

Standard Content Guide

ArcSight System and
ArcSight Administration

ArcSight Express 4.0
with CORR-Engine

March 4, 2013



Copyright © 2013 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>

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

This document is confidential.

Contact Information

| | |
|------------------------------|---|
| Phone | A list of phone numbers is available on the HP ArcSight Technical Support page: http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWI . |
| Support Web Site | http://support.openview.hp.com |
| Protect 724 Community | https://protect724.arcsight.com |

Revision History

| Date | Product Version | Description |
|------------|---|-----------------------------|
| 03/04/2013 | ArcSight System and ArcSight Administration content for ArcSight Express 4.0 with CORR-Engine | Final revision for release. |

Contents

| | |
|---|-----------|
| Chapter 1: Standard Content Overview | 5 |
| What is Standard Content? | 5 |
| Standard Content Documentation | 6 |
| Chapter 2: Installation and Configuration | 7 |
| Installing the Content | 7 |
| Configuring the Content | 7 |
| Modeling the Network | 8 |
| Categorizing Assets | 8 |
| Configuring Active Lists | 9 |
| Configuring Filters | 9 |
| Enabling Rules | 9 |
| Configuring Notification Destinations | 10 |
| Configuring Notifications and Cases | 10 |
| Rules with Notifications to the CERT Team | 10 |
| Rules with Notifications to SOC Operators | 10 |
| Scheduling Reports | 11 |
| Configuring Trends | 11 |
| Monitoring Trend Performance | 11 |
| Viewing Use Case Resources | 12 |
| Chapter 3: ArcSight System Content | 13 |
| Actor Support Resources | 14 |
| Resources | 14 |
| Priority Formula Resources | 18 |
| Configuration | 18 |
| Resources | 18 |
| System Resources | 26 |
| Configuration | 26 |
| Resources | 27 |
| Chapter 4: ArcSight Administration Content | 35 |
| Connector Overview | 37 |
| Configuration | 37 |

| | |
|---|------------|
| Resources | 37 |
| ESM Overview | 43 |
| Resources | 43 |
| Logger Overview | 45 |
| Configuration | 45 |
| Resources | 46 |
| Connector Configuration Changes | 54 |
| Resources | 54 |
| Connector Connection and Cache Status | 60 |
| Configuration | 60 |
| Resources | 61 |
| Device Monitoring | 72 |
| Configuration | 72 |
| Resources | 73 |
| ESM Licensing | 81 |
| Resources | 81 |
| ESM User Sessions | 84 |
| Resources | 84 |
| Actor Configuration Changes | 88 |
| Resources | 88 |
| ESM Resource Configuration Changes | 97 |
| Resources | 97 |
| ESM Events | 100 |
| Resources | 100 |
| ESM Reporting Resource Monitoring | 106 |
| Resources | 106 |
| ESM Resource Monitoring | 112 |
| Configuration | 112 |
| Resources | 112 |
| ESM Storage Monitoring (CORR) | 120 |
| Devices | 120 |
| Configuration | 120 |
| Resources | 120 |
| ESM Storage Monitoring (Oracle) | 130 |
| Devices | 130 |
| Configuration | 130 |
| Resources | 130 |
| Logger Events | 138 |
| Resources | 138 |
| Logger System Health | 139 |
| Configuration | 139 |
| Resources | 140 |
| Index | 147 |

Chapter 1

Standard Content Overview

This chapter discusses the following topics.

["What is Standard Content?" on page 5](#)

["Standard Content Documentation" on page 6](#)

What is Standard Content?

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

Standard content is pre-installed on the ArcSight Express appliance to provide essential system health and status operations. Standard content consists of the following:

- **ArcSight Administration** provides statistics about the health and performance of ArcSight products. ArcSight Administration is essential for managing and tuning the performance of the content and system components.
- **ArcSight System** is 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 Express** is organized into the topics listed below. To provide easy access, the most valuable content from each of these topics is linked directly under the ArcSight Express group. Content in each topic is also grouped in a use case resource, for easy access through the use case home page.
 - ◆ **Cisco Monitoring** provides both a broad overview of your Cisco infrastructure and visibility into specific Cisco devices. Powerful analysis tools allow you to monitor activity, configuration changes, availability, and threats across Cisco devices in your environment. A comprehensive and easily customizable set of dashboards, active channels, and reports allows you to measure and report on the status of devices and a variety of other activities taking place in your network.
 - ◆ **Devices** provides resources that monitor the devices in your environment, such as firewalls, Intrusion Detection Systems (IDS), and virtual private networks (VPN), as well as cross-device functions such as logins and configuration management.
 - ◆ **NetFlow Monitoring** is designed specifically for NetFlow; a network protocol developed by Cisco Systems to run on Cisco IOS-enabled equipment for collecting

IP traffic information. In addition to Cisco IOS, NetFlow also supports Juniper routers and Linux. Using ArcSight Express to leverage session-level data provided by NetFlow can help you monitor network bandwidth usage and correlate it with other security logs (such as firewall, IDS, authentication logs, and so on).

- ◆ **Operations** provides resources for monitoring operations in your environment, including traffic monitoring and case management.
- ◆ **Security and Threat** provides resources for monitoring the security of your environment, including malware and reconnaissance attempts.
- ◆ **Microsoft Windows Monitoring** provides resources for monitoring network activity specific to Windows operating systems. The resources help you monitor additions, modifications, and deletions to user accounts and computer accounts, login activity and failed authentications. You can also monitor policy changes and violations, new and removed system services, and the status of critical services.
- **ArcSight Solutions** contains the HP Reputation Security Monitor solution (RepSM) that uses data received from TippingPoint DVLabs about malicious domains and addresses to detect malware infection, zero day attacks, and dangerous browsing on your network.

Standard Content Documentation

This guide describes the ArcSight System and ArcSight Administration content, and is designed for ArcSight Administrators. As an ArcSight Administrator, you can view resources that are not available to other users and can edit resources to tailor the content to your environment.

For information about ArcSight Express content, refer to the ArcSight Express Standard Content Guide. For information about the RepSM solution, refer to the HP Reputation Security Monitor Solution Guide.

ArcSight 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 content. For information about installing and configuring ArcSight Express content, refer to the ArcSight Express Standard Content Guide. For information about installing and configuring the RepSM solution, refer to the HP Reputation Security Monitor Solution Guide.

This chapter discusses the following topics.

[Installing the Content](#)

[Configuring the Content](#)

Installing the Content

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

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.

- ["Modeling the Network" on page 8](#)
- ["Categorizing Assets" on page 8](#)
- ["Configuring Active Lists" on page 9](#)
- ["Configuring Filters" on page 9](#)
- ["Enabling Rules" on page 9](#)
- ["Configuring Notification Destinations" on page 10](#)
- ["Configuring Notifications and Cases" on page 10](#)
- ["Scheduling Reports" on page 11](#)
- ["Configuring Trends" on page 11](#)
- ["Viewing Use Case Resources" on page 12](#)

Modeling the Network

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

There are several ways to model your network. For information about populating the network model, refer to the ArcSight Console User's Guide. To learn more about the architecture of the ArcSight 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 `/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 *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 `/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 the criticality of an event. Asset criticality is one of the four factors used by the Priority Formula to generate an overall event priority rating.

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

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

For more information 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 provide more information about the assets in your environment.

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

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

For a list of the ArcSight System active lists you need to configure manually, refer to the configuration information for each resource group presented in [Chapter 3, ArcSight System Content, on page 13](#).

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 35](#).

Configuring Filters

For a list of the ArcSight System filters you need to configure, refer to the configuration information for each resource group presented in [Chapter 3, ArcSight System Content, on page 13](#).

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 35](#).

Enabling Rules

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 for the Logger System Health rules, are enabled. You can enable the Logger System Health rules if you have a Logger connected to your system. The Logger System Health rules are described in ["Logger Overview" on page 45](#).

To enable or disable a rule:

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

Configuring 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. However, the ArcSight Administrator can configure the destinations *and* enable the notification in the rules. For information about enabling the notifications in rules, see [Configuring Notifications and Cases](#), below.

ArcSight System and ArcSight Administration rules reference two notification destination 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 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 ArcSight tools used to track and resolve the security issues that the content is designed to find. By default, notifications to the CERT Team and the SOC Operators notification destination groups, and create case actions are disabled in the standard content rules.

To configure 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 for details about enabling notifications and opening cases.

Rules with Notifications to the CERT Team

These rules send notifications to the **CERT Team** notification destination group:

| Rule Name | Rule URI |
|------------------------|---|
| License Limit Exceeded | ArcSight Administration/ESM/Licensing/ |
| Out of Domain Fields | ArcSight Administration/ESM/System Health/Resources/Domains |

Rules with Notifications to SOC Operators

These rules send notifications to the **SOC Operators** notification destination group:

| Rule Name | Rule URI |
|------------------------------------|--|
| Connector Dropping Events | ArcSight Administration/Connectors/System Health/ |
| Connector Still Down | ArcSight Administration/Connectors/System Health/ |
| Connector Still Caching | ArcSight Administration/Connectors/System Health/ |
| Critical Device Not Reporting | ArcSight Administration/Connectors/System Health/Custom/ |
| Excessive Rule Recursion | ArcSight Administration/ESM/System Health/Resources/Rules/ |
| Rule Matching Too Many Events | ArcSight Administration/ESM/System Health/Resources/Rules/ |
| ASM Database Free Space - Critical | ArcSight Administration/ESM/System Health/Storage/ |

Scheduling Reports

You can schedule reports based on cases, notifications, assets, or events to run automatically or on a regular schedule. 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.

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 the ArcSight Console User's Guide.

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.

Viewing Use Case Resources

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



Note

Currently, ArcSight System content does not contain any use case resources. [Chapter 3, ArcSight System Content, on page 13](#) documents System resources by grouping them by function.

To view the resources associated with a use case resource:

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

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

The use case resource tables listed in [Chapter 4, ArcSight Administration Content, on page 35](#) describe all the resources that have been assigned to the use case and include dependent resources.

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 14 | The Actor Support Resources group includes resources that support the actors feature. The actors feature maps people and their activity to events from applications and network assets by leveraging user attributes defined within identity management systems, and correlating them with user account information from the user authentication systems in your network. |
| "Priority Formula Resources" on page 18 | 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 26 | The System Resources group includes resources that are either required by the system to operate or are customizable so you can adjust the behavior of the system. |

Actor Support Resources

The Actor Support Resources group includes resources that support the actors feature. The actors feature maps people and their activity to events from applications and network assets by leveraging user attributes defined within identity management systems, and correlating them with user account information from the user authentication systems in your network.

Correlating user identifiers from the event traffic that reflects their activity throughout the day makes it possible to ensure that users are doing role-appropriate activity across the assets in your organization, and to detect and track inappropriate access and suspicious activity. For more information on Actors, see the ArcSight Console User's Guide.



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

Resources

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

Table 3-1 Resources that Support the Actor Support Resources Group

| Resource | Description | Type | URI |
|---|--|--------|-----------------------|
| Monitor Resources | | | |
| Actor Context Report by Target Username | This report shows activity related to an actor based on the ActorByTargetUserName global variable. | Report | ArcSight System/Core/ |
| Actor Context Report by Account ID | This report shows activity related to an actor based on the ActorByAccountID global variable. | Report | ArcSight System/Core/ |
| Actor Context Report by Attacker Username | This report shows activity related to an actor based on the ActorByAttackerUserName global variable. | Report | ArcSight System/Core/ |
| Actor Context Report by Custom Fields | This report shows activity related to an actor based on the ActorByCustomFields global variable. | Report | ArcSight System/Core/ |

| Resource | Description | Type | URI |
|--------------------------|--|-----------------|-------------------------------------|
| Library Resources | | | |
| Account Authenticators | This active list is used by the actor global variables to determine the Identity Management authenticator (based on the event), so that an actor can be determined from event information. | Active List | ArcSight System/Actor Data Support/ |
| Actor Data Support | This group contains session lists for actor variables created by users. | Session Group | ArcSight System |
| Actor Data | This group contains actor session lists. | Session Group | 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 |
| ActorByAttacker UserName | 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 |

| Resource | Description | Type | URI |
|----------------------------|---|-----------------|----------------------------------|
| ActorByCustom Fields | 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 |
| ActorByTargetUserName | 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 |
| 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 |
| 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/ |

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

Priority Formula Resources

The Priority Formula Resources group includes resources that directly or indirectly affect the Priority Formula. The Priority Formula is a series of five criteria against which each event is evaluated to determine its relative importance, or urgency, to your network. The Priority Formula is also referred to as the Threat Level Formula.

For more information about the Priority Formula, refer to the ArcSight Console User's Guide or the ESM 101 guide.

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 9](#).



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 all the resources in the Priority Formula Resources group.

Table 3-2 Resources that Support the Priority Formula Resources Group

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

| Resource | Description | Type | URI |
|-------------------------------------|--|------|---|
| Hostile - Success | This rule detects any successful hostile attempts on a device that is not already compromised from a source not listed in a trusted active list. The rule triggers whenever an event is categorized as Success and Hostile, and the target does not belong to a compromised active list. On the first event, the severity is set to medium, the attacker address is added to the Hostile List active list, and the target address is added to the Hit List active list. | Rule | ArcSight System/Threat Tracking/Hostile/ |
| 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 List active list. On the time window expiration, the target is added to the Scanned List 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 List active list, and the target address is added to the Hit List active list. | Rule | ArcSight System/Threat Tracking/Compromise/ |

| Resource | Description | Type | URI |
|--------------------------------------|--|----------------|--|
| Incident Resolved - Remove From List | This rule detects a Resolved message in an ArcSight Data Monitor Value Change event from the Attacked or Compromised Systems data monitor (in the Executive View dashboard), which is sent when a user marks an asset within the data monitor as resolved. | Rule | ArcSight 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/ |
| 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 for an information system can 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 can 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 can 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 |

| Resource | Description | Type | URI |
|-----------------|--|----------------|---|
| Moderate | The disruption of access to or use of information for an information system can 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 can 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 for an information system can have a limited adverse effect on organizational operations, organizational assets, or individuals. | Asset Category | Site Asset Categories/Compliance Requirement/FIPS-199/Availability Criticality |
| Criticality | This is a system asset category. | Asset Category | System Asset Categories |
| Low | The unauthorized disclosure of information can 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 can 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 |

| Resource | Description | Type | URI |
|--|--|----------------|--|
| Low | The unauthorized modification or destruction of information can 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/ |
| 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/ |

| Resource | Description | Type | URI |
|----------------------------------|--|--------|--|
| 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 creates assets in the asset model automatically for events whose devices are not already modeled either manually or using an asset scanner. Depending on what devices you have reporting to ArcSight and what devices report in to your network, this can cause more individual assets to be added to your asset model than necessary. For example, every time a laptop logs onto the network via a VPN or wireless network, a new asset ID is generated for that device.

By default, the Device Asset Auto Creation Controller filter is configured with the generic condition `True`, which matches all events. Configure this filter to specify traffic from specific devices and device vendors, or event categories, such as `Hostile`. When you specify an event category, the filter directs the system to only create assets for events with this severity.

- ◆ Modify the [SNMP Trap Sender](#) filter if you have the SNMP Trap Sender enabled to forward events through SNMP to a network management system, such as HP Openview.

By default, this filter is configured with the filter `/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 Express Administrator's Guide.

