

Standard Content Guide

Configuration Monitoring

ArcSight ESM 6.5c

October 11, 2013



Copyright © 2013 Hewlett-Packard Development Company, L.P.

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

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

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

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

Contact Information

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

Revision History

| Date | Product Version | Description |
|-------------|--|-----------------------------|
| 10/11/2013 | Configuration Monitoring content for ArcSight ESM 6.5c | Final revision for release. |

Contents

| | |
|--|-----------|
| Chapter 1: Configuration Monitoring Overview | 5 |
| What is Standard Content? | 5 |
| Standard Content Packages | 7 |
| Configuration Monitoring Content | 7 |
| Chapter 2: Installation and Configuration | 9 |
| Installing the Configuration Monitoring Package | 9 |
| Configuring the Configuration Monitoring Content | 10 |
| Modeling the Network | 10 |
| Categorizing Assets | 11 |
| Configuring Active Lists | 12 |
| Ensuring Filters Capture Relevant Data | 12 |
| Enabling Rules | 13 |
| Configuring Notification Destinations | 13 |
| Configuring Notifications and Cases | 13 |
| Scheduling Reports | 13 |
| Configuring Trends | 14 |
| Chapter 3: Configuration Monitoring Content | 15 |
| Assets | 16 |
| Resources | 16 |
| Configuration Changes Overview | 20 |
| Configuring the Configuration Changes Overview Resource Group | 20 |
| Resources | 20 |
| Device Configuration Changes | 23 |
| Resources | 23 |
| Hosts and Applications Overview | 32 |
| Configuring the Hosts and Applications Overview Resource Group | 32 |
| Resources | 32 |
| Security Application and Device Configuration Changes | 40 |
| Devices | 40 |
| Resources | 40 |
| User Configuration Changes | 49 |
| Resources | 49 |

Vulnerabilities 60

 Devices 60

 Resources 60

Index 69

Chapter 1

Configuration Monitoring Overview

This chapter discusses the following topics.

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

["Standard Content Packages" on page 7](#)

["Configuration Monitoring Content" on page 7](#)

What is Standard Content?

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

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

Standard content consists of the following:

- **ArcSight Core Security** content is installed automatically with the ArcSight Manager and consists of key resources for monitoring Microsoft Windows, firewall, IPS and IDS, NetFlow, and other essential security information.
- **ArcSight Administration** content contains several packages that provide statistics about the health and performance of ArcSight products.
 - ◆ ArcSight Administration is installed automatically with the ArcSight Manager and is essential for managing and tuning the performance of content and components.
 - ◆ ArcSight Admin DB CORR is installed automatically with the ArcSight Manager for ArcSight ESM with CORR- (Correlation Optimized Retention and Retrieval) Engine and provides information on the health of the CORR-Engine.
 - ◆ ArcSight Content Management is an optional package that shows information about content package synchronization with the ESM Content Management feature. The information includes a history of content packages synchronized from a primary ESM source to multiple ESM destinations, and any common issues or errors encountered. You can install this package during ArcSight ESM installation or from the ArcSight Console any time after installation.

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

**Note**

The ArcSight Admin DB CORR and ArcSight Search Filters content packages are installed automatically when you perform a new ArcSight ESM installation. However, when you upgrade your ArcSight ESM system, these content packages are not installed automatically. You can install these packages from the ArcSight Console any time after upgrade by right-clicking the package on the Packages tab in the Navigator and selecting Install Package.

Refer to the ArcSight ESM Upgrade Guide for information about upgrading ArcSight ESM.

- **ArcSight System** content is installed automatically with the ArcSight 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 Foundation** content (such as Cisco Monitoring, Configuration Monitoring, Intrusion Monitoring, IPv6, NetFlow Monitoring, Network Monitoring, and Workflow) provide a coordinated system of resources with real-time monitoring capabilities for a specific area of focus, as well as after-the-fact analysis in the form of reports and trends. You can extend these foundations with additional resources specific to your needs or you can use them as a template for building your own resources and tasks. You can install a Foundation during ArcSight ESM installation or from the ArcSight Console any time after installation.
- **Shared Libraries** - ArcSight Administration and several of the ArcSight Foundations rely on a series of common resources that provide core functionality for common security scenarios. Dependencies between these resources and the packages they support are managed by the Package resource.
 - ◆ Anti Virus content is a set of filters, reports, and report queries used by ArcSight Foundations, such as Configuration Monitoring and Intrusion Monitoring.
 - ◆ Conditional Variable Filters content is a library of filters used by variables in standard content report queries, filters, and rule definitions. The Conditional Variable Filters are used by ArcSight Administration and certain ArcSight Foundations, such as Configuration Monitoring, Intrusion Monitoring, Network Monitoring, and Workflow.
 - ◆ Global Variables content is a set of variables used to create other resources and to provide event-based fields that cover common event information, asset, host, and user information, and commonly used timestamp formats. The Global Variables are used by ArcSight Administration and certain ArcSight Foundations.
 - ◆ Monitoring Support Data content is a set of active lists that store mapping information for HTTP return status code classes, Cisco firewall syslog message types, and encoded logon types.
 - ◆ Network filters content is a set of filters required by ArcSight Administration and certain ArcSight Foundations, such as Intrusion Monitoring and Network Monitoring.

**Caution**

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

Standard Content Packages

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

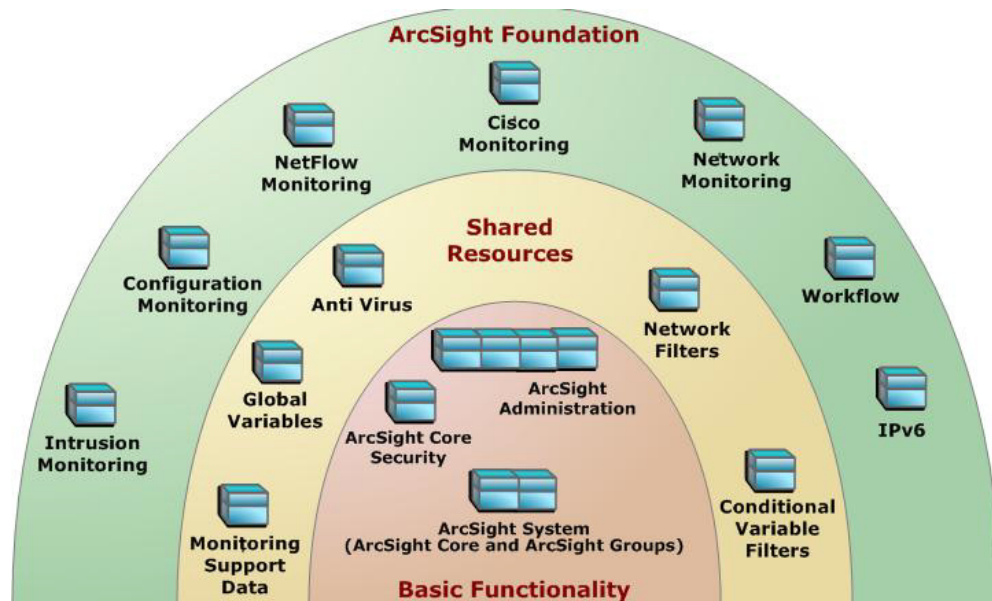


Figure 1-1 The ArcSight Core Security, ArcSight Administration, and ArcSight System packages at the base provide content required for basic ArcSight functionality. The common packages in the center contain shared resources that support multiple packages. The packages shown on top are ArcSight Foundations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

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



Caution

When creating your own packages, you can explicitly include or exclude system resources in the package. Exercise caution if you delete packages that might have system resources; 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 Core Security, ArcSight Administration, or ArcSight System content, refer to the ArcSight Core Security, ArcSight Administration, and ArcSight System Standard Content Guide. 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.

