Resource	Description	URI
Low Volume Connector EPS - Weekly	This report shows the daily average EPS for low volume connectors. The default time frame is one week. By default, a connector with a daily average EPS less than 100 is considered a low volume connector.	`/All Reports/ArcSight Administration/Connectors/System Health/EPS/`
New Devices Detected - Last 24 Hours	This report shows new devices detected within the last 24 hours.	`/All Reports/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/`
New Devices Detected - Last 7 Days	This report shows new devices detected within the last seven days.	`/All Reports/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/`
Number of Events Matching Rules	This report shows the total number of events matching rules within the last hour, grouping them by ten minute intervals. A chart shows the number of events matching filter rules, join rules, and the total of both types of rules.	`/All Reports/ArcSight Administration/ESM/System Health/Resources/Rules/`
Query Counts by Type	This report shows query counts grouped by type. The default time frame is one week.	`/ArcSight Administration/ESM/System Health/Resources/Reporting/`
Resource Created Report	This report shows a list of all the resources created by ArcSight users in the previous day. Note: This report does not populate all values when running in Turbo Mode Fastest.	`ArcSight Administration/ESM/Configuration Changes/Resources/`
Resource Deleted Report	This report shows a list of all the resources deleted by ArcSight users during the previous day. Note: This report does not populate all values when running in Turbo Mode Fastest.	`/All Reports/ArcSight Administration/ESM/Configuration Changes/Resources/`
Resource History Report	This report shows a list of all the resources that have been created, updated, or deleted by ArcSight users within the previous day. Note: This report does not populate all values when running in Turbo Mode Fastest.	`/All Reports/ArcSight Administration/ESM/Configuration Changes/Resources/`
Resource Updated Report	This report shows a list of all the resources updated by ArcSight users within the previous day. Note: This report does not populate all values when running in Turbo Mode Fastest.	`/All Reports/ArcSight Administration/ESM/Configuration Changes/Resources/`
Rules Engine Warning Messages	This report shows warning messages received from the rules engine.	`/All Reports/ArcSight Administration/ESM/System Health/Resources/Rules/`

Report Resources, continued

Resource	Description	URI
Session List Access	This report shows session list access statistics. A chart shows the number of added, deleted, and updated session list entries in the last hour, grouping the counts by 10 minute intervals. A table shows the details of the session list access, grouping the number by time interval and active list name.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Session Lists/
Source Counts by Connector Type	This report shows the connector type, the source zones and IP addresses, and the count from each source within the specified time period. Make sure that a filter parameter other than the default of All Events is selected. You can also adjust the start and end times of the report to reduce the number of events selected.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Source Counts by Event Name	This report shows event names by source address in addition to event counts.	/All Reports/ArcSight Administration/ESM/System Health/Events/
Storage Licensing Report	This report shows an overview of the storage used by the system for each day, with a breakdown of the raw event data size sent by each connector and by connector type.	/All Reports/ArcSight Administration/ESM/Licensing/
Successful Connector Upgrades	This report lists the connectors with successful upgrades (within the last seven days by default). The list is sorted chronologically.	/All Reports/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Top 10 Events	This report shows the top events ordered by their counts.	/All Reports/ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Top 10 Inbound Events	This report shows the top inbound events ordered by their counts.	/All Reports/ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Top 10 Outbound Events	This report shows the top outbound events ordered by their counts.	/All Reports/ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Top Accessed Active Lists	This report shows the top ten accessed active lists. A chart shows the top ten accessed active lists in the previous day, grouping the counts by ten minute intervals. A table shows the details of the active list access, grouping the number by active list name and time interval.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Active Lists/

Report Resources, continued

Resource	Description	URI
Top Accessed Session Lists	This report shows the top ten accessed session lists. A chart shows the top ten accessed session lists within the last hour, grouping the counts by ten minute intervals. A table shows details of the session list access, grouping the number by active list name and time interval.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Session Lists/
Top Connector Types Chart	This report shows connector details with event counts for each connector type.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Updated	This report shows a list of all the actors updated on the previous day. Note: This Report does not populate all values when running in Turbo Mode Fastest.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/
Upgrade History by Connector	This report shows the upgrade history by connector (within the last seven days by default) sorted chronologically. Note: When running the report, be sure to use the connector ID located in the connector resource and copy-paste the ID in to the ConnectorID field in the Custom Parameters for the report.	/All Reports/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Upgrade History by Connector Type	This report shows the upgrade history by connector type (within the last seven days by default). The report is grouped by connector zone, connector address, connector name, and connector ID.	/All Reports/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
User Login Logout Report	This report shows user login events (success and fail) and logout events.	/All Reports/ArcSight Administration/ESM/User Access/User Sessions/

Report Resources, continued

Resource	Description	URI
Version History by Connector	This report shows the version history by connector (within the last seven days by default) sorted chronologically. Note: When running the report, use the connector ID (located in the connector resource) and copy-paste it in to the ConnectorID field in the Custom Parameters for the report.	`/All Reports/ArcSight Administration/Connectors/Configuration Changes/Versions/`
Version History by Connector Type	This report shows the version history by connector type (within the last seven days by default). The list is grouped by connector zone, connector address, connector name, and connector ID.	`/All Reports/ArcSight Administration/Connectors/Configuration Changes/Versions/`
Web Users Licensing Report	This report shows the licensing history for web users. The chart shows the current count and the count limit in a chart. The licensing history is over the last 7 days, by default.	`/ArcSight Administration/ESM/ Licensing/`

Report Templates

The following table lists all the report templates.

Report Template Resources

Resource	Description	URI
Licensing Report	This report template is used by the licensing reports and shows one chart (bar and line). The orientation is landscape.	`/All Report Templates/ArcSight Administration/Licensing/`
Licensing Report (All)	This report template is used by the licensing reports and shows several charts (bar and line). The orientation is portrait.	`/All Report Templates/ArcSight Administration/Licensing/`

Rules

The following table lists all the rules.

Rule Resources

Resource	Description	URI
ASM Database Free Space - Critical	This rule detects internal events showing that one (or more) of the ASM database table spaces has a very low free space percentage. This is considered critical when the free space goes below the threshold defined in the server.properties file (two percent by default). A notification is sent to the Database Storage Operator group.	/All Rules/ArcSight Administration/ESM/System Health/Storage/
ASM Database Free Space - Warning	This rule detects internal events showing that one (or more) of the ASM database table spaces has a low free space percentage. This is considered a warning when the free space goes below the threshold defined in the server.properties file (five percent by default).	/All Rules/ArcSight Administration/ESM/System Health/Storage/
ASM Database Status Change - Critical	This rule detects if the database status is critical. This rule detects the insert and retrieval time for an event; the status is considered critical when the EventInsertTimeNanos field is greater than or equal to 50,000. This rule requires two such events within three minutes. After the first event, the agentSeverity event field is set to very high.	/All Rules/ArcSight Administration/ESM/System Health/Storage/
ASM Database Status Change - Down	This rule detects if the database status is down. This rule detects the insert and retrieval time for an event; the status is considered down when the EventInsertTimeNanos field is equal to zero. This rule requires two such events within three minutes. After the first event, the agentSeverity event field is set to unknown.	/All Rules/ArcSight Administration/ESM/System Health/Storage/
ASM Database Status Change - Normal	This rule detects if the database status is normal. This rule detects the insert and retrieval time of the event; the status is considered normal when the EventInsertTimeNanos (insert time in nanoseconds) field is less than or equal to 20,000. This rule requires two such events within two minutes. After the first event, the agentSeverity event field is set to low.	/All Rules/ArcSight Administration/ESM/System Health/Storage/

Rule Resources, continued

Resource	Description	URI
ASM Database Status Change - Space Critical	This rule detects if the database status is critical due to storage concerns. This rule detects a base event indicating that the database storage space is low. This rule only requires one such event to trigger. After the first event, the agentSeverity event field is set to very high.	`/All Rules/ArcSight Administration/ESM/System Health/Storage/`
ASM Database Status Change - Space Now Available	This rule detects if the database status has returned to normal because storage space has been freed or added. This rule detects a base event indicating that database storage space is available. This rule only requires one such event to trigger. After the first event, the agentSeverity event field is set to Low.	`/All Rules/ArcSight Administration/ESM/System Health/Storage/`
ASM Database Status Change - Warning	This rule detects if the database status is at a warning level. This rule detects the insert and retrieval time for an event; the status is considered a warning when the EventInsertTimeNanos field is between 20,000 and 50,000. This rule requires two such events within three minutes. After the first event, the agentSeverity event field is set to medium.	`/All Rules/ArcSight Administration/ESM/System Health/Storage/`
Alert - Critical Devices inactive for more than 1 hour	This rule triggers when a Connector Device Status event for critical devices has a zero in Device Custom Number2 and a Device Custom Date earlier than 60 minutes ago, which indicates that the device has been inactive for more than one hour. After the rule triggers, a notification is sent to the Device Administrators.	`/All Rules/ArcSight Administration/Devices/`
All Monitored Devices	This rule triggers when a Connector Device Status event has a non-zero Device Custom Number2 (indicating that the device is active and sending base events to the connector since the last check). After the rule triggers, the entry is created or updated in the All Monitored Devices active list.	`/All Rules/ArcSight Administration/Devices/`
ArcSight User Login	This rule detects ArcSight user login events. This rule adds the user information to the ArcSight User Sessions session list.	`/All Rules/ArcSight Administration/ESM/User Access/User Sessions/`
ArcSight User Login Timeout	This rule detects ArcSight user login timeout events. This rule terminates the ArcSight user session in the ArcSight User Sessions session list when an ArcSight user login timeout occurs.	`/All Rules/ArcSight Administration/ESM/User Access/User Sessions/`

Rule Resources, continued

Resource	Description	URI
ArcSight User Logout	This rule detects ArcSight user logout events. This rule terminates the ArcSight user session in the ArcSight User Sessions session list when an ArcSight user logout occurs.	`/All Rules/ArcSight Administration/ESM/User Access/User Sessions/`
Connector Added to Black List	This rule monitors the Black List - Connectors active list for new connector information. When a connector is added to the black list, this rule updates the other Connector Monitoring active lists to remove that connector from the status displays.	`/All Rules/ArcSight Administration/Connectors/System Health/Custom/`
Connector Cache Empty	This rule triggers when there is a connector cache empty event. The rule removes the connector from the Connector Caching and Connector Dropping Events active lists, and terminates the entry in the Connector - Caches session list.	`/All Rules/ArcSight Administration/Connectors/System Health/`
Connector Caching	This rule triggers when there is a connector caching event. The rule adds the connector and cache related information to the Connector Caching active list and the Connector - Caches session list.	`/All Rules/ArcSight Administration/Connectors/System Health/`
Connector Deleted	This rule identifies connector deleted events that are sent when a connector is deleted from the resource tree. On the first event, the session for the corresponding connector is terminated in the Connector Versions session list, and the connector is also removed from the Connectors - Down active list.	`/All Rules/ArcSight Administration/Connectors/Configuration Changes/`
Connector Discovered or Updated	This rule detects new connectors reporting to ESM and adds them to active lists to be monitored. Device Event Class ID = agent:007 is related to Agent Registration events. Device Event Class ID = agent:030 is related to Agent Start events. Device Event Class ID = agent:031 is related to Agent Shutdown events. Device Event Class ID = agent:101 is related to Agent Connection events. Device Event Class ID = agent:103 is related to Agent Heartbeat Timeout events. These events contain the detailed information necessary to populate the Connectors active lists.	`/All Rules/ArcSight Administration/Connectors/System Health/`

