

Standard Content Guide

IPv6

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	IPv6 content for ArcSight ESM 6.5c	Final revision for release.

Contents

- Chapter 1: IPv6 Overview 5**
 - What is Standard Content? 5
 - Standard Content Packages 7
 - IPv6 Content 7
- Chapter 2: Installation and Configuration 9**
 - Installing the IPv6 Package 9
 - Configuring IPv6 Content 10
- Chapter 3: IPv6 Use Case 11**
 - Configuration 11
 - Resources 11
- Index 19**

Chapter 1

IPv6 Overview

This chapter discusses the following topics.

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

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

["IPv6 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.

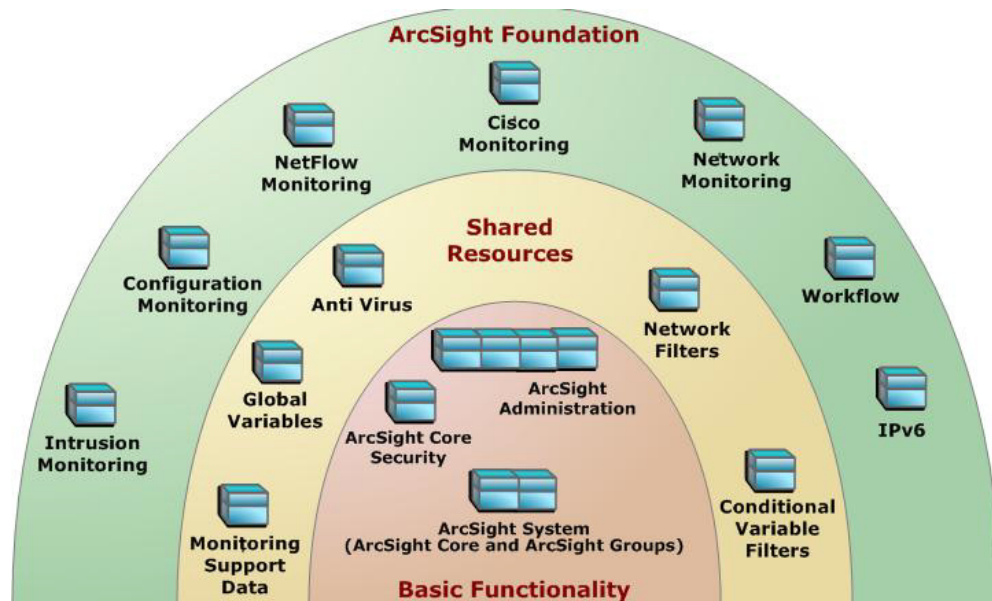


Figure 1-1 The ArcSight Core Security, ArcSight Administration, and ArcSight System packages at the base provide content required for basic ArcSight functionality. The common packages in the center contain shared resources that support multiple packages. The packages shown on top are ArcSight Foundations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

IPv6 Content

The IPv6 content reports on data that comes from networks with IPv6 addresses.

This guide describes the IPv6 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 IPv6 Package” on page 9](#)

[“Configuring IPv6 Content” on page 10](#)

Installing the IPv6 Package

The IPv6 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 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 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 IPv6 Content

The IPv6 content is triggered by events from IPv6-enabled SmartConnectors. Contact your HP ArcSight sales representative for a list of IPv6-enabled SmartConnectors.

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. 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.

The IPv6 content contains many reports. You can run reports on demand, automatically on a regular schedule, or both. By default, IPv6 reports are not scheduled to run automatically. Evaluate the reports that come with IPv6, 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.

Chapter 3

IPv6 Use Case

The IPv6 content shows data that comes from networks with IPv6 addresses.

Configuration

Refer to [“Configuring IPv6 Content” on page 10](#) for configuration information.

Resources

The following table lists all the resources explicitly assigned to the IPv6 use case and includes dependent resources. Dependent resources are not listed in a use case resource on the ArcSight Console.

