



HP ArcSight ESM

Software Version: 6.8c

ArcSight Core Security, ArcSight Administration and ArcSight System Standard Content Guide

December 9, 2014

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HP ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2015 Hewlett-Packard Development Company, L.P.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

Support

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support Page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hp.com
Protect 724 Community	https://protect724.hp.com

Contents

Chapter 1: Standard Content Overview	6
What is Standard Content?	6
Standard Content Packages	8
Standard Content Documentation	9
Chapter 2: Installing and Configuring the Content	10
Modeling the Network	10
Categorizing Assets	11
Configuring Active Lists	12
Configuring Filters	12
Enabling Rules	12
Configuring Notifications and Cases	13
Configuring Notification Destinations	13
Rules with Notifications to the CERT Team	14
Rules with Notifications to SOC Operators	14
Rules with Notifications to the Device Administrators Group	15
Scheduling Reports	15
Configuring Trends	15
Viewing Use Case Resources	16
Chapter 3: ArcSight Core Security Content	17
Configuring the ArcSight Core Security Use Case	17
Using the ArcSight Core Security Use Case	18
Using the Firewall Monitoring Overview Dashboard	19
Using the IDS - IPS Overview Dashboard	20
Using the Microsoft Windows Monitoring Overview Dashboard	21
Using the NetFlow Bandwidth Usage Overview Dashboard	22
Using the Security Alerts Overview Dashboard	23
ArcSight Core Security Resources	25
Chapter 4: ArcSight Administration Content	32
Connector Overview	35

Configuring the Connector Overview Use Case	35
Using the Connector Overview Use Case	35
Connector Overview Resources	37
ESM Overview	44
Using the ESM Overview Use Case	44
ESM Overview Resources	45
Logger Overview	47
Configuring the Logger Overview Use Case	47
Using the Logger Overview Use Case	48
Logger Overview Resources	49
Connector Configuration Changes	61
Connector Configuration Changes Resources	61
Connector Connection and Cache Status	71
Configuring the Connector Connection and Cache Status Use Case	71
Connector Connection and Cache Status Resources	72
Device Monitoring	89
Configuring the Device Monitoring Use Case	89
Device Monitoring Resources	90
ArcSight ESM Device Monitoring	101
Understanding Connector Device Status Events	101
Configuring the ArcSight ESM Device Monitoring Use Case	102
Using the ArcSight ESM Device Monitoring Use Case	103
ArcSight ESM Device Monitoring Resources	107
ESM Licensing	116
ESM Licensing Resources	116
ESM User Sessions	123
ESM User Sessions Resources	123
Actor Configuration Changes	127
Actor Configuration Changes Resources	127
ESM Resource Configuration Changes	138
ESM Resource Configuration Changes Resources	138
Content Management	142
Configuring the Content Management Use Case	142
Content Management Resources	142
HA Monitoring	145
HA Monitoring Audit Events	145
Configuring the HA Monitoring Use Case	146

Using the HA Monitoring Use Case	146
HA Monitoring Resources	151
ESM Events	154
ESM Events Resources	154
ESM Reporting Resource Monitoring	166
ESM Reporting Resource Monitoring Resources	166
ESM Resource Monitoring	177
Configuring the ESM Resource Monitoring Use Case	177
ESM Resource Monitoring Resources	177
ESM Storage Monitoring (CORR)	188
Configuring the ESM Storage Monitoring (CORR) Use Case	188
ESM Storage Monitoring (CORR) Resources	188
ESM Storage Monitoring (Oracle)	199
ESM Storage Monitoring (Oracle) Resources	199
Logger Events	208
Logger Events Resources	208
Logger System Health	210
Configuring the Logger System Health Use Case	210
Logger System Health Resources	211
Chapter 5: ArcSight System Content	224
Actor Support Resources	224
Actor Support Resources	225
Priority Formula Resources	230
Configuring the Priority Formula Resources Group	230
Priority Formula Resources	231
System Resources	237
Configuring the System Resources Group	237
System Resources	238
Send Documentation Feedback	251

Chapter 1: Standard Content Overview

This chapter discusses the following topics.

What is Standard Content?	6
Standard Content Packages	8
Standard Content Documentation	9

What is Standard Content?

Standard content is a series of coordinated resources (filters, rules, dashboards, reports, and so on) that address common security and management tasks. Standard content is designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out-of-the box with minimal configuration. The content provides a full spectrum of security, network, and configuration monitoring tasks, as well as a comprehensive set of tasks that monitor the health of the system.

Standard content is installed using a series of packages, 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 organized by category.

Standard content consists of the following:

- **ArcSight Core Security** content is installed automatically with the ArcSight Manager and consists of key resources for monitoring Microsoft Windows, firewall, IPS and IDS, NetFlow, and other essential security information.
- **ArcSight Administration** content contains several packages that provide statistics about the health and performance of ArcSight products.
 - ArcSight Administration is installed automatically with the ArcSight Manager and is essential for managing and tuning the performance of content and components.
 - ArcSight Admin DB CORR 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.

- ArcSight Content Management 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.

- ArcSight ESM HA Monitoring 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.
- ArcSight Search Filters is installed automatically with the ArcSight Manager for use in the ArcSight Command Center. You cannot edit or use these filters in the ArcSight Console. For information about the search filters, refer to the *ArcSight Command Center User's Guide*.

Note: The ArcSight Search Filters 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.

- **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 out-of-the-box functionality. The ArcSight Networks package contains the zones that were in the ArcSight Core package in previous releases, in addition to local and global network resources.
- **ArcSight Foundation** content (such as Cisco Monitoring, Configuration Monitoring, Intrusion Monitoring, IPv6, NetFlow Monitoring, Network Monitoring, and Workflow) provide a coordinated system of resources with real-time monitoring capabilities for a specific area of focus, as well as after-the-fact analysis in the form of reports and trends. You can extend these foundations with additional resources specific to your needs or you can use them as a template for building your own resources and tasks. You can install a Foundation during installation or from the ArcSight Console any time after installation.
- **Shared Libraries** - ArcSight Administration and several of the ArcSight Foundations rely on a series of common resources that provide core functionality for common security scenarios. Dependencies between these resources and the packages they support are managed by the Package resource.
 - Anti Virus content is a set of filters, reports, and report queries used by ArcSight Foundations, such as Configuration Monitoring and Intrusion Monitoring.
 - Conditional Variable Filters content is a library of filters used by variables in standard content report queries, filters, and rule definitions. The Conditional Variable Filters are used by ArcSight Administration and certain ArcSight Foundations, such as Configuration Monitoring, Intrusion Monitoring, Network Monitoring, and Workflow.
 - Global Variables content is 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

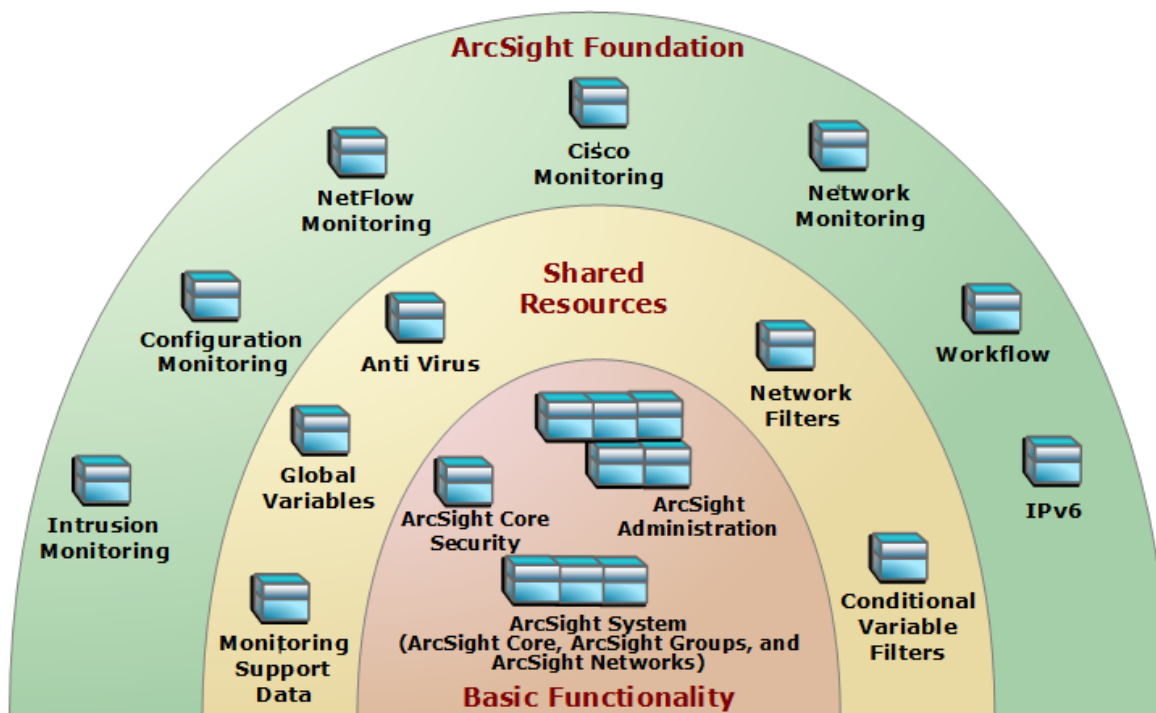
commonly used timestamp formats. The Global Variables are used by ArcSight Administration and certain ArcSight Foundations.

- Monitoring Support Data content is a set of active lists that store mapping information for HTTP return status code classes, Cisco firewall syslog message types, and encoded logon types.
- Network filters content is a set of filters required by ArcSight Administration and certain ArcSight Foundations, such as Intrusion Monitoring and Network Monitoring.

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

Standard Content Packages

Standard content comes in packages (.arb files) that are either installed automatically or presented as install-time options. The following graphic outlines the packages.



The ArcSight Core Security, ArcSight Administration, and ArcSight System packages at the base provide content required for basic functionality. The common packages in the center contain shared resources that support multiple packages. The packages shown on top are ArcSight Foundations that address common network security and management scenarios.

Depending on the options you install, you will see the ArcSight Core Security, ArcSight Administration, and ArcSight System resources and some or all of the other package content.

Caution: When creating your own packages, you can explicitly include or exclude system resources in the package. Exercise caution if you delete packages that might have system resources. Make sure the system resources either belong to a locked group or are themselves locked. For more information about packages, refer to the *ArcSight Console User's Guide*.

Standard Content Documentation

This guide describes the content. For information about an optional ArcSight Foundation, refer to the Standard Content Guide for that Foundation. ArcSight documentation is available on [Protect 724](https://protect724.hp.com) (<https://protect724.hp.com>).

Chapter 2: Installing and Configuring the Content

This section provides installation and basic configuration instructions for content. For information about installing and configuring an optional Foundation, refer to the Standard Content Guide for that Foundation.

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** and **ESM HA Monitoring** are *optional* content packages provided in the ArcSight Administration package group when you perform a new ArcSight Manager installation. You can install either of these packages during ArcSight Manager installation or from the ArcSight Console any time after installation.

To install either of these packages 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 *ESM Installation and Configuration Guide*.

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

Modeling the Network	10
Categorizing Assets	11
Configuring Active Lists	12
Configuring Filters	12
Enabling Rules	12
Configuring Notifications and Cases	13
Configuring Notification Destinations	13
Scheduling Reports	15
Configuring Trends	15
Viewing Use Case Resources	16

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	<p>Categorize all assets (or the zones to which the assets belong) that are internal to the network with this asset category.</p> <p>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 <i>Protected</i>.</p> <p>Note: Assets with a private IP address (such as 192.168.0.0) are considered <i>Protected</i> by the system, even if they are not categorized as such.</p>
/System Asset Categories/ Criticality/High	<p>Categorize all assets that are considered <i>critical</i> 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.</p> <p>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.</p>
/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 Core Security active lists you need to configure manually, refer to the configuration information for the use case presented in ["ArcSight Core Security Content" on page 17](#).

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 32](#).

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 224](#).

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 32](#).

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 224](#).

ArcSight Core Security content does not include filters that you need to configure.

Enabling Rules

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

- By default, all the ArcSight Core Security and **ArcSight System** rules are deployed in the `Real-Time Rules` group and are also enabled.
- By default, all the **ArcSight Administration** rules are deployed in the `Real-Time Rules` group and all rules, except for the Logger System Health rules, are enabled. 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 47](#).

- 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** package 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 users 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 rules are configured to send notifications to the **CERT Team** notification destination group.

Rule Name	Rule URI
High Number of IDS Alerts for DoS	ArcSight Core Security/Security Activity/
SYN Flood Detected by IDS or Firewall	ArcSight Core Security/Security Activity/
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
Probable Successful Brute Force Attack	ArcSight Core Security/Security Activity/
Connector Dropping Events	ArcSight Administration/Connectors/System Health/
Connector Still Down	ArcSight Administration/Connectors/System Health/
Connector Still Caching	ArcSight Administration/Connectors/System Health/
Critical Device Not Reporting	ArcSight Administration/Connectors/System Health/Custom/
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 ["Configuring the ArcSight ESM Device Monitoring Use Case" on page 102](#).

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, which can 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 Core Security and ArcSight Administration content includes trends, which are enabled by default. 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. 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 Trends Details dashboard shows the runtime status for all enabled trends. The trend reports show statistics about trend performance for all enabled trends.

Viewing Use Case Resources

The ArcSight Core Security and ArcSight Administration resources are grouped together in the ArcSight Console using use case resources. A use case resource provides a way to group a set of resources that help address a specific security issue or business requirement.

Note: Currently, ArcSight System content does not contain any use case resources. ["ArcSight System Content" on page 224](#) documents System resources by grouping them by function.

To view the resources associated with a use case resource:

1. In the Navigator panel, select the **Use Cases** tab.
2. Browse for a use case resource such as ArcSight Administration/ESM Overview.
3. Right-click the use case resource and select the **Open Use Case** option, or double-click the use case resource.

The resources that make up a use case resource are displayed in the Viewer.

The use case resource tables listed in ["ArcSight Core Security Content" on page 17](#) and ["ArcSight Administration Content" on page 32](#) describe all the resources that have been assigned to each use case and include dependent resources.

Chapter 3: ArcSight Core Security Content

The ArcSight Core Security content provides essential information about activity in your environment that might be a security concern. Focusing on Microsoft Windows, firewall, and intrusion detection and prevention activity, the ArcSight Core Security content monitors:

- Anti-virus activity
- Outbound traffic to suspicious destinations
- Brute force attacks
- Denial of service attacks
- Suspicious mail
- Reconnaissance activity
- Network bandwidth usage

Rules in the ArcSight Core Security and ArcSight System rule groups detect the activities listed above. You can create your own rules to detect any activity specific to your organization. When the rules are triggered, the activity appears in the dashboards provided by the ArcSight Core Security use case.

The key ArcSight Core Security resources are listed in the ArcSight Core Security use case.

Caution: ArcSight Core Security resources are **not** locked even though they manage core functionality; HP recommends that you do not delete or modify these resources unless you are an advanced user who understands fully the resources and their dependencies.

Configuring the ArcSight Core Security Use Case

The ArcSight Core Security use case requires the following configuration for your environment:

- Populate the **Suspicious Countries** active list with the countries that your organization identifies as suspicious.
- Populate the **Non-Security Alerts** active list with the names of the rules you consider insignificant or that do not trigger security-related alerts; the rules you specify in this active list are not used by this use case.

Using the ArcSight Core Security Use Case

This section highlights some key features of the ArcSight Core Security use case. Follow the steps below to get started.

1. For an overall, event-level view of security activity in your organization, click the **Resources** tab in the Navigator panel and open the **Security Analysis** active channel located in:

All Active Channels/ArcSight Core Security/

This active channel shows the correlation events during the last two hours that you need to investigate. Double-click an event to see details about both the correlation event and base event that triggered it.

2. For a broader view of activity, based on various areas of security, click the **Use Cases** tab in the Navigator panel and open the **ArcSight Core Security** use case located in:

All Use Cases/ArcSight Core Security

This use case provides access to the following overview dashboards, which you can monitor to ensure that your environment is secure.

- Firewall Monitoring Overview
- IDS - IPS Overview
- Microsoft Windows Monitoring Overview
- NetFlow Bandwidth Usage Overview
- Security Alerts Overview

The following sections highlight some of the key features of these dashboards.

Using the Firewall Monitoring Overview Dashboard

The Firewall Monitoring Overview dashboard shows you a high-level view of the firewall related activity in your environment. The dashboard focuses on inbound, outbound, and internal communications that have been blocked by firewalls.

1. In the ArcSight Core Security use case, click the **Firewall Monitoring Overview** hyperlink to open the dashboard. A sample is shown below.



Internal dropped connections might indicate that either the firewall is not configured properly, or the internal host is sending suspicious events.

Blocked outbound communication is also of particular interest; it might indicate that the firewall prevented malware running on an internal host from *phoning home*, perhaps to store extracted confidential information.

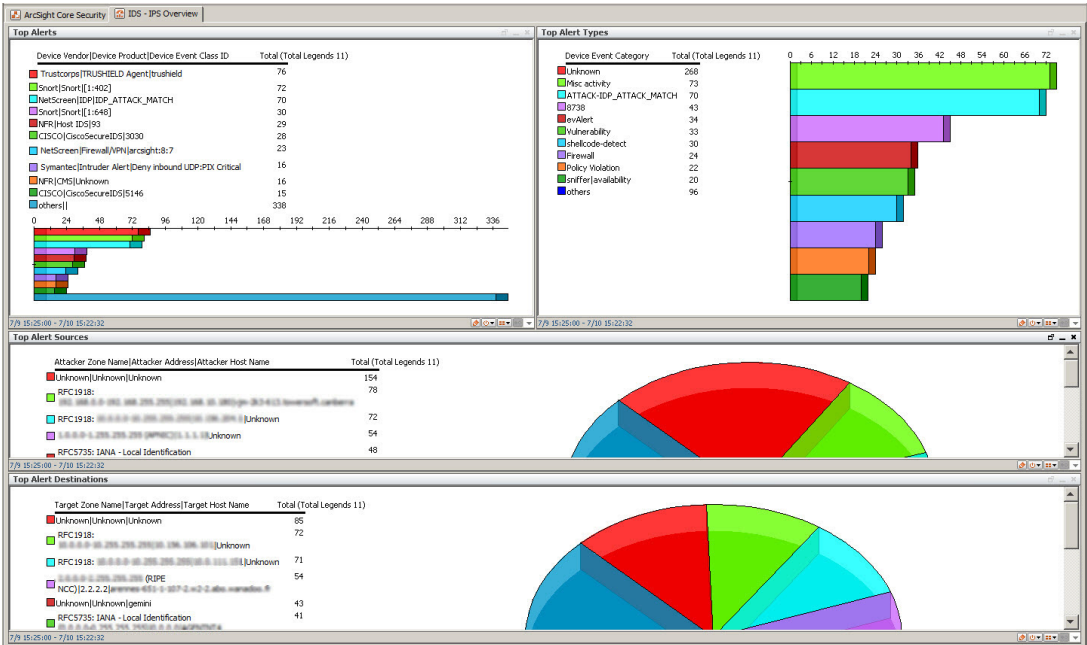
2. Analyze the graph in the **Denied Outbound Connections** component.

The graph shows the internal host, access port, and external host involved in the blocked communication. This information can help you determine whether an internal host failed to communicate with more than one external host, or several internal hosts tried to reach the same external host and failed.

Using the IDS - IPS Overview Dashboard

The IDS - IPS Overview dashboard shows the top alerts from intrusion detection and prevention systems, organized by device, event category, attacker, and target.

- 1. In the ArcSight Core Security use case, click the **IDS - IPS Overview** hyperlink to open the dashboard. A sample is shown below.



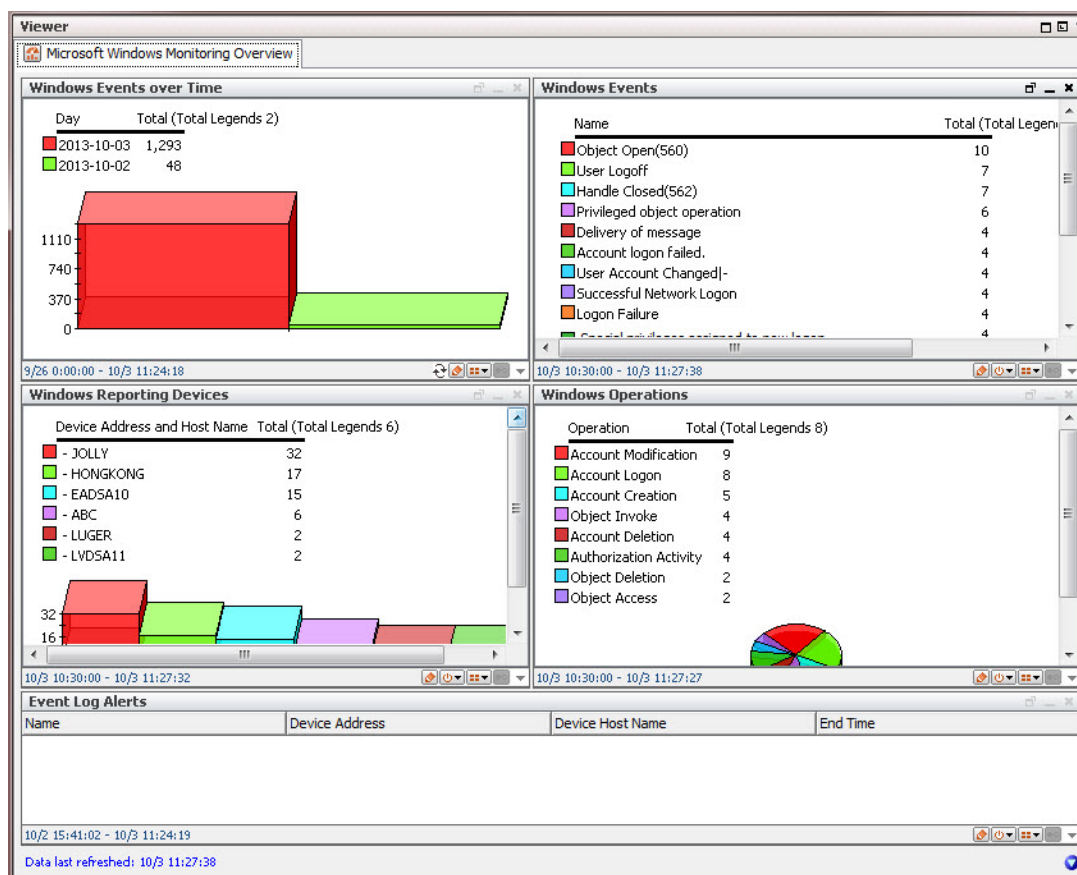
- 2. Review the components in the dashboard.

Use the information in the data monitors to identify any vulnerabilities or attacks, and any assets that are already compromised.

Using the Microsoft Windows Monitoring Overview Dashboard

The Microsoft Windows Monitoring Overview dashboard shows the most common Microsoft Windows operations, the top devices that report Microsoft Windows events, and information about Microsoft Windows events.

1. In the ArcSight Core Security use case, click the **Microsoft Windows Monitoring Overview** hyperlink to open the dashboard. A sample is shown below.

