

Standard Content Guide

ArcSight System and ArcSight Administration

for ArcSight ESM 5.6

March 1, 2015



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

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.

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

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

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

Contact Information

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

Revision History

Date	Product Version	Description
03/01/2015	ESM 5.6	Updated for ESM 5.6

Contents

Chapter 1: Standard Content Overview	7
What is Standard Content?	7
Standard Content Packages	8
Chapter 2: Installation and Configuration	11
Installing the Content	11
Configuring the Content	11
Modeling the Network	12
Categorizing Assets	12
Configuring Active Lists	13
Enabling Rules	13
Ensuring Filters Capture Relevant Events	14
Configuring Notification Destinations	14
Configuring Notifications and Cases	14
Scheduling Reports	15
Configuring Trends	15
Monitoring Trend Performance	15
Chapter 3: ArcSight System Content	17
Actor Support Resources	18
Resources	18
Priority Formula Resources	22
Configuration	22
Resources	22
System Resources	29
Configuration	29
Resources	30
Chapter 4: ArcSight Administration Content	39
Connector Overview	41
Configuration	41
Resources	41
ESM Overview	46
Resources	46

Logger Overview	48
Configuration	48
Resources	49
Connector Configuration Changes	56
Resources	56
Connector Connection and Cache Status	61
Configuration	61
Resources	62
Device Monitoring	71
Configuration	71
Resources	72
ESM Licensing	79
Resources	79
ESM User Sessions	81
Resources	81
Actor Configuration Changes	84
Resources	84
ESM Resource Configuration Changes	92
Resources	92
ESM Events	95
Resources	95
ESM Reporting Resource Monitoring	101
Resources	101
ESM Resource Monitoring	107
Configuration	107
Resources	107
ESM Storage Monitoring (CORR)	115
Devices	115
Configuration	115
Resources	115
ESM Storage Monitoring (Oracle)	123
Devices	123
Configuration	123
Resources	123
Logger Events	130
Resources	130
Logger System Health	131
Configuration	131
Resources	132
Appendix A: Upgrading Standard Content	139
Preparing Existing Content for Upgrade	139
Configurations Preserved During Upgrade	139

Configurations that Require Restoration After Upgrade	139
Backing Up Existing Resources Before Upgrade	140
Performing the Upgrade	140
Checking and Restoring Content After Upgrade	140
Verifying and Reapplying Configurations	141
Verifying Customized Content	141
Fixing Invalid Resources	141

Chapter 1

Standard Content Overview

This chapter discusses the following topics.

["What is Standard Content?" on page 7](#)

["Standard Content Packages" on page 8](#)

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.

The standard content is installed using a series of packages, some of which are installed automatically with the 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 System** content is installed automatically with the Manager and 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.
- **ArcSight Administration** content is installed automatically with the Manager, and provides statistics about the health and performance of ArcSight products. ArcSight Administration is essential for managing and tuning the performance of content and components.
- **ArcSight Foundations** content (such as Configuration Monitoring, Intrusion Monitoring, Network Monitoring, NetFlow Monitoring, and Workflow) are presented as install-time options and 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.
- **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 are 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 are 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.
- ◆ Network filters are a set of filters required by ArcSight Administration and certain ArcSight Foundations, such as Intrusion Monitoring and Network Monitoring.

Standard Content Packages

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

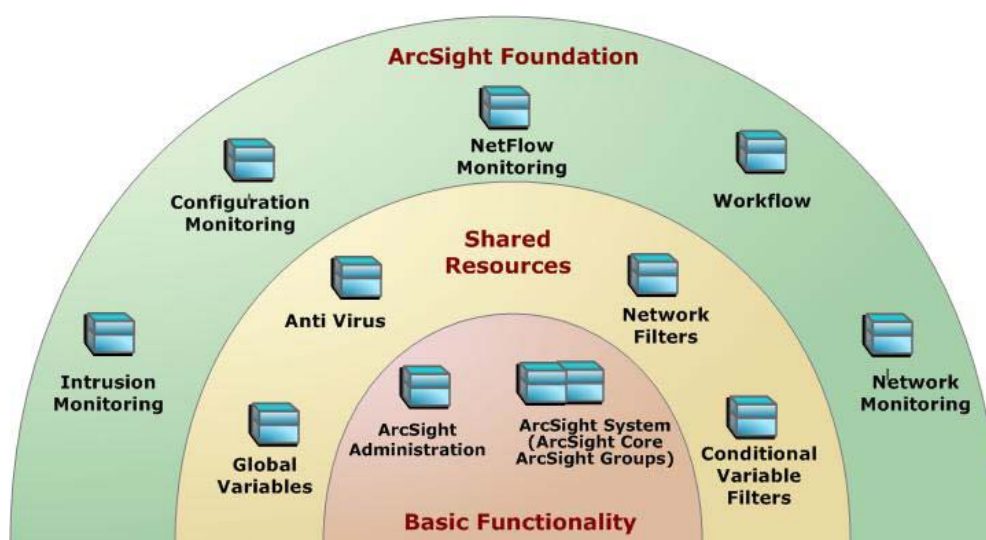


Figure 1-1 The ArcSight System and ArcSight Administration packages at the base provide content required for basic ArcSight functionality. The common packages in the center contain shared resources that support ArcSight Administration and the ArcSight Foundation packages. The packages shown on top are ArcSight Foundations that address common network security and management scenarios.

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



The ArcSight Express package is present in ESM installations, but is not installed by default. The package offers an alternate view of the Foundation resources. You can install or uninstall the ArcSight Express package without impact to the system.



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; for example, zones. 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*.

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

Chapter 2

Installation and Configuration

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

["Installing the Content" on page 11](#)

["Configuring the Content" on page 11](#)

Installing the Content

ArcSight System and ArcSight Administration contain content required for basic ArcSight functionality and are installed automatically with ArcSight ESM. You do not have to perform any additional installation tasks. However, some basic configuration is recommended to tailor the content for your operating environment. See [Configuring the Content](#), below.

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

Configuring the Content

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



This document organizes the ArcSight System and ArcSight Administration content into use cases, which group a set of resources that help address a specific issue or function. Configuration specific to a use case is described in the configuration section for that use case.

- ["Modeling the Network" on page 12](#)
- ["Categorizing Assets" on page 12](#)
- ["Configuring Active Lists" on page 13](#)
- ["Enabling Rules" on page 13](#)
- ["Ensuring Filters Capture Relevant Events" on page 14](#)
- ["Configuring Notification Destinations" on page 14](#)
- ["Configuring Notifications and Cases" on page 14](#)
- ["Scheduling Reports" on page 15](#)
- ["Configuring Trends" on page 15](#)

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 most 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* or the ESM online Help. To learn more about the architecture of the ESM 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 so that you can apply criticality and business context to events.

- Categorize all assets (or the zones to which the assets belong) that are internal to the network with the [/All Asset Categories/Site Asset Categories/Address Spaces/Protected](#) asset category.

Internal Assets are assets inside the company network. Assets that are not categorized as internal to the network are considered to be external. Make sure that you also categorize assets that have public addresses but are controlled by the organization (such as web servers) as *Protected*.



Assets with a private IP address (such as 192.168.0.0) are considered as *Protected* by the system, even if they are not categorized as such.

- Categorize all assets that are considered *critical* to protect (including assets that host proprietary content, financial data, cardholder data, top secret data, or perform functions critical to basic operations) with the [/All Asset Categories/System Asset Categories/Criticality/High](#) or [Very High](#) asset category.

The asset categories most essential to basic event processing are those used by the Priority Formula to calculate an event's criticality. Asset criticality is one of the four factors used by the priority formula to generate an overall event priority rating.

Asset categories can be assigned 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 Console tools, refer to the *ArcSight Console User's Guide* or the online Help.

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 cross-referenced by active channels, filters, rules, reports, and data monitors to give ESM 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 System active lists you need to configure manually, refer to the configuration information for each use case presented in [Chapter 3, ArcSight System 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 [Chapter 4, ArcSight Administration Content, on page 39](#).

Enabling Rules

ESM rules trigger only if they are deployed in the [Real-Time Rules](#) group and are enabled.

- By default, all the 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 a few are 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.

For a list of the ArcSight Administration rules you need to enable, refer the configuration information for each use case presented in [Chapter 4, ArcSight Administration Content, on page 39](#).

Ensuring Filters Capture Relevant Events

Standard content relies on specific event field values to identify events of interest. Although this method applies to most of the events and devices, be sure to test key filters to verify that they actually capture the required events.

To ensure that a filter captures relevant events:

- 1** Generate or identify the required events and verify that they are being processed by viewing them in an active channel or query viewer.
- 2** Navigate to the appropriate filter, right-click the filter and choose **Create Channel with Filter**. If you see the events of interest in the newly created channel, the filter is functioning properly.

If you do not see the events of interest:

- a** Verify that the configuration of the active channel is suitable for the events in question. For example, ensure that the event time is within the start and end time of the channel.
- b** Modify the filter condition to capture the events of interest. After applying the change, repeat [Step 2](#) to verify that the modified filter captures the required events.

For a list of the ArcSight System filters you need to configure, refer to the configuration information for each use case presented in [Chapter 3, ArcSight System Content, on page 17](#).

For a list of the ArcSight Administration filters you need to configure, refer to the configuration information for each use case presented in [Chapter 4, ArcSight Administration Content, on page 39](#).

Configuring Notification Destinations

Configure notification destinations if you want to be notified when some of the standard content rules are triggered. By default, notifications are disabled in the standard content rules, so the admin user needs to configure the destinations *and* enable the notification in the rules. For details about enabling the notifications in rules, see [Configuring Notifications and Cases](#), below.

ArcSight System and ArcSight Administration rules reference two notification groups: CERT Team and SOC Operators. Add new destinations for notification levels 1, 2, and 3 as appropriate to the personnel in your security operations center. See the *ArcSight Console User's Guide* or the online Help for more details.

Configuring Notifications and Cases

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

By default, the notifications and create case actions are disabled in the standard content rules that send notifications about security-related events to the Cert Team notification group. However, for ArcSight Administration content, notifications are enabled for the SOC Operators notification group, but case creation is disabled.

To enable rules to send notifications and open cases, first configure notification destinations, then enable the notification and case actions in the rules. Refer to the

ArcSight Console User's Guide or the online Help for details about enabling notifications and opening cases.

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 ArcSight System and ArcSight Administration, 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* or the online Help.

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 Administration content includes several 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 backfills 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* or the ESM online Help.

Monitoring Trend Performance

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.

Chapter 3

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" on page 18	The Actor Support Resources group includes resources that support the ESM actors feature. The ESM 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 on your network.
"Priority Formula Resources" on page 22	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 29	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 ESM actors feature. The ESM 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 on 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*.



Actors are a licensed feature so they do not apply to every environment.

Resources

The following table lists the information presentation and data processing resources that support the Actor Support Resources group.

Table 3-1 Resources that Support the Actor Support Resources Use Case

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/

Resource	Description	Type	URI
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.	Asset Category	ArcSight System
ActorByAccountID	This global 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 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
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/Event Fields/
createTime	This resource has no description.	Global Variable	ArcSight System/Actor Fields

Resource	Description	Type	URI
alias	This resource has no description.	Global Variable	ArcSight System/Actor Fields
ActorByTarget Username	This global 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
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/
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/

Resource	Description	Type	URI
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/

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*, the *ESM 101* guide, or the ESM online Help.

Configuration

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 13](#).



Note

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

Resources

The following table lists the information presentation and data processing resources that support the Priority Formula Resources group.

Table 3-2 Resources that Support the Priority Formula Resources Use Case

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 active list and the target address is added to the /Scanned active list.	Rule	ArcSight System/Threat Tracking/Reconnaissance/

Resource	Description	Type	URI
Reconnaissance - Network Service Scan	This rule detects a single source that scans multiple targets on the same port or service. This rule triggers when three events occur within five minutes with the same target port and attacker address, but with a different target host name each time. On the first threshold, the attacker is added to the /Reconnaissance active list and the target is added to the /Scanned active list.	Rule	ArcSight System/Threat Tracking/Reconnaissance/
Reconnaissance - Distributed Host Port Scan	This rule detects port scans on a host by different attackers. The rule triggers when three events occur within five minutes detected by the same device with the same target, but with a different attacker address and zone resource each time. On the first threshold, the target address is added to the /Scanned active list.	Rule	ArcSight System/Threat Tracking/Reconnaissance/
Reconnaissance - Stealthy Host Port Scan	This rule detects a stealthy host port scan. It correlates two events: Stealthy_packet, which monitors any anomaly in the transport layer protocol, and Host_Port_Scan, which monitors port scans on an host. The correlation implies that the two events have the same attacker and target, and Stealthy_packet starts before Host_Port_Scan. The rule triggers whenever four correlated events occur within one minute with the same attacker and target pair, but the target source port is different each time. The rule does not trigger if the attacker is on a trusted active list. On the first threshold, the attacker is added to the /Reconnaissance active list and the target is added to /Scanned active list.	Rule	ArcSight System/Threat Tracking/Reconnaissance/
Reconnaissance - Multiple Host Scan	This rule detects port scans by looking for many scan events from the same source against multiple targets on the same network within a short period of time. Note: This rule does not trigger when running in Turbo Mode Fastest.	Rule	ArcSight System/Threat Tracking/Reconnaissance/

Resource	Description	Type	URI
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, 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 System/Threat Tracking/Compromise/
Reconnaissance - Distributed Network Host Scan	This rule detects port scans on a host by different attackers. The rule triggers when three events are detected by the same device within five minutes with the same target, but with a different attacker address and zone each time. On the first threshold, the target address is added to the /Scanned active list.	Rule	ArcSight System/Threat Tracking/Reconnaissance/
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 active list, and the target address is added to the /Hit active list."	Rule	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 first event agent, severity is set to medium, the attacker address is added to the /Hostile active list, and the target address is added to the /Hit active list."	Rule	ArcSight System/Threat Tracking/Hostile/

Resource	Description	Type	URI
Reconnaissance - Script Scan	This rule detects potential script vulnerability scans based on multiple events from a single attacker to a single target where the event names differ and the events are categorized as script attacks. Note: This rule does not trigger when running in Turbo Mode Fastest.	Rule	ArcSight System/Threat Tracking/Reconnaissance/
Reconnaissance - Vulnerability Scan	This rule detects vulnerability scans. The rule monitors events with the vulnerability ID field set, which indicates an access or execution attempt. The rule triggers when five events occur within two minutes with the same attacker and target pair, but when the vulnerability ID is different each time. The rule does not trigger if the attacker is listed on a trusted active list. On the first threshold, the attacker is added to the /Reconnaissance active list. On the time window expiration, the target is added to the /Scanned active list.	Rule	ArcSight System/Threat Tracking/Reconnaissance/
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 active list, and the target address is added to the /Hit active list."	Rule	ArcSight System/Threat Tracking/Compromise/
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 last state data monitor (in the Executive View dashboard), which is sent when a user marks an asset within the data monitor as resolved.	Rule	ArcSight System/Threat Tracking/Compromise/
Library Resources			
Hit List	This resource has no description.	Active List	ArcSight System/Targets/
Suspicious List	This resource has no description.	Active List	ArcSight System/Threat Tracking/
Hostile List	This resource has no description.	Active List	ArcSight System/Threat Tracking/
Compromised List	This resource has no description.	Active List	ArcSight System/Threat Tracking/

Resource	Description	Type	URI
Infiltrators List	This resource has no description.	Active List	ArcSight System/Threat Tracking/
Trusted List	This resource has no description.	Active List	ArcSight System/Attackers/
Untrusted List	This resource has no description.	Active List	ArcSight System/Attackers/
Scanned List	This resource has no description.	Active List	ArcSight System/Targets/
Reconnaissance List	This resource has no description.	Active List	ArcSight System/Threat Tracking/
High	The disruption of access to or use of information or an information system 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/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 or 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 or 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

Resource	Description	Type	URI
Criticality	This is a system asset category.	Asset Category	System Asset Categories
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 resource has no description.	Filter	ArcSight System/Core/Threat Level Filters/
High Criticality Assets	This resource has no description.	Filter	ArcSight System/Core/Threat Level Filters/
Unknown Criticality Assets	This resource has no description.	Filter	ArcSight System/Core/Threat Level Filters/
Very Low Criticality Assets	This resource has no description.	Filter	ArcSight System/Core/Threat Level Filters/

Resource	Description	Type	URI
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 resource has no description.	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 resource has no description.	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.

Configuration

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 ESM creates assets in the ArcSight 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 filter [/All Filters/ArcSight System/Event Types/ArcSight Correlation Events](#). 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*.

