Standard Content Guide

NetFlow Monitoring 1.1

for ArcSight ESM 5.5

March 1, 2013

ArcSight™
An HP Company

Standard Content Guide - NetFlow Monitoring 1.1

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.arcsight.com/copyrightnotice

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

This document is confidential.

Revision History

Date	Product Version	Description
03/01/2013	NetFlow Monitoring 1.1	Final revision for release.

Document template version: 1.0.5

Contact Information

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

Contents

Chapter 1

NetFlow Monitoring Overview

This chapter discusses the following topics.

What is Standard Content?

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

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

Standard content consists of the following:

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

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

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

Standard Content Packages

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

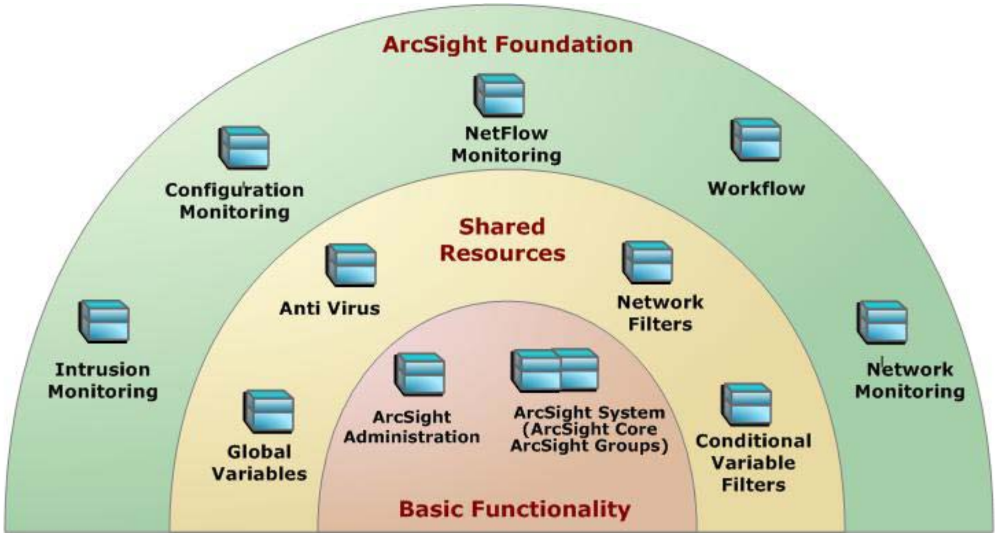


Figure 1-1 The ArcSight System and ArcSight Administration packages at the base provide content required for basic ArcSight functionality. The common packages in the center contain shared resources that support ArcSight Administration and the ArcSight Foundation packages. The packages shown on top are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

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

Note

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

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*.

NetFlow Monitoring Content

NetFlow is a network protocol developed by Cisco Systems to run on Cisco IOS-enabled equipment for collecting IP traffic information. It is proprietary, but supported by platforms other than Cisco IOS, such as Juniper routers and Linux.

NetFlow provides session-level data. Leveraging this information using ESM can help to monitor network bandwidth usage and correlate it with other security logs (such as firewall, IDS, authentication logs, and so on).

The NetFlow Monitoring content provides resources to monitor and report on top bandwidth usage by source, destination and port.

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

Chapter 2

Installation and Configuration

This chapter discusses the following topics.

For information about upgrading standard content, see Appendix A, Upgrading Standard Content, on page 23.

Installing the NetFlow Monitoring Package

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

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

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

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

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

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

To uninstall a package that is installed:

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

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

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

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

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

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

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

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

The package is removed from the Navigator panel package view.