Rule Resources, continued

Resource	Description	URI
Connector Down	This rule triggers when it there is a connector shutdown or heartbeat timeout event (except for connectors listed in the Black List - Connectors filter). The rule adds connector information to the Connectors - Down active list.	/All Rules/ArcSight Administration/Connectors/System Health/
Connector Dropping Events	This rule triggers when there is a connector dropping events event. The rule adds the connector and cache related information to the Connector Dropping Events active list and the Connector - Caches session list. A case can be created and a notification can be sent to the SOC operators. Note: The case creation and notification actions are disabled by default.	/All Rules/ArcSight Administration/Connectors/System Health/
Connector Still Caching	This rule triggers when the TTL (two hours by default) for an entry in the Connectors - Caching active list expires. It then puts the connector information into the Connectors - Still Caching active list, creates a case and sends a notification to SOC Operators. Note: The case creation and notification actions are disabled by default.	/All Rules/ArcSight Administration/Connectors/System Health/
Connector Still Down	This rule triggers when the TTL (20 minutes by default) for an entry in the Connectors - Down active list expires. The rule then adds the connector information to the Connectors - Still Down active list, creates a case and sends a notification to SOC Operators. Note: The case creation and notification actions are disabled by default.	/All Rules/ArcSight Administration/Connectors/System Health/
Connector Up	This rule triggers when there is a connector started event (except for connectors that match the conditions in the Black List - Connectors filter). The rule removes the connector from the connector connection status active lists.	/All Rules/ArcSight Administration/Connectors/System Health/
Connector Upgrade Failed	This rule detects failed connector upgrades. On every event, the connector information is added to the Connector Upgrades active list.	/All Rules/ArcSight Administration/Connectors/Configuration Changes/
Connector Upgrade Successful	This rule detects successful connector upgrades. On every event, the connector information is added to the Connector Upgrades active list. A new session is created in the Connector Versions session list. Note: The Agent configuration updated events are removed to avoid duplicate entries in the active list and session list.	/All Rules/ArcSight Administration/Connectors/Configuration Changes/

Rule Resources, continued

Resource	Description	URI
Connector Version Detected	This rule detects connector start events. The rule triggers if the connector is not yet in the Connector Versions session list. On every event, a new session with the connector information is created in the Connector Versions session list.	/All Rules/ArcSight Administration/Connectors/Configuration Changes/
Critical Monitored Devices	This rule triggers when a Connector Device Status event has a non-zero Device Custom Number2 (indicating that the device is active and sending base events to the connector since the last check) and if the device entry exists in the Critical Monitored Devices active list. After the rule triggers, the active list entry is updated.	/All Rules/ArcSight Administration/Devices/
Detect Event Counts for Persistor	This rule populates the event counts for distributed correlation to a list.	/All Rules/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Detect Events for Distributed Correlation	This rule populates the event counts for distributed correlation to a list.	/All Rules/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Excessive Rule Recursion	This rule detects excessive rule recursion. This rule looks for events coming from the ArcSight Security Manager with the Device Event Category set to /Rule/Warning/Loop. This rule only requires one such event within five minutes. After this rule is triggered, a notification is sent to the SOC Operators.	/All Rules/ArcSight Administration/ESM/System Health/Resources/Rules/
Invalid Resource Deleted	This rule removes an invalid resource from the Invalid Resources active list when that resource is deleted. The rule triggers only if the resource that has been deleted is in the Invalid Resources active list.	/All Rules/ArcSight Administration/ESM/System Health/Resources/
License Audit Event Detected	This rule triggers when a license audit event is detected. The rule adds the license type, the current count, and the count limit to the License History session list.	/All Rules/ArcSight Administration/ESM/Licensing/
Logger Sensor Status	This rule identifies Logger system health events related to hardware sensor status. The rule updates the Logger Status and Logger Sensor Type Status with the Logger IP address, the sensor type, the sensor name, and the sensor status. This rule is disabled by default. Enable the rule if you have Logger in your environment.	/All Rules/ArcSight Administration/Logger/System Health/

Rule Resources, continued

Resource	Description	URI
Logger Sensor Type Status	This rule identifies Logger Sensor Status correlation events and triggers only if all the sensor statuses for the same sensor type for a Logger are in an OK state. This rule is disabled by default. Enable the rule if you have Logger in your environment.	/All Rules/ArcSight Administration/Logger/System Health/
Logger Status	This rule identifies Logger Sensor Status correlation events and triggers only if all the sensor statuses for a Logger are in an OK state. This rule is disabled by default. Enable the rule if you have Logger in your environment.	/All Rules/ArcSight Administration/Logger/System Health/
Out of Domain Fields	This rule triggers when there is no more free domain field available for a field type.	/All Rules/ArcSight Administration/ESM/System Health/Resources/Domains/
Query Running Time	This rule triggers when a query audit event is detected. The rule adds or updates the corresponding entry in the active list.	/All Rules/ArcSight Administration/ESM/System Health/Resources/
Resource Became Invalid	This rule triggers when a resource becomes invalid. The rule adds the resource ID, name, URI, and type to the Invalid Resources active list.	/All Rules/ArcSight Administration/ESM/System Health/Resources/
Resource Became Valid	This rule triggers when an invalid resource becomes valid. The rule removes the resource from the Invalid Resources active list.	/All Rules/ArcSight Administration/ESM/System Health/Resources/
Rule Matching Too Many Events	This rule detects rules that match too many events. The rule identifies events that come from the ArcSight Security Manager with the Device Event Category set to /Rule/Error/Deactivate/Unsafe. This rule only requires one such event within five minutes. After this rule is triggered, a notification is sent to the SOC Operators.	/All Rules/ArcSight Administration/ESM/System Health/Resources/Rules/
Storage Licensing Audit event Detected	This rule detects connector raw event statistic events and stores them in an active list.	/All Rules/ArcSight Administration/ESM/Licensing/

Rule Resources, continued

Resource	Description	URI
Update Connector Caching Status	This rule detects active list audit events for changes in the related connector caching/dropping active lists. The rule then sets the device custom number and string information to be used by the Connector Cache Status data monitor.	`/All Rules/ArcSight Administration/Connectors/System Health/`
Update Connector Connection Status	This rule monitors audit events for changes in the connector connection status active lists. The rule then sets the device custom number and the string information used by the Connector Connection Status data monitor.	`/All Rules/ArcSight Administration/Connectors/System Health/`
Warning - System Resources Exhausted	This rule indicates that a device has detected a system resource issue. The rule triggers whenever a resource is exhausted or a resource check fails. On the first event, a notification is sent to SOC operators. Note: This rule does not produce completely accurate results when running in Turbo Mode Fastest.	`/All Rules/ArcSight Administration/ESM/System Health/Resources/`

Session Lists

The following table lists all the session lists.

Session List Resources

Resource	Description	URI
ArcSight User Sessions	This session list stores the client username, client address and zone used by an ArcSight user to access the ArcSight Manager to monitor the login times, logout times, or Console timeouts and to determine who had access to the system over specific time periods.	/All Session Lists/ArcSight Administration/ESM/User Access/User Sessions/
Connector - Caches	This session list stores the cache history for all the connectors. A new session is created every time a connector starts caching or dropping events.	/All Session Lists/ArcSight Administration/Connectors/System Health/
Connector Versions	This session list stores the version history for all the connectors. The fields in the session list are: Connector ID, Connector Name, Connector Version, Connector Type, Connector Address, and Connector Zone. The session list is populated by the Connector Upgrade Successful and Connector Version Detected rules.	/All Session Lists/ArcSight Administration/Connectors/Configuration Changes/
Licensing History	This session list stores the licensing history for the various license types. The session list stores the license type, the current count, and the count limit.	/All Session Lists/ArcSight Administration/ESM/Licensing/

Trends

The following table lists all the trends.

Trend Resources

Resource	Description	URI
ASM Database Free Space	This trend stores the free space percentages by hour for the four ASM database table spaces (ARC_EVENT_DATA, ARC_EVENT_INDEX, ARC_SYSTEM_DATA, and ARC_SYSTEM_INDEX).	/All Trends/ArcSight Administration/ESM/System Health/Storage/
ArcSight User Login Trends - Hourly	This trend tracks the counts of how many users logged into ArcSight ESM within the previous hour. The trend checks if the Login tracking rule triggered and then populated a data monitor with currently logged in users.	/All Trends/ArcSight Administration/ESM/User Access/

Trend Resources, continued

Resource	Description	URI
Connector Average EPS - Last 7 days	This trend stores the average EPS for all connectors during the last seven days and writes the data to an active list by leveraging the trend action feature.	/All Trends/ArcSight Administration/Connector/System Health/EPS/
Connector Daily Average EPS	This trend stores the daily average EPS for all connectors and writes the data to an active list by leveraging the trend action feature.	/All Trends/ArcSight Administration/Connector/System Health/EPS/
Connector Total Events - Hourly	This trend stores the hourly average EPS for all connectors.	/All Trends/ArcSight Administration/Connector/System Health/EPS/
Events Count	This trend stores the total number of non ArcSight events.	/All Trends/ArcSight Administration/ESM/Events Analysis Overview/
Failed Queries	This trend stores failed queries for reports, trends, and query viewers.	/All Trends/ArcSight Administration/ESM/System Health/Resources/Reporting/
Hourly EPS in Persistor	This trend stores hourly EPS in persistor.	/All Trends/ArcSight Administration/ESM/Distributed Correlation Monitoring/
QueryViewer Queries	This trend stores the top longest query viewer queries by day.	/All Trends/ArcSight Administration/ESM/System Health/Resources/Reporting/
Report Queries	This trend stores the top longest report queries by day.	/All Trends/ArcSight Administration/ESM/System Health/Resources/Reporting/
Storage Licensing Data	This trend stores the raw event length reported by the raw event statistic events for each connector.	/All Trends/ArcSight Administration/ESM/Licensing/
Trend Queries	This trend stores the top longest trend queries by day.	/All Trends/ArcSight Administration/ESM/System Health/Resources/Reporting/

Use Cases

The following table lists all the use cases.

Use Case Resources

Resource	Description	URI
ArcSight ESM Device Monitoring	This use case monitors the status of ArcSight ESM devices using the Device Status Monitoring (DSM) functionality that comes with SmartConnectors.	`/All Cases/ArcSight Administration/Devices/`
Connector Configuration Changes	This use case provides information about configuration changes (such as upgrades) and connector version changes on the system.	`/All Cases//All Active Channels/ArcSight Administration/Connectors/`
Connector Connection and Cache Status	This use case provides information about the connection status and caching status of connectors in the system. Connectors can be connected directly to ESM or through Loggers.	`/All Cases/ArcSight Administration/Connectors/`
Connector Overview	This use case covers administration content for monitoring connectors and devices.	`/All Cases/ArcSight Administration/`
Device Monitoring	This use case provides information about the devices reporting to ESM.	`/All Cases/ArcSight Administration/Connectors/`
ESM Events	This use case provides statistics about the flow of events through ESM.	`/All Cases/ArcSight Administration/ESM/System Health/`
ESM Licensing	This use case provides information about ESM licensing compliance.	`/All Cases/ArcSight Administration/ESM/`
ESM Overview	This use case provides information about administration content for monitoring ESM.	`/All Cases/ArcSight Administration/`
ESM Reporting Resource Monitoring	This use case provides information about performance statistics for reports, trends, and query viewers.	`/All Cases/ArcSight Administration/ESM/System Health/`
ESM Resource Configuration Changes	This use case provides information about changes to the ESM resources, such as rules, reports, and so on.	`/All Cases/ArcSight Administration/ESM/Configuration Changes/`
ESM Resource Monitoring	This use case provides processing statistics for various ESM resources, such as trends, rules, and so on.	`/All Cases/ArcSight Administration/ESM/System Health/`
ESM User Sessions	This use case provides information about user access to ESM.	`/All Cases/ArcSight Administration/ESM/`

Use Case Resources, continued

Resource	Description	URI
Logger Events	This use case provides information about statistics for events sent through Loggers to ESM.	/All Cases/ArcSight Administration/Logger/
Logger Overview	This use case provides Logger status and statistics.	/All Cases/ArcSight Administration/
Logger System Health	This use case provides performance statistics for the Loggers connected to ESM.	/All Cases/ArcSight Administration/Logger/

ArcSight CORRE Resources By Type

This section lists all the resources by type.