[“Installing the Configuration Monitoring Package” on page 9](#)

[“Configuring the Configuration Monitoring Content” on page 10](#)

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 a Foundation package during ESM installation, the package is *imported* into the Packages tab in the Navigator panel automatically, but is not available in the resource view. The package icon in the package view appears 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 On the Navigator panel Packages tab, 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 On the Navigator Panel Packages tab, 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 Packages tab, and can be re-installed at another time.

To delete a package and remove it from the ArcSight Console and the ArcSight Database:

- 1** On the Navigator Panel Packages tab, navigate to the package you want to delete.
- 2** Right-click the package and select **Delete Package**.
- 3** When prompted for confirmation, click **Delete**.

The package is removed from the Navigator panel Packages tab.

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 12](#)
- ["Enabling Rules" on page 13](#)
- ["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 14](#)

Modeling the Network

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

There are several ways to model your network. For information about populating the network model, refer to the ArcSight Console User's Guide. To learn more about the architecture of the 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 listed in the following table to activate standard content that uses these categories so that you can apply criticality and business context to events.

| Asset Category | Description |
|---|--|
| /Site Asset Categories/ Address Spaces/Protected | <p>Categorize all assets (or the zones to which the assets belong) that are internal to the network with this asset category.</p> <p>Internal Assets are assets inside the company network. Assets that are not categorized as internal to the network are considered to be external. Make sure that you also categorize assets that have public addresses but are controlled by the organization (such as web servers) as <i>Protected</i>.</p> <p>Note: Assets with a private IP address (such as 192.168.0.0) are considered <i>Protected</i> by the system, even if they are not categorized as such.</p> |
| /System Asset Categories/ Criticality/High | <p>Categorize all assets that are considered <i>critical</i> to protect (including assets that host proprietary content, financial data, cardholder data, top secret data, or perform functions critical to basic operations) with this asset category.</p> <p>The asset categories most essential to basic event processing are those used by the Priority Formula to calculate the criticality of an event. Asset criticality is one of the four factors used by the Priority Formula to generate an overall event priority rating.</p> |
| /System Asset Categories/ Criticality/Very High | See /System Asset Categories/Criticality/High |

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

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

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

Configuring Active Lists

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

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

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

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

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 the CERT Team notification group. 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 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.

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.

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 ArcSight 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.

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 60 | 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 start up 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 | This filter 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 |
|---|--|-----------------|--|
| Simple Table Portrait | This template is designed to show a table. The orientation is portrait. | Report Template | ArcSight System/1 Table |
| Chart and Table Landscape | This template is designed to show one chart and a table. The orientation is landscape. | Report Template | ArcSight System/1 Chart/With Table |
| Chart and Table Portrait | This template is designed to show one chart and a table. The orientation is portrait. | Report Template | ArcSight System/1 Chart/With Table |
| 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.

Configuring the Configuration Changes Overview Resource Group

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. After this rule triggers, 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/ |
| Standard | This field set contains several fields that are useful at a glance for selecting events for inspection. It uses the end time field for the timestamp. | Field Set | ArcSight System/Event Field Sets/Active Channels |
| 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 in which the category device group is 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 in which the category behavior is /Modify/Configuration and the category outcome is Success. | Filter | ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/ |

| Resource | Description | Type | URI |
|---|--|----------|--|
| 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/ |
| 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 filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included. | Filter | ArcSight System/Event Types |
| Non-ArcSight Events | This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors. | Filter | ArcSight System/Event Types |
| Security Application and Device Configuration Changes | This use case provides information about the configuration change 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 change on host 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 that focus 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/Switch/ |
| Misconfigurations | This resource has no description. | Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/VPN/ |
| 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 grouped by user and type, and sorted 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. A chart shows the top ten errors and warnings. A 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 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, grouped by type and user, and sorted chronologically. Use this report to find all configuration changes of a certain type. | Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Common/ |
| VPN Configuration Changes | This resource has no description. | Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/VPN/ |

| Resource | Description | Type | URI |
|------------------------------|--|--------|---|
| 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 triggers, 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/ |
| Criticality | This is a system asset category. | Asset Category | System Asset Categories |
| Scanned | This is a site asset category. | Asset Category | Site Asset Categories |

| Resource | Description | Type | URI |
|---|--|-----------------|--|
| 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. | 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. | 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 | 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 | Global Variable | ArcSight Foundation/Variables Library |
| VPN Events | This filter identifies events in which the category device group is 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 |

| Resource | Description | Type | URI |
|----------------------------------|--|--------|--|
| 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 | This filter matches all events. | Filter | ArcSight System/Core |
| ArcSight Events | This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included. | Filter | ArcSight System/Event Types |
| 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 |
| 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/ |

| Resource | Description | Type | URI |
|--|---|----------------|---|
| 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 filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors. | Filter | ArcSight System/Event Types |
| Configuration Changes by User | This report shows recent VPN configuration changes grouped by user, sorted chronologically. Use this report to find all the configuration changes made by a specific user. | Focused Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/VPN/ |
| Configuration Changes by Type | This report shows recent VPN configuration changes grouped by type (name), sorted chronologically. Use this report to find all the configuration changes of a certain type. | Focused Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/VPN/ |
| 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/ |

| Resource | Description | Type | URI |
|---|---|-------|---|
| 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/Configu ration 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/Critica l 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/ |
| 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/Configu ration 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/Configu ration Changes/Device/Database Errors and Warnings/ |
| Switch Configuration Changes | This resource has no description. | Query | ArcSight Foundation/Configuration Monitoring/Details/Configu ration 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/ |

| Resource | Description | Type | URI |
|--|---|-------|--|
| Misconfigurations | This resource has no description. | Query | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/VPN/ |
| 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/ |
| 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/Switch/ |
| 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 might 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/ |