Configuring NetFlow Monitoring Content

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

- "Setting Up SmartConnectors and Modeling the Network" on page 10
- "Categorizing Assets" on page 11
- "Ensuring Filters Capture Relevant Events" on page 12
- "Scheduling Reports" on page 12
- "Restricting Access to Vulnerability View Reports" on page 12
- "Configuring Trends" on page 13

Setting Up SmartConnectors and Modeling the Network

Configuring NetFlow Monitoring content starts with installing SmartConnectors and configuring zones and networks for devices that report to ESM. The NetFlow Monitoring content is triggered by NetFlow events from the following SmartConnectors:

SmartConnector	Device Version Supported
ArcSight IP Flow SmartConnector	• Cisco NetFlow versions 5 and 9 • Flexible NetFlow from IOS 15.0 • Cisco ASA 8.2, and Juniper Networks J-Flow versions 5 and 9
ArcSight QoSient ARGUS SmartConnector	• QoSient ARGUS versions 2 and 3

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

There are several ways to model your network. For information about populating the network model, refer to the *ArcSight Console User's Guide* or the ESM online Help. To learn more about the architecture of the ESM network modeling tools, refer to the *ESM 101* guide*.*

Categorizing Assets

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

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

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

Note

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

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

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

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

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

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

Ensuring Filters Capture Relevant Events

Standard content relies on specific event field values to identify events of interest. Although this method applies to most of the events and devices, be sure to test key filters to verify that they actually capture the required events. For NetFlow Monitoring, follow the procedure below to make sure that the NetFlow Traffic Reporting Devices filter captures relevant 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 ESM by viewing them in an active channel or query viewer.
2. Navigate to the **NetFlow Traffic Reporting Devices** 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.

Scheduling Reports

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

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

Restricting Access to Vulnerability View Reports

The Vulnerability View detail reports display a list of vulnerabilities generated by scanner report events, and are therefore considered sensitive material. By default, the reports are configured with read access for Administrators, Default User Groups, and Analyzer Administrators. Administrators and Analyzer Administrators also have write access to this group.

To eliminate these events from view, you have to create a special filter and apply it to the appropriate users groups. When restricting access to the Vulnerability View reports, be aware of the following:

- Because access is inherited, the parent group must have the same or more liberal permissions than the vulnerability reports.
- If you need to move the reports to a group with tighter permissions, also move the trends and queries that support them, in both the Detail and Operational Summaries sections.
- To get a complete view of the resources attached to these reports, run a resource graph on the individual filters or the parent group (right-click the resource or group and select **Graph View**).

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.

NetFlow Monitoring content includes several trends, which are all enabled by default.

To disable a trend, go to the Navigator panel, right-click the trend you want to disable and select **Disable Trend**.

Caution

To enable a disabled trend, you must first **change the default start date** in the Trend editor.

If the start date is not changed, the trend takes the default start date (derived from when the trend was first installed), and backfills the data from that time. For example, if you enable the trend six months after the first install, these trends try to get all the data for the last six months, which might cause performance problems, overwhelm system resources, or cause the trend to fail if that event data is not available.

For more information about trends, refer to the the *ArcSight Console User's Guide* or the ESM online Help.

Adjusting Trend Schedules

NetFlow Monitoring content contains five trends. Four of the trends are trend-on-trends, which all collect data from a single base trend (`Top Bandwidth Usage Events`). Do not schedule the four trend-on-trends to run before the base trend completes its daily query run. By default, the trends are scheduled to run daily at the times indicated below:

Trend Name	Scheduled run time
Top Bandwidth Usage by Destination	3:33:36 AM
Top Bandwidth Usage by Hour	2:40:34 AM
Top Bandwidth Usage by Port	3:15:50 AM
Top Bandwidth Usage by Source	3:07:08 AM
Top Bandwidth Usage Events (base trend)	1:15:09 AM

By default, each trend uses midnight of the date the package was installed as the date and time the trend will start collecting information. To adjust the schedule or start date/time for the trend, edit the values in the **Schedule** tab of the Inspect/Edit panel for the trend.