Active Lists

The following table lists all the active lists.

CORR-Engine Active List Resources

Resource	Description	URI
Archive Task Failures	This active list stores archive task failure events, which include activation, deactivation, and scheduling.	/All Active Lists/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Critical Archive Failures	This active list stores archive archival failure events.	/All Active Lists/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Dashboards

The following table lists all the dashboards.

CORR-Engine Dashboard Resources

Resource	Description	URI
Archive Status	This dashboard shows database archive related information.	/All Dashboards/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Database Performance Statistics	This dashboard shows an overview of database related statistics, such as available space, insert, and retrieval times.	/All Dashboards/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Data Monitors

The following table lists all the data monitors.

CORR-Engine Data Monitor Resources

Resource	Description	URI
Archive Disk Space	This data monitor shows the state of archive disk space used: OK, Warning, and Critical Warning.	/All Data Monitors/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Archive Status/
Database Free Space	This data monitor displays the database free space.	/All Data Monitors/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics/
Database Insert Time - Last 24 Hours	This data monitor displays the moving average for database insert time during the last 24 hours.	/All Data Monitors/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics/
Database Insert Time - Last Hour	This data monitor displays the moving average for database insert time during the last hour.	/All Data Monitors/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics/

CORR-Engine Data Monitor Resources, continued

Resource	Description	URI
Database Retrieval Time - Last 24 Hours	This data monitor displays the moving average for database retrieval time during the last 24 hours.	/All Data Monitors/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics/
Database Retrieval Time - Last Hour	This data monitor displays the moving average for database retrieval time during the last hour.	/All Data Monitors/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics/
Recent Archive Events	This data monitor shows last ten archive events.	/All Data Monitors/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Archive Status/

Filters

The following table lists all the filters.

CORR-Engine Filter Resources

Resource	Description	URI
Archive Archival Success	This filter selects archive archival success audit events.	/All Filters/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters/
Archive Disk Space	This filter selects archive disk space audit events.	/All Filters/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Disk space status is Critical	This filter selects archive disk space audit events where custom number 1, which is the Used Space Percentage, is greater than a certain value. 95 is the default number.	/All Filters/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters/
Archive Disk space status is OK	This filter selects archive disk space audit events where custom number 1, which is Used Space Percentage, is less than a certain value. 85 is the default number.	/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters/
Archive Events	This filter selects all archive audit events.	/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

CORR-Engine Filter Resources, continued

Resource	Description	URI
Archive Failure Events	This filter selects all archive failure audit events.	/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters/
Archive Settings Updated Event	This filter selects archive settings updated audit events.	/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters/
File Path StartsWith All Rules	This filter selects events in which the file path starts with /All Rules.	/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters/

Focused Reports

The following table lists all the focused reports.

CORR-Engine Focused Report Resources

Resource	Description	URI
Event Data Free Space - Last 30 Days	This report shows the free space percentages by day for the ARC_EVENT_DATA database table space for the last 30 days. The source report is ASM Database Free Space - by Day.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
System Data Free Space - Last 30 Days	This focused report shows the free space percentages by day for the ARC_SYSTEM_DATA database table space for the last 30 days. The source report is ASM Database Free Space - by Day.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Queries

The following table lists all the queries.

CORR-Engine Query Resources

Resource	Description	URI
Archive Activation Statistics	This query selects archive activation audit events from the Archive Events session list.	/All Queries/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Archival Statistics	This query selects archive archival audit events from the Archive Events session list.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Archival Success	This query selects archive archival information from the Archive Events session list.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Deactivation Statistics	This query selects archive deactivation audit events from the Archive Events session list.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Disk Space Usage	This query selects archive disk space used information from the Archive Events session list.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Non-success events	This query selects non-successful archive audit events from the Archive Events session list.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Scheduling Statistics	This query selects archive scheduling audit events from the Archive Events session list.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Space status	This query selects archive space audit events.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Task Failure Details	This query selects archive task failure events from the active list: Archive Task Failures.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive status	This query selects archive audit events from the Archive Events session list that have not been terminated, which are the latest event for each archive name.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Critical Archive Failure Details	This query selects archive archival failure events from the active list: Critical Archive Failures.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Query Viewers

The following table lists all the query viewers.

CORR-Engine Query Viewer Resources

Resource	Description	URI
Archive Task Failure Details	This query viewer shows the current archive task failure events, which include activation, deactivation and scheduling.	/All Query Viewers/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Critical Archive Failure Details	This query viewer shows the current archive archival failure events.	/All Query Viewers/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Reports

The following table lists all the reports.

CORR-Engine Report Resources

Resource	Description	URI
ASM Database Free Space	This report shows the current free space percentages for the ASM database table spaces. The report shows the percentages for the ARC_EVENT_DATA and ARC_SYSTEM_DATA table spaces.	/All Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
ASM Database Free Space - by Day	This report shows the free space percentages by day for one of the ASM database table spaces. The report has one chart and one table, and has a custom parameter that can be used to choose one of the table spaces (ARC_EVENT_DATA or ARC_SYSTEM_DATA, if this is an Oracle installation, ARC_EVENT_INDEX and ARC_SYSTEM_INDEX are also available).	/All Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
ASM Database Free Space - by Hour	This report shows the free space percentages by hour for the ASM database table spaces. The report shows the percentages by hour for the ARC_EVENT_DATA and ARC_SYSTEM_DATA table spaces.	/All Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Processing	This report shows the longest to process archives and the time to archive information.	/All Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Status Report	This report shows the current status of archive and disk space used.	/All Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Report Templates

The following table lists all the report templates.

CORR-Engine Report Template Resources

Resource	Description	URI
Archive Template	This report template contains two tables. It is designed for the archive status report and includes scripting to make the first column in the tables a color: red, yellow or green, based on the value in another column.	/All Report Templates/ArcSight Administration/System Health/Storage/CORR-Engine/

Rules

The following table lists all the rules.

CORR-Engine Rule Resources

Resource	Description	URI
Archive Events	This rule is triggered by archive audit events and writes to the Archive Events session list.	/All Rules/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Task Failures	This rule is triggered by archive task failure events, which include activation, deactivation and scheduling events, and writes to the Archive Task Failures active list.	/All Rules/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Task Success	This rule is triggered by successful archive activation, deactivation, and scheduling audit events where the archive name is in the Archive Task Failures active list. This rule removes the entry from the active list.	/All Rules/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Critical Archive Failures	This rule is triggered by archive archival failure events and writes to the Critical Archive Failures active list.	/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Critical Archive Success	This rule is triggered by archive archival success events where the archive name is in the Critical Archival Failures active list. This rule removes the entry from the active list.	/All Rules/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Session Lists

The following table lists all the session lists.

CORR-Engine Session List Resources

Resource	Description	URI
Archive Events	This session list stores archive audit events.	/All Session Lists/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Use Cases

The following table lists all the use cases.

CORR-Engine Use Case Resources

Resource	Description	URI
ESM Storage Monitoring (CORR-Engine)	This use case provides information about the health of the CORR Engine (ArcSight Express 3.0 and beyond).	/ArcSight Administration/ESM/System Health/

ArcSight Content Management Resources By Type

This section lists all the resources by type.

Active Lists

The following table lists all the active lists.

Content Management Active List Resources

Resource	Description	URI
Content Management History	This active list stores data about Content Management activity.	`/ArcSight Administration/ESM/Content Management/`

Dashboards

The following table lists all the dashboards.

Content Management Dashboard Resources

Resource	Description	URI
Synchronization Status History	This dashboard shows information about the history of content packages synchronized across peered ArcSight Managers or subscribers.	`/ArcSight Administration/ESM/Content Management/`

Queries

The following table lists all the queries.

Content Management Query Resources

Resource	Description	URI
Top Packages with Synchronization Errors	This query selects information about the content packages with the most issues related to either package update delivery or installation after the package has been delivered.	`/ArcSight Administration/ESM/Content Management/`
Top Subscribers with Errors	This query selects information about the subscribers experiencing the most issues with managed package delivery or installation.	`/ArcSight Administration/ESM/Content Management/`
Top Synchronization Errors	This query selects information about the most common issues with the delivery or installation of managed packages.	`/ArcSight Administration/ESM/Content Management/`

Query Viewers

The following table lists all the query viewers.

Content Management Query Viewer Resources

Resource	Description	URI
Top Packages with Synchronization Errors	This query viewer displays information about the content packages with the most issues related to either package update delivery or to installation after the package has been delivered.	`/ArcSight Administration/ESM/Content Management/`
Top Subscribers with Errors	This query viewer displays information about the subscribers experiencing the most issues with managed package delivery or installation.	`/ArcSight Administration/ESM/Content Management/`
Top Synchronization Errors	This query viewer displays information about the most common issues with delivery or installation of managed packages.	`/ArcSight Administration/ESM/Content Management/`

Reports

The following table lists all the reports.

Content Management Report Resources

Resource	Description	URI
Synchronization Status History	This report shows information about the history of content packages synchronized across peered Arcsight Managers or subscribers.	`/ArcSight Administration/ESM/Content Management/`
Top Packages with Synchronization Errors	This report shows information about the content packages with the most update delivery issues or installation issues after the package has been delivered.	`/ArcSight Administration/ESM/Content Management/`
Top Subscribers with Errors	This report shows information about the subscribers experiencing the most issues with managed package delivery or installation.	`/ArcSight Administration/ESM/Content Management/`
Top Synchronization Errors	This report shows information about the most common issues experienced by subscribers with managed package delivery or installation.	`/ArcSight Administration/ESM/Content Management/`

Rules

The following table lists all the rules.

Content Management Rule Resources

Resource	Description	URI
Content Management Data	This rule maintains list information for the Content Management feature.	`/ArcSight Administration/ESM/Content Management/`

Use Cases

The following table lists all the use cases.

Content Management Use Case Resources

Resource	Description	URI
Content Management	This use case contains resources that track content that is managed across multiple ESM systems with the Content Management feature.	`/ArcSight Administration/ESM/Content Management/`

Event Broker Monitoring Resources by Type

This section lists all the resources by type.

Active Channels

The following table lists all the active channels.

Event Broker Monitoring Active Channel Resources

Resource	Description	URI
Event Broker Audit Events	This active channel shows Event Broker audit events.	/ArcSight Administration/ESM/Event Broker Monitoring/

Active Lists

The following table lists all the active lists.

Event Broker Monitoring Active List Resources

Resource	Description	URI
Event Counts from Event Broker	This list holds information on EB Address and Port, Topic Name, Hour of Day, and total count of events as detected by the Event Broker rule.	/ArcSight Administration/ESM/Event Broker Monitoring/

Dashboards

The following table lists all the dashboards.