Resources

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

Table 3-3 Resources that Support the System Resources Group

| Resource | Description | Type | URI |
|--------------------------|--|----------------|-----------------------------|
| Monitor Resources | | | |
| Personal Live | This active channel shows events received during the last two hours. The active channel includes a sliding window that always displays the last two hours of event data. A filter prevents the channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events. This active channel also hides all the events that have been assigned to the current user. | Active Channel | ArcSight System/Core/ |
| Today | This active channel shows events received today since midnight. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events. | Active Channel | ArcSight System/ |
| Last 5 Minutes | This active channel shows events received during the last five minutes. The active channel includes a sliding window that always displays the last five minutes of event data. | Active Channel | ArcSight System/All Events/ |
| Live | This active channel shows events received during the last two hours. The active channel includes a sliding window that always displays the last two hours of event data. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events. | Active Channel | ArcSight System/Core/ |

| Resource | Description | Type | URI |
|-----------------------------|--|----------------|--|
| Last Hour | This active channel shows events received during the last hour. The active channel includes a sliding window that always displays an hour of event data. | Active Channel | ArcSight System/All Events/ |
| System Events Last Hour | This active channel shows all events generated during the last hour. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events. | Active Channel | ArcSight 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 |

| Resource | Description | Type | URI |
|------------------------------------|--|-----------|--|
| 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 |
| 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, focusing on case resources. | Field Set | ArcSight System/Case Field Sets/ |
| Connector Monitoring Events | This field set contains fields used to examine connector monitoring events, such as specific connector audit events and correlation events resulting from rules in the Connector Monitoring use cases. | Field Set | ArcSight Administration/Connector/ |
| Standard-MgrRcpt | This resource has no description. | Field Set | ArcSight System/Event Field Sets/Active Channels |
| TurboMode Fastest | This resource has no description. | Field Set | ArcSight System/Event Field Sets/Inspect - Edit |
| 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/ |

| Resource | Description | Type | URI |
|--|---|-----------|--|
| 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/ |
| 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/ |

| Resource | Description | Type | URI |
|--|---|---------------------|----------------------------------|
| ArcSight Events | This filter selects all events generated by ArcSight, including ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. For SmartConnectors, the data from the devices the SmartConnectors collect is not included. | 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/ |
| 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 filter selects all events not generated by ArcSight or ArcSight SmartConnectors related to system health monitoring. | 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/ |

| Resource | Description | Type | URI |
|----------------------|---|---------------------|--------------------------------|
| Web Search | This integration command is used to run a search with the selected item, device vendor, and device product in the selected event. | Integration Command | ArcSight System/Tools/ |
| Nslookup (Linux) | This integration command is used to find details about the Domain Name System (DNS). Run this command from a Linux console. | Integration Command | ArcSight System/Tools/Linux/ |
| Nslookup (Windows) | This integration command is used to find details about the Domain Name System (DNS). Run this command from a Windows console. | Integration Command | ArcSight System/Tools/Windows/ |
| Portinfo (Windows) | This integration command is used to find information about the selected port. Run this command from a Windows console. | Integration Command | ArcSight System/Tools/Windows/ |
| Ping (Windows) | This integration command is used to test whether a particular host is reachable across an IP network. Run this command from a Windows console. | Integration Command | ArcSight System/Tools/Windows/ |
| Traceroute (Windows) | This integration command is used to determine the route taken by packets across an IP network. Run this command from a Windows console. | Integration Command | ArcSight System/Tools/Windows/ |
| 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/ |

| Resource | Description | Type | URI |
|----------------------------------|---|---------------------------|--|
| 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/ |
| 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 | / |
| Chart and 2 Tables Landscape | This template is designed to show one chart and two tables. The orientation is landscape. | Report Template | ArcSight System/1 Chart/With 2 Tables/ |
| Chart and 2 Tables Portrait | This template is designed to show one chart and two tables. The orientation is portrait. | Report Template | ArcSight System/1 Chart/With 2 Tables/ |
| Chart and Table Landscape | This template is designed to show one chart and a table. The orientation is landscape. | Report Template | ArcSight System/1 Chart/With Table/ |
| Chart and Table Portrait | This template is designed to show one chart and a table. The orientation is portrait. | Report Template | ArcSight System/1 Chart/With Table/ |

| Resource | Description | Type | URI |
|----------------------------------|---|-----------------|---|
| Four Charts Landscape | This template is designed to show four charts. The orientation is landscape. | Report Template | ArcSight System/ 4 Charts/Without Table/ |
| Four Charts and Table Landscape | This template is designed to show four charts and a table. The orientation is landscape. | Report Template | ArcSight System/ 4 Charts/With Table/ |
| Simple Chart Landscape | This template is designed to show one chart. The orientation is landscape. | Report Template | ArcSight System/ 1 Chart/Without Table |
| Simple Chart Portrait | This template is designed to show one chart. The orientation is portrait. | Report Template | ArcSight System/ 1 Chart/Without Table |
| Simple Table Landscape | This template is designed to show a table. The orientation is landscape. | Report Template | ArcSight System/1 Table/ |
| Simple Table Portrait | This template is designed to show a table. The orientation is portrait. | Report Template | ArcSight System/1 Table/ |
| Three Charts Landscape | This template is designed to show three charts and a description field. The orientation is landscape. | Report Template | ArcSight System/ 3 Charts/Without Table/ |
| Three Charts and Table Landscape | This template is designed to show three charts and a table. The orientation is landscape. | Report Template | ArcSight System/ 3 Charts/With Table/ |
| Three Tables Portrait | This template is designed to show three tables. The orientation is portrait. | Report Template | ArcSight System/ 3 Tables/ |
| Two Charts Landscape | This template is designed to show two charts and a description field. The orientation is landscape. | Report Template | ArcSight System/ 2 Charts/Without Table/ |
| Two Charts One Table Landscape | This template is designed to show two charts and a table. The orientation is landscape. | Report Template | ArcSight System/ 2 Charts/With Table/ |
| Two Charts One Table Portrait | This template is designed to show two charts and a table. The orientation is portrait. | Report Template | ArcSight System/ 2 Charts/With Table/ |
| Two Charts Portrait | This template is designed to show two charts. The orientation is portrait. | Report Template | ArcSight System/ 2 Charts/Without Table/ |
| Two Tables Landscape | This template is designed to show two tables. The orientation is landscape. | Report Template | ArcSight System/2 Tables |
| Two Tables Portrait | This template is designed to show two tables. The orientation is portrait. | Report Template | ArcSight System/2 Tables |

Chapter 4

ArcSight Administration Content



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

The ArcSight Administration resources are grouped together according to use cases. A use case provides a way to group a set of resources that help address a specific issue or function. The ArcSight Administration use cases are listed in the table below.



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 37 | The Connector Overview use case provides administration content for monitoring SmartConnectors and devices. |
| "ESM Overview" on page 43 | The ESM Overview use case provides administration content for monitoring the ArcSight system. |
| "Logger Overview" on page 45 | The Logger Overview use case provides Logger status and statistics. |
| Connectors | |
| "Connector Configuration Changes" on page 54 | The Connector Configuration Changes use case provides information about configuration changes (such as upgrades) and the versions of the SmartConnectors on the system. |
| "Connector Connection and Cache Status" on page 60 | The Connector Connection and Cache Status use case provides the connection status and caching status of SmartConnectors in the system. SmartConnectors can be connected directly to the ArcSight system or through Loggers. |
| "Device Monitoring" on page 72 | The Device Monitoring use case provides information about the devices reporting to the ArcSight system. |

| Use Case | Purpose |
|---|---|
| ESM | |
| "ESM Licensing" on page 81 | The ESM Licensing use case provides information about licensing compliance. |
| "ESM User Sessions" on page 84 | The ESM User Sessions use case provides information about user access to the ArcSight system. |
| ESM - Configuration Changes | |
| "Actor Configuration Changes" on page 88 | The Actor Configuration Changes use case provides information about changes to the actor resources. |
| "ESM Resource Configuration Changes" on page 97 | The ESM Resource Configuration Changes use case provides information about changes to the various resources, such as rules, reports, and so on. |
| ESM - System Health | |
| "ESM Events" on page 100 | The ESM Events use case provides statistics on the flow of events through the ArcSight system. |
| "ESM Reporting Resource Monitoring" on page 106 | The ESM Reporting Resource Monitoring use case provides performance statistics for reports, trends, and query viewers. |
| "ESM Resource Monitoring" on page 112 | The ESM Resource Monitoring use case provides processing statistics for various resources, such as trends, rules, and so on. |
| "ESM Storage Monitoring (CORR)" on page 120 | 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 130 | The ESM Storage Monitoring (Oracle) use case provides information on the health of the Oracle database. This does not apply if you are using ESM with CORR-Engine or ArcSight Express with CORR-Engine. |
| Logger | |
| "Logger Events" on page 138 | The Logger Events use case provides statistics for events sent through a Logger. |
| "Logger System Health" on page 139 | The Logger System Health use case provides performance statistics for the a Logger connected to the ArcSight system. |

Connector Overview

The Connector Overview use case provides administration content for monitoring SmartConnectors 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 60](#).

Resources

The following table lists all the resources explicitly assigned to the Connector Overview use case and includes dependent resources.

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/ |

| Resource | Description | Type | URI |
|--|---|--------------|---|
| 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/ |
| 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/ |

| Resource | Description | Type | URI |
|------------------------------|---|-------------|---|
| Library Resources | | | |
| Connector Information | This active list stores available information about connectors, whether they are directly connected to an ArcSight manager or indirectly through a Logger. Note: Information is derived from connector audit events and some information might be incomplete (blank) until the appropriate audit event arrives and is processed by the Connector Monitoring rules. | Active List | ArcSight Administration/Connectors/System Health/ |
| Connectors - Still Caching | This active list stores available information about connectors that have been caching for over two hours (by default). | Active List | ArcSight Administration/Connectors/System Health/ |
| Connectors - Dropping Events | This active list stores the connectors that are currently dropping events (for example, when the cache is full). 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/ |

| Resource | Description | Type | URI |
|-----------------------------|--|--------------|--|
| Connectors - Still Down | This active list stores the ID and the name of the connectors that are have been down for 20 minutes or more (either 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/ |
| 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/ |

| Resource | Description | Type | URI |
|------------------------------|---|--------------|---|
| Connector Cache Status | This data monitor shows the current status of caching across all connectors. If one or more connectors have been caching for longer than two hours (by default), the status is yellow (long-term caching). If one or more connectors are 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 filter selects all events generated by ArcSight, including ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. For SmartConnectors, the data from the devices the SmartConnectors collect is not included. | Filter | ArcSight System/Event Types/ |
| Non-ArcSight Events | This filter selects all events not generated by ArcSight or ArcSight SmartConnectors related to system health monitoring. | 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 20 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 connector version changes on the system. | Use Case | ArcSight Administration/Connectors/ |
| Device Monitoring | This use case provides information about the devices reporting to ESM. | Use Case | ArcSight Administration/Connectors/ |
| Connector Connection and Cache Status | This use case provides information about the connection status and caching status of connectors in the system. Connectors can be connected directly to ESM or through Loggers. | Use Case | ArcSight Administration/Connectors/ |

ESM Overview

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

Resources

The following table lists all the resources explicitly assigned to the ESM Overview use case and includes dependent resources.

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 active 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. | 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 the ArcSight system:

- Enable the following rules:
 - ◆ [Logger Sensor Status](#)—This rule detects Logger system health events related to hardware sensor status. The rule updates the Logger Status and Logger Sensor Type Status active lists with the Logger address, sensor type, sensor name, and sensor status.
 - ◆ [Logger Sensor Type Status](#)—This rule detects Logger Sensor Status correlation events and triggers only if all the sensors statuses for the same sensor type for a Logger indicate OK.
 - ◆ [Logger Status](#)—This rule detects Logger Sensor Status correlation events and triggers only if all the sensor statuses for a Logger indicate OK.

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

- Enable the notification action for the above listed rules, if appropriate for your organization. For information on how to enable notifications, refer to the ArcSight Console User's Guide.
- Enable the following data monitors (described in the table under ["Resources" on page 46](#)).
 - ◆ [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](#)



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 all the resources explicitly assigned to the Logger Overview use case and includes dependent resources.

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, and Connector Appliance Disk Usage data monitors. | Dashboard | ArcSight Administration/Logger/ |
| Library - Correlation Resources | | | |
| Logger Sensor Status | This rule identifies Logger system health events related to hardware sensor status. The rule updates the Logger Status and Logger Sensor Type Status with the Logger IP address, the sensor type, the sensor name, and the sensor status. This rule is disabled by default. Enable the rule if you have Logger in your environment. | Rule | ArcSight Administration/Logger/ System Health/ |
| 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/ |

| Resource | Description | Type | URI |
|---------------------------|--|--------------|--|
| 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/ |
| 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/ |

| Resource | Description | Type | URI |
|---|--|--------------|--|
| Network Usage (Bytes) - Last 10 Minutes | This data monitor shows the network usage for the Logger defined in the My Logger filter 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/ |
| 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/ |

| Resource | Description | Type | URI |
|------------------------------|--|-----------------|--|
| 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/ |
| 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/ |

| Resource | Description | Type | URI |
|-----------------------------|--|-----------|---|
| Logger System Health Events | This field set is used by the Logger System Health Events active channel. The field set identifies the end time, the Logger address, the device event category, the value, unit, time frame, and status of the system health events. | Field Set | ArcSight Administration/Logger/ |
| Sensor Type is CPU | This filter is designed for conditional expression variables. The filter passes events in which the sensor type is CPU. | Filter | ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/ |
| Memory Usage | This filter identifies Logger system health events related to memory usage that originate from the Logger defined in the My Logger filter. | Filter | ArcSight Administration/Logger/System Health/CPU and Memory/ |
| Logger System Health Events | This filter identifies Logger system health events. | Filter | ArcSight Administration/Logger/Event Types/ |
| 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 in which the sensor type is FAN. | Filter | ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/ |

| Resource | Description | Type | URI |
|-----------------------------|--|--------|---|
| 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 in which 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/ |
| 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 in which the device event category ends with /In. | Filter | ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/ |

| Resource | Description | Type | URI |
|----------------------------|---|---------------------|---|
| Remaining Disk < 5 Percent | This filter is designed for conditional expression variables. The filter passes events in which the remaining disk space is less than five percent. | Filter | ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/ |
| Disk Read and Write | This filter identifies Logger system health events related to disk read/write speed that originate from the Logger defined in the My Logger filter. | Filter | ArcSight Administration/Logger/System Health/Storage/ |
| By Event Name | This integration command enables you to run a search by event name on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours. | Integration Command | ArcSight Administration/Logger/ |
| By User | This integration command enables you to run a search by user on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours. | Integration Command | ArcSight Administration/Logger/ |
| By Source | This integration command enables you to run a search by source address on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours. | Integration Command | ArcSight Administration/Logger/ |
| By Destination | This integration command enables you to run a search by destination address on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours. | Integration Command | ArcSight Administration/Logger/ |
| By Source and Destination | This integration command enables you to run a search by source and destination address on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours. | Integration Command | ArcSight Administration/Logger/ |

| Resource | Description | Type | URI |
|-----------------------|--|---------------------------|---------------------------------|
| By Vendor and Product | This integration command enables you to run a search by device vendor and product on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours. | Integration Command | ArcSight Administration/Logger/ |
| Logger Quick Search | This integration command enables you to run a search on an ArcSight Logger appliance. The search takes the selected field type and value as parameters, and returns all the events matching the condition within the last two hours. | Integration Command | ArcSight Administration/Logger/ |
| Logger Quick Search | This integration configuration is used to configure the Logger Quick Search command. | Integration Configuration | ArcSight Administration/Logger/ |
| Logger Search | This integration configuration is used to configure the Logger Search command. | Integration Configuration | ArcSight Administration/Logger/ |
| Logger Appliance 1 | This integration target stores the IP address of an ArcSight Logger appliance. This target is used by the set of integration commands for Logger. | Integration Target | ArcSight Administration/Logger/ |
| Logger Appliance 2 | This integration target stores the IP address of an ArcSight Logger appliance. This target is used by the set of integration commands for Logger. | Integration Target | ArcSight Administration/Logger/ |
| Logger System Health | This use case provides performance statistics for the Loggers connected to ESM. | Use Case | ArcSight Administration/Logger/ |
| Logger Events | This use case provides information about statistics for events sent through Loggers to ESM. | Use Case | ArcSight Administration/Logger/ |

Connector Configuration Changes

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

Resources

The following table lists all the resources explicitly assigned to the Connector Configuration Changes use case and includes dependent resources.