Resources

The following table lists the information presentation and data processing resources that support the System Resources group.

Table 3-3 Resources that Support the System Resources Use Case

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

Resource	Description	Type	URI
System Events Last Hour	This active channel shows all events generated during the last hour. A filter prevents the channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events.	Active Channel	ArcSight Administration/
Vulnerabilities of an Asset	This resource has no description.	Report	ArcSight System/Core/
Assets having Vulnerability	This resource has no description.	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/
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 resource has no description.	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-MgrRcpt	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

Resource	Description	Type	URI
Export	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Active Channels
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 resource has no description.	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 resource has no description.	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, focused 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
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 resource has no description.	Filter	ArcSight System/Event Types/
Manager Internal AgentsFilters'	This filter looks for events coming from the Manager Internal Agent.	Filter	ArcSight System/Connector Filters/
Severity Very High	This resource has no description.	Filter	ArcSight System/Event Types/

Resource	Description	Type	URI
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/
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 resource has no description.	Filter	ArcSight Administration/ESM/System Health/
All Events	This filter matches all events.	Filter	ArcSight System/Core/
ArcSight Events	This resource has no description.	Filter	ArcSight System/Event Types/
ArcSight Correlation Events	This resource has no description.	Filter	ArcSight System/Event Types/
Severity Low	This resource has no description.	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 resource has no description.	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 resource has no description.	Filter	ArcSight System/Event Types/

Resource	Description	Type	URI
Severity High	This resource has no description.	Filter	ArcSight System/Event Types/
Non-ArcSight Internal Events	This resource has no description.	Filter	ArcSight System/Event Types/
Severity Unknown	This resource has no description.	Filter	ArcSight System/Event Types/
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 resource has no description.	Filter	ArcSight System/Event Types/
Severity Medium	This resource has no description.	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, the device vendor, and the device product in the selected event.	Integration Command	ArcSight System/Tools/
Nslookup (Linux)	This integration command is used to find details related to the Domain Name System (DNS). Run this command from a Linux console.	Integration Command	ArcSight System/Tools/Linux/
Nslookup (Windows)	This integration command is used to find details related to 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 related to 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/

Resource	Description	Type	URI
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 related to 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/
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/

Resource	Description	Type	URI
Web Search	This integration configuration is used to configure the web search command. You can run the command on any cell selected in the viewer.	Integration Configuration	ArcSight System/Tools/
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/
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/

Resource	Description	Type	URI
Daily Pattern Discovery	This resource has no description.	Profile	ArcSight System/
Quarter Hourly Pattern Discovery	This resource has no description.	Profile	ArcSight System/
Closed	This stage indicates that the event is closed.	Stage	/
Queued	This stage indicates that the event has not been inspected.	Stage	/
Final	This stage indicates that the investigation has concluded.	Stage	/
Monitoring	This stage indicates further monitoring of an occurrence of this event or pattern.	Stage	/
Flagged as Similar	This stage indicates that the event is similar to an event already under investigation.	Stage	/
Follow-Up	This stage indicates that the event is under investigation.	Stage	/
Initial	This stage indicates that the event has been inspected.	Stage	/
Rule Created	This stage indicates that a rule was created to detect further occurrences of this event or pattern.	Stage	/

Chapter 4

ArcSight Administration Content



The ArcSight Administration foundation is a coordinated set of resources that provide statistics about the health and performance of ArcSight ESM and its components. This foundation is essential for managing and tuning ESM performance.

The ArcSight Administration resources are grouped together using 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.



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 41	The Connector Overview use case provides administration content for monitoring connectors and devices.
"ESM Overview" on page 46	The ESM Overview use case provides administration content for monitoring ESM.
"Logger Overview" on page 48	The Logger Overview use case provides Logger status and statistics.
Connectors	
"Connector Configuration Changes" on page 56	The Connector Configuration use case provides information about configuration changes, such as upgrades and the versions of the connectors on the system.
"Connector Connection and Cache Status" on page 61	The Connector Connection and Cache Status use case provides the connection status and caching status of connectors in the system. Connectors can be connected directly to ESM or through Loggers.
"Device Monitoring" on page 71	The Device Monitoring use case provides information about the devices reporting to ESM.
ESM	
"ESM Licensing" on page 79	The ESM Licensing use case provides information about ESM licensing compliance.

Use Case	Purpose
"ESM User Sessions" on page 81	The ESM User Sessions use case provides information about user access to ESM.
ESM - Configuration Changes	
"Actor Configuration Changes" on page 84	The Actor Configuration Changes use case provides information about changes to the actor resources.
"ESM Resource Configuration Changes" on page 92	The ESM Resource Configuration Changes use case provides information about changes to the various ESM resources, such as rules, reports, and so on.
ESM - System Health	
"ESM Events" on page 95	The ESM Events use case provides statistics on the flow of events through ESM.
"ESM Reporting Resource Monitoring" on page 101	The ESM Reporting Resource Monitoring use case provides performance statistics for reports, trends, and query viewers.
"ESM Resource Monitoring" on page 107	The ESM Resource Monitoring use case provides processing statistics for various ESM resources, such as trends, rules, and so on.
"ESM Storage Monitoring (CORR)" on page 115	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 123	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 the CORR Engine.
Logger	
"Logger Events" on page 130	The Logger Events use case provides statistics for events sent through Loggers to ESM.
"Logger System Health" on page 131	The Logger System Health use case provides performance statistics for the Loggers connected to ESM.

Connector Overview

The Connector Overview use case provides administration content for monitoring connectors and devices.

Configuration

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 61.](#)

Resources

The following table lists the information presentation and data processing resources that support the Connector Overview use case.

Table 4-1 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 twenty 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/

Resource	Description	Type	URI
Connectors - Down - Long Term	This query viewer displays data on connectors that have been down for longer than twenty 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/
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 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/

Resource	Description	Type	URI
Connectors - Still Caching	This active list maintains the 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, the cache is full). A connector is removed from the active list when the cache is empty again.	Active List	ArcSight Administration/Connectors/System Health/
Connectors - Down	This active list stores the IDs and names of connectors that are currently down (either the connector shut down or there was a heartbeat timeout for that connector). 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. A connector is removed from the active list when it starts again 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 the connector shut down or there was a heartbeat timeout for that connector). 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. A connector is removed from the active list when it starts again 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/
Top Event Sources	This data monitor tracks the most common event generating products and displays a listing of the top 20.	Data Monitor	ArcSight Administration/Connectors/System Health/Current Event Sources/

Resource	Description	Type	URI
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 have been 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/
Connector Cache Status	This filter detects correlation events from the Update Connector Caching Status rule.	Filter	ArcSight Administration/Connectors/System Health/
Connector Connection Status	This filter detects correlation events related to connector connection status.	Filter	ArcSight Administration/Connectors/System Health/
ArcSight Events	This resource has no description.	Filter	ArcSight System/Event Types/
Non-ArcSight Events	This resource has no description.	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 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 twenty minutes (by default). The queries are on an active list that is maintained by the Connector Monitoring content (rules).	Query	ArcSight Administration/Connectors/System Health/Connector Monitoring/

Resource	Description	Type	URI
Connectors - Still Down	This query identifies data on connectors that have been down for longer than twenty minutes (by default). The query is on an active list that is maintained by the Connector Monitoring content (rules).	Query	ArcSight Administration/Connectors/System Health/Connector Monitoring/
Connectors - Caching - Long Term	This query identifies data on connectors that have been caching for more than two hours (by default). The query is 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 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 SmartConnector 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 ESM.

Resources

The following table lists the information presentation and data processing resources that support the ESM Overview use case.

Table 4-2 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 during the last hour. A filter prevents the channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events.	Active Channel	ArcSight Administration/
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 resource has no description.	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
ArcSight Internal Events	This resource has no description.	Filter	ArcSight System/Event Types/
ASM Events	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/

Resource	Description	Type	URI
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 later).	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 Storage Monitoring (Oracle)	This use case provides information about the health of the Oracle database.	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.

Configuration

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

- 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 13](#).

- 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 [Table 4-3 on page 49](#)).
 - ◆ **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*.

Resources

The following table lists the information presentation and data processing resources that support the Logger Overview use case.

Table 4-3 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, 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/
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			

Resource	Description	Type	URI
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/
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/
Network Usage (Bytes) - Last 10 Minutes	This data monitor shows the network usage 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/
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/

Resource	Description	Type	URI
CPU Usage (Percent) - Last 10 Minutes	This data monitor shows the CPU usage 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/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 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/
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 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/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 Status	This resource has no description.	Global Variable	ArcSight Administration/Logger/
Sensor Name	This resource has no description.	Global Variable	ArcSight Administration/Logger/
Free Space	This resource has no description.	Global Variable	ArcSight Administration/Logger/
Timeframe	This resource has no description.	Global Variable	ArcSight Administration/Logger/
Disk Usage	This resource has no description.	Global Variable	ArcSight Administration/Logger/
DiskUsageCritical	This resource has no description.	Global Variable	ArcSight Administration/Logger/
ReadOrWrite	This resource has no description.	Global Variable	ArcSight Administration/Logger/

Resource	Description	Type	URI
Disk Name	This resource has no description.	Global Variable	ArcSight Administration/Logger/
IndexOfUsage	This resource has no description.	Global Variable	ArcSight Administration/Logger/
Inbound and Outbound	This resource has no description.	Global Variable	ArcSight Administration/Logger/
Field Value	This resource has no description.	Global Variable	ArcSight Administration/Logger/
Unit	This resource has no description.	Global Variable	ArcSight Administration/Logger/
Logger IP	This resource has no description.	Global Variable	ArcSight Administration/Logger/
Memory Name	This resource has no description.	Global Variable	ArcSight Administration/Logger/
All Receivers and Forwarders	This resource has no description.	Global Variable	ArcSight Administration/Logger/
Logger Address	This resource has no description.	Global Variable	ArcSight Administration/Logger/
Sensor Type	This resource has no description.	Global Variable	ArcSight Administration/Logger/
CPU Name	This resource has no description.	Global Variable	ArcSight Administration/Logger/
Field Status	This resource has no description.	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 is designed for conditional expression variables. The filter passes events where 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/

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 is designed for conditional expression variables. The filter passes events where the device event category is "/Monitor/Receiver/All/EPS".	Filter	ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/
Sensor Type is FAN	This filter is designed for conditional expression variables. The filter passes events where 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 > 10 Percent	This filter is designed for conditional expression variables. The filter passes events where the remaining disk space is greater than 10 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/

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/
ArcSight Correlation Events	This resource has no description.	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/
Inbound Network	This filter is designed for conditional expression variables. The filter passes events where the device event category ends with "/In".	Filter	ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/
Remaining Disk < 5 Percent	This filter is designed for conditional expression variables. The filter passes events where the remaining disk space is less than 5 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 in 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 in 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 in the last two hours.	Integration Command	ArcSight Administration/Logger/
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 in the last two hours.	Integration Command	ArcSight Administration/Logger/

Resource	Description	Type	URI
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 in 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 in 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 in 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/
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 use case provides information about configuration changes, such as upgrades and the versions of the connectors on the system.

Resources

The following table lists the information presentation and data processing resources that support the Connector Configuration use case.

Table 4-4 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/
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 of failure.	Report	ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Upgrade History by Connector	This report shows the upgrade history by SmartConnector (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/

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 SmartConnectors 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 reports 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 SmartConnector 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			
Connector Upgrade Failed	This rule detects failed connector upgrades. On the first event, the connector ID, name, version, type, address, zone, and reason of failure are 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 identifies connector start events. The rule triggers if the connector is not yet in the Connector Versions session list. On the first event, a new session with the connector ID, name, version, type, address, and zone is created in the Connector Versions session list.	Rule	ArcSight Administration/Connectors/Configuration Changes/

Resource	Description	Type	URI
Connector Upgrade Successful	"This rule detects successful connector upgrades. On the first event, the connector ID, name, new version, type, address, and zone are 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 maintains the available information about connectors that have been caching for over two hours (by default).	Active List	ArcSight Administration/Connectors/System Health/
Connector Upgrades	This active list stores information related to successful and failed connector upgrades. When an upgrade is successful, the active list stores the Upgrade Time, Connector ID, Connector Name, Connector Version, Connector Type, Connector Address, and Connector Zone. When an upgrade fails, the active list also stores the reason for the failure. The active list is populated by the Connector Upgrade Failed and Connector Upgrade Successful rules.	Active List	ArcSight Administration/Connectors/Configuration Changes/

Resource	Description	Type	URI
Connectors - Down	This active list stores the IDs and names of connectors that are currently down (either the connector shut down or there was a heartbeat timeout for that connector). 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. A connector is removed from the active list when it starts again 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 the connector shut down or there was a heartbeat timeout for that connector). 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. A connector is removed from the active list when it starts again 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
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/

Resource	Description	Type	URI
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/
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 of 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/
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 connectors in the system. Connectors can be connected directly to ESM or through Loggers.

Configuration

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 2 hours. A SmartConnector that has been caching for fewer than 2 hours is considered to be caching for a short term. Connectors caching for up to 2 hours are not considered to be a problem. After 2 hours, the entry for this active list expires and the connector information is moved to the **Connectors - Still Caching** active list, unless the connector cache is emptied in fewer than two hours, and it is removed by the Connector Cache Empty rule.
 - ◆ Populate the **Black List - Connectors** active list with the URI and IP address of each 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 SupportInformation 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 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 13](#).

- 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*.

Resources

The following table lists the information presentation and data processing resources that support the Connector Connection and Cache Status use case.

Table 4-5 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/
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 twenty 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/

Resource	Description	Type	URI
Connectors - Down - Long Term	This query viewer displays data on connectors that have been down for longer than twenty 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/
Cache History by Connectors	This report shows the cache history by connector (within the last 24 hours by default) sorted chronologically. Notes: When running this report, you can specify the Connector URI (located in the connector resource navigator or the Connector Information active list) in the ConnectorURI field in the custom parameters for the report. By default, the report reports on 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 for the past 3-4 months.	Report	ArcSight Administration/Connectors/System Health/Cache/
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

Resource	Description	Type	URI
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/
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/
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 into 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 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/
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 device custom number and string information to be used by the Connector Cache Status data monitor.	Rule	ArcSight Administration/Connectors/System Health/

Resource	Description	Type	URI
Connector Version Detected	This rule identifies connector start events. The rule triggers if the connector is not yet in the Connector Versions session list. On the first event, a new session with the connector ID, name, version, type, address, and zone is created in the Connector Versions session list.	Rule	ArcSight Administration/Connectors/Configuration Changes/
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/
Connector Down	This rule triggers when 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/
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 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/
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/

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 List.	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 maintains the 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, the cache is full). A connector is removed from the active list when the cache is empty again.	Active List	ArcSight Administration/Connectors/System Health/

Resource	Description	Type	URI
Connectors - Down	This active list stores the IDs and names of connectors that are currently down (either the connector shut down or there was a heartbeat timeout for that connector). 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. A connector is removed from the active list when it starts again 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 the connector shut down or there was a heartbeat timeout for that connector). 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. A connector is removed from the active list when it starts again or reconnects.	Active List	ArcSight Administration/Connectors/System Health/
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 on 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 to 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/

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/
Connector Connection Status	This data monitor shows the current status of the connector connections across all connectors. If one or more connectors have been 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/

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 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 twenty minutes (by default). The queries are 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 twenty minutes (by default). The query is on an active list that is maintained by the Connector Monitoring content (rules).	Query	ArcSight Administration/Connectors/System Health/Connector Monitoring/
Connectors - Caching - Long Term	This query identifies data on connectors that have been caching for more than two hours (by default). The query is 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 on an active list that is maintained by the Connector Monitoring content (rules).	Query	ArcSight Administration/Connectors/System Health/Cache/

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 ESM.

Configuration

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 `/All Asset Categories/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 (`All Asset Categories/System Asset Categories/Criticality/High`).

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

- 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 ["Enabling Rules" on page 13](#).

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 14](#).

- 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*.

Resources

The following table lists the information presentation and data processing resources that support the Device Monitoring use case.

