

ESM System Content

Reference Guide

ArcSight ESM™ v4.0

April 3, 2007



ESM System Content Reference Guide

April 3, 2007

Copyright © 2006 ArcSight, Inc. All rights reserved. ArcSight, the ArcSight logo, ArcSight NRM, ArcSight NCM, ArcSight Enterprise Security Alliance, ArcSight Interactive, ArcSight Pattern Discovery, ArcSight Logger, Flex-Connector, SmartConnector, SmartStorage and CounterACT are trademarks of ArcSight, Inc. All other brands, products and company names used herein may be trademarks of their respective owners.

To see a complete statement of ArcSight's copyrights, trademarks, and acknowledgements, visit: <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 ArcSight Confidential.

Revision History

Date	Product Version	Description
3/17/07	4.0	Final ESM 4.0 release.
4/3/07		Update permissions in appendix B; update index.

ArcSight Customer Support

Contact	
Phone:	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail:	support@arcsight.com
Web:	https://support.arcsight.com

Contents

About ArcSight Content	1
Who Should Read this Guide	1
How to Use this Guide	2
Text Conventions	3
Related Documentation	4
ArcSight Customer Support	5
What's Next	5
 Chapter 1: Standard Content for ESM v4.0	 7
Standard Content Overview	8
ArcSight Foundations	9
Configuration Monitoring	9
Intrusion Monitoring	9
Network Monitoring	10
ArcSight Workflow	10
ArcSight Administration	10
Shared Resources	10
ArcSight System	11
Standard Content Special Features	12
Packages	12
Resource Locking	13
Resource IDs	14
ArcSight System User	14
SANS Institute Top 5 Essential Log Reports	15
What's Next	15
 Chapter 2: Standard Content Installation, Upgrade, and Configuration	 17
How Standard Content is Installed and Upgraded	17
Standard Content Upgrade Overview	18
Deprecated Resources and Resource Groups	19
Preparing Existing Content for Upgrade	20
Checking Existing Content After Upgrade	20
Fixing Invalid Resources	22
Persist Conflicts to the Database	22
Fixing and Re-Enabling Invalid Resources	22
Verify Proper Function of Customer-Created Content	23
Changes to Expect After the Upgrade	23

Core Customer-Configured Filters	23
Standard Content Package Overview	25
Package States: Imported and Installed	26
Configuration Planning	28
Standard Content-Related SmartConnectors	28
Network Modeling	29
Assets	29
Zones	29
Networks	30
Asset Categories	30
How ArcSight Determines the Protected Network	31
Criticality Asset Categories for Priority Formula	31
How to Assign Asset Categories	31
Assign Asset Categories Using Console UI	32
Assign Asset Categories Using the ArcSight Asset Import Connector	33
Configure Resources with Network-Specific Values	35
Configure Asset Auto-Creation Filters	35
Configure Connector Asset Auto-Creation Events Filter	36
Configure Device Asset Auto Creation Events Filter	38
Configure SNMP Trap Forwarding Filter	39
Change Default Condition in SNMP Trap Forwarding Filter	40
Change SNMP Trap Sender in server.properties	40
Configure Active Lists	41
Configure Active Lists Using Console Active List Editor	41
Configure Active Lists from Imported CSV	41
Configure Dynamic Active Lists	42
Trends	43
ArcSight Administration Trends	43
Configuration Monitoring Trends	43
Intrusion Monitoring Trends	44
Network Monitoring Trends	44
How to Enable/Disable Trends	45
How to Monitor Trend Performance	45
What's Next	45
Chapter 3: ArcSight System	47
System Content Overview	48
Internal ArcSight Function	48
Network Modeling Standard Resources	48
Asset Categories	49
Site Asset Categories	49
System Asset Categories	51
Vulnerabilities	51

