Standard Content Guide

Configuration Monitoring

for ArcSight ESM 5.5

March 1, 2013

ArcSight™
An HP Company

Standard Content Guide - Configuration Monitoring

Revision History

Date	Product Version	Description
03/01/2013	Configuration Monitoring 5.5	Final revision for release.

Document template version: 2.1

Contact Information

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Contents

Chapter 1

Configuration Monitoring Overview

This chapter discusses the following topics.

What is Standard Content?

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

The standard content is installed using a series of packages, some of which are installed automatically with the Manager to provide essential system health and status operations. The remaining packages are presented as install-time options organized by category.

Standard content consists of the following:

- **ArcSight System** content is installed automatically with the Manager and consists of resources required for basic security processing functions, such as threat escalation and priority calculations, as well as basic throughput channels required for out-of-the-box functionality.
- **ArcSight Administration** content is installed automatically with the Manager, and provides statistics about the health and performance of ArcSight products. ArcSight Administration is essential for managing and tuning the performance of content and components.
- **ArcSight Foundations** content (such as Configuration Monitoring, Intrusion Monitoring, Network Monitoring, NetFlow Monitoring, and Workflow) are presented as install-time options and provide a coordinated system of resources with real-time monitoring capabilities for a specific area of focus, as well as after-the-fact analysis in the form of reports and trends. You can extend these foundations with additional resources specific to your needs or you can use them as a template for building your own resources and tasks.
- **Shared Libraries -** ArcSight Administration and several of the ArcSight Foundations rely on a series of common resources that provide core functionality for common

security scenarios. Dependencies between these resources and the packages they support are managed by the Package resource.

- Anti-Virus content is a set of filters, reports, and report queries used by ArcSight Foundations, such as Configuration Monitoring and Intrusion Monitoring.
- Conditional Variable Filters are a library of filters used by variables in standard content report queries, filters, and rule definitions. The Conditional Variable Filters are used by ArcSight Administration and certain ArcSight Foundations, such as Configuration Monitoring, Intrusion Monitoring, Network Monitoring, and Workflow.
- Global Variables are a set of variables used to create other resources and to provide event-based fields that cover common event information, asset, host, and user information, and commonly used timestamp formats. The Global Variables are used by ArcSight Administration and certain ArcSight Foundations.
- Network filters are a set of filters required by ArcSight Administration and certain ArcSight Foundations, such as Intrusion Monitoring and Network Monitoring.

Standard Content Packages

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

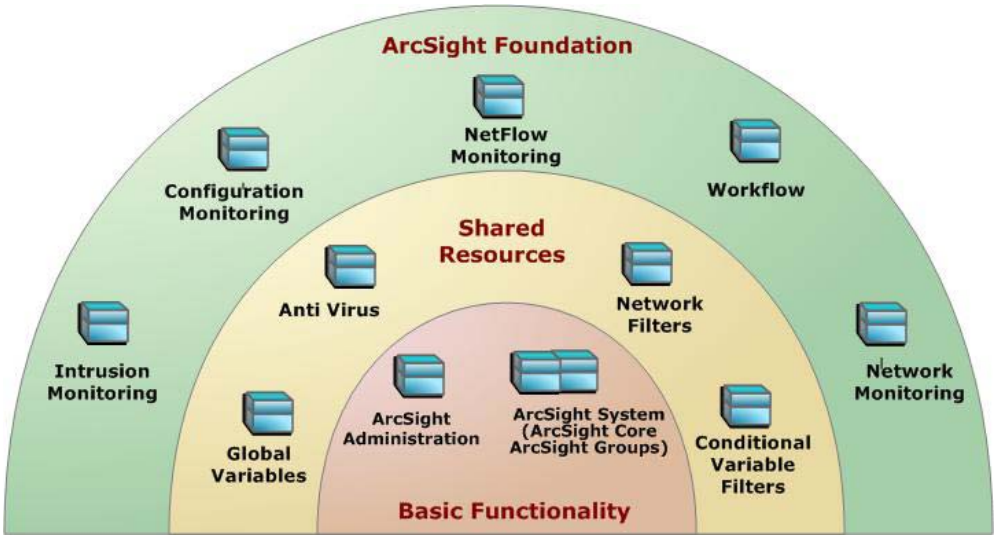

Figure 1-1 The ArcSight System and ArcSight Administration packages at the base provide content required for basic ArcSight functionality. The common packages in the center contain shared resources that support ArcSight Administration and the ArcSight Foundation packages. The packages shown on top are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

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

Note

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

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

Configuration Monitoring Content

The Configuration Monitoring content identifies, analyzes, and remediates undesired modifications to systems, devices, and applications. These modifications include installing new applications, adding new systems to the network, anti-virus/network scanner/IDS engine and signature updates, and asset vulnerability postures. This content helps IT and security staff pinpoint and resolve problems quickly, and provides essential visibility into the network configuration so you understand the systems you have, where they are, what they host, and what vulnerabilities they expose.

Windows systems provide ample user and host account modification information. In most cases, if an adequate auditing level is enabled, you can see modifications to applications, changes to user privilege levels, system configuration changes, even file access.

Unix-based systems provide less visibility into internal system activity. Because there is little consistency to what is reported from system to system, it is often not possible to easily identify actions, such as software installations. In some cases, auditing can be enabled on Unix-based systems, although the output might be too granular to be useful during analysis.

Other network devices, such as routers and firewalls, can be configured to report software or operating system updates and provide basic log information that is useful to the Configuration Monitoring content.

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

Chapter 2

Installation and Configuration

This chapter discusses the following topics.

For information about upgrading standard content, see Appendix A, Upgrading Standard Content, on page 69.

Installing the Configuration Monitoring Package

The Configuration Monitoring Foundation is one of the standard content packages that are presented as install-time options. If you selected all the standard content packages to be installed at installation time, the packages and their resources will be installed in the ArcSight database and available in the Navigator panel resource tree. The package icon in the Navigator panel package view will appear blue.

If you opted to exclude any packages at installation time, the package is imported into the ESM package view in the Navigator panel, but is not available in the resource view. The package icon in the package view will appear grey.

If you do not want the package to be available in any form, you can delete the package.

To install a package that is imported, but not installed:

1. In the Navigator panel Package view, navigate to the package you want to install.
2. Right-click the package and select **Install Package**.
3. In the Install Package dialog, click **OK**.
4. When the installation is complete, review the summary report and click **OK**.

   The package resources are fully installed to the ArcSight database, the resources are fully enabled and operational, and available in the Navigator panel resource tree.

To uninstall a package that is installed:

1. In the Navigator Panel Package view, navigate to the package you want to uninstall.
2. Right-click the package and select **Uninstall Package**.
3. In the Uninstall Package dialog, click **OK**.

   The progress of the uninstall displays in the Progress tab of the Uninstalling Packages dialog. If a message displays indicating that there is a conflict, select an option in the Resolution Options area and click **OK**.

4 When uninstall is complete, review the summary and click **OK**.

The package is removed from the ArcSight database and the Navigator panel resource tree, but remains available in the Navigator panel package view, and can be re-installed at another time.

To delete a package and remove it from the Console and the database:

1 In the Navigator Panel Package view, navigate to the package you want to delete.

2 Right-click the package and select **Delete Package**.

3 When prompted for confirmation of the delete, click **Delete**.

The package is removed from the Navigator panel package view.

Configuring the Configuration Monitoring Content

Some Configuration Monitoring resources require configuration to be functional, and some rely on universal configurations. Most require no additional configuration.

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

- "Modeling the Network" on page 10
- "Categorizing Assets" on page 11
- "Configuring Active Lists" on page 11
- "Enabling Rules" on page 12
- "Ensuring Filters Capture Relevant Data" on page 12
- "Configuring Notification Destinations" on page 13
- "Configuring Notifications and Cases" on page 13
- "Scheduling Reports" on page 13
- "Configuring Trends" on page 13

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* or the ESM online Help. To learn more about the architecture of the ESM network modeling tools, refer to the *ESM 101* guide.

Categorizing Assets

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

- Categorize all assets (or the zones to which the assets belong) that are internal to the network with the `/All Asset Categories/Site Asset Categories/Address Spaces/Protected` 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 `/All Asset Categories/System Asset Categories/Criticality/High` or `Very High` 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.

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

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

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

Configuring Active Lists

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

You must configure the `All Active Lists/ArcSight Foundation/Configuration Monitoring/Local User Allowed Systems` active list with the IP address, zone, and customer (if applicable) of systems that allow local users to be created. These are typically systems operated by IT or network development groups.

The entries in this static active list are used by the Local Windows User Creation - Disallowed Host and the Local Windows User Creation - Allowed Host rules. If this active list is not configured, or is not relevant to your operating environment, the rules will not yield appropriate results. This does not affect overall content functionality.

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.

Ensuring Filters Capture Relevant Data

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

To ensure that a filter captures the relevant events:

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

   If you do not see the events of interest:

   a. Verify that the configuration of the active channel is suitable for the events in question. For example, ensure that the event time is within the start and end time of the channel.

   b. Modify the filter condition to capture the events of interest. After applying the change, repeat Step 2 to verify that the modified filter captures the required events.

For a list of the Configuration Monitoring filters you need to configure, refer to the configuration information for each use case presented in Chapter 3, Configuration Monitoring Content, on page 15.

Enabling Rules

ESM rules trigger only if they are deployed in the `Real-Time Rules` group and are enabled. All Configuration Monitoring rules are deployed by default in the `Real-Time Rules` group and are enabled.

To 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 disable.
3. Right-click the rule and select **Disable 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, so the admin user needs to configure the destinations *and* enable the notification in the rules. For details about enabling the notifications in rules, see Configuring Notifications and Cases, below.

Some Configuration Monitoring rules reference two notification groups: CERT Team and SOC Operators. Add new destinations for notification levels 1, 2, and 3 as appropriate to the personnel in your security operations center. Refer to the *ArcSight Console User's Guide* or the ESM online Help for information on how to configure notification destinations.

Configuring Notifications and Cases

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

By default, the notifications and create case actions are disabled in the standard content rules that send notifications about security-related events to the Cert Team notification group.

To enable rules to send notifications and open cases, first configure notification destinations as described in Configuring Notification Destinations above, then enable the notification and case actions in the rules.

For more information about working with rule actions in the Rules Editor, refer to the *ArcSight Console User's Guide* or the ESM online Help.

Scheduling Reports

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

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

Configuring Trends

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

Configuration Monitoring content includes several trends, some of 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. These schedules can be customized to suit your needs using the Trend scheduler in the Console.