Event Broker Monitoring Dashboard Resources

Resource	Description	URI
Event Broker Monitoring	This dashboard displays Event Broker monitoring.	/ArcSight Administration/ESM/Event Broker Monitoring/

Data Monitors

The following table lists all the data monitors.

Event Broker Monitoring Data Monitor Resources

Resource	Description	URI
Event Broker Status	This data monitor shows status of Event Broker.	/ArcSight Administration/ESM/Event Broker Monitoring/
Message Count Remaining in Event Broker	This data monitor shows status of message count remaining in Event Broker.	/ArcSight Administration/ESM/Event Broker Monitoring/

Field Sets

The following table lists all the field sets.

Event Broker Monitoring Field Set Resources

Resource	Description	URI
Event Broker	This field set is for Event Broker monitoring.	/ArcSight Administration/ESM/Event Broker Monitoring/

Filters

The following table lists all the filters.

Event Broker Monitoring Filter Resources

Resource	Description	URI
Event Broker Audit Events	This filter selects all Event Broker audit events.	/ArcSight Administration/ESM/Event Broker Monitoring/
Message Count Remaining in Event Broker	This filter selects audit events for messages remaining in Event Broker.	/ArcSight Administration/ESM/Event Broker Monitoring/

Queries

The following table lists all the queries.

Event Broker Monitoring Query Resources

Resource	Description	URI
EPS Forwarded from Event Broker	This query retrieves EPS count for events sent from Event Broker.	/ArcSight Administration/ESM/Event Broker Monitoring/

Query Viewers

The following table lists all the query viewers.

Event Broker Monitoring Query Viewer Resources

Resource	Description	URI
Hourly EPS Forwarded from Event Broker	This query viewer displays hourly EPS count forwarded from Event Broker.	/ArcSight Administration/ESM/Event Broker Monitoring/

Rules

The following table lists all the rules.

Event Broker Monitoring Rule Resources

Resource	Description	URI
Detect Events for Event Broker	This rule triggers when eventbroker:103 (Event Count forwarded to ESM) event occurs. This rule populates the Event Counts from Event Broker active list every hour.	`/ArcSight Administration/ESM/Event Broker Monitoring/`

ESM HA Monitoring Resources By Type

This section lists all the resources by type.

Active Channels

The following table lists all the active channels.

ESM High Availability Monitoring Active Channel Resources

Resource	Description	URI
HA Monitoring	This active channel shows HA status events.	/ArcSight Administration/ESM/HA Monitoring/

Active Lists

The following table lists all the active lists.

ESM High Availability Active List Resources

Resource	Description	URI
Current Primary System	This active list is populated by the ESM System Started rule. The active list is used by a query to retrieve the IP address and hostname of the current Primary System. This information is then displayed in the ESM HA Status dashboard.	/ArcSight Administration/ESM/HA Monitoring/

Dashboards

The following table lists all the dashboards.

ESM High Availability Dashboard Resources

Resource	Description	URI
ESM HA Status	This dashboard shows an overview of the ESM HA state. The top panel shows the current HA state. The second panel shows the IP address and hostname of the current Primary System. The third panel shows ESM system changes, such as a Manager restart or HA failover during the last 24 hours. The bottom panel shows the last ten HA status changes.	/ArcSight Administration/ESM/HA Monitoring/

Data Monitors

The following table lists all the data monitors.

ESM High Availability Data Monitor Resources

Resource	Description	URI
ESM HA Status	This data monitor shows the current ESM HA status.	/ArcSight Administration/ESM/HA Monitoring/
Last 10 HA Status Changes	This data monitor shows the last ten HA status changes.	/ArcSight Administration/ESM/HA Monitoring/

Field Sets

The following table lists all the field sets.

ESM High Availability Field Set Resources

Resource	Description	URI
HA Management	This field set contains fields used to examine HA status events.	/ArcSight Administration/ESM/HA Monitoring/

Filters

The following table lists all the filters.

ESM High Availability Filter Resources

Resource	Description	URI
ESM HA Status	This filter detects events generated by the HA module.	/ArcSight Administration/ESM/HA Monitoring/

Queries

The following table lists all the queries.

ESM High Availability Query Resources

Resource	Description	URI
Current Primary System	This query retrieves details for the current Primary System from the Current Primary System active list. The details are displayed in the ESM HA Status dashboard.	/ArcSight Administration/ESM/HA Monitoring/
Current Primary System Details	This query retrieves details for the Primary System from the Current Primary System Status Change session list. It is used for the query viewer, which is in turn used in the dashboard drilldown.	/ArcSight Administration/ESM/HA Monitoring/
ESM HA Status - last 7 days	This query retrieves details of the HA module status changes within the last seven days. It is used in the ESM HA Status Updates - last 7 days report.	/ArcSight Administration/ESM/HA Monitoring/
System Status Changes	This query retrieves Primary System status change details from the Current Primary System Status Change session list. It is used for the query viewer, which is in turn used in the dashboard drilldown.	/ArcSight Administration/ESM/HA Monitoring/
System Status Changes - Last 24 hours	This query retrieves details for the ESM System status changes (restarts or HA failovers) from the Current Primary System Status Change session list. It is used by the query viewer to populate the data in the dashboard.	ArcSight Administration/ESM/HA Monitoring/

Query Viewers

The following table lists all the query viewers.

ESM High Availability Query Viewer Resources

Resource	Description	URI
Current Primary System	This query viewer displays details for the current Primary System.	/ArcSight Administration/ESM/HA Monitoring/
Current Primary System Details	This query viewer displays details for the Primary System. It is used for the dashboard drilldown.	/ArcSight Administration/ESM/HA Monitoring/
System Status Changes	This query viewer displays details for the ESM System status changes (restarts or HA failovers). It is used for the dashboard drilldown.	/ArcSight Administration/ESM/HA Monitoring/
System Status Changes - Last 24 hours	This query viewer displays details about the ESM System status changes (restarts or HA failovers). The information is displayed in the dashboard.	/ArcSight Administration/ESM/HA Monitoring/

Reports

The following table lists all the reports.

ESM High Availability Report Resources

Resource	Description	URI
ESM HA Status Updates - last 7 days	This report shows all HA status updates within the last seven days.	/ArcSight Administration/ESM/HA Monitoring/

Rules

The following table lists all the rules.

ESM High Availability Rule Resources

Resource	Description	URI
Alert - HA Status Change	This rule triggers when an HA status change event is generated. After the rule triggers, a notification is sent to the SOC Operators team.	/ArcSight Administration/ESM/HA Monitoring/
ESM System Started	This rule triggers when a Primary System starts up; for example, the ESM manager restarts or there is an HA failover. After the rule triggers, the entry is created or updated in the Current Primary System active list and in the Current Primary System Status Change session list.	/ArcSight Administration/ESM/HA Monitoring/

Session Lists

The following table lists all the session lists.

ESM High Availability Session List Resources

Resource	Description	URI
Current Primary System Status Change	This session list is populated by the ESM System Started rule. It stores a history of the Primary System restarts and failovers. A new session is created every time a system restarts or the HA failover occurs. This session list is used by the query to retrieve the system status changes and populates the HA Monitoring dashboard and the ESM HA Status Updates - last 7 days report.	/ArcSight Administration/ESM/HA Monitoring/

Use Cases

The following table lists all the use cases.

ESM High Availability Use Case Resources

Resource	Description	URI
HA Monitoring	This use case monitors the status of the ESM High Availability Module (HA module).	/ArcSight Administration/ESM/HA Monitoring/

Appendix B: ArcSight Foundation Resources

This appendix lists all the resources by type in the ArcSight Foundation packages.

ArcSight ClusterView Resources By Type

This section lists all ClusterView Resources by type.

Data Monitors

The following table lists all the data monitors.

ArcSight ClusterView Data Monitor Resources

Resource	Description	URI
Aggregator Audit Events	Data Monitor to display Aggregator Audit Events	/All Data Monitors/ArcSight Foundation/ArcSight ClusterView/
Aggregator Message Bus	Data Monitor to display remaining event count in message bus for Aggregator.	/All Data Monitors/ArcSight Foundation/ArcSight ClusterView/
Aggregator MPS	Data Monitor to display Aggregator MPS (Messages per Second)	/All Data Monitors/ArcSight Foundation/ArcSight ClusterView/
Correlator Audit Events	Data Monitor to display Correlator Audit Events	/All Data Monitors/ArcSight Foundation/ArcSight ClusterView/
Correlator EPS	Data Monitor to display Correlator EPS	/All Data Monitors/ArcSight Foundation/ArcSight ClusterView/
Correlator Message Bus	Data Monitor to display remaining event count in message bus for Correlator.	/All Data Monitors/ArcSight Foundation/ArcSight ClusterView/
Distributed Correlation Audit Events	Data Monitor to display Distributed Mode Audit Events	/All Data Monitors/ArcSight Foundation/ArcSight ClusterView/
Manager Message Bus	Data Monitor to display remaining event count in message bus for Manager.	/All Data Monitors/ArcSight Foundation/ArcSight ClusterView/

Fields

The following table lists all the fields.

ArcSight ClusterView Field Resources

Resource	Description	URI
Service Message	This variable returns service message for distributed correlation audit events.	/All Fields/ArcSight Foundation/ArcSight ClusterView/
Service Name And Id	This variable returns name and ID for distributed correlation audit events.	/All Fields/ArcSight Foundation/ArcSight ClusterView/

Filters

The following table lists all the filters.

ArcSight ClusterView Filter Resources

Resource	Description	URI
Aggregator Audit Events - Message Bus	This filter selects audit events for the remaining event count in message bus for aggregator.	/All Filters/ArcSight Foundation/ArcSight ClusterView/
Aggregator Audit Events - MPS	This filter selects audit events for Aggregator MPS (Messages per Second).	/All Filters/ArcSight Foundation/ArcSight ClusterView/
Correlator Audit Events - EPS	This filter selects audit events for Correlator EPS	/All Filters/ArcSight Foundation/ArcSight ClusterView/
Correlator Audit Events - Message Bus	This filter selects audit events for the remaining event count in message bus for Correlator.	/All Filters/ArcSight Foundation/ArcSight ClusterView/
Manager Audit Events - Message Bus	This filter selects audit events for the remaining event count in message bus for Manager.	/All Filters/ArcSight Foundation/ArcSight ClusterView/

ArcSight SOCView Resources By Type

This section lists all SOCView Resources by type.

Data Monitors

The following table lists all the data monitors.

ArcSight SocView Data Monitor Resources

Resource	Description	URI
Live Activity	This data monitor shows non-Arcsight internal live events.	/All Data Monitors/ArcSight Foundation/ArcSight SocView/
Malicious Activity	This data monitor shows malicious activity.	/All Data Monitors/ArcSight Foundation/ArcSight SocView/
Rule Counts	This data monitor shows rule correlation event count.	/All Data Monitors/ArcSight Foundation/ArcSight SocView/
Rules Activity	This data monitor shows rule correlation events.	/All Data Monitors/ArcSight Foundation/ArcSight SocView/
Top Attack Types	This data monitor shows top attack types.	/All Data Monitors/ArcSight Foundation/ArcSight SocView/
Top Destination Address	This data monitor shows top destination addresses.	/All Data Monitors/ArcSight Foundation/ArcSight SocView/
Top Source Address	This data monitor shows top source addresses.	/All Data Monitors/ArcSight Foundation/ArcSight SocView/
Top Source Geo	This data monitor shows top source geo..	/All Data Monitors/ArcSight Foundation/ArcSight SocView/

Filters

The following table lists all the filters.