Locations	53
Files	54
Correlation Evaluation	54
Priority Evaluation Infrastructure	54
Threat Escalation Active Lists	56
System Filters	58
Core Filters	58
Event Type Filters	60
SNMP Forwarding Filters	61
SOC Operations and Monitoring	62
System Active Channels	62
ArcSight System Active Channels	62
All Events Active Channels	63
Core Active Channels	63
System Field Sets	64
Active Channels	64
Inspect - Edit Field Sets	65
Sortable Field Sets	65
Benchmarking and Analysis	66
Pattern Discovery Profiles	66
Core Reports	66
Standard Report Templates	68
Customize Branding in Standard Templates	69
Making Custom Modifications to Standard Templates	69
What's Next	70
Chapter 4: Configuration Monitoring Foundation	71
Configuration Monitoring Foundation Overview	72
Supported Devices	73
Configuration Summary	74
Required Configuration	74
Verify Asset Model	75
Configuration Monitoring Filters	75
Detail Filters	77
Configuration Changes by Device	78
Configuration Changes by User	81
Vulnerability Filters	83
Operational Summaries Filters	84
Configuration Monitoring Active Channels	86
Configuration Monitoring Field Sets	87
Configuration Monitoring Active Lists	88
Configuration Monitoring Dashboards and Data Monitors	89
Configuration Monitoring Data Monitors	91

Configuration Monitoring Reports	93
Configuration Monitoring Trends	93
Executive Summary Reports	96
Executive Summary Queries	97
Operational Summary Reports	98
Operational Summary Queries	100
Detail Reports	102
Current Configuration Report	102
Configuration Changes by Device Reports	103
Configuration Changes by User Reports	106
Inventory Reports	112
Vulnerability Reports	114
SANS Top 5 Reports for Configuration Monitoring	118
Configuration Monitoring Rules	119
What's Next	120
Chapter 5: Intrusion Monitoring Foundation	121
Intrusion Monitoring Foundation Overview	121
Anti-Virus	121
Attack Monitoring	122
Attackers	122
Business Impact Analysis/Business Roles	123
Environment State	123
Reconnaissance	123
Targets	123
User Accounts	124
Vulnerability View	124
Worm Outbreak	124
User-Relevant Views	124
Supported Devices	124
Configuration Summary	125
Restrict Access to Vulnerability View Reports	125
Configure Network Management Filter	125
Intrusion Monitoring Filters	127
Attack Monitoring Filters	128
Conditional Variable Filters	131
Environment State Filters	133
Reconnaissance Filters	135
Resource Access Filters	137
Targets Filters	139
Asset Criticality Filters	141
Business Roles Filters	143
By Port or Protocol Filters	146

Vulnerability View Filters	147
Worm Outbreak Filters	148
Intrusion Monitoring Active Channels	150
Intrusion Monitoring Field Sets	153
Intrusion Monitoring Active Lists	155
Intrusion Monitoring Dashboards and Data Monitors	156
Detail Dashboards	156
Attackers Data Monitors	159
Attack Monitoring Data Monitors	160
Reconnaissance Data Monitors	164
Security Activity Data Monitors	165
Targets Data Monitors	166
Virus Data Monitors	168
Worm Outbreak Data Monitors	169
Executive Summary Dashboards	170
Executive Summary Data Monitors	171
Operational Summary Dashboards	172
Operational Summary Data Monitors	174
Last-State Data Monitors - Usage Instructions	176
Intrusion Monitoring Rules	177
Attackers Rules	178
Attack Monitoring Rules	179
Reconnaissance Rules	187
Resource Access Rules	188
Targets Rule	189
Worm Outbreak Rules	190
Cases	191
Intrusion Monitoring Reports	192
Detail Reports	192
Anti-Virus Detail Reports	192
Attack Monitoring Detail Reports	194
Attackers Detail Reports	198
Environment State Detail Reports	200
Reconnaissance Detail Reports	203
Target Detail Reports	206
Vulnerability View Detail Reports	208
Worm Outbreak Detail Report	210
Executive Summary Reports	212
Executive Summary Queries	213
Intrusion Monitoring Operational Summary Reports	215
Operational Summary Queries	218
Operational Summary Trends	231
SANS Top 5 Reports for Intrusion Monitoring	234