Table 4-6 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 resource has no description.	Report	ArcSight Administration/Connectors/System Health/Event Breakdown/
Connector Severity Hourly Stacked Chart	This resource has no description.	Report	ArcSight Administration/Connectors/System Health/Event Breakdown/
Events by Connector Type (Summary)	This resource has no description.	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/

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 resource has no description.	Report	ArcSight Administration/Connectors/System Health/Event Breakdown/
Source Counts by Connector Type	This report displays a table that 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 resource has no description.	Report	ArcSight Administration/Connectors/System Health/Event Breakdown/
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/

Resource	Description	Type	URI
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 resource has no description.	Report	ArcSight Administration/Connectors/System Health/Event Breakdown/
Events from a Source by Connector Type	This report displays a table of all events showing time, destination, and connector information based on the Attacker Zone and Attacker Address fields. These fields are used as the source of the events, and default to RFC1918: 192.168.0.0-192.168.255.255 and 192.168.10.10. You can 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/
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/

Resource	Description	Type	URI
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 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
Top Event Sources	This data monitor tracks 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/
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/

Resource	Description	Type	URI
ArcSight Events	This resource has no description.	Filter	ArcSight System/Event Types/
Non-ArcSight Events	This resource has no description.	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 the following correlation events: Critical Device Reported and Critical Device Not Reporting.	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/
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 resource has no description.	Query	ArcSight Administration/Connectors/System Health/Event Breakdown/
Connector Monitor Event	This query identifies the total number of events that connectors forward to the Manager per hour.	Query	ArcSight Administration/Connectors/System Health/EPS/
Event Distribution Chart for a Connector Type	This resource has no description.	Query	ArcSight Administration/Connectors/System Health/Event Breakdown/

Resource	Description	Type	URI
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/
Events by Selected Connector Type	This resource has no description.	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 the 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 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/
Events by Connector Type (Summary)	This resource has no description.	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 resource has no description.	Query	ArcSight Administration/Connectors/System Health/Event Breakdown/

Resource	Description	Type	URI
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/
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/
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 last seven days and writes the data to an active list by leveraging the trend action feature.	Trend	ArcSight Administration/Connector/System Health/EPS/

ESM Licensing

The ESM Licensing use case provides information about ESM licensing compliance.

Resources

The following table lists the information presentation and data processing resources that support the ESM Licensing use case.

Table 4-7 Resources that Support the ESM Licensing Use Case

Resource	Description	Type	URI
Monitor Resources			
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/
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			
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/
License Limit Approaching	This rule triggers when one of the licensed features approaches the allowed limit. The rule triggers when the current count is over 90% of the allowed limit.	Rule	ArcSight Administration/ESM/Licensing/
License Limit Exceeded	This rule triggers when one of the licensed features exceeds the allowed limit. A notification is sent when this happens. The notification is disabled by default.	Rule	ArcSight Administration/ESM/Licensing/
Library Resources			
admindcert	This destination is pre-defined for the CERT team. Add more information, such as email addresses.	Destination	CERT Team/1/

Resource	Description	Type	URI
Assets Licensing Report	This report shows the licensing history for assets. The chart shows the current count and the count limit in a chart. 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. The chart shows the current count and the count limit in a chart. By default, the licensing history is over the last seven days.	Focused Report	ArcSight Administration/ESM/Licensing/
Web Users Licensing Report	This report shows the licensing history for web users. The chart shows the current count and the count limit in a chart. 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. The chart shows the current count and the count limit in a chart. By default, the licensing history is over the last seven days.	Focused Report	ArcSight Administration/ESM/Licensing/
EPS Licensing Report	This report shows the licensing history for EPS. The chart shows the current count and the count limit in a chart. 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. The chart shows the current count and the count limit in a chart. By default, the licensing history is over the last seven days.	Focused Report	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/
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/

ESM User Sessions

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

Resources

The following table lists the information presentation and data processing resources that support the ESM User Sessions use case.

Table 4-8 Resources that Support the ESM User Sessions Use Case

Resource	Description	Type	URI
Monitor Resources			
Console and ArcSight Web Status	This resource has no description.	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 in the previous day. The report contains a bar chart and a table. The bar chart shows the total number of logins by user and the table shows the number of logins by user per hour.	Report	ArcSight Administration/ESM/User Access/User Sessions/
User Login Logout Report	This resource has no description.	Report	ArcSight Administration/ESM/User Access/User Sessions/
ArcSight User Logins - Last Hour	This report shows the 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			
ArcSight User Logout	This rule identifies 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/

Resource	Description	Type	URI
ArcSight User Login	This rule identifies ArcSight user login events. This rule adds the user name, the attacker address, the attacker zone, and the login time to the ArcSight User Sessions session list. The user name of the user logging in is mapped to the file name field for login events.	Rule	ArcSight Administration/ESM/User Access/User Sessions/
ArcSight User Login Timeout	This rule identifies 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 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 resource has no description.	Data Monitor	ArcSight Administration/ESM/User Access/User Sessions/Console and ArcSight Web Status/
User Access Log	This 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 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/
ArcSight Login Tracking	This filter identifies events that contain ArcSight login and logout information. The deviceEventCategory used in this filter is generated by the ArcSight User Login, ArcSight User Login Timeout, and ArcSight User Logout rules.	Filter	ArcSight Administration/ESM/User Access/User Sessions/
Notification Actions	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/Events/Event Flow/

Resource	Description	Type	URI
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 resource has no description.	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 resource has no description.	Query	ArcSight Administration/ESM/User Access/User Sessions/
ArcSight User Hourly Login Trends	This query on the ArcSight User Login Trends - Hourly trend selects 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/
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 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 over 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.

Resources

The following table lists the information presentation and data processing resources that support the Actor Configuration Changes use case.

Table 4-9 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/
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 the 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/

Resource	Description	Type	URI
Actor Full Name and Email Changes	This query viewer displays information from actor audit events that result from changes to the Full Name or Email attribute of an actor. This query viewer shows the old and the new information.	Query Viewer	ArcSight Administration/ESM/Configuration Changes/Actor/
Actor Title and Status Changes	This query viewer displays information from actor audit events that results 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/
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 in a table. The 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 the 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/

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 in a table. The 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 for 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/
Department New Value	This global variable extracts the new value for the 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 the 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 the Full Name in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/

Resource	Description	Type	URI
Org New Value	This global variable extracts the new value for the 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 the Title in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/
ActorFromFile Name	This global variable selects the actor based on the value in the file name. It is intended to be used with actor audit events.	Global Variable	ArcSight Administration/ESM/Actor/
Location Old Value	This global variable extracts the old value for the Location in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/
Change Source	This resource has no description.	Global Variable	ArcSight Administration/ESM/Actor/
Manager New Value	This global variable extracts the new value for the Manager in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/
Actor	This resource has no description.	Global Variable	ArcSight Administration/ESM/Actor/
Employee Type Old Value	This global variable extracts the old value for the 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 the 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 the Location in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/

Resource	Description	Type	URI
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 will not show a placeholder. Examples: RFC1918: 192.168.0.0-192.168.255.255 Itwiki.sv.arcsight.com 192.168.10.20:80 RFC1918: 192.168.0.0-192.168.255.255 192.168.10.30:53 RFC1918: 192.168.0.0-192.168.255.255:53 192.168.10.30:53 unknown	Global Variable	ArcSight Foundation/Variables Library/Host Information/
Manager Old Value	This global variable extracts the old value for the 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 the Email Address 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 the Email Address in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/
Status New Value	This global variable extracts the new value for the Status 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 the 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 the 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 the 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 the Title in actor update audit events (single-value parameters).	Global Variable	ArcSight Administration/ESM/Actor/

Resource	Description	Type	URI
Department Old Value	This global variable extracts the old value for the 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/
Attacker Information is NULL	This variable is designed to be used by variables to select events where 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 adding or deleting 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 variable is designed to be used by variables to select events where either the attacker zone or attacker host name field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Zone is NULL	This variable is designed to be used by variables to select events where the attacker zone field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Port is NULL	This variable is designed to be used by variables to select events where 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/
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	This variable is designed to be used by variables to select events where the attacker zone and attacker address fields are NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/

Resource	Description	Type	URI
Attacker Zone AND Host are NULL but Address is NOT NULL	This variable is designed to be used by variables to select events where either the attacker zone or attacker address field is NULL, but not both.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Host Name is NULL	This variable is designed to be used by variables to select events where the attacker host name field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target User Name is NULL	This filter is designed for conditional expression variables. It passes events where the Target User Name is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/User/
Attacker Address is NULL	This variable is designed to be used by variables to select events where 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 the list of all the authenticators for actors.	Query	ArcSight Administration/ESM/Configuration Changes/Actors/
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/

Resource	Description	Type	URI
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/
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/

ESM Resource Configuration Changes

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

Resources

The following table lists the information presentation and data processing resources that support the ESM Resource Configuration Changes use case.

Table 4-10 Resources that Support the ESM Resource Configuration Changes Use Case

Resource	Description	Type	URI
Monitor Resources			
Resource Change Log	This resource has no description.	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 in a table. The 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/
Resource History Report	This report shows a list of all the resources that have been created, updated, or deleted 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 Type	This report shows recent ArcSight ESM configuration changes in a table. The 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	Description	Type	URI
Resource Updated Report	This report shows a list of all the resources updated 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/
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/
Resource Change Overview	This data monitor shows an overview of the ArcSight resource changes (the total number of changes by type for 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 resource has no description.	Filter	ArcSight Administration/ESM/Configuration Changes/Resource Update Tracking/
Resource Updates	This resource has no description.	Filter	ArcSight Administration/ESM/Configuration Changes/Resource Update Tracking/
Resource Deletes	This resource has no description.	Filter	ArcSight Administration/ESM/Configuration Changes/Resource Update Tracking/
Target User Name is NULL	This filter is designed for conditional expression variables. It passes events where the Target User Name is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/User/
Resource Changes	This resource has no description.	Filter	ArcSight Administration/ESM/Configuration Changes/Resource Update Tracking/
All Events	This filter matches all events.	Filter	ArcSight System/Core/

Resource	Description	Type	URI
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/
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/

ESM Events

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

Resources

The following table lists the information presentation and data processing resources that support the ESM Events use case.

Table 4-11 Resources that Support the ESM Events Use Case

Resource	Description	Type	URI
Monitor Resources			
ASM Events	This resource has no description.	Active Channel	ArcSight Administration/ESM/System Health/Events/
System Events Last Hour	This active channel shows all events generated during the last hour. A filter prevents the channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events.	Active Channel	ArcSight Administration/
Latest Events By Priority	This resource has no description.	Dashboard	ArcSight Administration/ESM/System Health/Events/
Event Throughput	This dashboard displays the Event Throughput and Event Throughput Statistics data monitors, providing an overview of the system activity related to the connectors.	Dashboard	ArcSight Administration/ESM/System Health/Events/
Top 10 Inbound Events	This resource has no description.	Report	ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart)	This resource has no description.	Report	ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Top 10 Events	This resource has no description.	Report	ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Source Counts by Event Name	This resource has no description.	Report	ArcSight Administration/ESM/System Health/Events/
Event Name Counts	This resource has no description.	Report	ArcSight Administration/ESM/System Health/Events/

Resource	Description	Type	URI
Hourly Event Counts (Area Chart)	This resource has no description.	Report	ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Destination Counts	This resource has no description.	Report	ArcSight Administration/ESM/System Health/Events/
Hourly Distribution Chart for Event	This resource has no description.	Report	ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Hourly Distribution Chart for a Source Port	This resource has no description.	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 resource has no description.	Report	ArcSight Administration/ESM/System Health/Events/
Hourly Distribution Chart for a Destination Port	This resource has no description.	Report	ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Event Count by Source Destination Pairs	This resource has no description.	Report	ArcSight Administration/ESM/System Health/Events/
Top 10 Outbound Events	This resource has no description.	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/

Resource	Description	Type	URI
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 resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/
Latest Low Threat Events	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/
Latest High Threat Events	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/
Latest Severe Threat Events	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/
Event Throughput Statistics	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Events/Event Throughput/
Event Throughput	This data monitor shows the average EPS (events per second) for all the events over 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 resource has no description.	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 resource has no description.	Filter	ArcSight Administration/ESM/System Health/
ASM Event Flow	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/Events/

Resource	Description	Type	URI
ASM CPU Load	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/Resources/
ASM Database Load Statistics	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/Storage/
Internal Source	This filter is looking for events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
ASM Events	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/
High Threat Condition	This resource has no description.	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 is looking for events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Severe Threat Condition	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
Inbound Events	This filter is looking for events coming from the outside network targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters/
ASM Load Overview	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/
Guarded Threat Condition	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
ASM Resource and Memory Load	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/Resources/
External Source	This filter is looking for events coming from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Notification Actions	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/Events/Event Flow/
Outbound Events	This filter is looking for events coming from inside the company network targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters/

Resource	Description	Type	URI
Low Threat Condition	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
Elevated Threat Condition	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
ArcSight Internal Events	This resource has no description.	Filter	ArcSight System/Event Types/
Non-ArcSight Internal Events	This resource has no description.	Filter	ArcSight System/Event Types/
External Target	This filter is looking for events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
ASM Standing Load	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/Resources/
ArcSight Audit Events	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/Events/Audit/
ASM Flow Load	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/Resources/
Top 10 Inbound Events	This resource has no description.	Query	ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Top 10 Events	This resource has no description.	Query	ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Event Count by Agent Severity	This resource has no description.	Query	ArcSight Administration/ESM/System Health/Events/
Destination Counts	This resource has no description.	Query	ArcSight Administration/ESM/System Health/Events/
Hourly Distribution Chart for a Source Port	This resource has no description.	Query	ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart)	This resource has no description.	Query	ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/

Resource	Description	Type	URI
Hourly Event Counts (Area Chart)	This resource has no description.	Query	ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Source Counts by Event Name	This resource has no description.	Query	ArcSight Administration/ESM/System Health/Events/
Event Name Counts	This resource has no description.	Query	ArcSight Administration/ESM/System Health/Events/
Event Count by Source Destination Pairs	This resource has no description.	Query	ArcSight Administration/ESM/System Health/Events/
Top 10 Outbound Events	This resource has no description.	Query	ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Hourly Distribution Chart for a Destination Port	This resource has no description.	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 for use in the Events by ArcSight Priority (Summary) report.	Query	ArcSight Administration/ESM/System Health/Events/
Hourly Distribution Chart for Event	This resource has no description.	Query	ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/

ESM Reporting Resource Monitoring

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

Resources

The following table lists the information presentation and data processing resources that support the ESM Reporting Resource Monitoring use case.

Table 4-12 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/
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 /

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

Resource	Description	Type	URI
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/
Query Counts by Type	This report shows a 3D bar chart of 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 viewer. The chart shows the top ten longest queries for a query viewer, and the 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. The chart shows the top ten longest trend queries and the 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 on query audit events. The rule adds or updates the corresponding entry to the 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/
Currently Running Reports	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Reporting/Reporting Subsystem Statistics/

Resource	Description	Type	URI
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 resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Reporting/Reporting Subsystem Statistics/
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/
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/

Resource	Description	Type	URI
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/
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/

Resource	Description	Type	URI
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/
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/
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 top longest report queries by day.	Trend	ArcSight Administration/ESM/System Health/Resources/Reporting/
QueryViewer Queries	This trend stores 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 ESM resources, such as trends, rules, and so on.

Configuration

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*.

Resources

The following table lists the information presentation and data processing resources that support the ESM Resource Monitoring use case.