Configuring the TotalBytes Variable

SmartConnectors can be configured to aggregate events and sum the counts in fields, such as `bytesIn` and `bytesOut`. SmartConnectors also set the aggregated event count. By default, ESM interprets the count in fields such as `bytesIn` and `bytesOut` as an average, and if the SmartConnector is configured to sum certain fields, ESM multiplies those summed fields by aggregated event count, which creates an inaccurate value. By default, the NetFlow Monitoring content compensates for this by dividing the `bytesIn` and `bytesOut` fields by aggregated event count using the `TotalBytes` variable.

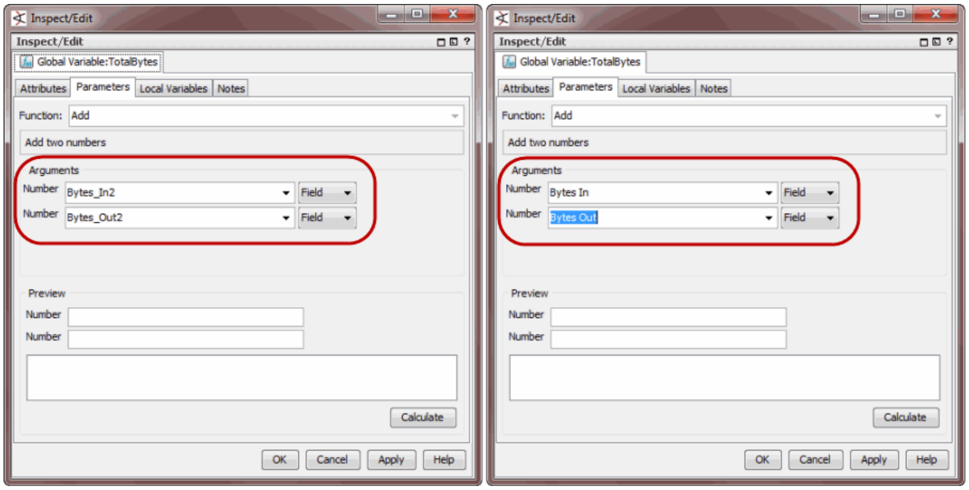
The Connector Summation Fields property is an ESM configuration option that enables you to indicate which fields are sums, so that ESM can report the correct value without requiring that content compensate by adding a divide-by-aggregated-count function.

For example, the `connector.summation.fields=bytesIn,bytesOut` property added to the `server.properties` file on the ESM Manager indicates that the `bytesIn` and `bytesOut` fields coming from the SmartConnector are sums, and therefore exempts those fields from being multiplied by aggregated event count. If this property is set in your ESM installation, you must configure the NetFlow Monitoring content that uses the `TotalBytes` variable to use a variable that will add the values, not multiply them.

To configure the TotalBytes global variable:

1. From the **Resources** tab in the Navigator panel, go to **Field Sets**.
2. Click the **Fields & Global Variables** tab and navigate to `ArcSight Foundation/Variables Library/TotalBytes`.
3. Right-click `TotalBytes` and select **Edit Field**.

   The global variable displays in the Inspect/Edit panel.
4. Click the Parameters tab and change the arguments from `BytesIn_2` and `BytesOut_2` to `Bytes_In` and `Bytes_Out`, as shown in the following figure.



Global Variable:TotalBytes

Function: Add

Add two numbers

Arguments
Number Bytes_In2 Field
Number Bytes_Out2 Field

Global Variable:TotalBytes

Function: Add

Add two numbers

Arguments
Number Bytes In Field
Number Bytes Out Field

For information about the `server.properties` file on the ESM Manager, refer to the *ArcSight ESM Administrator’s Guide*.

For instructions about how to configure a SmartConnector to aggregate and sum on fields, such as `bytesIn` and `bytesOut`, and `targetPort`, refer to the *ArcSight SmartConnector User’s Guide*.

Chapter 3

NetFlow Monitoring Content

The NetFlow Monitoring content contains resources that:

- Monitor, investigate, and report on bandwidth usage by source, destination, and port.
- Monitor the bandwidth moving average and identify top bandwidth usage by source, destination, and port.
- Report on bandwidth usage in daily or weekly increments using trends and by source, destination, and port.