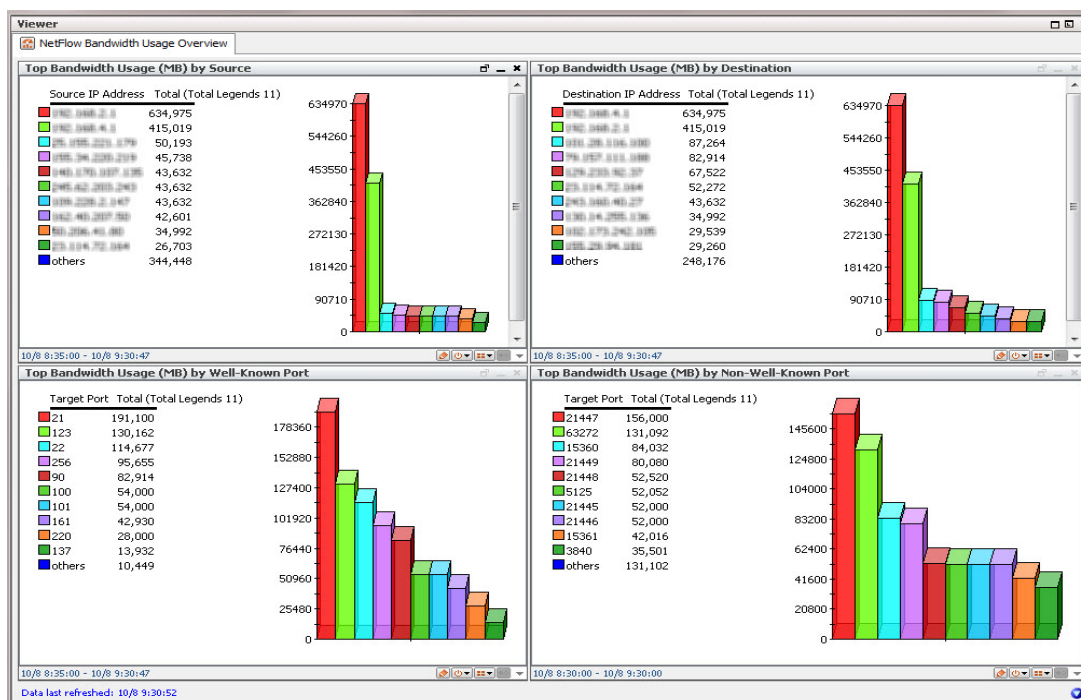


2. Examine the **Windows Operations** component showing the ten most common Windows operations. Investigate any suspicious activity.
3. Examine the **Windows Reporting Devices** bar chart showing the addresses and hostnames of the top 20 devices that reported Windows events.
4. Examine the **Windows Events** component to see the most common Windows event names received within the last hour.

Using the NetFlow Bandwidth Usage Overview Dashboard

NetFlow is a network protocol developed by Cisco Systems to collect IP traffic information. If your organization uses NetFlow and has enabled the ArcSight NetFlow Monitoring content, you can use the NetFlow Bandwidth Usage Overview dashboard to determine top network bandwidth usage by source and destination IP addresses, and ports.

1. In the ArcSight Core Security use case, click the **NetFlow Bandwidth Usage Overview** hyperlink to open the dashboard. A sample is shown below.



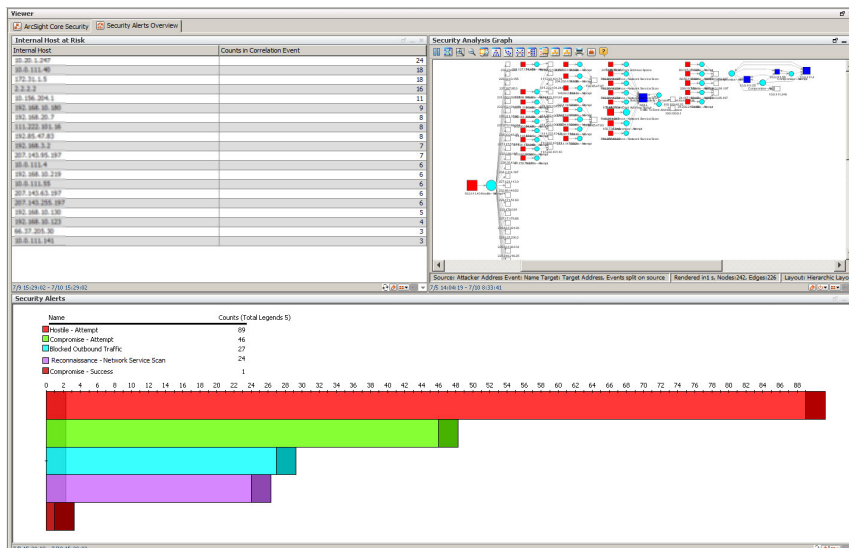
2. Review the components in the dashboard.

High bandwidth usage might be the result of acceptable activity, such as video conferencing or business critical applications. However, it might also indicate activities that you need to investigate, such as excessive, non-essential audio or video streaming.

Using the Security Alerts Overview Dashboard

The Security Alerts Overview dashboard shows all security activity on your network that requires your attention, including the top hosts at risk. The dashboard provides data from the last hour.

1. In the ArcSight Core Security use case, click the **Security Alerts Overview** hyperlink to open the dashboard. A sample is shown below.



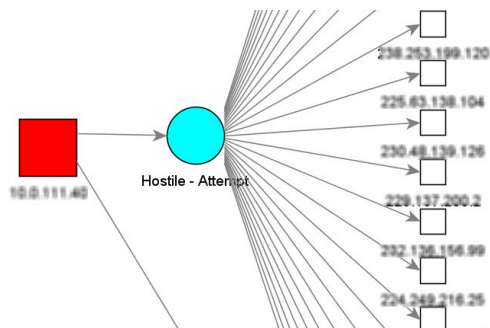
The **Internal Hosts at Risk** component shows the internal hosts in your environment most affected by the security issues. The higher the correlation count, the higher the risk potential. Investigate these hosts to determine which issues are affecting them.

2. In the **Internal Hosts at Risk** component, right-click the top host IP address and select **Investigate > Create Channel [Internal Host=nnn.nnn.nnn.nnn]**.
3. In the resulting display, right-click a row and select **Show Event Details** to see additional information about the base event in the Event Inspector.
4. Click the **Details** tab in the Event Inspector to see if there are any links to reference pages or vulnerability pages. These pages typically provide a detailed explanation of the event from the device vendor and information about associated vulnerabilities.
5. Return to the **Security Alerts Overview** dashboard and review the **Security Analysis Graph** component.

This component shows the top issues found in your network. The alert names correspond to the rules in the ArcSight Core Security and ArcSight System rule groups. If you determine that a particular alert is not a valid security concern and you do not want it to appear in this component, you can add the alert's corresponding rule name to the **Non-Security Alerts** active list.

- Return to the **Security Alerts Overview** dashboard and review the **Security Analysis Graph** component (undock the component and zoom in to improve readability).

This component provides a unique perspective on security activity in your network. It shows the relationship between the source address involved in a suspicious security event and the destination addresses, through the name of the event.

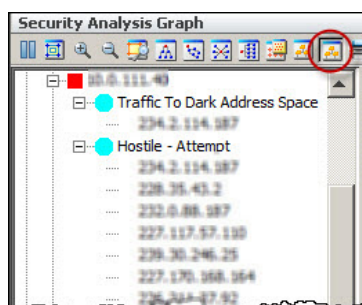


By examining the relationships in the graph, you can determine whether the host is:

- *both the source and destination* of the events, which might indicate the host is compromised and affecting other hosts
- involved in more than one type of suspicious security activity

In either case, investigate these hosts immediately.

- Click the **Analysis Tree** icon above the graph for an easy-to-navigate tree view, as shown below.



ArcSight Core Security Resources

The following table lists all the resources in the ArcSight Core Security use case.

Resources that Support the ArcSight Core Security Use Case

Resource	Description	Type	URI
Monitor Resources			
Security Analysis	This active channel shows correlation events that should be investigated. Double-click an event to see details about both the correlation event and the base event that triggered it.	Active Channel	ArcSight Core Security/
IDS - IPS Overview	This dashboard shows an overview of IDS alerts.	Dashboard	ArcSight Core Security/
Firewall Monitoring Overview	This dashboard provides top level firewall activity statistics for denied inbound and outbound connections.	Dashboard	ArcSight Core Security/
NetFlow Bandwidth Usage Overview	This dashboard shows the top bandwidth usage as reported by NetFlow events, showing the top bandwidth usage by source, destination, well-known port, and non well-known port.	Dashboard	ArcSight Core Security/
Security Alerts Overview	This dashboard provides an overview of various network intrusions from both external and internal sources.	Dashboard	ArcSight Core Security/
Microsoft Windows Monitoring Overview	This dashboard monitors the top Windows event, Windows operations, Windows Reporting Devices, Event Log Alerts, and Windows Events over Time.	Dashboard	ArcSight Core Security/
Windows Events over Time	This query viewer shows the total number of Windows events per day over the last 7 days.	Query Viewer	ArcSight Core Security/Microsoft Windows Monitoring/
Library Resources			

Resources that Support the ArcSight Core Security Use Case, continued

Resource	Description	Type	URI
Event Operations	This active list stores the conversion between the category behavior value and the user friendly name. This list is pre-populated and the entries never expire by default.	Active List	ArcSight Core Security/Microsoft Windows Monitoring/
Non-Security Alerts	This active list stores the names of non-security related rules.	Active List	ArcSight Core Security/Security Activity/
Suspicious Countries	This active list stores suspicious country names.	Active List	ArcSight Core Security/Security Activity/
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Windows Reporting Devices	This data monitor shows the top devices that reported Windows events.	Data Monitor	ArcSight Core Security/Microsoft Windows Monitoring/
Top Bandwidth Usage (MB) by Destination	This data monitor displays the total bandwidth usage in MegaBytes (MB) from NetFlow events for top Destination IP Addresses.	Data Monitor	ArcSight Core Security/NetFlow Monitoring/
Windows Operations	This data monitor shows the top Windows operations.	Data Monitor	ArcSight Core Security/Microsoft Windows Monitoring/
Security Analysis Graph	This data monitor shows the relationship between the attacker and target for security alerts.	Data Monitor	ArcSight Core Security/Security Activity/
Windows Events	This data monitor displays the top Windows event names.	Data Monitor	ArcSight Core Security/Microsoft Windows Monitoring/
Top Denied Inbound Connections by Port	This data monitor shows the top denied inbound firewall connections by port.	Data Monitor	ArcSight Core Security/Firewall Monitoring/

Resources that Support the ArcSight Core Security Use Case, continued

Resource	Description	Type	URI
Top Bandwidth Usage (MB) by Well-Known Port	This data monitor displays the total bandwidth usage in MegaBytes (MB) from NetFlow events for Well Known Ports.	Data Monitor	ArcSight Core Security/NetFlow Monitoring/
Internal Connection Drops	This data monitor shows internal firewall connection drops.	Data Monitor	ArcSight Core Security/Firewall Monitoring/
Top Bandwidth Usage (MB) by Non-Well-Known Port	This data monitor displays the total bandwidth usage in MegaBytes (MB) from NetFlow events for Non Well Known Ports.	Data Monitor	ArcSight Core Security/NetFlow Monitoring/
Top Alert Types	This data monitor shows the top IDS alert types.	Data Monitor	ArcSight Core Security/IDS-IPS Monitoring/
Top Bandwidth Usage (MB) by Source	This data monitor displays the total bandwidth usage in MegaBytes (MB) from NetFlow events for the top Source IP Addresses.	Data Monitor	ArcSight Core Security/NetFlow Monitoring/
Top Alert Destinations	This data monitor shows the top ten destination hosts with IDS alert counts.	Data Monitor	ArcSight Core Security/IDS-IPS Monitoring/
Event Log Alerts	This data monitor shows the last 20 Windows events indicating the event log was cleared, discarded, or unable to log event and the audit policy was changed.	Data Monitor	ArcSight Core Security/Microsoft Windows Monitoring/
Denied Outbound Connections	This data monitor shows denied outbound firewall connections.	Data Monitor	ArcSight Core Security/Firewall Monitoring/
Top Alert Sources	This data monitor shows the top source hosts with IDS alert counts.	Data Monitor	ArcSight Core Security/IDS-IPS Monitoring/
Internal Hosts at Risk	This data monitor shows internal hosts perceived to be at risk.	Data Monitor	ArcSight Core Security/Security Activity/

Resources that Support the ArcSight Core Security Use Case, continued

Resource	Description	Type	URI
Security Alerts	This data monitor shows a bucketized bar chart of various security alerts.	Data Monitor	ArcSight Core Security/Security Activity/
Top Denied Inbound Connections by Address	This data monitor shows the top denied inbound firewall connections by address.	Data Monitor	ArcSight Core Security/Firewall Monitoring/
Top Alerts	This data monitor shows the top IDS alerts.	Data Monitor	ArcSight Core Security/IDS-IPS Monitoring/
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).	Global Variable	ArcSight Foundation/Variables Library/Bytes
TotalBytes	This variable sums the values of Bytes In and Bytes Out for each event.	Global Variable	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).	Global Variable	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).	Global Variable	ArcSight Foundation/Variables Library/Bytes

Resources that Support the ArcSight Core Security Use Case, continued

Resource	Description	Type	URI
Bandwidth Usage Alerts	This field set contains fields of interest for bandwidth usage alerts.	Field Set	ArcSight Core Security/
Security Alerts	This field set contains fields of interest for security alerts.	Field Set	ArcSight Core Security/
Windows Alerts	This field set contains fields of interest for windows alerts.	Field Set	ArcSight Core Security/
Firewall Alerts	This field set contains fields of interest for firewall alerts.	Field Set	ArcSight Core Security/
Denied Outbound Connections	This filter identifies firewall events in which the category behavior is /Access and the category outcome is /Failure. The filter identifies outbound events.	Filter	ArcSight Core Security/Firewall Monitoring/
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Outbound Events	This filter identifies events originating from inside the company network, targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
Bytes Out is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Bytes Out is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Bytes
Event Operations	This filter provides the Windows events which have Category Behavior information.	Filter	ArcSight Core Security/Microsoft Windows Monitoring/
Denied Inbound Connections	This filter identifies firewall events in which the category behavior is /Access and the category outcome is /Failure. The filter identifies inbound events.	Filter	ArcSight Core Security/Firewall Monitoring/
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters

Resources that Support the ArcSight Core Security Use Case, continued

Resource	Description	Type	URI
Internal Firewall Events	This filter identifies firewall events in which the category outcome is /Failure	Filter	ArcSight Core Security/Firewall Monitoring/
Security Alerts	This filter identifies security alerts.	Filter	ArcSight Core Security/Security Activity/
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
QoSient Argus Events	This filter identifies events from Argus SmartConnectors.	Filter	ArcSight Core Security/NetFlow Monitoring/
Event Log Alerts	This filter provides the Windows events indicating the event log was cleared, discarded, or unable to log event and the audit policy was changed.	Filter	ArcSight Core Security/Microsoft Windows Monitoring/
Bytes In is NULL	This filter is designed for conditional expression variables. The filter identifies events in which the Bytes In is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Bytes
IDS -IPS Events	This filter identifies Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) Base events.	Filter	ArcSight Core Security/IDS-IPS Monitoring/
Windows Events	This filter is designed to provide only Windows events.	Filter	ArcSight Core Security/Microsoft Windows Monitoring/
NetFlow Traffic Reporting Devices	This filter identifies NetFlow traffic reporting devices. By default, the filter contains QoSient Argus, NetFlow V5, and NetFlow V9 events.	Filter	ArcSight Core Security/NetFlow Monitoring/
Internal to Internal Events	This filter retrieves events internal to the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters

Resources that Support the ArcSight Core Security Use Case, continued

Resource	Description	Type	URI
Inbound Events	This filter identifies events coming from the outside network targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
External Target	This filter identifies events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
NetFlow V9 Events	This filter identifies NetFlow version 9 events.	Filter	ArcSight Core Security/NetFlow Monitoring/
NetFlow Traffic for Non-Well-Known Ports	This filter identifies events from NetFlow Traffic Reporting Devices where the Target Port is not NULL and is greater than or equal to 1024.	Filter	ArcSight Core Security/NetFlow Monitoring/
NetFlow Traffic for Well-Known Ports	This filter identifies events from NetFlow Traffic Reporting devices where the Target Port is not NULL and is less than 1024.	Filter	ArcSight Core Security/NetFlow Monitoring/
NetFlow V5 Events	This filter identifies NetFlow version 5 events.	Filter	ArcSight Core Security/NetFlow Monitoring/
Windows Events over Time	This query looks for Windows events.	Query	ArcSight Core Security/Microsoft Windows Monitoring/
Windows Events by Device Trend	This query selects the device address, device event class ID, and device hostname of Windows events.	Query	ArcSight Core Security/Microsoft Windows Monitoring/For Trends/
Windows Events by Event and Device	This trend tracks the number of Windows events by device. It stores the number of Windows events, device address, device event class id, and device host name.	Trend	ArcSight Core Security/Microsoft Windows Monitoring/

Chapter 4: 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 resources are grouped together according to use cases. A use case provides a way to group a set of resources that help address a specific issue or function. 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 listed in the resource tables for the use cases 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 35	"The Connector Overview use case provides administration content for monitoring SmartConnectors and devices."
"ESM Overview" on page 44	"The ESM Overview use case provides administration content for monitoring the ArcSight system."
"Logger Overview" on page 47	"The Logger Overview use case provides Logger status and statistics."
Connectors	
"Connector Configuration Changes" on page 61	"The Connector Configuration Changes use case provides information about configuration changes (such as upgrades) and the versions of the SmartConnectors on the system."
"Connector Connection and Cache Status" on page 71	"The Connector Connection and Cache Status use case provides the connection status and caching status of SmartConnectors in the system. SmartConnectors can be connected directly to the ArcSight system or through Loggers."

Use Case	Purpose
"Device Monitoring" on page 89	"The Device Monitoring use case provides information about the devices reporting to the ArcSight system. "
Devices	
"ArcSight ESM Device Monitoring" on page 101	"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."
ESM	
"ESM Licensing" on page 116	"The ESM Licensing use case provides information about licensing compliance."
"ESM User Sessions" on page 123	"The ESM User Sessions use case provides information about user access to the ArcSight system."
ESM - Configuration Changes	
"Actor Configuration Changes" on page 127	"The Actor Configuration Changes use case provides information about changes to the actor resources."
"ESM Resource Configuration Changes" on page 138	"The ESM Resource Configuration Changes use case provides information about changes to the various resources, such as rules, reports, and so on."
ESM - Content Management	
"Content Management" on page 142	"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."
ESM - HA Monitoring	
"HA Monitoring" on page 145	"The 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. "

Use Case	Purpose
ESM - System Health	
"ESM Events" on page 154	"The ESM Events use case provides statistics on the flow of events through the ArcSight system."
"ESM Reporting Resource Monitoring" on page 166	"The ESM Reporting Resource Monitoring use case provides performance statistics for reports, trends, and query viewers."
"ESM Resource Monitoring" on page 177	"The ESM Resource Monitoring use case provides processing statistics for various resources, such as trends, rules, and so on."
"ESM Storage Monitoring (CORR)" on page 188	"The ESM Storage Monitoring (CORR) 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."
"ESM Storage Monitoring (Oracle)" on page 199	"The ESM Storage Monitoring (Oracle) use case provides information on the health of the Oracle database. This does not apply if you are using ESM with CORR-Engine or ArcSight Express with CORR-Engine."
Logger	
"Logger Events" on page 208	"The Logger Events use case provides statistics for events sent through a Logger."
"Logger System Health" on page 210	"The Logger System Health use case provides performance statistics for any Logger connected to the ArcSight system."

Connector Overview

The Connector Overview use case provides administration content for monitoring SmartConnectors 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 - Down**
- **Connectors - Caching**
- **Black List - Connectors**

For information about configuring these active lists, refer to the configuration section in "[Connector Connection and Cache Status](#)" on page 71.

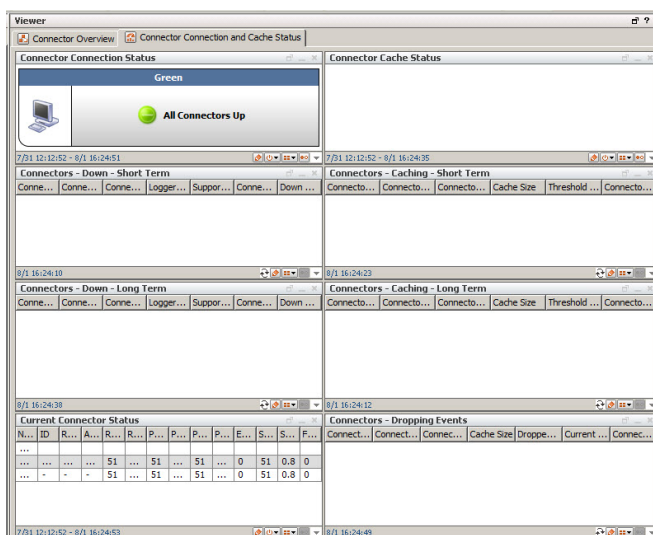
Using the Connector Overview Use Case

This section highlights some key features of the Connector Overview use case. Follow the steps below to get started.

1. In the Navigator panel, click the **Use Cases** tab and open the **Connector Overview** use case located in:

All Use Cases/ArcSight Administration

2. Click the **Connector Connection and Cache Status** hyperlink to open the dashboard. A sample is shown below.



Focus on any yellow or red icons, as they represent connectors that might require attention.

3. The center, left components show connectors that have been down for less than 20 minutes (yellow icons) and 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 improperly configured or needs to be restarted; or there is an underlying network, connection, or hardware problem.

4. You can find more information about each connector in the Connector Connection and Cache Status component. 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.)
5. 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.
6. Check the **Cache Size** and **Threshold Size** columns to determine if the cache is nearing its maximum capacity.
7. Check the Connector Connection and Cache Status component 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 its configuration guide. For information about connector caching issues, check the [Protect 724](#) community.

Connector Overview Resources

The following table lists all the resources in the Connector Overview use case.

Resources that Support the Connector Overview Use Case

Resource	Description	Type	URI
Monitor Resources			
Connector Connection and Cache Status	This dashboard displays the overall status of connectors and information on connectors that are down, caching, or dropping events.	Dashboard	ArcSight Administration/Connectors/System Health/
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.	Dashboard	ArcSight Administration/Connectors/System Health/
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.	Query Viewer	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.	Query Viewer	ArcSight Administration/Connectors/System Health/

Resources that Support the Connector Overview Use Case, continued

Resource	Description	Type	URI
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.	Query Viewer	ArcSight Administration/Connectors/System Health/
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.	Query Viewer	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.	Query Viewer	ArcSight Administration/Connectors/System Health/
Library - Correlation Resources			
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.	Rule	ArcSight Administration/Connectors/System Health/

Resources that Support the Connector Overview Use Case, continued

Resource	Description	Type	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.	Rule	ArcSight Administration/Connectors/System Health/
Library Resources			
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.	Active List	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).	Active List	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.	Active List	ArcSight Administration/Connectors/System Health/

Resources that Support the Connector Overview Use Case, continued

Resource	Description	Type	URI
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.	Active List	ArcSight Administration/Connectors/System Health/
Connectors - Still Down	This active list stores the ID and the name of the connectors that 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.	Active List	ArcSight Administration/Connectors/System Health/
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).	Active List	ArcSight Administration/Connectors/System Health/

Resources that Support the Connector Overview Use Case, continued

Resource	Description	Type	URI
Top Event Sources	This data monitor shows the most common event generating products and displays a listing of the top 20.	Data Monitor	ArcSight Administration/Connectors/System Health/Current Event Sources/
Current Connector Status	This data monitor displays information about the connectors that are registered with the system and reporting events.	Data Monitor	ArcSight Administration/Connectors/System Health/Current Event Sources/
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).	Data Monitor	ArcSight Administration/Connectors/System Health/Connector Connection and Cache Status/
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.	Data Monitor	ArcSight Administration/Connectors/System Health/Connector Connection and Cache Status/
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.	Field Set	ArcSight System/Event Field Sets/Active Channels
Connector Cache Status	This filter detects correlation events from the Update Connector Caching Status rule.	Filter	ArcSight Administration/Connectors/System Health/

Resources that Support the Connector Overview Use Case, continued

Resource	Description	Type	URI
Connector Connection Status	This filter detects correlation events related to connector connection status.	Filter	ArcSight Administration/Connectors/System Health/
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.	Filter	ArcSight System/Event Types
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types
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).	Query	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).	Query	ArcSight Administration/Connectors/System Health/Connector Monitoring/
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).	Query	ArcSight Administration/Connectors/System Health/Connector Monitoring/

Resources that Support the Connector Overview Use Case, continued

Resource	Description	Type	URI
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).	Query	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).	Query	ArcSight Administration/Connectors/System Health/Cache/
Connector Configuration Changes	This use case provides information about configuration changes (such as upgrades) and connector version changes on the system.	Use Case	ArcSight Administration/Connectors/
Device Monitoring	This use case provides information about the devices reporting to ESM.	Use Case	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.	Use Case	ArcSight Administration/Connectors/

ESM Overview

The ESM Overview use case provides administration content for monitoring the ArcSight system.

