



HP ArcSight ESM

Software Version: 6.8c

NetFlow Monitoring Standard Content Guide

November 17, 2014

Legal Notices

Warranty

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.

The information contained herein is subject to change without notice.

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

HP ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

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.

Copyright Notice

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

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

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

Support

Contact Information

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

Contents

Chapter 1: NetFlow Monitoring Overview	4
What is Standard Content?	4
Standard Content Packages	6
NetFlow Monitoring Content	7
Chapter 2: Installation and Configuration	8
Installing the NetFlow Monitoring Package	8
Modeling the Network	9
Categorizing Assets	10
Ensuring Filters Capture Relevant Events	11
Scheduling Reports	11
Restricting Access to Vulnerability View Reports	11
Configuring Trends	12
Adjusting Trend Schedules	12
Configuring the TotalBytes Variable	13
Viewing a Use Case Resource	14
Chapter 3: NetFlow Monitoring Use Case	15
Devices	15
NetFlow Monitoring Resources	15
Send Documentation Feedback	26

Chapter 1: NetFlow Monitoring Overview

This chapter discusses the following topics.

What is Standard Content?	4
Standard Content Packages	6
NetFlow Monitoring Content	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 the CORR-Engine (Correlation Optimized Retention and Retrieval) and provides information on the health of the CORR-Engine.

Note: The ArcSight Admin DB CORR content package is installed automatically when you perform a new ArcSight Manager installation. However package installation is different during upgrade. If you are upgrading your system from a previous version, check to see if the package is installed after upgrade. If the package is not installed, install it from the ArcSight Console.

- ArcSight Content Management is an optional package that shows information about content package synchronization with the ArcSight Content Management feature. The information

includes a history of content packages synchronized from a primary source to multiple destinations, and any common issues or errors encountered. You can install this package during ArcSight Manager installation or from the ArcSight Console any time after installation.

- ArcSight ESM HA Monitoring is an optional package that lets you monitor systems that use the ESM High Availability Module. You can install this package during ArcSight Manager 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 Search Filters content package is installed automatically when you perform a new ArcSight Manager installation. However package installation is different during upgrade. If you are upgrading your system from a previous version, check to see if the package is installed after upgrade. If the package is not installed, install it from the ArcSight Console.

- **ArcSight System** content is installed automatically with the ArcSight Manager and consists of three packages: ArcSight Core, ArcSight Groups, and ArcSight Networks. ArcSight Core and ArcSight Groups contain 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. The ArcSight Networks package contains the zones that were in the ArcSight Core package in previous releases, in addition to local and global network resources.
- **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 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

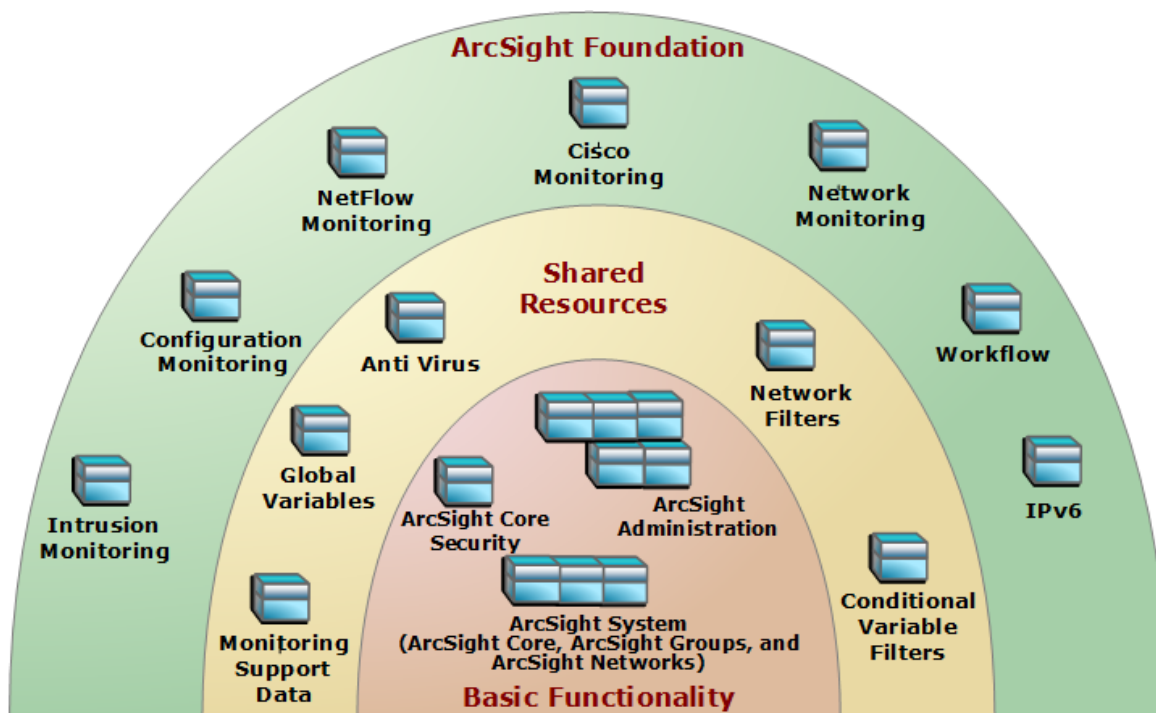
commonly used timestamp formats. The Global Variables are used by ArcSight Administration and certain ArcSight Foundations.