Table 3-1 Resources that Support the IPv6 Group

Resource	Description	Type	URI
Monitor Resources			
Successful Logins by Destination IPv6 Address	This report shows authentication successes from login attempts by destination IPv6 address. A chart shows the top destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Report	ArcSight Foundation/IPv6/
Top Alert IPv6 Destinations	This report shows the top IDS and IPS alert destinations per day.	Report	ArcSight Foundation/IPv6/
Top IDS Signature IPv6 Sources per Day	This report shows the top IDS signature sources per day.	Report	ArcSight Foundation/IPv6/
Attacker IPv6 Counts by ArcSight Priority	This report displays a table with the priority, attacker IPv6 address and the count of attack events where the category significance starts with Compromise or Hostile.	Report	ArcSight Foundation/IPv6/

Resource	Description	Type	URI
Attacker Counts by IPv6 Device	This report displays a table with the device IPv6 address, attacker IPv6 address, and the count of attacker events where the category significance starts with Compromise or Hostile.	Report	ArcSight Foundation/IPv6/
Top IDS Signature IPv6 Destinations per Day	This report shows the top IDS signature destinations per day.	Report	ArcSight Foundation/IPv6/
Target Counts by IPv6 Attacker	This report displays the attacker address, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/IPv6/
Target Counts by IPv6 Device	This report displays the device address, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/IPv6/
Denied Outbound Connections by IPv6 Address	This report shows a summary of the denied outbound traffic by local address. A chart shows the top IPv6 addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/IPv6/
Target IPv6 Counts by ArcSight Priority	This report displays the priority, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/IPv6/
Top Alert IPv6 Sources	This report shows the top IDS and IPS alert sources per day. A chart shows the top IDS and IPS alert source IP addresses. A table shows the top alert source IP addresses, as well as the device vendor and product of the reporting device.	Report	ArcSight Foundation/IPv6/
Successful Logins by Source IPv6 Address	This report shows authentication successes from login attempts by source IPv6 address. A chart shows the top source addresses with successful login attempts. A table shows the count of authentication successes by source-destination pair and by user.	Report	ArcSight Foundation/IPv6/

Resource	Description	Type	URI
Top IPv6 Talkers	This report shows the top talkers and a detailed list of the top talkers.	Report	ArcSight Foundation/IPv6/
Denied Inbound Connections by IPv6 Address	This report shows a summary of the denied inbound traffic by foreign address. A chart shows the top IPv6 addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/IPv6/
Top N Attacked IPv6 Targets	This report shows the Target Address and the sum of the Aggregated Event Count for events matching the Attack Events filter.	Report	ArcSight Foundation/IPv6/
Alert Counts by IPv6 Device	This report shows the count of IDS and IPS alerts by device. A chart shows the top device IPv6 addresses with the highest counts. A table shows the list of all the devices, grouped by device vendor and product, then sorted by count.	Report	ArcSight Foundation/IPv6/
Top IPv6 Attackers	This report displays a chart of the attacker address, and the count of events where the category significance starts with Compromise or Hostile.	Report	ArcSight Foundation/IPv6/
Top N IPv6 Attacker Details	This report displays the priority, attacker address, and the count of attack events where the category significance starts with Compromise or Hostile. The query uses the sum of the aggregated event count instead of counting the EventID so that attackers are not split by the attack type.	Report	ArcSight Foundation/IPv6/
Failed Logins by Destination IPv6 Address	This report shows authentication failures from login attempts by destination IPv6 address. A chart shows the top destination addresses with failed login attempts. A table shows the count of authentication failures by destination-source pair and by user.	Report	ArcSight Foundation/IPv6/

Resource	Description	Type	URI
Failed Logins by Source IPv6 Address	This report shows authentication failures from login attempts by source IPv6 address. A chart shows the top source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Report	ArcSight Foundation/IPv6/
Attacker Counts By IPv6 Target	This report displays the attacker IPv6 address, the event name, and the count of attack events where the category significance starts with Compromise or Hostile, for the address specified in the parameters.	Report	ArcSight Foundation/IPv6/
Target IPv6 Counts by Event Name	This report displays the event name, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/IPv6/
Library Resources			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Agent IPv6 Address	This variable is an alias for Device Custom IPv6 Address4.	Global Variable	ArcSight Foundation/Variables Library/IPv6
Target IPv6 Address	This field denotes the Target IPv6 address. The term target is dependent upon the originator field, such as Source or Destination, depending on the specific event. If the originator field is Destination, return Device Custom IPv6 Address2 (aliased as Destination IPv6 Address), or return Device Custom IPv6 Address1 (aliased as Source IPv6 Address).	Global Variable	ArcSight Foundation/Variables Library/IPv6
Source IPv6 Address	This variable is an alias for Device Custom IPv6 Address1.	Global Variable	ArcSight Foundation/Variables Library/IPv6
Destination IPv6 Address	This variable is an alias for Device Custom IPv6 Address2.	Global Variable	ArcSight Foundation/Variables Library/IPv6