Using the ESM Overview Use Case

This section highlights some key features of the ESM Overview use case. Follow the steps below to get started.

1. For an event-level view of ESM, click the **Resources** tab in the Navigator panel and open the active channel located in:

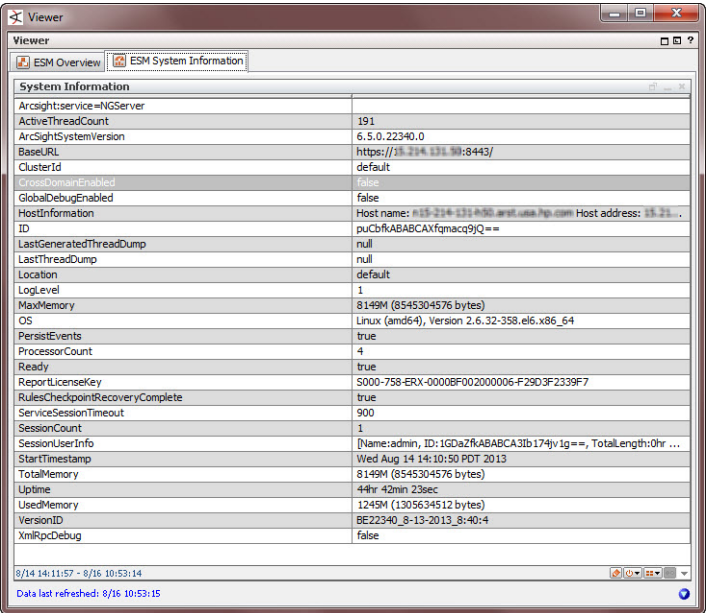
All Active Channels/ArcSight Administration/

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 correlation events. Double-click an event to see details about the event in the Event Inspector.

2. For a broader view of ESM, click the **Use Cases** tab in the Navigator panel and open the **ESM Overview** use case located in:

All Use Cases/ArcSight Administration

3. Click the hyperlink to open the dashboard. Review the System Information shown, which provides version, licensing, system resource availability and statistics, and other important settings and status for your ArcSight system. A sample is shown below.



ESM Overview Resources

The following table lists all the resources in the ESM Overview use case.

Resources that Support the ESM Overview Use Case

Resource	Description	Type	URI
Monitor 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.	Active Channel	ArcSight Administration/ESM/System Health/Events
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.	Dashboard	ArcSight Administration/ESM/System Health/
Library Resources			
System Information	This data monitor shows detailed system information about this ArcSight ESM.	Data Monitor	ArcSight Administration/ESM/System Health/ESM System Information/
Event Base	This field set contains all the ESM event fields.	Field Set	ArcSight System/Event Field Sets
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.	Field Set	ArcSight Administration/Connector/
ArcSight Admin	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Active Channels

Resources that Support the ESM Overview Use Case, continued

Resource	Description	Type	URI
ArcSight Internal Events	This filter selects events that are internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types
ASM Events	This filter selects ArcSight System Monitoring events generated by the local ESM system (in an hierarchical deployment).	Filter	ArcSight System/Event Types
ESM Resource Monitoring	This use case provides processing statistics for various ESM resources, such as trends, rules, and so on.	Use Case	ArcSight Administration/ESM/System Health/
Actor Configuration Changes	This use case provides information about changes made to the actor resources.	Use Case	ArcSight Administration/ESM/Configuration Changes/
ESM User Sessions	This use case provides information about user access to ESM.	Use Case	ArcSight Administration/ESM/
ESM Storage Monitoring (CORR)	This use case provides information about the health of the CORR Engine (ArcSight Express 3.0 and beyond).	Use Case	ArcSight Administration/ESM/System Health
ESM Licensing	This use case provides information about ESM licensing compliance.	Use Case	ArcSight Administration/ESM/
ESM Events	This use case provides statistics about the flow of events through ESM.	Use Case	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.	Use Case	ArcSight Administration/ESM/Configuration Changes/
ESM Reporting Resource Monitoring	This use case provides information about performance statistics for reports, trends, and query viewers.	Use Case	ArcSight Administration/ESM/System Health/

Logger Overview

The Logger Overview use case provides Logger status and statistics.

Configuring the Logger Overview Use Case

The Logger Overview use case requires the following configuration for your environment if you have a Logger connected to the ArcSight system:

- Enable the following rules:
 - **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 ["Enabling Rules" on page 12](#).

- Enable the notification action for the above listed rules, if appropriate for your organization. For information on how to enable notifications, refer to the *ArcSight Console User's Guide*.
- 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 Logger.

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

Using the Logger Overview Use Case

This section highlights some key features of the Logger Overview use case. Follow the steps below to get started.

1. In the Navigator panel, click the **Use Cases** tab and open the **Logger Overview** use case located in:

All Use Cases/ArcSight Administration

2. Click the **My Logger Overview** hyperlink to open the dashboard.
3. 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 over the last ten minutes.
4. In the Logger Overview use case, click the **ArcSight Appliances Overview** hyperlink to open the dashboard.

Review the data monitors on the 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.

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.

Logger Overview Resources

The following table lists all the resources in the Logger Overview use case.

Resources that Support the Logger Overview Use Case

Resource	Description	Type	URI
Monitor Resources			
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.	Dashboard	ArcSight Administration/Logger/My Logger/
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.	Dashboard	ArcSight Administration/Logger/
Library - Correlation Resources			
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.	Rule	ArcSight Administration/Logger/System Health/

Resources that Support the Logger Overview Use Case, continued

Resource	Description	Type	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.	Rule	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.	Rule	ArcSight Administration/Logger/System Health/
Library Resources			
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.	Active List	ArcSight Administration/Logger/System Health/

Resources that Support the Logger Overview Use Case, continued

Resource	Description	Type	URI
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.	Active List	ArcSight Administration/Logger/System Health/
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.	Data Monitor	ArcSight Administration/Logger/ArcSight Appliances Overview/
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.	Data Monitor	ArcSight Administration/Logger/ArcSight Appliances Overview/

Resources that Support the Logger Overview Use Case, continued

Resource	Description	Type	URI
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.	Data Monitor	ArcSight Administration/Logger/My Logger/Network
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.	Data Monitor	ArcSight Administration/Logger/My Logger/My Logger Overview/
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.	Data Monitor	ArcSight Administration/Logger/My Logger/CPU and Memory/
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.	Data Monitor	ArcSight Administration/Logger/My Logger/Network

Resources that Support the Logger Overview Use Case, continued

Resource	Description	Type	URI
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.	Data Monitor	ArcSight Administration/Logger/My Logger/CPU and Memory/
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.	Data Monitor	ArcSight Administration/Logger/My Logger/My Logger Overview/
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.	Data Monitor	ArcSight Administration/Logger/My Logger/My Logger Overview/
Sensor Name	This field is an alias for Device Custom String5.	Global Variable	ArcSight Administration/Logger/
Sensor Status	This field is an alias for Device Custom String3.	Global Variable	ArcSight Administration/Logger/
Free Space	This field is an alias field for Device Custom Number1.	Global Variable	ArcSight Administration/Logger/
Timeframe	This field is an alias for Device Custom String2.	Global Variable	ArcSight Administration/Logger/

Resources that Support the Logger Overview Use Case, continued

Resource	Description	Type	URI
Disk Usage	This field returns the disk usage status whether it is normal or nearing critical usage (less than ten percent).	Global Variable	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.	Global Variable	ArcSight Administration/Logger/
ReadOrWrite	This field returns whether the logger event is a read or write event.	Global Variable	ArcSight Administration/Logger/
Disk Name	This field returns the name of the disk currently being used.	Global Variable	ArcSight Administration/Logger/
IndexOfUsage	This field returns the index position of the string /Usage within the Device Event Category field.	Global Variable	ArcSight Administration/Logger/
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.	Global Variable	ArcSight Administration/Logger/
Field Value	This field is an alias field for Device Custom Number1.	Global Variable	ArcSight Administration/Logger/
Unit	This field is an alias for Device Custom String1.	Global Variable	ArcSight Administration/Logger/
Logger IP	This field is an alias to Destination Translated Address.	Global Variable	ArcSight Administration/Logger/
Memory Name	This field returns a memory related value located within the Device Event Category field.	Global Variable	ArcSight Administration/Logger/

Resources that Support the Logger Overview Use Case, continued

Resource	Description	Type	URI
All Receivers and Forwarders	This field shows the EPS from all connector and forwarder agents connected to this ArcSight ESM.	Global Variable	ArcSight Administration/Logger/
Logger Address	This field is an alias to the Device Address field.	Global Variable	ArcSight Administration/Logger/
Sensor Type	This field is an alias for Device Custom String4.	Global Variable	ArcSight Administration/Logger/
CPU Name	The field returns the name of the CPU currently used.	Global Variable	ArcSight Administration/Logger/
Field Status	This field is an alias field for Device Custom String3.	Global Variable	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.	Field Set	ArcSight Administration/Logger/
Sensor Type is CPU	This filter identifies events in which the sensor type is CPU.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance
Memory Usage	This filter identifies Logger system health events related to memory usage that originate from the Logger defined in the My Logger filter.	Filter	ArcSight Administration/Logger/System Health/CPU and Memory/
Logger System Health Events	This filter identifies Logger system health events.	Filter	ArcSight Administration/Logger/Event Types/

Resources that Support the Logger Overview Use Case, continued

Resource	Description	Type	URI
Network Usage	This filter identifies Logger system health events related to network usage that originate from the Logger defined in the My Logger filter.	Filter	ArcSight Administration/Logger/System Health/Network/
Logger Events	This filter identifies Logger events.	Filter	ArcSight Administration/Logger/Event Types/
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.	Filter	ArcSight Administration/Logger/ArcSight Appliances Overview/
All Receivers EPS	This filter identifies events in which the device event category is /Monitor/Receiver/All/EPS.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance
CPU Usage	This filter identifies Logger system health events related to CPU usage that originate from the Logger defined in the My Logger filter.	Filter	ArcSight Administration/Logger/System Health/CPU and Memory/
Sensor Type is FAN	This filter identifies events in which the sensor type is FAN.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance

Resources that Support the Logger Overview Use Case, continued

Resource	Description	Type	URI
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.	Filter	ArcSight Administration/Logger/System Health/
Remaining Disk More than 10 Percent	This filter identifies events in which the remaining disk space is greater than ten percent.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance
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.	Filter	ArcSight Administration/Logger/System Health/Hardware/
EPS Usage	This filter identifies Logger system health events related to EPS usage that originate from the Logger defined in the My Logger filter.	Filter	ArcSight Administration/Logger/System Health/Network/
ArcSight Correlation Events	This filter identifies correlation events generated by ArcSight systems.	Filter	ArcSight System/Event Types
Logger Disk Usage	This filter detects Logger system health events related to remaining disk space.	Filter	ArcSight Administration/Logger/ArcSight Appliances Overview/

Resources that Support the Logger Overview Use Case, continued

Resource	Description	Type	URI
Inbound Network	This filter identifies events in which the device event category ends with /In.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance
Remaining Disk Less than 5 Percent	This filter identifies events in which the remaining disk space is less than five percent.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance
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.	Filter	ArcSight Administration/Logger/System Health/Storage/
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.	Integration Command	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.	Integration Command	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.	Integration Command	ArcSight Administration/Logger/

Resources that Support the Logger Overview Use Case, continued

Resource	Description	Type	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.	Integration Command	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.	Integration Command	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.	Integration Command	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.	Integration Command	ArcSight Administration/Logger/
Logger Quick Search	This integration configuration is used to configure the Logger Quick Search command.	Integration Configuration	ArcSight Administration/Logger/

Resources that Support the Logger Overview Use Case, continued

Resource	Description	Type	URI
Logger Search	This integration configuration is used to configure the Logger Search command.	Integration Configuration	ArcSight Administration/Logger/
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.	Integration Target	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.	Integration Target	ArcSight Administration/Logger/
Logger System Health	This use case provides performance statistics for the Loggers connected to ESM.	Use Case	ArcSight Administration/Logger/
Logger Events	This use case provides information about statistics for events sent through Loggers to ESM.	Use Case	ArcSight Administration/Logger/

Connector Configuration Changes

The Connector Configuration Changes use case provides information about configuration changes (such as upgrades) and the versions of the SmartConnectors on the system.

Connector Configuration Changes Resources

The following table lists all the resources in the Connector Configuration Changes use case.

Resources that Support the Connector Configuration Changes Use Case

Resource	Description	Type	URI
Monitor Resources			
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.	Active Channel	ArcSight Administration/Connectors/Configuration Changes/
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.	Report	ArcSight Administration/Connectors/Configuration Changes/Versions/
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.	Report	ArcSight Administration/Connectors/Configuration Changes/Versions/

Resources that Support the Connector Configuration Changes Use Case, continued

Resource	Description	Type	URI
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.	Report	ArcSight Administration/Connectors/Configuration Changes/Upgrades/
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.	Report	ArcSight Administration/Connectors/Configuration Changes/Upgrades/
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.	Report	ArcSight Administration/Connectors/Configuration Changes/Upgrades/

Resources that Support the Connector Configuration Changes Use Case, continued

Resource	Description	Type	URI
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.	Report	ArcSight Administration/Connectors/Configuration Changes/Versions/
Successful Connector Upgrades	This report lists the connectors with successful upgrades (within the last seven days by default). The list is sorted chronologically.	Report	ArcSight Administration/Connectors/Configuration Changes/Upgrades/
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.	Report	ArcSight Administration/Connectors/Configuration Changes/Versions/
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).	Report	ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Library - Correlation Resources			

Resources that Support the Connector Configuration Changes Use Case, continued

Resource	Description	Type	URI
Connector Upgrade Failed	This rule detects failed connector upgrades. On every event, the connector information is added to the Connector Upgrades active list.	Rule	ArcSight Administration/Connectors/Configuration Changes/
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.	Rule	ArcSight Administration/Connectors/Configuration Changes/
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.	Rule	ArcSight Administration/Connectors/Configuration Changes/

Resources that Support the Connector Configuration Changes Use Case, continued

Resource	Description	Type	URI
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.	Rule	ArcSight Administration/Connectors/Configuration Changes/
Library Resources			
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.	Active List	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).	Active List	ArcSight Administration/Connectors/System Health/

Resources that Support the Connector Configuration Changes Use Case, continued

Resource	Description	Type	URI
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.	Active List	ArcSight Administration/Connectors/Configuration Changes/
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.	Active List	ArcSight Administration/Connectors/System Health/

Resources that Support the Connector Configuration Changes Use Case, continued

Resource	Description	Type	URI
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.	Active List	ArcSight Administration/Connectors/System Health/
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).	Active List	ArcSight Administration/Connectors/System Health/
Event Base	This field set contains all the ESM event fields.	Field Set	ArcSight System/Event Field Sets

Resources that Support the Connector Configuration Changes Use Case, continued

Resource	Description	Type	URI
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.	Field Set	ArcSight Administration/Connector/
Upgrade History by Connector	This query identifies all the connector upgrades (successful and failed) by connector in the Connector Upgrades active list.	Query	ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Connector Versions	This query identifies all the connectors with their latest versions in the Connector Versions session list.	Query	ArcSight Administration/Connectors/Configuration Changes/Versions/
Connector Upgrades Count	This query identifies the count of successful and failed connector upgrades per day in the Connector Upgrades active list.	Query	ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Version History by Connector Type	This query identifies all the connectors and connector versions by connector type in the Connector Versions session list.	Query	ArcSight Administration/Connectors/Configuration Changes/Versions/
Upgrade History by Connector Type	This query identifies all the connector upgrades (successful and failed) by connector type in the Connector Upgrades active list.	Query	ArcSight Administration/Connectors/Configuration Changes/Upgrades/

Resources that Support the Connector Configuration Changes Use Case, continued

Resource	Description	Type	URI
Connector Upgrades Count (Total)	This query identifies the total count of successful and failed connector upgrades in the Connector Upgrades active list.	Query	ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Successful Connector Upgrades	This query identifies the connectors with successful upgrades (and the new connector version) in the Connectors Upgrades active list.	Query	ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Connector Versions by Type	This query identifies all the connectors with their latest versions by connector type in the Connector Versions session list.	Query	ArcSight Administration/Connectors/Configuration Changes/Versions/
Failed Connector Upgrades	This query identifies the connectors with failed upgrades (and the reason for the failure) in the Connector Upgrades active list.	Query	ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Version History by Connector	This query identifies all the connector versions by connector in the Connector Versions session list.	Query	ArcSight Administration/Connectors/Configuration Changes/Versions/
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	ArcSight System/1 Table

Resources that Support the Connector Configuration Changes Use Case, continued

Resource	Description	Type	URI
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table
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.	Session List	ArcSight Administration/Connectors/Configuration Changes/

Connector Connection and Cache Status

The Connector Connection and Cache Status use case provides the connection status and caching status of SmartConnectors in the system. SmartConnectors 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 SmartConnector 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 SmartConnector 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 SmartConnector that has been caching for fewer than two hours is considered to be caching for a short term. SmartConnectors 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 SmartConnector 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 SmartConnector you want to exclude from being evaluated by the Connector UP and Connector Down rules.

The Connector UP and Connector Down rules detect SmartConnectors 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 SmartConnectors have been down for a certain period of time. You might want to exclude SmartConnectors that you start and stop manually, SmartConnectors that are scheduled to run once every week (such as vulnerability scanners), or SmartConnectors 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 SmartConnector, if needed. For example, you can add contact information for SmartConnectors 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 SmartConnectors that have reported into the system, as well as information from the ArcSight Manager when the SmartConnector is first registered. Do not add information to this active list for SmartConnectors that are not already reported into the system and registered.

For information about how to configure an active list, refer to ["Configuring Active Lists" on page 12](#).

- Optional: Enable the notification action for the following rules, if appropriate for your organization:
 - **Connector Up**
 - **Connector Down**
 - **Connector Dropping Events**
 - **Connector Still Down**

For information on how to enable notifications, refer to the *ArcSight Console User's Guide*.

Connector Connection and Cache Status Resources

The following table lists all the resources in the Connector Connection and Cache Status use case.

Resources that Support the Connector Connection and Cache Status Use Case

Resource	Description	Type	URI
Monitor Resources			
Connector Caching Events	This active channel displays information about Connector cache status audit events and correlation events from the related Connector Monitoring rules.	Active Channel	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.	Active Channel	ArcSight Administration/Connectors/System Health/

Resources that Support the Connector Connection and Cache Status Use Case, continued

Resource	Description	Type	URI
Connector Connection and Cache Status	This dashboard displays the overall status of connectors and information on connectors that are down, caching, or dropping events.	Dashboard	ArcSight Administration/Connectors/System Health/
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.	Query Viewer	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.	Query Viewer	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.	Query Viewer	ArcSight Administration/Connectors/System Health/

Resources that Support the Connector Connection and Cache Status Use Case, continued

Resource	Description	Type	URI
Connector s - 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.	Query Viewer	ArcSight Administration/Connectors/System Health/
Connector s - 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.	Query Viewer	ArcSight Administration/Connectors/System Health/

Resources that Support the Connector Connection and Cache Status Use Case, continued

Resource	Description	Type	URI
Cache History by Connectors	<p>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.</p>	Report	ArcSight Administration/Connectors/System Health/Cache/

Resources that Support the Connector Connection and Cache Status Use Case, continued

Resource	Description	Type	URI
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.	Report	ArcSight Administration/Connectors/System Health/Cache/
Library - Correlation Resources			
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.	Rule	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.	Rule	ArcSight Administration/Connectors/System Health/

Resources that Support the Connector Connection and Cache Status Use Case, continued

Resource	Description	Type	URI
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.	Rule	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.	Rule	ArcSight Administration/Connectors/System Health/
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.	Rule	ArcSight Administration/Connectors/System Health/

Resources that Support the Connector Connection and Cache Status Use Case, continued

Resource	Description	Type	URI
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.	Rule	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.	Rule	ArcSight Administration/Connectors/Configuration Changes/
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.	Rule	ArcSight Administration/Connectors/System Health/Custom/

Resources that Support the Connector Connection and Cache Status Use Case, continued

Resource	Description	Type	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.	Rule	ArcSight Administration/Connectors/Configuration Changes/
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.	Rule	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.	Rule	ArcSight Administration/Connectors/System Health/

Resources that Support the Connector Connection and Cache Status Use Case, continued

Resource	Description	Type	URI
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.	Rule	ArcSight Administration/Connectors/System Health/
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.	Rule	ArcSight Administration/Connectors/System Health/
Library Resources			

Resources that Support the Connector Connection and Cache Status Use Case, continued

Resource	Description	Type	URI
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.	Active List	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).	Active List	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.	Active List	ArcSight Administration/Connectors/System Health/

Resources that Support the Connector Connection and Cache Status Use Case, continued

Resource	Description	Type	URI
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.	Active List	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.	Active List	ArcSight Administration/Connectors/System Health/

Resources that Support the Connector Connection and Cache Status Use Case, continued

Resource	Description	Type	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).	Active List	ArcSight Administration/Connectors/System Health/Custom/
Black List - Connectors	This active list maintains a list of connectors that are not monitored by the Connector Monitoring rules.	Active List	ArcSight Administration/Connectors/System Health/Custom/

Resources that Support the Connector Connection and Cache Status Use Case, continued

Resource	Description	Type	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).	Active List	ArcSight Administration/Connectors/System Health/
Current Connector Status	This data monitor displays information about the connectors that are registered with the system and reporting events.	Data Monitor	ArcSight Administration/Connectors/System Health/Current Event Sources/
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.	Data Monitor	ArcSight Administration/Connectors/System Health/Connector Connection and Cache Status/

Resources that Support the Connector Connection and Cache Status Use Case, continued

Resource	Description	Type	URI
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).	Data Monitor	ArcSight Administration/Connectors/System Health/Connector Connection and Cache Status/
Event Base	This field set contains all the ESM event fields.	Field Set	ArcSight System/Event Field Sets
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.	Field Set	ArcSight Administration/Connector/
Connector Cache Status	This filter detects correlation events from the Update Connector Caching Status rule.	Filter	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.	Filter	ArcSight Administration/Connectors/System Health/Conditional Variable Filters/
Connector Caching Event	This filter detects connector caching events.	Filter	ArcSight Administration/Connectors/System Health/Conditional Variable Filters/

Resources that Support the Connector Connection and Cache Status Use Case, continued

Resource	Description	Type	URI
Connector Connection Status	This filter detects correlation events related to connector connection status.	Filter	ArcSight Administration/Connectors/System Health/
Cache History by Connectors	This query identifies the cache history for one connector (using a parameter) in the Connector - Caches session list.	Query	ArcSight Administration/Connectors/System Health/Cache/
Current Cache Status - Dropping Events	This query identifies the connectors in the Connectors - Dropping Events active list.	Query	ArcSight Administration/Connectors/System Health/Cache/
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).	Query	ArcSight Administration/Connectors/System Health/Cache/
Current Cache Status - Caching Events	This query identifies the connectors in the Connectors - Caching session list.	Query	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).	Query	ArcSight Administration/Connectors/System Health/Connector Monitoring/

Resources that Support the Connector Connection and Cache Status Use Case, continued

Resource	Description	Type	URI
Connector s - 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).	Query	ArcSight Administration/Connectors/System Health/Connector Monitoring/
Connector s - 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).	Query	ArcSight Administration/Connectors/System Health/Cache/
Connector s - 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).	Query	ArcSight Administration/Connectors/System Health/Cache/
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	ArcSight System/1 Table
Two Tables Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	ArcSight System/2 Tables

Resources that Support the Connector Connection and Cache Status Use Case, continued

Resource	Description	Type	URI
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.	Session List	ArcSight Administration/Connectors/Configuration Changes/
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.	Session List	ArcSight Administration/Connectors/System Health/

Device Monitoring

The Device Monitoring use case provides information about the devices reporting to the ArcSight system.