You can use this information to build correlation content; for example, you can build a rule that correlates NetFlow events with other security logs, such as firewall or IDS logs.

Configuration

Refer to "Configuring NetFlow Monitoring Content" on page 10 for general content configuration.

Devices

The following device types can supply events that apply to the NetFlow Monitoring resources:

- Network devices with NetFlow enabled

Resources

The following table lists the information presentation and data processing resources in the NetFlow Monitoring content.

Table 3-1 Resources in the NetFlow Monitoring Content

Resource	Description	Type	URI
Monitor Resources			
Top NetFlow Bandwidth Usage Monitoring	This dashboard shows the top bandwidth usage as reported by NetFlow events, showing top bandwidth usage by source, destination, well known port, and non well known port.	Dashboard	ArcSight Foundation/NetFlow Monitoring/

Resource	Description	Type	URI
NetFlow Bandwidth Usage Overview	This dashboard shows an overview of bandwidth usage reported by NetFlow events. The report displays the top bandwidth usage events, and the inbound and outbound bandwidth moving average.	Dashboard	ArcSight Foundation/NetFlow Monitoring/
List of Top Bandwidth Usage Events	This query viewer displays the top ten bandwidth usage events and contains several drilldowns for investigation.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Well-Known Port	This query viewer displays the top ten well known destination ports, and the total bytes from NetFlow events, sorted by bytes. This query viewer contains several drilldowns for investigation.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source-Destination Pairs and Port	This query viewer displays the top ten source addresses, destination addresses, destination ports, counts, and total bytes from NetFlow events, sorted by bytes.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination	This query viewer displays the top ten destination addresses, and the total bytes from NetFlow events, sorted by bytes. This query viewer contains several drilldowns for investigation.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Non-Well-Known Port	This query viewer displays the top ten non well known destination ports, and the total bytes from NetFlow events, sorted by bytes. This query viewer contains several drilldowns for investigation.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source-Destination Pairs	This query viewer displays the top ten source addresses, destination addresses, and the total bytes from NetFlow events, sorted by bytes.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source	This query viewer displays the top ten source addresses and the total bytes from NetFlow events, sorted by bytes. This query viewer contains several drilldowns for investigation.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source and Port	This query viewer displays the top ten source addresses, destination ports, flow counts, and total bytes from NetFlow events, sorted by bytes.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/

Resource	Description	Type	URI
Top Bandwidth Usage by Destination and Port	This query viewer displays the top ten destination addresses, destination ports, flow counts, and total bytes from NetFlow events, sorted by bytes.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage Weekly Report	This report displays the bandwidth usage, the top bandwidth usage by source, the top bandwidth usage by destination, and the top bandwidth usage by port. The default time range for this report is the past seven days.	Report	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination Port	This report displays top bandwidth usage by destination port. The default time range for this report is yesterday.	Report	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source	This report displays top bandwidth usage by source. The default time range for this report is yesterday.	Report	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination	This report displays top bandwidth usage by destination. The default time range for this report is yesterday.	Report	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage Daily Report	This report displays an hourly chart showing the bandwidth usage, a chart showing the top bandwidth usage by source, a chart showing the top bandwidth usage by destination, and a chart showing the top bandwidth usage by port. The default time range for this report is yesterday.	Report	ArcSight Foundation/NetFlow Monitoring/
Library Resources			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Outbound Bandwidth (Bytes Per Second)	This data monitor shows the average outbound bandwidth (bytes/sec) for the last hour. The values are updated every five minutes.	Data Monitor	ArcSight Foundation/NetFlow Monitoring/
Inbound Bandwidth (Bytes Per Second)	This data monitor shows the average inbound bandwidth (bytes/sec) for the last hour. The values are updated every five minutes.	Data Monitor	ArcSight Foundation/NetFlow Monitoring/
TotalBytes	This variable sums the values of Bytes In and Bytes Out for each event.	Global Variable	ArcSight Foundation/Variables Library/