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

Configuring the Hosts and Applications Overview Resource Group

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 grouped by user and type, and sorted 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. A chart shows the top ten errors and warnings. A 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, grouped by type and user, and sorted chronologically. Use this report to find all configuration changes of a certain type. | Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Common/ |
| Host Summary by Business Role | This report shows the breakdown of assets by business role and displays an overview of the asset configurations. This report is part of the Configuration Monitoring content. | Report | ArcSight Foundation/Configuration Monitoring/Executive Summaries/Overall Host Configuration/ |
| Host Configuration Events By Zone | This report shows the breakdown of host configuration events by zone and displays an overview of the asset configurations. This report is part of the Configuration Monitoring content. | Report | ArcSight Foundation/Configuration Monitoring/Executive Summaries/Overall Host Configuration/ |
| Host Summary by Criticality | This report shows the breakdown of assets by criticality and displays an overview of the asset configurations. This report is part of the Configuration Monitoring content. | Report | ArcSight Foundation/Configuration Monitoring/Executive Summaries/Overall Host Configuration/ |
| 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/ |

| Resource | Description | Type | URI |
|---------------------------|---|----------------|--|
| 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 part of the Configuration Monitoring content. | Report | ArcSight Foundation/Configuration Monitoring/Details/Inventory/ |
| Host Summary by Data Role | This report shows the breakdown of assets by data role and displays an overview of the asset configurations. This report is 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/ |
| 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. | Data Monitor | ArcSight Foundation/Configuration Monitoring/Operational Summaries/Host Problems Overview/ |

| Resource | Description | Type | URI |
|---|--|-----------------|--|
| 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. | 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. | 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 | 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 | Global Variable | ArcSight Foundation/Variables Library |
| 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 |

| Resource | Description | Type | URI |
|----------------------------------|--|--------|--|
| 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 where the category device group is Application, the category object is /Host/Application/Database, and the category significance is /Informational/Warning or /Informational/Error. | Filter | ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/Database/ |
| All Events | This filter 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 filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included. | Filter | ArcSight System/Event Types |
| 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 |
| 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/ |

| Resource | Description | Type | URI |
|------------------------------------|---|----------------|--|
| 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 filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors. | Filter | ArcSight System/Event Types |
| Configuration Changes by User | This report shows recent database configuration changes and lists all the changes grouped by user, sorted chronologically. Use this report to find all the configuration changes made by a specific user. | Focused Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Database/ |
| Configuration Changes by Type | This report shows recent database configuration changes and lists all the changes, grouped by type, sorted chronologically. Use this report to find all the configuration changes of a certain type. | Focused Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Database/ |
| 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/ |

| Resource | Description | Type | URI |
|--|---|-----------------|---|
| 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/ |
| 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/ |
| Simple Table Portrait | This template is designed to show a table. The orientation is portrait. | Report Template | ArcSight System/1 Table |

| Resource | Description | Type | URI |
|----------------------------------|--|-----------------|---|
| Simple Chart Portrait | This template is designed to show one chart. The orientation is portrait. | Report Template | ArcSight System/1 Chart/Without Table |
| Chart and Table Landscape | This template is designed to show one chart and a table. The orientation is landscape. | Report Template | ArcSight System/1 Chart/With Table |
| 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 yesterdayseventsonassetscategorizedashavingaregulationrequirement.' | Report | ArcSight Foundation/Intrusion Monitoring/Operational Summaries/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/Configuration Monitoring/Details/Configuration Changes/Device/Anti-Virus |

| Resource | Description | Type | URI |
|--|---|--------|---|
| 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/Configuration Monitoring/Details/Configuration Changes/Device/Anti-Virus |
| 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/Configuration Monitoring/Details/Configuration Changes/Device/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/Intrusion Monitoring/Operational Summaries/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/Configuration Monitoring/Details/Configuration Changes/Device/Anti-Virus |
| Update Summary | This report displays a summary of the results of anti-virus update activity by zones since yesterday. | Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/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/Configuration Monitoring/Details/Configuration Changes/Device/Anti-Virus |
| HIDS Misconfigurations | This resource has no description. | Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/IDS/ |

| Resource | Description | Type | URI |
|--|--|----------------|--|
| Configuration Changes by User | This report shows recent configuration changes grouped by user and type, and sorted 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/ |
| 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 yesterdayseventsonassetscategorizedashavingaregulationrequirement.' | Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Anti-Virus |
| Top Infected Systems | This report displays summaries of the systems reporting the most infections during the previous day. | Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Anti-Virus |
| Configuration Changes by Type | This report shows recent configuration changes, grouped by type and user, and sorted chronologically. Use this report to find all 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 | This filter matches all events. | Filter | ArcSight System/Core |
| Host IDS | This resource has no description. | Filter | ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/IDS/ |

| Resource | Description | Type | URI |
|-------------------------------|--|----------------|---|
| ArcSight Events | This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included. | Filter | ArcSight System/Event Types |
| Anti-Virus Events | This filter identifies events in which the category device group is /IDS/Host/Antivirus. | Filter | ArcSight Foundation/Common/Anti-Virus |
| 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 /Success, 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 filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors. | Filter | ArcSight System/Event Types |
| Configuration Changes by User | This report shows recent firewall configuration changes grouped by user, and sorted chronologically. Use this report to find all the configuration changes made by a specific user. | Focused Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Firewall/ |

| Resource | Description | Type | URI |
|-------------------------------|---|----------------|--|
| Configuration Changes by Type | This report shows recent identity management configuration changes grouped by type (name), and sorted chronologically. Use this report to find all the configuration changes of a certain type. | Focused Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Identity Management/ |
| 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/Configuration Monitoring/Details/Configuration Changes/Device/Anti-Virus |
| Configuration Changes by Type | This report shows recent network configuration changes grouped by type (name), and sorted chronologically. Use this report to find all the configuration changes of a certain type quickly. | Focused Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Network/ |
| 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/Configuration Monitoring/Details/Configuration Changes/Device/Anti-Virus |
| Configuration Changes by Type | This report shows recent firewall configuration changes grouped by type, and sorted chronologically. Use this report to find all the configuration changes of a certain type. | Focused Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Firewall/ |
| Configuration Changes by User | This report shows recent network configuration changes grouped by user, and sorted chronologically. Use this report to find all the configuration changes made by a specific user. | Focused Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Network/ |
| Configuration Changes by User | This report shows recent identity management configuration changes grouped by user, and sorted chronologically. Use this report to find all the configuration changes made by a specific user. | Focused Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Identity Management/ |
| Failed Anti-Virus Updates | This query identifies the device vendor, device product, target zone name, target host name, target address, and time (EndTime) from events that match the AV - Failed Updates filter. | Query | ArcSight Foundation/Intrusion Monitoring/Detail/Anti-Virus |

| Resource | Description | Type | URI |
|---|--|-------|---|
| 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 |
| 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/Intrusion Monitoring/Operational Summaries/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/Intrusion Monitoring/Operational Summaries/Anti-Virus |
| Firewall Configuration Changes | This resource has no description. | Query | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Firewall/ |

| Resource | Description | Type | URI |
|--|--|-------|--|
| 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 |
| 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/Intrusion Monitoring/Detail/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 /Success, and the Category Behavior is /Found/Vulnerable). | Query | ArcSight Foundation/Intrusion Monitoring/Detail/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 AV - Found Infected filter where the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Success, and the Category Behavior is /Found/Vulnerable. | Query | ArcSight Foundation/Intrusion Monitoring/Detail/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/Intrusion Monitoring/Detail/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 |
| Simple Table Portrait | This template is designed to show a table. The orientation is portrait. | Report Template | ArcSight System/1 Table |
| Chart and Table Landscape | This template is designed to show one chart and a table. The orientation is landscape. | Report Template | ArcSight System/1 Chart/With Table |
| Chart and Table Portrait | This template is designed to show one chart and a table. The orientation is portrait. | Report Template | ArcSight System/1 Chart/With Table |
| Two Charts One Table Landscape | This template is designed to show two charts and a table. The orientation is landscape. | Report Template | ArcSight System/2 Charts/With Table |