To disable or enable a trend, go to the Navigator panel, right-click the trend and select **Disable Trend** or **Enable Trend**.

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* or the ESM online Help.

Chapter 3

Configuration Monitoring Content

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

Resource Group	Purpose
"Assets" on page 16	The Assets resources provide information about systems that have been started, shutdown, or restarted.
"Configuration Changes Overview" on page 20	The Configuration Changes Overview resources provide an overview of the current system configuration, system configuration changes, and systems with a criticality rating by zone.
"Device Configuration Changes" on page 23	The Device Configuration Changes resources provide information about configuration changes to hosts and applications.
"Hosts and Applications Overview" on page 32	The Hosts and Applications Overview resources provide an overview of the configuration of systems with common applications, such as email servers and databases.
"Security Application and Device Configuration Changes" on page 40	The Security Application and Device Configuration Changes resources provide information about configuration changes to security applications.
"User Configuration Changes" on page 49	The User Configuration Changes resources provide information about user configuration by identifying and monitoring user accounts and the hosts/addresses associated with them. This ties a user to certain IP addresses, MAC addresses, host-names, zones, and so on. The reports cover user account additions, modifications to those accounts, and account removal.
"Vulnerabilities" on page 61	The Vulnerabilities resources provide an overview about current vulnerabilities on systems.

Assets

The Assets resources provide information about systems that have been started, shutdown, or restarted.

Resources

The following table lists all the resources in the Assets resource group and any dependant resources.

Table 3-1 Resources that Support the Assets Group

Resource	Description	Type	URI
Monitor Resources			
User Login Failures Trend - Past Week	This report provides aggregate information about the user accounts that experience failed logins most often during the past 7 days.	Report	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Access Tracking/
Top User Logins - Last Week	This report provides an overview of the top users attempting logins during the past week.	Report	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Access Tracking/
Critical Asset Startup and Shutdown Event Log - Last Day	This report provides a listing of the critical system startup and shutdown events seen during the past day.	Report	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Asset Restarts/
Critical Asset Startup and Shutdown Trend	This report displays summary data from a trend table to provide a count of how often your critical systems startup or shut down. Note: The Critical System Startup and Shutdown Events - Daily Trend is not enabled by default.	Report	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Asset Restarts/
Asset Startup and Shutdown Log - Last Week	This report queries a trend table to retrieve a listing of all system startup and shutdown events seen during the past week.	Report	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Asset Restarts/
Assets Restarting Twice or More - Last Week	This report displays a list of assets that appear to be restarting twice or more per week. Depending on the function of these assets, these events might indicate a problem and need to be investigated.	Report	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Asset Restarts/
Asset Startup and Shutdown Event Log - Last Day	This report provides a listing of the system startup and shutdown events seen during the past day.	Report	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Asset Restarts/

Resource	Description	Type	URI
Top User Logins - Yesterday	This report displays a summary of the top N user logins that occurred yesterday and lists the login counts by user.	Report	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Access Tracking/
Library - Correlation Resources			
Critical Host Shutdown Detected	This rule detects when a host with high or very high criticality is shut down. This rule is a part of the Configuration Monitoring content.	Rule	ArcSight Foundation/Configuration Monitoring/
Library Resources			
Criticality	This is a system asset category.	Asset Category	System Asset Categories
High	This is a system asset category.	Asset Category	System Asset Categories/Criticality
Very High	This is a system asset category.	Asset Category	System Asset Categories/Criticality
User Account Login Attempts	This filter uses ArcSight categories to choose events that indicate user login attempts. These might be successful or failures.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/User/Access Tracking/
System Startup Events	This filter identifies events that indicate a system has started up. This is often indicative of a reboot.	Filter	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Asset Restarts/
Failed User Account Login Attempts	This filter uses the ArcSight event categories to identify failed user account login attempts.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/User/Access Tracking/
System Shutdown Events	This filter identifies events that indicate a system has shutdown. This is often indicative of a reboot.	Filter	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Asset Restarts/
Successful User Account Login Attempts	This filter uses the ArcSight event categories to identify successful user account login attempts.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/User/Access Tracking/
All Events	Filter that matches all events.	Filter	ArcSight System/Core
Most Common Account Logins by Target User (Yesterday)	This query selects events passed by the Successful User Account Login Attempts filter.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Access Tracking/

Resource	Description	Type	URI
Systems Restarted Twice or More - Last Week	This query checks the system startup and shutdown trend table, and retrieves a list of the systems that have restarted more than once in the past week. The query shows the restart history for each system each day.	Query	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Asset Restarts/
Most Common Account Login Attempts - Last Day	This query selects events passed by the User Account Login Attempts filter.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Access Tracking/
Critical System Startup and Shutdown Events - By Zone and Asset	This query collects summary data from a trend table to provide a count of how often your critical systems startup or shut down. Note: The Critical System Startup and Shutdown Events - Daily Trend is not enabled by default.	Query	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Asset Restarts/
Most Common Account Login Attempts Trend - Last Week	This query retrieves a listing of the count of target user account logins by zone for the last seven days.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Access Tracking/
System Startups and Shutdowns	This query collects information about system startup and shutdown events that occurred yesterday. The startup events typically indicate a system restart, but may not be reliably matched with shutdown events.	Query	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Asset Restarts/
Critical System Startups and Shutdowns - Trend Query	This query collects information about critical system startup and shutdown events that occurred yesterday. The startup events typically indicate a system restart, but may not be reliably matched with shutdown events.	Query	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Asset Restarts/
Failed User Account Login Attempts (Yesterday)	This query selects events passed by the Failed User Account Login Attempts filter.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Access Tracking/
User Account Login Failures - Weekly Trend	This query retrieves aggregated information about failed logins over the past week from a trend table.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Access Tracking/
Restart Log by Zone - Last Week	This query retrieves a list of all asset startup and shutdown events over the past week.	Query	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Asset Restarts/

Resource	Description	Type	URI
Most Common Account Login Attempts - Daily Trend	This trend collects daily statistics about User Account Login Attempts to track the most frequent user logins.	Trend	ArcSight Foundation/Configuration Monitoring/User Access Tracking/
Asset Startup and Shutdown Events - Daily Trend	This trend collects daily statistics on shutdown and startup events from your different assets. The trend query includes information on the device product and vendor so that you can query the trend for statistics by operating system.	Trend	ArcSight Foundation/Configuration Monitoring/Asset Restarts/
Critical System Startup and Shutdown Events - Daily Trend	This trend collects daily statistics about critical system startup and shutdown events. The startup events typically indicate a system restart, but may not be reliably matched with shutdown events. This trend is a more focused view (assets modeled with criticality categorization) of the Asset Startup and Shutdown Events - Daily Trend. Note: This trend is not enabled by default.	Trend	ArcSight Foundation/Configuration Monitoring/Asset Restarts/
User Account Login Failures	This trend collects aggregate information about failed user account login attempts. It also collects other information including the target zone as well as the target device vendor and product.	Trend	ArcSight Foundation/Configuration Monitoring/User Access Tracking/

Configuration Changes Overview

The Configuration Changes Overview resources provide an overview of the current system configuration, system configuration changes, and systems with a criticality rating by zone.

Configuration

The Configuration Changes Overview resource group requires the following configuration for your environment:

- Adjust the value of the **TTL Days** field in the Assets with Recent Configuration Modifications active list, if needed**.**

  The Assets with Recent Configuration Modifications active list tracks devices and hosts that have had some sort of configuration modification within the time period specified. The default value is set to a seven day period.

Resources

The following table lists all the resources in the Configuration Changes Overview resource group and any dependant resources.

Table 3-2 Resources that Support the Configuration Changes Overview Group

Resource	Description	Type	URI
Monitor Resources			
Configuration Changes Overview	This dashboard shows an overview of the successful configuration changes for databases, firewalls, VPNs, and network devices.	Dashboard	ArcSight Foundation/Configuration Monitoring/Operational Summaries/
Library - Correlation Resources			
Successful Configuration Change	This rule detects events with successful configuration changes. This rule only requires one such event within two minutes. After this rule has triggered, the target asset and user information is added to the Assets with Recent Configuration Modifications active list.	Rule	ArcSight Foundation/Configuration Monitoring/
Library Resources			
Assets with Recent Configuration Modifications	This active list tracks devices and hosts that have had some sort of configuration modification in the past seven days.	Active List	ArcSight Foundation/Configuration Monitoring/
Last 10 Database Configuration Changes	This data monitor shows the last ten successful database configuration changes.	Data Monitor	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Configuration Changes Overview/

Resource	Description	Type	URI
Last 10 Firewall Configuration Changes	This data monitor shows the last ten successful firewall configuration changes.	Data Monitor	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Configuration Changes Overview/
Last 10 VPN Configuration Changes	This data monitor shows the last ten successful VPN configuration changes.	Data Monitor	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Configuration Changes Overview/
Last 10 Network Configuration Changes	This data monitor shows the last ten successful configuration changes on network devices.	Data Monitor	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Configuration Changes Overview/
Network Events	This filter identifies events with the category object starts with Network or the category device group starts with Network Equipment.	Filter	ArcSight Foundation/Common/Device Class Filters/
VPN Events	This filter identifies events with the category device group of VPN.	Filter	ArcSight Foundation/Common/Device Class Filters/
Configuration Modifications	This filter identifies configuration modifications on any system or device. This resource is a part of the Configuration Monitoring content.	Filter	ArcSight Foundation/Configuration Monitoring/
Network Configuration Changes	This filter identifies successful configuration change events that match the Network Events filter.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/Network/
VPN Configuration Changes	This filter identifies successful configuration change events that match the VPN Events filter.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/VPN/
Firewall Configuration Changes	This filter identifies successful configuration change events that match the Firewall Events filter.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/Firewall/
Successful Configuration Changes	This filter identifies events with the category behavior of /Modify/Configuration and category outcome of Success.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/
Database Configuration Changes	This filter identifies successful configuration change events that match the Database Events filter.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/Database/

Resource	Description	Type	URI
Firewall Events	This filter retrieves events with the Firewall category device group.	Filter	ArcSight Foundation/Common/Device Class Filters/
Database Events	This filter identifies events with the category object /Host/Application/Database.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/Database/
ArcSight Events	This resource has no description.	Filter	ArcSight System/Event Types
Non-ArcSight Events	This resource has no description.	Filter	ArcSight System/Event Types
Security Application and Device Configuration Changes	This use case provides information about configuration changes on security applications.	Use Case	ArcSight Foundation/Configuration Monitoring/Configuration Changes/
User Configuration Changes	This use case provides information about user management.	Use Case	ArcSight Foundation/Configuration Monitoring/Configuration Changes/
Device Configuration Changes	This use case provides information about the configuration changes on hosts and applications.	Use Case	ArcSight Foundation/Configuration Monitoring/Configuration Changes/

Device Configuration Changes

The Device Configuration Changes resources provide information about configuration changes to hosts and applications.