For more comprehensive information, use the ArcSight ESM Device Monitoring use case; see ["ArcSight ESM Device Monitoring" on page 101](#).

Configuring the Device Monitoring Use Case

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

Customize the following filters:

- Modify the **White List - Devices** filter to specify only the devices you want to insert in the Reporting Devices active list. Entries in this active list never expire.

The **White List - Devices** filter is used by the Device Reported rule to track the devices that send Device Status events to the Manager. By default, the condition in the filter is True, which means that all the devices that send Device Status events are inserted in the Reporting Devices active list.

- Modify the **White List - Critical Devices** filter to specify the critical devices you want to monitor closely and about which you want to be notified when they are not reporting. By default, the filter picks all the assets that are categorized as `/System Asset Categories/Criticality/High`.

The **White List - Critical Devices** filter is used by the Critical Device Reported rule to track the devices that send Device Status events and are also categorized as criticality High (`/System Asset Categories/Criticality/High`).

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

- Enable the **Critical Device Not Reporting** rule (disabled by default) if you want to be notified when one of your critical devices is down. Enable the rule only after you modify the **White List - Critical Devices** filter. For information about how to enable a rule, refer to the ["Enabling Rules" on page 12](#)
- To create a case when the **Critical Device Not Reporting** rule conditions are met, edit the Create New Case action to provide an owner and enable the action. See ["Configuring Notifications and Cases" on page 13](#)
- Enable the notification action for the **Critical Device Not Reporting** rule, if appropriate for your organization. For information about how to enable notification actions, see the *ArcSight Console User's Guide*.

Device Monitoring Resources

The following table lists all the resources in the Device Monitoring use case.

Resources that Support the Device Monitoring Use Case

Resource	Description	Type	URI
Monitor Resources			
Device Status	This dashboard displays the Device Status Monitor and Device Status Log (Throughput) data monitors, and provides an overview of the devices, their status, and how much they are reporting.	Dashboard	ArcSight Administration/Connectors/System Health/
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.	Dashboard	ArcSight Administration/Connectors/System Health/
Events by Device (Summary)	This report shows various devices and event counts for each device.	Report	ArcSight Administration/Connectors/System Health/Event Breakdown/
Connector Severity Hourly Stacked Chart	This report shows hourly event count data ordered by severity in a stacked chart.	Report	ArcSight Administration/Connectors/System Health/Event Breakdown/
Events by Connector Type (Summary)	This report shows events by connector type and the event counts for each connector type.	Report	ArcSight Administration/Connectors/System Health/Event Breakdown/
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.	Report	ArcSight Administration/Connectors/System Health/EPS/

Resources that Support the Device Monitoring Use Case, continued

Resource	Description	Type	URI
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.	Report	ArcSight Administration/Connectors/System Health/Event Breakdown/
Events by Selected Connector Type	This report shows events and their counts for a specific connector type.	Report	ArcSight Administration/Connectors/System Health/Event Breakdown/
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.	Report	ArcSight Administration/Connectors/System Health/Event Breakdown/
Event Distribution Chart for a Connector Type	This report shows the hourly distribution of events for a specific connector type.	Report	ArcSight Administration/Connectors/System Health/Event Breakdown/

Resources that Support the Device Monitoring Use Case, continued

Resource	Description	Type	URI
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.	Report	ArcSight Administration/Connectors/System Health/EPS/
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.	Report	ArcSight Administration/Connectors/System Health/Event Breakdown/
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.	Report	ArcSight Administration/Connectors/System Health/EPS/
Top Connector Types Chart	This report shows connector details with event counts for each connector type.	Report	ArcSight Administration/Connectors/System Health/Event Breakdown/

Resources that Support the Device Monitoring Use Case, continued

Resource	Description	Type	URI
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 change these default values either in the Parameters tab of the report or manually when running the report.	Report	ArcSight Administration/Connectors/System Health/Event Breakdown/
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.	Report	ArcSight Administration/Connectors/System Health/EPS/
Library - Correlation Resources			
Device Reported	This rule detects Connector device status events for devices that match the conditions in the White List - Devices filter. The rule adds (or updates) the device in the Reporting Devices active list.	Rule	ArcSight Administration/Connectors/System Health/
Critical Device Not Reporting	This rule triggers when the TTL for an entry in the Reporting Devices - Critical active list expires (30 minutes by default) and sends a notification to the SOC operators. This rule is disabled by default.	Rule	ArcSight Administration/Connectors/System Health/Custom/

Resources that Support the Device Monitoring Use Case, continued

Resource	Description	Type	URI
Critical Device Reported	This rule detects Connector Device Status events for critical devices that match the conditions in the White List - Critical Devices filter. The rule adds (or updates) the device in the Critical Reporting Devices active list.	Rule	ArcSight Administration/Connectors/System Health/Custom/
Library Resources			
Reporting Devices - Critical	This active list stores the devices that are considered critical, with the total count of events, the event count since last check, and the timestamp of the last event received by the device. The active list is updated every time the Manager receives a Connector Device Status event for that device.	Active List	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.	Active List	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.	Active List	ArcSight Administration/Connectors/System Health/EPS/
Reporting Devices	This active list stores the devices with the total count of events, the event count since last check, and the timestamp of the last event received by the device. The active list is updated every time the Manager receives a Connector Device Status event for that device.	Active List	ArcSight Administration/Connectors/System Health/
High	This is a system asset category.	Asset Category	System Asset Categories/Criticality

Resources that Support the Device Monitoring Use Case, continued

Resource	Description	Type	URI
Top Event Sources	This data monitor shows the most common event generating products and displays a listing of the top 20.	Data Monitor	ArcSight Administration/Connectors/System Health/Current Event Sources/
Critical Devices - Heads Up Display	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).	Data Monitor	ArcSight Administration/Connectors/System Health/Device Status/
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.	Field Set	ArcSight System/Event Field Sets/Active Channels
Critical Device Not Reporting	This filter identifies Critical Device Not Reporting rule events. The filter is used by a conditionalEvaluation variable in the Critical Devices - Heads Up Display data monitor.	Filter	ArcSight Administration/Connectors/System Health/Conditional Variable Filters/
White List - Critical Devices	This filter identifies the list of devices that are considered critical and are stored in the Reporting Devices - Critical active list.	Filter	ArcSight Administration/Connectors/System Health/Custom/
All Events	This filter matches all events.	Filter	ArcSight System/Core
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.	Filter	ArcSight System/Event Types

Resources that Support the Device Monitoring Use Case, continued

Resource	Description	Type	URI
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types
White List - Devices	This filter defines the list of devices that are stored in the Reporting Devices active list.	Filter	ArcSight Administration/Connectors/System Health/Custom/
Critical Devices Up Down	This filter identifies Critical Device Reported and Critical Device Not Reporting correlation events.	Filter	ArcSight Administration/Connectors/System Health/
Low Volume Connector EPS - By Day	This query defines the daily average EPS for low volume connectors from a trend.	Query	ArcSight Administration/Connectors/System Health/EPS/
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.	Query	ArcSight Administration/Connectors/System Health/Event Breakdown/

Resources that Support the Device Monitoring Use Case, continued

Resource	Description	Type	URI
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.	Query	ArcSight Administration/Connectors/System Health/Event Breakdown/
Events by Device (Summary)	This query retrieves the various devices and event counts for each device.	Query	ArcSight Administration/Connectors/System Health/Event Breakdown/
Connector Monitor Event	This query identifies the total number of events that connectors forward to the ArcSight Manager per hour.	Query	ArcSight Administration/Connectors/System Health/EPS/
Event Distribution Chart for a Connector Type	This query retrieves the hourly distribution of events for a specific connector type.	Query	ArcSight Administration/Connectors/System Health/Event Breakdown/
High Volume Connector EPS - By Day	This query identifies the daily average EPS for high volume connectors from a trend.	Query	ArcSight Administration/Connectors/System Health/EPS/

Resources that Support the Device Monitoring Use Case, continued

Resource	Description	Type	URI
Events by Selected Connector Type	This query retrieves events and their counts for a specific connector type.	Query	ArcSight Administration/Connectors/System Health/Event Breakdown/
Low Volume Connector EPS - Hourly	This query defines the hourly average EPS for low volume connectors from a trend.	Query	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.	Query	ArcSight Administration/Connectors/System Health/EPS/
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.	Query	ArcSight Administration/Connectors/System Health/Event Breakdown/
Connector Average EPS - Last 7 Days	This query identifies the average EPS for all connectors during the last seven days from a trend.	Query	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.	Query	ArcSight Administration/Connectors/System Health/EPS/

Resources that Support the Device Monitoring Use Case, continued

Resource	Description	Type	URI
Events by Connector Type (Summary)	This query retrieves details about various connectors and event counts for each connector.	Query	ArcSight Administration/Connectors/System Health/Event Breakdown/
Connector Severity Hourly Stacked Chart	This query replaces the Agent Severity Hourly Stacked Chart Query.	Query	ArcSight Administration/Connectors/System Health/Event Breakdown/
Top Connector Types Chart	This query retrieves connector details with event counts for each connector type.	Query	ArcSight Administration/Connectors/System Health/Event Breakdown/
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.	Query	ArcSight Administration/Connectors/System Health/Event Breakdown/
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	ArcSight System/1 Table
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	ArcSight System/1 Chart/Without Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table
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.	Trend	ArcSight Administration/Connector/System Health/EPS/

Resources that Support the Device Monitoring Use Case, continued

Resource	Description	Type	URI
Connector Total Events - Hourly	This trend stores the hourly average EPS for all connectors.	Trend	ArcSight Administration/Connector/System Health/EPS/
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.	Trend	ArcSight Administration/Connector/System Health/EPS/

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:

- 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.

To enable DSM on a connector:

- 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. HP recommends that you set DSM to ten minutes or more; for example, 600000.

- c. Restart the connector.
- 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.

- 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.
- 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

This section highlights some key features of the ArcSight ESM Device Monitoring use case. Follow the steps below to get started.

To see device status events and details about all known devices:

1. Click the **Resources** tab in the Navigator panel and open the **ArcSight ESM Device Monitoring** active channel located in:

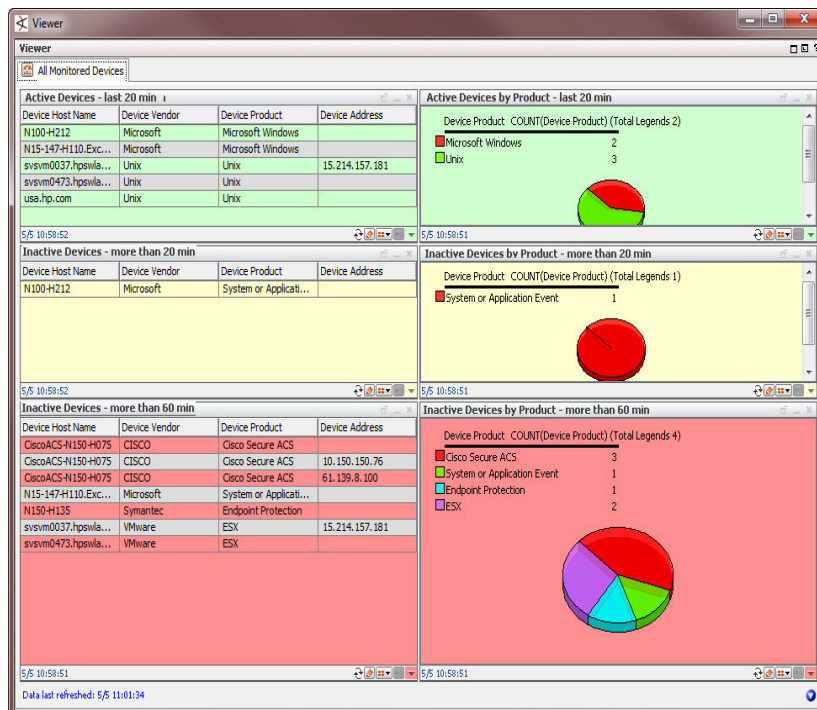
All Active Channels/ArcSight Administration/Devices

This active channel shows Device Status events. Double-click an event to see details about the event in the Event Inspector.

- Click the **Use Cases** tab in the Navigator panel and open the **ArcSight ESM Device Monitoring** use case located in:

All Use Cases/ArcSight Administration/Devices


- Click the **All Monitored Devices** hyperlink to open the dashboard. A sample is shown below.

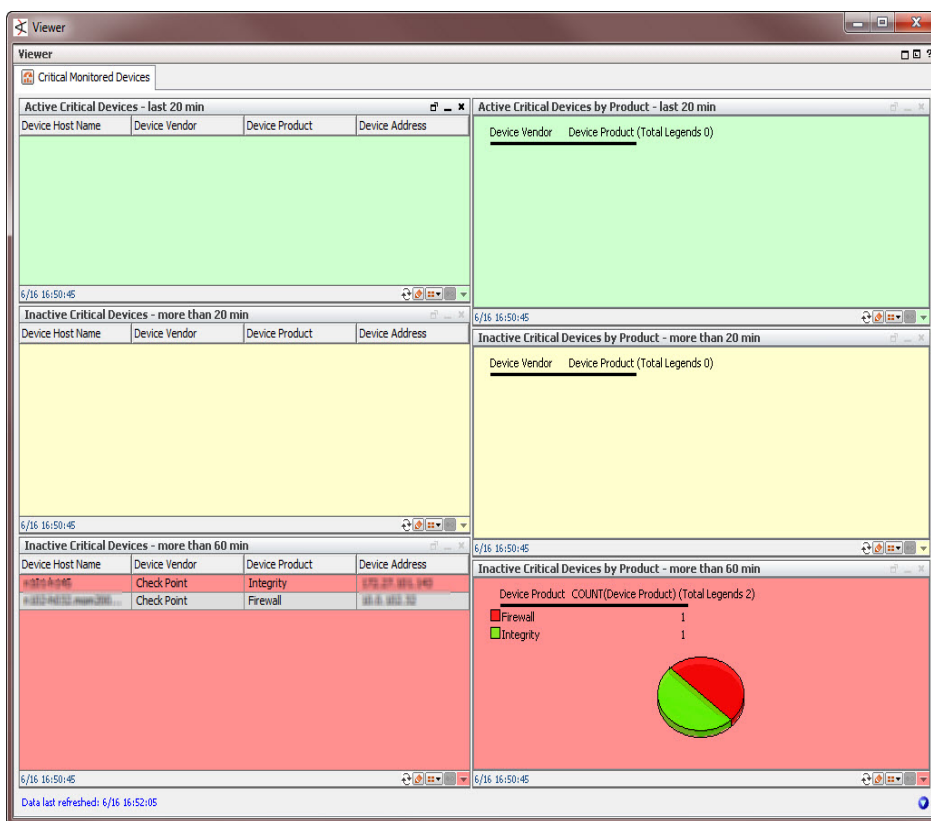


This dashboard shows information about all known devices (all the devices in the **All Monitored Devices** active list). The dashboard panels are color coded so you can identify problems quickly.

- The **Active Devices - last 20 min** panel displays information about devices that have reported events within the last 20 minutes. The **Active Devices by Product - last 20 min** panel 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** panel 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** panel 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** panel displays information about devices that have not reported events within the last 60 minutes. The **Inactive Devices by Product - more than 60 min** panel 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** panels, 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.

4. Drill down to see details about an event on the dashboard, such as the Agent Name, Event Count SLC, Creation Time, and so on:
 - a. If the panel view is a pie chart, change the panel view from a pie chart to a table (click the **View as** button  on the bottom right of the panel).
 - b. Right click an event in the panel and select **Drilldown > Show device details for selected Device Product**.
5. In the **ArcSight ESM Device Monitoring** use case, click the ["Critical Monitored Devices"](#) hyperlink to open the dashboard. A sample is shown below.



This dashboard shows an overview of your critical devices (the devices in the **Critical Monitored Devices** active list).

- The **Active Critical Devices - last 20 min** panel displays information about critical devices that have reported events within the last 20 minutes. The **Active Critical Devices by Product - last 20 min** panel 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** panel 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** panel 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** panel 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** panel 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** panels, 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.

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 ["To run reports for long-term monitoring:" below](#).

To run reports for long-term monitoring:

You can run the following reports for longer-term activity and inactivity monitoring (from one to a few days):

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

- 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.

ArcSight ESM Device Monitoring Resources

The following table lists all the resources in the ArcSight ESM Device Monitoring use case.

Resources that Support the ArcSight ESM Device Monitoring Use Case

Resource	Description	Type	URI
Monitor Resources			
ArcSight ESM Device Monitoring	This active channel shows device status events.	Active Channel	ArcSight Administration/Devices/
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.	Dashboard	ArcSight Administration/Devices/
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.	Dashboard	ArcSight Administration/Devices/

Resources that Support the ArcSight ESM Device Monitoring Use Case, continued

Resource	Description	Type	URI
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.	Query Viewer	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Inactive Critical Devices - more than 60 min	This query viewer displays details for the critical devices detected as inactive for more than 60 minutes.	Query Viewer	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Critical Monitored Devices	This query viewer displays details for all critical devices.	Query Viewer	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.	Query Viewer	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Active Critical Devices - last 20 min	This query viewer displays details for the critical devices detected as active for the last 20 minutes.	Query Viewer	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
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.	Query Viewer	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Inactive Devices - more than 60 min	This query viewer displays details for the devices detected as inactive for more than 60 minutes.	Query Viewer	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
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.	Query Viewer	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/

Resources that Support the ArcSight ESM Device Monitoring Use Case, continued

Resource	Description	Type	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.	Query Viewer	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
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.	Query Viewer	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.	Query Viewer	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
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.	Query Viewer	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
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.	Query Viewer	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices	This query viewer displays details for the devices detected within the last 365 days.	Query Viewer	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Critical Devices Detected Inactive - Last 7 Days	This report shows critical devices detected as inactive within the last seven days.	Report	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/

Resources that Support the ArcSight ESM Device Monitoring Use Case, continued

Resource	Description	Type	URI
All Devices Detected Inactive - Last 24 Hours	This report shows all devices detected as inactive within the last 24 hours.	Report	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.	Report	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.	Report	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
New Devices Detected - Last 24 Hours	This report shows new devices detected within the last 24 hours.	Report	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices	This report shows all devices detected within the last 365 days.	Report	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Critical Devices Detected Inactive - Last 24 Hours	This report shows critical devices detected as inactive within the last 24 hours.	Report	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Critical Monitored Devices	This report shows all critical devices currently being monitored.	Report	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Library - Correlation Resources			

Resources that Support the ArcSight ESM Device Monitoring Use Case, continued

Resource	Description	Type	URI
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.	Rule	ArcSight Administration/Devices/
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.	Rule	ArcSight Administration/Devices/
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.	Rule	ArcSight Administration/Devices/
Library Resources			
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.	Active List	ArcSight Administration/Devices/

Resources that Support the ArcSight ESM Device Monitoring Use Case, continued

Resource	Description	Type	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.	Active List	ArcSight Administration/Devices/
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.	Active List	ArcSight Administration/Devices/
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.	Active List	ArcSight Administration/Devices/
ArcSight ESM Device Monitoring	This field set contains fields used to examine device status events.	Field Set	ArcSight Administration/Devices/
Critical Devices Detected Inactive - Last 24 Hours	This query retrieves critical devices detected as inactive within the last 24 hours.	Query	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.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
All Monitored Devices - Yellow	This query retrieves devices detected as inactive for more than 20 minutes but less than 60 minutes.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/

Resources that Support the ArcSight ESM Device Monitoring Use Case, continued

Resource	Description	Type	URI
All Devices Detected Inactive - Last 7 Days	This query retrieves devices detected as inactive within the last seven days.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
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.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
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.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Critical Monitored Devices - Red Counter	This query retrieves critical devices detected as inactive for more than 60 minutes and sorts them by device product.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
New Devices Detected - Last 7 Days	This query retrieves all new devices detected within the last seven days.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Critical Monitored Devices	This query retrieves critical devices from the Critical Monitored Devices active list.	Query	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.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
All Monitored Devices - Green	This query retrieves devices detected as active within the last 20 minutes.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/

Resources that Support the ArcSight ESM Device Monitoring Use Case, continued

Resource	Description	Type	URI
New Devices Detected - Last 24 Hours	This query retrieves all new devices detected within the last 24 hours.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices - Green Counter	This query retrieves devices detected as active within the last 20 minutes and sorts them by device product.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices	This query retrieves devices from the All Monitored Devices active list.	Query	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.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Critical Devices Detected Inactive - Last 7 Days	This query retrieves critical devices detected as inactive within the last seven days.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
All Devices Detected Inactive - Last 24 Hours	This query retrieves devices detected as inactive within the last 24 hours.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Critical Monitored Devices - Green Counter	This query retrieves critical devices detected as active within the last 20 minutes and sorts them by product.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
All Monitored Devices - Red	This query retrieves devices detected as inactive for more than 60 minutes.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/

Resources that Support the ArcSight ESM Device Monitoring Use Case, continued

Resource	Description	Type	URI
Critical Monitored Devices - Green	This query retrieves critical devices detected as active within the last 20 minutes.	Query	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table

ESM Licensing

The ESM Licensing use case provides information about licensing compliance.

ESM Licensing Resources

The following table lists all the resources in the ESM Licensing use case.