Table 4-13 Resources that Support the ESM Resource Monitoring Use Case

Resource	Description	Type	URI
Monitor Resources			
Rules Status	This resource has no description.	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 /
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 /
Top 10 longest Trend Queries During Last 24 hr	This query viewer shows the duration information for the top 10 longest trend queries during last 24 hours.	Query Viewer	ArcSight Administration/ESM/System Health/Resources/Reporting /Trends/
Query Failures During Last 24 hr	This query viewers displays failed queries for reports, trends, and query viewers.	Query Viewer	ArcSight Administration/ESM/System Health/Resources/Reporting /

Resource	Description	Type	URI
Top 10 Longest Query Viewer Queries During Last 24 hr	This query viewer shows the duration information for the top 10 longest query viewers during 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 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 10 longest report queries during last 24 hours.	Query Viewer	ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Active List Access	This report shows active list access statistics. The report contains a curve chart and a table. The chart shows the number of added, deleted, and updated active list entries within the previous day, grouping the counts by ten minute intervals. The 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 resource has no description.	Report	ArcSight Administration/ESM/System Health/Resources/Rules/
Session List Access	This report shows session list access statistics. The report contains a curve chart and a table. The chart shows the number of added, deleted, and updated session list entries in the last hour, grouping the counts by ten minute intervals. The 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 the list of resources that became invalid using a chart and a table. The chart shows the count of invalid resources by resource type. The table lists all the invalid resources grouped by type and sorted by URI.	Report	ArcSight Administration/ESM/System Health/Resources/

Resource	Description	Type	URI
Top Accessed Active Lists	This report shows the top ten accessed active lists. The report contains a 3d bar chart and a table. The chart shows the top ten accessed active lists in the previous day, grouping the counts by ten minutes intervals. The 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. This report contains a line chart. The 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. The report contains a 3d bar chart and a table. The chart shows the Top ten accessed session lists within the last hour, grouping the counts by 10 minute intervals. The table shows the 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/
Correlation Events Statistics	This report shows correlation events statistics. The report contains a 3d bar chart and a table. The chart shows the number of correlation events within the last hour, grouping them by ten minutes intervals. The table shows the 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/

Resource	Description	Type	URI
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 in a time frame of 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 in a time frame of five minutes. After this rule is triggered, a notification is sent to the SOC Operators.	Rule	ArcSight Administration/ESM/System Health/Resources/Rules/
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 resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Reporting /Reporting Subsystem Statistics/
Rules Engine Internal Stats	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/

Resource	Description	Type	URI
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/
Recent Fired Rules	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/
Partial Matches per Rule	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/
Report Statistics	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Reporting/Reporting Subsystem Statistics/
Top Firing Rules	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/
Rule Error Logs	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/
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 resource has no description.	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 resource has no description.	Filter	ArcSight Administration/ESM/System Health/Resources/Rules/

Resource	Description	Type	URI
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 QueryViewer Queries	This query retrieves query duration information for query viewers ordered by duration.	Query	ArcSight Administration/ESM/System Health/Resources/Reporting/QueryViewers/
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/
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 minutes 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 by ten minutes 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 minutes intervals.	Query	ArcSight Administration/ESM/System Health/Resources/Rules/

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 resource has no description.	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) by ten minutes 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 minutes intervals for the last hour.	Query	ArcSight Administration/ESM/System Health/Resources/Active Lists/
Average Data Monitor Evaluations Per Second	This query identifies the average number of data monitor evaluations per second by ten minutes 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) by ten minutes 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/

Resource	Description	Type	URI
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.

Devices

ArcSight Express 3.0 and later.

Configuration

The ESM Storage Monitoring (CORR) use case requires the following configuration for your environment:

- 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*.

Resources

The following table lists the information presentation and data processing resources that support the ESM Storage Monitoring (CORR) use case.

Table 4-14 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, and insert and retrieval times.	Dashboard	ArcSight Administration/ESM/System Health/Storage/CORR/
Archive Status	This dashboard shows database archive related information.	Dashboard	ArcSight Administration/ESM/System Health/Storage/CORR/
Critical Archive Failure Details	This query viewer shows the current archive archival failure events.	Query Viewer	ArcSight Administration/ESM/System Health/Storage/CORR/
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/
Archive Status Report	This report shows the current status of archive and disk space used.	Report	ArcSight Administration/ESM/System Health/Storage/CORR/

Resource	Description	Type	URI
ASM Database Free Space	This report shows the current free space percentages for the ASM database table spaces. The report has bar charts showing the percentages for the ARC_EVENT_DATA and ARC_SYSTEM_DATA table spaces.	Report	ArcSight Administration/ESM/System Health/Storage/CORR/
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. You can use the custom parameter 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/
Archive Processing	This report displays a chart showing the longest to process archives, and a table showing time to archive information.	Report	ArcSight Administration/ESM/System Health/Storage/CORR/
ASM Database Free Space - by Hour	This trend shows the free space percentages by hour for the ASM database table spaces. The report has two stacked area charts showing the percentages by hour for the ARC_EVENT_DATA and ARC_SYSTEM_DATA table spaces.	Report	ArcSight Administration/ESM/System Health/Storage/CORR/
Library - Correlation Resources			
Archive Task Success	This rule is triggered by successful archive activation, deactivation, and scheduling audit events in which the archive name is in the Archive Task Failures active list . This rule removes the entry from the active list.	Rule	ArcSight Administration/ESM/System Health/Storage/CORR/
Critical Archive Failures	This rule is triggered by archive archival failure events and adds them to the Critical Archive Failures active list.	Rule	ArcSight Administration/ESM/System Health/Storage/CORR/
ASM Database Status Change - Down	This rule detects if the database status is down. This rule identifies the event insert and retrieval time. The status is considered down when the EventInsertTimeNanos field is equal to zero. This rule requires two such events in a time frame of three minutes. After the first event, the agentSeverity event field is set to unknown.	Rule	ArcSight Administration/ESM/System Health/Storage/

Resource	Description	Type	URI
Archive Events	This rule is triggered by archive audit events and adds them to the Archive Events session list.	Rule	ArcSight Administration/ESM/System Health/Storage/CORR/
ASM Database Free Space - Critical	This rule identifies 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 a threshold that can be 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 looks for an event insert and retrieval time. The status is considered critical when the EventInsertTimeNanos field is greater than or equal to 50,000. This rule requires two such events in a time frame of three minutes. After the first event, the agentSeverity event field will be set to very-high.	Rule	ArcSight Administration/ESM/System Health/Storage/
ASM Database Status Change - Space Now Available	This rule detects if the database status has returned to normal because storage space has been freed or added. This rule looks for a base event indicating that database storage space is available. This rule only requires one such event to fire. 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 looks for the event insert and retrieval time. The status is considered normal when the EventInsertTimeNanos field is less than or equal to 20,000. This rule requires two such events in a time frame of three minutes. After the first event, the agentSeverity event field is set to low.	Rule	ArcSight Administration/ESM/System Health/Storage/

Resource	Description	Type	URI
ASM Database Free Space - Warning	This rule identifies internal events showing that one (or more) of the ASM database table spaces has a low free space percentage. This is considered as a warning when the free space goes below a threshold that can be 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 events in which the archive name is in the Critical Archival Failures active list. This rule removes the entry from the active list.	Rule	ArcSight Administration/ESM/System Health/Storage/CORR/
Archive Task Failures	This rule is triggered by archive task failure events (activation, deactivation, and scheduling events) and writes them to the Archive Task Failures active list.	Rule	ArcSight Administration/ESM/System Health/Storage/CORR/
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. The rule looks for a base event that indicates that the database storage space is low. This rule only requires one such event to trigger. After the first event, the agentSeverity event field will be 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 identifies the event insert and retrieval time. The status is considered a warning when the EventInsertTimeNanos field is between 20,000 and 50,000. This rule requires two such events in a time frame of 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/
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/

Resource	Description	Type	URI
Database Retrieval Time - Last Hour	This data monitor displays a moving average for the database retrieval time during last hour.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR/Datase Performance Statistics/
Database Insert Time - Last 24 Hours	This data monitor displays a moving average for the database insert time during last 24 hour.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR/Datase Performance Statistics/
Database Transaction Volume	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/
Database Insert Time - Last Hour	This data monitor displays a moving average for the database insert time during last hour.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR/Datase Performance Statistics/
Database Retrieval Time - Last 24 Hours	This data monitor displays a moving average for the database retrieval time during last 24 hour.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR/Datase Performance Statistics/
Database Free Space	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR/Datase Performance Statistics/
Archive Disk Space	This data monitor shows the state of archive disk space used. The three states are: OK, Warning, and Critical Warning.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR/Archive Status/
Recent Archive Events	This data monitor shows the last ten archive events.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR/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 resource has no description.	Filter	ArcSight Administration/ESM/System Health/Storage/
ASM Database Statistics	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/Storage/
Archive Settings Updated Event	This filter identifies archive setting updated audit events.	Filter	ArcSight Administration/ESM/System Health/Storage/CORR/Conditional Variable Filters/
Archive Archival Success	This filter identifies archive archival success audit events.	Filter	ArcSight Administration/ESM/System Health/Storage/CORR/Conditional Variable Filters/

Resource	Description	Type	URI
Archive Disk Space	This filter identifies archive disk space audit events.	Filter	ArcSight Administration/ESM/System Health/Storage/CORR/
Archive Disk space status is OK	This filter identifies archive disk space audit events in which custom number 1 (Used Space Percentage) is less than a certain value. 85 is the default number.	Filter	ArcSight Administration/ESM/System Health/Storage/CORR/Conditional Variable Filters/
Threshold - Warning	This filter is used in the ASM Database Free Space - Warning rule. The filter passes 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 identifies all archive audit events.	Filter	ArcSight Administration/ESM/System Health/Storage/CORR/
Threshold - Critical	This filter is used in the ASM Database Free Space - Critical rule. The filter passes events where 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 identifies all archive failure audit events.	Filter	ArcSight Administration/ESM/System Health/Storage/CORR/Conditional Variable Filters/
Archive Disk space status is Critical	This filter identifies archive disk space audit events in which custom number 1, (Used Space Percentage) is greater than a certain value. 95 is the default number.	Filter	ArcSight Administration/ESM/System Health/Storage/CORR/Conditional Variable Filters/
File Path StartsWith All Rules	This filter identifies events in which the file path starts with /All Rules.	Filter	ArcSight Administration/ESM/System Health/Storage/CORR/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 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 the ASM Database Free Space - by Day.	Focused Report	ArcSight Administration/ESM/System Health/Storage/CORR/

Resource	Description	Type	URI
Event Data Free Space - Last 30 Days	This report shows the free space percentages by day for the ARC_EVENT_DATA database table space for the last 30 days. The source report is the ASM Database Free Space - by Day.	Focused Report	ArcSight Administration/ESM/System Health/Storage/CORR/
Critical Archive Failure Details	This query retrieves archive archival failure events from the Critical Archive Failures active list.	Query	ArcSight Administration/ESM/System Health/Storage/CORR/
Archive Activation Statistics	This query retrieves archive activation audit events from the Archive Events session list.	Query	ArcSight Administration/ESM/System Health/Storage/CORR/
Archive Task Failure Details	This query retrieves archive task failure events from the Archive Task Failures active list.	Query	ArcSight Administration/ESM/System Health/Storage/CORR/
ASM Database Free Space - by Day	This query on the ASM Database Free Space trend retrieves 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 retrieves archive disk space used information from the Archive Events session list.	Query	ArcSight Administration/ESM/System Health/Storage/CORR/
ASM Database Free Space - by Hour	This query on the ASM Database Free Space trend retrieves 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 retrieves archive deactivation audit events from the Archive Events session list.	Query	ArcSight Administration/ESM/System Health/Storage/CORR/
Archive status	This query retrieves 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/
Archive Non-success events	This query retrieves non-successful archive audit events from the Archive Events session list.	Query	ArcSight Administration/ESM/System Health/Storage/CORR/
ASM Database Free Space	This query retrieves internal events showing a free space percentage for ASM database table spaces. The query identifies 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/

Resource	Description	Type	URI
Archive Archival Success	This query retrieves archive archival information from the Archive Events session list.	Query	ArcSight Administration/ESM/System Health/Storage/CORR/
Archive Space status	This query active list archive space audit events.	Query	ArcSight Administration/ESM/System Health/Storage/CORR/
Archive Archival Statistics	This query retrieves archive archival audit events from the Archive Events session list.	Query	ArcSight Administration/ESM/System Health/Storage/CORR/
ASM Database Free Space (current)	This query retrieves internal events showing a free space percentage for ASM database table spaces. The query identifies 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 retrieves archive scheduling audit events from the Archive Events session list.	Query	ArcSight Administration/ESM/System Health/Storage/CORR/
Archive Events	This session list stores archive audit events.	Session List	ArcSight Administration/ESM/System Health/Storage/CORR/
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 the CORR Engine.

Devices

ESM using Oracle or ArcSight Express earlier than v3.0.

Configuration

The ESM Storage Monitoring (Oracle) use case requires the following configuration for your environment:

- 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*.

Resources

The following table lists the information presentation and data processing resources that support the ESM Storage Monitoring (Oracle) use case.

Table 4-15 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, and insert and retrieval times.	Dashboard	ArcSight Administration/ESM/System Health/Storage/CORR/
Partition Manager and Archiver Status	This dashboard shows the status and details of the partition manager and partition archiver.	Dashboard	ArcSight Administration/ESM/System Health/Storage/Oracle/
ASM Database Free Space - by Hour	This trend shows the free space percentages by hour for the ASM database table spaces. The report has two stacked area charts showing the percentages by hour for the ARC_EVENT_DATA and ARC_SYSTEM_DATA table spaces.	Report	ArcSight Administration/ESM/System Health/Storage/CORR/

Resource	Description	Type	URI
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. You can use the custom parameter 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/
ASM Database Free Space	This report shows the current free space percentages for the ASM database table spaces. The report has bar charts showing the percentages for the ARC_EVENT_DATA and ARC_SYSTEM_DATA table spaces.	Report	ArcSight Administration/ESM/System Health/Storage/CORR/
Library - Correlation Resources			
ASM Database Status Change - Critical	This rule detects if the database status is critical. This rule looks for an event insert and retrieval time. The status is considered critical when the EventInsertTimeNanos field is greater than or equal to 50,000. This rule requires two such events in a time frame of three minutes. After the first event, the agentSeverity event field will be set to very-high.	Rule	ArcSight Administration/ESM/System Health/Storage/
ASM Database Status Change - Space Now Available	This rule detects if the database status has returned to normal because storage space has been freed or added. This rule looks for a base event indicating that database storage space is available. This rule only requires one such event to fire. 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 identifies the event insert and retrieval time. The status is considered down when the EventInsertTimeNanos field is equal to zero. This rule requires two such events in a time frame of three minutes. After the first event, the agentSeverity event field is set to unknown.	Rule	ArcSight Administration/ESM/System Health/Storage/

Resource	Description	Type	URI
ASM Database Status Change - Normal	This rule detects if the database status is normal. This rule looks for the event insert and retrieval time. The status is considered normal when the EventInsertTimeNanos field is less than or equal to 20,000. This rule requires two such events in a time frame of three 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 identifies internal events showing that one (or more) of the ASM database table spaces has a low free space percentage. This is considered as a warning when the free space goes below a threshold that can be defined in the server.properties file (five percent by default).	Rule	ArcSight Administration/ESM/System Health/Storage/
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 identifies the event insert and retrieval time. The status is considered a warning when the EventInsertTimeNanos field is between 20,000 and 50,000. This rule requires two such events in a time frame of 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 identifies 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 a threshold that can be 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. The rule looks for a base event that indicates that the database storage space is low. This rule only requires one such event to trigger. After the first event, the agentSeverity event field will be set to very high.	Rule	ArcSight Administration/ESM/System Health/Storage/

Resource	Description	Type	URI
Library Resources			
Partition Manager and Archiver Details	This data monitor displays the last ten system audit events for the partition manager and partition archiver.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle/
Database Retrieval Time - Last Hour	This data monitor displays a moving average for the database retrieval time during last hour.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR/Database Performance Statistics/
Database Insert Time - Last 24 Hours	This data monitor displays a moving average for the database insert time during last 24 hour.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR/Database Performance Statistics/
Sidetable Sizes (Rows)	This data monitor shows the average number of rows of the database side tables for the last 10 minutes. The sampling interval is one minute. A correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle/Database Performance Statistics/
Database Transaction Volume	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/
Partition Manager and Archiver - Heads Up Display	This data monitor shows the status of the partition manager and partition archiver.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle/
ASM Database Responsiveness - Last Hour	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle/Database Performance Statistics/
Database Insert Time - Last Hour	This data monitor displays a moving average for the database insert time during last hour.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR/Database Performance Statistics/
Database Retrieval Time - Last 24 Hours	This data monitor displays a moving average for the database retrieval time during last 24 hour.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR/Database Performance Statistics/
Database Free Space	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/CORR/Database Performance Statistics/

Resource	Description	Type	URI
Sidetable Cache Hit Rates	This data monitor shows the average value of the database side table cash hit rate for the last 15 minutes. The sampling interval is one minute. A correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle/Data base Performance Statistics/
ASM Database Responsiveness - Last 24 hours	This resource has no description.	Data Monitor	ArcSight Administration/ESM/System Health/Storage/Oracle/Data base Performance Statistics/
Threshold - Warning	This filter is used in the ASM Database Free Space - Warning rule. The filter passes 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 passes events where 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 resource has no description.	Filter	ArcSight Administration/ESM/System Health/Storage/
ASM Sidetable Sizes	This filter identifies ArcSight System Monitor events containing 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 presently in the cache.	Filter	ArcSight Administration/ESM/System Health/Storage/
ASM Database Statistics	This resource has no description.	Filter	ArcSight Administration/ESM/System Health/Storage/

Resource	Description	Type	URI
Partition without Submission Events	This filter detects system audit events of partition manager and partition archiver in which the device event category does not contain the remote command submission.	Filter	ArcSight Administration/ESM/System Health/Storage/Oracle/
Partition Manager and Archiver Events	This filter identifies system audit events for partition manager and partition archiver.	Filter	ArcSight Administration/ESM/System Health/Storage/Oracle/
ASM Sidetable Cache Hit Rates	This filter identifies ArcSight System Monitor events containing side table cache hit rates 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 to find entries occurred in 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/
Event Index Free Space - Last 30 Days	This 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 the ASM Database Free Space - by Day.	Focused Report	ArcSight Administration/ESM/System Health/Storage/Oracle/
System Index Free Space - Last 30 Days	This 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 the ASM Database Free Space - by Day.	Focused Report	ArcSight Administration/ESM/System Health/Storage/Oracle/
System Data Free Space - Last 30 Days	This 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 the ASM Database Free Space - by Day.	Focused Report	ArcSight Administration/ESM/System Health/Storage/CORR/
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 the ASM Database Free Space - by Day.	Focused Report	ArcSight Administration/ESM/System Health/Storage/CORR/

Resource	Description	Type	URI
ASM Database Free Space	This query retrieves internal events showing a free space percentage for ASM database table spaces. The query identifies 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/
ASM Database Free Space (current)	This query retrieves internal events showing a free space percentage for ASM database table spaces. The query identifies 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 retrieves 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 retrieves 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 Loggers to ESM.