ArcSight SocView Filter Resources

Resource	Description	URI
Live Activity	This filter selects non-arcsight internal events.	/All Filters/ArcSight Foundation/ArcSight SocView/
Malicious Activity	This filter selects malicious activity detected by antivirus.	/All Filters/ArcSight Foundation/ArcSight SocView/
Rule Activity	This filter selects rule correlation events.	/All Filters/ArcSight Foundation/ArcSight SocView/

Query Viewers

The following table lists the query viewers.

ArcSight SocView Query Viewer Resources

Resource	Description	URI
Asset Counts	This query viewer shows number of assets.	/All Query Viewers/ArcSight Foundation/ArcSight SocView/

Queries

The following table lists the queries.

ArcSight SocView Query Resources

Resource	Description	URI
Number of Assets	This query selects number of assets.	/All Queries/ArcSight Foundation/ArcSight SocView/

Common Resources By Type

This section lists all Common Resources by type. The resources listed here are part of the `/ArcSight Foundation/Shared Libraries/` packages that are automatically installed with ESM.

Conditional Variable Filters

The following table lists all the filters.

Conditional Variable Filters

Resource	Description	URI
All Device Information is NULL	This filter identifies events in which there is no device information, meaning that the device vendor, device product, and device version fields are all NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/
All Protocol Information is NULL	This filter identifies events in which there is no protocol information (the transport protocol, application protocol, and target port fields are all NULL).	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
All Receivers EPS	This filter identifies events in which the device event category is /Monitor/Receiver/All/EPS or /Monitor/Receiver/EPS/All.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/
Application Protocol is not NULL	This filter identifies if an event has an entry for the Application Protocol field.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
Application Protocol is NULL	This filter identifies if the event target has an application protocol associated with it.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
Attacker Address is NULL	This variable identifies events in which the attacker address field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Asset has Criticality	This filter identifies events in which the attacker asset is categorized under /All Asset Categories/System Asset Categories/Criticality.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Attacker Asset has OS Categorization	This filter identifies if the attacker in an event has an asset category in /Site Asset Categories/Operating System.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/

Conditional Variable Filters, continued

Resource	Description	URI
Attacker Asset ID is NULL	This filter is used by variables to determine if an event has an attacker asset ID.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/
Attacker Asset Information is NULL	This filter identifies if an event has any attacker asset information. This information consists of the attacker zone, attacker asset name, and attacker address.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Attacker Host Name is NULL	This filter is used by variables to identify events in which the attacker host name field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Information is NULL	This filter identifies events in which the attacker zone, attacker host name, and attacker address fields are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Port is NULL	This variable identifies events in which the attacker port field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker User ID is NULL	This filter identifies events where the Attacker User ID is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Attacker User Name and ID are NULL	This filter identifies events in which the Attacker User Name and Attacker User ID are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Attacker User Name is NULL	This filter identifies events where the Attacker User Name is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Attacker Zone AND Address are NULL	This filter identifies events in which the attacker zone and attacker address fields are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Zone AND Asset Name are NOT NULL	This filter is used by variables to determine if an event has both an attacker zone and an attacker asset name.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Attacker Zone AND Asset Name are NULL	This filter is used by variables to determine if an event has neither an attacker zone or an attacker asset name.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Attacker Zone AND Host are NULL	This filter identifies events in which the attacker zone and attacker address fields are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/

Conditional Variable Filters, continued

Resource	Description	URI
Attacker Zone AND Host are NULL but Address is NOT NULL	This filter identifies events in which either the attacker zone or attacker address field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Zone is NULL	This filter identifies events in which the attacker zone field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Zone OR Address is NULL	This filter identifies events where the attacker zone or attacker address field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Zone OR Host is NULL	This filter identifies events in which either the attacker zone or attacker host name field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Bytes In is NULL	This filter is designed for conditional expression variables. The filter identifies events in which the Bytes In is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Bytes/
Bytes Out is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Bytes Out is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Bytes/
Case File Type	This filter identifies events in which the File Type field is Case.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Database Events	This filter identifies events in which the category object is /Host/Application/Database.	/All Filters/ArcSight Foundation/Common/Device Class Filters/
Device Address is NULL	This filter is used by variables to identify events in which the device address field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Device/
Device Asset has Criticality	This filter identifies events in which the device asset is categorized under /All Asset Categories/System Asset Categories/Criticality.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Device Asset has OS Categorization	This filter identifies if the device in an event has an asset category in /Site Asset Categories/Operating System.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Device Asset ID is NULL	This filter is used by variables to determine if an event has an device asset ID.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/

Conditional Variable Filters, continued

Resource	Description	URI
Device Asset Information is NULL	This filter is used by variables to determine if an event has any device asset information. This information consists of the device zone, device asset name, and device address.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Device Vendor AND Product are NULL	This filter identifies events in which the device vendor and device product fields are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Device/
Device Vendor OR Product is NULL	This filter identifies events in which the device vendor or device product field is NULL, but not both.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Device/
Device Version is NULL	This filter identifies events in which the device product field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Device/
Device Zone AND Address are NULL	This variable is used by variables to identify events in which the device zone and device address fields are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Device Zone AND Asset Name are NOT NULL	This filter is used by variables to determine if an event has both an device zone and an device asset name.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Device Zone AND Asset Name are NULL	This filter identifies if an event has neither a device zone or an device asset name.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Device Zone OR Address is NULL	This filter is used by variables to identify events in which the device zone or device address field is NULL, but not both.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Double-digit Julian Day	This filter supports the variable Julian Day by checking the end time for a double digit day. The Julian Day variable prepends 0 or 00 to days with a single Julian digit, so that the format is always DDD (for example, January 1st displays as 001 instead of 1).	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/
Email Address in Attacker User ID	This filter identifies events in which the attacker user ID field has an email address.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Email Address in Attacker User Name	This filter identifies events in which the attacker user name field has an email address.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Email Address in Target User ID	This filter identifies events in which the target user ID field has an email address.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/

Conditional Variable Filters, continued

Resource	Description	URI
Email Address in Target User Name	This filter identifies events in which the target user name field has an email address.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Event Has Actor by Account Information	This filter identifies events in which the global variable ActorByAccountID returns actor information.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Event Has Actor by Custom Account Information	This filter identifies events in which the global variable ActorByCustomFields returns actor information.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Event Has E-mail Address	This filter identifies events in which one or more user ID or user name field has an email address.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Firewall Events	This filter retrieves events with the Firewall category device group.	/All Filters/ArcSight Foundation/Common/Device Class Filters/
Identity Management Events	This filter identifies events in which the Category Device Group starts with Identity Management.	/All Filters/ArcSight Foundation/Common/Device Class Filters/
Inbound Network	This filter identifies events in which the device event category ends with /In.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/
Network Events	This filter identifies events with the category object starts with Network or the category device group starts with Network Equipment.	/All Filters/ArcSight Foundation/Common/Device Class Filters/
Notification Event has Acknowledgement Status	This filter identifies notification events that have a Device Custom String 6 label set as Acknowledgement Status.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Event has Configuration Resource	This filter identifies notification events that have a Device Custom String 2 label set as Configuration Resource.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/
Notification Event has Destination Group	This filter identifies notification events that have a Device Custom String 4 label set as Group.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/

Conditional Variable Filters, continued

Resource	Description	URI
Notification Event has Rule Name	This filter identifies notification events that have a Device Custom String 3 label set as Rule Name.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Event has User Name	This filter identifies notification events that have an attacker user name to represent the user who acknowledged or resolved a notification.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Operating System Events	This filter identifies events in which the category device group is Operating System.	/All Filters/ArcSight Foundation/Common/Device Class Filters/
Remaining Disk Less than 5 Percent	This filter identifies events in which the remaining disk space is less than five percent.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/
Remaining Disk More than 10 Percent	This filter identifies events in which the remaining disk space is greater than ten percent.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/
Sensor Type is CPU	This filter identifies events in which the sensor type is CPU.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/Sensor Type is CPU
Sensor Type is FAN	This filter identifies events in which the sensor type is FAN.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/Sensor Type is FAN
Single-digit Day	This filter identifies the Day variable by checking the end time to see if it is a single or double digit day. The Day variable prepends 0 to days with a single digit, so that the format is always DD (for example, the 1st displays as 01 instead of 1).	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/Single-digit Day
Single-digit Hour	This filter supports the Hour variable by checking the end time to see if it is a single or double digit hour. The Hour variable prepends 0 to hours with a single digit, so that the format is always HH (for example, 7:00 displays as 07 instead of 7).	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/Single-digit Hour

Conditional Variable Filters, continued

Resource	Description	URI
Single-digit Julian Day	This filter supports the Julian Day variable by checking the end time for a double digit day. The Julian Day variable prepends 0 or 00 to days with a single Julian digit, so that the format is always DDD (for example, January 1st displays as 001 instead of 1).	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/Single-digit Julian Day
Single-digit Minute	This filter supports the Minute variable by checking the end time to see if it is a single or double digit minute. The Minute variable prepends 0 to minutes with a single digit, so that the format is always mm.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/Single-digit Minute
Single-digit Month	This filter supports the Month variable by checking the end time to see if it is a single or double digit month. The Month variable prepends 0 to months with a single digit, so that the format is always MM (for example, July displays as 07 instead of 7).	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/Single-digit Month
Target Address is NULL	This filter is designed for conditional expression variables. The filter identifies events where the target address is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/Target Address is NULL
Target Asset has Application Categorization	This filter identifies if the target of an event has an Asset Category in /Site Asset Categories/Application.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Target Asset has Asset Name	This filter is used by some of the query variables to determine if an event has an entry for the Target Asset Name field.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Target Asset has Criticality	This filter identifies events in which the target asset is categorized under /All Asset Categories/System Asset Categories/Criticality.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Target Asset has OS Categorization	This filter identifies if the target in an event has an Asset Category within /Site Asset Categories/Operating System.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Target Asset ID is NULL	This filter determines if an event has a target asset ID.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Target Asset Information is NULL	This filter is used by variables to determine if an event has any target asset information. This information consists of the target zone, target asset name, and target address.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Target Host Name is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Target Host Name is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/

Conditional Variable Filters, continued

Resource	Description	URI
Target Information is NULL	This filter identifies events in which the target zone, target host name, and target address fields are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Object starts with Host Application	This filter identifies if an event Category Object is within /Host/Application.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Categories/
Target Port is not NULL	This filter identifies if an event has an entry for the Target Port field.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
Target Port is NULL	This filter is used by variables to check if the event target has a port number associated with it.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
Target Service Name is not NULL	This filter identifies if an event has an entry for the Target Service Name field.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
Target User ID is NULL	This filter is designed for conditional expression variables. The filter identifies events in which the Target User ID is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Target User Name and ID are NULL	This filter identifies events in which the Target User Name and Target User ID are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Target User Name is NULL	This filter identifies events where the Target User Name is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Target Zone AND Address are NULL	This filter identifies events in which the target zone and target address fields are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Zone AND Asset Name are NOT NULL	This filter is used by variables to determine if an event has both a target zone and a target asset name.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Target Zone AND Asset Name are NULL	This filter determines if an event has neither a target zone or a target asset name.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Target Zone AND Host are NULL	This filter identifies events in which the target zone and target host name fields are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Zone AND Host are NULL but Address is NOT NULL	This filter identifies events in which either the target zone or target address field is NULL, but not both.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/

Conditional Variable Filters, continued

Resource	Description	URI
Target Zone is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Target Zone is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Zone OR Address is NULL	This filter identifies events in which the target zone or target address field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Zone OR Host is NULL	This filter identifies events in which either the target zone or target host name field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Transport AND Application Protocols are NULL	This filter is used by variables to identify events in which the transport and application protocols are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
Transport OR Application Protocol is NULL	This variable identifies events in which either the transport protocol or the application protocol is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
Transport Protocol is not NULL	This filter identifies if an event has an entry for the Transport Protocol field.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
Transport Protocol is NULL	This filter is used by variables to determine if an event has an entry for the Transport Protocol field.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
VPN Events	This filter identifies events in which the category device group is VPN.	/All Filters/ArcSight Foundation/Common/Device Class Filters/

Network Filters

The following tables list all the filters.