Resources that Support the ESM Licensing Use Case

Resource	Description	Type	URI
Monitor Resources			
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.	Report	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.	Report	ArcSight Administration/ESM/Licensing/

Resources that Support the ESM Licensing Use Case, continued

Resource	Description	Type	URI
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.	Report	ArcSight Administration/ESM/Licensing/
Library - Correlation Resources			
Storage Licensing Audit event Detected	This rule detects connector raw event statistic events and stores them in an active list.	Rule	ArcSight Administration/ESM/Licensing/
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.	Rule	ArcSight Administration/ESM/Licensing/
Library Resources			

Resources that Support the ESM Licensing Use Case, continued

Resource	Description	Type	URI
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.	Active List	ArcSight Administration/Connectors/System Health/
Storage Licensing Data by Connector	This active list stores the raw event length reported by the raw event statistics events for each connector.	Active List	ArcSight Administration/ESM/Licensing/
admincert	This destination is pre-defined for the CERT team. Add more information, such as email addresses.	Destination	CERT Team/1
ConnectorName	This variable returns the name of the connector.	Global Variable	ArcSight Administration/ESM/Licensing/

Resources that Support the ESM Licensing Use Case, continued

Resource	Description	Type	URI
ConnectorID	This variable returns the Resource ID of the connector.	Global Variable	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.	Global Variable	ArcSight Administration/ESM/Licensing/
ConnectorType	This variable returns the type of connector.	Global Variable	ArcSight Administration/ESM/Licensing/
Assets Licensing Report	This report shows the licensing history for assets. A chart shows the current count and the count limit. By default, the licensing history is over the last seven days.	Focused Report	ArcSight Administration/ESM/Licensing/
Console Users Licensing Report	This report shows the licensing history for console users. A chart shows the current count and the count limit. By default, the licensing history is over the last seven days.	Focused Report	ArcSight Administration/ESM/Licensing/

Resources that Support the ESM Licensing Use Case, continued

Resource	Description	Type	URI
Web Users Licensing Report	This report shows the licensing history for web users. A chart shows the current count and the count limit. By default, the licensing history is over the last seven days.	Focused Report	ArcSight Administration/ESM/Licensing/
Actors Licensing Report	This report shows the licensing history for actors. A chart shows the current count and the count limit. By default, the licensing history is over the last seven days.	Focused Report	ArcSight Administration/ESM/Licensing/
Devices Licensing Report	This report shows the licensing history for devices. A chart shows the current count and the count limit. By default, the licensing history is over the last seven days.	Focused Report	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.	Query	ArcSight Administration/ESM/Licensing/

Resources that Support the ESM Licensing Use Case, continued

Resource	Description	Type	URI
Storage Licensing Data - trend	This query selects the raw event length for each day for all the connectors from a trend.	Query	ArcSight Administration/ESM/Licensing/
Licensing Query	This query retrieves the licensing history for the various license types taken from the License History session list.	Query	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.	Query	ArcSight Administration/ESM/Licensing/
Storage Licensing Data	This query selects the raw event length for each day for all the connectors from an active list.	Query	ArcSight Administration/ESM/Licensing/
Chart and 2 Tables Portrait	This template is designed to show one chart and two tables. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With 2 Tables
Licensing Report	This report template is used by the licensing reports and shows one chart (bar and line). The orientation is landscape.	Report Template	ArcSight Administration/Licensing/

Resources that Support the ESM Licensing Use Case, continued

Resource	Description	Type	URI
Licensing Report (All)	This report template is used by the licensing reports and shows several charts (bar and line). The orientation is portrait.	Report Template	ArcSight Administration/Licensing/
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.	Session List	ArcSight Administration/ESM/Licensing/
Storage Licensing Data	This trend stores the raw event length reported by the raw event statistic events for each connector.	Trend	ArcSight Administration/ESM/Licensing/

ESM User Sessions

The ESM User Sessions use case provides information about user access to the ArcSight system.

ESM User Sessions Resources

The following table lists all the resources in the ESM User Sessions use case.

Resources that Support the ESM User Sessions Use Case

Resource	Description	Type	URI
Monitor Resources			
Console and ArcSight Web Status	This dashboard shows login session information and notification activity for ArcSight ESM users.	Dashboard	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.	Dashboard	ArcSight Administration/ESM/User Access/User Sessions/
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.	Report	ArcSight Administration/ESM/User Access/User Sessions/
User Login Logout Report	This report shows user login events (success and fail) and logout events.	Report	ArcSight Administration/ESM/User Access/User Sessions/
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.	Report	ArcSight Administration/ESM/User Access/User Sessions/
Library - Correlation Resources			

Resources that Support the ESM User Sessions Use Case, continued

Resource	Description	Type	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.	Rule	ArcSight Administration/ESM/User Access/User Sessions/
ArcSight User Login	This rule detects ArcSight user login events. This rule adds the user information to the ArcSight User Sessions session list.	Rule	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.	Rule	ArcSight Administration/ESM/User Access/User Sessions/
Library Resources			
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.	Data Monitor	ArcSight Administration/ESM/User Access/User Sessions/Console and ArcSight Web Status/
Current Users Logged In	This data monitor shows information about the users currently logged into the ArcSight ESM system.	Data Monitor	ArcSight Administration/ESM/User Access/User Sessions/Console and ArcSight Web 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.	Data Monitor	ArcSight Administration/ESM/User Access/User Sessions/Console and ArcSight Web Status/
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.	Data Monitor	ArcSight Administration/ESM/User Access/User Sessions/ArcSight User Status/

Resources that Support the ESM User Sessions Use Case, continued

Resource	Description	Type	URI
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.	Filter	ArcSight Administration/ESM/User Access/User Sessions/
Notification Actions	This filter selects events that are related to notifications generated by a rule in the ArcSight ESM system.	Filter	ArcSight Administration/ESM/System Health/Events/Event Flow/
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.	Filter	ArcSight Administration/ESM/User Access/User Sessions/
All Events	This filter matches all events.	Filter	ArcSight System/Core
ArcSight Login Events	This filter selects events that are associated with logins to the ArcSight ESM system.	Filter	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.	Query	ArcSight Administration/ESM/User Access/User Sessions/
User Login Logout Report	This query retrieves user login (success/fail) and logout events.	Query	ArcSight Administration/ESM/User Access/User Sessions/
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.	Query	ArcSight Administration/ESM/User Access/User Sessions/
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table

Resources that Support the ESM User Sessions Use Case, continued

Resource	Description	Type	URI
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	ArcSight System/1 Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table
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.	Session List	ArcSight Administration/ESM/User Access/User Sessions/
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.	Trend	ArcSight Administration/ESM/User Access/

Actor Configuration Changes

The Actor Configuration Changes use case provides information about changes to the actor resources.

Actor Configuration Changes Resources

The following table lists all the resources in the Actor Configuration Changes use case.

Resources that Support the Actor Configuration Changes Use Case

Resource	Description	Type	URI
Monitor Resources			
Actor Audit Events	This active channel displays events in which there are changes to data in the actor resources.	Active Channel	ArcSight Administration/ESM/Configuration Changes/Actors/
Actor Administration	This dashboard shows the Actor Authenticators query viewer.	Dashboard	ArcSight Administration/ESM/Configuration Changes/Actors/
Actor Change Log	This dashboard shows an overview of actor resource changes.	Dashboard	ArcSight Administration/ESM/Configuration Changes/Actors/
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.	Query Viewer	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.	Query Viewer	ArcSight Administration/ESM/Configuration Changes/Actor/

Resources that Support the Actor Configuration Changes Use Case, continued

Resource	Description	Type	URI
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.	Query Viewer	ArcSight Administration/ESM/Configuration Changes/Actor/
Actor Authenticators	This query viewer displays a list of all the authenticators for actors.	Query Viewer	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.	Query Viewer	ArcSight Administration/ESM/Configuration Changes/Actor/
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.	Query Viewer	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.	Query Viewer	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.	Query Viewer	ArcSight Administration/ESM/Configuration Changes/Actor/

Resources that Support the Actor Configuration Changes Use Case, continued

Resource	Description	Type	URI
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.	Query Viewer	ArcSight Administration/ESM/Configuration Changes/Actor/
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.	Report	ArcSight Administration/ESM/Configuration Changes/Actors/
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.	Report	ArcSight Administration/ESM/Configuration Changes/Actors/
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.	Report	ArcSight Administration/ESM/Configuration Changes/Actors/
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.	Report	ArcSight Administration/ESM/Configuration Changes/Actors/
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.	Report	ArcSight Administration/ESM/Configuration Changes/Actors/

Resources that Support the Actor Configuration Changes Use Case, continued

Resource	Description	Type	URI
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.	Report	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.	Report	ArcSight Administration/ESM/Configuration Changes/Actors/
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.	Report	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.	Report	ArcSight Administration/ESM/Configuration Changes/Actors/
Library Resources			
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.	Data Monitor	ArcSight Administration/ESM/Configuration Changes/Actors/Actor Change Log/
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.	Data Monitor	ArcSight Administration/ESM/Configuration Changes/Actors/Actor Change Log/

Resources that Support the Actor Configuration Changes Use Case, continued

Resource	Description	Type	URI
Department New Value	This global variable extracts the new value for Department in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/
DN New Value	This global variable extracts the new value for DN (Distinguished Name) in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/
Full Name New Value	This global variable extracts the new value for Full Name in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/
Org New Value	This global variable extracts the new value for Org in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/
Title New Value	This global variable extracts the new value for Title in actor update audit events (single-value parameters).	Global Variable	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.	Global Variable	ArcSight Administration/ESM/Actor/
Location Old Value	This global variable extracts the old value for Location in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/
Change Source	This field returns the source of the change that modified the actor resource.	Global Variable	ArcSight Administration/ESM/Actor/
Manager New Value	This global variable extracts the new value for Manager in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/
Actor	This field returns the actor name.	Global Variable	ArcSight Administration/ESM/Actor/

Resources that Support the Actor Configuration Changes Use Case, continued

Resource	Description	Type	URI
Employee Type Old Value	This global variable extracts the old value for Employee Type in actor update audit events (single-value parameters).	Global Variable	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).	Global Variable	ArcSight Administration/ESM/Actor/
Location New Value	This global variable extracts the new value for Location in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/
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 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	Global Variable	ArcSight Foundation/Variables Library/Host Information
Manager Old Value	This global variable extracts the old value for Manager in actor update audit events (single-value parameters).	Global Variable	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).	Global Variable	ArcSight Administration/ESM/Actor/

Resources that Support the Actor Configuration Changes Use Case, continued

Resource	Description	Type	URI
Status New Value	This global variable extracts the new value for Status in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/
Email Address New Value	This global variable extracts the new value for Email Address in actor update audit events (single-value parameters).	Global Variable	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).	Global Variable	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).	Global Variable	ArcSight Administration/ESM/Actor/
Status Old Value	This global variable extracts the old value for Status in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/
Org Old Value	This global variable extracts the old value for Org in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/
Title Old Value	This global variable extracts the old value for Title in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/
Department Old Value	This global variable extracts the old value for Department in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/
Actor Audit Field Set	This field set contains fields of interest for monitoring changes to actor resources.	Field Set	ArcSight Administration/ESM/Actor/

Resources that Support the Actor Configuration Changes Use Case, continued

Resource	Description	Type	URI
Attacker Information is NULL	This filter identifies events in which the attacker zone, attacker host name, and attacker address fields are NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host
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.	Filter	ArcSight Administration/ESM/Configuration Changes/Actor Update Tracking/
All Events	This filter matches all events.	Filter	ArcSight System/Core
Attacker Zone OR Host is NULL	This filter identifies events in which either the attacker zone or attacker host name field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host
Attacker Zone is NULL	This filter identifies events in which the attacker zone field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host
Attacker Port is NULL	This variable identifies events in which the attacker port field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host
Actor Deletes	This filter detects deleted actor resources. Note: This filter only detects deleted actor events and ignores deleted entries for multi-value parameters.	Filter	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.	Filter	ArcSight Administration/ESM/Configuration Changes/Actor Update Tracking/

Resources that Support the Actor Configuration Changes Use Case, continued

Resource	Description	Type	URI
Actor Inserts	This filter detects new actor resources. Note: This filter searches for new actors only and ignores new entries for multi-value parameters.	Filter	ArcSight Administration/ESM/Configuration Changes/Actor Update Tracking/
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.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host
Attacker Zone AND Host are NULL	This filter identifies events in which the attacker zone and attacker address fields are NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host
Attacker Host Name is NULL	This filter is used by variables to identify events in which the attacker host name field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host
Target User Name is NULL	This filter identifies events where the Target User Name is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/User
Attacker Address is NULL	This variable identifies events in which the attacker address field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host
Actor Changes	This filter detects actor resource audit events.	Filter	ArcSight Administration/ESM/Configuration Changes/Actor Update Tracking/
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.	Query	ArcSight Administration/ESM/Configuration Changes/Actors/
Actor Authenticators	This query identifies all the authenticators for actors.	Query	ArcSight Administration/ESM/Configuration Changes/Actors/

Resources that Support the Actor Configuration Changes Use Case, continued

Resource	Description	Type	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.	Query	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.	Query	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.	Query	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.	Query	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.	Query	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.	Query	ArcSight Administration/ESM/Configuration Changes/Actors/

Resources that Support the Actor Configuration Changes Use Case, continued

Resource	Description	Type	URI
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.	Query	ArcSight Administration/ESM/Configuration Changes/Actors/
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table

ESM Resource Configuration Changes

The ESM Resource Configuration Changes use case provides information about changes to the various resources, such as rules, reports, and so on.

ESM Resource Configuration Changes Resources

The following table lists all the resources in the ESM Resource Configuration Changes use case.

Resources that Support the ESM Resource Configuration Changes Use Case

Resource	Description	Type	URI
Monitor Resources			
Resource Change Log	This dashboard shows the changes (add, update, delete) to content resources and detailed information about logs associated with those actions.	Dashboard	ArcSight Administration/ESM/Configuration Changes/Resources/
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.	Report	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.	Report	ArcSight Administration/ESM/Configuration Changes/Resources/

Resources that Support the ESM Resource Configuration Changes Use Case, continued

Resource	Description	Type	URI
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.	Report	ArcSight Administration/ESM/Configuration Changes/Resources/
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.	Report	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.	Report	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.	Report	ArcSight Administration/ESM/Configuration Changes/Resources/
Library Resources			
Recent System Resource Inserts	This data monitor does not populate all values when running in Turbo Mode Fastest.	Data Monitor	ArcSight Administration/ESM/Configuration Changes/Resources/
Recent System Resource Updates	This data monitor does not populate all values when running in Turbo Mode Fastest.	Data Monitor	ArcSight Administration/ESM/Configuration Changes/Resources/

Resources that Support the ESM Resource Configuration Changes Use Case, continued

Resource	Description	Type	URI
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).	Data Monitor	ArcSight Administration/ESM/Configuration Changes/Resources/Resource Change Log/
Recent System Resource Deletes	This data monitor does not populate all values when running in Turbo Mode Fastest.	Data Monitor	ArcSight Administration/ESM/Configuration Changes/Resources/
Resource Change Log	This data monitor does not populate all values when running in Turbo Mode Fastest.	Data Monitor	ArcSight Administration/ESM/Configuration Changes/Resources/Resource Change Log/
Resource Inserts	This filter detects new resources.	Filter	ArcSight Administration/ESM/Configuration Changes/Resource Update Tracking/
Resource Updates	This filter detects updates to resources.	Filter	ArcSight Administration/ESM/Configuration Changes/Resource Update Tracking/
Resource Deletes	This filter detects deleted resources.	Filter	ArcSight Administration/ESM/Configuration Changes/Resource Update Tracking/
Target User Name is NULL	This filter identifies events where the Target User Name is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/User
Resource Changes	This filter detects resource change audit events.	Filter	ArcSight Administration/ESM/Configuration Changes/Resource Update Tracking/
All Events	This filter matches all events.	Filter	ArcSight System/Core
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.	Query	ArcSight Administration/ESM/Configuration Changes/Resources/

Resources that Support the ESM Resource Configuration Changes Use Case, continued

Resource	Description	Type	URI
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.	Query	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.	Query	ArcSight Administration/ESM/Configuration Changes/Resources/
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.	Query	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.	Query	ArcSight Administration/ESM/Configuration Changes/Resources/
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	ArcSight System/1 Table

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. Refer to ["Installing and Configuring the Content" on page 10](#).

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. See ["Enabling Rules" on page 12](#).

Content Management Resources

The following table lists all the resources in the Content Management use case.

Resources that Support the Content Management Use Case

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

Resources that Support the Content Management Use Case, continued

Resource	Description	Type	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.	Query Viewer	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.	Report	ArcSight Administration/ESM/Content Management/
Synchronization Status History	This report shows information about the history of content packages synchronized across peered ArcSight Managers or subscribers.	Report	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.	Report	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.	Report	ArcSight Administration/ESM/Content Management/
Library - Correlation Resources			
Content Management Data	This rule maintains list information for the Content Management feature.	Rule	ArcSight Administration/ESM/Content Management/
Library Resources			
Content Management History	This active list stores data about Content Management activity.	Active List	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.	Query	ArcSight Administration/ESM/Content Management/

Resources that Support the Content Management Use Case, continued

Resource	Description	Type	URI
Top Subscribers with Errors	This query selects information about the subscribers experiencing the most issues with managed package delivery or installation.	Query	ArcSight Administration/ESM/Content Management/
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.	Query	ArcSight Administration/ESM/Content Management/
Three Charts Landscape	This template is designed to show three charts and a description field. The orientation is landscape.	Report Template	ArcSight System/3 Charts/Without Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table

HA Monitoring

The 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 ArcSight Administration/ESM/HA Monitoring/**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

This section describes the key features of the HA Monitoring use case.

To view HA status events and see an overview of the HA state:

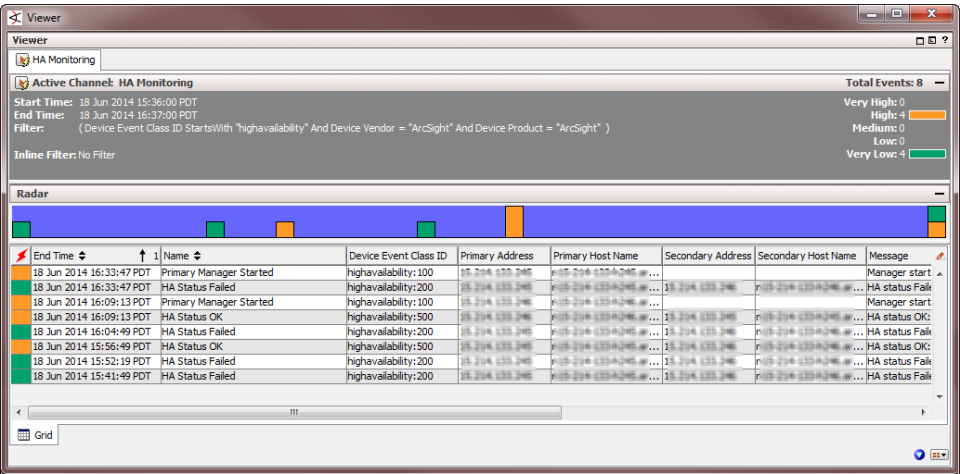
1. Click the **Uses Cases** tab in the Navigator panel and open the **HA Monitoring** use case located in:

All Use Cases/ArcSight Administration/ESM/HA Monitoring

2. Click the **HA Monitoring** active channel to open the display and see HA status events, such as when the Primary Manager started, when HA failed, and when HA returned to an OK state.

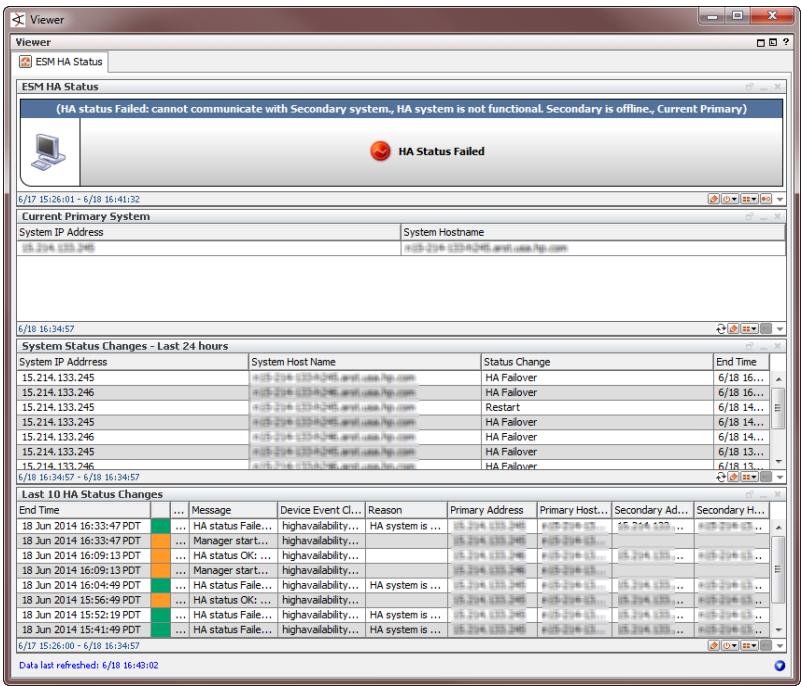
The active channel shows detailed information about the HA audit events generated by the ArcSight Manager, such as the Device Event Class ID, the Event Name, the Event Message, and other information. The IP address and hostname of both the Primary System and Secondary System are also shown. See ["HA Monitoring Audit Events" on page 145](#) 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.

- 3. In the **HA Monitoring** use case, click the **ESM HA Status** hyperlink to open the dashboard. An example is shown below.



The **ESM HA Status** dashboard shows an overview of the ArcSight ESM High Availability (HA) state. The dashboard panels are described below.

- The **ESM HA Status** panel 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 panel.

Tip: To find out details about the current Primary System, such as the system hostname, IP address, and start time, click the panel heading. When the panel heading changes color, right click anywhere in the panel 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 panel 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** panel on the **ESM HA Status** dashboard and provides a description for each, including general troubleshooting tips. "[HA Monitoring Audit Events](#)" on [page 145](#) 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	<p>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.</p> <p>Investigate the failure. Possible causes are:</p> <ul style="list-style-type: none"> ◦ 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	<p>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.</p>
HA Status Unknown	<p>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:</p> <ul style="list-style-type: none"> ◦ 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.

ESM HA Status	Description
DRBD Sync in Progress	<p>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.</p> <p>Note: This status is typically short. The system detects the HA status as soon as the Primary System starts up.</p>
iPDU status Failed	<p>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.</p>

- The **Current Primary System** panel on the dashboard 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** panel on the dashboard shows System changes, such as restarts and failovers, within the last 24 hours.
- The **Last 10 HA Status Changes** panel on the dashboard 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.

To run the ESM HA Status Updates 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.

- From the **Uses Cases** tab in the Navigator panel, open the **HA Monitoring** use case, then click the **ESM HA Status - last 7 days** link. When the Report Parameters dialog opens, modify the parameters if necessary, then click **OK**.
- From the **ESM HA Status** panel of the **ESM HA Status** dashboard, right click the panel heading and select **Drilldown > ESM HA Status - last 7 days**.

HA Monitoring Resources

The following table lists all the resources in the HA Monitoring use case.

Resources that Support the HA Monitoring Use Case

Resource	Description	Type	URI
Monitor Resources			
HA Monitoring	This active channel shows HA status events.	Active Channel	ArcSight Administration/ESM/HA Monitoring
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 within the last 24 hours. The bottom panel shows the last ten HA status changes.	Dashboard	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.	Query Viewer	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.	Query Viewer	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.	Query Viewer	ArcSight Administration/ESM/HA Monitoring
Current Primary System	This query viewer displays details for the current Primary System.	Query Viewer	ArcSight Administration/ESM/HA Monitoring
ESM HA Status Updates - last 7 days	This report shows all HA status updates within the last seven days.	Report	ArcSight Administration/ESM/HA Monitoring
Library - Correlation Resources			

Resources that Support the HA Monitoring Use Case, continued

Resource	Description	Type	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.	Rule	ArcSight Administration/ESM/HA Monitoring
ESM System Started	This rule triggers when a Primary System starts up; for example, the Arcsight 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.	Rule	ArcSight Administration/ESM/HA Monitoring
Library Resources			
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.	Active List	ArcSight Administration/ESM/HA Monitoring
Last 10 HA Status Changes	This data monitor shows the last ten HA status changes.	Data Monitor	ArcSight Administration/ESM/HA Monitoring
ESM HA Status	This data monitor shows the current ESM HA status.	Data Monitor	ArcSight Administration/ESM/HA Monitoring
HA Management	This field set contains fields used to examine HA status events.	Field Set	ArcSight Administration/ESM/HA Monitoring
ESM HA Status	This filter detects events generated by the HA module.	Filter	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. The query is used for the query viewer, which is in turn used in the dashboard drilldown.	Query	ArcSight Administration/ESM/HA Monitoring
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.	Query	ArcSight Administration/ESM/HA Monitoring

Resources that Support the HA Monitoring Use Case, continued

Resource	Description	Type	URI
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 a query viewer to populate the data in the dashboard.	Query	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.	Query	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. The query is used in the ESM HA Status Updates - last 7 days report.	Query	ArcSight Administration/ESM/HA Monitoring
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table
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 a HA failover occurs. This session list is used by a query to retrieve the system status changes, and populates the ESM HA Status dashboard.	Session List	ArcSight Administration/ESM/HA Monitoring

ESM Events

The ESM Events use case provides statistics on the flow of events through the ArcSight system.