Resources

The following table lists the information presentation and data processing resources that support the Logger Events use case.

Table 4-16 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 over the last hour.	Active Channel	ArcSight Administration/Logger/
Logger Platform Events	This active channel shows all the Logger platform events over 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, the event name, the Logger user, the client address (browser), and the 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, the event name, the Logger user, the client address (browser), and the 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/
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 the Loggers connected to ESM.

Configuration

If you have a Logger connected to ArcSight ESM, 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 13](#).

- 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 [Table 4-17 on page 132](#)):
 - ◆ **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*.

Resources

The following table lists the information presentation and data processing resources that support the Logger System Health use case.

Table 4-17 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 over 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 for the last 10 minutes and the last hour.	Dashboard	ArcSight Administration/Logger/My Logger/
CPU and Memory	This dashboard shows the CPU and Memory usage for the Logger defined in the My Logger filter for the last 10 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 for the last 10 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/

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/
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 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/
Network Usage (Bytes) - Last Hour	This data monitor shows the network 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/Network/

Resource	Description	Type	URI
EPS Usage (Events per Second) - Last Hour	This data monitor shows the EPS 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/Network/
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 last N events 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 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/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 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/
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/
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/

Resource	Description	Type	URI
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/
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 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/Storage/
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 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/CPU and Memory/
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/

Resource	Description	Type	URI
Logger IP	This resource has no description.	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 is designed for conditional expression variables. The filter passes events where 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/
Sensor Type is FAN	This filter is designed for conditional expression variables. The filter passes events where 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/

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/
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/
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 resource has no description.	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/
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/

Appendix A

Upgrading Standard Content

This appendix discusses the following topics.

[“Preparing Existing Content for Upgrade” on page 139](#)

[“Performing the Upgrade” on page 140](#)

[“Checking and Restoring Content After Upgrade” on page 140](#)

Preparing Existing Content for Upgrade

The majority of standard content does not need configuration and does not require special preparation for upgrade. Upgrade preparation is recommended only for content that has been configured and for which configuration is not preserved after the upgrade.

Configurations Preserved During Upgrade

The following resource configurations are preserved during the upgrade process. No restoration is required for these resources after the upgrade.

- Asset modeling for network assets, including:
 - ◆ Assets, and asset groups and their settings
 - ◆ Asset categories applied to assets and asset groups
 - ◆ Vulnerabilities applied to assets
 - ◆ Custom zones
- SmartConnectors
- Users and user groups
- Report schedules
- Notification destinations and priority settings
- Cases

Configurations that Require Restoration After Upgrade

The following resource configurations require restoration after upgrade.

- Any standard content resource that you have modified, including active lists
- Any custom content or special modifications not already described in this document (including customizations performed by ArcSight Professional Services)

Backing Up Existing Resources Before Upgrade



Before you back up existing resources, run the resource validator (`resvalidate.bat`) located on the ESM Manager in `<ARCSIGHT_HOME>\bin\scripts` to check that the resources are working correctly before the upgrade. This prevents you from attributing broken resources with the upgrade.

During the upgrade process, the content is run through a resource validator automatically (see ["Fixing Invalid Resources" on page 141](#)).

To help the process of reconfiguring resources that require restoration after upgrade, back up the resources you identify in ["Configurations that Require Restoration After Upgrade" on page 139](#) and export them in a package. After upgrade, you can re-import the package and use the existing resources as a reference for restoring the configurations to the upgraded environment.

To create a backup of the resources that require restoration after upgrade:

- 1 For each resource type (filter, rule, active list), create a new group under your personal group. Provide a name that identifies the contents.
 - ◆ Right-click your group name and select **New Group**.
- 2 Copy the resources into the new group. Repeat this process for every resource type you want to back up.
 - ◆ Select the resources you want to back up and drag them into the backup folder you created in [Step 1](#). In the *Drag & Drop Options* dialog box, select **Copy**.
- 3 Export the backup groups in a package.
 - ◆ In the Navigator panel Packages tab, right-click your group name and select **New Package**. In the Packages editor in the Inspect/Edit panel, name the package to identify the contents.



Copy and paste configurations from the old resources to the new

Instead of overwriting the new resources with backup copies of the old ones, copy and paste configurations from the old resources one by one into the new ones. This procedure ensures that you preserve your configurations without overwriting any improvements provided in the upgrade.

Performing the Upgrade

After exporting a copy of the configured resources in a backup package, you are ready to perform the upgrade the process. Refer to the ESM upgrade documentation for upgrade procedures.

Checking and Restoring Content After Upgrade

After the upgrade is complete, perform the following checks to verify that all your content has been transferred to the new environment successfully.

Verifying and Reapplying Configurations

Verify and restore standard content after upgrade.

- 1 Verify that your configured resources listed in the section [“Configurations Preserved During Upgrade” on page 139](#) retained their configurations as expected.
- 2 Reconfigure the resources that require restoration.
 - a Re-import the package you created in [“Backing Up Existing Resources Before Upgrade” on page 140](#).
 - b One resource at a time, copy and paste the configurations preserved in the package of copied resources into the new resources installed with the upgrade. Copying your configurations one resource at a time instead of overwriting the new resources with the old ensures that you retain your configurations without overwriting any improvements provided with the upgraded content.

Verifying Customized Content

It is possible during upgrade that updates to the standard content cause resources you created to work in a way that is not intended. For example, a rule might trigger too often or not at all if it uses a filter in which conditions have been changed.

To verify that the resources you rely upon work as expected, check the following:

- **Trigger events.** Send events that you know trigger the content through the system using the Replay with Rules feature. For more about this feature, refer to the *ArcSight Console User's Guide* or the ESM online Help.
- **Check Live Events.** Check the Live or All Events active channel to verify if the correlation event is triggered. Check that the data monitors you created are returning the expected output based on the test events you send through.
- **Verify notification destinations.** Verify that notifications are sent to the recipients in your notification destinations as expected.
- **Verify active lists.** Check that any active lists you have created to support your content are gathering the replay with rules data as expected.
- **Repair any invalid resources.** During the upgrade process, the resource validator identifies any resources that are rendered invalid (conditions that no longer work) during the upgrade. Find invalid resources and fix their conditions as appropriate. For more about invalid resources, see [Fixing Invalid Resources](#), below.

Fixing Invalid Resources



During the upgrade process, the content is run through a resource validator, which verifies that the values expressed in the resource condition statement still apply to the resource in its new format, and that any resources upon which it depends are still present and also valid. The resource validator runs on any resource that contains a condition statement or populates the asset model, such as:

- Active channels
- Filters
- Data Monitors
- Rules
- Report queries and schedules
- Assets and Asset ranges

■ Zones

It is possible that during upgrade, the condition statement for a resource you created or modified becomes invalid. For example, if the schema of an ArcSight-supplied active list changes from one release to another and a resource you created reads entries from this list, the condition statement in the created resource no longer matches the schema of the active list, and the logic is invalid.

When the installer performs the resource validation check and finds an invalid resource, it identifies why the resource is invalid in the report it generates at the end of the upgrade. The upgrade installer also lets you choose to save the reason the resource is invalid in the database (**Persist conflicts to the database=TRUE**). If you choose this option, the upgrade installer:

- Saves the reason the resource is found to be invalid in the database so you can generate a list of invalid resources that you can use later to repair the problems manually.
- Disables the resource so it does not try to evaluate live events in its invalid state.

If you choose not to save the reasons the resource is invalid in the database (**Persist conflicts to the database=FALSE**), the resources remain enabled, which means they try to evaluate the event stream in their invalid state.



If you choose not to persist conflicts to the database and disable invalid resources, the Manager might throw exceptions when the invalid resources try to evaluate live events.

Index

A

Account Authenticators active list 18

active channels

- Actor Audit Events 84
- ASM Events 95
- Connector Caching Events 62
- Connector Connection Status Events 62
- Connector Upgrades 56
- Last 5 Minutes 30
- Last Hour 30
- Live 30
- Logger Application Events 130
- Logger Platform Events 130
- Logger System Health Events 132
- Personal Live 30
- Query Viewers Status 101
- Reports Status 101
- System Events Last Hour 31, 46, 95
- Today 30
- Trends Status 101

Active List Access (Details) query 113

Active List Access query 113

Active List Access report 108

active lists

- Account Authenticators 18
- Archive Task Failures 118
- Black List - Connectors 67
- Black List - Reverse Look Up 67
- Compromised List 25
- Connector Average EPS - Last 7 Days 75
- Connector Daily Average EPS 75
- Connector Information 42, 58, 66
- Connector Upgrades 58
- Connectors - Caching 43, 59, 68
- Connectors - Down 43, 59, 67
- Connectors - Dropping Events 43, 66
- Connectors - Still Caching 43, 58, 66
- Connectors - Still Down 43, 59, 67
- Critical Archive Failures 118
- Event-based Rule Exclusions 31
- general configuration 13, 14, 15
- Hit List 25
- Hostile List 25
- Infiltrators List 26
- Invalid Resources 110
- Logger Sensor Type Status 50, 133
- Logger Status 50, 133
- Query Running Time 103, 110
- Reconnaissance List 26
- Reporting Devices 75
- Reporting Devices - Critical 75

Scanned List 26

Suspicious List 25

Trusted List 26

Untrusted List 26

User-based Rule Exclusions 31

- Actor Administration dashboard 84
- Actor Audit Events active channel 84
- Actor Audit Field Set field set 89
- Actor Authenticators query 90
- Actor Authenticators query viewer 84
- Actor Base field set 20
- Actor Change Log dashboard 84
- Actor Change Log data monitor 86
- Actor Change Overview data monitor 86
- Actor Changes filter 90
- Actor Configuration Changes query 90
- Actor Configuration Changes query viewer 84
- Actor Configuration Changes use case 47
- Actor Context Report by Account ID report 18
- Actor Context Report by Attacker Username report 18
- Actor Context Report by Custom Fields report 18
- Actor Context Report by Target Username report 18
- Actor Data asset category 19
- Actor Data Support asset category 19
- Actor Deletes filter 89
- Actor Event Count by Account ID query 21
- Actor Event Count by Attacker Username query 20
- Actor Event Count by Custom Fields query 21
- Actor Event Count by Target Username query 21
- Actor Events by Account ID query 21
- Actor Events by Attacker Username query 20
- Actor Events by Custom Fields query 21
- Actor Events by Target Username query 20
- Actor Full Name and Email Changes query 90
- Actor Full Name and Email Changes query viewer 85
- Actor Full Name and Email Changes report 85
- Actor global variable 87
- Actor Information field set 20
- Actor Information query 21
- Actor Inserts filter 89
- Actor Manager and Department Changes query 90
- Actor Manager and Department Changes query viewer 84
- Actor Manager and Department Changes report 86
- Actor Name or UUID filter 89
- Actor Title and Status Changes query 91
- Actor Title and Status Changes query viewer 85
- Actor Title and Status Changes report 86
- Actor Updates filter 89
- ActorByAccountID global variable 19
- ActorByAttackerUserName global variable 19

- ActorByCustomFields global variable 19
- ActorByDN global variable 20
- ActorByTargetUserName global variable 20
- ActorByUUID global variable 20
- ActorFromFileName global variable 87
- Actors Created query 91
- Actors Created query viewer 85
- Actors Deleted query 90
- Actors Deleted query viewer 85
- Actors Licensing Report focused report 80
- Actors Updated query 91
- Actors Updated query viewer 84
- admincert destination 79
- alias global variable 20
- All Events filter 33, 75, 83, 89, 93, 98, 112
- All Receivers and Forwarders global variable 52
- All Receivers EPS filter 53
- Annotation field set 32
- Annotation-MgrRcpt field set 31
- Archive Activation Statistics query 121
- Archive Archival Statistics query 122
- Archive Archival Success filter 119
- Archive Archival Success query 122
- Archive Deactivation Statistics query 121
- Archive Disk Space data monitor 119
- Archive Disk Space filter 120
- Archive Disk space status is Critical filter 120
- Archive Disk space status is OK filter 120
- Archive Disk Space Usage query 121
- Archive Events filter 120
- Archive Events rule 117
- Archive Events session list 122
- Archive Failure Events filter 120
- Archive Non-success events query 121
- Archive Processing report 116
- Archive Scheduling Statistics query 122
- Archive Settings Updated Event filter 119
- Archive Space status query 122
- Archive Status dashboard 115
- Archive status query 121
- Archive Status Report report 115
- Archive Task Failure Details query 121
- Archive Task Failure Details query viewer 115
- Archive Task Failures active list 118
- Archive Task Failures rule 118
- Archive Task Success rule 116
- ArcSight Admin field set 32, 46, 97
- ArcSight Administration
 - configuring 11
 - installing 11
 - overview 7
- ArcSight Appliances Overview dashboard 49
- ArcSight Audit Events filter 99
- ArcSight Correlation Events filter 33, 54, 137
- ArcSight Events filter 33, 44, 76
- ArcSight Foundations overview 7
- ArcSight Internal Events filter 33, 46, 99
- ArcSight Login Events filter 83
- ArcSight Login Rule Firings filter 83
- ArcSight Login Tracking filter 82
- ArcSight Reporting Statistics data monitor 104, 111
- ArcSight Rules filter 111
- ArcSight Status Monitoring Events filter 97
- ArcSight System
 - configuring 11
 - installing 11
 - overview 7
- ArcSight User Hourly Login Trends query 83
- ArcSight User Login rule 82
- ArcSight User Login Timeout rule 82
- ArcSight User Login Trends - Hourly trend 83
- ArcSight User Login Trends report 81
- ArcSight User Logins - Last Hour query 83
- ArcSight User Logins - Last Hour report 81
- ArcSight User Logout rule 81
- ArcSight User Sessions data monitor 82
- ArcSight User Sessions session list 83
- ArcSight User Status dashboard 81
- ASM CPU Load filter 98
- ASM Database Free Space - by Day query 121, 129
- ASM Database Free Space - by Day report 116, 124
- ASM Database Free Space - by Hour query 121, 129
- ASM Database Free Space - by Hour report 116, 123
- ASM Database Free Space - Critical rule 117, 125
- ASM Database Free Space - Warning rule 118, 125
- ASM Database Free Space (current) query 122, 129
- ASM Database Free Space query 121, 129
- ASM Database Free Space report 116, 124
- ASM Database Free Space trend 122, 129
- ASM Database Load Statistics filter 98, 119, 127
- ASM Database Responsiveness - Last 24 hours data monitor 127
- ASM Database Responsiveness - Last Hour data monitor 126
- ASM Database Statistics filter 119, 127
- ASM Database Status Change - Critical rule 117, 124
- ASM Database Status Change - Down rule 116, 124
- ASM Database Status Change - Normal rule 117, 125
- ASM Database Status Change - Space Critical rule 118, 125
- ASM Database Status Change - Space Now Available rule 117, 124
- ASM Database Status Change - Warning rule 118, 125
- ASM Event Flow filter 97
- ASM Events active channel 95
- ASM Events field set 97
- ASM Events filter 33, 46, 98
- ASM Flow Load filter 99
- ASM Load Overview filter 98
- ASM Reports Statistics filter 104, 111
- ASM Resource and Memory Load filter 98
- ASM Sidetable Cache Hit Rates filter 128
- ASM Sidetable Sizes filter 127
- ASM Standing Load filter 99
- asset categories
 - Actor Data 19
 - Actor Data Support 19
 - Criticality 27
 - FIPS-199 27
 - High 26, 27, 75
 - Low 26, 27
 - Medium 27
 - Moderate 26
 - Open Ports 26
 - Protected 96
 - Very High 27
 - Very Low 27
 - Vulnerabilities 26
- Asset field set 32
- Asset Information field set 32