Network Filters Resources

Resource	Description	URI
External Source	This filter identifies events originating from outside the company network.	/All Filters/ArcSight Foundation/Common/Network Filters/Boundary Filters/
External Target	This filter identifies events targeting the outside network.	/All Filters/ArcSight Foundation/Common/Network Filters/Boundary Filters/
External to External Events	This filter identifies events external to the company network.	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/
Inbound Events	This filter identifies events coming from the outside network targeting inside the company network.	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/
Internal Source	This filter identifies events coming from inside the company network.	/All Filters/ArcSight Foundation/Common/Network Filters/Boundary Filters/
Internal Target	This filter identifies events targeting inside the company network.	/All Filters/ArcSight Foundation/Common/Network Filters/Boundary Filters/
Internal to Internal Events	This filter retrieves events internal to the company network.	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/
Outbound Events	This filter identifies events originating from inside the company network, targeting the outside network.	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/

Variables Library Fields

The following table lists all the global variable fields.

Global Variable Fields

Resource	Description	URI
ActingSystem	This variable returns the attacker host (if known) or the target host if it is the only host information available within the event. The format is the same as the AttackerHost or TargetHost variable.	/All Fields/ArcSight Foundation/Variables Library/Host Information/
ActingUser	This variable returns the AttackerUser, if known, or the TargetUser, if that is the only user information available within the event. The format is the same as the AttackerUser or TargetUser variables.	/All Fields/ArcSight Foundation/Variables Library/User Information/
Agent IPv6 Address	This variable is an alias for Device Custom IPv6 Address4.	/All Fields/ArcSight Foundation/Variables Library/IPv6/
Attacker IPv6 Address	This field denotes the Attacker IPv6 address. The term attacker is dependent upon the originator field, i.e., Source or Destination, depending on the specific event. If the originator field is Source, return Device Custom IPv6 Address1 (aliased as Source IPv6 Address), or return Device Custom IPv6 Address2 (aliased as Destination IPv6 Address)	/All Fields/ArcSight Foundation/Variables Library/IPv6/
AttackerAsset	This variable returns the attacker asset information from an event. The asset information is in the format <attackerZoneName>.| <attackerAssetName> | <attackerAddress> Examples: RFC1918: 192.168.0.0-192.168.255.255 | Itwiki.sv.arcsight.com | 192.168.10.20 RFC1918: 192.168.0.0-192.168.255.255 | 192.168.10.30 unknown|	/All Fields/ArcSight Foundation/Variables Library/Asset Information/
AttackerAssetCriticality	This variable returns the criticality categorization of the attacker asset as categorized using the /All Asset Categories/System Asset Categories/Criticality asset categories (Very High, High, Medium, Low, Very Low, or unknown).	/All Fields/ArcSight Foundation/Variables Library/Asset Information/
AttackerHost	This variable returns available attacker information from an event. The format of the information is: <attackerZoneName>.| <attackerHostName> | <attackerAddress>:<attackerPort>. Information that is not in the event does not show a place-holder. For example: RFC1918: 192.168.0.0-192.168.255.255 | Itwiki.sv.arcsight.com | 192.168.10.20:80 RFC1918: 192.168.0.0-192.168.255.255 | 192.168.10.30:53 RFC1918: 192.168.0.0-192.168.255.255:53 192.168.10.30:53 unknown|	/All Fields/ArcSight Foundation/Variables Library/Host Information/
AttackerOS	This variable returns the operating system of the attacker asset (if available) or unknown. For example: Microsoft/Windows XP, Microsoft/Windows 2000/Server, Unknown.	/All Fields/ArcSight Foundation/Variables Library/Asset Information/

Global Variable Fields, continued

Resource	Description	URI
AttackerUser	This variable displays the attacker user name. If the attacker user name is unavailable, the variable displays the attacker user ID. If neither field is available, the variable displays unknown.	/All Fields/ArcSight Foundation/Variables Library/User Information/
DateTime	This variable returns the date and time in the year/month/day-hour:minute format. For example: 2009/10/03-00:43	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
DateValue	This variable returns the date in the year/month/day format. For example: 2009/10/03.	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
Day	This variable returns the day in a two-digit format. For example: 03	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
DayOfWeek	This variable returns the day of the week, spelled out. When using this variable in a query, do not use it for sorting, as the sort will be alphabetical on the name of the day, not the order of the days in the week.	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
Destination IPv6 Address	This variable is an alias for Device Custom IPv6 Address2.	/All Fields/ArcSight Foundation/Variables Library/IPv6/
Device IPv6 Address	This variable is an alias for Device Custom IPv6 Address3.	/All Fields/ArcSight Foundation/Variables Library/IPv6/
DeviceAsset	This variable returns the device asset information from an event. The asset information is in the format: <deviceZoneName>. | <deviceAssetName> | <deviceAddress>. For example: RFC1918: 192.168.0.0-192.168.255.255 | ltwiki.sv.arcsight.com | 192.168.10.20 RFC1918: 192.168.0.0-192.168.255.255 | 192.168.10.30 unknown|	/All Fields/ArcSight Foundation/Variables Library/Asset Information/
DeviceAssetCriticality	This variable returns the criticality categorization of the device asset as categorized using the /All Asset Categories/System Asset Categories/Criticality asset categories (for example, Very High, High, Medium, Low, Very Low, unknown).	/All Fields/ArcSight Foundation/Variables Library/Asset Information/
DeviceInfo	This variable returns the device information, including the device vendor, the device product, and the device version, if available within the event. The format is deviceVendor. | <deviceProduct> or <deviceVendor> | <deviceProduct> v. <deviceVersion>	/All Fields/ArcSight Foundation/Variables Library/

Global Variable Fields, continued

Resource	Description	URI
DeviceOS	This variable returns the operating system of the device asset (if available) or unknown. For example: Microsoft/Windows XP, Microsoft/Windows 2000/Server, Unknown.	/All Fields/ArcSight Foundation/Variables Library/Asset Information/
EndTimeValue	This variable returns the hour and minute in the hour:minute format. For example: 00:10	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
GBytesIn	This variable converts the Bytes In field to GBytes, where a GByte is defined as 1,000,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example when Bytes In < 10,000,000, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
GBytesIn_Labeled	This variable converts the Bytes In field to GBytes, where a GByte is defined as 1,000,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In < 10,000,000, the result is 0). It is then converted to a string, and labeled with the suffix GB (for example, 0.01 GB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
GBytesOut	This variable converts the Bytes Out field to GBytes, where a GByte is defined as 1,000,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes Out < 10,000,000, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
GBytesOut_Labeled	This variable converts the Bytes Out field to GBytes, where a GByte is defined as 1,000,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes Out < 10,000,000, the result is 0). It is then converted to a string, and labeled with the suffix GB (for example, 0.01 GB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
GBytesTotal	This variable converts the combination of the Bytes In and Bytes Out fields to GBytes, where a GByte is defined as 1,000,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example when Bytes In + Bytes Out < 10,000,000, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
GBytesTotal_Labeled	This variable converts the combination of the Bytes In and Bytes Out fields to GBytes, where a GByte is defined as 1,000,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In + Bytes Out < 10,000,000, the result is 0). It is then converted to a string and labeled with the suffix GB (for example, 0.01 GB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/

Global Variable Fields, continued

Resource	Description	URI
GetEmailAddress	This variable does a simple check on the target user name, target user ID, attacker user name, and attacker user ID fields to display the email address. The precedence is attacker user name, then attacker user ID, then target user name, then finally, target user ID, (if all fields have an email address, the attacker user name is the one returned).	/All Fields/ArcSight Foundation/Variables Library/User Information/
Hour	This variable returns the hour in a two-digit format. For example: 02	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
JulianDate	This variable returns the date and time in the year/julian day format. For example: 2009/003, 2010/084, or 2007/363.	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
JulianDateTime	This variable returns the date and time in the year/julian day-hour:minute format. For example: 2009/003-00:53, 2010/084-08:00, 2007/363-15:45.	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
JulianDay	This variable returns the day in a three-digit, julian day format. For example, 003, 084, 363.	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
KBytesIn	This variable converts the Bytes In field to KBytes, where a KByte is defined as 1,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In < 10, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
KBytesIn_Labeled	This variable converts the Bytes In field to KBytes, where a KByte is defined as 1,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (when Bytes In < 10, the result will be 0). It is then converted to a string, and labeled with the suffix KB (such as, 0.01 KB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
KBytesOut	This variable converts the Bytes Out field to KBytes, where a KByte is defined as 1,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes Out < 10, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
KBytesOut_Labeled	This variable converts the Bytes Out field to KBytes, where a KByte is defined as 1,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes Out < 10, the result is 0). It is then converted to a string, and labeled with the suffix KB (for example, 0.01 KB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/

Global Variable Fields, continued

Resource	Description	URI
KBytesTotal	This variable converts the combination of the Bytes In and Bytes Out fields to KBytes, where a KByte is defined as 1,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (when Bytes In + Bytes Out < 10, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
KBytesTotal_Labeled	This variable converts the combination of the Bytes In and Bytes Out fields to KBytes, where a KByte is defined as 1,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In+ Bytes Out < 10, the result is 0). It is then converted to a string, and labeled with the suffix KB (for example, 0.01 KB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
MBytesIn	This variable converts the Bytes In field to MBytes, where a MByte is defined as 1,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In < 10,000, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
MBytesIn_Labeled	This variable converts the Bytes In field to MBytes, where a MByte is defined as 1,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In < 10,000, the result is 0). It is then converted to a string, and labeled with the suffix MB (for example, 0.01 MB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
MBytesOut	This variable converts the Bytes Out field to MBytes, where a MByte is defined as 1,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes Out < 10,000, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
MBytesOut_Labeled	This variable converts the Bytes Out field to MBytes, where a MByte is defined as 1,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes Out < 10,000, the result is 0). It is then converted to a string, and labeled with the suffix MB (for example, 0.01 MB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
MBytesTotal	This variable converts the combination of the Bytes In and Bytes Out fields to MBytes, where a MByte is defined as 1,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In + Bytes Out < 10,000, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
MBytesTotal_Labeled	This variable converts the combination of Bytes In andBytes Out fields to MBytes, where a MByte is defined as 1,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In + Bytes Out < 10,000, the result is 0). It is then converted to a string, and labeled with the suffix MB (for example, 0.01 MB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/