ESM Events Resources

The following table lists all the resources in the ESM Events use case.

Resources that Support the ESM Events Use Case

Resource	Description	Type	URI
Monitor Resources			
ASM Events	This active channel shows ArcSight System Monitoring events generated by the local ArcSight ESM system.	Active Channel	ArcSight Administration/ESM/System Health/Events/
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.	Active Channel	ArcSight Administration/ESM/System Health/Events
Event Count History	This dashboard displays the total number of non-ArcSight events within the last seven days and the last 30 days.	Dashboard	ArcSight Administration/ESM/Event Analysis Overview/
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.	Dashboard	ArcSight Administration/ESM/System Health/Events/
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.	Dashboard	ArcSight Administration/ESM/Event Analysis Overview/

Resources that Support the ESM Events Use Case, continued

Resource	Description	Type	URI
Event Throughput	This dashboard displays the Event Throughput and Event Throughput Statistics data monitors, providing an overview of the system activity related to connectors.	Dashboard	ArcSight Administration/ESM/System Health/Events/
Breakdown by Event Priority From Connector	This query viewer shows the event priority within the last 24 hours by connector.	Query Viewer	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.	Query Viewer	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.	Query Viewer	ArcSight Administration/ESM/Event Analysis Overview/by Priority/
Breakdown by Device Address From Connector	This query viewer shows the top 20 devices within the last 24 hours by connector.	Query Viewer	ArcSight Administration/ESM/Event Analysis Overview/by Device Address/
Events Count Last 7 Days	This query viewer shows the total number of non-ArcSight events each day for the last seven days.	Query Viewer	ArcSight Administration/ESM/Event Analysis Overview/
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.	Query Viewer	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.	Query Viewer	ArcSight Administration/ESM/Event Analysis Overview/by Name/

Resources that Support the ESM Events Use Case, continued

Resource	Description	Type	URI
Breakdown by Event Names From Device	This query viewer shows the top 20 event names within the last 24 hours by device.	Query Viewer	ArcSight Administration/ESM/Event Analysis Overview/by Name/
Events Count Last 30 Days	This query viewer shows the total number of non-ArcSight events within the last 30 days.	Query Viewer	ArcSight Administration/ESM/Event Analysis Overview/
Event Details	This query viewer shows the event details.	Query Viewer	ArcSight Administration/ESM/Event Analysis Overview/
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.	Query Viewer	ArcSight Administration/ESM/Event Analysis Overview/by Name/
Top 10 Inbound Events	This report shows the top inbound events ordered by their counts.	Report	ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart)	This report shows the hourly distribution of events by priority rating.	Report	ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Top 10 Events	This report shows the top events ordered by their counts.	Report	ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Source Counts by Event Name	This report shows event names by source address in addition to event counts.	Report	ArcSight Administration/ESM/System Health/Events/
Event Name Counts	This report shows event names and their event counts.	Report	ArcSight Administration/ESM/System Health/Events/

Resources that Support the ESM Events Use Case, continued

Resource	Description	Type	URI
Hourly Event Counts (Area Chart)	This report shows the hourly distribution of event counts.	Report	ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Destination Counts	This report shows destination details and the sum of event counts for each destination.	Report	ArcSight Administration/ESM/System Health/Events/
Hourly Distribution Chart for Event	This report shows the hourly distribution of specific events.	Report	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.	Report	ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
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.	Report	ArcSight Administration/ESM/System Health/Events/
Event Count by Agent Severity	This report shows events by agent severity with event counts.	Report	ArcSight Administration/ESM/System Health/Events/
Hourly Distribution Chart for a Destination Port	This report shows the hourly distribution of events for destinations with a specific port.	Report	ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Event Count by Source Destination Pairs	This report shows event counts ordered by source-destination pairs.	Report	ArcSight Administration/ESM/System Health/Events/

Resources that Support the ESM Events Use Case, continued

Resource	Description	Type	URI
Top 10 Outbound Events	This report shows the top outbound events ordered by their counts.	Report	ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Library Resources			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Events By Priority	This data monitor does not populate all values when running in Turbo Mode Fastest.	Data Monitor	ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/
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).	Data Monitor	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.	Data Monitor	ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/
Events by Connector	This data monitor shows the total number of non-ArcSight events by connector.	Data Monitor	ArcSight Administration/ESM/Event Analysis Overview/Event Overview/
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.	Data Monitor	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.	Data Monitor	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.	Data Monitor	ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/

Resources that Support the ESM Events Use Case, continued

Resource	Description	Type	URI
Event Counts	This data monitor shows all non-ArcSight events	Data Monitor	ArcSight Administration/ESM/Event Analysis Overview/Event Overview/
Events by Device Address	This data monitor shows all non-ArcSight events by device address.	Data Monitor	ArcSight Administration/ESM/Event Analysis Overview/Event Overview/
Event Throughput Statistics	This data monitor shows event throughput from various connectors sending events to this ArcSight ESM.	Data Monitor	ArcSight Administration/ESM/System Health/Events/Event Throughput/
Events by Vendor and Product	This data monitor shows all non-ArcSight events by vendor and product.	Data Monitor	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.	Data Monitor	ArcSight Administration/ESM/System Health/Events/Event Throughput/
Event Base	This field set contains all the ESM event fields.	Field Set	ArcSight System/Event Field Sets
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.	Field Set	ArcSight Administration/Connector/
ASM Events	This field set contains fields of interest for monitoring ASM events.	Field Set	ArcSight Administration/ESM/
ArcSight Admin	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Active Channels
ArcSight Status Monitoring Events	This filter selects ArcSight Status Monitoring events generated by the local ArcSight ESM system.	Filter	ArcSight Administration/ESM/System Health/

Resources that Support the ESM Events Use Case, continued

Resource	Description	Type	URI
ASM Event Flow	This filter captures events that identify the ESM load through flow levels of events.	Filter	ArcSight Administration/ESM/System Health/Events/
ASM CPU Load	This filter identifies ArcSight ESM monitoring events related to CPU load.	Filter	ArcSight Administration/ESM/System Health/Resources/
ASM Database Load Statistics	This filter identifies events related to ArcSight ESM database load.	Filter	ArcSight Administration/ESM/System Health/Storage/
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
ASM Events	This filter selects ArcSight System Monitoring events generated by the local ESM system (in an hierarchical deployment).	Filter	ArcSight System/Event Types
High Threat Condition	This filter identifies events with a Priority level rating of 7 or 8.	Filter	ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
All Events	This filter matches all events.	Filter	ArcSight System/Core
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Severe Threat Condition	This filter identifies events with Priority level rating greater than 8.	Filter	ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
Inbound Events	This filter identifies events coming from the outside network targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
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.	Filter	ArcSight Administration/ESM/System Health/

Resources that Support the ESM Events Use Case, continued

Resource	Description	Type	URI
Guarded Threat Condition	This filter identifies events with a Priority level rating of 3 or 4.	Filter	ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
ASM Resource and Memory Load	This filter identifies ArcSight ESM monitoring events related to resource and memory load.	Filter	ArcSight Administration/ESM/System Health/Resources/
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Notification Actions	This filter selects events that are related to notifications generated by a rule in the ArcSight ESM system.	Filter	ArcSight Administration/ESM/System Health/Events/Event Flow/
Outbound Events	This filter identifies events originating from inside the company network, targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
Low Threat Condition	This filter identifies events with a Priority level rating less than or equal to 2.	Filter	ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
Elevated Threat Condition	This filter identifies events with a Priority level rating of 5 or 6.	Filter	ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
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.	Filter	ArcSight System/Event Types
ArcSight Internal Events	This filter selects events that are internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types

Resources that Support the ESM Events Use Case, continued

Resource	Description	Type	URI
Non-ArcSight Internal Events	This filter selects events that are not internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types
External Target	This filter identifies events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
ASM Standing Load	This filter identifies currently active, data monitor, rules, and active channel related events.	Filter	ArcSight Administration/ESM/System Health/Resources/
ArcSight Audit Events	This filter captures ArcSight ESM audit events.	Filter	ArcSight Administration/ESM/System Health/Events/Audit/
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types
ASM Flow Load	This filter identifies ArcSight ESM monitoring events related to event flow.	Filter	ArcSight Administration/ESM/System Health/Resources/
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.	Query	ArcSight Administration/ESM/Event Analysis Overview/by Device Address/
Breakdown by Event Names From Connector	This query selects the top 20 event names within the last 24 hours by connector.	Query	ArcSight Administration/ESM/Event Analysis Overview/by Event Name/
Breakdown by Device Address From Connector	This query selects the top 20 devices within the last 24 hours by connector.	Query	ArcSight Administration/ESM/Event Analysis Overview/by Device Address/
Top 10 Events	This query retrieves the top events ordered by their counts.	Query	ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/

Resources that Support the ESM Events Use Case, continued

Resource	Description	Type	URI
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.	Query	ArcSight Administration/ESM/Event Analysis Overview/by Event Name/
Event Count by Agent Severity	This query retrieves events by agent severity with event counts.	Query	ArcSight Administration/ESM/System Health/Events/
Destination Counts	This query retrieves destination details and the sum of event counts for each destination.	Query	ArcSight Administration/ESM/System Health/Events/
Breakdown by Event Priority From Device	This query selects the event priority within the last 24 hours by device.	Query	ArcSight Administration/ESM/Event Analysis Overview/by Priority/
Source Counts by Event Name	This query retrieves event names by source address in addition to event counts.	Query	ArcSight Administration/ESM/System Health/Events/
Top 10 Outbound Events	This query retrieves the top outbound events ordered by their counts.	Query	ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Event Count by Source Destination Pairs	This query retrieves event counts ordered by source-destination pairs.	Query	ArcSight Administration/ESM/System Health/Events/
Top 10 Inbound Events	This query retrieves the top inbound events ordered by their counts.	Query	ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Breakdown by Event Priority From Connector	This query selects the event priority within the last 24 hours by connector.	Query	ArcSight Administration/ESM/Event Analysis Overview/by Priority/

Resources that Support the ESM Events Use Case, continued

Resource	Description	Type	URI
Breakdown by Event Names From Device	This query selects the top 20 event names within the last 24 hours by device.	Query	ArcSight Administration/ESM/Event Analysis Overview/by Event Name/
Breakdown by Event Priority From Vendor and Product	This query selects the events priority within the last 24 hours by vendor and product.	Query	ArcSight Administration/ESM/Event Analysis Overview/by Priority/
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.	Query	ArcSight Administration/ESM/Event Analysis Overview/
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.	Query	ArcSight Administration/ESM/Event Analysis Overview/
Hourly Distribution Chart for a Source Port	This query retrieves the hourly distribution of events for sources with a specific port.	Query	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.	Query	ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Hourly Event Counts (Area Chart)	This query retrieves the hourly distribution of event counts.	Query	ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/

Resources that Support the ESM Events Use Case, continued

Resource	Description	Type	URI
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.	Query	ArcSight Administration/ESM/Event Analysis Overview/
Event Name Counts	This query retrieves the event names and their event counts.	Query	ArcSight Administration/ESM/System Health/Events/
Hourly Distribution Chart for a Destination Port	This query retrieves the hourly distribution of events for destinations with a specific port.	Query	ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
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.	Query	ArcSight Administration/ESM/Event Analysis Overview/
Hourly Distribution Chart for Event	This query retrieves the hourly distribution of specific events.	Query	ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
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.	Query	ArcSight Administration/ESM/System Health/Events/
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	ArcSight System/1 Chart/Without Table
Events Count	This trend stores the total number of non ArcSight events.	Trend	ArcSight Administration/ESM/Events Analysis Overview/

ESM Reporting Resource Monitoring

The ESM Reporting Resource Monitoring use case provides performance statistics for reports, trends, and query viewers.

ESM Reporting Resource Monitoring Resources

The following table lists all the resources in the ESM Reporting Resource Monitoring use case.

Resources that Support the ESM Reporting Resource Monitoring Use Case

Resource	Description	Type	URI
Monitor Resources			
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.	Active Channel	ArcSight Administration/ESM/System Health/Resources/
Reports Status	This active channel shows all the report-related events within the last two hours.	Active Channel	ArcSight Administration/ESM/System Health/Resources/
Query Viewers Status	This active channel shows all the query viewer-related events within the last two hours.	Active Channel	ArcSight Administration/ESM/System Health/Resources/

Resources that Support the ESM Reporting Resource Monitoring Use Case, continued

Resource	Description	Type	URI
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.	Dashboard	ArcSight Administration/ESM/System Health/Resources/Reporting/
Trend Details	This dashboard shows query details for trends.	Dashboard	ArcSight Administration/ESM/System Health/Resources/Reporting/
Query Viewer Details	This dashboard shows query details for query viewers.	Dashboard	ArcSight Administration/ESM/System Health/Resources/Reporting/
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.	Dashboard	ArcSight Administration/ESM/System Health/Resources/Reporting/
Report Details	This dashboard shows query details for reports.	Dashboard	ArcSight Administration/ESM/System Health/Resources/Reporting/
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.	Query Viewer	ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Last 10 Trend Queries	This query viewer shows the duration information for the last ten trend queries.	Query Viewer	ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/

Resources that Support the ESM Reporting Resource Monitoring Use Case, continued

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

Resources that Support the ESM Reporting Resource Monitoring Use Case, continued

Resource	Description	Type	URI
Query Counts During Last 24 hr	This query viewer shows the query and its counts during the last 24 hours.	Query Viewer	ArcSight Administration/ESM/System Health/Resources/Reporting/
Running Trend Queries	This query viewer shows the currently running trend queries.	Query Viewer	ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Last 10 Query Viewer Queries	This query viewer shows the last ten query viewer query duration information.	Query Viewer	ArcSight Administration/ESM/System Health/Resources/Reporting/Query Viewers/
Query Viewer Failures During Last 24 hr	This query viewer shows the failed query viewers during the last 24 hours.	Query Viewer	ArcSight Administration/ESM/System Health/Resources/Reporting/Query Viewers/
Failed Queries	This report shows the failed queries for trend, report, and query viewers. The default time frame is one week.	Report	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.	Report	ArcSight Administration/ESM/System Health/Resources/Reporting/

Resources that Support the ESM Reporting Resource Monitoring Use Case, continued

Resource	Description	Type	URI
Query Counts by Type	This report shows query counts grouped by type. The default time frame is one week.	Report	ArcSight Administration/ESM/System Health/Resources/Reporting/
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.	Report	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.	Report	ArcSight Administration/ESM/System Health/Resources/Reporting/
Library - Correlation Resources			
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.	Rule	ArcSight Administration/ESM/System Health/Resources/
Library Resources			

Resources that Support the ESM Reporting Resource Monitoring Use Case, continued

Resource	Description	Type	URI
Query Running Time	This active list stores query information used to monitor and report the query duration.	Active List	ArcSight Administration/ESM/System Health/Resources/
Currently Running Reports	This data monitor shows report statistics for currently running reports.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Reporting/Reporting Subsystem Statistics/
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.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Reporting/Reporting Subsystem Statistics/
Last 10 Trend Queries Returning No Results	This data monitor shows the last ten trend queries that return no results.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Trends/
Report Statistics	This data monitor shows reporting statistics related to runtimes for currently running and past run reports.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Reporting/Reporting Subsystem Statistics/

Resources that Support the ESM Reporting Resource Monitoring Use Case, continued

Resource	Description	Type	URI
Event Base	This field set contains all the ESM event fields.	Field Set	ArcSight System/Event Field Sets
Query Status	This field set displays detailed information about queries.	Field Set	ArcSight Administration/ESM/
Hour less than 10	This filter is used by a Conditional DV. The condition in the filter is Hour (EndTime) is less than 10.	Filter	ArcSight Administration/ESM/System Health/Resources/Trends/Conditional Variable Filters/
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.	Filter	ArcSight Administration/ESM/System Health/Resources/Reporting/
Trend Query Returning No Results	This filter detects successful trend query events that return no results.	Filter	ArcSight Administration/ESM/System Health/Resources/Trends/
Minute less than 10	This filter is used by a Conditional DV. The condition in the filter is Minute (EndTime) is less than 10.	Filter	ArcSight Administration/ESM/System Health/Resources/Trends/Conditional Variable Filters/
Longest QueryViewer Queries	This query retrieves query duration information for query viewers, ordered by duration.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/QueryViewers/

Resources that Support the ESM Reporting Resource Monitoring Use Case, continued

Resource	Description	Type	URI
QueryViewer Queries	This query retrieves query duration information for query viewers used to build a trend.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/QueryViewers/
Last 10 QueryViewer Queries	This query retrieves query duration information for query viewers, ordered by end time.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/QueryViewers/
Trend Query	This query retrieves trend query duration information used to build a trend.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
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.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Queries/
QueryViewer Failures	This query retrieves query duration information for failed query viewers.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/QueryViewers/
Last 10 Report Queries	This query retrieves report query duration information, ordered by end time.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Longest QueryViewer Queries - Trend	This query retrieves query viewer query duration information from trends, ordered by duration.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/QueryViewers/

Resources that Support the ESM Reporting Resource Monitoring Use Case, continued

Resource	Description	Type	URI
Longest Trend Queries	This query retrieves trend query duration information, ordered by duration.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Trend Query Failures	This query retrieves failed trend query duration information.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Longest Report Queries	This query retrieves report query duration information, ordered by duration.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Query Counts During Last 24 hr	This query identifies the resource type and its counts from the Query Running Time active list.	Query	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.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Queries/
Longest Trend Queries - Trend	This query retrieves trend query duration information from a trend, ordered by duration.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Running Report Queries	This query retrieves currently running report queries.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Report Query Failures	This query retrieves failed query duration information for reports.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Report Queries	This query retrieves report query duration information used to build a trend.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/

Resources that Support the ESM Reporting Resource Monitoring Use Case, continued

Resource	Description	Type	URI
Query Counts During Last Week	This query retrieves resource types and their counts from the Query Running Time active list.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Queries/
Last 10 Trend Queries	This query retrieves trend query duration information, ordered by end time.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Running Trend Queries	This query retrieves running trend query duration information.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Longest Report Queries - Trend	This query retrieves report query duration information from trends, ordered by duration.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	ArcSight System/1 Chart/Without Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With Table
Trend Queries	This trend stores the top longest trend queries by day.	Trend	ArcSight Administration/ESM/System Health/Resources/Reporting/
Report Queries	This trend stores the top longest report queries by day.	Trend	ArcSight Administration/ESM/System Health/Resources/Reporting/

Resources that Support the ESM Reporting Resource Monitoring Use Case, continued

Resource	Description	Type	URI
QueryViewer Queries	This trend stores the top longest query viewer queries by day.	Trend	ArcSight Administration/ESM/System Health/Resources/Reporting/
Failed Queries	This trend stores failed queries for reports, trends, and query viewers.	Trend	ArcSight Administration/ESM/System Health/Resources/Reporting/

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

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

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*.

ESM Resource Monitoring Resources

The following table lists all the resources in the ESM Resource Monitoring use case.

Resources that Support the ESM Resource Monitoring Use Case

Resource	Description	Type	URI
Monitor 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.	Dashboard	ArcSight Administration/ESM/System Health/Resources/Rules/
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.	Dashboard	ArcSight Administration/ESM/System Health/Resources/Reporting/

Resources that Support the ESM Resource Monitoring Use Case, continued

Resource	Description	Type	URI
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.	Dashboa rd	ArcSight Administration/ESM/System Health/Resources/Reporting/
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.	Query Viewer	ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Query Failures During Last 24 hr	This query viewer displays failed queries for reports, trends, and query viewers.	Query Viewer	ArcSight Administration/ESM/System Health/Resources/Reporting/
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.	Query Viewer	ArcSight Administration/ESM/System Health/Resources/Reporting/Query Viewers/
Query Counts During Last 24 hr	This query viewer shows the query and its counts during the last 24 hours.	Query Viewer	ArcSight Administration/ESM/System Health/Resources/Reporting/
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.	Query Viewer	ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/

Resources that Support the ESM Resource Monitoring Use Case, continued

Resource	Description	Type	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.	Report	ArcSight Administration/ESM/System Health/Resources/Active Lists/
Rules Engine Warning Messages	This report shows warning messages received from the rules engine.	Report	ArcSight Administration/ESM/System Health/Resources/Rules/
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.	Report	ArcSight Administration/ESM/System Health/Resources/Session Lists/
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.	Report	ArcSight Administration/ESM/System Health/Resources/

Resources that Support the ESM Resource Monitoring Use Case, continued

Resource	Description	Type	URI
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.	Report	ArcSight Administration/ESM/System Health/Resources/Active Lists/
Data Monitor Evaluations Statistics	This report shows a chart with the average number of data monitor evaluations per second.	Report	ArcSight Administration/ESM/System Health/Resources/Data Monitors/
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.	Report	ArcSight Administration/ESM/System Health/Resources/Rules/
Fired Rule Events	This report does not populate all values when running in Turbo Mode Fastest.	Report	ArcSight Administration/ESM/System Health/Resources/Rules/
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.	Report	ArcSight Administration/ESM/System Health/Resources/Session Lists/

Resources that Support the ESM Resource Monitoring Use Case, continued

Resource	Description	Type	URI
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.	Report	ArcSight Administration/ESM/System Health/Resources/Rules/
Library - Correlation 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.	Rule	ArcSight Administration/ESM/System Health/Resources/
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.	Rule	ArcSight Administration/ESM/System Health/Resources/Rules/
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.	Rule	ArcSight Administration/ESM/System Health/Resources/Rules/

Resources that Support the ESM Resource Monitoring Use Case, continued

Resource	Description	Type	URI
Resource Became Valid	This rule triggers when an invalid resource becomes valid. The rule removes the resource from the Invalid Resources active list.	Rule	ArcSight Administration/ESM/System Health/Resources/
Library Resources			
Query Running Time	This active list stores query information used to monitor and report the query duration.	Active List	ArcSight Administration/ESM/System Health/Resources/
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.	Active List	ArcSight Administration/ESM/System Health/Resources/
Currently Running Reports	This data monitor shows report statistics for currently running reports.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Reporting/Reporting Subsystem Statistics/
Rules Engine Internal Stats	This data monitor shows internal statistics about the rules engine.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/
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.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Reporting/Reporting Subsystem Statistics/

Resources that Support the ESM Resource Monitoring Use Case, continued

Resource	Description	Type	URI
Recent Fired Rules	This data monitor shows detailed information about the most recently fired rules.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/
Partial Matches per Rule	This data monitor shows event counts for partial rule matches.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/
Report Statistics	This data monitor shows reporting statistics related to runtimes for currently running and past run reports.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Reporting/Reporting Subsystem Statistics/
Top Firing Rules	This data monitor shows detailed information about the top firing rules.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/
Sortable Rule Stats	<p>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.</p> <p>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.</p>	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/
Rule Error Logs	This data monitor shows the most recent errors received from the rules engine.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/