Resource	Description	Type	URI
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Inbound NetFlow Traffic	This filter identifies NetFlow events coming from external sources targeting the internal network.	Filter	ArcSight Foundation/NetFlow Monitoring/
Outbound Events	This filter identifies events originating from inside the company network, targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters/
Outbound NetFlow Traffic	This filter identifies NetFlow events coming from internal sources targeting the external network.	Filter	ArcSight Foundation/NetFlow Monitoring/
Bytes Out is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Bytes Out is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Bytes/
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
QoSient Argus Events	This filter identifies events from Argus SmartConnectors.	Filter	ArcSight Foundation/NetFlow Monitoring/
Bytes In is NULL	This filter is designed for conditional expression variables. The filter identifies events in which the Bytes In is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Bytes/
NetFlow Traffic Reporting Devices	This filter identifies NetFlow traffic reporting devices. By default, the filter contains QoSient Argus, NetFlow V5, and NetFlow V9 events.	Filter	ArcSight Foundation/NetFlow Monitoring/
External Target	This filter identifies events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
NetFlow V9 Events	This filter identifies NetFlow version 9 events.	Filter	ArcSight Foundation/NetFlow Monitoring/
Inbound Events	This filter identifies events coming from the outside network targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters/
Non-Well-Known Ports	This filter identifies events in which the Target Port is not NULL and is greater than 1024.	Filter	ArcSight Foundation/NetFlow Monitoring/

Resource	Description	Type	URI
NetFlow V5 Events	This filter identifies NetFlow version 5 events.	Filter	ArcSight Foundation/NetFlow Monitoring/
Well-Known Ports	This filter identifies events in which the Target Port is not NULL and is less than or equal to 1024.	Filter	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source-Destination Pairs	This query returns the source address, destination address, flow counts, and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour.	Query	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination - Trend on Trend	This query identifies the destination address, destination zone, flow counts, and total bytes from the Top Bandwidth Usage by Destination trend.	Query	ArcSight Foundation/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Source	This query returns the source address and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour.	Query	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Hour - Trend on Trend	This query returns bandwidth usage information by hour from the Top Bandwidth Usage by Hour trend.	Query	ArcSight Foundation/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Source and Port	This query identifies the source address, destination port, flow counts, and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour.	Query	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination	This query identifies the destination address and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour.	Query	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage Events	This query identifies the source address, destination address, destination port, flow counts, and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour. This query is used by the Top Bandwidth Usage Events trend.	Query	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Day - Trend on Trend	This query identifies the bandwidth usage information by day from the Top Bandwidth Usage by Hour trend.	Query	ArcSight Foundation/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Port - Trend	This query identifies the destination port, flow counts, and total bytes from the trend Top Bandwidth Usage Events.	Query	ArcSight Foundation/NetFlow Monitoring/Trend/

Resource	Description	Type	URI
Top Bandwidth Usage by Well-Known Port	This query returns the destination port and total bytes (Bytes In + Bytes Out) from NetFlow events in which the destination port is well-known in the last hour.	Query	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Hour - Trend	This query returns bandwidth usage information by hour from the Top Bandwidth Usage Events trend.	Query	ArcSight Foundation/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Port - Trend on Trend	This query identifies the target Port, flow counts, and total bytes from the Top Bandwidth Usage by Port trend.	Query	ArcSight Foundation/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Destination and Port	This query identifies the destination address, destination port, flow counts, and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour.	Query	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source - Trend	This query returns the source address, source zone, and total bytes from the Top Bandwidth Usage Events trend.	Query	ArcSight Foundation/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Non-Well-Known Port	This query returns the destination port and total bytes (Bytes In + Bytes Out) from NetFlow events in which the destination port is not well-known within the last hour.	Query	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination - Trend	This query identifies the destination address, destination zone, flow counts, and total bytes from the Top Bandwidth Usage Events trend.	Query	ArcSight Foundation/NetFlow Monitoring/Trend/
List of Top Bandwidth Usage Events	This query returns the source address, destination address, destination port, flow counts, and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour.	Query	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source-Destination Pairs and Port	This query identifies the source address, destination address, destination port, flow counts, and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour.	Query	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source - Trend on Trend	This query returns the source address, source zone, and total bytes from the Top Bandwidth Usage by Source trend.	Query	ArcSight Foundation/NetFlow Monitoring/Trend/