Resource	Description	Type	URI
Attacker IPv6 Address	This field denotes the Attacker IPv6 address. The term attacker is dependent upon the originator field, such as Source or Destination, depending on the specific event. If the originator field is Source, return Device Custom IPv6 Address1 (aliased as Source IPv6 Address), or return Device Custom IPv6 Address2 (aliased as Destination IPv6 Address).	Global Variable	ArcSight Foundation/Variables Library/IPv6
Device IPv6 Address	This variable is an alias for Device Custom IPv6 Address3.	Global Variable	ArcSight Foundation/Variables Library/IPv6
Attack IPv6 Events	This filter selects events where the category significance starts with Compromise or Hostile.	Filter	ArcSight Foundation/IPv6/
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Inbound Events	This filter identifies events coming from the outside network targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
External Target	This filter identifies events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
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
IDS -IPS IPv6 Events	This filter passes Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) events.	Filter	ArcSight Foundation/IPv6/
Denied Inbound Connections by IPv6 Address	This query identifies the count of denied inbound connections by foreign address (address and hostname).	Query	ArcSight Foundation/IPv6/

Resource	Description	Type	URI
Failed Logins by IPv6 Source-Destination Pair	This query returns authentication failure events from login attempts. The query returns the source address, source host name, destination address, destination host name, user name, user ID, count of failed logins, and device group.	Query	ArcSight Foundation/IPv6/
Denied Outbound Connections by IPv6 Address	This query identifies the count of denied outbound connections by local address (address and hostname).	Query	ArcSight Foundation/IPv6/
Failed Logins by Destination IPv6 Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Foundation/IPv6/
Target IPv6 Counts by Event Name	This query returns the event name, target address and the sum of the aggregated event count for events matching the Attack Events filter.	Query	ArcSight Foundation/IPv6/
Top 10 IPv6 Attackers	This query identifies the attacker address, and the count of events where the category significance starts with Compromise or Hostile. The query uses the sum of the aggregated event count instead of counting the EventID so that attackers are not split by the attack type.	Query	ArcSight Foundation/IPv6/
Target Counts by IPv6 Attacker	This query returns the attacker address, target address and the sum of the aggregated event count for events matching the Attack Events filter.	Query	ArcSight Foundation/IPv6/
Target Counts by IPv6 Device	This query returns the device address, target address and the sum of the aggregated event count for events matching the Attack Events filter.	Query	ArcSight Foundation/IPv6/
Top 10 Attacked IPv6 Targets	This query selects the Target IPv6 Address and the sum of the Aggregated Event Count for events matching the Attack IPv6 Events filter.	Query	ArcSight Foundation/IPv6/

Resource	Description	Type	URI
Attacker Counts by IPv6 Device	This query identifies the device address, attacker address, and the count of events where the category significance starts with Compromise or Hostile.	Query	ArcSight Foundation/IPv6/
Successful Logins by Source IPv6 Address (Chart)	This query returns authentication success events from login attempts.	Query	ArcSight Foundation/IPv6/
Alert Counts by IPv6 Device	This query returns the count of IDS and IPS alerts by device vendor, product, address and hostname.	Query	ArcSight Foundation/IPv6/
Top 10 IPv6 Talkers	This query returns the attacker address and the count of events in which the category significance starts with Compromise or Hostile. The query uses the sum of the aggregated event count instead of counting the EventID so that attackers are not split by the event name.	Query	ArcSight Foundation/IPv6/
Top IDS Signature IPv6 Sources per Day	This query returns the attacker address, device vendor, device product, and the count of the events within the query timeframe.	Query	ArcSight Foundation/IPv6/
Top IDS Signature IPv6 Destinations per Day	This query returns the target address, device vendor, device product, and the count of the events within the query timeframe.	Query	ArcSight Foundation/IPv6/
Successful Logins by Destination IPv6 Address (Chart)	This query returns authentication success events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Foundation/IPv6/
Top Alert IPv6 Sources	This query identifies the count of IDS and IPS alerts by source address, device vendor, and device product.	Query	ArcSight Foundation/IPv6/
Top 10 IPv6 Attacker Details	This query identifies the priority, attacker address, and the count of events where the category significance starts with Compromise or Hostile. The query uses the sum of the aggregated event count instead of counting the EventID so that attackers are not split by the attack type.	Query	ArcSight Foundation/IPv6/