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/Accounts Modified/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/Accounts Deleted/ |

| 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/Accounts Modified/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/Accounts Deleted/ |
| 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/Accounts Created/ |
| 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/Accounts Created/ |
| 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/ |
| 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/Accounts Modified/ |
| 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/Accounts Created/ |

| Resource | Description | Type | URI |
|---|--|----------------|---|
| User Account Creation | This resource has no description. | Report | ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/User/Accounts Created/ |
| 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/Accounts Deleted/ |
| 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/Accounts Created/ |
| 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/Accounts Modified/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/Accounts Modified/Password/ |
| Library Resources | | | |
| Business Role | This is a site asset category. | Asset Category | Site Asset Categories/Business Impact Analysis |
| VPN Events | This filter identifies events in which the category device group is VPN. | Filter | ArcSight Foundation/Common/Device Class Filters |

| Resource | Description | Type | URI |
|------------------------------------|--|--------|---|
| 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/ |
| 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 filter selects events related to successful password changes, defined as having the category behavior of /Authentication/Modify and the category outcome of success. | 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 | This filter 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 filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included. | Filter | ArcSight System/Event Types |

| Resource | Description | Type | URI |
|---|--|----------------|---|
| 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 in which the category device group is 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/ |
| Non-ArcSight Events | This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors. | 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 identity management 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/Identity Management/ |

| Resource | Description | Type | URI |
|---------------------------------------|---|----------------|---|
| 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 VPN 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/VPN/ |
| 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 operating system 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/Operating System/ |
| 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/ |
| 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/ |
| 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/ |

| Resource | Description | Type | URI |
|-----------------------------------|---|-------|---|
| 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/ |
| 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 query returns information related to successful password changes, defined as having the category behavior of /Authentication/Modify and the category outcome of Success. | 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/ |

| Resource | Description | Type | URI |
|--|--|-------|---|
| 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/Configu ration 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/Configu ration Changes/ |
| By User Account - Accounts Deleted | This resource has no description. | Query | ArcSight Foundation/Configuration Monitoring/Details/Configu ration Changes/User/Deletion/ |
| 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/Configu ration 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/Configu ration 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/Configu ration Changes/User/Deletion/ |

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

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

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

| Resource | Description | Type | URI |
|---|--|--------|---|
| Exposed Vulnerabilities by Asset | This report shows a table of exposed vulnerabilities by asset. | Report | ArcSight Foundation/Configuration Monitoring/Details/Vulnerabilities/ |
| 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 Vulnerabilities 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 | This filter 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 query counts the vulnerabilities for each asset that is categorized under /All Asset Categories/System Asset Categories/Criticality and returns the ten assets with the most vulnerabilities. | 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/ |

| Resource | Description | Type | URI |
|---|---|-------|---|
| 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/ |
| Exposed Vulnerability Count by Asset | This query counts the vulnerabilities for each asset that is categorized under /All Asset Categories/System Asset Categories/Criticality. | 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 query lists the vulnerabilities for each asset, up to 10,000 asset/vulnerability tuples. | 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/ |

| Resource | Description | Type | URI |
|---|--|-----------------|---|
| 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/ |
| Simple Table Portrait | This template is designed to show a table. The orientation is portrait. | Report Template | ArcSight System/1 Table |
| Simple Table Landscape | This template is designed to show a table. The orientation is landscape. | Report Template | ArcSight System/1 Table |
| Chart and Table Landscape | This template is designed to show one chart and a table. The orientation is landscape. | Report Template | ArcSight System/1 Chart/With Table |
| Simple Chart Landscape | This template is designed to show one chart. The orientation is landscape. | Report Template | ArcSight System/1 Chart/Without Table |
| 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/ |

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

Index

Numerics

- 10 Most Vulnerable Assets in Confidential Data Group query 64
- 10 Most Vulnerable Assets in Confidential Data Group report 60

A

- AAA User Account Creation report 50
- AAA User Account Creation trend 59
- AAA User Account Creation Trend query 55
- AAA User Account Creations filter 52
- AAA User Account Deletions - Last 30 Days report 51
- AAA User Account Deletions filter 53
- AAA User Account Deletions on Trend query 58
- AAA User Account Deletions trend 58
- AAA User Account Deletions Trend query 54
- AAA User Configuration Activity filter 53
- Account Creation by Host - Last Week report 51
- Account Creation by Host on Trend query 55
- Account Creation by Host query 56
- Account Creation by Host trend 58
- Accounts Deleted by Host report 49
- Accounts Deleted by Host Trend query 56
- active lists
 - Assets with Recent Configuration Modifications 20, 25
 - general configuration 12, 13
- Address Spaces asset category 62
- All Device Information is NULL filter 27, 36
- All Events filter 17, 27, 36, 42, 52, 63
- All Exposed Vulnerabilities query 64
- All Exposed Vulnerabilities report 61
- All Revenue Generating Assets query 37
- All Revenue Generating Assets report 33
- All Vulnerabilities in Email and Web Server Assets query 65
- All Vulnerabilities in Email and Web Server Assets report 61
- Anti-Virus Errors query 47
- Anti-Virus Events filter 43
- Application asset category 26, 34
- ArcSight Administration overview 5
- ArcSight Core Security overview 5
- ArcSight Events filter 22, 27, 36, 43, 52
- ArcSight Foundations overview 6
- ArcSight System overview 6
- asset categories
 - Address Spaces 62
 - Application 26, 34
 - Business Role 34, 51
 - Compliance Requirement 42
 - Confidential Data 62
 - Criticality 17, 25, 34, 62
 - Data Role 34
 - Email 34, 62
 - High 17, 63
 - North America 63
 - Open Port 26
 - Operating System 26, 34
 - Port 135 62
 - Port 139 62
 - Port 445 62
 - Protected 62
 - Revenue Generation 34
 - Scanned 25
 - Very High 17, 63
 - Web Server 34, 62
- Asset Startup and Shutdown Event Log - Last Day report 16
- Asset Startup and Shutdown Events - Daily Trend trend 19
- Asset Startup and Shutdown Log - Last Week report 16
- Assets resource group 16
- Assets Restarting Twice or More - Last Week report 16
- Assets with Applications query 38
- Assets with Applications report 34
- Assets with Configuration Changes - Last Day report 24
- Assets with Configuration Changes - Past Week report 24
- Assets with Configuration Modifications- Last 7 Days query 29
- Assets with Configuration Modifications- Last Day query 29
- Assets with Recent Configuration Modifications (Daily) trend 31, 59
- Assets with Recent Configuration Modifications active list 20, 25
- Assets with Recent Configuration Modifications by Vendor and Product query 30, 56
- AV - Failed Updates filter 43
- AV - Found Infected filter 43