- Assets having Vulnerability report 31
- Assets Licensing Report focused report 80
- Attacker Address is NULL filter 90
- Attacker Host Name is NULL filter 90
- Attacker Information is NULL filter 89
- Attacker Port is NULL filter 89
- Attacker User Name is NULL filter 20, 34
- Attacker Zone AND Host are NULL but Address is NOT NULL filter 90
- Attacker Zone AND Host are NULL filter 89
- Attacker Zone is NULL filter 89
- Attacker Zone OR Host is NULL filter 89
- AttackerHost global variable 88
- Attackers on Hostile List filter 28
- Attackers on Infiltrators List filter 28
- Attackers on Reconnaissance List filter 28
- Attackers on Suspicious List filter 28
- Average Data Monitor Evaluations Per Second query 113

B

- Black List - Connectors active list 67
- Black List - Reverse Look Up active list 67
- Blocked ArcSight Internal Events filter 33
- By Destination integration command 54
- By Event Name integration command 54
- By Source and Destination integration command 55
- By Source integration command 54
- By User integration command 54
- By Vendor and Product integration command 55

C

- Cache History by Connectors query 69
- Cache History by Connectors report 63
- Case Information field set 32
- Categories field set 32
- Change Source global variable 87
- Closed stage 37
- Common Conditions Editor field set 31
- Compromise - Attempt rule 25
- Compromise - Success rule 24
- Compromised List active list 25
- Compromised Targets filter 28
- configuration
 - active lists 13, 14, 15
 - ArcSight Administration 11
 - ArcSight System 11
- Configuration Changes by Type report 85
- Configuration Changes by User report 86
- Connector - Caches session list 70
- Connector Added to Black List rule 65
- Connector Asset Auto Creation Controller filter 33
- Connector Average EPS - Last 7 Days active list 75
- Connector Average EPS - Last 7 Days query 77
- Connector Average EPS - Last 7 days trend 78
- Connector Cache Empty rule 65
- Connector Cache Status data monitor 44, 68
- Connector Cache Status filter 44, 68
- Connector Caching Event filter 68
- Connector Caching Events active channel 62
- Connector Caching rule 65
- Connector Configuration Changes use case 45
- Connector Connection and Cache Status dashboard 41, 62

- Connector Connection and Cache Status use case 45
- Connector Connection Status data monitor 44, 68
- Connector Connection Status Events active channel 62
- Connector Connection Status filter 44, 69
- Connector Daily Average EPS active list 75
- Connector Daily Average EPS query 77
- Connector Daily Average EPS trend 78
- Connector Deleted rule 57, 64
- Connector Discovered or Updated rule 66
- Connector Down rule 65
- Connector Dropping Events rule 65
- Connector Information active list 42, 58, 66
- Connector Monitor Event query 76
- Connector Monitoring Events field set 32, 46, 68, 97
- Connector Registered or Heartbeat Event filter 68
- Connector Severity Hourly Stacked Chart query 77
- Connector Severity Hourly Stacked Chart report 72
- Connector Still Caching rule 64
- Connector Still Down rule 64
- Connector Total Events - Hourly trend 78
- Connector Up rule 64
- Connector Upgrade Failed rule 57
- Connector Upgrade Successful rule 58
- Connector Upgrades active channel 56
- Connector Upgrades active list 58
- Connector Upgrades Count (Total) query 60
- Connector Upgrades Count query 60
- Connector Upgrades Count report 57
- Connector Upgrades field set 59
- Connector Version Detected rule 57, 65
- Connector Versions by Type query 60
- Connector Versions by Type report 56
- Connector Versions query 60
- Connector Versions report 56
- Connector Versions session list 60, 70
- Connectors - Caching - Long Term query 45, 69
- Connectors - Caching - Long Term query viewer 42, 63
- Connectors - Caching - Short Term query 45, 69
- Connectors - Caching - Short Term query viewer 42, 63
- Connectors - Caching active list 43, 59, 68
- Connectors - Down - Long Term query viewer 42, 63
- Connectors - Down - Short Term query viewer 41, 62
- Connectors - Down active list 43, 59, 67
- Connectors - Down query 44, 69
- Connectors - Dropping Events active list 43, 66
- Connectors - Dropping Events query 44, 69
- Connectors - Dropping Events query viewer 41, 62
- Connectors - Still Caching active list 43, 58, 66
- Connectors - Still Down active list 43, 59, 67
- Connectors - Still Down query 45, 69
- Console and ArcSight Web Status dashboard 81
- Console Users Licensing Report focused report 80
- content packages 8
- Correlation Events Count (Details) query 112
- Correlation Events Count query 112
- Correlation Events filter 20, 34
- Correlation Events Statistics report 109
- CPU and Memory dashboard 132
- CPU Name global variable 52
- CPU Sensors data monitor 134
- CPU Sensors filter 136
- CPU Usage (Percent) - Last 10 Minutes data monitor 51, 135
- CPU Usage (Percent) - Last Hour data monitor 134
- CPU Usage filter 53, 136

Created report 86
 createTime global variable 19
 creator global variable 19
 Critical Archive Failure Details query 121
 Critical Archive Failure Details query viewer 115
 Critical Archive Failures active list 118
 Critical Archive Failures rule 116
 Critical Archive Success rule 118
 Critical Device Not Reporting filter 75
 Critical Device Not Reporting rule 74
 Critical Device Reported rule 74
 Critical Devices - Heads Up Display data monitor 75
 Critical Devices Up Down filter 76
 Criticality asset category 27
 Current Cache Status - Caching Events query 69
 Current Cache Status - Dropping Events query 69
 Current Cache Status report 63
 Current Connector Status data monitor 44, 68
 Current Event Sources dashboard 41, 72
 Current Users Logged In data monitor 82
 Currently Running Reports data monitor 103, 110

D

Daily Pattern Discovery profile 37
 dashboards
 Actor Administration 84
 Actor Change Log 84
 Archive Status 115
 ArcSight Appliances Overview 49
 ArcSight User Status 81
 Connector Connection and Cache Status 41, 62
 Console and ArcSight Web Status 81
 CPU and Memory 132
 Current Event Sources 41, 72
 Database Performance Statistics 115, 123
 Device Status 72
 ESM System Information 46
 Event Throughput 95
 Hardware 132
 Latest Events By Priority 95
 My Logger Overview 49, 132
 Network 132
 Partition Manager and Archiver Status 123
 Query Running Time Overview 101, 107
 Query Viewer Details 101
 Report Details 101
 Reporting Subsystem Statistics 101, 107
 Resource Change Log 92
 Rules Status 107
 Storage 132
 Trend Details 101
 Data Monitor Evaluations Statistics report 109
 data monitors
 Actor Change Log 86
 Actor Change Overview 86
 Archive Disk Space 119
 ArcSight Reporting Statistics 104, 111
 ArcSight User Sessions 82
 ASM Database Responsiveness - Last 24 hours 127
 ASM Database Responsiveness - Last Hour 126
 Connector Cache Status 44, 68
 Connector Connection Status 44, 68
 CPU Sensors 134
 CPU Usage (Percent) - Last 10 Minutes 51, 135

CPU Usage (Percent) - Last Hour 134
 Critical Devices - Heads Up Display 75
 Current Connector Status 44, 68
 Current Users Logged In 82
 Currently Running Reports 103, 110
 Database Free Space 119, 126
 Database Insert Time - Last 24 Hours 119, 126
 Database Insert Time - Last Hour 119, 126
 Database Retrieval Time - Last 24 Hours 119, 126
 Database Retrieval Time - Last Hour 119, 126
 Database Transaction Volume 119, 126
 Disk Read and Write (Kbytes per Second) - Last 10 Minutes 51, 135
 Disk Read and Write (Kbytes per Second) - Last Hour 135
 Disk Usage 50, 135
 Disk Usage (Percent) 134
 EPS Usage (Events per Second) - Last 10 Minutes 51, 134
 EPS Usage (Events per Second) - Last Hour 134
 Event Throughput 97
 Event Throughput Statistics 97
 Events By Priority 96
 FAN Sensors 135
 Last 10 Trend Queries Returning No Results 104
 Latest Elevated Threat Events 97
 Latest Guarded Threat Events 97
 Latest High Threat Events 97
 Latest Low Threat Events 97
 Latest Severe Threat Events 97
 Logger Disk Usage 50
 Logger Hardware Status 50
 Memory Usage (Mbytes per Second) - Last 10 Minutes 51, 134
 Memory Usage (Mbytes per Second) - Last Hour 135
 Network Usage (Bytes) - Last 10 Minutes 50, 133
 Network Usage (Bytes) - Last Hour 133
 Notification Log 82
 Partial Matches per Rule 111
 Partition Manager and Archiver - Heads Up Display 126
 Partition Manager and Archiver Details 126
 Recent Archive Events 119
 Recent Fired Rules 111
 Recent System Resource Deletes 93
 Recent System Resource Inserts 93
 Recent System Resource Updates 93
 Report Statistics 104, 111
 Resource Change Log 93
 Resource Change Overview 93
 Rule Error Logs 111
 Rules Engine Internal Stats 110
 Sensor Type Status 51, 134
 Sidetable Cache Hit Rates 127
 Sidetable Sizes (Rows) 126
 System Information 46
 System Sensors 135
 Top Event Sources 43, 75
 Top Firing Rules 111
 User Access Log 82
 Database Free Space data monitor 119, 126
 Database Insert Time - Last 24 Hours data monitor 119, 126
 Database Insert Time - Last Hour data monitor 119, 126

Database Insert Time Statistics filter 119, 127
 Database Performance Statistics dashboard 115, 123
 Database Retrieval Time - Last 24 Hours data monitor 119, 126
 Database Retrieval Time - Last Hour data monitor 119, 126
 Database Retrieval Time Statistics filter 120, 128
 Database Transaction Volume data monitor 119, 126
 Deleted report 85
 Department New Value global variable 86
 Department Old Value global variable 89
 description global variable 20
 Destination Counts by Connector Type query 78
 Destination Counts by Connector Type report 73
 Destination Counts query 99
 Destination Counts report 96
 destinations
 admincert 79
 Device Asset Auto Creation Controller filter 33
 Device Monitoring use case 45
 Device Reported rule 74
 Device Status dashboard 72
 Devices Licensing Report focused report 80
 Disk Name global variable 52
 Disk Read and Write (Kbytes per Second) - Last 10 Minutes data monitor 51, 135
 Disk Read and Write (Kbytes per Second) - Last Hour data monitor 135
 Disk Read and Write filter 54, 137
 Disk Usage (Percent) data monitor 134
 Disk Usage data monitor 50, 135
 Disk Usage filter 137
 Disk Usage global variable 51
 DiskUsageCritical global variable 51
 DN New Value global variable 86
 DN Old Value global variable 87

E

Elevated Threat Condition filter 99
 Email Address New Value global variable 88
 Email Address Old Value global variable 88
 Employee Type New Value global variable 88
 Employee Type Old Value global variable 87
 EPS Licensing Report focused report 80
 EPS Usage (Events per Second) - Last 10 Minutes data monitor 51, 134
 EPS Usage (Events per Second) - Last Hour data monitor 134
 EPS Usage filter 54, 137
 ESM Configuration Changes by Type report 92
 ESM Configuration Changes by User report 92
 ESM Configuration Changes query 94
 ESM Events use case 47
 ESM Licensing use case 47
 ESM Reporting Resource Monitoring use case 47, 114
 ESM Resource Configuration Changes use case 47
 ESM Resource Monitoring use case 47
 ESM Storage Monitoring (CORR) use case 47
 ESM Storage Monitoring (Oracle) use case 47
 ESM System Information dashboard 46
 ESM User Sessions use case 47
 Event Base field set 31, 46, 59, 68, 97, 104
 Event Count by Agent Severity query 99
 Event Count by Agent Severity report 96

Event Count by Source Destination Pairs query 100
 Event Count by Source Destination Pairs report 96
 Event Data Free Space - Last 30 Days focused report 121, 128
 Event Distribution Chart for a Connector Type query 76
 Event Distribution Chart for a Connector Type report 73
 Event Index Free Space - Last 30 Days focused report 128
 Event Inspector field set 32
 Event Name Counts query 100
 Event Name Counts report 95
 Event Throughput dashboard 95
 Event Throughput data monitor 97
 Event Throughput Statistics data monitor 97
 Event-based Rule Exclusions active list 31
 Events by ArcSight Priority (Summary) query 100
 Events by ArcSight Priority (Summary) report 96
 Events by Connector Type (Summary) query 77
 Events by Connector Type (Summary) report 72
 Events by Device (Summary) query 76
 Events by Device (Summary) report 72
 Events By Priority data monitor 96
 Events by Selected Connector Type query 77
 Events by Selected Connector Type report 73
 Events for a Destination by Connector Type query 76
 Events for a Destination by Connector Type report 73
 Events from a Source by Connector Type query 77
 Events from a Source by Connector Type report 74
 Excessive Rule Recursion rule 110
 Executive field set 31
 Export field set 32
 External Source filter 98
 External Target filter 99
 externalID global variable 19

F

Failed Connector Upgrades query 60
 Failed Connector Upgrades report 56
 Failed Queries - Trend query 105, 113
 Failed Queries query 105, 112
 Failed Queries report 103
 Failed Queries trend 106, 114
 FAN Sensors data monitor 135
 FAN Sensors filter 137
 Field Set Based On ARC_E_ET Index field set 31
 Field Set Based On ARC_E_MRT Index field set 31
 field sets
 Actor Audit Field Set 89
 Actor Base 20
 Actor Information 20
 Annotation 32
 Annotation-MgrRcpt 31
 ArcSight Admin 32, 46, 97
 ASM Events 97
 Asset 32
 Asset Information 32
 Case Information 32
 Categories 32
 Common Conditions Editor 31
 Connector Monitoring Events 32, 46, 68, 97
 Connector Upgrades 59
 Event Base 31, 46, 59, 68, 97, 104
 Event Inspector 32
 Executive 31

- Export 32
- Field Set Based On ARC_E_ET Index 31
- Field Set Based On ARC_E_MRT Index 31
- Logger Application Events 130
- Logger Platform Events 130
- Logger System Health Events 52, 136
- Minimal 32
- MSSP 32
- Query Status 104
- Rule Action - Set Event Field 32
- Security 32
- Standard 31
- Standard-MgrRcpt 32
- Super Minimal 31
- TurboMode Comprehensive 31
- TurboMode Fastest 32
- Field Status global variable 52
- Field Value global variable 52
- File Path StartsWith All Rules filter 120
- filters
 - Actor Changes 90
 - Actor Deletes 89
 - Actor Inserts 89
 - Actor Name or UUID 89
 - Actor Updates 89
 - All Events 33, 75, 83, 89, 93, 98, 112
 - All Receivers EPS 53
 - Archive Archival Success 119
 - Archive Disk Space 120
 - Archive Disk space status is Critical 120
 - Archive Disk space status is OK 120
 - Archive Events 120
 - Archive Failure Events 120
 - Archive Settings Updated Event 119
 - ArcSight Audit Events 99
 - ArcSight Correlation Events 33, 54, 137
 - ArcSight Events 33, 44, 76
 - ArcSight Internal Events 33, 46, 99
 - ArcSight Login Events 83
 - ArcSight Login Rule Firings 83
 - ArcSight Login Tracking 82
 - ArcSight Rules 111
 - ArcSight Status Monitoring Events 97
 - ASM CPU Load 98
 - ASM Database Load Statistics 98, 119, 127
 - ASM Database Statistics 119, 127
 - ASM Event Flow 97
 - ASM Events 33, 46, 98
 - ASM Flow Load 99
 - ASM Load Overview 98
 - ASM Reports Statistics 104, 111
 - ASM Resource and Memory Load 98
 - ASM Sidetable Cache Hit Rates 128
 - ASM Sidetable Sizes 127
 - ASM Standing Load 99
 - Attacker Address is NULL 90
 - Attacker Host Name is NULL 90
 - Attacker Information is NULL 89
 - Attacker Port is NULL 89
 - Attacker User Name is NULL 20, 34
 - Attacker Zone AND Host are NULL 89
 - Attacker Zone AND Host are NULL but Address is NOT NULL 90
 - Attacker Zone is NULL 89
 - Attacker Zone OR Host is NULL 89
 - Attackers on Hostile List 28
 - Attackers on Infiltrators List 28
 - Attackers on Reconnaissance List 28
 - Attackers on Suspicious List 28
 - Blocked ArcSight Internal Events 33
 - Compromised Targets 28
 - Connector Asset Auto Creation Controller 33
 - Connector Cache Status 44, 68
 - Connector Caching Event 68
 - Connector Connection Status 44, 69
 - Connector Registered or Heartbeat Event 68
 - Correlation Events 20, 34
 - CPU Sensors 136
 - CPU Usage 53, 136
 - Critical Device Not Reporting 75
 - Critical Devices Up Down 76
 - Database Insert Time Statistics 119, 127
 - Database Retrieval Time Statistics 120, 128
 - Device Asset Auto Creation Controller 33
 - Disk Read and Write 54, 137
 - Disk Usage 137
 - Elevated Threat Condition 99
 - EPS Usage 54, 137
 - External Source 98
 - External Target 99
 - FAN Sensors 137
 - File Path StartsWith All Rules 120
 - Guarded Threat Condition 98
 - High Criticality Assets 27
 - High Threat Condition 98
 - Hour less than 10 104, 111
 - Inbound Events 98
 - Inbound Network 54
 - Internal Source 98
 - Internal Target 98
 - Logger Application Events 130
 - Logger Disk Usage 54, 137
 - Logger Events 53, 130, 136
 - Logger Hardware Status 53
 - Logger Platform Events 130
 - Logger System Health Events 52, 130, 136
 - Low Criticality Assets 28
 - Low Threat Condition 99
 - ManagerInternalAgent'sFilters' 32
 - Medium Criticality Assets 28
 - Memory Usage 52, 136
 - Minute less than 10 104, 112
 - My Logger 53, 137
 - Network Usage 53, 136
 - No Events 33
 - Non-ArcSight Events 34, 44, 76
 - Non-ArcSight Internal Events 34, 99
 - Non-Categorized Events 32
 - Not Correlated and Not Closed 33
 - Not Correlated and Not Closed and Not Hidden 33
 - Notification Actions 82, 98
 - Outbound Events 98
 - Partition Manager and Archiver Events 128
 - Partition without Submission Events 128
 - Remaining Disk 54
 - Remaining Disk > 10 Percent 53
 - Resource Changes 93
 - Resource Deletes 93
 - Resource Inserts 93
 - Resource Updates 93