- 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 install-time options. The following graphic outlines the packages.



The ArcSight Core Security, ArcSight Administration, and ArcSight System packages at the base provide content required for basic 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. 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 ArcSight 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 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 \(https://protect724.hp.com\)](https://protect724.hp.com).

Chapter 2: Installation and Configuration

This chapter discusses the following topics:

Installing the NetFlow Monitoring Package	8
Modeling the Network	9
Categorizing Assets	10
Ensuring Filters Capture Relevant Events	11
Scheduling Reports	11
Restricting Access to Vulnerability View Reports	11
Configuring Trends	12
Configuring the TotalBytes Variable	13
Viewing a Use Case Resource	14

Installing the NetFlow Monitoring Package

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

If you opted to exclude a Foundation package during ArcSight Manager 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.

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**.
4. 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**.
5. 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.

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

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.

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	Devices
ArcSight IP Flow SmartConnector	<ul style="list-style-type: none">• Cisco NetFlow version 5 and 9• Flexible NetFlow from IOS 15.0• Cisco ASA 8.2, and Juniper Networks J-Flow version 5 and 9
ArcSight QoSient ARGUS SmartConnector	<ul style="list-style-type: none">• QoSient ARGUS version 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*. To learn more about the architecture of the 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.

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	Same as /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*.

Ensuring Filters Capture Relevant Events

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

To ensure that a filter captures 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 and apply the change.
- c. Right-click the filter and choose **Create Channel with Filter** 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, reports are not scheduled to run automatically.

Evaluate the reports that come with the content, 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*.

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**.

Note: 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 back fills the data from that time. For example, if you enable the trend six months after the first install, these trends try to get all the data for the last six months, which might cause performance problems, overwhelm system resources, or cause the trend to fail if that event data is not available.

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

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

Trend Name	Scheduled run time
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

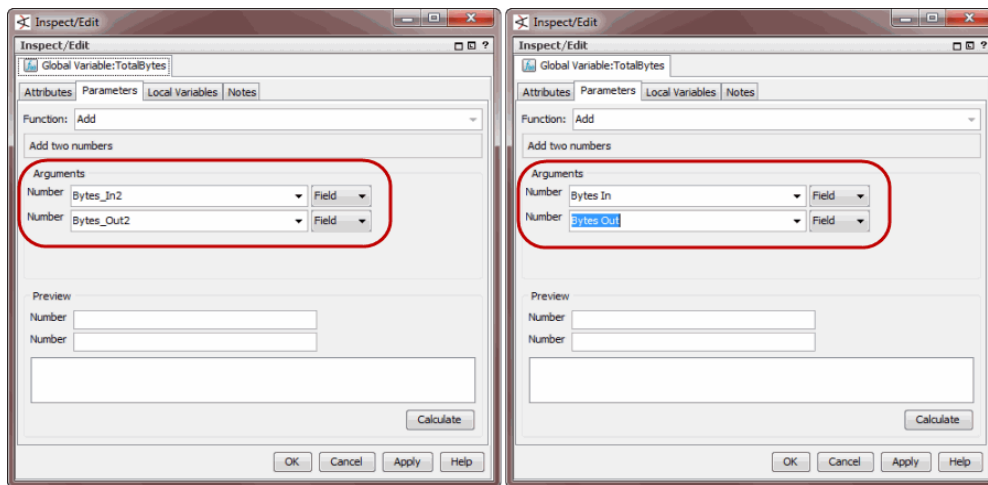
SmartConnectors can be configured to aggregate events and sum the counts in fields, such as `bytesIn` and `bytesOut`. SmartConnectors also set the aggregated event count. By default, ESM interprets the count in fields such as `bytesIn` and `bytesOut` as an average, and if the SmartConnector is configured 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 ArcSight 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/Bytes.
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.