B

- Blaster Vulnerable Hosts query 65
- Blaster Vulnerable Hosts report 61
- Business Role asset category 34, 51
- By User Account - Accounts Created query 57
- By User Account - Accounts Created report 50
- By User Account - Accounts Deleted query 56
- By User Account - Accounts Deleted report 50

C

- Chart and Table Landscape report template 19, 31, 39, 48, 58, 66
- Chart and Table Portrait report template 19, 31, 48, 58
- Cisco - IOS Configuration Changed rule 25
- Compliance Requirement asset category 42
- Confidential Data asset category 62
- Configuration
 - Configuration Monitoring Foundation 10
- configuration
 - active lists 12, 13
- Configuration Changes by Type focused report 28, 37, 44
- Configuration Changes by Type report 24, 33, 42
- Configuration Changes by User focused report 28, 37, 43, 44
- Configuration Changes by User report 24, 32, 42
- Configuration Changes by Zone Last Week Trend Query query 29
- Configuration Changes Overview dashboard 20
- Configuration Changes Overview resource group 20
- Configuration Changes per User by Zone Last Week report 49
- Configuration Changes per User Last Week report 50
- Configuration Changes query 30, 38, 46
- Configuration Modifications filter 21, 26, 35, 42, 52
- Configuration Monitoring Foundation
 - Configuration 10
- content packages 7
- Critical Asset Startup and Shutdown Event Log - Last Day report 16
- Critical Asset Startup and Shutdown Trend report 16
- Critical Host Shutdown Detected rule 17
- Critical System Startup and Shutdown Events - By Zone and Asset query 18
- Critical System Startup and Shutdown Events - Daily Trend trend 19
- Critical System Startups and Shutdowns - Trend Query query 18
- Criticality asset category 17, 25, 34, 62
- Current Asset Configurations query 30
- Current Asset Configurations report 25
- CVE - CAN-2003-0605 vulnerability 67

D

- dashboards
 - Configuration Changes Overview 20
 - Database Errors 32
 - Host Configuration Modifications 23
 - Host Problems Overview 32
- data monitors
 - Host Configuration Change Event Counts by Zone 26
 - Host Problem Event Counts by Zone 35
 - Last 10 Database Configuration Changes 20
 - Last 10 Database Errors 34
 - Last 10 Firewall Configuration Changes 21
 - Last 10 Network Configuration Changes 21
 - Last 10 VPN Configuration Changes 21
 - Last 20 Host Configuration Modification Events 26
 - Last 20 Host Problems 34
 - Most Common Host Configuration Change Events 26

- Most Common Host Problem Events 35

- Top 10 Database Errors 35

- Data Role asset category 34
- Database Configuration Changes filter 22
- Database Errors and Warnings (Chart) query 29, 38
- Database Errors and Warnings query 31, 38
- Database Errors and Warnings report 24, 33
- Database Errors dashboard 32
- Database Errors filter 36
- Database Events filter 22, 36, 52
- Device Configuration Changes resource group 23
- Device Configuration Changes use case 22
- Device Vendor AND Product are NULL filter 28, 37
- Device Vendor OR Product is NULL filter 27, 36
- Device Version is NULL filter 27, 36
- DeviceInfo global variable 26, 35

E

- Email asset category 34, 62
- Errors Detected in Anti-Virus Deployment report 41
- Exposed Vulnerabilities - High and Very High Criticality Assets - Trend Query query 66
- Exposed Vulnerabilities - High and Very High Criticality Assets by Zone - Trend Query query 65
- Exposed Vulnerabilities by Asset query 65
- Exposed Vulnerabilities by Asset report 61
- Exposed Vulnerabilities by Zone Trend - Last 90 Days report 60
- Exposed Vulnerabilities by Zone Trend - Last Month report 61
- Exposed Vulnerabilities by Zone Trend - Last Week query 64
- Exposed Vulnerabilities by Zone Trend - Last Week report 61
- Exposed Vulnerability Count by Asset query 65
- Exposed Vulnerability Count by Asset report 61
- Exposed Vulnerability Count by Critical Asset focused report 63

F

- Failed Anti-Virus Updates - Regulated Systems (MSSP) query 46
- Failed Anti-Virus Updates - Regulated Systems (MSSP) report 41
- Failed Anti-Virus Updates - Regulated Systems query 45
- Failed Anti-Virus Updates - Regulated Systems report 41
- Failed Anti-Virus Updates (MSSP) query 46
- Failed Anti-Virus Updates (MSSP) report 41
- Failed Anti-Virus Updates Chart - Regulated Systems (MSSP) query 47
- Failed Anti-Virus Updates Chart - Regulated Systems query 45
- Failed Anti-Virus Updates Chart (MSSP) query 47
- Failed Anti-Virus Updates Chart query 47
- Failed Anti-Virus Updates query 44
- Failed Anti-Virus Updates report 41
- Failed User Account Login Attempts (Yesterday) query 18
- Failed User Account Login Attempts filter 17, 52
- field sets
 - Standard 21
- filters
 - AAA User Account Creations 52