Resource	Description	Type	URI
Target IPv6 Counts by ArcSight Priority	This query returns the priority, target address and the sum of the aggregated event count for events matching the Attack Events filter.	Query	ArcSight Foundation/IPv6/
Attacker Counts By IPv6 Target	This query identifies the attacker IPv6 address, the event name, and the count of events where the category significance starts with Compromise or Hostile for the target information given in the parameters.	Query	ArcSight Foundation/IPv6/
Failed Logins by Source IPv6 Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by source address.	Query	ArcSight Foundation/IPv6/
Attacker IPv6 Counts by ArcSight Priority	This query identifies the priority, attacker address, and the count of events where the category significance starts with Compromise or Hostile.	Query	ArcSight Foundation/IPv6/
Successful Logins by IPv6 Source-Destination Pair	This query returns authentication success events from login attempts.	Query	ArcSight Foundation/IPv6/
Top Alert IPv6 Destinations	This query returns the count of IDS and IPS alerts by destination address, device vendor, and device product.	Query	ArcSight Foundation/IPv6/
Top 10 IPv6 Targets	This query returns the target address and the sum of the aggregated event count for events matching the Attack Events filter used in several reports.	Query	ArcSight Foundation/IPv6/

Index

A

- Agent IPv6 Address global variable 14
- Alert Counts by IPv6 Device query 16
- Alert Counts by IPv6 Device report 13
- ArcSight Administration overview 5
- ArcSight Core Security overview 5
- ArcSight Foundations overview 6
- ArcSight System overview 6
- asset categories
 - Protected 14
- Attack IPv6 Events filter 15
- Attacker Counts by IPv6 Device query 16
- Attacker Counts by IPv6 Device report 12
- Attacker Counts By IPv6 Target query 17
- Attacker Counts By IPv6 Target report 14
- Attacker IPv6 Address global variable 14
- Attacker IPv6 Counts by ArcSight Priority query 17
- Attacker IPv6 Counts by ArcSight Priority report 11

C

- content packages 7

D

- Denied Inbound Connections by IPv6 Address query 15
- Denied Inbound Connections by IPv6 Address report 13
- Denied Outbound Connections by IPv6 Address query 15
- Denied Outbound Connections by IPv6 Address report 12
- Destination IPv6 Address global variable 14
- Device IPv6 Address global variable 14

E

- External Source filter 15
- External Target filter 15

F

- Failed Logins by Destination IPv6 Address (Chart) query 15
- Failed Logins by Destination IPv6 Address report 13
- Failed Logins by IPv6 Source-Destination Pair query 15
- Failed Logins by Source IPv6 Address (Chart) query 17
- Failed Logins by Source IPv6 Address report 13
- filters
 - Attack IPv6 Events 15
 - External Source 15
 - External Target 15
 - IDS -IPS IPv6 Events 15
 - Inbound Events 15
 - Internal Source 15

- Internal Target 15
- Outbound Events 15

G

- global variables
 - Agent IPv6 Address 14
 - Attacker IPv6 Address 14
 - Destination IPv6 Address 14
 - Device IPv6 Address 14
 - Source IPv6 Address 14
 - Target IPv6 Address 14

I

- IDS -IPS IPv6 Events filter 15
- Inbound Events filter 15
- Internal Source filter 15
- Internal Target filter 15

O

- Outbound Events filter 15

P

- packages
 - deleting 10
 - installing 9
 - uninstalling 9
- Protected asset category 14