Resource	Description	Type	URI
Top Bandwidth Usage by Hour	This trend stores hourly information of top bandwidth usage, which includes the end time hour, flow counts, and total bytes. This trend depends on the /All Trends/ArcSight Foundation/NetFlow Monitoring/Top Bandwidth Usage Events trend.	Trend	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage Events	This trend stores bandwidth usage information reported by NetFlow, which contains the end time hour, source address, source zone, destination address, destination zone, destination port, flow counts, and total bytes. This trend is the base trend, collecting a broad amount of aggregated NetFlow data for a short period of time, that is to be used by several other trends to further aggregate data and store for a longer period of time. The default retention period for this trend is eight days.	Trend	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source	This trend stores top bandwidth usage information by source, which includes source address, source zone, flow counts, and total bytes. This trend depends on the /All Trends/ArcSight Foundation/NetFlow Monitoring/Top Bandwidth Usage Events trend.	Trend	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination	This trend stores top bandwidth usage information by destination, which includes destination address, destination zone, flow counts, and total bytes. This trend depends on the /All Trends/ArcSight Foundation/NetFlow Monitoring/Top Bandwidth Usage Events trend.	Trend	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Port	This trend stores top bandwidth usage information by port, which includes destination port, flow counts, and total bytes. This trend depends on the /All Trends/ArcSight Foundation/NetFlow Monitoring/Top Bandwidth Usage Events trend.	Trend	ArcSight Foundation/NetFlow Monitoring/

Appendix A

Upgrading Standard Content

This appendix discusses the following topics.

Preparing Existing Content for Upgrade

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

Configurations Preserved During Upgrade

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

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

Configurations that Require Restoration After Upgrade

The following resource configurations require restoration after upgrade.

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

Backing Up Existing Resources Before Upgrade

Tip

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

During the upgrade process, the content is run through a resource validator automatically (see "Fixing Invalid Resources" on page 25).

To help the process of reconfiguring resources that require restoration after upgrade, back up the resources you identify in "Configurations that Require Restoration After Upgrade" on page 23 and export them in a package. After upgrade, you can re-import the package and use the existing resources as a reference for restoring the configurations to the upgraded environment.

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

1 For each resource type (filter, rule, active list), create a new group under your personal group. Provide a name that identifies the contents.

- Right-click your group name and select **New Group**.

2 Copy the resources into the new group. Repeat this process for every resource type you want to back up.

- Select the resources you want to back up and drag them into the backup folder you created in Step 1. In the *Drag & Drop Options* dialog box, select **Copy**.

3 Export the backup groups in a package.

- In the Navigator panel Packages tab, right-click your group name and select **New Package**. In the Packages editor in the Inspect/Edit panel, name the package to identify the contents.

Tip

Copy and paste configurations from the old resources to the new

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

Performing the Upgrade

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

Checking and Restoring Content After Upgrade

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

Verifying and Reapplying Configurations

Verify and restore standard content after upgrade.

1. Verify that your configured resources listed in the section "Configurations Preserved During Upgrade" on page 23 retained their configurations as expected.

2. Reconfigure the resources that require restoration.

   a. Re-import the package you created in "Backing Up Existing Resources Before Upgrade" on page 24.

   b. One resource at a time, copy and paste the configurations preserved in the package of copied resources into the new resources installed with the upgrade. Copying your configurations one resource at a time instead of overwriting the new resources with the old ensures that you retain your configurations without overwriting any improvements provided with the upgraded content.

Verifying Customized Content

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

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

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

Fixing Invalid Resources

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

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

- Zones

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

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

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

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

Caution

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

Index