- AAA User Account Deletions 53
 - AAA User Configuration Activity 53
 - All Device Information is NULL 27, 36
 - All Events 17, 27, 36, 42, 52, 63
 - Anti-Virus Events 43
 - ArcSight Events 22, 27, 36, 43, 52
 - AV - Failed Updates 43
 - AV - Found Infected 43
 - Configuration Modifications 21, 26, 35, 42, 52
 - Database Configuration Changes 22
 - Database Errors 36
 - Database Events 22, 36, 52
 - Device Vendor AND Product are NULL 28, 37
 - Device Vendor OR Product is NULL 27, 36
 - Device Version is NULL 27, 36
 - Failed User Account Login Attempts 17, 52
 - Firewall 43
 - Firewall Configuration Changes 21
 - Firewall Events 22, 43
 - High-Priority Scan Event for Critical Asset 63
 - Host Configuration Modifications 28, 36
 - Host IDS 42
 - Host Problems 35
 - Identity Management Events 43, 53
 - Network Configuration Changes 21
 - Network Events 21, 42
 - Network IDS 43
 - Non-ArcSight Events 22, 28, 37, 43, 53
 - Operating System Events 53
 - Router 27
 - Successful Configuration Changes 21
 - Successful Password Changes 52
 - Successful User Account Login Attempts 17
 - Switch 27
 - System Shutdown Events 17
 - System Startup Events 17
 - Target Address is NULL 26, 35
 - Target Host Name is NULL 27, 35
 - Target Information is NULL 27, 36
 - Target Port is NULL 27, 36
 - Target Zone AND Host are NULL 28, 37
 - Target Zone AND Host are NULL but Address is NOT NULL 26, 35
 - Target Zone is NULL 28, 37
 - Target Zone OR Host is NULL 28, 37
 - Update Events 42
 - User Account Creations 52
 - User Account Deletions 53
 - User Account Login Attempts 17, 52
 - User Account Modifications 52
 - Virtual Private Network 27
 - VPN Configuration Changes 21
 - VPN Events 21, 26, 51
 - VPN User Account Creations 53
 - VPN User Configuration Activity 53
 - Firewall Configuration Changes filter 21
 - Firewall Configuration Changes query 45
 - Firewall Configuration Changes report 40
 - Firewall Events filter 22, 43
 - Firewall filter 43
 - Firewall Misconfigurations query 46
 - Firewall Misconfigurations report 41
 - focused reports
 - Configuration Changes by Type 28, 37, 44
 - Configuration Changes by User 28, 37, 43, 44
 - Exposed Vulnerability Count by Critical Asset 63
 - Password Changes 53, 54
 - Password Changes - Last 30 Days 54
 - User Account Creations - Last 30 Days 54
 - User Account Deletions - Last 30 Days 54
 - User Account Modifications - Last 30 Days 53
 - Vulnerability Exposure by Asset Criticality - Last 3 Months 63
 - Vulnerability Exposure by Asset Criticality - Last 6 Months 63
- ## G
- global variables
 - DeviceInfo 26, 35
 - TargetHost 26, 35
- ## H
- HIDS Misconfigurations query 47
 - HIDS Misconfigurations report 41
 - High asset category 17, 63
 - High-Priority Scan Event for Critical Asset filter 63
 - High-Priority Scan Events Directed Toward High-Criticality Assets - Today query viewer 60
 - High-Priority Scan Events Directed Toward High-Criticality Assets - Yesterday query viewer 60
 - High-Priority Scan Events Directed Toward High-Criticality Assets query 64
 - High-Priority Vulnerabilities Detected on Critical Assets - Yesterday query 65
 - High-Priority Vulnerabilities Detected on Critical Assets - Yesterday report 60
 - Host Configuration Change Event Counts by Zone data monitor 26
 - Host Configuration Events By Zone query 38
 - Host Configuration Events By Zone report 33
 - Host Configuration Modifications - Today query viewer 23
 - Host Configuration Modifications - Yesterday query viewer 23
 - Host Configuration Modifications by Customer query 30
 - Host Configuration Modifications by Customer report 24
 - Host Configuration Modifications by OS query 28
 - Host Configuration Modifications by OS report 24
 - Host Configuration Modifications dashboard 23
 - Host Configuration Modifications filter 28, 36
 - Host Configuration Modifications on Trend query 29
 - Host Configuration Modifications query 28
 - Host Configuration Modifications Summary query 30, 38
 - Host Configuration Modifications Summary report 23
 - Host Configuration Modifications trend 31, 39
 - Host IDS filter 42
 - Host Problem Event Counts by Zone data monitor 35
 - Host Problems filter 35
 - Host Problems Overview dashboard 32
 - Host Summary by Business Role query 37
 - Host Summary by Business Role report 33
 - Host Summary by Criticality query 38
 - Host Summary by Criticality report 33
 - Host Summary by Data Role query 37
 - Host Summary by Data Role report 34
 - Host Summary by Operating System query 38
 - Host Summary by Operating System report 33
 - Hosts and Applications Overview resource group 32

I

Identity Management Events filter 43, 53
Infected Systems query 46

L

Last 10 Database Configuration Changes data monitor 20
Last 10 Database Errors data monitor 34
Last 10 Firewall Configuration Changes data monitor 21
Last 10 Network Configuration Changes data monitor 21
Last 10 VPN Configuration Changes data monitor 21
Last 20 Host Configuration Modification Events data monitor 26
Last 20 Host Problems data monitor 34

M

Mail Servers query 38
Mail Servers report 33
Misconfigurations query 28, 30
Misconfigurations report 23, 24
Most Common Account Login Attempts - Daily Trend trend 19
Most Common Account Login Attempts - Last Day query 18
Most Common Account Login Attempts Trend - Last Week query 18
Most Common Account Login Failures by Attacker User (Yesterday) query 56
Most Common Account Login Failures by Attacker User (Yesterday) report 50
Most Common Account Logins by Target User (Yesterday) query 17
Most Common Host Configuration Change Events data monitor 26
Most Common Host Problem Events data monitor 35

N

Network Configuration Changes filter 21
Network Events filter 21, 42
Network IDS filter 43
NIDS Misconfigurations query 45
NIDS Misconfigurations report 42
Non-ArcSight Events filter 22, 28, 37, 43, 53
North America asset category 63

O

Open Port asset category 26
Operating System asset category 26, 34
Operating System Events filter 53

P

packages
 deleting 10
 installing 9
 uninstalling 9
Password Changes - Last 30 Days focused report 54
Password Changes by System report 51
Password Changes by User report 51
Password Changes by Zone report 49
Password Changes focused report 53, 54

Password Changes query 55
Password Changes report 50
Password Modifications trend 59
Password Modifications Trend query 56
Port 135 asset category 62
Port 139 asset category 62
Port 445 asset category 62
Protected asset category 62

Q

queries

10 Most Vulnerable Assets in Confidential Data Group 64
AAA User Account Creation Trend 55
AAA User Account Deletions on Trend 58
AAA User Account Deletions Trend 54
Account Creation by Host 56
Account Creation by Host on Trend 55
Accounts Deleted by Host Trend 56
All Exposed Vulnerabilities 64
All Revenue Generating Assets 37
All Vulnerabilities in Email and Web Server Assets 65
Anti-Virus Errors 47
Assets with Applications 38
Assets with Configuration Modifications- Last 7 Days 29
Assets with Configuration Modifications- Last Day 29
Assets with Recent Configuration Modifications by Vendor and Product 30, 56
Blaster Vulnerable Hosts 65
By User Account - Accounts Created 57
By User Account - Accounts Deleted 56
Configuration Changes 30, 38, 46
Configuration Changes by Zone Last Week Trend Query 29
Critical System Startup and Shutdown Events - By Zone and Asset 18
Critical System Startups and Shutdowns - Trend Query 18
Current Asset Configurations 30
Database Errors and Warnings 31, 38
Database Errors and Warnings (Chart) 29, 38
Exposed Vulnerabilities - High and Very High Criticality Assets - Trend Query 66
Exposed Vulnerabilities - High and Very High Criticality Assets by Zone - Trend Query 65
Exposed Vulnerabilities by Asset 65
Exposed Vulnerabilities by Zone Trend - Last Week 64
Exposed Vulnerability Count by Asset 65
Failed Anti-Virus Updates 44
Failed Anti-Virus Updates - Regulated Systems 45
Failed Anti-Virus Updates - Regulated Systems (MSSP) 46
Failed Anti-Virus Updates (MSSP) 46
Failed Anti-Virus Updates Chart 47
Failed Anti-Virus Updates Chart - Regulated Systems 45
Failed Anti-Virus Updates Chart - Regulated Systems (MSSP) 47
Failed Anti-Virus Updates Chart (MSSP) 47