Global Variable Fields, continued

Resource	Description	URI
Minute	This variable returns the minute in a two-digit format. For example: 02	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
Month	This variable returns the numeric value of the month from the end time date field. The Month variable prepends 0 to months with a single digit, so that the format is always MM (for example, July displays as 07 instead of 7).	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
Protocol	This variable returns the available protocol information within the event. The format is <transportProtocol> .| <applicationProtocol>(targetPort) Examples: TCP | HTTP(80) TCP(1024) ICMP DNS(53) unknown	/All Fields/ArcSight Foundation/Variables Library/
Source IPv6 Address	This variable is an alias for Device Custom IPv6 Address1.	/All Fields/ArcSight Foundation/Variables Library/IPv6/
SystemActedUpon	This variable returns the target host (if known) or the attacker host if it is the only host information available within the event. The format is the same as the TargetHost or AttackerHost variables.	/All Fields/ArcSight Foundation/Variables Library/Asset Information/
Target IPv6 Address	This field denotes the Target IPv6 address. The term target is dependent upon the originator field, i.e., Source or Destination, depending on the specific event. If the originator field is Destination, return Device Custom IPv6 Address2 (aliased as Destination IPv6 Address), or return Device Custom IPv6 Address1 (aliased as Source IPv6 Address)	/All Fields/ArcSight Foundation/Variables Library/IPv6/
TargetAsset	This variable returns the target asset information from an event. The asset information is in the format <targetZoneName>.| <targetAssetName> | <targetAddress> Examples: RFC1918: 192.168.0.0-192.168.255.255, ltwiki.sv.arcsight.com | 192.168.10.20 RFC1918: 192.168.0.0-192.168.255.255 | 192.168.10.30 unknown|	/All Fields/ArcSight Foundation/Variables Library/Asset Information/
TargetAssetCriticality	This variable returns the criticality categorization of the target asset as categorized using the /All Asset Categories/System Asset Categories/Criticality asset categories (for example, Very High, High, Medium, Low, Very Low, unknown).	/All Fields/ArcSight Foundation/Variables Library/Asset Information/
TargetHost	This variable returns available target information from an event. The format of the information is targetZoneName. | <targetHostName> | <targetAddress>:<targetPort> Information that is not in the event will not show a place-holder. Examples: RFC1918: 192.168.0.0-192.168.255.255 | ltwiki.sv.arcsight.com | 192.168.10.20:80 RFC1918: 192.168.0.0-192.168.255.255 | 192.168.10.30:53 RFC1918: 192.168.0.0-192.168.255.255:53 192.168.10.30:53 unknown	/All Fields/ArcSight Foundation/Variables Library/Host Information/

Global Variable Fields, continued

Resource	Description	URI
TargetOS	This variable returns the operating system of the target asset (if available), or unknown. For example: Microsoft/Windows XP, Microsoft/Windows 2000/Server, Unknown.	/All Fields/ArcSight Foundation/Variables Library/Asset Information/
TargetUser	This variable displays the target user name. If the target user name is unavailable, the variable displays the target user ID. If neither field is available, the variable displays unknown.	/All Fields/ArcSight Foundation/Variables Library/User Information/
TotalBytes	This variable sums the values of Bytes In and Bytes Out for each event.	/All Fields/ArcSight Foundation/Variables Library/Bytes/
UserActedUpon	This variable selects the target user (if known) or the attacker user if it is the only user information available within the event. The format is the same as the TargetUser or AttackerUser variable.	/All Fields/ArcSight Foundation/Variables Library/User Information/
Year	This variable returns the year. For example: 2002	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/

Appendix C: ArcSight System Resources

This appendix lists all the resources by type in the ArcSight System packages.

Active Channels

The following table lists all the active channels.

Active Channel Resources

Resource	Description	URI
Last 5 Minutes	This active channel shows events received during the last five minutes. The active channel includes a sliding window that always displays the last five minutes of event data.	/All Active Channels/ArcSight System/All Events/
Last Hour	This active channel shows events received during the last hour. The active channel includes a sliding window that always displays an hour of event data.	/All Active Channels/ArcSight System/All Events/
Live	This active channel shows events received during the last two hours. The active channel includes a sliding window that always displays the last two hours of event data. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events.	/All Active Channels/ArcSight System/Core/

Active Channel Resources, continued

Resource	Description	URI
Personal Live	This active channel shows events received during the last two hours. The active channel includes a sliding window that always displays the last two hours of event data. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events. This active channel also hides all the events that have been assigned to the current user.	/All Active Channels/ArcSight System/Core/
System Events Last Hour	This active channel shows all events generated by ArcSight during the last hour. A filter prevents the active channel from showing events that contributed to a rule triggering, commonly referred to as correlated events.	/All Active Channels/ArcSight System/
Today	This active channel shows events received today since midnight. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events.	/All Active Channels/ArcSight System/

Active Lists

The following table lists all the active lists.

Active List Resources

Resource	Description	URI
Account Authenticators	This active list is used by the actor global variables to determine the Identity Management authenticator, based on the event, so that an actor can be determined from event information.	/All Active Lists/ArcSight System/Actor Data Support/
Compromised List	This active list contains hosts that may have been compromised by an attack.	/All Active Lists/ArcSight System/Threat Tracking/
Event-based Rule Exclusions	This active list stores event information that is used to exclude specific events from one system to another system that has been determined to be not relevant to the rules that would otherwise trigger on these events.	/All Active Lists/ArcSight System/Tuning/
Hit List	This active list contains hosts targeted by a potential attacker.	/All Active Lists/ArcSight System/Targets/
Hostile List	This active list contains hosts that have been attempting attacks on systems.	/All Active Lists/ArcSight System/Threat Tracking/

Active List Resources, continued

Resource	Description	URI
Infiltrators List	This active list contains hosts which have compromised (infiltrated) a system.	/All Active Lists/ArcSight System/Threat Tracking/
Reconnaissance List	This active list contains IP addresses of hosts which have performed reconaissance activity.	/All Active Lists/ArcSight System/Threat Tracking/
Scanned List	This active list contains hosts that have been scanned by a potential attacker.	/All Active Lists/ArcSight System/Targets/
Suspicious List	This active list contains hosts which have performed suspicious activity, either on the local system or over the network.	/All Active Lists/ArcSight System/Threat Tracking/
Trusted List	This active list is to be manually populated with the addresses of trusted systems that are typically used for security scanning.	/All Active Lists/ArcSight System/Attackers/
Untrusted List	This active list is to be manually populated with the addresses of known malicious systems.	/All Active Lists/ArcSight System/Attackers/
User-based Rule Exclusions	This active list contains target user information of specific users to be excluded from certain rule conditions where the rule tracks user activity.	/All Active Lists/ArcSight System/Tuning/

Destinations

The following table lists all the destinations.

Destination Resources

Resource	Description	URI
admin	This destination is pre-defined for SOC operators. Add additional information, such as email address.	/All Destinations/SOC Operators/1/
admincert	This destination is pre-defined for the CERT team. Add more information, such as email addresses.	/All DestinationsCERT Team/1/

Field Sets

The following table lists all the field sets.

Field Set Resources

Resource	Description	URI
Actor Base	This field set contains all the fields related to actors.	/All Field Sets/ArcSight System/Actor Field Sets
Actor Information	This field set contains a set of fields used to view actor data in events.	/All Field Sets/ArcSight System/Actor Field Sets
Asset Information	This field set contains a collection of fields used to view asset data in asset channels, queries, and so on, focusing on asset resources.	/All Field Sets/ArcSight System/Asset Field Sets
Case Information	This field set contains a collection of fields used to view case attributes in case channels, queries, and so on, focusing on case resources.	/All Field Sets/ArcSight System/Case Field Sets
Event Base	This field set contains all the ESM event fields.	/All Field Sets/ArcSight System/Event Field Sets
Annotation	This field set contains annotation attributes for events.	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Annotation-MgrRcpt	None	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
ArcSight Admin	None	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
ArcSight Express	This field set contains basic fields for reviewing events in an active channel to select which ones to investigate.	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Assets	None	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Categories	This field set shows all the categorization fields for events.	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Executive	None	/All Field Sets/ArcSight System/Event Field Sets/Active Channels

Field Set Resources, continued

Resource	Description	URI
Export	None	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
MSSP	None	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Security	This field set contains several fields that are formatted to show more detailed information for security-related fields without needing to use the event inspector.	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Standard	This field set contains several fields that are useful at a glance for selecting events for inspection. It uses the end time field for the timestamp.	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Standard-MgrRcpt	None	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Super Minimal	None	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Annotation	None	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit
Categories	This field set shows all the categorization fields for events.	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit
Common Conditions Editor	None	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit
Event Inspector	None	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit
Minimal	None	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit
Rule Action - Set Event Field	None	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit

Field Set Resources, continued

Resource	Description	URI
Super Minimal	None	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit
TurboMode Comprehensive	None	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit
TurboMode Fastest	None	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit

Filters

The following table lists all the filters.

Filter Resources

Resource	Description	URI
ASM Events	This filter selects ArcSight System Monitoring events generated by the local ESM system (in an hierarchical deployment).	/All Filters/ArcSight System/Event Types/
All Events	This filter matches all events.	/All Filters/ArcSight System/Core/
ArcSight Correlation Events	This filter identifies correlation events generated by ArcSight systems.	/All Filters/ArcSight System/Event Types/
ArcSight Events	This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included.	/All Filters/ArcSight System/Event Types/
ArcSight Internal Events	This filter selects events that are internal events generated by the ArcSight ESM system.	/All Filters/ArcSight System/Event Types/
Attacker User Name is NULL	This filter identifies events in which the attacker user name is NULL.	/All Filters/ArcSight System/Core/

Filter Resources, continued

Resource	Description	URI
Attackers on Hostile List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.	ArcSight System/Core/Threat Level Filters/
Attackers on Infiltrators List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.	/All Filters/ArcSight System/Core/Threat Level Filters/
Attackers on Reconnaissance List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.	/All Filters/ArcSight System/Core/Threat Level Filters/
Attackers on Suspicious List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.	/All Filters/ArcSight System/Core/Threat Level Filters/
Blocked ArcSight Internal Events	This filter is applied to audit events before they are inserted. Modify this filter to disable internal events as needed.	/All Filters/ArcSight System/Event Types/
Compromised Targets	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.	/All Filters/ArcSight System/Core/Threat Level Filters/
Connector Asset Auto-Creation Controller	This filter is used internally by the asset auto-creation feature for connectors. The asset auto-creation feature automatically creates assets in the ArcSight Asset model for events whose connectors are not already modeled. You can configure the filter to include or exclude connectors from the asset auto-creation feature.	/All Filters/ArcSight System/Asset Auto-Creation/
Correlation Events	This filter identifies correlation events.	/All Filters/ArcSight System/Event Types/
Device Asset Auto-Creation Controller	This filter is used internally by the asset auto-creation feature for devices. The asset auto-creation feature automatically creates assets in the ArcSight Asset model for events whose devices are not already modeled. You can configure the filter to include or exclude devices from the asset auto-creation feature.	/All Filters/ArcSight System/Asset Auto-Creation/
High Criticality Assets	This filter captures events where the target asset ID has been categorized as having a High criticality.	/All Filters/ArcSight System/Core/Threat Level Filters/

Filter Resources, continued

Resource	Description	URI
Low Criticality Assets	This filter captures events where the target asset ID has been categorized as having a Low criticality.	/All Filters/ArcSight System/Core/Threat Level Filters/
Medium Criticality Assets	This filter captures events where the target asset ID has been categorized as having a Medium criticality.	/All Filters/ArcSight System/Core/Threat Level Filters/
No Events	This is a utility filter that does not match any events passing through the system.	/All Filters/ArcSight System/Core/
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	/All Filters/ArcSight System/Event Types/
Non-ArcSight Internal Events	This filter selects events that are not internal events generated by the ArcSight ESM system.	/All Filters/ArcSight System/Event Types/
Non-Categorized Events	This filter selects events that have no categorization.	/All Filters/ArcSight System/Event Types/
Not Correlated and Not Closed	This filter selects events that have not had their event annotation flags set to correlated (by a rule) or close (by an analyst).	/All Filters/ArcSight System/Event Types/
Not Correlated and Not Closed and Not Hidden	This filter selects events that have not had their event annotation flags set to correlated (by a rule), close (by an analyst) or hidden (by system settings).	/All Filters/ArcSight System/Event Types/
SNMP Trap Sender	This resource has no description.	/All Filters/ArcSight System/SNMP Forwarding/
Severity High	This filter captures events where the agent severity is High.	/All Filters/ArcSight System/Event Types/
Severity Low	This filter captures events where the agent severity is Low.	/All Filters/ArcSight System/Event Types/