- Rules Engine Internal Events 111
- Sensor Type is CPU 52, 136
- Sensor Type is FAN 53, 136
- Sensor Type Update 53, 137
- Severe Threat Condition 98
- Severity High 34
- Severity Low 33
- Severity Medium 34
- Severity Unknown 34
- Severity Very High 32
- SNMP Trap Sender 33
- System Sensors 137
- Target Asset Scanned for Open Ports 27
- Target Asset Scanned for Vulnerabilities 28
- Target User Name is NULL 90, 93
- Threshold - Critical 120, 127
- Threshold - Warning 120, 127
- Trend Query Returning No Results 104
- Unknown Criticality Assets 27
- Very High Criticality Assets 27
- Very Low Criticality Assets 27
- White List - Critical Devices 75
- White List - Devices 76
- Final stage 37
- FIPS-199 asset category 27
- Fired Rule Events query 112
- Fired Rule Events report 109
- Flagged as Similar stage 37
- focused reports
 - Actors Licensing Report 80
 - Assets Licensing Report 80
 - Console Users Licensing Report 80
 - Devices Licensing Report 80
 - EPS Licensing Report 80
 - Event Data Free Space - Last 30 Days 121, 128
 - Event Index Free Space - Last 30 Days 128
 - System Data Free Space - Last 30 Days 120, 128
 - System Index Free Space - Last 30 Days 128
 - Web Users Licensing Report 80
- Follow-Up stage 37
- Free Space global variable 51
- Full Name New Value global variable 86
- Full Name Old Value global variable 88

G

- global variables
 - Actor 87
 - ActorByAccountID 19
 - ActorByAttackerUserName 19
 - ActorByCustomFields 19
 - ActorByDN 20
 - ActorByTargetUserName 20
 - ActorByUUID 20
 - ActorFromFileName 87
 - alias 20
 - All Receivers and Forwarders 52
 - AttackerHost 88
 - Change Source 87
 - CPU Name 52
 - createTime 19
 - creator 19
 - Department New Value 86
 - Department Old Value 89
 - description 20

- Disk Name 52
- Disk Usage 51
- DiskUsageCritical 51
- DN New Value 86
- DN Old Value 87
- Email Address New Value 88
- Email Address Old Value 88
- Employee Type New Value 88
- Employee Type Old Value 87
- externalID 19
- Field Status 52
- Field Value 52
- Free Space 51
- Full Name New Value 86
- Full Name Old Value 88
- groupId 19
- id 20
- Inbound and Outbound 52
- IndexOfUsage 52
- Location New Value 87
- Location Old Value 87
- Logger Address 52
- Logger IP 52, 136
- Manager New Value 87
- Manager Old Value 88
- Memory Name 52
- modificationTime 20
- name 19
- Org New Value 87
- Org Old Value 88
- owner 20
- ReadOrWrite 51
- Sensor Name 51
- Sensor Status 51
- Sensor Type 52
- Status New Value 88
- Status Old Value 88
- Timeframe 51
- Title New Value 87
- Title Old Value 88
- Unit 52
- groupId global variable 19
- Guarded Threat Condition filter 98

H

- Hardware dashboard 132
- High asset category 26, 27, 75
- High Criticality Assets filter 27
- High Threat Condition filter 98
- High Volume Connector EPS - By Day query 77
- High Volume Connector EPS - Daily report 74
- High Volume Connector EPS - Hourly query 77
- High Volume Connector EPS - Weekly report 73
- Hit List active list 25
- Hostile - Attempt rule 24
- Hostile - Success rule 24
- Hostile List active list 25
- Hour less than 10 filter 104, 111
- Hourly Distribution Chart for a Destination Port query 100
- Hourly Distribution Chart for a Destination Port report 96
- Hourly Distribution Chart for a Source Port query 99
- Hourly Distribution Chart for a Source Port report 96
- Hourly Distribution Chart for Event query 100

- Hourly Distribution Chart for Event report 96
- Hourly Event Counts (Area Chart) query 100
- Hourly Event Counts (Area Chart) report 96
- Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart) query 99
- Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart) report 95

I

- id global variable 20
- IDM Deletions of Actors query 90
- IDM Deletions of Actors query viewer 84
- IDM Deletions of Actors report 85
- Inbound and Outbound global variable 52
- Inbound Events filter 98
- Inbound Network filter 54
- Incident Resolved - Remove From List rule 25
- IndexOfUsage global variable 52
- Infiltrators List active list 26
- Initial stage 37
- installing
 - ArcSight Administration 11
 - ArcSight System 11
- integration commands
 - By Destination 54
 - By Event Name 54
 - By Source 54
 - By Source and Destination 55
 - By User 54
 - By Vendor and Product 55
 - Logger Quick Search 55
 - Nslookup (Linux) 34
 - Nslookup (Windows) 34
 - Ping (Linux) 34
 - Ping (Windows) 34
 - Portinfo (Linux) 35
 - Portinfo (Windows) 34
 - Traceroute (Linux) 35
 - Traceroute (Windows) 34
 - Web Search 34
 - Whois (Linux) 35
 - Whois (Windows) 35
- integration configurations
 - Logger Quick Search 55
 - Logger Search 55
 - Nslookup (Linux) 35
 - Nslookup (Windows) 35
 - Ping (Linux) 36
 - Ping (Windows) 36
 - Portinfo (Linux) 35
 - Portinfo (Windows) 36
 - Traceroute (Linux) 36
 - Traceroute (Windows) 35
 - Web Search 36
 - Whois (Linux) 36
 - Whois (Windows) 36
- integration targets
 - Logger Appliance 1 55
 - Logger Appliance 2 55
- Internal Source filter 98
- Internal Target filter 98
- invalid resources 141
- Invalid Resources (Chart) query 112
- Invalid Resources active list 110
- Invalid Resources query 112
- Invalid Resources report 108

L

- Last 10 Query Viewer Queries query viewer 102
- Last 10 QueryViewer Queries query 105
- Last 10 Report Queries query 105
- Last 10 Report Queries query viewer 102
- Last 10 Trend Queries query 106
- Last 10 Trend Queries query viewer 102
- Last 10 Trend Queries Returning No Results data monitor 104
- Last 5 Minutes active channel 30
- Last Hour active channel 30
- Latest Elevated Threat Events data monitor 97
- Latest Events By Priority dashboard 95
- Latest Guarded Threat Events data monitor 97
- Latest High Threat Events data monitor 97
- Latest Low Threat Events data monitor 97
- Latest Severe Threat Events data monitor 97
- License Audit Event Detected rule 79
- License Limit Approaching rule 79
- License Limit Exceeded rule 79
- Licensing History session list 80
- Licensing Query query 80
- Licensing Report (All) report 79
- Licensing Report report 79
- Live active channel 30
- Location New Value global variable 87
- Location Old Value global variable 87
- Logger Address global variable 52
- Logger Appliance 1 integration target 55
- Logger Appliance 2 integration target 55
- Logger Application Events active channel 130
- Logger Application Events field set 130
- Logger Application Events filter 130
- Logger Disk Usage data monitor 50
- Logger Disk Usage filter 54, 137
- Logger Events filter 53, 130, 136
- Logger Events use case 55
- Logger Hardware Status data monitor 50
- Logger Hardware Status filter 53
- Logger IP global variable 52, 136
- Logger Platform Events active channel 130
- Logger Platform Events field set 130
- Logger Platform Events filter 130
- Logger Quick Search integration command 55
- Logger Quick Search integration configuration 55
- Logger Search integration configuration 55
- Logger Sensor Status rule 49, 132
- Logger Sensor Type Status active list 50, 133
- Logger Sensor Type Status rule 49, 133
- Logger Status active list 50, 133
- Logger Status rule 49, 133
- Logger System Health Events active channel 132
- Logger System Health Events field set 52, 136
- Logger System Health Events filter 52, 130, 136
- Logger System Health use case 55
- Longest QueryViewer Queries - Trend query 105
- Longest QueryViewer Queries query 104, 112
- Longest QueryViewer Queries report 103
- Longest Report Queries - Trend query 106
- Longest Report Queries query 105, 113
- Longest Report Queries report 103

Longest Trend Queries - Trend query 105
 Longest Trend Queries query 105, 112
 Longest Trend Query report 103
 Low asset category 26, 27
 Low Criticality Assets filter 28
 Low Threat Condition filter 99
 Low Volume Connector EPS - By Day query 76
 Low Volume Connector EPS - Daily report 72
 Low Volume Connector EPS - Hourly query 77
 Low Volume Connector EPS - Weekly report 74

M

Manager Internal AgentsFiltersfilter 32
 Manager New Value global variable 87
 Manager Old Value global variable 88
 Medium asset category 27
 Medium Criticality Assets filter 28
 Memory Name global variable 52
 Memory Usage (Mbytes per Second) - Last 10 Minutes data monitor 51, 134
 Memory Usage (Mbytes per Second) - Last Hour data monitor 135
 Memory Usage filter 52, 136
 Minimal field set 32
 Minute less than 10 filter 104, 112
 Moderate asset category 26
 modificationTime global variable 20
 Monitoring stage 37
 MSSP field set 32
 My Logger filter 53, 137
 My Logger Overview dashboard 49, 132

N

name global variable 19
 Network dashboard 132
 Network Usage (Bytes) - Last 10 Minutes data monitor 50, 133
 Network Usage (Bytes) - Last Hour data monitor 133
 Network Usage filter 53, 136
 No Events filter 33
 Non-ArcSight Events filter 34, 44, 76
 Non-ArcSight Internal Events filter 34, 99
 Non-Categorized Events filter 32
 Not Correlated and Not Closed and Not Hidden filter 33
 Not Correlated and Not Closed filter 33
 Notification Actions filter 82, 98
 Notification Log data monitor 82
 Nslookup (Linux) integration command 34
 Nslookup (Linux) integration configuration 35
 Nslookup (Windows) integration command 34
 Nslookup (Windows) integration configuration 35
 Number of Events matching Rules query 113
 Number of Events Matching Rules report 109

O

Open Ports asset category 26
 Org New Value global variable 87
 Org Old Value global variable 88
 Out of Domain Fields rule 118, 125
 Outbound Events filter 98
 owner global variable 20

P

Partial Matches per Rule data monitor 111
 Partition Manager and Archiver - Heads Up Display data monitor 126
 Partition Manager and Archiver Details data monitor 126
 Partition Manager and Archiver Events filter 128
 Partition Manager and Archiver Status dashboard 123
 Partition without Submission Events filter 128
 Personal Live active channel 30
 Ping (Linux) integration command 34
 Ping (Linux) integration configuration 36
 Ping (Windows) integration command 34
 Ping (Windows) integration configuration 36
 Portinfo (Linux) integration command 35
 Portinfo (Linux) integration configuration 35
 Portinfo (Windows) integration command 34
 Portinfo (Windows) integration configuration 36
 profiles
 Daily Pattern Discovery 37
 Quarter Hourly Pattern Discovery 37
 Protected asset category 96

Q

Quarter Hourly Pattern Discovery profile 37
 queries
 Active List Access 113
 Active List Access (Details) 113
 Actor Authenticators 90
 Actor Configuration Changes 90
 Actor Event Count by Account ID 21
 Actor Event Count by Attacker Username 20
 Actor Event Count by Custom Fields 21
 Actor Event Count by Target Username 21
 Actor Events by Account ID 21
 Actor Events by Attacker Username 20
 Actor Events by Custom Fields 21
 Actor Events by Target Username 20
 Actor Full Name and Email Changes 90
 Actor Information 21
 Actor Manager and Department Changes 90
 Actor Title and Status Changes 91
 Actors Created 91
 Actors Deleted 90
 Actors Updated 91
 Archive Activation Statistics 121
 Archive Archival Statistics 122
 Archive Archival Success 122
 Archive Deactivation Statistics 121
 Archive Disk Space Usage 121
 Archive Non-success events 121
 Archive Scheduling Statistics 122
 Archive Space status 122
 Archive status 121
 Archive Task Failure Details 121
 ArcSight User Hourly Login Trends 83
 ArcSight User Logins - Last Hour 83
 ASM Database Free Space 121, 129
 ASM Database Free Space - by Day 121, 129
 ASM Database Free Space - by Hour 121, 129
 ASM Database Free Space (current) 122, 129
 Average Data Monitor Evaluations Per Second 113
 Cache History by Connectors 69
 Connector Average EPS - Last 7 Days 77