- Failed User Account Login Attempts (Yesterday) 18
 - Firewall Configuration Changes 45
 - Firewall Misconfigurations 46
 - HIDS Misconfigurations 47
 - High-Priority Scan Events Directed Toward High-Criticality Assets 64
 - High-Priority Vulnerabilities Detected on Critical Assets - Yesterday 65
 - Host Configuration Events By Zone 38
 - Host Configuration Modifications 28
 - Host Configuration Modifications by Customer 30
 - Host Configuration Modifications by OS 28
 - Host Configuration Modifications on Trend 29
 - Host Configuration Modifications Summary 30, 38
 - Host Summary by Business Role 37
 - Host Summary by Criticality 38
 - Host Summary by Data Role 37
 - Host Summary by Operating System 38
 - Infected Systems 46
 - Mail Servers 38
 - Misconfigurations 28, 30
 - Most Common Account Login Attempts - Last Day 18
 - Most Common Account Login Attempts Trend - Last Week 18
 - Most Common Account Login Failures by Attacker User (Yesterday) 56
 - Most Common Account Logins by Target User (Yesterday) 17
 - NIDS Misconfigurations 45
 - Password Changes 55
 - Password Modifications Trend 56
 - Restart Log by Zone - Last Week 18
 - Router Configuration Changes 29
 - Switch Configuration Changes 29
 - System Startups and Shutdowns 18
 - Systems Restarted Twice or More - Last Week 18
 - Systems With Criticality Ratings by Zone 29
 - Top 10 Assets by Exposed Vulnerability Counts 64
 - Top 10 Exposed Vulnerabilities by Asset Counts 64
 - Top Anti-Virus Errors 48
 - Top Infected Systems 46
 - Top Vulnerability Exposure of Critical Assets on Trend 65
 - Top Zones with Anti-Virus Errors 45
 - Trend on AAA User Account Creation 54
 - Trend on Password Modifications 55
 - Trend on User Account Creation 57
 - Trend on User Account Modifications 57
 - Trend on VPN User Account Creation 57
 - Update Overview - Regulated Systems (MSSP) 48
 - Update Overview (MSSP) 45
 - Update Overview Chart - Regulated Systems (MSSP) 47
 - Update Overview Chart (MSSP) 46
 - Update Summary 46
 - Update Summary - Regulated Systems 45
 - Update Summary Chart 48
 - Update Summary Chart - Regulated Systems 47
 - User Account Creation Trend 55
 - User Account Login Failures - Weekly Trend 18
 - User Account Modifications Trend 57
 - User Administration 58
 - User Administration (Chart) 57
 - User Configuration Modifications 56
 - User Removals 55
 - User Removals on Trend 55
 - Users That Performed Configuration Modifications Past Week 57
 - VPN Configuration Changes 29
 - VPN User Account Creation Trend 54
 - Vulnerabilities of Assets in North America 64
 - Vulnerability Exposure by Asset Criticality 65
 - Vulnerability Exposure by Asset Criticality - Trend Query - Snapshot 63
 - Vulnerability Exposure of Critical Assets on Trend 64
 - Web Servers 37
- query viewers
- High-Priority Scan Events Directed Toward High-Criticality Assets - Today 60
 - High-Priority Scan Events Directed Toward High-Criticality Assets - Yesterday 60
 - Host Configuration Modifications - Today 23
 - Host Configuration Modifications - Yesterday 23
 - User Configuration Modifications - Today 49
 - User Configuration Modifications - Yesterday 49
- ## R
- report templates
- Chart and Table Landscape 19, 31, 39, 48, 58, 66
 - Chart and Table Portrait 19, 31, 48, 58
 - Simple Chart Landscape 66
 - Simple Chart Portrait 39
 - Simple Table Landscape 31, 58, 66
 - Simple Table Portrait 19, 31, 38, 48, 58, 66
 - Two Charts One Table Landscape 48
- reports
- 10 Most Vulnerable Assets in Confidential Data Group 60
 - AAA User Account Creation 50
 - AAA User Account Deletions - Last 30 Days 51
 - Account Creation by Host - Last Week 51
 - Accounts Deleted by Host 49
 - All Exposed Vulnerabilities 61
 - All Revenue Generating Assets 33
 - All Vulnerabilities in Email and Web Server Assets 61
 - Asset Startup and Shutdown Event Log - Last Day 16
 - Asset Startup and Shutdown Log - Last Week 16
 - Assets Restarting Twice or More - Last Week 16
 - Assets with Applications 34
 - Assets with Configuration Changes - Last Day 24
 - Assets with Configuration Changes - Past Week 24
 - Blaster Vulnerable Hosts 61
 - By User Account - Accounts Created 50
 - By User Account - Accounts Deleted 50
 - Configuration Changes by Type 24, 33, 42
 - Configuration Changes by User 24, 32, 42
 - Configuration Changes per User by Zone Last Week 49
 - Configuration Changes per User Last Week 50
 - Critical Asset Startup and Shutdown Event Log - Last Day 16
 - Critical Asset Startup and Shutdown Trend 16
 - Current Asset Configurations 25
 - Database Errors and Warnings 24, 33
 - Errors Detected in Anti-Virus Deployment 41

- Exposed Vulnerabilities by Asset 61
 - Exposed Vulnerabilities by Zone Trend - Last 90 Days 60
 - Exposed Vulnerabilities by Zone Trend - Last Month 61
 - Exposed Vulnerabilities by Zone Trend - Last Week 61
 - Exposed Vulnerability Count by Asset 61
 - Failed Anti-Virus Updates 41
 - Failed Anti-Virus Updates - Regulated Systems 41
 - Failed Anti-Virus Updates - Regulated Systems (MSSP) 41
 - Failed Anti-Virus Updates (MSSP) 41
 - Firewall Configuration Changes 40
 - Firewall Misconfigurations 41
 - HIDS Misconfigurations 41
 - High-Priority Vulnerabilities Detected on Critical Assets - Yesterday 60
 - Host Configuration Events By Zone 33
 - Host Configuration Modifications by Customer 24
 - Host Configuration Modifications by OS 24
 - Host Configuration Modifications Summary 23
 - Host Summary by Business Role 33
 - Host Summary by Criticality 33
 - Host Summary by Data Role 34
 - Host Summary by Operating System 33
 - Mail Servers 33
 - Misconfigurations 23, 24
 - Most Common Account Login Failures by Attacker User (Yesterday) 50
 - NIDS Misconfigurations 42
 - Password Changes 50
 - Password Changes by System 51
 - Password Changes by User 51
 - Password Changes by Zone 49
 - Router Configuration Changes 25
 - Switch Configuration Changes 25
 - Systems With Criticality Ratings by Zone 24
 - Top 10 Assets by Exposed Vulnerability Counts 61
 - Top 10 Exposed Vulnerabilities by Asset Counts 61
 - Top Infected Systems 42
 - Top User Logins - Last Week 16
 - Top User Logins - Yesterday 17
 - Top Vulnerability Exposure of Critical Assets 62
 - Update Overview - Regulated Systems (MSSP) 42
 - Update Overview (MSSP) 40
 - Update Summary 41
 - Update Summary - Regulated Systems 40
 - User Account Creation 51
 - User Account Modifications 50
 - User Administration 51
 - User Login Failures Trend - Past Week 16
 - User Removals - Last 30 Days 50
 - VPN Configuration Changes 24
 - VPN User Account Creation 50
 - Vulnerabilities of Assets in North America 62
 - Vulnerability Exposure by Asset Criticality - Current Month 61
 - Web Servers 33
 - Zones by Configuration Change Count Past Week 23
 - resource groups
 - Assets 16
 - Configuration Changes Overview 20
 - Device Configuration Changes 23
 - Hosts and Applications Overview 32
 - Security Application and Device Configuration Changes 40
 - User Configuration Changes 49
 - Vulnerabilities 60
 - Restart Log by Zone - Last Week query 18
 - Revenue Generation asset category 34
 - Router Configuration Changes query 29
 - Router Configuration Changes report 25
 - Router filter 27
 - rules
 - Cisco - IOS Configuration Changed 25
 - Critical Host Shutdown Detected 17
 - Successful Configuration Change 20
 - Warning - Insecure Configuration 62
 - Warning - Vulnerable Software 62
- ## S
- Scanned asset category 25
 - Security Application and Device Configuration Changes resource group 40
 - Security Application and Device Configuration Changes use case 22
 - shared libraries 6
 - Simple Chart Landscape report template 66
 - Simple Chart Portrait report template 39
 - Simple Table Landscape report template 31, 58, 66
 - Simple Table Portrait report template 19, 31, 38, 48, 58, 66
 - Standard field set 21
 - Successful Configuration Change rule 20
 - Successful Configuration Changes filter 21
 - Successful Password Changes filter 52
 - Successful User Account Login Attempts filter 17
 - Switch Configuration Changes query 29
 - Switch Configuration Changes report 25
 - Switch filter 27
 - System Shutdown Events filter 17
 - System Startup Events filter 17
 - System Startups and Shutdowns query 18
 - Systems Restarted Twice or More - Last Week query 18
 - Systems With Criticality Ratings by Zone query 29
 - Systems With Criticality Ratings by Zone report 24
- ## T
- Target Address is NULL filter 26, 35
 - Target Host Name is NULL filter 27, 35
 - Target Information is NULL filter 27, 36
 - Target Port is NULL filter 27, 36
 - Target Zone AND Host are NULL but Address is NOT NULL filter 26, 35
 - Target Zone AND Host are NULL filter 28, 37
 - Target Zone is NULL filter 28, 37
 - Target Zone OR Host is NULL filter 28, 37
 - TargetHost global variable 26, 35
 - Top 10 Assets by Exposed Vulnerability Counts query 64
 - Top 10 Assets by Exposed Vulnerability Counts report 61
 - Top 10 Database Errors data monitor 35
 - Top 10 Exposed Vulnerabilities by Asset Counts query 64
 - Top 10 Exposed Vulnerabilities by Asset Counts report 61
 - Top Anti-Virus Errors query 48
 - Top Infected Systems query 46
 - Top Infected Systems report 42