Q

- queries
 - Alert Counts by IPv6 Device 16
 - Attacker Counts by IPv6 Device 16
 - Attacker Counts By IPv6 Target 17
 - Attacker IPv6 Counts by ArcSight Priority 17
 - Denied Inbound Connections by IPv6 Address 15
 - Denied Outbound Connections by IPv6 Address 15
 - Failed Logins by Destination IPv6 Address (Chart) 15
 - Failed Logins by IPv6 Source-Destination Pair 15
 - Failed Logins by Source IPv6 Address (Chart) 17
 - Successful Logins by Destination IPv6 Address (Chart) 17
 - Successful Logins by IPv6 Source-Destination Pair 18
 - Successful Logins by Source IPv6 Address (Chart) 16
 - Target Counts by IPv6 Attacker 16

- Target Counts by IPv6 Device 16
- Target IPv6 Counts by ArcSight Priority 17
- Target IPv6 Counts by Event Name 16
- Top 10 Attacked IPv6 Targets 16
- Top 10 IPv6 Attacker Details 17
- Top 10 IPv6 Attackers 16
- Top 10 IPv6 Talkers 16
- Top 10 IPv6 Targets 18
- Top Alert IPv6 Destinations 18
- Top Alert IPv6 Sources 17
- Top IDS Signature IPv6 Destinations per Day 17
- Top IDS Signature IPv6 Sources per Day 17

R

reports

- Alert Counts by IPv6 Device 13
- Attacker Counts by IPv6 Device 12
- Attacker Counts By IPv6 Target 14
- Attacker IPv6 Counts by ArcSight Priority 11
- Denied Inbound Connections by IPv6 Address 13
- Denied Outbound Connections by IPv6 Address 12
- Failed Logins by Destination IPv6 Address 13
- Failed Logins by Source IPv6 Address 13
- Successful Logins by Destination IPv6 Address 11
- Successful Logins by Source IPv6 Address 12
- Target Counts by IPv6 Attacker 12
- Target Counts by IPv6 Device 12
- Target IPv6 Counts by ArcSight Priority 12
- Target IPv6 Counts by Event Name 14
- Top Alert IPv6 Destinations 11
- Top Alert IPv6 Sources 12
- Top IDS Signature IPv6 Destinations per Day 12
- Top IDS Signature IPv6 Sources per Day 11
- Top IPv6 Attackers 13
- Top IPv6 Talkers 12
- Top N Attacked IPv6 Targets 13
- Top N IPv6 Attacker Details 13

S

- shared libraries 6
- Source IPv6 Address global variable 14
- Successful Logins by Destination IPv6 Address (Chart) query 17
- Successful Logins by Destination IPv6 Address report 11
- Successful Logins by IPv6 Source-Destination Pair query 18
- Successful Logins by Source IPv6 Address (Chart) query 16
- Successful Logins by Source IPv6 Address report 12

T

- Target Counts by IPv6 Attacker query 16
- Target Counts by IPv6 Attacker report 12
- Target Counts by IPv6 Device query 16
- Target Counts by IPv6 Device report 12
- Target IPv6 Address global variable 14
- Target IPv6 Counts by ArcSight Priority query 17
- Target IPv6 Counts by ArcSight Priority report 12
- Target IPv6 Counts by Event Name query 16
- Target IPv6 Counts by Event Name report 14
- Top 10 Attacked IPv6 Targets query 16
- Top 10 IPv6 Attacker Details query 17
- Top 10 IPv6 Attackers query 16
- Top 10 IPv6 Talkers query 16
- Top 10 IPv6 Targets query 18
- Top Alert IPv6 Destinations query 18
- Top Alert IPv6 Destinations report 11
- Top Alert IPv6 Sources query 17
- Top Alert IPv6 Sources report 12
- Top IDS Signature IPv6 Destinations per Day query 17
- Top IDS Signature IPv6 Destinations per Day report 12
- Top IDS Signature IPv6 Sources per Day query 17
- Top IDS Signature IPv6 Sources per Day report 11
- Top IPv6 Attackers report 13
- Top IPv6 Talkers report 12
- Top N Attacked IPv6 Targets report 13
- Top N IPv6 Attacker Details report 13