Resources

The following table lists all the resources in the Device Configuration Changes resource group and any dependant resources.

Table 3-3 Resources that Support the Device Configuration Changes Group

Resource	Description	Type	URI
Monitor Resources			
Host Configuration Modifications	This dashboard shows three data monitors focusing on host configuration change events. The two Top Value Counts (Bucketized) data monitors show charts of the event counts by zone or the most common events. The Last N Events data monitor shows the last 20 events.	Dashboard	ArcSight Foundation/Configuration Monitoring/Operational Summaries/
Host Configuration Modifications - Today	This query viewer displays host related configuration modification events since midnight of the current day.	Query Viewer	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/
Host Configuration Modifications - Yesterday	This query viewer displays host related configuration modification events since midnight of the previous day.	Query Viewer	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/
Zones by Configuration Change Count Past Week	This report provides a summary chart and table to show the zones with the most configuration changes within the past week.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/
Misconfigurations	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Router/
Misconfigurations	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Router/
Host Configuration Modifications Summary	This report provides a summary of the host configuration modification activity seen over the preceding week. Use the Zone parameter to focus the report on a certain zone, and provide a manageable and useful data set. This report is part of the Configuration Monitoring content.	Report	ArcSight Foundation/Configuration Monitoring/Operational Summaries/

Resource	Description	Type	URI
Misconfigurations	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Router/
Assets with Configuration Changes - Last Day	This report provides a listing of the assets that have been modified within the last day and the users that made the modifications. The listing is sorted first by zone, then by asset name.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/
Configuration Changes by User	This report shows recent configuration changes in a table. The table lists all the changes, grouped by user and type, and sorts them chronologically. Use this report to find all the configuration changes made by a specific user.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Common/
Database Errors and Warnings	This report shows recent database errors and warnings in a chart and a table. The chart shows the top 10 errors and warnings. The table lists all the errors and warnings chronologically.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Database/
Host Configuration Modifications by Customer	This report shows the host configuration modifications by customer.	Report	ArcSight Foundation/Configuration Monitoring/Operational Summaries/
Systems With Criticality Ratings by Zone	This report displays a table with the address, device zone name, and names of assets that are modeled under the Criticality asset category.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Critical Systems/
Assets with Configuration Changes - Past Week	This report provides a listing of assets that have been modified within the last week and the user that made the modifications. The listing is sorted first by zone, then by asset name.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/
Host Configuration Modifications by OS	This report shows the host configuration modifications by operating system.	Report	ArcSight Foundation/Configuration Monitoring/Operational Summaries/
Configuration Changes by Type	This report shows recent configuration changes in a table. The table lists all the changes, grouped by type and user, and sorts them chronologically. Use this report to find all the configuration changes of a certain type.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Common/

Resource	Description	Type	URI
VPN Configuration Changes	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/VPN/
Router Configuration Changes	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Router/
Switch Configuration Changes	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Switch/
Current Asset Configurations	This report provides a listing of the assets modeled in and monitored by the ArcSight system, and the current configuration information available to the system regarding those assets. This report provides information on the operating system and the services running on the selected set of hosts. For information about vulnerabilities, see the reports in the Detail/Vulnerabilities section. This report is part of the host-specific Configuration Monitoring content. Note: This report contains data on the number of assets defined by the Row Limit (10,000 by default). Running this report might affect performance, especially if your system contains several hundred thousand assets.	Report	ArcSight Foundation/Configuration Monitoring/Details/
Library - Correlation Resources			
Cisco - IOS Configuration Changed	This rule detects an IOS configuration change. This rule looks for events with a Device Event Class ID of SYS:CONFIG for Cisco Routers. This rule only requires one such event within one minute. After this rule is triggered, the agentSeverity event field is set to medium. This rule is triggered by events generated by CISCO routers.	Rule	ArcSight Foundation/Configuration Monitoring/Detail/Devices/Routers/Cisco/
Library Resources			
Assets with Recent Configuration Modifications	This active list tracks devices and hosts that have had some sort of configuration modification in the past seven days.	Active List	ArcSight Foundation/Configuration Monitoring/

Resource	Description	Type	URI
Criticality	This is a system asset category.	Asset Category	System Asset Categories
Scanned	This is a site asset category.	Asset Category	Site Asset Categories
Open Port	This is a site asset category.	Asset Category	Site Asset Categories
Application	This is a site asset category.	Asset Category	Site Asset Categories
Operating System	This is a site asset category.	Asset Category	Site Asset Categories
Most Common Host Configuration Change Events	This data monitor displays the top ten most common host configuration changes. By default, the data monitor displays a pie chart. This data monitor is a part of the Configuration Monitoring content.	Data Monitor	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Host Configuration Modifications/
Host Configuration Change Event Counts by Zone	This data monitor displays the top ten zones with configuration changes. By default, the data monitor displays a pie chart. This data monitor is a part of the Configuration Monitoring content.	Data Monitor	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Host Configuration Modifications/
Last 20 Host Configuration Modification Events	This data monitor displays the last 20 host configuration events seen by the system. Events are noted by customer, system, and reporting device in addition to the change type information.	Data Monitor	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Host Configuration Modifications/
TargetHost	This variable returns available target information from an event. The format of the information is targetZoneName. | <targetHostName> | <targetAddress>:<targetPort> Information that is not in the event will not show a place-holder. Examples: RFC1918: 192.168.0.0-192.168.255.255 | 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/

Resource	Description	Type	URI
DeviceInfo	This variable returns the device information, including the device vendor, the device product, and the device version, if available within the event. The format is deviceVendor. | <deviceProduct> or <deviceVendor> | <deviceProduct> v. <deviceVersion>	Global Variable	ArcSight Foundation/Variables Library/
VPN Events	This filter identifies events with the category device group of VPN.	Filter	ArcSight Foundation/Common/Device Class Filters/
Configuration Modifications	This filter identifies configuration modifications on any system or device. This resource is a part of the Configuration Monitoring content.	Filter	ArcSight Foundation/Configuration Monitoring/
Target Address is NULL	This filter is designed for conditional expression variables. The filter identifies events where the target address is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Zone AND Host are NULL but Address is NOT NULL	This filter identifies events in which either the target zone or target address field is NULL, but not both.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Virtual Private Network	This resource has no description.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/VPN/
Target Host Name is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Target Host Name is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Information is NULL	This filter identifies events in which the target zone, target host name, and target address fields are NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
All Events	Filter that matches all events.	Filter	ArcSight System/Core
ArcSight Events	This resource has no description.	Filter	ArcSight System/Event Types
Target Port is NULL	This filter identifies events in which the target port field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Device Version is NULL	This filter identifies events in which the device product field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Device/

Resource	Description	Type	URI
All Device Information is NULL	This filter identifies events in which there is no device information, meaning that the device vendor, device product, and device version fields are all NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Device/
Device Vendor OR Product is NULL	This filter identifies events in which the device vendor or device product field is NULL, but not both.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Device/
Router	This resource has no description.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/Router/
Switch	This resource has no description.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/Switch/
Host Configuration Modifications	This filter provides a more focused subset of configuration modification events for use when monitoring or reporting on host-specific configuration changes. This filter is a part of the host-specific Configuration Monitoring content.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/
Target Zone OR Host is NULL	This filter identifies events in which either the target zone or target host name field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Device Vendor AND Product are NULL	This filter identifies events in which the device vendor and device product fields are NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Device/
Target Zone AND Host are NULL	This filter identifies events in which the target zone and target host name fields are NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Zone is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Target Zone is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Non-ArcSight Events	This resource has no description.	Filter	ArcSight System/Event Types
Configuration Changes by User	This report displays anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes made by a specific user.	Focused Report	ArcSight Foundation/Common/Anti-Virus/

Resource	Description	Type	URI
Configuration Changes by Type	This report displays the configuration change name, the user making the change, device information, and the time of the change for anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes of a certain type.	Focused Report	ArcSight Foundation/Common/Anti-Virus/
Host Configuration Modifications	This query retrieves host related configuration modification events since midnight of the current day.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/
Misconfigurations	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Router/
Host Configuration Modifications by OS	This query retrieves host configuration modification data (restricted by the Host Configuration Modifications filter).	Query	ArcSight Foundation/Configuration Monitoring/Operational Summaries/
Assets with Configuration Modifications-Last Day	This query retrieves a list of assets that have had configuration changes in the last day. The data is retrieved from the Assets with Recent Configuration Modifications active list.	Query	ArcSight Foundation/Configuration Monitoring/Details/
Router Configuration Changes	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Router/
Systems With Criticality Ratings by Zone	This query returns the address, device zone name, and names of assets that are modeled under the Criticality asset category.	Query	ArcSight Foundation/Configuration Monitoring/Details/Critical Systems/
Configuration Changes by Zone Last Week Trend Query	This query retrieves information about the total number of configuration changes that occurred in your zones over the past seven days. The events are counted and grouped by day and month for ease of use in a chart or summary table.	Query	ArcSight Foundation/Configuration Monitoring/Details/

Resource	Description	Type	URI
Host Configuration Modifications on Trend	This query retrieves data from the Host Configuration Modifications trend to provide a summary of the host configuration modification activity. This query is a part of the Configuration Monitoring content.	Query	ArcSight Foundation/Configuration Monitoring/Operational Summaries/
VPN Configuration Changes	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/VPN/
Database Errors and Warnings (Chart)	This query returns the count of database errors and warnings by event name.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Database Errors and Warnings/
Switch Configuration Changes	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Switch/
Assets with Configuration Modifications-Last 7 Days	This query retrieves a list of assets have had configuration changes within the last 7 days. This query checks the Assets with Recent Configuration Modifications active list.	Query	ArcSight Foundation/Configuration Monitoring/Details/
Misconfigurations	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Router/
Assets with Recent Configuration Modifications by Vendor and Product	This query collects information about a day's worth of configuration changes to your various assets. The data retrieved includes information about the asset affected, the asset causing the change (if any), and the vendor and product information about the asset that was changed.	Query	ArcSight Foundation/Configuration Monitoring/Details/
Configuration Changes	This query returns all the successful configuration changes made to devices. The query returns the name, the user, the device, and the time the change was made.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/

Resource	Description	Type	URI
Host Configuration Modifications Summary	This query retrieves data providing a summary of the host configuration modification activity for the Host Configuration Modifications trend. This query is a part of the Configuration Monitoring content.	Query	ArcSight Foundation/Configuration Monitoring/Operational Summaries/
Misconfigurations	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Router/
Current Asset Configurations	This query provides a listing of the assets modeled in and monitored by the ArcSight system and the current configuration information available to the system regarding those assets. It provides information on the operating system and services running on the selected set of hosts. Note: This query returns data up to the Row Limit (10,000 by default) assets. Running this query night affect performance.	Query	ArcSight Foundation/Configuration Monitoring/Details/
Host Configuration Modifications by Customer	This query returns host configuration modification data (restricted by the Host Configuration Modifications filter).	Query	ArcSight Foundation/Configuration Monitoring/Operational Summaries/
Database Errors and Warnings	This query retrieves all the database error and warning events. The query returns the time, event name, result, user name, and category significance.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Database Errors and Warnings/
Host Configuration Modifications	This trend provides a summary of the host configuration modification activity.	Trend	ArcSight Foundation/Configuration Monitoring/Asset Configuration Change Tracking/
Assets with Recent Configuration Modifications (Daily)	This trend retrieves changes to assets within the last day and stores information about the change itself as well as who made the change.	Trend	ArcSight Foundation/Configuration Monitoring/Asset Configuration Change Tracking/

Hosts and Applications Overview

The Hosts and Applications Overview resources provide an overview of the configuration of systems with common applications, such as email servers and databases.