Resources that Support the ESM Resource Monitoring Use Case, continued

Resource	Description	Type	URI
Hour less than 10	This filter is used by a Conditional DV. The condition in the filter is Hour (EndTime) is less than 10.	Filter	ArcSight Administration/ESM/System Health/Resources/Trends/Conditional Variable Filters/
ArcSight Rules	This filter identifies ArcSight ESM correlation events generated by rules.	Filter	ArcSight Administration/ESM/System Health/Resources/Rules/
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.	Filter	ArcSight Administration/ESM/System Health/Resources/Reporting/
Rules Engine Internal Events	This filter identifies internal ArcSight ESM rules engine base events.	Filter	ArcSight Administration/ESM/System Health/Resources/Rules/
Minute less than 10	This filter is used by a Conditional DV. The condition in the filter is Minute(EndTime) is less than 10.	Filter	ArcSight Administration/ESM/System Health/Resources/Trends/Conditional Variable Filters/
All Events	This filter matches all events.	Filter	ArcSight System/Core
Longest QueryView er Queries	This query retrieves query duration information for query viewers, ordered by duration.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/QueryView ers/
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.	Query	ArcSight Administration/ESM/System Health/Resources/Active Lists/

Resources that Support the ESM Resource Monitoring Use Case, continued

Resource	Description	Type	URI
Fired Rule Events	This report does not populate all values when running in Turbo Mode Fastest.	Query	ArcSight Administration/ESM/System Health/Resources/Rules/
Invalid Resources (Chart)	This query retrieves the count of invalid resources by resource type from the Invalid Resources active list.	Query	ArcSight Administration/ESM/System Health/Resources/
Correlation Events Count	This query retrieves the total number of correlation events within the last hour, grouping them by ten minute intervals.	Query	ArcSight Administration/ESM/System Health/Resources/Rules/
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.	Query	ArcSight Administration/ESM/System Health/Resources/Session Lists/
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.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Queries/
Invalid Resources	This query retrieves a list of invalid resources from the Invalid Resources active list.	Query	ArcSight Administration/ESM/System Health/Resources/
Longest Trend Queries	This query retrieves trend query duration information, ordered by duration.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Correlation Events Count (Details)	This query retrieves the number of correlation events per rule within the last hour, grouping them by ten minute intervals.	Query	ArcSight Administration/ESM/System Health/Resources/Rules/

Resources that Support the ESM Resource Monitoring Use Case, continued

Resource	Description	Type	URI
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.	Query	ArcSight Administration/ESM/System Health/Resources/Session Lists/
Longest Report Queries	This query retrieves report query duration information, ordered by duration.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Query Counts During Last 24 hr	This query identifies the resource type and its counts from the Query Running Time active list.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Queries/
Rules Engine Warning Messages	This query retrieves warning messages received from the rules engine.	Query	ArcSight Administration/ESM/System Health/Resources/Rules/
Failed Queries - Trend	This query retrieves failed queries for reports, trends, and query viewers from a trend.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/Queries/
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.	Query	ArcSight Administration/ESM/System Health/Resources/Session 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.	Query	ArcSight Administration/ESM/System Health/Resources/Active Lists/

Resources that Support the ESM Resource Monitoring Use Case, continued

Resource	Description	Type	URI
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.	Query	ArcSight Administration/ESM/System Health/Resources/Data Monitors/
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.	Query	ArcSight Administration/ESM/System Health/Resources/Active Lists/
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.	Query	ArcSight Administration/ESM/System Health/Resources/Rules/
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	ArcSight System/1 Chart/Without Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With Table
Failed Queries	This trend stores failed queries for reports, trends, and query viewers.	Trend	ArcSight Administration/ESM/System Health/Resources/Reporting/
ESM Reporting Resource Monitoring	This use case provides information about performance statistics for reports, trends, and query viewers.	Use Case	ArcSight Administration/ESM/System Health/

ESM Storage Monitoring (CORR)

The ESM Storage Monitoring (CORR) 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.

Configuring the ESM Storage Monitoring (CORR) Use Case

Enable the notification action for the **ASM Database Free Space - Critical** rule if appropriate for your organization. For information about how to enable notification actions, see the *ArcSight Console User's Guide*.

ESM Storage Monitoring (CORR) Resources

The following table lists all the resources in the ESM Storage Monitoring (CORR) use case.

Resources that Support the ESM Storage Monitoring (CORR) Use Case

Resource	Description	Type	URI
Monitor Resources			
Database Performance Statistics	This dashboard shows an overview of database related statistics, such as available space, insert, and retrieval times.	Dashboard	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
Archive Status	This dashboard shows database archive related information.	Dashboard	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
Critical Archive Failure Details	This query viewer shows the current archive archival failure events.	Query Viewer	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
Archive Task Failure Details	This query viewer shows the current archive task failure events, which include activation, deactivation and scheduling.	Query Viewer	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
Archive Status Report	This report shows the current status of archive and disk space used.	Report	ArcSight Administration/ESM/System Health/Storage/CORR-Engine

Resources that Support the ESM Storage Monitoring (CORR) Use Case, continued

Resource	Description	Type	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.	Report	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).	Report	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
Archive Processing	This report shows the longest to process archives and the time to archive information.	Report	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.	Report	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
Library - Correlation Resources			
Archive Task Success	This rule is triggered by successful archive activation, deactivation and scheduling audit events where its archive name is in the active list - Archive Task Failures. This rule will remove the entry from the active list.	Rule	ArcSight Administration/ESM/System Health/Storage/ CORR-Engine/
Critical Archive Failures	This rule is triggered by archive archival failure event and writes it to the active list - Critical Archive Failures.	Rule	ArcSight Administration/ESM/System Health/Storage/ CORR-Engine/

Resources that Support the ESM Storage Monitoring (CORR) Use Case, continued

Resource	Description	Type	URI
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.	Rule	ArcSight Administration/ESM/System Health/Storage/
Archive Events	This rule is triggered by archive audit event and writes it to the Archive Events session list.	Rule	ArcSight Administration/ESM/System Health/Storage/ CORR-Engine/
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.	Rule	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.	Rule	ArcSight Administration/ESM/System Health/Storage/

Resources that Support the ESM Storage Monitoring (CORR) Use Case, continued

Resource	Description	Type	URI
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.	Rule	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.	Rule	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).	Rule	ArcSight Administration/ESM/System Health/Storage/
Critical Archive Success	This rule is triggered by archive archival success event where the archive name is in the active list - Critical Archival Failures. This rule will remove the entry from the active list.	Rule	ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Task Failures	This rule is triggered by archive task failure event, which includes activation, deactivation and scheduling events, and writes it to the active list - Archive Task Failures.	Rule	ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Resources that Support the ESM Storage Monitoring (CORR) Use Case, continued

Resource	Description	Type	URI
Out of Domain Fields	This rule triggers when there is no more free domain field available for a field type.	Rule	ArcSight Administration/ESM/System Health/Resources/Domains/
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.	Rule	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.	Rule	ArcSight Administration/ESM/System Health/Storage/
Library Resources			
Critical Archive Failures	This active list stores archive archival failure events.	Active List	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
Archive Task Failures	This active list stores archive task failure events, which include activation, deactivation, and scheduling.	Active List	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
Database Retrieval Time - Last Hour	This data monitor displays the moving average for database retrieval time during the last hour.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics

Resources that Support the ESM Storage Monitoring (CORR) Use Case, continued

Resource	Description	Type	URI
Database Insert Time - Last 24 Hours	This data monitor displays the moving average for database insert time during the last 24 hours.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics
Database Transaction Volume	This data monitor shows transaction settings and detailed information about database transactions.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/
Database Insert Time - Last Hour	This data monitor displays the moving average for database insert time during the last hour.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics
Database Retrieval Time - Last 24 Hours	This data monitor displays the moving average for database retrieval time during the last 24 hours.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics
Database Free Space	This data monitor displays the database free space.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics
Archive Disk Space	This data monitor shows the state of archive disk space used: OK, Warning, and Critical Warning.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Archive Status
Recent Archive Events	This data monitor shows last ten archive events.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Archive Status
Database Insert Time Statistics	This filter identifies ArcSight system events where the Device Event Category is /Monitor/EventBroker/InsertTime.	Filter	ArcSight Administration/ESM/System Health/Storage/
ASM Database Load Statistics	This filter identifies events related to ArcSight ESM database load.	Filter	ArcSight Administration/ESM/System Health/Storage/

Resources that Support the ESM Storage Monitoring (CORR) Use Case, continued

Resource	Description	Type	URI
ASM Database Statistics	This filter identifies events related to ArcSight ESM database statistics (such as insertion/retrieval).	Filter	ArcSight Administration/ESM/System Health/Storage/
Archive Settings Updated Event	This filter selects archive settings updated audit events.	Filter	ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters
Archive Archival Success	This filter selects archive archival success audit events.	Filter	ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters
Archive Disk Space	This filter selects archive disk space audit events.	Filter	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
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.	Filter	ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters
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.	Filter	ArcSight Administration/ESM/System Health/Storage/Custom/
Archive Events	This filter selects all archive audit events.	Filter	ArcSight Administration/ESM/System Health/Storage/CORR-Engine

Resources that Support the ESM Storage Monitoring (CORR) Use Case, continued

Resource	Description	Type	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.	Filter	ArcSight Administration/ESM/System Health/Storage/Custom/
Archive Failure Events	This filter selects all archive failure audit events.	Filter	ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters
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.	Filter	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.	Filter	ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters
Database Retrieval Time Statistics	This filter identifies ArcSight system events where the Device Event Category is /Monitor/EventBroker/RetrievalTime.	Filter	ArcSight Administration/ESM/System Health/Storage/
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.	Focused Report	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
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.	Focused Report	ArcSight Administration/ESM/System Health/Storage/CORR-Engine

Resources that Support the ESM Storage Monitoring (CORR) Use Case, continued

Resource	Description	Type	URI
Critical Archive Failure Details	This query selects archive archival failure events from the active list: Critical Archive Failures.	Query	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
Archive Activation Statistics	This query selects archive activation audit events from the Archive Events session list.	Query	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.	Query	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
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.	Query	ArcSight Administration/ESM/System Health/Storage/Trend Queries/
Archive Disk Space Usage	This query selects archive disk space used information from the Archive Events session list.	Query	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
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.	Query	ArcSight Administration/ESM/System Health/Storage/Trend Queries/
Archive Deactivation Statistics	This query selects archive deactivation audit events from the Archive Events session list.	Query	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.	Query	ArcSight Administration/ESM/System Health/Storage/CORR-Engine

Resources that Support the ESM Storage Monitoring (CORR) Use Case, continued

Resource	Description	Type	URI
Archive Non-success events	This query selects non-successful archive audit events from the Archive Events session list.	Query	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
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.	Query	ArcSight Administration/ESM/System Health/Storage/Event Queries/
Archive Archival Success	This query selects archive archival information from the Archive Events session list.	Query	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
Archive Space status	This query selects archive space audit events.	Query	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
Archive Archival Statistics	This query selects archive archival audit events from the Archive Events session list.	Query	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
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.	Query	ArcSight Administration/ESM/System Health/Storage/
Archive Scheduling Statistics	This query selects archive scheduling audit events from the Archive Events session list.	Query	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
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.	Report Template	ArcSight Administration/System Health/Storage/CORR-Engine

Resources that Support the ESM Storage Monitoring (CORR) Use Case, continued

Resource	Description	Type	URI
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With Table
Two Charts Landscape	This template is designed to show two charts and a description field. The orientation is portrait.	Report Template	ArcSight System/2 Charts/Without Table
Archive Events	This session list stores archive audit events.	Session List	ArcSight Administration/ESM/System Health/Storage/CORR-Engine
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).	Trend	ArcSight Administration/ESM/System Health/Storage/

ESM Storage Monitoring (Oracle)

The ESM Storage Monitoring (Oracle) use case provides information on the health of the Oracle database. This does not apply if you are using ESM with CORR-Engine or ArcSight Express with CORR-Engine.

ESM Storage Monitoring (Oracle) Resources

The following table lists all the resources in the ESM Storage Monitoring (Oracle) use case.

Resources that Support the ESM Storage Monitoring (Oracle) Use Case

Resource	Description	Type	URI
Monitor Resources			
Database Performance Statistics	This dashboard shows an overview of database related statistics, such as available space, insert and retrieval times, etc.	Dashboard	ArcSight Administration/ESM/System Health/Storage/Oracle
Partition Manager and Archiver Status	This dashboard shows the status and details of partition manager and partition archiver.	Dashboard	ArcSight Administration/ESM/System Health/Storage/Oracle
ASM Database Free Space - by Hour	This trend report shows the free space percentages by hour for the ASM database table spaces. The report has 4 stacked area charts showing the percentages by hour for the ARC_EVENT_DATA, ARC_EVENT_INDEX, ARC_SYSTEM_DATA, and ARC_SYSTEM_INDEX table spaces.	Report	ArcSight Administration/ESM/System Health/Storage/Oracle

Resources that Support the ESM Storage Monitoring (Oracle) Use Case, continued

Resource	Description	Type	URI
ASM Database Free Space - by Day	This trend 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).	Report	ArcSight Administration/ESM/System Health/Storage/Oracle
ASM Database Free Space	This report shows the current free space percentages for the ASM database table spaces. The report has 4 bar charts showing the percentages for the ARC_EVENT_DATA, ARC_EVENT_INDEX, ARC_SYSTEM_DATA, and ARC_SYSTEM_INDEX table spaces.	Report	ArcSight Administration/ESM/System Health/Storage/Oracle
Library - Correlation Resources			
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.	Rule	ArcSight Administration/ESM/System Health/Storage/

Resources that Support the ESM Storage Monitoring (Oracle) Use Case, continued

Resource	Description	Type	URI
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.	Rule	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.	Rule	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.	Rule	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).	Rule	ArcSight Administration/ESM/System Health/Storage/

Resources that Support the ESM Storage Monitoring (Oracle) Use Case, continued

Resource	Description	Type	URI
Out of Domain Fields	This rule triggers when there is no more free domain field available for a field type.	Rule	ArcSight Administration/ESM/System Health/Resources/Domains/
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.	Rule	ArcSight Administration/ESM/System Health/Storage/
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.	Rule	ArcSight Administration/ESM/System Health/Storage/
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.	Rule	ArcSight Administration/ESM/System Health/Storage/
Library Resources			
Partition Manager and Archiver Details	This data monitor displays last 10 system audit events for partition manager and partition archiver.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle

Resources that Support the ESM Storage Monitoring (Oracle) Use Case, continued

Resource	Description	Type	URI
Database Retrieval Time - Last Hour	This data monitor displays moving average for database retrieval time during last hour.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle/Datab ase Performance Statistics
Database Insert Time - Last 24 Hours	This data monitor displays moving average for database insert time during last 24 hour.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle/Datab ase Performance Statistics
Sidetable Sizes (Rows)	This moving average data monitor shows the average number of rows of the database sidetables for the last 10 minutes. The sampling interval is one minute and a correlation event will be generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle/Datab ase Performance Statistics
Database Transaction Volume	This data monitor shows transaction settings and detailed information about database transactions.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/
Partition Manager and Archiver - Heads Up Display	This data monitor shows the status of partition manager and partition archiver.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle
ASM Database Responsivene ss - Last Hour	This data monitor displays moving average for database response time during last hour.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle/Datab ase Performance Statistics
Database Insert Time - Last Hour	This data monitor displays moving average for database insert time during last hour.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle/Datab ase Performance Statistics
Database Retrieval Time - Last 24 Hours	This data monitor displays moving average for database retrieval time during last 24 hour.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle/Datab ase Performance Statistics

Resources that Support the ESM Storage Monitoring (Oracle) Use Case, continued

Resource	Description	Type	URI
Database Free Space	This data monitor displays the database free space	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle/Database Performance Statistics
Sidetable Cache Hit Rates	This moving average data monitor shows the average value of the database sidetable cash hit rate for the last 15 minutes. The sampling interval is one minute and a correlation event will be generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle/Database Performance Statistics
ASM Database Responsiveness - Last 24 hours	This data monitor displays moving average for database response time during last 24 hour.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle/Database Performance Statistics
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.	Filter	ArcSight Administration/ESM/System Health/Storage/Custom/
Database Insert Time Statistics	This filter identifies ArcSight system events where the Device Event Category is /Monitor/EventBroker/InsertTime.	Filter	ArcSight Administration/ESM/System Health/Storage/
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.	Filter	ArcSight Administration/ESM/System Health/Storage/Custom/
ASM Database Load Statistics	This filter identifies events related to ArcSight ESM database load.	Filter	ArcSight Administration/ESM/System Health/Storage/

Resources that Support the ESM Storage Monitoring (Oracle) Use Case, continued

Resource	Description	Type	URI
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.	Filter	ArcSight Administration/ESM/System Health/Storage/
ASM Database Statistics	This filter identifies events related to ArcSight ESM database statistics (such as insertion/retrieval).	Filter	ArcSight Administration/ESM/System Health/Storage/
Partition Manager and Archiver Events	This filter selects system audit events of partition manager and partition archiver.	Filter	ArcSight Administration/ESM/System Health/Storage/Oracle
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.	Filter	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.	Filter	ArcSight Administration/ESM/System Health/Storage/

Resources that Support the ESM Storage Monitoring (Oracle) Use Case, continued

Resource	Description	Type	URI
Event Index Free Space - Last 30 Days	This focused report shows the free space percentages by day for the ARC_EVENT_INDEX database table space for the last 30 days. The source report is "ASM Database Free Space - by Day" report.	Focused Report	ArcSight Administration/ESM/System Health/Storage/Oracle
System Index Free Space - Last 30 Days	This focused report shows the free space percentages by day for the ARC_SYSTEM_INDEX database table space for the last 30 days. The source report is "ASM Database Free Space - by Day" report.	Focused Report	ArcSight Administration/ESM/System Health/Storage/Oracle
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" report.	Focused Report	ArcSight Administration/ESM/System Health/Storage/Oracle
Event Data Free Space - Last 30 Days	This focused 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" report.	Focused Report	ArcSight Administration/ESM/System Health/Storage/Oracle
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.	Query	ArcSight Administration/ESM/System Health/Storage/Event Queries/

Resources that Support the ESM Storage Monitoring (Oracle) Use Case, continued

Resource	Description	Type	URI
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.	Query	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.	Query	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.	Query	ArcSight Administration/ESM/System Health/Storage/Trend Queries/
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).	Trend	ArcSight Administration/ESM/System Health/Storage/

Logger Events

The Logger Events use case provides statistics for events sent through a Logger.

Logger Events Resources

The following table lists all the resources in the Logger Events use case.

Resources that Support the Logger Events Use Case

Resource	Description	Type	URI
Monitor Resources			
Logger Application Events	This active channel shows all the Logger application events within the last hour.	Active Channel	ArcSight Administration/Logger/
Logger Platform Events	This active channel shows all the Logger platform events within the last hour.	Active Channel	ArcSight Administration/Logger/
Library Resources			
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.	Field Set	ArcSight Administration/Logger/
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.	Field Set	ArcSight Administration/Logger/
Logger Platform Events	This filter identifies Logger platform events.	Filter	ArcSight Administration/Logger/Event Types/
Logger System Health Events	This filter identifies Logger system health events.	Filter	ArcSight Administration/Logger/Event Types/
Logger Events	This filter identifies Logger events.	Filter	ArcSight Administration/Logger/Event Types/

Resources that Support the Logger Events Use Case, continued

Resource	Description	Type	URI
Logger Application Events	This filter identifies Logger application events.	Filter	ArcSight Administration/Logger/Event Types/

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:

- Enable the following rules:
 - **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 ["Enabling Rules" on page 12](#).

- Enable the notification action for the above listed rules, if appropriate for your organization. For information on how to enable notifications, refer to the *ArcSight Console User's Guide*.
- Enable the following data monitors, described in the table under ["Logger System Health Resources" on the next page](#):
 - **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*.

Logger System Health Resources

The following table lists all the resources in the Logger System Health use case.