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 for the failure. | Report | ArcSight Administration/Connectors/ Configuration Changes/Upgrades/ |

| Resource | Description | Type | URI |
|--|--|--------|--|
| Upgrade History by Connector | This report shows the upgrade history by connector (within the last seven days by default) sorted chronologically. Note: When running the report, be sure to use the connector ID located in the connector resource and copy-paste the ID in to the ConnectorID field in the Custom Parameters for the report. | Report | ArcSight Administration/Connectors/ Configuration Changes/Upgrades/ |
| Version History by Connector Type | This report shows the version history by connector type (within the last seven days by default). The list is grouped by connector zone, connector address, connector name, and connector ID. | Report | ArcSight Administration/Connectors/ Configuration Changes/Versions/ |
| Successful Connector Upgrades | This report lists the connectors with successful upgrades (within the last seven days by default). The list is sorted chronologically. | Report | ArcSight Administration/Connectors/ Configuration Changes/Upgrades/ |
| Version History by Connector | This 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 connector upgrades in a pie chart, and the counts per day in a table (within the last seven days by default). | Report | ArcSight Administration/Connectors/ Configuration Changes/Upgrades/ |
| Library - Correlation Resources | | | |
| Connector Upgrade Failed | This rule detects failed connector upgrades. On the first event, the connector ID, name, version, type, address, zone, and reason for the failure are added to the Connector Upgrades active list. | Rule | ArcSight Administration/Connectors/ Configuration Changes/ |

| Resource | Description | Type | URI |
|------------------------------|---|-------------|--|
| 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/ |
| 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 ArcSight 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/ |
| Connector Upgrades | This active list stores information related to successful and failed connector upgrades. When an upgrade is successful, the active list stores the Upgrade Time, Connector ID, Connector Name, Connector Version, Connector Type, Connector Address, and Connector Zone. When an upgrade fails, the active list also stores the reason for the failure. The active list is populated by the Connector Upgrade Failed and Connector Upgrade Successful rules. | Active List | ArcSight Administration/Connectors/ Configuration Changes/ |
| Connectors - Down | This active list stores the IDs and names of connectors that are currently down (either 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/ |

| Resource | Description | Type | URI |
|------------------------------|--|-------------|--|
| Connectors - Still Down | This active list stores the ID and the name of the connectors that are have been down for 20 minutes or more (either 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/ |
| 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/ |

| Resource | Description | Type | URI |
|-----------------------------------|--|--------------|--|
| 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 for the failure) in the Connector Upgrades active list. | Query | ArcSight Administration/Connectors/ Configuration Changes/Upgrades/ |
| Version History by Connector | This query identifies all the connector versions by connector in the Connector Versions session list. | Query | ArcSight Administration/Connectors/ Configuration Changes/Versions/ |
| Connector Versions | This session list stores the version history for all the connectors. The fields in the session list are: Connector ID, Connector Name, Connector Version, Connector Type, Connector Address, and Connector Zone. The session list is populated by the Connector Upgrade Successful and Connector Version Detected rules. | Session List | ArcSight Administration/Connectors/ Configuration Changes/ |

Connector Connection and Cache Status

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

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

The Connector UP and Connector Down rules detect SmartConnectors that are started and are reporting events, and those that are shut down. These rules can send a notification (if notifications are enabled) when the SmartConnectors have been down for a certain period of time. You might want to exclude SmartConnectors that you start and stop manually, SmartConnectors that are scheduled to run once every week (such as vulnerability scanners), or SmartConnectors that you are testing (starting and stopping frequently during the setup process).
 - ◆ *Optional:* Populate the [Connector Information](#) active list with the contact information for each SmartConnector, if needed. For example, you can add contact information for SmartConnectors maintained by other individuals or organizations. Add the contact information in the 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 ArcSight Manager when the SmartConnector is first registered. Do not add information to this active list for SmartConnectors that are not already reported into the system and registered.

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

- 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 all the resources explicitly assigned to the Connector Connection and Cache Status use case and includes dependent resources.

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/ |

| Resource | Description | Type | URI |
|-----------------------------------|---|--------------|---|
| Connectors - Down - Short Term | This query viewer displays data on connectors that have been down for under 20 minutes (by default). This query viewer queries on an active list that is maintained by the Connector Monitoring content (rules), so it can update every minute. | Query Viewer | ArcSight Administration/Connectors/System Health/ |
| Connectors - Down - Long Term | This query viewer displays data on connectors that have been down for longer than 20 minutes (by default). This query viewer queries on an active list that is maintained by the Connector Monitoring content (rules), so it can update every minute. | Query Viewer | ArcSight Administration/Connectors/System Health/ |
| 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/ |

| Resource | Description | Type | URI |
|--|---|--------|--|
| Cache History by Connectors | <p>This report shows the cache history by connector (within the last 24 hours by default) sorted chronologically.</p> <p>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.</p> | Report | ArcSight Administration/Connectors/ System Health/Cache/ |
| Current Cache Status | <p>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.</p> | Report | ArcSight Administration/Connectors/ System Health/Cache/ |
| Library - Correlation Resources | | | |
| Connector Still Caching | <p>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.</p> | Rule | ArcSight Administration/Connectors/ System Health/ |

| Resource | Description | Type | URI |
|------------------------------------|---|------|--|
| 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 it there is a connector shutdown or heartbeat timeout event (except for connectors listed in the Black List - Connectors filter). The rule adds connector information to the Connectors - Down active list. | Rule | ArcSight Administration/Connectors/ System Health/ |
| 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/ |

| Resource | Description | Type | URI |
|---------------------------------|---|-------------|--|
| 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/ |
| 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 ArcSight 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/ |

| Resource | Description | Type | URI |
|------------------------------|--|-------------|--|
| Connectors - Dropping Events | This active list stores the connectors that are currently dropping events (for example, when 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 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/ |

| Resource | Description | Type | URI |
|------------------------------|--|--------------|--|
| Black List - Reverse Look Up | This active list stores look-up data to enable the rules to update the connector connection and caching status displays when a connector is added to the Black List - Connectors active list. Note: This list should contain all the information that is also included 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/ |
| 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/ |

| Resource | Description | Type | URI |
|---|--|--------------|---|
| Connector Connection Status | This data monitor shows the current status of the connector connections across all connectors. If one or more connectors 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/ |
| 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/ |

| Resource | Description | Type | URI |
|---------------------------------------|---|-------|--|
| 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 the ArcSight system.

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 `/System Asset Categories/Criticality/High`.

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

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

- Enable the [Critical Device Not Reporting](#) rule (disabled by default) if you want to be notified when one of your critical devices is down. Enable the rule only after you modify the White List - Critical Devices filter. For information about how to enable a rule, refer to the ArcSight Console User's Guide.

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 the ArcSight Console User's Guide.

- 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 all the resources explicitly assigned to the Device Monitoring use case and includes dependent resources.

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/ |

| Resource | Description | Type | URI |
|--|---|--------|---|
| Destination Counts by Connector Type | This report displays a table showing the connector type, the destination zones and addresses, and the count from each source. Make sure you select a filter parameter other than the default of All Events. You can also adjust the Start and End times of the report to reduce the number of events selected. | Report | ArcSight Administration/Connectors/ System Health/Event Breakdown/ |
| High Volume Connector EPS - Daily | This report shows the hourly average EPS for high volume connectors. The default time frame is yesterday. By default, a connector with a daily average EPS greater than or equal to 100 is considered a high volume connector. | Report | ArcSight Administration/Connectors/ System Health/EPS/ |
| Top Connector Types Chart | This 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/ |

| Resource | Description | Type | URI |
|-------------------------------------|---|----------------|---|
| 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/ |
| Library Resources | | | |
| Reporting Devices - Critical | This active list stores the devices that are considered critical, with the total count of events, the event count since last check, and the timestamp of the last event received by the device. The active list is updated every time the Manager receives a Connector Device Status event for that device. | Active List | ArcSight Administration/Connectors/ System Health/Custom/ |
| Connector Average EPS - Last 7 Days | This active list stores the average EPS for all connectors during the last seven days. The data is from a trend. | Active List | ArcSight Administration/Connectors/ System Health/EPS/ |
| Connector Daily Average EPS | This active list stores the daily average EPS for all connectors. The data is from a trend. | Active List | ArcSight Administration/Connectors/ System Health/EPS/ |
| Reporting Devices | This active list stores the devices with the total count of events, the event count since last check, and the timestamp of the last event received by the device. The active list is updated every time the Manager receives a Connector Device Status event for that device. | Active List | ArcSight Administration/Connectors/ System Health/ |
| High | This is a system asset category. | Asset Category | System Asset Categories/ Criticality |
| 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 |
|-------------------------------------|---|--------------|--|
| 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/ |
| ArcSight Events | This filter selects all events generated by ArcSight, including ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. For SmartConnectors, the data from the devices the SmartConnectors collect is not included. | Filter | ArcSight System/Event Types/ |
| Non-ArcSight Events | This filter selects all events not generated by ArcSight or ArcSight SmartConnectors related to system health monitoring. | 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/ |

| Resource | Description | Type | URI |
|---|--|-------|---|
| Events for a Destination by Connector Type | This query identifies the Priority, End Time, Agent Type, Attacker Zone Name, Attacker Address, event Name, and the sum of the Aggregated Event Count, ordered by descending priority and by time (hour). The events selected are from the Target Zone and Target Address fields, which default to RFC1918: 192.168.0.0-192.168.255.255 and 192.168.10.10. You can change these default values, either in the Parameters tab of the report or manually when running the report. The Attacker and Target fields are used instead of Source and Destination fields. Note: This report does not populate all values when running in Turbo Mode Fastest. | Query | ArcSight Administration/Connectors/System Health/Event Breakdown/ |
| Events by Device (Summary) | This 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/ |
| 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/ |

| Resource | Description | Type | URI |
|---|---|-------|---|
| Events from a Source by Connector Type | This query identifies the Priority, End Time, Agent Type, Target Zone Name, Target Address, event Name, and the sum of the Aggregated Event Count, ordered by descending priority and by time. The events selected are from the Attacker Zone and Attacker Address fields, which default to RFC1918: 192.168.0.0-192.168.255.255 and 192.168.10.10. You can change these default values either in the Parameters tab of the report or manually when running the report. The Attacker and Target fields are used instead of Source and Destination fields. | Query | ArcSight Administration/Connectors/System Health/Event Breakdown/ |
| Connector Average EPS - Last 7 Days | This query identifies the average EPS for all connectors during the last seven days from a trend. | Query | ArcSight Administration/Connectors/System Health/EPS/ |
| Connector Daily Average EPS | This query identifies the daily average EPS for all connectors from a trend. It is used to build a trend-on-trend. | Query | ArcSight Administration/Connectors/System Health/EPS/ |
| 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/ |
| 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/ |

| Resource | Description | Type | URI |
|-------------------------------------|---|-------|---|
| Connector Total Events - Hourly | This trend stores the hourly average EPS for all connectors. | Trend | ArcSight Administration /Connector/System Health/EPS/ |
| Connector Average EPS - Last 7 days | This trend stores the average EPS for all connectors during the last seven days and writes the data to an active list by leveraging the trend action feature. | Trend | ArcSight Administration/Connector/System Health/EPS/ |

ESM Licensing

The ESM Licensing use case provides information about licensing compliance.

Resources

The following table lists all the resources explicitly assigned to the ESM Licensing use case and includes dependent resources.

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/ |

| Resource | Description | Type | URI |
|--------------------------------|---|----------------|--|
| Library Resources | | | |
| admindcert | This destination is pre-defined for the CERT team. Add more information, such as email addresses. | Destination | CERT Team/1/ |
| 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/ |

| Resource | Description | Type | URI |
|--------------------------|---|-----------------|--|
| 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/ |
| Toolbox Resources | | | |
| Licensing Report | This report template is used by the licensing reports and shows one chart (bar and line). The orientation is landscape. | Report Template | ArcSight Administration/Licensing/ |
| Licensing Report (All) | This report template is used by the licensing reports and shows six charts (bar and line). The orientation is portrait. | Report Template | ArcSight Administration/Licensing/ |

ESM User Sessions

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

Resources

The following table lists all the resources explicitly assigned to the ESM User Sessions use case and includes dependent resources.

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/ |

| Resource | Description | Type | URI |
|--|--|--------------|--|
| 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/ |
| 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/ |

| Resource | Description | Type | URI |
|-----------------------------------|---|--------|--|
| 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/ |
| 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/ |

| Resource | Description | Type | URI |
|-------------------------------------|--|--------------|--|
| ArcSight User Sessions | This session list stores the client username, client address and zone used by an ArcSight user to access the ArcSight manager to monitor the login times, logout times, or console timeouts and 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 all the resources explicitly assigned to the Actor Configuration Changes use case and includes dependent resources.

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 system. 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 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/ |
| 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/ |

| Resource | Description | Type | URI |
|--------------------------------------|--|--------|---|
| IDM Deletions of Actors | This report shows the list of all the actors that have been marked as deleted by the IDM. This is not the same as deleting the actor resource from the ArcSight 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/ |
| 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/ |

| Resource | Description | Type | URI |
|--------------------------|--|-----------------|--|
| 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/ |
| 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/ |
| ActorFromFileName | 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/ |

| Resource | Description | Type | URI |
|-------------------------|--|-----------------|---|
| 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/ |
| 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 place-holder. 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/ |

| Resource | Description | Type | URI |
|------------------------------|---|-----------------|---|
| 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/ |
| 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/ |

| Resource | Description | Type | URI |
|---------------------------------|---|--------|--|
| 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 addition or deletion of multi-value parameters. | Filter | ArcSight Administration/ESM/Configuration Changes/Actor Update Tracking/ |
| All Events | This filter matches all events. | Filter | ArcSight System/Core/ |
| Attacker Zone OR Host is NULL | This 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 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/ |

| Resource | Description | Type | URI |
|--------------------------------|--|-------|--|
| Actors Deleted | This query identifies audit events for actors that have been deleted. Note: This query does not populate all values when running in Turbo Mode Fastest. | Query | ArcSight Administration/ ESM/Configuration Changes/Actors/ |
| Actor Configuration Changes | This query identifies all configuration change audit events made to actor resources. Note: This query does not populate all values when running in Turbo Mode Fastest. | Query | ArcSight Administration/ ESM/Configuration Changes/Actors/ |
| Actors Created | This query identifies audit events for actors that have been created. Note: This query does not populate all values when running in Turbo Mode Fastest. | Query | ArcSight Administration/ ESM/Configuration Changes/Actors/ |
| Actor Title and Status Changes | This query identifies information from actor audit events that result from changes to the Title or Status attribute of an actor. This query shows the old and the new information. | Query | ArcSight Administration/ ESM/Configuration Changes/Actors/ |
| 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 resources, such as rules, reports, and so on.

Resources

The following table lists all the resources explicitly assigned to the ESM Resource Configuration Changes use case and includes dependent resources.