Configuration

The Hosts and Applications Overview resource group requires the following configuration for your environment:

- Categorize the the assets in your environment in the following groups (unless the assets were categorized automatically by vulnerability scanners):
  - Site Asset Categories/Business Impact Analysis/Business Role
  - System Asset Categories/Criticality
  - Site Asset Categories/Business Impact Analysis/Data Role
  - Site Asset Categories/Operating System
  - Site Asset Categories/Application/Type/Email
  - Site Asset Categories/Application/Type/Web Server

Resources

The following table lists all the resources in the Hosts and Applications Overview resource group and any dependant resources.

Table 3-4 Resources that Support the Hosts and Applications Overview Group

Resource	Description	Type	URI
Monitor Resources			
Database Errors	This dashboard shows the most recent and the top errors affecting database applications on the network.	Dashboard	ArcSight Foundation/Configuration Monitoring/Operational Summaries/
Host Problems Overview	This dashboard shows several data monitors that focus on host problem events. The two Top Value Counts (Bucketized) data monitors show charts of the event counts by zone or the most common events. The Last N Events data monitor shows the last 20 events.	Dashboard	ArcSight Foundation/Configuration Monitoring/Operational Summaries/
Configuration Changes by User	This report shows recent configuration changes in a table. The table lists all the changes, grouped by user and type, and sorts them chronologically. Use this report to find all the configuration changes made by a specific user.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Common/

Resource	Description	Type	URI
Database Errors and Warnings	This report shows recent database errors and warnings in a chart and a table. The chart shows the top 10 errors and warnings. The table lists all the errors and warnings chronologically.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Database/
All Revenue Generating Assets	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Inventory/Roles/
Mail Servers	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Inventory/Roles/
Web Servers	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Inventory/Roles/
Configuration Changes by Type	This report shows recent configuration changes in a table. The table lists all the changes, grouped by type and user, and sorts them chronologically. Use this report to find all the configuration changes of a certain type.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Common/
Host Summary by Business Role	This report provides a summary pie chart showing the breakdown of assets by business role. This chart and others are combined to produce an overview of the asset configurations. This report is a part of the Configuration Monitoring content.	Report	ArcSight Foundation/Configuration Monitoring/Executive Summaries/Overall Host Configuration/
Host Configuration Events By Zone	This report provides a summary pie chart showing the breakdown of host configuration events by zone. This chart and others are combined to produce an overview of the asset configurations. This report is a part of the Configuration Monitoring content.	Report	ArcSight Foundation/Configuration Monitoring/Executive Summaries/Overall Host Configuration/
Host Summary by Criticality	This report provides a summary pie chart showing the breakdown of assets by criticality. This chart and others are combined to produce an overview of the asset configurations. This report is a part of the Configuration Monitoring content.	Report	ArcSight Foundation/Configuration Monitoring/Executive Summaries/Overall Host Configuration/

Resource	Description	Type	URI
Host Summary by Operating System	This report provides a summary pie chart showing the breakdown of assets by operating system. This chart and others are combined to produce an overview of the asset configurations. This report is a part of the Configuration Monitoring content.	Report	ArcSight Foundation/Configuration Monitoring/Executive Summaries/Overall Host Configuration/
Assets with Applications	This report provides a listing of all assets that have been scanned for applications or that have been categorized manually with applications. This report is a part of the Configuration Monitoring content.	Report	ArcSight Foundation/Configuration Monitoring/Details/Inventory/
Host Summary by Data Role	This report provides a summary pie chart showing the breakdown of assets by data role. This chart and others are combined to produce an overview of the asset configurations. This report is a part of the Configuration Monitoring content.	Report	ArcSight Foundation/Configuration Monitoring/Executive Summaries/Overall Host Configuration/
Library Resources			
Email	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type
Data Role	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis
Criticality	This is a system asset category.	Asset Category	System Asset Categories
Business Role	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis
Application	This is a site asset category.	Asset Category	Site Asset Categories
Web Server	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type
Operating System	This is a site asset category.	Asset Category	Site Asset Categories
Revenue Generation	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis/Business Role
Last 10 Database Errors	This data monitor displays the most recent database error events.	Data Monitor	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Database Errors/

Resource	Description	Type	URI
Last 20 Host Problems	This data monitor shows the last 20 host issues noted by ArcSight. This data monitor is used in the Host Problems Overview data monitor and these resources are part of the Configuration Monitoring content.	Data Monitor	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Host Problems Overview/
Top 10 Database Errors	This data monitor shows the top ten systems with events matching the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Failure, and the Category Behavior is /Found/Vulnerable).	Data Monitor	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Database Errors/
Host Problem Event Counts by Zone	This data monitor shows host-specific problems noted by ArcSight, by Zone. By default this data monitor displays a pie chart of the top ten zones by problem event volume. This data monitor is a part of the Configuration Monitoring content.	Data Monitor	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Host Problems Overview/
Most Common Host Problem Events	This data monitor shows the top ten most common problems seen on your monitored hosts. This data monitor is a part of the Host Problems Overview dashboard and is a part of the Configuration Monitoring content.	Data Monitor	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Host Problems Overview/
TargetHost	This variable returns available target information from an event. The format of the information is targetZoneName. | <targetHostName> | <targetAddress>:<targetPort> Information that is not in the event will not show a place-holder. Examples: RFC1918: 192.168.0.0-192.168.255.255 | 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/
DeviceInfo	This variable returns the device information, including the device vendor, the device product, and the device version, if available within the event. The format is deviceVendor. | <deviceProduct> or <deviceVendor> | <deviceProduct> v. <deviceVersion>	Global Variable	ArcSight Foundation/Variables Library/

Resource	Description	Type	URI
Configuration Modifications	This filter identifies configuration modifications on any system or device. This resource is a part of the Configuration Monitoring content.	Filter	ArcSight Foundation/Configuration Monitoring/
Host Problems	This filter identifies host-related problems and errors. This filter is part of the Configuration Monitoring content.	Filter	ArcSight Foundation/Configuration Monitoring/Operational Summaries/
Target Address is NULL	This filter is designed for conditional expression variables. The filter identifies events where the target address is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Zone AND Host are NULL but Address is NOT NULL	This filter identifies events in which either the target zone or target address field is NULL, but not both.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Host Name is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Target Host Name is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Information is NULL	This filter identifies events in which the target zone, target host name, and target address fields are NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Database Errors	This filter identifies events with the category device group of Application, category object of /Host/Application/Database, and a category significance of /Informational/Warning or /Informational/Error.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/Database/
All Events	Filter that matches all events.	Filter	ArcSight System/Core
Database Events	This filter identifies events with the category object /Host/Application/Database.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/Database/
ArcSight Events	This resource has no description.	Filter	ArcSight System/Event Types
Target Port is NULL	This filter identifies events in which the target port field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Device Version is NULL	This filter identifies events in which the device product field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Device/

Resource	Description	Type	URI
All Device Information is NULL	This filter identifies events in which there is no device information, meaning that the device vendor, device product, and device version fields are all NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Device/
Device Vendor OR Product is NULL	This filter identifies events in which the device vendor or device product field is NULL, but not both.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Device/
Host Configuration Modifications	This filter provides a more focused subset of configuration modification events for use when monitoring or reporting on host-specific configuration changes. This filter is a part of the host-specific Configuration Monitoring content.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/
Target Zone OR Host is NULL	This filter identifies events in which either the target zone or target host name field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Device Vendor AND Product are NULL	This filter identifies events in which the device vendor and device product fields are NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Device/
Target Zone AND Host are NULL	This filter identifies events in which the target zone and target host name fields are NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Zone is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Target Zone is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Non-ArcSight Events	This resource has no description.	Filter	ArcSight System/Event Types
Configuration Changes by User	This report displays anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes made by a specific user.	Focused Report	ArcSight Foundation/Common/Anti-Virus/
Configuration Changes by Type	This report displays the configuration change name, the user making the change, device information, and the time of the change for anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes of a certain type.	Focused Report	ArcSight Foundation/Common/Anti-Virus/

Resource	Description	Type	URI
Host Summary by Business Role	This query returns a breakdown of assets by Business Role. This query is a part of the Configuration Monitoring content.	Query	ArcSight Foundation/Configuration Monitoring/Executive Summaries/Overall Host Configuration/
Host Summary by Data Role	This query returns a breakdown of assets by Data Role. This query is part of the Configuration Monitoring content.	Query	ArcSight Foundation/Configuration Monitoring/Executive Summaries/Overall Host Configuration/
All Revenue Generating Assets	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Inventory/Roles/
Web Servers	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Inventory/Roles/
Database Errors and Warnings (Chart)	This query returns the count of database errors and warnings by event name.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Database Errors and Warnings/
Host Summary by Criticality	This query returns a breakdown of assets by Criticality. This query is part of the Configuration Monitoring content.	Query	ArcSight Foundation/Configuration Monitoring/Executive Summaries/Overall Host Configuration/
Assets with Applications	This report shows all Assets that have been scanned for applications or that have been manually categorized with Applications. This report is part of the Configuration Monitoring content.	Query	ArcSight Foundation/Configuration Monitoring/Details/Inventory/
Host Summary by Operating System	This query returns a breakdown of assets by operating system. This query is part of the Configuration Monitoring content.	Query	ArcSight Foundation/Configuration Monitoring/Executive Summaries/Overall Host Configuration/
Configuration Changes	This query returns all the successful configuration changes made to devices. The query returns the name, the user, the device, and the time the change was made.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/
Host Configuration Modifications Summary	This query retrieves data providing a summary of the host configuration modification activity for the Host Configuration Modifications trend. This query is a part of the Configuration Monitoring content.	Query	ArcSight Foundation/Configuration Monitoring/Operational Summaries/

Resource	Description	Type	URI
Mail Servers	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Inventory/Roles/
Database Errors and Warnings	This query retrieves all the database error and warning events. The query returns the time, event name, result, user name, and category significance.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Database Errors and Warnings/
Host Configuration Events By Zone	This query returns a breakdown of host configuration events by zone from the Host Configuration Modifications trend.	Query	ArcSight Foundation/Configuration Monitoring/Executive Summaries/Overall Host Configuration/
Host Configuration Modifications	This trend provides a summary of the host configuration modification activity.	Trend	ArcSight Foundation/Configuration Monitoring/Asset Configuration Change Tracking/

Security Application and Device Configuration Changes

The Security Application and Device Configuration Changes resources provide information about configuration changes to security applications.