- Connector Daily Average EPS 77
- Connector Monitor Event 76
- Connector Severity Hourly Stacked Chart 77
- Connector Upgrades Count 60
- Connector Upgrades Count (Total) 60
- Connector Versions 60
- Connector Versions by Type 60
- Connectors - Caching - Long Term 45, 69
- Connectors - Caching - Short Term 45, 69
- Connectors - Down 44, 69
- Connectors - Dropping Events 44, 69
- Connectors - Still Down 45, 69
- Correlation Events Count 112
- Correlation Events Count (Details) 112
- Critical Archive Failure Details 121
- Current Cache Status - Caching Events 69
- Current Cache Status - Dropping Events 69
- Destination Counts 99
- Destination Counts by Connector Type 78
- ESM Configuration Changes 94
- Event Count by Agent Severity 99
- Event Count by Source Destination Pairs 100
- Event Distribution Chart for a Connector Type 76
- Event Name Counts 100
- Events by ArcSight Priority (Summary) 100
- Events by Connector Type (Summary) 77
- Events by Device (Summary) 76
- Events by Selected Connector Type 77
- Events for a Destination by Connector Type 76
- Events from a Source by Connector Type 77
- Failed Connector Upgrades 60
- Failed Queries 105, 112
- Failed Queries - Trend 105, 113
- Fired Rule Events 112
- High Volume Connector EPS - By Day 77
- High Volume Connector EPS - Hourly 77
- Hourly Distribution Chart for a Destination Port 100
- Hourly Distribution Chart for a Source Port 99
- Hourly Distribution Chart for Event 100
- Hourly Event Counts (Area Chart) 100
- Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart) 99
- IDM Deletions of Actors 90
- Invalid Resources 112
- Invalid Resources (Chart) 112
- Last 10 QueryViewer Queries 105
- Last 10 Report Queries 105
- Last 10 Trend Queries 106
- Licensing Query 80
- Longest QueryViewer Queries 104, 112
- Longest QueryViewer Queries - Trend 105
- Longest Report Queries 105, 113
- Longest Report Queries - Trend 106
- Longest Trend Queries 105, 112
- Longest Trend Queries - Trend 105
- Low Volume Connector EPS - By Day 76
- Low Volume Connector EPS - Hourly 77
- Number of Events matching Rules 113
- Query Counts During Last 24 hr 105, 113
- Query Counts During Last Week 106
- QueryViewer Failures 105
- QueryViewer Queries 104
- Report Queries 106
- Report Query Failures 106
- Resource Created Report 94
- Resource Deleted Report 94
- Resource History Report 94
- Resource Updated Report 94
- Rules Engine Warning Messages 113
- Running Report Queries 106
- Running Trend Queries 106
- Session List Access 113
- Session List Access (Details) 112
- Source Counts by Connector Type 76
- Source Counts by Event Name 100
- Successful Connector Upgrades 60
- Top 10 Events 99
- Top 10 Inbound Events 99
- Top 10 Outbound Events 100
- Top Accessed Active Lists 112
- Top Accessed Session Lists 113
- Top Connector Types Chart 77
- Trend Query 105
- Trend Query Failures 105
- Upgrade History by Connector 59
- Upgrade History by Connector Type 60
- User Login Logout Report 83
- Version History by Connector 60
- Version History by Connector Type 60
- Query Counts by Type report 103
- Query Counts During Last 24 hr query 105, 113
- Query Counts During Last 24 hr query viewer 102, 108
- Query Counts During Last Week query 106
- Query Failures During Last 24 hr query viewer 102, 107
- Query Running Time active list 103, 110
- Query Running Time Overview dashboard 101, 107
- Query Running Time rule 103
- Query Status field set 104
- Query Viewer Details dashboard 101
- Query Viewer Failures During Last 24 hr query viewer 103
- query viewers
 - Actor Authenticators 84
 - Actor Configuration Changes 84
 - Actor Full Name and Email Changes 85
 - Actor Manager and Department Changes 84
 - Actor Title and Status Changes 85
 - Actors Created 85
 - Actors Deleted 85
 - Actors Updated 84
 - Archive Task Failure Details 115
 - Connectors - Caching - Long Term 42, 63
 - Connectors - Caching - Short Term 42, 63
 - Connectors - Down - Long Term 42, 63
 - Connectors - Down - Short Term 41, 62
 - Connectors - Dropping Events 41, 62
 - Critical Archive Failure Details 115
 - IDM Deletions of Actors 84
 - Last 10 Query Viewer Queries 102
 - Last 10 Report Queries 102
 - Last 10 Trend Queries 102
 - Query Counts During Last 24 hr 102, 108
 - Query Failures During Last 24 hr 102, 107
 - Query Viewer Failures During Last 24 hr 103
 - Report Query Failures During Last 24 hr 102
 - Running Report Queries 102
 - Running Trend Queries 102
 - Top 10 Longest Query Viewer Queries During Last 24 hr 102, 108
 - Top 10 Longest Report Queries During Last 24 hr

- 102, 108
 - Top 10 longest Trend Queries During Last 24 hr 102, 107
 - Trend Queries Failures During Last 24 hr 102
 - Query Viewers Status active channel 101
 - QueryViewer Failures query 105
 - QueryViewer Queries query 104
 - QueryViewer Queries trend 106
 - Queued stage 37
- R**
- ReadOrWrite global variable 51
 - Recent Archive Events data monitor 119
 - Recent Fired Rules data monitor 111
 - Recent System Resource Deletes data monitor 93
 - Recent System Resource Inserts data monitor 93
 - Recent System Resource Updates data monitor 93
 - Reconnaissance - Distributed Host Port Scan rule 23
 - Reconnaissance - Distributed Network Host Scan rule 24
 - Reconnaissance - In Progress rule 22
 - Reconnaissance - Multiple Host Scan rule 23
 - Reconnaissance - Network Service Scan rule 23
 - Reconnaissance - Script Scan rule 25
 - Reconnaissance - Stealthy Host Port Scan rule 23
 - Reconnaissance - Vulnerability Scan rule 25
 - Reconnaissance List active list 26
 - Remaining Disk 54
 - Remaining Disk > 10 Percent filter 53
 - Report Details dashboard 101
 - Report Queries query 106
 - Report Queries trend 106
 - Report Query Failures During Last 24 hr query viewer 102
 - Report Query Failures query 106
 - Report Statistics data monitor 104, 111
 - Reporting Devices - Critical active list 75
 - Reporting Devices active list 75
 - Reporting Subsystem Statistics dashboard 101, 107
 - reports
 - Active List Access 108
 - Actor Context Report by Account ID 18
 - Actor Context Report by Attacker Username 18
 - Actor Context Report by Custom Fields 18
 - Actor Context Report by Target Username 18
 - Actor Full Name and Email Changes 85
 - Actor Manager and Department Changes 86
 - Actor Title and Status Changes 86
 - Archive Processing 116
 - Archive Status Report 115
 - ArcSight User Login Trends 81
 - ArcSight User Logins - Last Hour 81
 - ASM Database Free Space 116, 124
 - ASM Database Free Space - by Day 116, 124
 - ASM Database Free Space - by Hour 116, 123
 - Assets having Vulnerability 31
 - Cache History by Connectors 63
 - Configuration Changes by Type 85
 - Configuration Changes by User 86
 - Connector Severity Hourly Stacked Chart 72
 - Connector Upgrades Count 57
 - Connector Versions 56
 - Connector Versions by Type 56
 - Correlation Events Statistics 109
 - Created 86
 - Current Cache Status 63
 - Data Monitor Evaluations Statistics 109
 - Deleted 85
 - Destination Counts 96
 - Destination Counts by Connector Type 73
 - ESM Configuration Changes by Type 92
 - ESM Configuration Changes by User 92
 - Event Count by Agent Severity 96
 - Event Count by Source Destination Pairs 96
 - Event Distribution Chart for a Connector Type 73
 - Event Name Counts 95
 - Events by ArcSight Priority (Summary) 96
 - Events by Connector Type (Summary) 72
 - Events by Device (Summary) 72
 - Events by Selected Connector Type 73
 - Events for a Destination by Connector Type 73
 - Events from a Source by Connector Type 74
 - Failed Connector Upgrades 56
 - Failed Queries 103
 - Fired Rule Events 109
 - High Volume Connector EPS - Daily 74
 - High Volume Connector EPS - Weekly 73
 - Hourly Distribution Chart for a Destination Port 96
 - Hourly Distribution Chart for a Source Port 96
 - Hourly Distribution Chart for Event 96
 - Hourly Event Counts (Area Chart) 96
 - Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart) 95
 - IDM Deletions of Actors 85
 - Invalid Resources 108
 - Licensing Report 79
 - Licensing Report (All) 79
 - Longest QueryViewer Queries 103
 - Longest Report Queries 103
 - Longest Trend Query 103
 - Low Volume Connector EPS - Daily 72
 - Low Volume Connector EPS - Weekly 74
 - Number of Events Matching Rules 109
 - Query Counts by Type 103
 - Resource Created Report 92
 - Resource Deleted Report 92
 - Resource History Report 92
 - Resource Updated Report 93
 - Rules Engine Warning Messages 108
 - Session List Access 108
 - Source Counts by Connector Type 73
 - Source Counts by Event Name 95
 - Successful Connector Upgrades 57
 - Top 10 Events 95
 - Top 10 Inbound Events 95
 - Top 10 Outbound Events 96
 - Top Accessed Active Lists 109
 - Top Accessed Session Lists 109
 - Top Connector Types Chart 74
 - Updated 85
 - Upgrade History by Connector 56
 - Upgrade History by Connector Type 56
 - User Login Logout Report 81
 - Version History by Connector 57
 - Version History by Connector Type 57
 - Vulnerabilities of an Asset 31
 - Reports Status active channel 101
 - Resource Became Invalid rule 109
 - Resource Became Valid rule 110
 - Resource Change Log dashboard 92

- Resource Change Log data monitor 93
- Resource Change Overview data monitor 93
- Resource Changes filter 93
- Resource Created Report query 94
- Resource Created Report report 92
- Resource Deleted Report query 94
- Resource Deleted Report report 92
- Resource Deletes filter 93
- Resource History Report query 94
- Resource History Report report 92
- Resource Inserts filter 93
- Resource Updated Report query 94
- Resource Updated Report report 93
- Resource Updates filter 93
- Rule Action - Set Event Field field set 32
- Rule Created stage 37
- Rule Error Logs data monitor 111
- Rule Matching Too Many Events rule 110
- rules
 - Archive Events 117
 - Archive Task Failures 118
 - Archive Task Success 116
 - ArcSight User Login 82
 - ArcSight User Login Timeout 82
 - ArcSight User Logout 81
 - ASM Database Free Space - Critical 117, 125
 - ASM Database Free Space - Warning 118, 125
 - ASM Database Status Change - Critical 117, 124
 - ASM Database Status Change - Down 116, 124
 - ASM Database Status Change - Normal 117, 125
 - ASM Database Status Change - Space Critical 118, 125
 - ASM Database Status Change - Space Now Available 117, 124
 - ASM Database Status Change - Warning 118, 125
 - Compromise - Attempt 25
 - Compromise - Success 24
 - Connector Added to Black List 65
 - Connector Cache Empty 65
 - Connector Caching 65
 - Connector Deleted 57, 64
 - Connector Discovered or Updated 66
 - Connector Down 65
 - Connector Dropping Events 65
 - Connector Still Caching 64
 - Connector Still Down 64
 - Connector Up 64
 - Connector Upgrade Failed 57
 - Connector Upgrade Successful 58
 - Connector Version Detected 57, 65
 - Critical Archive Failures 116
 - Critical Archive Success 118
 - Critical Device Not Reporting 74
 - Critical Device Reported 74
 - Device Reported 74
 - Excessive Rule Recursion 110
 - Hostile - Attempt 24
 - Hostile - Success 24
 - Incident Resolved - Remove From List 25
 - License Audit Event Detected 79
 - License Limit Approaching 79
 - License Limit Exceeded 79
 - Logger Sensor Status 49, 132
 - Logger Sensor Type Status 49, 133
 - Logger Status 49, 133

- Out of Domain Fields 118, 125
- Query Running Time 103
- Reconnaissance - Distributed Host Port Scan 23
- Reconnaissance - Distributed Network Host Scan 24
- Reconnaissance - In Progress 22
- Reconnaissance - Multiple Host Scan 23
- Reconnaissance - Network Service Scan 23
- Reconnaissance - Script Scan 25
- Reconnaissance - Stealthy Host Port Scan 23
- Reconnaissance - Vulnerability Scan 25
- Resource Became Invalid 109
- Resource Became Valid 110
- Rule Matching Too Many Events 110
- Update Connector Caching Status 42, 64
- Update Connector Connection Status 42, 64
- Rules Engine Internal Events filter 111
- Rules Engine Internal Stats data monitor 110
- Rules Engine Warning Messages query 113
- Rules Engine Warning Messages report 108
- Rules Status dashboard 107
- Running Report Queries query 106
- Running Report Queries query viewer 102
- Running Trend Queries query 106
- Running Trend Queries query viewer 102

S

- Scanned List active list 26
- Security field set 32
- Sensor Name global variable 51
- Sensor Status global variable 51
- Sensor Type global variable 52
- Sensor Type is CPU filter 52, 136
- Sensor Type is FAN filter 53, 136
- Sensor Type Status data monitor 51, 134
- Sensor Type Update filter 53, 137
- Session List Access (Details) query 112
- Session List Access query 113
- Session List Access report 108
- session lists
 - Archive Events 122
 - ArcSight User Sessions 83
 - Connector - Caches 70
 - Connector Versions 60, 70
 - Licensing History 80
- Severe Threat Condition filter 98
- Severity High filter 34
- Severity Low filter 33
- Severity Medium filter 34
- Severity Unknown filter 34
- Severity Very High filter 32
- shared libraries 7
- Sidetable Cache Hit Rates data monitor 127
- Sidetable Sizes (Rows) data monitor 126
- SNMP Trap Sender filter 33
- Source Counts by Connector Type query 76
- Source Counts by Connector Type report 73
- Source Counts by Event Name query 100
- Source Counts by Event Name report 95
- stages
 - Closed 37
 - Final 37
 - Flagged as Similar 37
 - Follow-Up 37
 - Initial 37

- Monitoring 37
- Queued 37
- Rule Created 37
- Standard field set 31
- Standard-MgrRcpt field set 32
- Status New Value global variable 88
- Status Old Value global variable 88
- Storage dashboard 132
- Successful Connector Upgrades query 60
- Successful Connector Upgrades report 57
- Super Minimal field set 31
- Suspicious List active list 25
- System Data Free Space - Last 30 Days focused report 120, 128
- System Events Last Hour active channel 31, 46, 95
- System Index Free Space - Last 30 Days focused report 128
- System Information data monitor 46
- System Sensors data monitor 135
- System Sensors filter 137

T

- Target Asset Scanned for Open Ports filter 27
- Target Asset Scanned for Vulnerabilities filter 28
- Target User Name is NULL filter 90, 93
- Threshold - Critical filter 120, 127
- Threshold - Warning filter 120, 127
- Timeframe global variable 51
- Title New Value global variable 87
- Title Old Value global variable 88
- Today active channel 30
- Top 10 Events query 99
- Top 10 Events report 95
- Top 10 Inbound Events query 99
- Top 10 Inbound Events report 95
- Top 10 Longest Query Viewer Queries During Last 24 hr query viewer 102, 108
- Top 10 Longest Report Queries During Last 24 hr query viewer 102, 108
- Top 10 longest Trend Queries During Last 24 hr query viewer 102, 107
- Top 10 Outbound Events query 100
- Top 10 Outbound Events report 96
- Top Accessed Active Lists query 112
- Top Accessed Active Lists report 109
- Top Accessed Session Lists query 113
- Top Accessed Session Lists report 109
- Top Connector Types Chart query 77
- Top Connector Types Chart report 74
- Top Event Sources data monitor 43, 75
- Top Firing Rules data monitor 111
- Traceroute (Linux) integration command 35
- Traceroute (Linux) integration configuration 36
- Traceroute (Windows) integration command 34
- Traceroute (Windows) integration configuration 35
- Trend Details dashboard 101
- Trend Queries Failures During Last 24 hr query viewer 102
- Trend Queries trend 106
- Trend Query Failures query 105
- Trend Query query 105
- Trend Query Returning No Results filter 104
- trends

- ArcSight User Login Trends - Hourly 83
- ASM Database Free Space 122, 129
- Connector Average EPS - Last 7 days 78
- Connector Daily Average EPS 78
- Connector Total Events - Hourly 78
- Failed Queries 106, 114
- QueryViewer Queries 106
- Report Queries 106
- Trend Queries 106
- Trends Status active channel 101
- Trusted List active list 26
- TurboMode Comprehensive field set 31
- TurboMode Fastest field set 32

U

- Unit global variable 52
- Unknown Criticality Assets filter 27
- Untrusted List active list 26
- Update Connector Caching Status rule 42, 64
- Update Connector Connection Status rule 42, 64
- Updated report 85
- upgrade
 - invalid resources 141
 - preparing for upgrade 139
 - restoring content 140
 - verify customer content 141
- Upgrade History by Connector query 59
- Upgrade History by Connector report 56
- Upgrade History by Connector Type query 60
- Upgrade History by Connector Type report 56
- use cases
 - Actor Configuration Changes 47
 - Connector Configuration Changes 45
 - Connector Connection and Cache Status 45
 - Device Monitoring 45
 - ESM Events 47
 - ESM Licensing 47
 - ESM Reporting Resource Monitoring 47, 114
 - ESM Resource Configuration Changes 47
 - ESM Resource Monitoring 47
 - ESM Storage Monitoring (CORR) 47
 - ESM Storage Monitoring (Oracle) 47
 - ESM User Sessions 47
 - Logger Events 55
 - Logger System Health 55
- User Access Log data monitor 82
- User Login Logout Report query 83
- User Login Logout Report report 81
- User-based Rule Exclusions active list 31

V

- Version History by Connector query 60
- Version History by Connector report 57
- Version History by Connector Type query 60
- Version History by Connector Type report 57
- Very High asset category 27
- Very High Criticality Assets filter 27
- Very Low asset category 27
- Very Low Criticality Assets filter 27
- Vulnerabilities asset category 26
- Vulnerabilities of an Asset report 31

W

Web Search integration command 34
Web Search integration configuration 36
Web Users Licensing Report focused report 80
White List - Critical Devices filter 75

White List - Devices filter 76
Whois (Linux) integration command 35
Whois (Linux) integration configuration 36
Whois (Windows) integration command 35
Whois (Windows) integration configuration 36