5. Click **Apply** to confirm the change.

For information about the `server.properties` file on the ArcSight 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*.

Viewing a Use Case Resource

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

To view the resources associated with a NetFlow Monitoring use case resource:

1. In the Navigator panel, select the **Use Cases** tab.
2. Open the ArcSight Foundation/NetFlow Monitoring group.
3. Right-click a NetFlow Monitoring use case resource and select the **Open Use Case** option, or double-click a use case resource.

The resources that make up a use case resource are displayed in the Viewer. The use case resource tables listed in "[NetFlow Monitoring Resources](#)" on [page 15](#) contain all the resources that have been explicitly assigned to the NetFlow Monitoring use case.

Chapter 3: NetFlow Monitoring Use Case

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 ArcSight can help to monitor network bandwidth usage and correlate it with other security logs (such as firewall, IDS, authentication logs, and so on).

NetFlow Monitoring content contains one use case with 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.

Devices

Network devices with NetFlow enabled supply events that apply to the NetFlow Monitoring resources.

NetFlow Monitoring Resources

The following table lists all the resources in the NetFlow Monitoring use case.

Resources that Support the NetFlow Monitoring Use Case

Resource	Description	Type	URI
Monitor Resources			
NetFlow Bandwidth Usage Overview	This dashboard shows the top bandwidth usage as reported by NetFlow events, showing the top bandwidth usage by source, destination, well-known port, and non well-known port.	Dashboard	/All Dashboards/ArcSight Core Security

Resources that Support the NetFlow Monitoring Use Case, continued

Resource	Description	Type	URI
NetFlow Bandwidth Usage Monitoring	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 bandwidth usage events sorted by well-known ports from NetFlow events and 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 bandwidth usage events sorted by source-destination address pairs and destination port from NetFlow events.	Query Viewer	ArcSight Foundation/NetFlow Monitoring
Top Bandwidth Usage by Destination	This query viewer displays the top ten bandwidth usage events sorted by destination address from NetFlow events and 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 bandwidth usage events sorted by source-destination address pairs from NetFlow events.	Query Viewer	ArcSight Foundation/NetFlow Monitoring

Resources that Support the NetFlow Monitoring Use Case, continued

Resource	Description	Type	URI
Top Bandwidth Usage by Non-Well-Known Port	This query viewer displays the top ten bandwidth usage events sorted by non-well-known ports from NetFlow events and contains several drilldowns for investigation.	Query Viewer	ArcSight Foundation/NetFlow Monitoring
Top Bandwidth Usage by Source	This query viewer displays the top ten bandwidth usage events sorted by source address from NetFlow events and 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 bandwidth usage events sorted by source address and destination port from NetFlow events.	Query Viewer	ArcSight Foundation/NetFlow Monitoring
Top Bandwidth Usage by Destination and Port	This query viewer displays the top ten bandwidth usage events sorted by destination address and destination port from NetFlow events.	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 the top bandwidth usage by source. The default time range for this report is yesterday.	Report	ArcSight Foundation/NetFlow Monitoring

Resources that Support the NetFlow Monitoring Use Case, continued

Resource	Description	Type	URI
Top Bandwidth Usage by Destination	This report displays the 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 several charts that show 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 yesterday.	Report	ArcSight Foundation/NetFlow Monitoring
Library Resources			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Top Bandwidth Usage (MB) by Destination	This data monitor displays the total bandwidth usage in MegaBytes (MB) from NetFlow events for top Destination IP Addresses.	Data Monitor	/All Data Monitors/ArcSight Core Security/NetFlow Monitoring
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/NetFlow Bandwidth Usage Monitoring
Top Bandwidth Usage (MB) by Well-Known Port	This data monitor displays the total bandwidth usage in MegaBytes (MB) from NetFlow events for Well Known Ports.	Data Monitor	/All Data Monitors/ArcSight Core Security/NetFlow Monitoring
Top Bandwidth Usage (MB) by Non-Well-Known Port	This data monitor displays the total bandwidth usage in MegaBytes (MB) from NetFlow events for Non Well Known Ports.	Data Monitor	/All Data Monitors/ArcSight Core Security/NetFlow Monitoring