Devices

The following device types can supply events that apply to the Security Application and Device Configuration Changes resource group:

- Anti-Virus
- Firewalls
- Intrusion Detection Systems

Resources

The following table lists all the resources in the Security Application and Device Configuration Changes resource group and any dependant resources.

Table 3-5 Resources that Support the Security Application and Device Configuration Changes Group

Resource	Description	Type	URI
Monitor Resources			
Firewall Configuration Changes	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Firewall/
Update Summary - Regulated Systems	This report displays the target zone name, target host name, target address, device vendor, device product, category outcome, and the sum of the aggregated event count from yesterday's events on assets categorized as having a regulation requirement.	Report	ArcSight Foundation/Common/Anti-Virus/
Update Overview (MSSP)	This report displays the customer, time, target zone name, target host name, target address, device vendor, device product, category outcome, and the sum of the aggregated event count of all events related to virus update information files for yesterday.	Report	ArcSight Foundation/Common/Anti-Virus/
Failed Anti-Virus Updates	This report displays a table with the anti-virus vendor and product name as well as the hostname, zone and IP address of the host on which the update failed. The time (EndTime) at which the update failed is also displayed. This report runs against events that occurred yesterday.	Report	ArcSight Foundation/Common/Anti-Virus/

Resource	Description	Type	URI
Failed Anti-Virus Updates (MSSP)	This report displays the customer, time, target zone name, target host name, target address, and device product of all events in the past 24 hours that have failed to update virus information files.	Report	ArcSight Foundation/Common/Anti-Virus/
Firewall Misconfigurations	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Firewall/
Failed Anti-Virus Updates - Regulated Systems	This report displays the device vendor, device product, target zone name, target host name, target address, and minute(EndTime) from events that match the AV - Failed Updates filter and target assets that are categorized in one of the regulated asset categories for yesterday.	Report	ArcSight Foundation/Common/Anti-Virus/
Failed Anti-Virus Updates - Regulated Systems (MSSP)	This report displays the customer, device vendor, device product target zone name, target host name, target address, and minute(EndTime) from events that match the AV - Failed Updates filter and target assets that are categorized in one of the regulated asset categories for yesterday.	Report	ArcSight Foundation/Common/Anti-Virus/
Update Summary	This report displays a summary of the results of anti-virus update activity by zones since yesterday.	Report	ArcSight Foundation/Common/Anti-Virus/
Errors Detected in Anti-Virus Deployment	This report displays the hosts reporting the most anti-virus errors for the previous day and includes the anti-virus product, host details, error information, and the number of errors.	Report	ArcSight Foundation/Common/Anti-Virus/
HIDS Misconfigurations	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/IDS/
Configuration Changes by User	This report shows recent configuration changes in a table. The table lists all the changes, grouped by user and type, and sorts them chronologically. Use this report to find all the configuration changes made by a specific user.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Common/

Resource	Description	Type	URI
Update Overview - Regulated Systems (MSSP)	This report displays the customer, target zone name, target host name, target address, device vendor, device product, category outcome, and the sum of the aggregated event count from yesterday's events on assets categorized as having a regulation requirement.	Report	ArcSight Foundation/Common/Anti-Virus/
Top Infected Systems	This report displays summaries of the systems reporting the most infections in the previous day.	Report	ArcSight Foundation/Common/Anti-Virus/
Configuration Changes by Type	This report shows recent configuration changes in a table. The table lists all the changes, grouped by type and user, and sorts them chronologically. Use this report to find all the configuration changes of a certain type.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Common/
NIDS Misconfigurations	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/IDS/
Library Resources			
Compliance Requirement	This is a site asset category.	Asset Category	Site Asset Categories
Network Events	This filter identifies events with the category object starts with Network or the category device group starts with Network Equipment.	Filter	ArcSight Foundation/Common/Device Class Filters/
Configuration Modifications	This filter identifies configuration modifications on any system or device. This resource is a part of the Configuration Monitoring content.	Filter	ArcSight Foundation/Configuration Monitoring/
Update Events	This filter identifies events related to anti-virus product data file updates.	Filter	ArcSight Foundation/Common/Anti-Virus/
All Events	Filter that matches all events.	Filter	ArcSight System/Core
Host IDS	This resource has no description.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/IDS/
ArcSight Events	This resource has no description.	Filter	ArcSight System/Event Types
Anti-Virus Events	This filter identifies events with the category device group of /IDS/Host/Antivirus.	Filter	ArcSight Foundation/Common/Anti-Virus/

Resource	Description	Type	URI
Network IDS	This resource has no description.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/IDS/
Firewall	This resource has no description.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/Firewall/
Identity Management Events	This filter identifies events in which the Category Device Group starts with Identity Management.	Filter	ArcSight Foundation/Common/Device Class Filters/
AV - Found Infected	This filter identifies all events where the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is Failure and the Category Behavior is /Found/Vulnerable.	Filter	ArcSight Foundation/Common/Anti-Virus/
Firewall Events	This filter retrieves events with the Firewall category device group.	Filter	ArcSight Foundation/Common/Device Class Filters/
AV - Failed Updates	This filter identifies all anti-virus update events (based on the Update Events filter), where the Category Outcome is Failure.	Filter	ArcSight Foundation/Common/Anti-Virus/
Non-ArcSight Events	This resource has no description.	Filter	ArcSight System/Event Types
Configuration Changes by User	This report displays anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes made by a specific user.	Focused Report	ArcSight Foundation/Common/Anti-Virus/
Configuration Changes by Type	This report displays the configuration change name, the user making the change, device information, and the time of the change for anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes of a certain type.	Focused Report	ArcSight Foundation/Common/Anti-Virus/
Configuration Changes by User	This report displays anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes made by a specific user.	Focused Report	ArcSight Foundation/Common/Anti-Virus/

Resource	Description	Type	URI
Configuration Changes by Type	This report displays the configuration change name, the user making the change, device information, and the time of the change for anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes of a certain type.	Focused Report	ArcSight Foundation/Common/Anti-Virus/
Configuration Changes by Type	This report displays the configuration change name, the user making the change, device information, and the time of the change for anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes of a certain type.	Focused Report	ArcSight Foundation/Common/Anti-Virus/
Configuration Changes by Type	This report displays the configuration change name, the user making the change, device information, and the time of the change for anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes of a certain type.	Focused Report	ArcSight Foundation/Common/Anti-Virus/
Configuration Changes by User	This report displays anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes made by a specific user.	Focused Report	ArcSight Foundation/Common/Anti-Virus/
Configuration Changes by User	This report displays anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes made by a specific user.	Focused Report	ArcSight Foundation/Common/Anti-Virus/
Failed Anti-Virus Updates	This query identifies the device vendor, device product target zone name, target host name, and target address and time (EndTime) from events that match the AV - Failed Updates filter.	Query	ArcSight Foundation/Common/Anti-Virus/
Update Overview (MSSP)	This query returns the customer, time, target zone name, target host name, target address, device vendor, device product, category outcome, and the sum of the aggregated event count of all events related to virus update information files.	Query	ArcSight Foundation/Common/Anti-Virus/

Resource	Description	Type	URI
Failed Anti-Virus Updates Chart - Regulated Systems	This query returns the target zone name and the sum of the aggregated event count from events that match the AV - Failed Updates filter.	Query	ArcSight Foundation/Common/Anti-Virus/
NIDS Misconfigurations	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/IDS/
Failed Anti-Virus Updates - Regulated Systems	This query returns the device vendor, device product target zone name, target host name, target address, and minute(EndTime) from events that match the AV - Failed Updates filter and target assets that are categorized in one of the regulated asset categories.	Query	ArcSight Foundation/Common/Anti-Virus/
Top Zones with Anti-Virus Errors	This query identifies data from events where the Category Device Group is /IDS/Host/Antivirus, the Category Object starts with /Host/Application, the Category Outcome is not Success and the Category Significance starts with Informational. The query returns the zone and the number of times the error occurred.	Query	ArcSight Foundation/Common/Anti-Virus/Errors/
Update Summary - Regulated Systems	This query returns the target zone name, target host name, target address, device vendor, device product, category outcome, and the sum of the aggregated event count from events that have the category behavior of /Modify/Content, the category object of /Host/Application, the category device group of /IDS/Host/Antivirus, and target assets that are categorized in one of the regulated asset categories.	Query	ArcSight Foundation/Common/Anti-Virus/
Firewall Configuration Changes	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Firewall/
Failed Anti-Virus Updates - Regulated Systems (MSSP)	This query returns the customer, time, target zone name, target host name, target address, and device product for all events in the past 24 hours that have failed to update virus information files for any asset categorized with a regulation compliance requirement.	Query	ArcSight Foundation/Common/Anti-Virus/

Resource	Description	Type	URI
Configuration Changes	This query returns all the successful configuration changes made to devices. The query returns the name, the user, the device, and the time the change was made.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/
Update Summary	This query identifies the target zone name, target host name, target address, device vendor, device product, category outcome, and the sum of the aggregated event count from events that match the Update Events filter.	Query	ArcSight Foundation/Common/Anti-Virus/
Top Infected Systems	This query identifies data matching the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is Failure and the Category Behavior is /Found/Vulnerable), and returns the host zone and a count of the infections per zone.	Query	ArcSight Foundation/Common/Anti-Virus/Top Infected Systems/
Firewall Misconfigurations	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Firewall/
Infected Systems	This query identifies data matching the filter the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is Failure and the Category Behavior is /Found/Vulnerable), and returns the host information and a count of the infections per host.	Query	ArcSight Foundation/Common/Anti-Virus/Top Infected Systems/
Failed Anti-Virus Updates (MSSP)	This query returns the customer, time, target zone name, target host Name, target address, and device product for all events in the past 24 hours that have failed to update virus information files.	Query	ArcSight Foundation/Common/Anti-Virus/
Update Overview Chart (MSSP)	This query returns the customer name, target zone name, category outcome, and the sum of the aggregated event count from events that match the Update Events filter.	Query	ArcSight Foundation/Common/Anti-Virus/