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 Express 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 within the previous day. Note: This report does not populate all values when running in Turbo Mode Fastest. | Report | ArcSight Administration/ESM/Configuration Changes/Resources/ |
| ESM Configuration Changes by Type | This report shows recent ArcSight Express 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 | Description | Type | URI |
|--------------------------------|---|--------------|--|
| Resource Deleted Report | This report shows a list of all the resources deleted by ArcSight users during the previous day. Note: This report does not populate all values when running in Turbo Mode Fastest. | Report | ArcSight Administration/ESM/Configuration Changes/Resources/ |
| Resource Updated Report | This report shows a list of all the resources updated by ArcSight users within the previous day. Note: This report does not populate all values when running in Turbo Mode Fastest. | Report | ArcSight Administration/ESM/Configuration Changes/Resources/ |
| Library Resources | | | |
| Recent System Resource Inserts | This data monitor does not populate all values when running in Turbo Mode Fastest. | Data Monitor | ArcSight Administration/ESM/Configuration Changes/Resources/ |
| Recent System Resource Updates | This data monitor does not populate all values when running in Turbo Mode Fastest. | Data Monitor | ArcSight Administration/ESM/Configuration Changes/Resources/ |
| 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/ |

| Resource | Description | Type | URI |
|---------------------------|---|--------|---|
| 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 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 Express. 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 the ArcSight system.

Resources

The following table lists all the resources explicitly assigned to the ESM Events use case and includes dependent resources.

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 active 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/ |

| Resource | Description | Type | URI |
|--|---|-------------------|--|
| Event Name Counts | This resource has no description. | Report | ArcSight Administration/ESM/System Health/Events/ |
| 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/ |

| Resource | Description | Type | URI |
|------------------------------|---|--------|---|
| ASM Event Flow | This resource has no description. | Filter | ArcSight Administration/ESM/System Health/Events/ |
| 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/ |

| Resource | Description | Type | URI |
|---|---|--------|---|
| 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/ |
| 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/ |

| Resource | Description | Type | URI |
|--|--|-------|--|
| 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/ |
| 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 all the resources explicitly assigned to the ESM Reporting Resource Monitoring use case and includes dependent resources.

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 10 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 the last 24 hours. | Query Viewer | ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/ |
| Last 10 Trend Queries | This query viewer shows the duration information for the last 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 the last 24 hours. | Query Viewer | ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/ |
| Trend Queries Failures During Last 24 hr | This query viewer shows the duration information for failed trend queries during the last 24 hours. | Query Viewer | ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/ |
| Running Report Queries | This query viewer shows the currently running report queries. | Query Viewer | ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/ |
| Top 10 Longest Report Queries During Last 24 hr | This query viewer shows the duration information for the top 10 longest report queries during the last 24 hours. | Query Viewer | ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/ |
| Query Failures During Last 24 hr | This query viewer displays failed queries for reports, trends, and query viewers. | Query Viewer | ArcSight Administration/ESM/System Health/Resources/Reporting/ |
| Last 10 Report Queries | This query viewer shows the duration information for the last 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 the last 24 hours. | Query Viewer | ArcSight Administration/ESM/System Health/Resources/Reporting/Query Viewers/ |
| Query Counts During Last 24 hr | This query viewer shows the query and its counts during the last 24 hours. | Query Viewer | ArcSight Administration/ESM/System Health/Resources/Reporting/ |
| 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/ |
| 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/ |

| Resource | Description | Type | URI |
|--|--|--------------|---|
| 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. A chart shows the top 10 longest report queries and a 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 query counts grouped by type. The default time frame is one week. | Report | ArcSight Administration/ ESM/System Health/Resources/ Reporting/ |
| Longest QueryViewer Queries | This report shows query duration information for query viewers. A chart shows the top 10 longest queries for a query viewer, and a table shows the duration details for query viewers. The default time frame is one week. | Report | ArcSight Administration/ ESM/System Health/Resources/ Reporting/ |
| Longest Trend Query | This report shows query duration information for trends. A chart shows the top 10 longest trend queries and a table shows the duration details for trend queries. The default time frame is one week. | Report | ArcSight Administration/ ESM/System Health/Resources/ Reporting/ |
| Library - Correlation Resources | | | |
| Query Running Time | This rule triggers 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 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 10 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/ |

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

| Resource | Description | Type | URI |
|--------------------------------|---|-------|--|
| Longest Trend Queries - Trend | This query retrieves trend query duration information from a trend, ordered by duration. | Query | ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/ |
| Running Report Queries | This query retrieves currently running report queries. | Query | ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/ |
| Report Query Failures | This query retrieves failed query duration information for reports. | Query | ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/ |
| Report Queries | This query retrieves report query duration information used to build a trend. | Query | ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/ |
| 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 the top longest report queries by day. | Trend | ArcSight Administration/ESM/System Health/Resources/Reporting/ |
| QueryViewer Queries | This trend stores the top longest query viewer queries by day. | Trend | ArcSight Administration/ESM/System Health/Resources/Reporting/ |
| Failed Queries | This trend stores failed queries for reports, trends, and query viewers. | Trend | ArcSight Administration/ESM/System Health/Resources/Reporting/ |

ESM Resource Monitoring

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

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 all the resources explicitly assigned to the ESM Resource Monitoring use case and includes dependent resources.

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 10 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 the last 24 hours. | Query Viewer | ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/ |
| Query Failures During Last 24 hr | This query viewer displays failed queries for reports, trends, and query viewers. | Query Viewer | ArcSight Administration/ESM/System Health/Resources/Reporting/ |

| 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 the last 24 hours. | Query Viewer | ArcSight Administration/ESM/System Health/Resources/Reporting/Query Viewers/ |
| Query Counts During Last 24 hr | This query viewer shows the query and its counts during the last 24 hours. | Query Viewer | ArcSight Administration/ESM/System Health/Resources/Reporting/ |
| Top 10 Longest Report Queries During Last 24 hr | This query viewer shows the duration information for the top 10 longest report queries during the last 24 hours. | Query Viewer | ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/ |
| Active List Access | This report shows active list access statistics. A chart shows the number of added, deleted, and updated active list entries within the previous day, grouping the counts by 10 minute intervals. A table shows 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. A chart shows the number of added, deleted, and updated session list entries in the last hour, grouping the counts by 10 minute intervals. A table shows the details of the session list access, grouping the number by time interval and active list name. | Report | ArcSight Administration/ESM/System Health/Resources/Session Lists/ |
| Invalid Resources | This report shows the list of resources that are invalid. A chart shows the count of invalid resources by resource type. A table lists all the invalid resources grouped by type and sorted by URI. | Report | ArcSight Administration/ESM/System Health/Resources/ |
| Top Accessed Active Lists | This report shows the top 10 accessed active lists. A chart shows the top 10 accessed active lists during the previous day, grouping the counts by 10 minute intervals. A table shows the details of the active list access, grouping the number by active list name and time interval. | Report | ArcSight Administration/ESM/System Health/Resources/Active Lists/ |

| Resource | Description | Type | URI |
|--|---|--------|---|
| 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 10 minute intervals. A chart shows the number of events matching filter rules, join rules, and the total of both types of rules. | Report | ArcSight Administration/ESM/System Health/Resources/Rules/ |
| Fired Rule Events | This report does not populate all values when running in Turbo Mode Fastest. | Report | ArcSight Administration/ESM/System Health/Resources/Rules/ |
| Top Accessed Session Lists | This report shows the top 10 accessed session lists. A chart shows the top 10 accessed session lists within the last hour, grouping the counts by 10 minute intervals. A 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. A chart shows the number of correlation events within the last hour, grouping them by 10 minute intervals. A 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 10 minute intervals. | Query | ArcSight Administration/ESM/System Health/Resources/Rules/ |
| Session List Access (Details) | This query retrieves details of session list access (addition, deletion, and update of active list entries) per session list by 10 minute intervals for the last hour. | Query | ArcSight Administration/ESM/System Health/Resources/Session Lists/ |
| Failed Queries | This query identifies failed queries for reports, trends, and query viewers. The query is used to build a trend and a query viewer. | Query | ArcSight Administration/ESM/System Health/Resources/Reporting/Queries/ |
| Invalid Resources | This query retrieves a list of invalid resources from the Invalid Resources active list. | Query | ArcSight Administration/ESM/System Health/Resources/ |
| Longest Trend Queries | This query retrieves trend query duration information, ordered by duration. | Query | ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/ |
| Correlation Events Count (Details) | This query retrieves the number of correlation events per rule within the last hour, grouping them by 10 minute 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 10 minute intervals for the last hour. | Query | ArcSight Administration/ESM/System Health/Resources/Session Lists/ |
| Active List Access (Details) | This query retrieves details about the active lists that are accessed (addition, deletion, and update of active list entries) per active list by 10 minute 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 10 minute intervals for the last hour. | Query | ArcSight Administration/ESM/System Health/Resources/Data Monitors/ |
| Active List Access | This query retrieves the number of times active lists are accessed (addition, deletion, and update of active list entries) by 10 minute intervals for the last hour. | Query | ArcSight Administration/ESM/System Health/Resources/Active Lists/ |

| Resource | Description | Type | URI |
|-----------------------------------|--|----------|--|
| 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 10 minute intervals. | Query | ArcSight Administration/ESM/System Health/Resources/Rules/ |
| 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

ESM with CORR-Engine or ArcSight Express with CORR-Engine.

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 all the resources explicitly assigned to the ESM Storage Monitoring (CORR) use case and includes dependent resources.

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-Engine/ |
| Archive Status | This dashboard shows database archive related information. | Dashboard | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/ |
| Critical Archive Failure Details | This query viewer shows the current archive archival failure events. | Query Viewer | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/ |
| Archive Task Failure Details | This query viewer shows the current archive task failure events, which include activation, deactivation, and scheduling. | Query Viewer | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/ |
| Archive Status Report | This report shows the current status of archive and disk space used. | Report | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/ |

| 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-Engine/ |
| ASM Database Free Space - by Day | This report shows the free space percentages by day for one of the ASM database table spaces. 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-Engine/ |
| 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-Engine/ |
| 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-Engine/ |
| 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-Engine/ |
| 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-Engine/ |

| Resource | Description | Type | URI |
|---------------------------------------|--|------|--|
| 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/ |
| 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-Engine/ |
| 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 the default threshold of two percent and a notification is sent to the Database Storage Operator group. You can set the threshold in the server.properties file. | 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 is set to very-high. | Rule | ArcSight Administration/ESM/System Health/Storage/ |

| Resource | Description | Type | URI |
|--|--|------|--|
| ASM Database Status Change - Space Now Available | This rule detects if the database status has returned to normal because storage space has been freed or added. This rule looks for a base event indicating that database storage space is available. This rule only requires one such event to trigger. After the first event, the agentSeverity event field is set to Low. | Rule | ArcSight Administration/ESM/System Health/Storage/ |
| ASM Database Status Change - Normal | This rule detects if the database status is normal. This rule 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 a warning when the free space goes below the default threshold of five percent. You can set the threshold in the server.properties file. | 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-Engine/ |
| 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-Engine/ |

| Resource | Description | Type | URI |
|---|--|--------------|--|
| Out of Domain Fields | This rule triggers when there is no more free domain field available for a field type. | Rule | ArcSight Administration/ESM/System Health/Resources/Domains/ |
| ASM Database Status Change - Space Critical | This rule detects if the database status is critical due to storage concerns. 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 is set to very high. | Rule | ArcSight Administration/ESM/System Health/Storage/ |
| ASM Database Status Change - Warning | This rule detects if the database status is at a warning level. This rule 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-Engine/ |
| Archive Task Failures | This active list stores archive task failure events, which include activation, deactivation, and scheduling. | Active List | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/ |
| Database Retrieval Time - Last Hour | This data monitor displays a moving average for the database retrieval time during the last hour. | Data Monitor | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics/ |
| Database Insert Time - Last 24 Hours | This data monitor displays a moving average for the database insert time during the last 24 hours. | Data Monitor | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics/ |
| Database Transaction Volume | This resource has no description. | Data Monitor | ArcSight Administration/ESM/System Health/Storage/ |

| Resource | Description | Type | URI |
|---|--|--------------|--|
| Database Insert Time - Last Hour | This data monitor displays a moving average for the database insert time during the last hour. | Data Monitor | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics/ |
| Database Retrieval Time - Last 24 Hours | This data monitor displays a moving average for the database retrieval time during the last 24 hours. | Data Monitor | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics/ |
| Database Free Space | This resource has no description. | Data Monitor | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics/ |
| Archive Disk Space | This data monitor shows the state of the archive disk space used. The three states are: OK, Warning, and Critical Warning. | Data Monitor | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Archive Status/ |
| Recent Archive Events | This data monitor shows the last 10 archive events. | Data Monitor | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Archive Status/ |
| Database Insert Time Statistics | This filter identifies ArcSight system events where the Device Event Category is /Monitor/EventBroker/InsertTime. | Filter | ArcSight Administration/ESM/System Health/Storage/ |
| ASM Database Load Statistics | This 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-Engine/Conditional Variable Filters/ |
| Archive Archival Success | This filter identifies archive archival success audit events. | Filter | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters/ |
| Archive Disk Space | This filter identifies archive disk space audit events. | Filter | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/ |

| Resource | Description | Type | URI |
|---------------------------------------|--|--------|---|
| 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-Engine/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-Engine/ |
| 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-Engine/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-Engine/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-Engine/Conditional Variable Filters/ |
| Database Retrieval Time Statistics | This filter identifies ArcSight system events where the Device Event Category is /Monitor/EventBroker/RetrievalTime. | Filter | ArcSight Administration/ESM/System Health/Storage/ |

| Resource | Description | Type | URI |
|---------------------------------------|---|----------------|--|
| 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-Engine/ |
| Event Data Free Space - Last 30 Days | This report shows the free space percentages by day for the ARC_EVENT_DATA database table space for the last 30 days. The source report is the ASM Database Free Space - by Day. | Focused Report | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/ |
| 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-Engine/ |
| Archive Activation Statistics | This query retrieves archive activation audit events from the Archive Events session list. | Query | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/ |
| Archive Task Failure Details | This query retrieves archive task failure events from the Archive Task Failures active list. | Query | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/ |
| 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-Engine/ |
| 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/ |

| Resource | Description | Type | URI |
|-----------------------------------|---|-------|--|
| Archive Deactivation Statistics | This query retrieves archive deactivation audit events from the Archive Events session list. | Query | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/ |
| 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-Engine/ |
| 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-Engine/ |
| 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/ |
| Archive Archival Success | This query retrieves archive archival information from the Archive Events session list. | Query | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/ |
| Archive Space status | This query retrieves archive space audit events. | Query | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/ |
| Archive Archival Statistics | This query retrieves archive archival audit events from the Archive Events session list. | Query | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/ |
| ASM Database Free Space (current) | This query 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-Engine/ |

| Resource | Description | Type | URI |
|--------------------------|--|-----------------|--|
| Archive Events | This session list stores archive audit events. | Session List | ArcSight Administration/ESM/System Health/Storage/CORR-Engine/ |
| ASM Database Free Space | This trend stores the free space percentages by hour for the four ASM database table spaces (ARC_EVENT_DATA, ARC_EVENT_INDEX, ARC_SYSTEM_DATA, and ARC_SYSTEM_INDEX). | Trend | ArcSight Administration/ESM/System Health/Storage/ |
| Toolbox Resources | | | |
| Archive Template | This report template contains two tables designed for archive status reports. The report template includes some scripting to make the first column in the tables a color: red, yellow, or green, based on the value in another column. | Report Template | ArcSight Administration/System Health/Storage/CORR-Engine/ |

ESM Storage Monitoring (Oracle)

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

Devices

ESM with Oracle.

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 all the resources explicitly assigned to the ESM Storage Monitoring (Oracle) use case and includes dependent resources.