Top User Logins - Last Week report 16
 Top User Logins - Yesterday report 17
 Top Vulnerability Exposure of Critical Assets on Trend query 65
 Top Vulnerability Exposure of Critical Assets report 62
 Top Vulnerability Exposure of Critical Assets trend 67
 Top Zones with Anti-Virus Errors query 45
 Trend on AAA User Account Creation query 54
 Trend on Password Modifications query 55
 Trend on User Account Creation query 57
 Trend on User Account Modifications query 57
 Trend on VPN User Account Creation query 57
 trends
 AAA User Account Creation 59
 AAA User Account Deletions 58
 Account Creation by Host 58
 Asset Startup and Shutdown Events - Daily Trend 19
 Assets with Recent Configuration Modifications (Daily) 31, 59
 Critical System Startup and Shutdown Events - Daily Trend 19
 Host Configuration Modifications 31, 39
 Most Common Account Login Attempts - Daily Trend 19
 Password Modifications 59
 Top Vulnerability Exposure of Critical Assets 67
 User Account Creation 59
 User Account Login Failures 19
 User Account Modifications 59
 User Removals 58
 VPN User Account Creation 59
 Vulnerability Exposure by Asset Criticality 66
 Vulnerability Exposure of Critical Assets 67
 Vulnerability Exposure of High and Very-High Criticality Assets by Zone - Daily Trend 66
 Two Charts One Table Landscape report template 48

U

Update Events filter 42
 Update Overview - Regulated Systems (MSSP) query 48
 Update Overview - Regulated Systems (MSSP) report 42
 Update Overview (MSSP) query 45
 Update Overview (MSSP) report 40
 Update Overview Chart - Regulated Systems (MSSP) query 47
 Update Overview Chart (MSSP) query 46
 Update Summary - Regulated Systems query 45
 Update Summary - Regulated Systems report 40
 Update Summary Chart - Regulated Systems query 47
 Update Summary Chart query 48
 Update Summary query 46
 Update Summary report 41
 use cases
 Device Configuration Changes 22
 Security Application and Device Configuration Changes 22
 User Configuration Changes 22
 User Account Creation report 51
 User Account Creation trend 59
 User Account Creation Trend query 55
 User Account Creations - Last 30 Days focused report 54
 User Account Creations filter 52
 User Account Deletions - Last 30 Days focused report 54

User Account Deletions filter 53
 User Account Login Attempts filter 17, 52
 User Account Login Failures - Weekly Trend query 18
 User Account Login Failures trend 19
 User Account Modifications - Last 30 Days focused report 53
 User Account Modifications filter 52
 User Account Modifications report 50
 User Account Modifications trend 59
 User Account Modifications Trend query 57
 User Administration (Chart) query 57
 User Administration query 58
 User Administration report 51
 User Configuration Changes resource group 49
 User Configuration Changes use case 22
 User Configuration Modifications - Today query viewer 49
 User Configuration Modifications - Yesterday query viewer 49
 User Configuration Modifications query 56
 User Login Failures Trend - Past Week report 16
 User Removals - Last 30 Days report 50
 User Removals on Trend query 55
 User Removals query 55
 User Removals trend 58
 Users That Performed Configuration Modifications Past Week query 57

V

Very High asset category 17, 63
 Virtual Private Network filter 27
 VPN Configuration Changes filter 21
 VPN Configuration Changes query 29
 VPN Configuration Changes report 24
 VPN Events filter 21, 26, 51
 VPN User Account Creation report 50
 VPN User Account Creation trend 59
 VPN User Account Creation Trend query 54
 VPN User Account Creations filter 53
 VPN User Configuration Activity filter 53
 vulnerabilities
 CVE - CAN-2003-0605 67
 Vulnerabilities of Assets in North America query 64
 Vulnerabilities of Assets in North America report 62
 Vulnerabilities resource group 60
 Vulnerability Exposure by Asset Criticality - Current Month report 61
 Vulnerability Exposure by Asset Criticality - Last 3 Months focused report 63
 Vulnerability Exposure by Asset Criticality - Last 6 Months focused report 63
 Vulnerability Exposure by Asset Criticality - Trend Query - Snapshot query 63
 Vulnerability Exposure by Asset Criticality query 65
 Vulnerability Exposure by Asset Criticality trend 66
 Vulnerability Exposure of Critical Assets on Trend query 64
 Vulnerability Exposure of Critical Assets trend 67
 Vulnerability Exposure of High and Very-High Criticality Assets by Zone - Daily Trend trend 66

W

Warning - Insecure Configuration rule 62

Warning - Vulnerable Software rule 62
Web Server asset category 34, 62
Web Servers query 37
Web Servers report 33

Z

Zones by Configuration Change Count Past Week report
23