Resource	Description	Type	URI
Anti-Virus Errors	This query identifies data from events where the Category Device Group is /IDS/Host/Antivirus, the Category Object starts with /Host/Application, the Category Outcome is not Success and the Category Significance starts with Informational. The query returns the priority, vendor information, host information, error name, and the number of times the error occurred.	Query	ArcSight Foundation/Common/Anti-Virus/Errors/
Failed Anti-Virus Updates Chart (MSSP)	This query returns the customer name and the sum of the aggregated event count from events that match the AV - Failed Updates filter.	Query	ArcSight Foundation/Common/Anti-Virus/
HIDS Misconfigurations	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/IDS/
Update Summary Chart - Regulated Systems	This query returns the target zone name, category outcome, and the sum of the aggregated event count from events that match the Update Events filter.	Query	ArcSight Foundation/Common/Anti-Virus/
Failed Anti-Virus Updates Chart - Regulated Systems (MSSP)	This query returns the customer name and the sum of the aggregated event count from events that match the AV - Failed Updates filter.	Query	ArcSight Foundation/Common/Anti-Virus/
Update Overview Chart - Regulated Systems (MSSP)	This query returns the customer name, target zone name, category outcome, and the sum of the aggregated event count from events that match the Update Events filter.	Query	ArcSight Foundation/Common/Anti-Virus/
Failed Anti-Virus Updates Chart	This query identifies the target zone name and the sum of the aggregated event count from events that match the AV - Failed Updates filter.	Query	ArcSight Foundation/Common/Anti-Virus/

Resource	Description	Type	URI
Update Overview - Regulated Systems (MSSP)	This query returns the customer, target zone name, target host name, target address, device vendor, device product, category outcome, and the sum of the aggregated event count from events that have the category behavior of /Modify/Content, the category object of /Host/Application, the category device group of /IDS/Host/Antivirus, and target assets that are categorized in one of the regulated asset categories.	Query	ArcSight Foundation/Common/Anti-Virus/
Update Summary Chart	This query identifies the target zone name, category outcome, and the sum of the aggregated event count from events that match the Update Events filter.	Query	ArcSight Foundation/Common/Anti-Virus/
Top Anti-Virus Errors	This query identifies data from events where the Category Device Group is /IDS/Host/Antivirus, the Category Object starts with /Host/Application, the Category Outcome is not Success, and the Category Significance starts with Informational. The query returns the error name and the number of times the error occurred.	Query	ArcSight Foundation/Common/Anti-Virus/Errors/

User Configuration Changes

The User Configuration Changes resources provide information about user configuration by identifying and monitoring user accounts and the hosts/addresses associated with them. This ties a user to certain IP addresses, MAC addresses, host-names, zones, and so on. The reports cover user account additions, modifications to those accounts, and account removal.

Monitoring user account activity can show changes to user privileges and roles, as well as user account creations or deletions. User account privileges should be associated with adding or removing access to network resources that the user no longer requires, and should be done by an administrator with the authority to change those privileges. Random account modifications by unexpected sources are indications of a security concern. Random creation or deletions of accounts are also suspect.

Resources

The following table lists all the resources in the User Configuration Changes resource group and any dependant resources.

Table 3-6 Resources that Support the User Configuration Changes Group

Resource	Description	Type	URI
Monitor Resources			
User Configuration Modifications - Today	This query viewer shows configuration modification events related to users for the current day.	Query Viewer	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/
User Configuration Modifications - Yesterday	This query viewer shows configuration modification events related to users for the previous day.	Query Viewer	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/
Password Changes by Zone	This report provides a listing of the password changes for the past 30 days.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Modification/Password/
Configuration Changes per User by Zone Last Week	This report provides a view of users that have made configuration changes over the past week (sorted by zone) and the number of changes each user made.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/
Accounts Deleted by Host	This report provides a listing of user deletions over the previous 30 days, ordered by customer, zone, and system. This report is a part of the Configuration Monitoring content.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Deletion/

Resource	Description	Type	URI
Password Changes	This report shows password changes for the previous day and groups the password changes by user sorted chronologically.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Modification/Password/
User Removals - Last 30 Days	This report provides a summary of the user removals over the last 30 days. Focus this report on a certain zone (use the FilterBy parameter) to provide a manageable and useful data set.	Report	ArcSight Foundation/Configuration Monitoring/Operational Summaries/
Most Common Account Login Failures by Attacker User (Yesterday)	This report displays the category object, attacker address, attacker asset name, attacker NT domain, attacker user ID, attacker user name, attacker zone name, and the sum of the aggregated event count.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Asset Tracking/
By User Account - Accounts Deleted	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Deletion/
By User Account - Accounts Created	This report generates a table of all user accounts created in the last day.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/
VPN User Account Creation	This report shows all VPN user account creations for the past 30 days. The fields Target Zone Name, Target User ID, and Attacker User Name are renamed Zone, New Account, and Creator in the report.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/
Local Windows User Creation - Disallowed Systems	This report displays the customer, attacker user name, target zone name, target address, target asset name, target user ID, target user name, the day and the sum of the aggregated event count for local Windows user creations on disallowed systems from the Local Windows User Creation - Disallowed Systems trend. Note: The Local Windows User Creation - Disallowed Systems trend is not enabled by default.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/
Configuration Changes per User Last Week	This report provides a view of users that have made configuration changes over the past week, sorted by the number of changes each user made.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/

Resource	Description	Type	URI
User Account Modifications	This report shows an overview of the user account modifications for the past 30 days.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Modification/
AAA User Account Creation	This report shows all AAA user account creation for the past 30 days.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/
User Account Creation	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/
AAA User Account Deletions - Last 30 Days	This report displays a table of the AAA user accounts that have been deleted over the past 30 days, based on data collected in the AAA User Account Deletions trend. Note: The AAA User Account Deletions Trend is not enabled by default.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Deletion/
User Administration	This report shows a summary of user and user group creation, modification, and deletion.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/
Account Creation by Host - Last Week	This report provides a listing of the account creation events seen over the past week on your monitored assets. Note: This report detects host-local user account creations, not authentication service account creations; therefore, the report does not pick up user additions in the Active Directory. The Account Creation by Host trend is not enabled by default. This report is a part of the Configuration Monitoring content.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/
Password Changes by System	This report provides a listing of the password changes for the past 30 days.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Modification/Password/
Password Changes by User	This report provides a listing of the password changes for the past 30 days.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Modification/Password/
Library - Correlation Resources			

Resource	Description	Type	URI
Local Windows User Creation - Allowed Host	This rule detects the creation of a local user on a Windows system. If this rule triggers, the system on which the user has been created is present in the Local User Allowed Systems active list. Treat this alert as normal activity. This rule is a part of the Configuration Monitoring content.	Rule	ArcSight Foundation/Configuration Monitoring/Detail/
Local Windows User Creation - Disallowed Host	This rule detects the creation of a local user on a Windows system. If this rule triggers, the system on which the user has been created is not present in the Local User Allowed Systems active list. Treat this as suspicious or hostile activity to be investigated immediately. This rule is a part of the Configuration Monitoring content.	Rule	ArcSight Foundation/Configuration Monitoring/Detail/
Library Resources			
Local User Allowed Systems	This active list is used to specify systems on which local user creation activity is allowed. This active list is part of the Configuration Monitoring content.	Active List	ArcSight Foundation/Configuration Monitoring/
Business Role	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis
Microsoft	This is a site asset category.	Asset Category	Site Asset Categories/Operating System
VPN Events	This filter identifies events with the category device group of VPN.	Filter	ArcSight Foundation/Common/Device Class Filters/
User Account Modifications	This filter identifies user account modification events. The filter is a part of the Configuration Monitoring content.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/User/
Configuration Modifications	This filter identifies configuration modifications on any system or device. This resource is a part of the Configuration Monitoring content.	Filter	ArcSight Foundation/Configuration Monitoring/
User Account Login Attempts	This filter uses ArcSight categories to choose events that indicate user login attempts. These might be successful or failures.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/User/Access Tracking/

Resource	Description	Type	URI
Failed User Account Login Attempts	This filter uses the ArcSight event categories to identify failed user account login attempts.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/User/Access Tracking/
Successful Password Changes	This resource has no description.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/User/
AAA User Account Creations	This filter identifies user account creation activity on AAA systems. This filter is part of the Configuration Monitoring content.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/AAA/
User Account Creations	This filter identifies user account addition events. The filter is a part of the Configuration Monitoring content.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/User/
All Events	Filter that matches all events.	Filter	ArcSight System/Core
Database Events	This filter identifies events with the category object /Host/Application/Database.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/Database/
ArcSight Events	This resource has no description.	Filter	ArcSight System/Event Types
VPN User Account Creations	This filter identifies events showing VPN user account creation information. The filter uses the VPN User Configuration Activity filter and looks for the /Authentication/Add category behavior.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/VPN/
Identity Management Events	This filter identifies events in which the Category Device Group starts with Identity Management.	Filter	ArcSight Foundation/Common/Device Class Filters/
Operating System Events	This filter identifies events with the category device group of Operating System.	Filter	ArcSight Foundation/Common/Device Class Filters/
AAA User Configuration Activity	This filter identifies user configuration activity on AAA systems. The filter is a part of the Configuration Monitoring content.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/AAA/
VPN User Configuration Activity	This filter identifies user configuration activity on VPN systems. This filter is a part of the Configuration Monitoring content.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/VPN/
AAA User Account Deletions	This filter identifies user account deletion activity on AAA systems. This filter is part of the Configuration Monitoring content.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/AAA/