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/Oracle/ |
| 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/Oracle/ |

| 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/Oracle/ |
| 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/Oracle/ |
| 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/ |

| Resource | Description | Type | URI |
|--------------------------------------|--|------|--|
| 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/ |
| 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 a warning when the free space goes below the default threshold of five percent. You can set the threshold in the server.properties file. | 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/ |

| Resource | Description | Type | URI |
|---|---|--------------|--|
| 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 the default threshold of two percent. You can set the threshold in the server.properties file. 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 is set to very high. | Rule | ArcSight Administration/ESM/System Health/Storage/ |
| Library Resources | | | |
| Partition Manager and Archiver Details | This data monitor displays the last 10 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 the last hour. | Data Monitor | ArcSight Administration/ESM/System Health/Storage/Oracle/Data base Performance Statistics/ |
| Database Insert Time - Last 24 Hours | This data monitor displays a moving average for the database insert time during the last 24 hours. | Data Monitor | ArcSight Administration/ESM/System Health/Storage/Oracle/Data base 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/Data base Performance Statistics/ |
| Database Transaction Volume | This resource has no description. | Data Monitor | ArcSight Administration/ESM/System Health/Storage/ |

| Resource | Description | Type | URI |
|---|--|--------------|--|
| 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/Data base Performance Statistics/ |
| Database Insert Time - Last Hour | This data monitor displays a moving average for the database insert time during the last hour. | Data Monitor | ArcSight Administration/ESM/System Health/Storage/Oracle/Data base Performance Statistics/ |
| Database Retrieval Time - Last 24 Hours | This data monitor displays a moving average for the database retrieval time during the last 24 hours. | Data Monitor | ArcSight Administration/ESM/System Health/Storage/Oracle/Data base Performance Statistics/ |
| Database Free Space | This resource has no description. | Data Monitor | ArcSight Administration/ESM/System Health/Storage/Oracle/Data base Performance Statistics/ |
| 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/Insert Time. | Filter | ArcSight Administration/ESM/System Health/Storage/ |

| Resource | Description | Type | URI |
|---------------------------------------|--|--------|---|
| 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/ |
| 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 the partition manager and partition archiver. | Filter | ArcSight Administration/ESM/System Health/Storage/Oracle/ |

| Resource | Description | Type | URI |
|--|---|-------------------|---|
| ASM Sidetable Cache Hit Rates | This filter identifies ArcSight System Monitor events containing side table cache hit rate information. Side tables are tables held in memory and in the database to retain common and relatively static information such as geographical information, categorization information, connector information, device information, and labels for custom strings and numbers. The cache hit rate identifies how many successful attempts 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 in which 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/Oracle/ |
| 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/Oracle/ |

| 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 a Logger.

Resources

The following table lists all the resources explicitly assigned to the Logger Events use case and includes dependent resources.

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, event name, Logger user, client address (browser), and Logger address. | Field Set | ArcSight Administration/Logger/ |
| Logger Platform Events | This field set is used by the Logger Platform Events active channel. The field set selects the end time, event name, Logger user, client address (browser), and Logger address. | Field Set | ArcSight Administration/Logger/ |
| Logger Platform Events | This filter identifies Logger platform events. | Filter | ArcSight Administration/Logger/Event Types/ |
| Logger System Health Events | This filter identifies Logger system health events. | Filter | ArcSight Administration/Logger/Event Types/ |
| Logger Events | This filter identifies Logger events. | Filter | ArcSight Administration/Logger/Event Types/ |
| 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 a Logger connected to the ArcSight system.

Configuration

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

- Enable the following rules:
 - ◆ [Logger Sensor Status](#)—This rule detects Logger system health events related to hardware sensor status. The rule updates the Logger Status and Logger Sensor Type Status active lists with the Logger address, sensor type, sensor name, and sensor status.
 - ◆ [Logger Sensor Type Status](#)—This rule detects Logger Sensor Status correlation events and triggers only if all the sensors statuses for the same sensor type for a Logger indicate OK.
 - ◆ [Logger Status](#)—This rule detects Logger Sensor Status correlation events and triggers only if all the sensor statuses for a Logger indicate OK.

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

- Enable the notification action for the above listed rules, if appropriate for your organization. For information on how to enable notifications, refer to the ArcSight Console User's Guide.
- Enable the following data monitors (described in the table under "[Resources](#)" on [page 140](#)):
 - ◆ [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 all the resources explicitly assigned to the Logger System Health use case and includes dependent resources.

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/ |

| Resource | Description | Type | URI |
|--|--|-------------|---|
| 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 | | | |
| 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/ |

| Resource | Description | Type | URI |
|--|--|--------------|--|
| Network Usage (Bytes) - Last 10 Minutes | This data monitor shows the network usage for the Logger defined in the My Logger filter 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/ |
| 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 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/ |

| Resource | Description | Type | URI |
|---|--|--------------|--|
| CPU Sensors | This data monitor shows the status for all the CPU sensors on the Logger defined in the My Logger filter. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment. | Data Monitor | ArcSight Administration/Logger/My Logger/Hardware/ |
| Sensor Type Status | This data monitor shows the hardware status by sensor type for the Logger defined in the My Logger filter. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment. | Data Monitor | ArcSight Administration/Logger/My Logger/My Logger Overview/ |
| Disk Read and Write (Kbytes per Second) - Last 10 Minutes | This data monitor shows the disk read/write speed for the Logger defined in the My Logger filter for the last 10 minutes. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment. | Data Monitor | ArcSight Administration/Logger/My Logger/My Logger Overview/ |
| 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/ |

| Resource | Description | Type | URI |
|---------------------------------------|--|-----------------|---|
| 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/ |
| 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, Logger address, Device Event Category, 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 in which the sensor type is CPU. | Filter | ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/ |
| Memory Usage | This filter identifies Logger system health events related to memory usage that originate from the Logger defined in the My Logger filter. | Filter | ArcSight Administration/Logger/System Health/CPU and Memory/ |
| Logger System Health Events | This filter identifies Logger system health events. | Filter | ArcSight Administration/Logger/Event Types/ |
| Logger Events | This filter identifies Logger events. | Filter | ArcSight Administration/Logger/Event Types/ |

| 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/ |
| 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/ |
| 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/ |

| Resource | Description | Type | URI |
|---------------------|---|--------|--|
| 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/ |

Index

A

Account Authenticators active list 15

active channels

- Actor Audit Events 88
- ASM Events 100
- Connector Caching Events 61
- Connector Connection Status Events 61
- Connector Upgrades 54
- Last 5 Minutes 27
- Last Hour 28
- Live 27
- Logger Application Events 138
- Logger Platform Events 138
- Logger System Health Events 140
- Personal Live 27
- Query Viewers Status 106
- Reports Status 106
- System Events Last Hour 28, 43, 100
- Today 27
- Trends Status 106

Active List Access (Details) query 118

Active List Access query 118

Active List Access report 113

active lists

- Account Authenticators 15
- Archive Task Failures 124
- Black List - Connectors 68
- Black List - Reverse Look Up 68
- Compromised List 22
- Connector Average EPS - Last 7 Days 76
- Connector Daily Average EPS 76
- Connector Information 39, 56, 66
- Connector Upgrades 57
- Connectors - Caching 40, 58, 68
- Connectors - Down 39, 57, 67
- Connectors - Dropping Events 39, 67
- Connectors - Still Caching 39, 57, 66
- Connectors - Still Down 40, 58, 67
- Critical Archive Failures 124
- Event-based Rule Exclusions 28
- general configuration 9, 10, 11
- Hit List 22
- Hostile List 22
- Infiltrators List 22
- Invalid Resources 115
- Logger Sensor Type Status 47, 141
- Logger Status 47, 141
- Query Running Time 108, 115
- Reconnaissance List 22
- Reporting Devices 76
- Reporting Devices - Critical 76

Scanned List 22

Suspicious List 22

Trusted List 22

Untrusted List 22

User-based Rule Exclusions 28

- Actor Administration dashboard 88
- Actor Audit Events active channel 88
- Actor Audit Field Set field set 93
- Actor Authenticators query 95
- Actor Authenticators query viewer 89
- Actor Base field set 16
- Actor Change Log dashboard 88
- Actor Change Log data monitor 91
- Actor Change Overview data monitor 91
- Actor Changes filter 95
- Actor Configuration Changes query 96
- Actor Configuration Changes query viewer 88
- Actor Configuration Changes use case 44
- Actor Context Report by Account ID report 14
- Actor Context Report by Attacker Username report 14
- Actor Context Report by Custom Fields report 14
- Actor Context Report by Target Username report 14
- Actor Data asset category 15
- Actor Data Support asset category 15
- Actor Deletes filter 94
- Actor Event Count by Account ID query 17
- Actor Event Count by Attacker Username query 17
- Actor Event Count by Custom Fields query 17
- Actor Event Count by Target Username query 17
- Actor Events by Account ID query 17
- Actor Events by Attacker Username query 17
- Actor Events by Custom Fields query 17
- Actor Events by Target Username query 17
- Actor Full Name and Email Changes query 95
- Actor Full Name and Email Changes query viewer 89
- Actor Full Name and Email Changes report 90
- Actor global variable 92
- Actor Information field set 16
- Actor Information query 17
- Actor Inserts filter 94
- Actor Manager and Department Changes query 95
- Actor Manager and Department Changes query viewer 88
- Actor Manager and Department Changes report 90
- Actor Name or UUID filter 94
- Actor Title and Status Changes query 96
- Actor Title and Status Changes query viewer 89
- Actor Title and Status Changes report 90
- Actor Updates filter 94
- ActorByAccountID global variable 15
- ActorByAttackerUserName global variable 15

- ActorByCustomFields global variable 16
- ActorByDN global variable 16
- ActorByTargetUserName global variable 16
- ActorByUUID global variable 16
- ActorFromFileName global variable 31
- Actors Created query 96
- Actors Created query viewer 89
- Actors Deleted query 96
- Actors Deleted query viewer 89
- Actors Licensing Report focused report 82
- Actors Updated query 96
- Actors Updated query viewer 89
- admincert destination 82
- All Events filter 30, 77, 86, 94, 99, 103, 117
- All Receivers and Forwarders global variable 49
- All Receivers EPS filter 50
- Annotation field set 29
- Annotation-MgrRcpt field set 29
- Archive Activation Statistics query 127
- Archive Archival Statistics query 128
- Archive Archival Success filter 125
- Archive Archival Success query 128
- Archive Deactivation Statistics query 128
- Archive Disk Space data monitor 125
- Archive Disk Space filter 125
- Archive Disk space status is Critical filter 126
- Archive Disk space status is OK filter 126
- Archive Disk Space Usage query 127
- Archive Events filter 126
- Archive Events rule 122
- Archive Events session list 129
- Archive Failure Events filter 126
- Archive Non-success events query 128
- Archive Processing report 121
- Archive Scheduling Statistics query 128
- Archive Settings Updated Event filter 125
- Archive Space status query 128
- Archive Status dashboard 120
- Archive status query 128
- Archive Status Report report 120
- Archive Task Failure Details query 127
- Archive Task Failure Details query viewer 120
- Archive Task Failures active list 124
- Archive Task Failures rule 123
- Archive Task Success rule 121
- ArcSight Admin field set 29, 43, 102
- ArcSight Administration
 - configuring 7
 - installing 7
 - overview 5
- ArcSight Appliances Overview dashboard 46
- ArcSight Audit Events filter 104
- ArcSight Correlation Events filter 31, 51, 145
- ArcSight Events filter 31, 41, 77
- ArcSight Foundations overview 6
- ArcSight Internal Events filter 31, 43, 104
- ArcSight Login Events filter 86
- ArcSight Login Rule Firings filter 86
- ArcSight Login Tracking filter 86
- ArcSight Reporting Statistics data monitor 109, 116
- ArcSight Rules filter 116
- ArcSight Status Monitoring Events filter 102
- ArcSight System
 - configuring 7
 - installing 7
- overview 5
- ArcSight User Hourly Login Trends query 86
- ArcSight User Login rule 85
- ArcSight User Login Timeout rule 85
- ArcSight User Login Trends - Hourly trend 87
- ArcSight User Login Trends report 84
- ArcSight User Logins - Last Hour query 86
- ArcSight User Logins - Last Hour report 84
- ArcSight User Logout rule 85
- ArcSight User Sessions data monitor 85
- ArcSight User Sessions session list 87
- ArcSight User Status dashboard 84
- ASM CPU Load filter 103
- ASM Database Free Space - by Day query 127, 137
- ASM Database Free Space - by Day report 121, 131
- ASM Database Free Space - by Hour query 127, 137
- ASM Database Free Space - by Hour report 121, 130
- ASM Database Free Space - Critical rule 122, 133
- ASM Database Free Space - Warning rule 123, 132
- ASM Database Free Space (current) query 128, 137
- ASM Database Free Space query 128, 137
- ASM Database Free Space report 121, 131
- ASM Database Free Space trend 129, 137
- ASM Database Load Statistics filter 103, 125, 135
- ASM Database Responsiveness - Last 24 hours data monitor 134
- ASM Database Responsiveness - Last Hour data monitor 134
- ASM Database Statistics filter 125, 135
- ASM Database Status Change - Critical rule 122, 131
- ASM Database Status Change - Down rule 122, 132
- ASM Database Status Change - Normal rule 123, 132
- ASM Database Status Change - Space Critical rule 124, 133
- ASM Database Status Change - Space Now Available rule 123, 131
- ASM Database Status Change - Warning rule 124, 132
- ASM Event Flow filter 103
- ASM Events active channel 100
- ASM Events field set 102
- ASM Events filter 30, 43, 103
- ASM Flow Load filter 104
- ASM Load Overview filter 103
- ASM Reports Statistics filter 109, 116
- ASM Resource and Memory Load filter 103
- ASM Sidetable Cache Hit Rates filter 136
- ASM Sidetable Sizes filter 135
- ASM Standing Load filter 104
- asset categories
 - Actor Data 15
 - Actor Data Support 15
 - Criticality 23
 - FIPS-199 24
 - High 22, 23, 76
 - Low 23, 24
 - Medium 23
 - Moderate 22, 23
 - Open Ports 23
 - Protected 101
 - Very High 24
 - Very Low 23
 - Vulnerabilities 23
- Asset field set 30
- Asset Information field set 29
- Assets having Vulnerability report 28

Assets Licensing Report focused report 82
 Attacker Address is NULL filter 95
 Attacker Host Name is NULL filter 95
 Attacker Information is NULL filter 93
 Attacker Port is NULL filter 94
 Attacker User Name is NULL filter 16, 31
 Attacker Zone AND Host are NULL but Address is NOT NULL filter 95
 Attacker Zone AND Host are NULL filter 94
 Attacker Zone is NULL filter 94
 Attacker Zone OR Host is NULL filter 94
 AttackerHost global variable 92
 Attackers on Hostile List filter 25
 Attackers on Infiltrators List filter 24
 Attackers on Reconnaissance List filter 25
 Attackers on Suspicious List filter 24
 Average Data Monitor Evaluations Per Second query 118

B

Black List - Connectors active list 68
 Black List - Reverse Look Up active list 68
 Blocked ArcSight Internal Events filter 30
 By Destination integration command 52
 By Event Name integration command 52
 By Source and Destination integration command 52
 By Source integration command 52
 By User integration command 52
 By Vendor and Product integration command 53

C

Cache History by Connectors query 69
 Cache History by Connectors report 63
 Case Information field set 29
 Categories field set 29
 Change Source global variable 92
 Closed stage 33
 Common Conditions Editor field set 28
 Compromise - Attempt rule 21
 Compromise - Success rule 20
 Compromised List active list 22
 Compromised Targets filter 25
 configuration
 active lists 9, 10, 11
 ArcSight Administration 7
 ArcSight System 7
 Configuration Changes by Type report 90
 Configuration Changes by User report 90
 Connector - Caches session list 71
 Connector Added to Black List rule 65
 Connector Asset Auto Creation Controller filter 30
 Connector Average EPS - Last 7 Days active list 76
 Connector Average EPS - Last 7 Days query 79
 Connector Average EPS - Last 7 days trend 80
 Connector Cache Empty rule 65
 Connector Cache Status data monitor 41, 68
 Connector Cache Status filter 41, 69
 Connector Caching Event filter 69
 Connector Caching Events active channel 61
 Connector Caching rule 66
 Connector Configuration Changes use case 42
 Connector Connection and Cache Status dashboard 37, 61
 Connector Connection and Cache Status use case 42