Resources that Support the NetFlow Monitoring Use Case, continued

Resource	Description	Type	URI
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/NetFlow Bandwidth Usage Monitoring
Top Bandwidth Usage (MB) by Source	This data monitor displays the total bandwidth usage in MegaBytes (MB) from NetFlow events for the top Source IP Addresses.	Data Monitor	/All Data Monitors/ArcSight Core Security/NetFlow Monitoring
List of Top Bandwidth Usage (MB) Events	This data monitor displays the top bandwidth usage events	Data Monitor	ArcSight Foundation/NetFlow Monitoring/NetFlow Bandwidth Usage Monitoring
TotalBytes	This variable sums the values of Bytes In and Bytes Out for each event.	Global Variable	ArcSight Foundation/Variables Library/Bytes
MBytesTotal	This variable converts the combination of the Bytes In and Bytes Out fields to MBytes, where a MByte is defined as 1,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In + Bytes Out < 10,000, the result is 0).	Global Variable	ArcSight Foundation/Variables Library/Bytes
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 originating from external sources targeting the internal 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

Resources that Support the NetFlow Monitoring Use Case, continued

Resource	Description	Type	URI
Outbound NetFlow Traffic	This filter identifies NetFlow events originating from internal sources targeting the external 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
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	/All Filters/ArcSight Core Security/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	/All Filters/ArcSight Core Security/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	/All Filters/ArcSight Core Security/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

Resources that Support the NetFlow Monitoring Use Case, continued

Resource	Description	Type	URI
NetFlow Traffic for Non-Well-Known Ports	This filter identifies events from NetFlow Traffic Reporting Devices where the Target Port is not NULL and is greater than or equal to 1024.	Filter	/All Filters/ArcSight Core Security/NetFlow Monitoring
NetFlow Traffic for Well-Known Ports	This filter identifies events from NetFlow Traffic Reporting devices where the Target Port is not NULL and is less than 1024.	Filter	/All Filters/ArcSight Core Security/NetFlow Monitoring
NetFlow V5 Events	This filter identifies NetFlow version 5 events.	Filter	/All Filters/ArcSight Core Security/NetFlow Monitoring
Top Bandwidth Usage by Source-Destination Pairs	This query returns the attacker address, target address, flow counts, and total bytes (Bytes In + Bytes Out) from NetFlow events.	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 attacker address and total bytes (Bytes In + Bytes Out) from NetFlow events	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 attacker address, target port, flow counts, and total bytes (Bytes In + Bytes Out) from NetFlow events.	Query	ArcSight Foundation/NetFlow Monitoring

Resources that Support the NetFlow Monitoring Use Case, continued

Resource	Description	Type	URI
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 Destination	This query identifies the target address and total bytes (Bytes In + Bytes Out) from NetFlow events.	Query	ArcSight Foundation/NetFlow Monitoring
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
Top Bandwidth Usage by Well-Known Port	This query returns the target port and total bytes (Bytes In + Bytes Out) from NetFlow events from a well-known target port.	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 target address, target port, flow counts, and total bytes (Bytes In + Bytes Out) from NetFlow events.	Query	ArcSight Foundation/NetFlow Monitoring

Resources that Support the NetFlow Monitoring Use Case, continued

Resource	Description	Type	URI
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 target port and total bytes (Bytes In + Bytes Out) from NetFlow events for non-well-known target ports.	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 attacker address, target address, target port, flow counts, and total bytes (Bytes In + Bytes Out) from NetFlow events.	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
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
Four Charts Landscape	This template is designed to show four charts. The orientation is landscape.	Report Template	ArcSight System/4 Charts/Without Table

Resources that Support the NetFlow Monitoring Use Case, continued

Resource	Description	Type	URI
Top Bandwidth Usage by Hour	This trend stores hourly information of top bandwidth usage and 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 and 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, 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 the top bandwidth usage information by source and includes the 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

Resources that Support the NetFlow Monitoring Use Case, continued

Resource	Description	Type	URI
Top Bandwidth Usage by Destination	This trend stores the top bandwidth usage information by destination and includes the 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 and includes the 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

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on NetFlow Monitoring Standard Content Guide (ESM 6.8c)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hp.com.

We appreciate your feedback!