Resource	Description	Type	URI
Non-ArcSight Events	This resource has no description.	Filter	ArcSight System/Event Types
User Account Deletions	This filter identifies user account deletion events. This filter is a part of the Configuration Monitoring content.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/User/
User Account Modifications - Last 30 Days	This resource has no description.	Focused Report	ArcSight Foundation/Configuration Monitoring/SANS Top 5 Reports/3 - Unauthorized Changes to Users, Groups and Services/
Password Changes	This report shows database password changes for the previous day and groups the password changes by user, sorted chronologically.	Focused Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Database/
Password Changes	This report shows database password changes for the previous day and groups the password changes by user, sorted chronologically.	Focused Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Database/
Password Changes - Last 30 Days	This resource has no description.	Focused Report	ArcSight Foundation/Configuration Monitoring/SANS Top 5 Reports/3 - Unauthorized Changes to Users, Groups and Services/
Password Changes	This report shows database password changes for the previous day and groups the password changes by user, sorted chronologically.	Focused Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Database/
User Account Deletions - Last 30 Days	This resource has no description.	Focused Report	ArcSight Foundation/Configuration Monitoring/SANS Top 5 Reports/3 - Unauthorized Changes to Users, Groups and Services/
User Account Creations - Last 30 Days	This resource has no description.	Focused Report	ArcSight Foundation/Configuration Monitoring/SANS Top 5 Reports/3 - Unauthorized Changes to Users, Groups and Services/
Password Changes	This report shows database password changes for the previous day and groups the password changes by user, sorted chronologically.	Focused Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Database/

Resource	Description	Type	URI
Local Windows User Creation - Disallowed Systems - on Trend	This query returns the customer, attacker user name, target zone name, target address, target asset name, target user ID, target user name, the day and the sum of the aggregated event count for local Windows user creations on disallowed systems from the Local Windows User Creation - Disallowed Systems trend. Note: The Local Windows User Creation - Disallowed Systems trend is not enabled by default.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/
VPN User Account Creation Trend	This query on events restricted by the VPN User Account Creations filter retrieves the customer, attacker user name, attacker zone, target address, target asset name, target host name, target Nt domain, target user ID, target user name, and target zone for the VPN User Account Creation trend.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/
AAA User Account Deletions Trend	This query returns the customer, attacker user name, attacker zone, target address, target asset name, target host name, target Nt domain, target user ID, and target user name for events matching the AAA User Account Deletions filter.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Deletion/
Trend on AAA User Account Creation	This query on the AAA User Account Creation trend retrieves the customer name, attacker user name, attacker zone name, target address, target asset name, target host name, target Nt domain, target user ID, target user name, and target zone name for the AAA User Account Creation report.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/
User Removals	This query retrieves user account deletion data (restricted by the User Account Deletions filter).	Query	ArcSight Foundation/Configuration Monitoring/Operational Summaries/
AAA User Account Creation Trend	This query retrieves events passed by the AAA User Account Creations filter, returning the customer, attacker user name, attacker zone, target address, target asset name, target host name, target Nt domain, target user ID, target user name, and target zone for the AAA User Account Creation trend.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/

Resource	Description	Type	URI
User Removals on Trend	This query retrieves the user account deletion data (restricted by the User Account Deletions filter), grouped by customer.	Query	ArcSight Foundation/Configuration Monitoring/Operational Summaries/
Trend on Password Modifications	This query returns data from the Password Modifications trend for use in the Password Changes by <System/User/Zone> reports.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Modification/Password/
Password Changes	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Modification/Password/
Account Creation by Host on Trend	This query on the Account Creation by Host trend provides a listing of the account creation events seen within the past week on your monitored assets. Note: The Account Creation by Host trend is not enabled by default. This query is a part of the Configuration Monitoring content.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/
User Account Creation Trend	This query on events restricted by the User Account Creations filter returns the customer, attacker user name, attacker zone, target address, target asset name, target host name, target Nt domain, target user ID, target user name, and target zone for the User Account Creation trend.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/
Account Creation by Host	This query provides a listing of the account creation events seen within the past day on your monitored assets. Note: This query retrieves host-local user account creations, instead of authentication service account creations so that it does not retrieve user additions in the Active Directory. This query is a part of the Configuration Monitoring content.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/
User Configuration Modifications	This query returns the previous day of configuration modification events related to users.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/
By User Account - Accounts Deleted	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Deletion/

Resource	Description	Type	URI
Assets with Recent Configuration Modifications by Vendor and Product	This query collects information about a day's worth of configuration changes to your various assets. The data retrieved includes information about the asset affected, the asset causing the change (if any), and the vendor and product information about the asset that was changed.	Query	ArcSight Foundation/Configuration Monitoring/Details/
Password Modifications Trend	This query on events restricted by the Successful Password Changes filter returns the attacker user ID, attacker user name, attacker zone, target address, target asset ID, target asset name, target Nt domain, target user ID, target user name, target zone, and sums the aggregated event count for use in the Password Modifications trend.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Modification/Password/
Most Common Account Login Failures by Attacker User (Yesterday)	This query returns the category object, attacker Address, attacker asset name, attacker Nt domain, attacker user ID, attacker user name, attacker zone name, and the sum of the aggregated event count for events matching the Failed User Account Login Attempts filter.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Access Tracking/
Accounts Deleted by Host Trend	This query on events restricted by the User Account Deletions filter provides a listing of the users deleted over the time interval by System & Zone for the Accounts Deleted by Host trend.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Deletion/
User Account Modifications Trend	The query on events restricted by the User Account Modifications filter retrieves the customer, target zone, target address, target asset ID, target asset name, name, target user ID, target user name, aggregated event count and end time for the User Account Modifications trend.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Modification/
Trend on User Account Modifications	This query on the User Account Modifications trend returns data for use in the User Account Modifications report.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Modification/

Resource	Description	Type	URI
Trend on VPN User Account Creation	This query on the VPN User Account Creation trend retrieves the customer, target zone name, target user ID, and attacker user name for the VPN User Account Creation report. The fields Target Zone Name, Target User ID, and Attacker User Name are renamed Zone, New Account, and Creator in the report.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/
Trend on User Account Creation	This query on the User Account Creation trend returns the customer, attacker user name, attacker zone, target address, target asset name, target host name, target Nt domain, target user ID, target user name, and target zone for the User Account Creation report.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/
By User Account - Accounts Created	This query retrieves events meeting the conditions Category Behavior = /Authentication/Add and Category Outcome = /Success, selecting End Time, Target User Name, Attacker User Name, Name, Target Zone Name and Target Host Name for the By User Account - Accounts Created report.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/
User Administration (Chart)	This query returns the count of user (and user group) creations, modifications, and deletions.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Operating System/
Local Windows User Creation - Disallowed Systems	This query returns the customer, attacker user name, target zone, target address, target asset name, target user ID, target user name, the day and the sum of the aggregated event count for successful local Windows user creations on disallowed systems.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Creation/
Users That Performed Configuration Modifications Past Week	This query retrieves a list of the users that performed configuration modifications to assets in the past week.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/
User Administration	This query returns the user (and user group), creation, modification, and deletion events.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Operating System/

Resource	Description	Type	URI
AAA User Account Deletions on Trend	This query retrieves the customer, attacker user name, attacker zone, target address, target asset name, target host name, target Nt domain, target user ID, and target user name from AAA User Account Deletions trend. Note: The AAA User Account Deletions trend is not enabled by default.	Query	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Deletion/
Local Windows User Creation - Disallowed Systems	This trend collects the customer, attacker user name, target zone, target address, target asset name, target user ID, target user name, the day and the sum of the aggregated event count for successful local Windows user creations on disallowed systems. Note: This trend is not enabled by default.	Trend	ArcSight Foundation/Configuration Monitoring/User Account Modifications/
User Removals	This trend collects user account deletion data, restricted by the User Account Deletions filter.	Trend	ArcSight Foundation/Configuration Monitoring/User Account Modifications/
AAA User Account Deletions	This trend collects information about AAA User Accounts that have been deleted. Note: This trend is not enabled by default.	Trend	ArcSight Foundation/Configuration Monitoring/User Account Modifications/
Account Creation by Host	This trend collects a listing of the account creation events seen over the past day on your monitored assets. Note: The query retrieves host-local user account creations instead of authentication service account creations so that the trend does not collect user additions in the Active Directory. Note: The trend data fields are renamed for clarity when creating reports. This trend is not enabled by default.	Trend	ArcSight Foundation/Configuration Monitoring/User Account Modifications/
Password Modifications	This trend collects data for monitoring password changes, including the ID for which the password was changed and the ID of the user making the change. Note: This trend is not enabled by default.	Trend	ArcSight Foundation/Configuration Monitoring/User Account Modifications/
VPN User Account Creation	This trend collects information about the creation of VPN user accounts. Note: This trend is not enabled by default.	Trend	ArcSight Foundation/Configuration Monitoring/User Account Modifications/

Resource	Description	Type	URI
User Account Creation	This trend collects data for the User Account Creation report.	Trend	ArcSight Foundation/Configuration Monitoring/User Account Modifications/
User Account Modifications	This trend collects data relevant to tracking modifications to user accounts, specifically for the User Account Modifications report.	Trend	ArcSight Foundation/Configuration Monitoring/User Account Modifications/
Assets with Recent Configuration Modifications (Daily)	This trend retrieves changes to assets within the last day and stores information about the change itself as well as who made the change.	Trend	ArcSight Foundation/Configuration Monitoring/Asset Configuration Change Tracking/
AAA User Account Creation	This trend collects data for the AAA User Account Creation report. Note: This trend is not enabled by default.	Trend	ArcSight Foundation/Configuration Monitoring/User Account Modifications/

Vulnerabilities

The Vulnerabilities resources provide an overview about current vulnerabilities on systems.

Devices

The following device type can supply events that apply to the Vulnerabilities resource group:

- Vulnerability scanners

Resources

The following table lists all the resources in the Vulnerabilities resource group and any dependant resources.