Connector Connection Status data monitor 40, 69
 Connector Connection Status Events active channel 61
 Connector Connection Status filter 41, 69
 Connector Daily Average EPS active list 76
 Connector Daily Average EPS query 79
 Connector Daily Average EPS trend 79
 Connector Deleted rule 56, 64
 Connector Discovered or Updated rule 66
 Connector Down rule 65
 Connector Dropping Events rule 65
 Connector Information active list 39, 56, 66
 Connector Monitor Event query 78
 Connector Monitoring Events field set 29, 43, 69, 102
 Connector Registered or Heartbeat Event filter 69
 Connector Severity Hourly Stacked Chart query 79
 Connector Severity Hourly Stacked Chart report 73
 Connector Still Caching rule 63
 Connector Still Down rule 64
 Connector Total Events - Hourly trend 80
 Connector Up rule 64
 Connector Upgrade Failed rule 55
 Connector Upgrade Successful rule 56
 Connector Upgrades active channel 54
 Connector Upgrades active list 57
 Connector Upgrades Count (Total) query 59
 Connector Upgrades Count query 58
 Connector Upgrades Count report 55
 Connector Upgrades field set 58
 Connector Version Detected rule 56, 65
 Connector Versions by Type query 59
 Connector Versions by Type report 54
 Connector Versions query 58
 Connector Versions report 54
 Connector Versions session list 59, 71
 Connectors - Caching - Long Term query 42, 70
 Connectors - Caching - Long Term query viewer 38, 62
 Connectors - Caching - Short Term query 42, 70
 Connectors - Caching - Short Term query viewer 38, 62
 Connectors - Caching active list 40, 58, 68
 Connectors - Down - Long Term query viewer 38, 62
 Connectors - Down - Short Term query viewer 38, 62
 Connectors - Down active list 39, 57, 67
 Connectors - Down query 41, 70
 Connectors - Dropping Events active list 39, 67
 Connectors - Dropping Events query 41, 70
 Connectors - Dropping Events query viewer 37, 61
 Connectors - Still Caching active list 39, 57, 66
 Connectors - Still Down active list 40, 58, 67
 Connectors - Still Down query 42, 70
 Console and ArcSight Web Status dashboard 84
 Console Users Licensing Report focused report 82
 Correlation Events Count (Details) query 117
 Correlation Events Count query 117
 Correlation Events filter 16, 31
 Correlation Events Statistics report 114
 CPU and Memory dashboard 140
 CPU Name global variable 49
 CPU Sensors data monitor 143
 CPU Sensors filter 145
 CPU Usage (Percent) - Last 10 Minutes data monitor 48, 144
 CPU Usage (Percent) - Last Hour data monitor 142
 CPU Usage filter 51, 145
 Created report 90
 Critical Archive Failure Details query 127

Critical Archive Failure Details query viewer 120
 Critical Archive Failures active list 124
 Critical Archive Failures rule 121
 Critical Archive Success rule 123
 Critical Device Not Reporting filter 77
 Critical Device Not Reporting rule 76
 Critical Device Reported rule 76
 Critical Devices - Heads Up Display data monitor 77
 Critical Devices Up Down filter 77
 Criticality asset category 23
 Current Cache Status - Caching Events query 70
 Current Cache Status - Dropping Events query 69
 Current Cache Status report 63
 Current Connector Status data monitor 40, 68
 Current Event Sources dashboard 37, 73
 Current Users Logged In data monitor 85
 Currently Running Reports data monitor 108, 115

D

Daily Pattern Discovery profile 33
 dashboards

- Actor Administration 88
- Actor Change Log 88
- Archive Status 120
- ArcSight Appliances Overview 46
- ArcSight User Status 84
- Connector Connection and Cache Status 37, 61
- Console and ArcSight Web Status 84
- CPU and Memory 140
- Current Event Sources 37, 73
- Database Performance Statistics 120, 130
- Device Status 73
- ESM System Information 43
- Event Throughput 100
- Hardware 140
- Latest Events By Priority 100
- My Logger Overview 46, 140
- Network 140
- Partition Manager and Archiver Status 130
- Query Running Time Overview 106, 112
- Query Viewer Details 106
- Report Details 106
- Reporting Subsystem Statistics 106, 112
- Resource Change Log 97
- Rules Status 112
- Storage 140
- Trend Details 106

Data Monitor Evaluations Statistics report 114

data monitors

- Actor Change Log 91
- Actor Change Overview 91
- Archive Disk Space 125
- ArcSight Reporting Statistics 109, 116
- ArcSight User Sessions 85
- ASM Database Responsiveness - Last 24 hours 134
- ASM Database Responsiveness - Last Hour 134
- Connector Cache Status 41, 68
- Connector Connection Status 40, 69
- CPU Sensors 143
- CPU Usage (Percent) - Last 10 Minutes 48, 144
- CPU Usage (Percent) - Last Hour 142
- Critical Devices - Heads Up Display 77
- Current Connector Status 40, 68
- Current Users Logged In 85

- Currently Running Reports 108, 115
- Database Free Space 125, 134
- Database Insert Time - Last 24 Hours 124, 133
- Database Insert Time - Last Hour 125, 134
- Database Retrieval Time - Last 24 Hours 125, 134
- Database Retrieval Time - Last Hour 124, 133
- Database Transaction Volume 124, 133
- Disk Read and Write (Kbytes per Second) - Last 10 Minutes 48, 143
- Disk Read and Write (Kbytes per Second) - Last Hour 143
- Disk Usage 48, 144
- Disk Usage (Percent) 142
- EPS Usage (Events per Second) - Last 10 Minutes 48, 142
- EPS Usage (Events per Second) - Last Hour 142
- Event Throughput 102
- Event Throughput Statistics 102
- Events By Priority 101
- FAN Sensors 143
- Last 10 Trend Queries Returning No Results 109
- Latest Elevated Threat Events 102
- Latest Guarded Threat Events 102
- Latest High Threat Events 102
- Latest Low Threat Events 102
- Latest Severe Threat Events 102
- Logger Disk Usage 47
- Logger Hardware Status 47
- Memory Usage (Mbytes per Second) - Last 10 Minutes 48, 142
- Memory Usage (Mbytes per Second) - Last Hour 143
- Network Usage (Bytes) - Last 10 Minutes 48, 142
- Network Usage (Bytes) - Last Hour 142
- Notification Log 85
- Partial Matches per Rule 116
- Partition Manager and Archiver - Heads Up Display 134
- Partition Manager and Archiver Details 133
- Recent Archive Events 125
- Recent Fired Rules 116
- Recent System Resource Deletes 98
- Recent System Resource Inserts 98
- Recent System Resource Updates 98
- Report Statistics 109, 116
- Resource Change Log 98
- Resource Change Overview 98
- Rule Error Logs 116
- Rules Engine Internal Stats 115
- Sensor Type Status 49, 143
- Sidetable Cache Hit Rates 134
- Sidetable Sizes (Rows) 133
- System Information 43
- System Sensors 144
- Top Event Sources 40, 76
- Top Firing Rules 116
- User Access Log 85
- Database Free Space data monitor 125, 134
- Database Insert Time - Last 24 Hours data monitor 124, 133
- Database Insert Time - Last Hour data monitor 125, 134
- Database Insert Time Statistics filter 125, 134
- Database Performance Statistics dashboard 120, 130
- Database Retrieval Time - Last 24 Hours data monitor 125, 134

- Database Retrieval Time - Last Hour data monitor 124, 133
 - Database Retrieval Time Statistics filter 126, 136
 - Database Transaction Volume data monitor 124, 133
 - Deleted report 89
 - Department New Value global variable 91
 - Department Old Value global variable 93
 - Destination Counts by Connector Type query 79
 - Destination Counts by Connector Type report 75
 - Destination Counts query 104
 - Destination Counts report 101
 - destinations
 - admincert 82
 - Device Asset Auto Creation Controller filter 30
 - Device Monitoring use case 42
 - Device Reported rule 75
 - Device Status dashboard 73
 - Devices Licensing Report focused report 82
 - Disk Name global variable 49
 - Disk Read and Write (Kbytes per Second) - Last 10 Minutes data monitor 48, 143
 - Disk Read and Write (Kbytes per Second) - Last Hour data monitor 143
 - Disk Read and Write filter 52, 146
 - Disk Usage (Percent) data monitor 142
 - Disk Usage data monitor 48, 144
 - Disk Usage filter 145
 - Disk Usage global variable 49
 - DiskUsageCritical global variable 49
 - DN New Value global variable 91
 - DN Old Value global variable 92
- E**
- Elevated Threat Condition filter 104
 - Email Address New Value global variable 93
 - Email Address Old Value global variable 93
 - Employee Type New Value global variable 93
 - Employee Type Old Value global variable 92
 - EPS Licensing Report focused report 82
 - EPS Usage (Events per Second) - Last 10 Minutes data monitor 48, 142
 - EPS Usage (Events per Second) - Last Hour data monitor 142
 - EPS Usage filter 51, 145
 - ESM Configuration Changes by Type report 97
 - ESM Configuration Changes by User report 97
 - ESM Configuration Changes query 99
 - ESM Events use case 44
 - ESM Licensing use case 44
 - ESM Reporting Resource Monitoring use case 44, 119
 - ESM Resource Configuration Changes use case 44
 - ESM Resource Monitoring use case 44
 - ESM Storage Monitoring (CORR) use case 44
 - ESM Storage Monitoring (Oracle) use case 44
 - ESM System Information dashboard 43
 - ESM User Sessions use case 44
 - Event Base field set 28, 43, 58, 69, 102, 109
 - Event Count by Agent Severity query 104
 - Event Count by Agent Severity report 101
 - Event Count by Source Destination Pairs query 105
 - Event Count by Source Destination Pairs report 101
 - Event Data Free Space - Last 30 Days focused report 127, 136
 - Event Distribution Chart for a Connector Type query 78
 - Event Distribution Chart for a Connector Type report 74
 - Event Index Free Space - Last 30 Days focused report 136
 - Event Inspector field set 29
 - Event Name Counts query 105
 - Event Name Counts report 101
 - Event Throughput dashboard 100
 - Event Throughput data monitor 102
 - Event Throughput Statistics data monitor 102
 - Event-based Rule Exclusions active list 28
 - Events by ArcSight Priority (Summary) query 105
 - Events by ArcSight Priority (Summary) report 101
 - Events by Connector Type (Summary) query 79
 - Events by Connector Type (Summary) report 73
 - Events by Device (Summary) query 78
 - Events by Device (Summary) report 73
 - Events By Priority data monitor 101
 - Events by Selected Connector Type query 78
 - Events by Selected Connector Type report 74
 - Events for a Destination by Connector Type query 78
 - Events for a Destination by Connector Type report 74
 - Events from a Source by Connector Type query 79
 - Events from a Source by Connector Type report 75
 - Excessive Rule Recursion rule 115
 - Executive field set 28
 - Export field set 29
 - External Source filter 103
 - External Target filter 104
- F**
- Failed Connector Upgrades query 59
 - Failed Connector Upgrades report 54
 - Failed Queries - Trend query 110, 118
 - Failed Queries query 110, 117
 - Failed Queries report 108
 - Failed Queries trend 111, 119
 - FAN Sensors data monitor 143
 - FAN Sensors filter 146
 - Field Set Based On ARC_E_ET Index field set 29
 - Field Set Based On ARC_E_MRT Index field set 29
 - field sets
 - Actor Audit Field Set 93
 - Actor Base 16
 - Actor Information 16
 - Annotation 29
 - Annotation-MgrRcpt 29
 - ArcSight Admin 29, 43, 102
 - ASM Events 102
 - Asset 30
 - Asset Information 29
 - Case Information 29
 - Categories 29
 - Common Conditions Editor 28
 - Connector Monitoring Events 29, 43, 69, 102
 - Connector Upgrades 58
 - Event Base 28, 43, 58, 69, 102, 109
 - Event Inspector 29
 - Executive 28
 - Export 29
 - Field Set Based On ARC_E_ET Index 29
 - Field Set Based On ARC_E_MRT Index 29
 - Logger Application Events 138
 - Logger Platform Events 138
 - Logger System Health Events 50, 144

- Minimal 29
- MSSP 29
- Query Status 109
- Rule Action - Set Event Field 29
- Security 29
- Standard 28
- Standard-MgrRcpt 29
- Super Minimal 28
- TurboMode Comprehensive 28
- TurboMode Fastest 29
- Field Status global variable 49
- Field Value global variable 49
- File Path StartsWith All Rules filter 126
- filters
 - Actor Changes 95
 - Actor Deletes 94
 - Actor Inserts 94
 - Actor Name or UUID 94
 - Actor Updates 94
 - All Events 30, 77, 86, 94, 99, 103, 117
 - All Receivers EPS 50
 - Archive Archival Success 125
 - Archive Disk Space 125
 - Archive Disk space status is Critical 126
 - Archive Disk space status is OK 126
 - Archive Events 126
 - Archive Failure Events 126
 - Archive Settings Updated Event 125
 - ArcSight Audit Events 104
 - ArcSight Correlation Events 31, 51, 145
 - ArcSight Events 31, 41, 77
 - ArcSight Internal Events 31, 43, 104
 - ArcSight Login Events 86
 - ArcSight Login Rule Firings 86
 - ArcSight Login Tracking 86
 - ArcSight Rules 116
 - ArcSight Status Monitoring Events 102
 - ASM CPU Load 103
 - ASM Database Load Statistics 103, 125, 135
 - ASM Database Statistics 125, 135
 - ASM Event Flow 103
 - ASM Events 30, 43, 103
 - ASM Flow Load 104
 - ASM Load Overview 103
 - ASM Reports Statistics 109, 116
 - ASM Resource and Memory Load 103
 - ASM Sidetable Cache Hit Rates 136
 - ASM Sidetable Sizes 135
 - ASM Standing Load 104
 - Attacker Address is NULL 95
 - Attacker Host Name is NULL 95
 - Attacker Information is NULL 93
 - Attacker Port is NULL 94
 - Attacker User Name is NULL 16, 31
 - Attacker Zone AND Host are NULL 94
 - Attacker Zone AND Host are NULL but Address is NOT NULL 95
 - Attacker Zone is NULL 94
 - Attacker Zone OR Host is NULL 94
 - Attackers on Hostile List 25
 - Attackers on Infiltrators List 24
 - Attackers on Reconnaissance List 25
 - Attackers on Suspicious List 24
 - Blocked ArcSight Internal Events 30
 - Compromised Targets 25
 - Connector Asset Auto Creation Controller 30
 - Connector Cache Status 41, 69
 - Connector Caching Event 69
 - Connector Connection Status 41, 69
 - Connector Registered or Heartbeat Event 69
 - Correlation Events 16, 31
 - CPU Sensors 145
 - CPU Usage 51, 145
 - Critical Device Not Reporting 77
 - Critical Devices Up Down 77
 - Database Insert Time Statistics 125, 134
 - Database Retrieval Time Statistics 126, 136
 - Device Asset Auto Creation Controller 30
 - Disk Read and Write 52, 146
 - Disk Usage 145
 - Elevated Threat Condition 104
 - EPS Usage 51, 145
 - External Source 103
 - External Target 104
 - FAN Sensors 146
 - File Path StartsWith All Rules 126
 - Guarded Threat Condition 103
 - High Criticality Assets 24
 - High Threat Condition 103
 - Hour less than 10 109, 116
 - Inbound Events 103
 - Inbound Network 51
 - Internal Source 103
 - Internal Target 103
 - Logger Application Events 138
 - Logger Disk Usage 51, 146
 - Logger Events 50, 138, 144
 - Logger Hardware Status 50
 - Logger Platform Events 138
 - Logger System Health Events 50, 138, 144
 - Low Criticality Assets 24
 - Low Threat Condition 104
 - ManagerInternalAgent'sFilters' 30
 - Medium Criticality Assets 24
 - Memory Usage 50, 144
 - Minute less than 10 109, 117
 - My Logger 51, 145
 - Network Usage 50, 145
 - No Events 31
 - Non-ArcSight Events 31, 41, 77
 - Non-ArcSight Internal Events 31, 104
 - Non-Categorized Events 30
 - Not Correlated and Not Closed 30
 - Not Correlated and Not Closed and Not Hidden 31
 - Notification Actions 86, 103
 - Outbound Events 104
 - Partition Manager and Archiver Events 135
 - Partition without Submission Events 135
 - Remaining Disk 52
 - Remaining Disk > 10 Percent 51
 - Resource Changes 99
 - Resource Deletes 98
 - Resource Inserts 98
 - Resource Updates 98
 - Rules Engine Internal Events 116
 - Sensor Type is CPU 50, 144
 - Sensor Type is FAN 50, 145
 - Sensor Type Update 51, 145
 - Severe Threat Condition 103
 - Severity High 31