Filter Resources, continued

Resource	Description	URI
Severity Medium	This filter captures events where the agent severity is Medium.	/All Filters/ArcSight System/Event Types/
Severity Unknown	This filter captures events where the agent severity is either NULL or Unknown.	/All Filters/ArcSight System/Event Types/
Severity Very High	This filter captures events where the agent severity is Very High.	/All Filters/ArcSight System/Event Types/
Target Asset Scanned for Open Ports	This filter detects events in which the Target Asset ID is categorized as scanned and showing open ports. This filter is used by the Priority Formula.	/All Filters/ArcSight System/Core/
Target Asset Scanned for Vulnerabilities	This filter detects events in which the Target Asset ID is categorized as scanned and showing vulnerabilities. This filter is used by the Priority Formula.	/All Filters/ArcSight System/Core/
Unknown Criticality Assets	This filter captures events where the target asset ID exists but has been categorized as having criticality.	/All Filters/ArcSight System/Core/Threat Level Filters/
Very High Criticality Assets	This filter captures events where the target asset ID has been categorized as having a Very High criticality.	/All Filters/ArcSight System/Core/Threat Level Filters/
Very Low Criticality Assets	This filter captures events where the target asset ID has been categorized as having a Very Low criticality.	/All Filters/ArcSight System/Core/Threat Level Filters/

Integration Commands

The following table lists all the integration commands.

Integration Command Resources

Resource	Description	URI
Web Search	This integration command is used to run a search with the selected item, device vendor, and device product in the selected event.	/All Integration Commands/ArcSight System/Tools/
Nslookup (Linux)	This integration command is used to find details about the Domain Name System (DNS). Run this command from a Linux console.	/All Integration Commands/ArcSight System/Tools/Linux/
Nslookup-IPv6 (Linux)	This integration command is used to find details about an IPv6 hostname in the Domain Name System (DNS). Run this command from a Linux console.	/All Integration Commands/ArcSight System/Tools/Linux/
Ping (Linux)	This integration command is used to test whether a particular host is reachable across an IP network. Run this command from a Linux console.	/All Integration Commands/ArcSight System/Tools/Linux/
Ping6 (Linux)	This integration command is used to test whether a particular host is reachable across an IPv6 network. Run this command from a Linux console.	/All Integration Commands/ArcSight System/Tools/Linux/
Portinfo (Linux)	This integration command is used to find information about the selected port. Run this command from a Linux console.	/All Integration Commands/ArcSight System/Tools/Linux/
Traceroute (Linux)	This integration command is used to determine the route taken by packets across an IP network. Run this command from a Linux console.	/All Integration Commands/ArcSight System/Tools/Linux/
Whois (Linux)	This integration command is used to determine the owner of a domain name or an IP address on the Internet. Run this command from a Linux console.	/All Integration Commands/ArcSight System/Tools/Linux/
Nslookup (Windows)	This integration command is used to find details about the Domain Name System (DNS). Run this command from a Windows console.	/All Integration Commands/ArcSight System/Tools/Windows/
Ping (Windows)	This integration command is used to test whether a particular host is reachable across an IP network. Run this command from a Windows console.	/All Integration Commands/ArcSight System/Tools/Windows/

Integration Command Resources, continued

Resource	Description	URI
Portinfo (Windows)	This integration command is used to find information about the selected port. Run this command from a Windows console.	/All Integration Commands/ArcSight System/Tools/Windows/
Traceroute (Windows)	This integration command is used to determine the route taken by packets across an IP network. Run this command from a Windows console.	/All Integration Commands/ArcSight System/Tools/Windows/
Whois (Windows)	This integration command is used to determine the owner of a domain name or an IP address on the Internet. Run this command from a Windows console.	/All Integration Commands/ArcSight System/Tools/Windows/

Integration Configurations

The following table lists all the integration configurations.

Integration Configuration Resources

Resource	Description	URI
Web Search	This integration configuration is used to configure the web search command. You can run the command on any cell selected in the viewer.	/All Integration Configurations/ArcSight System/Tools/
Nslookup (Linux)	This integration configuration is used to configure the Linux nslookup command. You can run the command on an IP address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Linux/
Nslookup-IPv6 (Linux)	This integration configuration is used to configure the Linux nslookup command. You can run the command on an IPv6 address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Linux/
Ping (Linux)	This integration configuration is used to configure the Linux ping command. You can run the command on an IP address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Linux/
Ping6 (Linux)	This integration configuration is used to configure the Linux ping command. You can run the command on an IPv6 address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Linux/
Portinfo (Linux)	This integration configuration is used to configure the Linux portinfo command. You can run the command on a port (Integer) selected in the viewer or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Linux/

Integration Configuration Resources, continued

Resource	Description	URI
Traceroute (Linux)	This integration configuration is used to configure the Linux traceroute command. You can run the command on an IP address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Linux/
Whois (Linux)	This integration configuration is used to configure the Linux whois command. You can run the command on an IP address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Linux/
Nslookup (Windows)	This integration configuration is used to configure the Windows nslookup command. You can run the command on an IP address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Windows/
Ping (Windows)	This integration configuration is used to configure the Windows ping command. You can run the command on an IP address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Windows/
Portinfo (Windows)	This integration configuration is used to configure the Windows portinfo command. You can run the command on a port (Integer) selected in the viewer or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Windows/
Traceroute (Windows)	This integration configuration is used to configure the Windows traceroute command. You can run the command on an IP address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Windows/
Whois (Windows)	This integration configuration is used to configure the Windows whois command. You can run the command on an IP address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Windows/

Queries

The following table lists all the queries.

Query Resources

Resource	Description	URI
Actor Event Count by Account ID	This query shows activity related to an actor based on the ActorByAccountID global variable.	/All Queries/ArcSight System/Core/Actor Context Report/
Actor Event Count by Attacker Username	This query shows activity related to an actor based on the ActorByAttackerUserName global variable.	/All Queries/ArcSight System/Core/Actor Context Report/
Actor Event Count by Custom Fields	This query shows activity related to an actor based on the AccountByCustomFields global variable.	/All Queries/ArcSight System/Core/Actor Context Report/
Actor Event Count by Target Username	This query shows activity related to an actor based on the AccountByTargetUserName global variable.	/All Queries/ArcSight System/Core/Actor Context Report/
Actor Events by Account ID	This query shows activity related to an actor based on the ActorByAccountID global variable.	/All Queries/ArcSight System/Core/Actor Context Report/
Actor Events by Attacker Username	This query shows activity related to an actor based on the ActorByAttackerUserName global variable.	/All Queries/ArcSight System/Core/Actor Context Report/
Actor Events by Custom Fields	This query shows activity related to an actor based on the ActorByCustomFields global variable.	/All Queries/ArcSight System/Core/Actor Context Report/
Actor Events by Target Username	This query shows activity related to an actor based on the ActorByTargetUsername global variable.	/All Queries/ArcSight System/Core/Actor Context Report/
Actor Information	This query shows activity related to an actor.	/All Queries/ArcSight System/Core/Actor Context Report/
Selected Case Query	This query returns information for the selected case. The query must contain a single parameter for the case resource ID.	/All Queries/ArcSight System/Core/Selected Case Report/

Reports

The following table lists all the reports.

Report Resources

Resource	Description	URI
Actor Context Report by Account ID	This report shows activity related to an actor based on the ActorByAccountID global variable.	/All Reports/ArcSight System/Core/
Actor Context Report by Attacker Username	This report shows activity related to an actor based on the ActorByAttackerUserName global variable.	/All Reports/ArcSight System/Core/
Actor Context Report by Custom Fields	This report shows activity related to an actor based on the ActorByCustomFields global variable.	/All Reports/ArcSight System/Core/
Actor Context Report by Target Username	This report shows activity related to an actor based on the ActorByTargetUserName global variable.	/All Reports/ArcSight System/Core/
Assets having Vulnerability	This report is used by the ArcSight console for internal processing, and is not meant to be run on its own.	/All Reports/ArcSight System/Core/
Selected Case Report	This report shows information for the selected case.	/All Reports/ArcSight System/Core/
Vulnerabilities of an Asset	This report is used by the ArcSight console for internal processing, and is not meant to be run on its own.	/All Reports/ArcSight System/Core/

Rules

The following table lists all the rules.

Rule Resources

Resource	Description	URI
Compromise - Attempt	This rule detects any attempt to compromise a device from a source that is not listed in a trusted active list. The rule triggers whenever an event is categorized as Attempt and Compromise. On the first event, agent severity is set to high, the attacker address is added to the Hostile List active list, and the target address is added to the Hit List active list.	`/All Rules/Real-Time Rules/ArcSight System/Threat Tracking/Compromise/`
Compromise - Success	This rule detects any successful attempt to compromise a device from a source that is not listed in a trusted active list, with either the attacker information (zone and address) or the target information present. The rule triggers whenever an event is categorized as Success and Compromise. On the first event, agent severity is set to high, the attacker address is added to the Hostile List and Infiltrators List active lists, and the target address is added to the Compromised List and Hit List active lists.	`/All Rules/Real-Time Rules/ArcSight System/Threat Tracking/Compromise/`
Hostile - Attempt	This rule detects any hostile attempt on a device that is not already compromised from a source that is not listed in a trusted active list. The rule triggers whenever an event is categorized as Attempt and Hostile, and the target does not belong to a compromised active list. On the first event, agent severity is set to medium, attacker address is added to the Hostile List active list, and the target address is added to the Hit List active list.	`/All Rules/Real-Time Rules/ArcSight System/Threat Tracking/Hostile/`
Hostile - Success	This rule detects any successful hostile attempts on a device that is not already compromised from a source not listed in a trusted active list. The rule triggers whenever an event is categorized as Success and Hostile, and the target does not belong to a compromised active list. On the first event, the severity is set to medium, the attacker address is added to the Hostile List active list, and the target address is added to the Hit List active list.	`/All Rules/Real-Time Rules/ArcSight System/Threat Tracking/Hostile/`

Rule Resources, continued

Resource	Description	URI
Incident Resolved - Remove From List	This rule detects a Resolved message in an ArcSight Data Monitor Value Change event from the Attacked or Compromised Systems data monitor (in the Executive View dashboard), which is sent when a user marks an asset within the data monitor as resolved. **Note**: This rule triggers only if you have the Intrusion Monitoring package installed from a previous ESM release.	`/All Rules/Real-Time Rules/ArcSight System/Threat Tracking/Compromise/`
Reconnaissance - Attackers	The rule identifies correlation events which originate from other reconnaissance rules. The events signify successful reconnaissance events from an attacker which is added to the Reconnaissance ActiveList.	`/All Rules/Real-Time Rules/ArcSight System/Threat Tracking/Reconnaissance/`
Reconnaissance - Targets	The rule identifies correlation events which originate from other reconnaissance rules. The events signify successful reconnaissance events targetted by an external attacker to an internal asset. The rule adds the target information into the Scanned ActiveList	`/All Rules/Real-Time Rules/ArcSight System/Threat Tracking/Reconnaissance/`

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on ArcSight Administration and ArcSight System Standard Content Guide (ESM 7.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!