Table 3-7 Resources that Support the Vulnerabilities Group

Resource	Description	Type	URI
Monitor Resources			
High-Priority Scan Events Directed Toward High-Criticality Assets - Today	This query viewer displays today's scan results for a view into high-priority vulnerabilities detected on highly-critical assets.	Query Viewer	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Asset Vulnerability Scans/
High-Priority Scan Events Directed Toward High-Criticality Assets - Yesterday	This query viewer displays yesterday's scan results for a view into high-priority vulnerabilities detected on highly-critical assets.	Query Viewer	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Asset Vulnerability Scans/
10 Most Vulnerable Assets in Confidential Data Group	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
Exposed Vulnerabilities by Zone Trend - Last 90 Days	This report provides a chart view of the exposed vulnerabilities across your top vulnerable zones over the course of a week. If you patch on a monthly or longer basis, use the reports with longer periods.	Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/Critical Assets/
High-Priority Vulnerabilities Detected on Critical Assets - Yesterday	This report displays scan events from yesterday where the priority of the scan event is greater than 5 (fairly severe) and the target asset has been categorized with a high or very-high criticality.	Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
Exposed Vulnerabilities by Asset	This report shows a table of exposed vulnerabilities by asset.	Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/

Resource	Description	Type	URI
Top 10 Assets by Exposed Vulnerability Counts	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
Vulnerability Exposure by Asset Criticality - Current Month	This report provides a weekly view into the vulnerability exposure trend of your critical assets for the current month. Note: If you run this report before the first trend run of the month, there will be no data.	Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/Critical Assets/
Exposed Vulnerability Count by Asset	This report lists the count of vulnerabilities per asset and the ten assets with the most exposed vulnerabilities.	Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
All Vulnerabilities in Email and Web Server Assets	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
Exposed Vulnerabilities by Zone Trend - Last Month	This report provides a chart view of the exposed vulnerabilities across your top vulnerable zones over the course of a month. If you patch on a monthly or longer basis, use the reports with longer periods.	Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/Critical Assets/
Exposed Vulnerabilities by Zone Trend - Last Week	This report provides a chart view of the exposed vulnerabilities across your top vulnerable zones over the course of a week. If you patch on a monthly or longer basis use the reports with longer periods.	Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/Critical Assets/
Top 10 Exposed Vulnerabilities by Asset Counts	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
Blaster Vulnerable Hosts	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
All Exposed Vulnerabilities	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/

Resource	Description	Type	URI
Top Vulnerability Exposure of Critical Assets	This report displays the top 1000 assets by vulnerability count for the past seven days from the Top Vulnerability Exposure of Critical Assets trend. Note: If you have fewer than 1000 assets, there might be more than seven days worth of data selected.	Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/Critical Assets/
Vulnerabilities of Assets in North America	This resource has no description.	Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
Library - Correlation Resources			
Warning - Vulnerable Software	This rule detects vulnerable software. The rule triggers whenever a vulnerable application or operating system is found. The vulnerability should not be a scan vulnerability. On the first event, a notification is sent to SOC operators.	Rule	ArcSight Foundation/Configuration Monitoring/Detail/Vulnerabilities/
Warning - Insecure Configuration	This rule detects insecure object configuration. The rule triggers whenever an insecure object is found or a security check fails. On the first event, a notification is sent to SOC operators.	Rule	ArcSight Foundation/Configuration Monitoring/Detail/Vulnerabilities/
Library Resources			
Address Spaces	This is a site asset category.	Asset Category	Site Asset Categories
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Port 135	This is a site asset category.	Asset Category	Site Asset Categories/Open Port/TCP
Web Server	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type
Port 139	This is a site asset category.	Asset Category	Site Asset Categories/Open Port/TCP
Email	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type
Port 445	This is a site asset category.	Asset Category	Site Asset Categories/Open Port/TCP
Criticality	This is a system asset category.	Asset Category	System Asset Categories
Confidential Data	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis/Data Role

Resource	Description	Type	URI
High	This is a system asset category.	Asset Category	System Asset Categories/Criticality
North America	This is a site asset category.	Asset Category	Site Asset Categories/Location
Very High	This is a system asset category.	Asset Category	System Asset Categories/Criticality
High-Priority Scan Event for Critical Asset	This filter identifies vulnerability scan events that indicate that a high-priority vulnerability was detected on a system you have marked with high or very-high criticality.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Vulnerabilities/
All Events	Filter that matches all events.	Filter	ArcSight System/Core
Vulnerability Exposure by Asset Criticality - Last 3 Months	This report provides a weekly view into the vulnerability exposure trend of your critical assets for the previous 3 months. This report is based on the Vulnerability Exposure by Asset Criticality - Current Month report.	Focused Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/Critical Assets/
Exposed Vulnerability Count by Critical Asset	This report shows a table of exposed vulnerabilities on assets categorized as high criticality.	Focused Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/Critical Assets/
Vulnerability Exposure by Asset Criticality - Last 6 Months	This report provides a weekly view into the vulnerability exposure trend of your critical assets for the previous 6 months. The report is based on the Vulnerability Exposure by Asset Criticality - Current Month report,	Focused Report	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/Critical Assets/
Vulnerability Exposure by Asset Criticality - Trend Query - Snapshot	This query on assets that have been categorized under /All Asset Categories/System Asset Categories/Criticality, returns the address, device zone ID, device zone name, name, a count of vulnerability, and the GetCriticality variable for the Vulnerability Exposure by Asset Criticality trend. Note: This query returns up to 10,000 (the default Row Limit) assets with the highest number of vulnerabilities (ORDER BY COUNT(Vulnerability) DESC. If you are using this query to populate a trend (as in the Vulnerability Exposure by Asset Criticality trend that is part of the Configuration Monitoring Standard Content), this Row Limit will be overridden by the Row Limit of the trend when it runs.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/Critical Assets/

Resource	Description	Type	URI
10 Most Vulnerable Assets in Confidential Data Group	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
Top 10 Assets by Exposed Vulnerability Counts	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
High-Priority Scan Events Directed Toward High-Criticality Assets	This query returns yesterday's scan results for a view into high-priority vulnerabilities detected on highly-critical assets.	Query	ArcSight Foundation/Configuration Monitoring/Operational Summaries/Asset Vulnerability Scans/
Vulnerability Exposure of Critical Assets on Trend	This query retrieves the top 1000 assets by vulnerability count from the Vulnerability Exposure of Critical Assets trend, to be used in the Top Vulnerability Exposure of Critical Assets trend.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/Critical Assets/
Exposed Vulnerabilities by Zone Trend - Last Week	This query on the Vulnerability Exposure of High and Very-High Criticality Assets by Zone - Trend Query returns the count of vulnerability, device zone name, and timeStamp for the Exposed Vulnerabilities by Zone Trend - <various time periods> reports.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/Critical Assets/
All Exposed Vulnerabilities	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
Top 10 Exposed Vulnerabilities by Asset Counts	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
Vulnerabilities of Assets in North America	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
Exposed Vulnerabilities - High and Very High Criticality Assets by Zone - Trend Query	This query tracks how many vulnerabilities highly and very-highly critical systems have over time, by zone. The query is most often used directly by a trend to store a daily snapshot of the information. To reduce storage requirements, this query only retrieves a count of the number of vulnerabilities in these zones, not the full list of vulnerabilities.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/Critical Assets/

Resource	Description	Type	URI
Exposed Vulnerability Count by Asset	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
All Vulnerabilities in Email and Web Server Assets	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
Top Vulnerability Exposure of Critical Assets on Trend	This query returns the top 1000 assets by vulnerability count for the past seven days from the Top Vulnerability Exposure of Critical Assets trend for the Top Vulnerability Exposure of Critical Assets report.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/Critical Assets/
Blaster Vulnerable Hosts	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
Vulnerability Exposure by Asset Criticality	This query retrieves a set of snapshot points providing vulnerability counts for critical assets.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/Critical Assets/
Exposed Vulnerabilities by Asset	This resource has no description.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
High-Priority Vulnerabilities Detected on Critical Assets - Yesterday	This query retrieves scan events from yesterday where the priority of the scan event is greater than five (fairly severe) and the target asset has been categorized as high or very-high criticality.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/
Exposed Vulnerabilities - High and Very High Criticality Assets - Trend Query	This query tracks how many vulnerabilities highly and very-highly critical systems have over time. The query is most often used directly by a trend to store a daily snapshots of the information. To reduce the storage requirements, this query only retrieves a count of the number of vulnerabilities on these assets, not the full list of vulnerabilities.	Query	ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/Critical Assets/

Resource	Description	Type	URI
Vulnerability Exposure by Asset Criticality	This trend provides a weekly snapshot of the vulnerability counts of assets marked as having criticality. The default snapshot size (Row Limit) for this trend is 50,000. If you have significantly more assets than this, increase this number to match your environment. Note: You do not need to adjust the Row Limit for the query that feeds this trend (Vulnerability Exposure by Asset Criticality - Trend Query - Snapshot), the trend overrides the query's Row Limit parameter when it runs.	Trend	ArcSight Foundation/Configuration Monitoring/Vulnerability Tracking/
Vulnerability Exposure of High and Very-High Criticality Assets by Zone - Daily Trend	This trend collects a weekly snapshot of the assets used to track how many vulnerabilities highly and very-highly critical systems have over time, by zone. To reduce storage requirements, this trend only collects a count of the number of vulnerabilities in these zones, not the full list of vulnerabilities. Note: This trend is not enabled by default.	Trend	ArcSight Foundation/Configuration Monitoring/Vulnerability Tracking/
Vulnerability Exposure of Critical Assets	This trend collects daily statistics on the vulnerability exposure of your assets that have been categorized as highly or very-highly critical. The trend includes information about the asset and a count of the number of vulnerabilities it currently exposes.	Trend	ArcSight Foundation/Configuration Monitoring/Vulnerability Tracking/
Top Vulnerability Exposure of Critical Assets	This trend collects the top 1000 assets by vulnerability count from the Vulnerability Exposure of Critical Assets trend, to be used in the Top Vulnerability Exposure of Critical Assets report.	Trend	ArcSight Foundation/Configuration Monitoring/Vulnerability Tracking/
CVE - CAN-2003-0605	This resource has no description.	Vulnerability	CVE/

Appendix A

Upgrading Standard Content

This appendix discusses the following topics.

Preparing Existing Content for Upgrade

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

Configurations Preserved During Upgrade

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

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

Configurations that Require Restoration After Upgrade

The following resource configurations require restoration after upgrade.

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

Backing Up Existing Resources Before Upgrade

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

During the upgrade process, the content is run through a resource validator automatically (see "Fixing Invalid Resources" on page 71).

To help the process of reconfiguring resources that require restoration after upgrade, back up the resources you identify in "Configurations that Require Restoration After Upgrade" on page 69 and export them in a package. After upgrade, you can re-import the package and use the existing resources as a reference for restoring the configurations to the upgraded environment.

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

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

Copy and paste configurations from the old resources to the new

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

Performing the Upgrade

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

Checking and Restoring Content After Upgrade

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

Verifying and Reapplying Configurations

Verify and restore standard content after upgrade.

1. Verify that your configured resources listed in the section "Configurations Preserved During Upgrade" on page 69 retained their configurations as expected.
2. Reconfigure the resources that require restoration.
   a. Re-import the package you created in "Backing Up Existing Resources Before Upgrade" on page 70.
   b. One resource at a time, copy and paste the configurations preserved in the package of copied resources into the new resources installed with the upgrade. Copying your configurations one resource at a time instead of overwriting the new resources with the old ensures that you retain your configurations without overwriting any improvements provided with the upgraded content.

Verifying Customized Content

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

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

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

Fixing Invalid Resources

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

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

- Zones

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

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

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

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

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

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Z