- Severity Low 31
 - Severity Medium 31
 - Severity Unknown 31
 - Severity Very High 30
 - SNMP Trap Sender 31
 - System Sensors 146
 - Target Asset Scanned for Open Ports 24
 - Target Asset Scanned for Vulnerabilities 24
 - Target User Name is NULL 95, 99
 - Threshold - Critical 126, 135
 - Threshold - Warning 126, 134
 - Trend Query Returning No Results 109
 - Unknown Criticality Assets 24
 - Very High Criticality Assets 24
 - Very Low Criticality Assets 24
 - White List - Critical Devices 77
 - White List - Devices 77
 - Final stage 33
 - FIPS-199 asset category 24
 - Fired Rule Events query 117
 - Fired Rule Events report 114
 - Flagged as Similar stage 33
 - focused reports
 - Actors Licensing Report 82
 - Assets Licensing Report 82
 - Console Users Licensing Report 82
 - Devices Licensing Report 82
 - EPS Licensing Report 82
 - Event Data Free Space - Last 30 Days 127, 136
 - Event Index Free Space - Last 30 Days 136
 - System Data Free Space - Last 30 Days 127, 136
 - System Index Free Space - Last 30 Days 136
 - Web Users Licensing Report 82
 - Follow-Up stage 33
 - Free Space global variable 49
 - Full Name New Value global variable 91
 - Full Name Old Value global variable 93
- ## G
- global variables
 - Actor 92
 - ActorByAccountID 15
 - ActorByAttackerUserName 15
 - ActorByCustomFields 16
 - ActorByDN 16
 - ActorByTargetUserName 16
 - ActorByUUID 16
 - ActorFromFile 91
 - All Receivers and Forwarders 49
 - AttackerHost 92
 - Change Source 92
 - CPU Name 49
 - Department New Value 91
 - Department Old Value 93
 - Disk Name 49
 - Disk Usage 49
 - DiskUsageCritical 49
 - DN New Value 91
 - DN Old Value 92
 - Email Address New Value 93
 - Email Address Old Value 93
 - Employee Type New Value 93
 - Employee Type Old Value 92
 - Field Status 49
 - Field Value 49
 - Free Space 49
 - Full Name New Value 91
 - Full Name Old Value 93
 - Inbound and Outbound 49
 - IndexOfUsage 49
 - Location New Value 92
 - Location Old Value 91
 - Logger Address 49
 - Logger IP 49, 144
 - Manager New Value 92
 - Manager Old Value 92
 - Memory Name 49
 - Org New Value 91
 - Org Old Value 93
 - ReadOrWrite 49
 - Sensor Name 49
 - Sensor Status 49
 - Sensor Type 49
 - Status New Value 93
 - Status Old Value 93
 - Timeframe 49
 - Title New Value 91
 - Title Old Value 93
 - Unit 49
 - Guarded Threat Condition filter 103
- ## H
- Hardware dashboard 140
 - High asset category 22, 23, 76
 - High Criticality Assets filter 24
 - High Threat Condition filter 103
 - High Volume Connector EPS - By Day query 78
 - High Volume Connector EPS - Daily report 75
 - High Volume Connector EPS - Hourly query 78
 - High Volume Connector EPS - Weekly report 74
 - Hit List active list 22
 - Hostile - Attempt rule 20
 - Hostile - Success rule 21
 - Hostile List active list 22
 - Hour less than 10 filter 109, 116
 - Hourly Distribution Chart for a Destination Port query 105
 - Hourly Distribution Chart for a Destination Port report 101
 - Hourly Distribution Chart for a Source Port query 104
 - Hourly Distribution Chart for a Source Port report 101
 - Hourly Distribution Chart for Event query 105
 - Hourly Distribution Chart for Event report 101
 - Hourly Event Counts (Area Chart) query 105
 - Hourly Event Counts (Area Chart) report 101
 - Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart) query 105
 - Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart) report 100
- ## I
- IDM Deletions of Actors query 95
 - IDM Deletions of Actors query viewer 88
 - IDM Deletions of Actors report 90
 - Inbound and Outbound global variable 49
 - Inbound Events filter 103
 - Inbound Network filter 51

- Incident Resolved - Remove From List rule 22
- IndexOfUsage global variable 49
- Infiltrators List active list 22
- Initial stage 33
- installing
 - ArcSight Administration 7
 - ArcSight System 7
- integration commands
 - By Destination 52
 - By Event Name 52
 - By Source 52
 - By Source and Destination 52
 - By User 52
 - By Vendor and Product 53
 - Logger Quick Search 53
 - Nslookup (Linux) 32
 - Nslookup (Windows) 32
 - Ping (Linux) 31
 - Ping (Windows) 32
 - Portinfo (Linux) 32
 - Portinfo (Windows) 32
 - Traceroute (Linux) 32
 - Traceroute (Windows) 32
 - Web Search 32
 - Whois (Linux) 32
- integration configurations
 - Logger Quick Search 53
 - Logger Search 53
 - Whois (Windows) 33
- integration targets
 - Logger Appliance 1 53
 - Logger Appliance 2 53
- Internal Source filter 103
- Internal Target filter 103
- Invalid Resources (Chart) query 117
- Invalid Resources active list 115
- Invalid Resources query 117
- Invalid Resources report 113

L

- Last 10 Query Viewer Queries query viewer 107
- Last 10 QueryViewer Queries query 110
- Last 10 Report Queries query 110
- Last 10 Report Queries query viewer 107
- Last 10 Trend Queries query 111
- Last 10 Trend Queries query viewer 107
- Last 10 Trend Queries Returning No Results data monitor 109
- Last 5 Minutes active channel 27
- Last Hour active channel 28
- Latest Elevated Threat Events data monitor 102
- Latest Events By Priority dashboard 100
- Latest Guarded Threat Events data monitor 102
- Latest High Threat Events data monitor 102
- Latest Low Threat Events data monitor 102
- Latest Severe Threat Events data monitor 102
- License Audit Event Detected rule 81
- License Limit Approaching rule 81
- License Limit Exceeded rule 81
- Licensing History session list 83
- Licensing Query query 82
- Licensing Report (All) report 81
- Licensing Report report 81
- Live active channel 27

- Location New Value global variable 92
- Location Old Value global variable 91
- Logger Address global variable 49
- Logger Appliance 1 integration target 53
- Logger Appliance 2 integration target 53
- Logger Application Events active channel 138
- Logger Application Events field set 138
- Logger Application Events filter 138
- Logger Disk Usage data monitor 47
- Logger Disk Usage filter 51, 146
- Logger Events filter 50, 138, 144
- Logger Events use case 53
- Logger Hardware Status data monitor 47
- Logger Hardware Status filter 50
- Logger IP global variable 49, 144
- Logger Platform Events active channel 138
- Logger Platform Events field set 138
- Logger Platform Events filter 138
- Logger Quick Search integration command 53
- Logger Quick Search integration configuration 53
- Logger Search integration configuration 53
- Logger Sensor Status rule 46, 141
- Logger Sensor Type Status active list 47, 141
- Logger Sensor Type Status rule 46, 141
- Logger Status active list 47, 141
- Logger Status rule 47, 141
- Logger System Health Events active channel 140
- Logger System Health Events field set 50, 144
- Logger System Health Events filter 50, 138, 144
- Logger System Health use case 53
- Longest QueryViewer Queries - Trend query 110
- Longest QueryViewer Queries query 109, 117
- Longest QueryViewer Queries report 108
- Longest Report Queries - Trend query 111
- Longest Report Queries query 110, 118
- Longest Report Queries report 108
- Longest Trend Queries - Trend query 111
- Longest Trend Queries query 110, 117
- Longest Trend Query report 108
- Low asset category 23, 24
- Low Criticality Assets filter 24
- Low Threat Condition filter 104
- Low Volume Connector EPS - By Day query 77
- Low Volume Connector EPS - Daily report 73
- Low Volume Connector EPS - Hourly query 78
- Low Volume Connector EPS - Weekly report 75

M

- Manager Internal AgentsFiltersfilter 30
- Manager New Value global variable 92
- Manager Old Value global variable 92
- Medium asset category 23
- Medium Criticality Assets filter 24
- Memory Name global variable 49
- Memory Usage (Mbytes per Second) - Last 10 Minutes data monitor 48, 142
- Memory Usage (Mbytes per Second) - Last Hour data monitor 143
- Memory Usage filter 50, 144
- Minimal field set 29
- Minute less than 10 filter 109, 117
- Moderate asset category 22, 23
- Monitoring stage 33
- MSSP field set 29

My Logger filter 51, 145
 My Logger Overview dashboard 46, 140

N

Network dashboard 140
 Network Usage (Bytes) - Last 10 Minutes data monitor 48, 142
 Network Usage (Bytes) - Last Hour data monitor 142
 Network Usage filter 50, 145
 No Events filter 31
 Non-ArcSight Events filter 31, 41, 77
 Non-ArcSight Internal Events filter 31, 104
 Non-Categorized Events filter 30
 Not Correlated and Not Closed and Not Hidden filter 31
 Not Correlated and Not Closed filter 30
 Notification Actions filter 86, 103
 Notification Log data monitor 85
 Nslookup (Linux) integration command 32
 Nslookup (Windows) integration command 32
 Number of Events matching Rules query 119
 Number of Events Matching Rules report 114

O

Open Ports asset category 23
 Org New Value global variable 91
 Org Old Value global variable 93
 Out of Domain Fields rule 124, 132
 Outbound Events filter 104

P

Partial Matches per Rule data monitor 116
 Partition Manager and Archiver - Heads Up Display data monitor 134
 Partition Manager and Archiver Details data monitor 133
 Partition Manager and Archiver Events filter 135
 Partition Manager and Archiver Status dashboard 130
 Partition without Submission Events filter 135
 Personal Live active channel 27
 Ping (Linux) integration command 31
 Ping (Windows) integration command 32
 Portinfo (Linux) integration command 32
 Portinfo (Windows) integration command 32
 profiles
 Daily Pattern Discovery 33
 Quarter Hourly Pattern Discovery 33
 Protected asset category 101

Q

Quarter Hourly Pattern Discovery profile 33
 queries
 Active List Access 118
 Active List Access (Details) 118
 Actor Authenticators 95
 Actor Configuration Changes 96
 Actor Event Count by Account ID 17
 Actor Event Count by Attacker Username 17
 Actor Event Count by Custom Fields 17
 Actor Event Count by Target Username 17
 Actor Events by Account ID 17
 Actor Events by Attacker Username 17
 Actor Events by Custom Fields 17

Actor Events by Target Username 17
 Actor Full Name and Email Changes 95
 Actor Information 17
 Actor Manager and Department Changes 95
 Actor Title and Status Changes 96
 Actors Created 96
 Actors Deleted 96
 Actors Updated 96
 Archive Activation Statistics 127
 Archive Archival Statistics 128
 Archive Archival Success 128
 Archive Deactivation Statistics 128
 Archive Disk Space Usage 127
 Archive Non-success events 128
 Archive Scheduling Statistics 128
 Archive Space status 128
 Archive status 128
 Archive Task Failure Details 127
 ArcSight User Hourly Login Trends 86
 ArcSight User Logins - Last Hour 86
 ASM Database Free Space 128, 137
 ASM Database Free Space - by Day 127, 137
 ASM Database Free Space - by Hour 127, 137
 ASM Database Free Space (current) 128, 137
 Average Data Monitor Evaluations Per Second 118
 Cache History by Connectors 69
 Connector Average EPS - Last 7 Days 79
 Connector Daily Average EPS 79
 Connector Monitor Event 78
 Connector Severity Hourly Stacked Chart 79
 Connector Upgrades Count 58
 Connector Upgrades Count (Total) 59
 Connector Versions 58
 Connector Versions by Type 59
 Connectors - Caching - Long Term 42, 70
 Connectors - Caching - Short Term 42, 70
 Connectors - Down 41, 70
 Connectors - Dropping Events 41, 70
 Connectors - Still Down 42, 70
 Correlation Events Count 117
 Correlation Events Count (Details) 117
 Critical Archive Failure Details 127
 Current Cache Status - Caching Events 70
 Current Cache Status - Dropping Events 69
 Destination Counts 104
 Destination Counts by Connector Type 79
 ESM Configuration Changes 99
 Event Count by Agent Severity 104
 Event Count by Source Destination Pairs 105
 Event Distribution Chart for a Connector Type 78
 Event Name Counts 105
 Events by ArcSight Priority (Summary) 105
 Events by Connector Type (Summary) 79
 Events by Device (Summary) 78
 Events by Selected Connector Type 78
 Events for a Destination by Connector Type 78
 Events from a Source by Connector Type 79
 Failed Connector Upgrades 59
 Failed Queries 110, 117
 Failed Queries - Trend 110, 118
 Fired Rule Events 117
 High Volume Connector EPS - By Day 78
 High Volume Connector EPS - Hourly 78
 Hourly Distribution Chart for a Destination Port 105
 Hourly Distribution Chart for a Source Port 104