Resources that Support the Logger System Health Use Case

Resource	Description	Type	URI
Monitor Resources			
Logger System Health Events	This active channel shows all the Logger system health events within the last hour.	Active Channel	ArcSight Administration/Logger/
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.	Dashboard	ArcSight Administration/Logger/My Logger/
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.	Dashboard	ArcSight Administration/Logger/My Logger/

Resources that Support the Logger System Health Use Case, continued

Resource	Description	Type	URI
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.	Dashboard	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.	Dashboard	ArcSight Administration/Logger/My Logger/
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.	Dashboard	ArcSight Administration/Logger/My Logger/
Library - Correlation Resources			
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.	Rule	ArcSight Administration/Logger/System Health/

Resources that Support the Logger System Health Use Case, continued

Resource	Description	Type	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.	Rule	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.	Rule	ArcSight Administration/Logger/System Health/
Library Resources			
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.	Active List	ArcSight Administration/Logger/System Health/

Resources that Support the Logger System Health Use Case, continued

Resource	Description	Type	URI
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.	Active List	ArcSight Administration/Logger/System Health/
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.	Data Monitor	ArcSight Administration/Logger/My Logger/Network
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.	Data Monitor	ArcSight Administration/Logger/My Logger/Network/
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.	Data Monitor	ArcSight Administration/Logger/My Logger/Network/

Resources that Support the Logger System Health Use Case, continued

Resource	Description	Type	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.	Data Monitor	ArcSight Administration/Logger/My Logger/CPU and Memory/
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.	Data Monitor	ArcSight Administration/Logger/My Logger/Storage/
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.	Data Monitor	ArcSight Administration/Logger/My Logger/CPU and Memory/
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.	Data Monitor	ArcSight Administration/Logger/My Logger/Network

Resources that Support the Logger System Health Use Case, continued

Resource	Description	Type	URI
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.	Data Monitor	ArcSight Administration/Logger/My Logger/Hardware/
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.	Data Monitor	ArcSight Administration/Logger/My Logger/Storage/
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.	Data Monitor	ArcSight Administration/Logger/My Logger/My Logger Overview/
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.	Data Monitor	ArcSight Administration/Logger/My Logger/My Logger Overview/

Resources that Support the Logger System Health Use Case, continued

Resource	Description	Type	URI
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.	Data Monitor	ArcSight Administration/Logger/My Logger/CPU and Memory/
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.	Data Monitor	ArcSight Administration/Logger/My Logger/Hardware/
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.	Data Monitor	ArcSight Administration/Logger/My Logger/My Logger Overview/
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.	Data Monitor	ArcSight Administration/Logger/My Logger/CPU and Memory/

Resources that Support the Logger System Health Use Case, continued

Resource	Description	Type	URI
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.	Data Monitor	ArcSight Administration/Logger/My Logger/Hardware/
Sensor Name	This field is an alias for Device Custom String5.	Global Variable	ArcSight Administration/Logger/
Sensor Status	This field is an alias for Device Custom String3.	Global Variable	ArcSight Administration/Logger/
Free Space	This field is an alias field for Device Custom Number1.	Global Variable	ArcSight Administration/Logger/
Timeframe	This field is an alias for Device Custom String2.	Global Variable	ArcSight Administration/Logger/
Disk Usage	This field returns the disk usage status whether it is normal or nearing critical usage (less than ten percent).	Global Variable	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.	Global Variable	ArcSight Administration/Logger/
ReadOrWrite	This field returns whether the logger event is a read or write event.	Global Variable	ArcSight Administration/Logger/
Disk Name	This field returns the name of the disk currently being used.	Global Variable	ArcSight Administration/Logger/
IndexOfUsage	This field returns the index position of the string /Usage within the Device Event Category field.	Global Variable	ArcSight Administration/Logger/

Resources that Support the Logger System Health Use Case, continued

Resource	Description	Type	URI
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.	Global Variable	ArcSight Administration/Logger/
Field Value	This field is an alias field for Device Custom Number1.	Global Variable	ArcSight Administration/Logger/
Unit	This field is an alias for Device Custom String1.	Global Variable	ArcSight Administration/Logger/
Logger IP	This field is an alias to Destination Translated Address.	Global Variable	ArcSight Administration/Logger/
Memory Name	This field returns a memory related value located within the Device Event Category field.	Global Variable	ArcSight Administration/Logger/
All Receivers and Forwarders	This field shows the EPS from all connector and forwarder agents connected to this ArcSight ESM.	Global Variable	ArcSight Administration/Logger/
Sensor Type	This field is an alias for Device Custom String4.	Global Variable	ArcSight Administration/Logger/
Logger Address	This field is an alias to the Device Address field.	Global Variable	ArcSight Administration/Logger/
CPU Name	The field returns the name of the CPU currently used.	Global Variable	ArcSight Administration/Logger/
Field Status	This field is an alias field for Device Custom String3.	Global Variable	ArcSight Administration/Logger/

Resources that Support the Logger System Health Use Case, continued

Resource	Description	Type	URI
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.	Field Set	ArcSight Administration/Logger/
Sensor Type is CPU	This filter identifies events in which the sensor type is CPU.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance
Memory Usage	This filter identifies Logger system health events related to memory usage that originate from the Logger defined in the My Logger filter.	Filter	ArcSight Administration/Logger/System Health/CPU and Memory/
Logger System Health Events	This filter identifies Logger system health events.	Filter	ArcSight Administration/Logger/Event Types/
Logger Events	This filter identifies Logger events.	Filter	ArcSight Administration/Logger/Event Types/
Network Usage	This filter identifies Logger system health events related to network usage that originate from the Logger defined in the My Logger filter.	Filter	ArcSight Administration/Logger/System Health/Network/
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.	Filter	ArcSight Administration/Logger/System Health/Hardware/Sensors/

Resources that Support the Logger System Health Use Case, continued

Resource	Description	Type	URI
All Receivers EPS	This filter identifies events in which the device event category is /Monitor/Receiver/All/EP S.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance
Sensor Type is FAN	This filter identifies events in which the sensor type is FAN.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance
CPU Usage	This filter identifies Logger system health events related to CPU usage that originate from the Logger defined in the My Logger filter.	Filter	ArcSight Administration/Logger/System Health/CPU and Memory/
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.	Filter	ArcSight Administration/Logger/System Health/
Remaining Disk More than 10 Percent	This filter identifies events in which the remaining disk space is greater than ten percent.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance
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.	Filter	ArcSight Administration/Logger/System Health/Hardware/

Resources that Support the Logger System Health Use Case, continued

Resource	Description	Type	URI
EPS Usage	This filter identifies Logger system health events related to EPS usage that originate from the Logger defined in the My Logger filter.	Filter	ArcSight Administration/Logger/System Health/Network/
Disk Usage	This filter identifies Logger system health events related to disk usage that originate from the Logger defined in the My Logger filter.	Filter	ArcSight Administration/Logger/System Health/Storage/
ArcSight Correlation Events	This filter identifies correlation events generated by ArcSight systems.	Filter	ArcSight System/Event Types
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.	Filter	ArcSight Administration/Logger/System Health/Hardware/Sensors/
Logger Disk Usage	This filter detects Logger system health events related to remaining disk space.	Filter	ArcSight Administration/Logger/ArcSight Appliances Overview/
Inbound Network	This filter identifies events in which the device event category ends with /In.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance
Remaining Disk Less than 5 Percent	This filter identifies events in which the remaining disk space is less than five percent.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance

Resources that Support the Logger System Health Use Case, continued

Resource	Description	Type	URI
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.	Filter	ArcSight Administration/Logger/System Health/Storage/
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.	Filter	ArcSight Administration/Logger/System Health/Hardware/Sensors/

Chapter 5: 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 out-of-the-box 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" below	"The Actor Support Resources group includes resources that support the actors feature. 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. "
"Priority Formula Resources" on page 230	"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."
"System Resources" on page 237	"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."

Actor Support Resources

The Actor Support Resources group includes resources that support the actors feature. 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.

Actor Support Resources

The following table lists all the resources in the Actor Support Resources resource group.

Resources that Support the Actor Support Resources Group

Resource	Description	Type	URI
Monitor Resources			
Actor Context Report by Target Username	This report shows activity related to an actor based on the ActorByTargetUserName global variable.	Report	ArcSight System/Core/
Actor Context Report by Account ID	This report shows activity related to an actor based on the ActorByAccountID global variable.	Report	ArcSight System/Core/
Actor Context Report by Attacker Username	This report shows activity related to an actor based on the ActorByAttackerUserName global variable.	Report	ArcSight System/Core/
Actor Context Report by Custom Fields	This report shows activity related to an actor based on the ActorByCustomFields global variable.	Report	ArcSight System/Core/
Library Resources			
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.	Active List	ArcSight System/Actor Data Support/
Actor Data Support	This group contains session lists for actor variables created by users.	Asset Category	ArcSight System
Actor Data	This group contains actor session lists. This is a locked group that hides system-maintained session lists for maintaining actor data.	Asset Category	ArcSight System

Resources that Support the Actor Support Resources Group, continued

Resource	Description	Type	URI
ActorByAccountID	This global variable maps the account information in an event with an actor. The account information consists of the device vendor and product, and information derived from the attacker or target user name, with preference to the attacker user name.	Global Variable	ArcSight System/Actor Variables
creator	This resource has no description.	Global Variable	ArcSight System/Actor Fields
ActorByAttackerUserName	This variable maps the account information in an event with an actor. The account information consists of the device vendor, device product, connector address, connector zone, and information derived from the attacker user name.	Global Variable	ArcSight System/Actor Variables
externalID	This resource has no description.	Global Variable	ArcSight System/Actor Fields
groupID	This resource has no description.	Global Variable	ArcSight System/Actor Fields

Resources that Support the Actor Support Resources Group, continued

Resource	Description	Type	URI
ActorByCustomFields	This variable retrieves actor information from events in which the authenticator information is maintained in device custom strings. It works in a similar way to the ActorByAccountID variable, but maps Device Custom String 1 to the vendor field and Device Custom String 2 to the product field. Device Custom String 3 holds the Account ID. If the events in your system are mapped in a different way, change the customVendor, customProduct, and getAccount local variables to map to the appropriate fields in your events. Note: When you upgrade the system in the future, this filter might be overwritten and your changes lost.	Global Variable	ArcSight System/Actor Variables
name	This resource has no description.	Global Variable	ArcSight System/Actor Fields
createTime	This resource has no description.	Global Variable	ArcSight System/Actor Fields
alias	This resource has no description.	Global Variable	ArcSight System/Actor Fields
ActorByTargetUserName	This variable maps the account information in an event with an actor. The account information consists of the device vendor, device product, connector address, connector zone, and information derived from the target user name.	Global Variable	ArcSight System/Actor Variables
id	This resource has no description.	Global Variable	ArcSight System/Actor Fields

Resources that Support the Actor Support Resources Group, continued

Resource	Description	Type	URI
modificationTime	This resource has no description.	Global Variable	ArcSight System/Actor Fields
ActorByDN	This global variable detects the Distinguished Name (DN) in Device Custom String1 and retrieves the actor with that DN.	Global Variable	ArcSight System/Actor Variables
owner	This resource has no description.	Global Variable	ArcSight System/Actor Fields
description	This resource has no description.	Global Variable	ArcSight System/Actor Fields
ActorByUUID	This global variable detects a UUID in Device Custom String1 and retrieves the actor with that UUID.	Global Variable	ArcSight System/Actor Variables
Actor Base	This field set contains all the fields related to actors.	Field Set	ArcSight System/Actor Field Sets
Actor Information	This field set contains a set of fields used to view actor data in events.	Field Set	ArcSight System/Actor Field Sets
Correlation Events	This filter identifies correlation events.	Filter	ArcSight System/Event Types/
Attacker User Name is NULL	This filter identifies events in which the attacker user name is NULL.	Filter	ArcSight System/Core/
Actor Events by Attacker Username	This query shows activity related to an actor based on the ActorByAttackerUserName global variable.	Query	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.	Query	ArcSight System/Core/Actor Context Report/

Resources that Support the Actor Support Resources Group, continued

Resource	Description	Type	URI
Actor Events by Target Username	This query shows activity related to an actor based on the ActorByTargetUsername global variable.	Query	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.	Query	ArcSight System/Core/Actor Context Report/
Actor Event Count by Account ID	This query shows activity related to an actor based on the ActorByAccountID global variable.	Query	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.	Query	ArcSight System/Core/Actor Context Report/
Actor Information	This query shows activity related to an actor.	Query	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.	Query	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.	Query	ArcSight System/Core/Actor Context Report/
Actor Context Report	This report template is used by the Actor Context Report.	Report Template	ArcSight System/

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.

Configuring the Priority Formula Resources Group

The Priority Formula Resources group requires the following configuration for your environment.

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 12](#).

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 Resources

The following table lists all the resources in the Priority Formula Resources group.

Resources that Support the Priority Formula Resources Group

Resource	Description	Type	URI
Library - Correlation Resources			
Reconnaissance - In Progress	This rule detects a reconnaissance in progress. The rule triggers whenever there are 10 attempts from the same attacker to the same target within three minutes. On the first threshold, the attacker address is added to the Reconnaissance List active list and the target address is added to the Scanned List active list.	Rule	ArcSight Administration/ArcSight System/Threat Tracking/Reconnaissance/
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.	Rule	ArcSight Administration/ArcSight System/Threat Tracking/Compromise/

Resources that Support the Priority Formula Resources Group, continued

Resource	Description	Type	URI
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.	Rule	ArcSight Administration/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.	Rule	ArcSight Administration/ArcSight System/Threat Tracking/Hostile/
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.	Rule	ArcSight Administration/ArcSight System/Threat Tracking/Compromise/

Resources that Support the Priority Formula Resources Group, continued

Resource	Description	Type	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.	Rule	ArcSight Administration/ArcSight System/Threat Tracking/Compromise/
Library Resources			
Hit List	This Active List contains hosts targeted by a potential attacker.	Active List	ArcSight System/Targets/
Suspicious List	This Active List contains hosts which have performed suspicious activity, either on the local system or over the network.	Active List	ArcSight System/Threat Tracking/
Hostile List	This Active List contains hosts that have been attempting attacks on systems.	Active List	ArcSight System/Threat Tracking/
Compromised List	This Active List contains hosts that may have been compromised by an attack.	Active List	ArcSight System/Threat Tracking/
Infiltrators List	This Active List contains hosts which have compromised (infiltrated) a system.	Active List	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.	Active List	ArcSight System/Attackers/
Untrusted List	This active list is to be manually populated with the addresses of known malicious systems.	Active List	ArcSight System/Attackers/
Scanned List	This Active List contains hosts that have been scanned by a potential attacker.	Active List	ArcSight System/Targets/
Reconnaissance List	This Active List contains IP addresses of hosts which have performed reconnaissance activity.	Active List	ArcSight System/Threat Tracking/

Resources that Support the Priority Formula Resources Group, continued

Resource	Description	Type	URI
High	The disruption of access to or use of information or an information system could be expected to have a sever or catastrophic adverse effect on organizational operations, organizational assets, or individuals.	Asset Category	Site Asset Categories/Compliance Requirement/FIPS-199/Availability Criticality
Moderate	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	Asset Category	Site Asset Categories/Compliance Requirement/FIPS-199/Confidentiality Criticality
High	The unauthorized modification of destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.	Asset Category	Site Asset Categories/Compliance Requirement/FIPS-199/Integrity Criticality
Moderate	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	Asset Category	Site Asset Categories/Compliance Requirement/FIPS-199/Availability Criticality
Vulnerabilities	This is a site asset category.	Asset Category	Site Asset Categories/Scanned
Moderate	The unauthorized modification of destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	Asset Category	Site Asset Categories/Compliance Requirement/FIPS-199/Integrity Criticality
Open Ports	This is a site asset category.	Asset Category	Site Asset Categories/Scanned
Low	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	Asset Category	Site Asset Categories/Compliance Requirement/FIPS-199/Availability Criticality
Criticality	This is a system asset category.	Asset Category	System Asset Categories

Resources that Support the Priority Formula Resources Group, continued

Resource	Description	Type	URI
Low	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	Asset Category	Site Asset Categories/Compliance Requirement/FIPS-199/Confidentiality Criticality
High	This is a system asset category.	Asset Category	System Asset Categories/Criticality
Medium	This is a system asset category.	Asset Category	System Asset Categories/Criticality
High	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.	Asset Category	Site Asset Categories/Compliance Requirement/FIPS-199/Confidentiality Criticality
Very Low	This is a system asset category.	Asset Category	System Asset Categories/Criticality
Low	This is a system asset category.	Asset Category	System Asset Categories/Criticality
Low	The unauthorized modification of destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	Asset Category	Site Asset Categories/Compliance Requirement/FIPS-199/Integrity Criticality
FIPS-199	This is a site asset category.	Asset Category	Site Asset Categories/Compliance Requirement
Very High	This is a system asset category.	Asset Category	System Asset Categories/Criticality
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.	Filter	ArcSight System/Core/
Very High Criticality Assets	This filter captures events where the target asset ID has been categorized as having a Very High criticality.	Filter	ArcSight System/Core/Threat Level Filters/

Resources that Support the Priority Formula Resources Group, continued

Resource	Description	Type	URI
High Criticality Assets	This filter captures events where the target asset ID has been categorized as having a High criticality.	Filter	ArcSight System/Core/Threat Level Filters/
Unknown Criticality Assets	This filter captures events where the target asset ID exists but has been categorized as having criticality.	Filter	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.	Filter	ArcSight System/Core/Threat Level Filters/
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.	Filter	ArcSight System/Core/
Low Criticality Assets	This filter captures events where the target asset ID has been categorized as having a Low criticality.	Filter	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.	Filter	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.	Filter	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.	Filter	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.	Filter	ArcSight System/Core/Threat Level Filters/
Compromised Targets	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.	Filter	ArcSight System/Core/Threat Level Filters/
Attackers on Hostile List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.	Filter	ArcSight System/Core/Threat Level Filters/

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 the System Resources Group

The System Resources group requires the following configuration for your environment:

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 SmartConnectors 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, such as HP Openview.
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*.

System Resources

The following table lists all the resources in the System Resources group.

Resources that Support the System Resources Group

Resource	Description	Type	URI
Monitor Resources			
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.	Active Channel	ArcSight System/Core/
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.	Active Channel	ArcSight System/
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.	Active Channel	ArcSight System/All Events/

Resources that Support the System Resources Group, continued

Resource	Description	Type	URI
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.	Active Channel	ArcSight System/Core/
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.	Active Channel	ArcSight System/All Events/
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.	Active Channel	ArcSight Administration/ESM/System Health/Events
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.	Report	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.	Report	ArcSight System/Core/
Library Resources			
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.	Active List	ArcSight System/Tuning/

Resources that Support the System Resources Group, continued

Resource	Description	Type	URI
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.	Active List	ArcSight System/Tuning/
Super Minimal	This resource has no description.	Field Set	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.	Field Set	ArcSight System/Event Field Sets/Active Channels
Common Conditions Editor	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Inspect - Edit
Executive	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Active Channels
Event Base	This field set contains all the ESM event fields.	Field Set	ArcSight System/Event Field Sets
TurboMode Comprehensive	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Inspect - Edit
Annotation-Mgr Rcpt	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Active Channels
Field Set Based On ARC_E_ET Index	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Sortable Field Sets
Field Set Based On ARC_E_MRT Index	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Sortable Field Sets
Export	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Active Channels

Resources that Support the System Resources Group, continued

Resource	Description	Type	URI
Event Inspector	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Inspect - Edit
ArcSight Admin	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Active Channels
MSSP	This resource has no description.	Field Set	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.	Field Set	ArcSight System/Event Field Sets/Active Channels
Minimal	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Inspect - Edit
Rule Action - Set Event Field	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Inspect - Edit
Categories	This field set shows all the categorization fields for events.	Field Set	ArcSight System/Event Field Sets/Active Channels
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.	Field Set	ArcSight System/Case Field Sets/
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.	Field Set	ArcSight Administration/Connector/
Standard-MgrRcpt	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Active Channels
TurboMode Fastest	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Inspect - Edit

Resources that Support the System Resources Group, continued

Resource	Description	Type	URI
Annotation	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Active Channels
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.	Field Set	ArcSight System/Asset Field Sets/
Asset	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Active Channels
Non-Categorized Events	This filter selects events that have no categorization.	Filter	ArcSight System/Event Types/
Severity Very High	This filter captures events where the agent severity is Very High.	Filter	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.	Filter	ArcSight System/Asset Auto-Creation/
Not Correlated and Not Closed	This resource has no description.	Filter	ArcSight System/Event Types/
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.	Filter	ArcSight System/Asset Auto-Creation/

Resources that Support the System Resources Group, continued

Resource	Description	Type	URI
Blocked ArcSight Internal Events	This filter is applied to audit events before they are inserted. Modify this filter to disable internal events as needed.	Filter	ArcSight System/Event Types/
ASM Events	This filter selects ArcSight System Monitoring events generated by the local ESM system (in an hierarchical deployment).	Filter	ArcSight System/Event Types
All Events	This filter matches all events.	Filter	ArcSight System/Core/
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.	Filter	ArcSight System/Event Types/
ArcSight Correlation Events	This filter identifies correlation events generated by ArcSight systems.	Filter	ArcSight System/Event Types/
Severity Low	This filter captures events where the agent severity is Low.	Filter	ArcSight System/Event Types/
SNMP Trap Sender	This resource has no description.	Filter	ArcSight System/SNMP Forwarding/
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).	Filter	ArcSight System/Event Types/
No Events	This is a utility filter that does not match any events passing through the system.	Filter	ArcSight System/Core/
ArcSight Internal Events	This filter selects events that are internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types/

Resources that Support the System Resources Group, continued

Resource	Description	Type	URI
Severity High	This filter captures events where the agent severity is High.	Filter	ArcSight System/Event Types/
Non-ArcSight Internal Events	This filter selects events that are not internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types/
Severity Unknown	This filter captures events where the agent severity is either NULL or Unknown.	Filter	ArcSight System/Event Types/
Manager Internal Agent's Filters	This filter looks for events coming from the Manager Internal Agent.	Filter	ArcSight System/Connector Filters/
Correlation Events	This filter identifies correlation events.	Filter	ArcSight System/Event Types/
Attacker User Name is NULL	This filter identifies events in which the attacker user name is NULL.	Filter	ArcSight System/Core/
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types/
Severity Medium	This filter captures events where the agent severity is Medium.	Filter	ArcSight System/Event Types/
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.	Integration Command	ArcSight System/Tools/Linux/
Web Search	This integration command is used to run a search with the selected item, device vendor, and device product in the selected event.	Integration Command	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.	Integration Command	ArcSight System/Tools/Linux/

Resources that Support the System Resources Group, continued

Resource	Description	Type	URI
Nslookup (Windows)	This integration command is used to find details about the Domain Name System (DNS). Run this command from a Windows console.	Integration Command	ArcSight System/Tools/Windows/
Portinfo (Windows)	This integration command is used to find information about the selected port. Run this command from a Windows console.	Integration Command	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.	Integration Command	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.	Integration Command	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.	Integration Command	ArcSight System/Tools/Windows/
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.	Integration Command	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.	Integration Command	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.	Integration Command	ArcSight System/Tools/Linux/

Resources that Support the System Resources Group, continued

Resource	Description	Type	URI
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.	Integration Configuration	ArcSight System/Tools/Linux/
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.	Integration Configuration	ArcSight System/Tools/Linux/
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.	Integration Configuration	ArcSight System/Tools/Windows/
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.	Integration Configuration	ArcSight System/Tools/Windows/
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.	Integration Configuration	ArcSight System/Tools/

Resources that Support the System Resources Group, continued

Resource	Description	Type	URI
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.	Integration Configuration	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.	Integration Configuration	ArcSight System/Tools/Windows/
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.	Integration Configuration	ArcSight System/Tools/Linux/
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.	Integration Configuration	ArcSight System/Tools/Windows/

Resources that Support the System Resources Group, continued

Resource	Description	Type	URI
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.	Integration Configuration	ArcSight System/Tools/Linux/
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.	Integration Configuration	ArcSight System/Tools/Linux/
Daily Pattern Discovery	This resource has no description.	Profile	ArcSight System
Quarter Hourly Pattern Discovery	This resource has no description.	Profile	ArcSight System
Chart and 2 Tables Landscape	This template is designed to show one chart and two tables. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With 2 Tables/
Chart and 2 Tables Portrait	This template is designed to show one chart and two tables. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With 2 Tables/
Four Charts and Table Landscape	This template is designed to show four charts and a table. The orientation is landscape.	Report Template	ArcSight System/4 Charts/With Table/
Simple Chart Portrait	This template is designed to show one chart. The orientation is portrait.	Report Template	ArcSight System/1 Chart/Without Table/
Three Charts Landscape	This template is designed to show three charts and a description field. The orientation is landscape.	Report Template	ArcSight System/3 Charts/Without Table/

Resources that Support the System Resources Group, continued

Resource	Description	Type	URI
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	ArcSight System/1 Chart/Without Table/
Two Charts Portrait	This template is designed to show two charts. The orientation is portrait.	Report Template	ArcSight System/2 Charts/Without Table/
Two Charts One Table Portrait	This template is designed to show two charts and a table. The orientation is portrait.	Report Template	ArcSight System/2 Charts/With Table/
Two Charts Landscape	This template is designed to show two charts and a description field. The orientation is portrait.	Report Template	ArcSight System/2 Charts/Without Table/
Two Charts One Table Landscape	This template is designed to show two charts and a table. The orientation is landscape.	Report Template	ArcSight System/2 Charts/With Table/
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table/
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	ArcSight System/1 Table/
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With Table/
Three Tables Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/3 Tables/
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table/
Two Tables Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/2 Tables/
Three Charts and Table Landscape	This template is designed to show three charts and a table. The orientation is landscape.	Report Template	ArcSight System/3 Charts/With Table/

Resources that Support the System Resources Group, continued

Resource	Description	Type	URI
Four Charts Landscape	This template is designed to show four charts. The orientation is landscape.	Report Template	ArcSight System/4 Charts/Without Table/
Two Tables Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	ArcSight System/2 Tables/
Closed	This stage indicates that the event is closed.	Stage	All Stages/
Queued	This stage indicates that the event has not been inspected.	Stage	All Stages/
Final	This stage indicates that the investigation has concluded.	Stage	All Stages/
Monitoring	This stage indicates further monitoring of an occurrence of this event or pattern.	Stage	All Stages/
Flagged as Similar	This stage indicates that the event is similar to an event already under investigation.	Stage	All Stages/
Follow-Up	This stage indicates that the event is under investigation.	Stage	All Stages/
Initial	This stage indicates that the event has been inspected.	Stage	All Stages/
Rule Created	This stage indicates that a rule was created to detect further occurrences of this event or pattern.	Stage	All Stages/

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 Core Security, ArcSight Administration and ArcSight System Standard Content Guide (ESM 6.8c)

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@hp.com.

We appreciate your feedback!