- Hourly Distribution Chart for Event 105
 - Hourly Event Counts (Area Chart) 105
 - Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart) 105
 - IDM Deletions of Actors 95
 - Invalid Resources 117
 - Invalid Resources (Chart) 117
 - Last 10 QueryViewer Queries 110
 - Last 10 Report Queries 110
 - Last 10 Trend Queries 111
 - Licensing Query 82
 - Longest QueryViewer Queries 109, 117
 - Longest QueryViewer Queries - Trend 110
 - Longest Report Queries 110, 118
 - Longest Report Queries - Trend 111
 - Longest Trend Queries 110, 117
 - Longest Trend Queries - Trend 111
 - Low Volume Connector EPS - By Day 77
 - Low Volume Connector EPS - Hourly 78
 - Number of Events matching Rules 119
 - Query Counts During Last 24 hr 110, 118
 - Query Counts During Last Week 111
 - QueryViewer Failures 110
 - QueryViewer Queries 110
 - Report Queries 111
 - Report Query Failures 111
 - Resource Created Report 99
 - Resource Deleted Report 99
 - Resource History Report 99
 - Resource Updated Report 99
 - Rules Engine Warning Messages 118
 - Running Report Queries 111
 - Running Trend Queries 111
 - Session List Access 118
 - Session List Access (Details) 117
 - Source Counts by Connector Type 77
 - Source Counts by Event Name 105
 - Successful Connector Upgrades 59
 - Top 10 Events 104
 - Top 10 Inbound Events 104
 - Top 10 Outbound Events 105
 - Top Accessed Active Lists 117
 - Top Accessed Session Lists 118
 - Top Connector Types Chart 79
 - Trend Query 110
 - Trend Query Failures 110
 - Upgrade History by Connector 58
 - Upgrade History by Connector Type 59
 - User Login Logout Report 86
 - Version History by Connector 59
 - Version History by Connector Type 59
 - Query Counts by Type report 108
 - Query Counts During Last 24 hr query 110, 118
 - Query Counts During Last 24 hr query viewer 107, 113
 - Query Counts During Last Week query 111
 - Query Failures During Last 24 hr query viewer 107, 112
 - Query Running Time active list 108, 115
 - Query Running Time Overview dashboard 106, 112
 - Query Running Time rule 108
 - Query Status field set 109
 - Query Viewer Details dashboard 106
 - Query Viewer Failures During Last 24 hr query viewer 107
 - query viewers
 - Actor Authenticators 89
 - Actor Configuration Changes 88
 - Actor Full Name and Email Changes 89
 - Actor Manager and Department Changes 88
 - Actor Title and Status Changes 89
 - Actors Created 89
 - Actors Deleted 89
 - Actors Updated 89
 - Archive Task Failure Details 120
 - Connectors - Caching - Long Term 38, 62
 - Connectors - Caching - Short Term 38, 62
 - Connectors - Down - Long Term 38, 62
 - Connectors - Down - Short Term 38, 62
 - Connectors - Dropping Events 37, 61
 - Critical Archive Failure Details 120
 - IDM Deletions of Actors 88
 - Last 10 Query Viewer Queries 107
 - Last 10 Report Queries 107
 - Last 10 Trend Queries 107
 - Query Counts During Last 24 hr 107, 113
 - Query Failures During Last 24 hr 107, 112
 - Query Viewer Failures During Last 24 hr 107
 - Report Query Failures During Last 24 hr 107
 - Running Report Queries 107
 - Running Trend Queries 107
 - Top 10 Longest Query Viewer Queries During Last 24 hr 107, 113
 - Top 10 Longest Report Queries During Last 24 hr 107, 113
 - Top 10 longest Trend Queries During Last 24 hr 107, 112
 - Trend Queries Failures During Last 24 hr 107
 - Query Viewers Status active channel 106
 - QueryViewer Failures query 110
 - QueryViewer Queries query 110
 - QueryViewer Queries trend 111
 - Queued stage 33
- ## R
- ReadOrWrite global variable 49
 - Recent Archive Events data monitor 125
 - Recent Fired Rules data monitor 116
 - Recent System Resource Deletes data monitor 98
 - Recent System Resource Inserts data monitor 98
 - Recent System Resource Updates data monitor 98
 - Reconnaissance - Distributed Host Port Scan rule 19
 - Reconnaissance - Distributed Network Host Scan rule 20
 - Reconnaissance - In Progress rule 18
 - Reconnaissance - Multiple Host Scan rule 19
 - Reconnaissance - Network Service Scan rule 19
 - Reconnaissance - Script Scan rule 21
 - Reconnaissance - Stealthy Host Port Scan rule 19
 - Reconnaissance - Vulnerability Scan rule 21
 - Reconnaissance List active list 22
 - Remaining Disk 52
 - Remaining Disk > 10 Percent filter 51
 - Report Details dashboard 106
 - Report Queries query 111
 - Report Queries trend 111
 - Report Query Failures During Last 24 hr query viewer 107
 - Report Query Failures query 111
 - Report Statistics data monitor 109, 116
 - Reporting Devices - Critical active list 76
 - Reporting Devices active list 76

Reporting Subsystem Statistics dashboard 106, 112 reports

- Active List Access 113
- Actor Context Report by Account ID 14
- Actor Context Report by Attacker Username 14
- Actor Context Report by Custom Fields 14
- Actor Context Report by Target Username 14
- Actor Full Name and Email Changes 90
- Actor Manager and Department Changes 90
- Actor Title and Status Changes 90
- Archive Processing 121
- Archive Status Report 120
- ArcSight User Login Trends 84
- ArcSight User Logins - Last Hour 84
- ASM Database Free Space 121, 131
- ASM Database Free Space - by Day 121, 131
- ASM Database Free Space - by Hour 121, 130
- Assets having Vulnerability 28
- Cache History by Connectors 63
- Configuration Changes by Type 90
- Configuration Changes by User 90
- Connector Severity Hourly Stacked Chart 73
- Connector Upgrades Count 55
- Connector Versions 54
- Connector Versions by Type 54
- Correlation Events Statistics 114
- Created 90
- Current Cache Status 63
- Data Monitor Evaluations Statistics 114
- Deleted 89
- Destination Counts 101
- Destination Counts by Connector Type 75
- ESM Configuration Changes by Type 97
- ESM Configuration Changes by User 97
- Event Count by Agent Severity 101
- Event Count by Source Destination Pairs 101
- Event Distribution Chart for a Connector Type 74
- Event Name Counts 101
- Events by ArcSight Priority (Summary) 101
- Events by Connector Type (Summary) 73
- Events by Device (Summary) 73
- Events by Selected Connector Type 74
- Events for a Destination by Connector Type 74
- Events from a Source by Connector Type 75
- Failed Connector Upgrades 54
- Failed Queries 108
- Fired Rule Events 114
- High Volume Connector EPS - Daily 75
- High Volume Connector EPS - Weekly 74
- Hourly Distribution Chart for a Destination Port 101
- Hourly Distribution Chart for a Source Port 101
- Hourly Distribution Chart for Event 101
- Hourly Event Counts (Area Chart) 101
- Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart) 100
- IDM Deletions of Actors 90
- Invalid Resources 113
- Licensing Report 81
- Licensing Report (All) 81
- Longest QueryViewer Queries 108
- Longest Report Queries 108
- Longest Trend Query 108
- Low Volume Connector EPS - Daily 73
- Low Volume Connector EPS - Weekly 75
- Number of Events Matching Rules 114

- Query Counts by Type 108
- Resource Created Report 97
- Resource Deleted Report 98
- Resource History Report 97
- Resource Updated Report 98
- Rules Engine Warning Messages 113
- Session List Access 113
- Source Counts by Connector Type 74
- Source Counts by Event Name 100
- Successful Connector Upgrades 55
- Top 10 Events 100
- Top 10 Inbound Events 100
- Top 10 Outbound Events 101
- Top Accessed Active Lists 113
- Top Accessed Session Lists 114
- Top Connector Types Chart 75
- Updated 90
- Upgrade History by Connector 55
- Upgrade History by Connector Type 54
- User Login Logout Report 84
- Version History by Connector 55
- Version History by Connector Type 55
- Vulnerabilities of an Asset 28
- Reports Status active channel 106
- Resource Became Invalid rule 114
- Resource Became Valid rule 115
- Resource Change Log dashboard 97
- Resource Change Log data monitor 98
- Resource Change Overview data monitor 98
- Resource Changes filter 99
- Resource Created Report query 99
- Resource Created Report report 97
- Resource Deleted Report query 99
- Resource Deleted Report report 98
- Resource Deletes filter 98
- Resource History Report query 99
- Resource History Report report 97
- Resource Inserts filter 98
- Resource Updated Report query 99
- Resource Updated Report report 98
- Resource Updates filter 98
- Rule Action - Set Event Field field set 29
- Rule Created stage 33
- Rule Error Logs data monitor 116
- Rule Matching Too Many Events rule 115
- rules
 - Archive Events 122
 - Archive Task Failures 123
 - Archive Task Success 121
 - ArcSight User Login 85
 - ArcSight User Login Timeout 85
 - ArcSight User Logout 85
 - ASM Database Free Space - Critical 122, 133
 - ASM Database Free Space - Warning 123, 132
 - ASM Database Status Change - Critical 122, 131
 - ASM Database Status Change - Down 122, 132
 - ASM Database Status Change - Normal 123, 132
 - ASM Database Status Change - Space Critical 124, 133
 - ASM Database Status Change - Space Now Available 123, 131
 - ASM Database Status Change - Warning 124, 132
 - Compromise - Attempt 21
 - Compromise - Success 20
 - Connector Added to Black List 65

- Connector Cache Empty 65
 - Connector Caching 66
 - Connector Deleted 56, 64
 - Connector Discovered or Updated 66
 - Connector Down 65
 - Connector Dropping Events 65
 - Connector Still Caching 63
 - Connector Still Down 64
 - Connector Up 64
 - Connector Upgrade Failed 55
 - Connector Upgrade Successful 56
 - Connector Version Detected 56, 65
 - Critical Archive Failures 121
 - Critical Archive Success 123
 - Critical Device Not Reporting 76
 - Critical Device Reported 76
 - Device Reported 75
 - Excessive Rule Recursion 115
 - Hostile - Attempt 20
 - Hostile - Success 21
 - Incident Resolved - Remove From List 22
 - License Audit Event Detected 81
 - License Limit Approaching 81
 - License Limit Exceeded 81
 - Logger Sensor Status 46, 141
 - Logger Sensor Type Status 46, 141
 - Logger Status 47, 141
 - Out of Domain Fields 124, 132
 - Query Running Time 108
 - Reconnaissance - Distributed Host Port Scan 19
 - Reconnaissance - Distributed Network Host Scan 20
 - Reconnaissance - In Progress 18
 - Reconnaissance - Multiple Host Scan 19
 - Reconnaissance - Network Service Scan 19
 - Reconnaissance - Script Scan 21
 - Reconnaissance - Stealthy Host Port Scan 19
 - Reconnaissance - Vulnerability Scan 21
 - Resource Became Invalid 114
 - Resource Became Valid 115
 - Rule Matching Too Many Events 115
 - Update Connector Caching Status 38, 64
 - Update Connector Connection Status 38, 64
 - Rules Engine Internal Events filter 116
 - Rules Engine Internal Stats data monitor 115
 - Rules Engine Warning Messages query 118
 - Rules Engine Warning Messages report 113
 - Rules Status dashboard 112
 - Running Report Queries query 111
 - Running Report Queries query viewer 107
 - Running Trend Queries query 111
 - Running Trend Queries query viewer 107
- S**
- Scanned List active list 22
 - Security field set 29
 - Sensor Name global variable 49
 - Sensor Status global variable 49
 - Sensor Type global variable 49
 - Sensor Type is CPU filter 50, 144
 - Sensor Type is FAN filter 50, 145
 - Sensor Type Status data monitor 49, 143
 - Sensor Type Update filter 51, 145
 - Session List Access (Details) query 117
 - Session List Access query 118
 - Session List Access report 113
 - session lists
 - Archive Events 129
 - ArcSight User Sessions 87
 - Connector - Caches 71
 - Connector Versions 59, 71
 - Licensing History 83
 - Severe Threat Condition filter 103
 - Severity High filter 31
 - Severity Low filter 31
 - Severity Medium filter 31
 - Severity Unknown filter 31
 - Severity Very High filter 30
 - Sidetable Cache Hit Rates data monitor 134
 - Sidetable Sizes (Rows) data monitor 133
 - SNMP Trap Sender filter 31
 - Source Counts by Connector Type query 77
 - Source Counts by Connector Type report 74
 - Source Counts by Event Name query 105
 - Source Counts by Event Name report 100
 - stages
 - Closed 33
 - Final 33
 - Flagged as Similar 33
 - Follow-Up 33
 - Initial 33
 - Monitoring 33
 - Queued 33
 - Rule Created 33
 - Standard field set 28
 - Standard-MgrRcpt field set 29
 - Status New Value global variable 93
 - Status Old Value global variable 93
 - Storage dashboard 140
 - Successful Connector Upgrades query 59
 - Successful Connector Upgrades report 55
 - Super Minimal field set 28
 - Suspicious List active list 22
 - System Data Free Space - Last 30 Days focused report 127, 136
 - System Events Last Hour active channel 28, 43, 100
 - System Index Free Space - Last 30 Days focused report 136
 - System Information data monitor 43
 - System Sensors data monitor 144
 - System Sensors filter 146
- T**
- Target Asset Scanned for Open Ports filter 24
 - Target Asset Scanned for Vulnerabilities filter 24
 - Target User Name is NULL filter 95, 99
 - Threshold - Critical filter 126, 135
 - Threshold - Warning filter 126, 134
 - Timeframe global variable 49
 - Title New Value global variable 91
 - Title Old Value global variable 93
 - Today active channel 27
 - Top 10 Events query 104
 - Top 10 Events report 100
 - Top 10 Inbound Events query 104
 - Top 10 Inbound Events report 100
 - Top 10 Longest Query Viewer Queries During Last 24 hr query viewer 107, 113
 - Top 10 Longest Report Queries During Last 24 hr query

viewer 107, 113
 Top 10 longest Trend Queries During Last 24 hr query viewer 107, 112
 Top 10 Outbound Events query 105
 Top 10 Outbound Events report 101
 Top Accessed Active Lists query 117
 Top Accessed Active Lists report 113
 Top Accessed Session Lists query 118
 Top Accessed Session Lists report 114
 Top Connector Types Chart query 79
 Top Connector Types Chart report 75
 Top Event Sources data monitor 40, 76
 Top Firing Rules data monitor 116
 Traceroute (Linux) integration command 32
 Traceroute (Windows) integration command 32
 Trend Details dashboard 106
 Trend Queries Failures During Last 24 hr query viewer 107
 Trend Queries trend 111
 Trend Query Failures query 110
 Trend Query query 110
 Trend Query Returning No Results filter 109
 trends
 ArcSight User Login Trends - Hourly 87
 ASM Database Free Space 129, 137
 Connector Average EPS - Last 7 days 80
 Connector Daily Average EPS 79
 Connector Total Events - Hourly 80
 Failed Queries 111, 119
 QueryViewer Queries 111
 Report Queries 111
 Trend Queries 111
 Trends Status active channel 106
 Trusted List active list 22
 TurboMode Comprehensive field set 28
 TurboMode Fastest field set 29

U

Unit global variable 49
 Unknown Criticality Assets filter 24
 Untrusted List active list 22
 Update Connector Caching Status rule 38, 64
 Update Connector Connection Status rule 38, 64
 Updated report 90
 Upgrade History by Connector query 58

Upgrade History by Connector report 55
 Upgrade History by Connector Type query 59
 Upgrade History by Connector Type report 54
 use cases
 Actor Configuration Changes 44
 Connector Configuration Changes 42
 Connector Connection and Cache Status 42
 Device Monitoring 42
 ESM Events 44
 ESM Licensing 44
 ESM Reporting Resource Monitoring 44, 119
 ESM Resource Configuration Changes 44
 ESM Resource Monitoring 44
 ESM Storage Monitoring (CORR) 44
 ESM Storage Monitoring (Oracle) 44
 ESM User Sessions 44
 Logger Events 53
 Logger System Health 53
 viewing 12
 User Access Log data monitor 85
 User Login Logout Report query 86
 User Login Logout Report report 84
 User-based Rule Exclusions active list 28

V

Version History by Connector query 59
 Version History by Connector report 55
 Version History by Connector Type query 59
 Version History by Connector Type report 55
 Very High asset category 24
 Very High Criticality Assets filter 24
 Very Low asset category 23
 Very Low Criticality Assets filter 24
 Vulnerabilities asset category 23
 Vulnerabilities of an Asset report 28

W

Web Search integration command 32
 Web Users Licensing Report focused report 82
 White List - Critical Devices filter 77
 White List - Devices filter 77
 Whois (Linux) integration command 32
 Whois (Windows) integration configuration 33