SANS Top 5 Queries	236
SANS Top 5 Trends	240
SIS Report Template	241
What's Next	241
Chapter 6: Network Monitoring Foundation	243
Network Monitoring Foundation Overview	243
Supported Devices	243
Calculating Bytes In and Bytes Out	244
Configuration Overview	246
Advanced Connector Configuration	248
Required Asset Modeling	249
Assets	249
Asset Categories	249
How to Interact with the Network Monitoring Content	249
Network Monitoring Filters	250
Application Filters	251
Mail Server Filters	251
Web Server Filters	251
Connector Filters	251
DV Filters	252
Moving Average Filters	253
Network Traffic Filters	254
Report Parameter Filters	256
Network Monitoring Active Channel	257
How to Use the Network Monitoring Active Channel	257
Network Monitoring Field Sets	258
Network Monitoring Dashboards and Data Monitors	259
Bandwidth Usage Dashboards	260
Bandwidth Usage Data Monitors	261
General Dashboards	262
General Data Monitors	263
Inbound Traffic Dashboards	265
Inbound Traffic Data Monitors	265
Outbound Traffic Dashboards	266
Outbound Traffic Data Monitors	267
Network Monitoring Reports	269
Network Monitoring Trends	269
Executive Summaries Reports	271
Executive Summary Queries	273
Operational Summaries Reports	274
Traffic Snapshot Report	275
Bandwidth Utilization Reports	277

Inbound Traffic Reports	281
Outbound Traffic Reports	289
Detail Reports	296
Detail Reports Queries	299
SANS Top 5 Reports for Network Monitoring	301
SANS Top 5 Reports Queries	303
Network Monitoring Rules	305
What's Next	306
Chapter 7: ArcSight Workflow Foundation	307
Workflow Foundation Overview	307
Configuration Summary	308
Workflow Active Channels	309
Workflow Active Channels	309
Incident Tracking Active Channels	310
Workflow Reports	311
Case Reports	311
Case Queries	312
Notification Reports	313
Notification Queries	314
What's Next	314
Chapter 8: ArcSight Administration Foundation	315
ArcSight Administration Overview	315
Configuration Summary	316
ArcSight Administration Filters	317
ArcSight Administration Filters	317
Agent Filters	318
Configuration Change Monitoring Filter	319
ESM Status Filters	320
Event Flow Filter	321
Event Priority Filters	322
Resource Monitoring Filters	323
User Filters	324
ArcSight Administration Active Channels	325
ArcSight Administration Field Sets	326
ArcSight Administration Active List	327
ArcSight Administration Dashboards and Data Monitors	328
Configuration Change Monitoring Data Monitors	329
Connector Data Monitors	330
ESM Status Data Monitors	331
Event Flow Data Monitors	332
Resource Monitoring Data Monitors	333

User Monitoring Data Monitor	334
ArcSight Administration Rules	335
Connector and Device Monitoring Rules	335
ESM Status Rules	337
Event Flow Rules	339
Resource Monitoring Rules	340
User Rules	341
ArcSight Administration Session List	342
ArcSight Administration Reports	343
Agent Reports	343
Agent Queries	344
Configuration Change Monitoring Reports	345
Configuration Change Monitoring Queries	345
Event Flow Reports	346
Event Breakdown by Event Field Reports	346
Time-Based Event Breakdown Reports	348
Top N Activity Reports	350
Licensing Reports	351
Licensing Queries	352
Resource Monitoring Reports	353
Resource Monitoring Trend	355
Resource Monitoring Queries	356
User Reports	357
User Trend	358
User Queries	358
Appendix A: Shared Package Inventory	361
Anti-Virus Package	362
Anti-Virus Filters	362
Anti-Virus Reports	362
Anti-Virus Queries	362
Network Filters Package	363
Network Filters	363
Appendix B: Default Access Permissions	365
: Index	371

About ArcSight Content

ArcSight Enterprise Security Management 4.0 (ESM) comes with a robust and coordinated set of resources, referred to as standard content. Standard content addresses common enterprise network security and ArcSight management tasks.

This book describes the standard content, how it's organized, and how to use it to get the most out of ArcSight ESM.

- [“Who Should Read this Guide” on page 1](#)
- [“How to Use this Guide” on page 2](#)
- [“Related Documentation” on page 4](#)

Who Should Read this Guide

This guide is intended for ArcSight users, administrators, and security managers with the responsibility to plan, implement, maintain, and use ESM to monitor, investigate, and manage events in their network environments.

The standard content is organized into groups that are targeted for different user audiences:

Foundation	User Audience
Network Monitoring	Network administrators
Intrusion Monitoring	Security analysts
Configuration Management	System administrators and security analysts, depending on interests
ArcSight Workflow	SOC members; analysts and security management
ArcSight System	Security analysts, operators, and anyone with responsibility to develop ESM content
ArcSight Administration	ArcSight administrators

Users should have knowledge of:

- Networks and network security
- Organizational policies and procedures regarding user access to resources stored on the protected network
- Using ArcSight tools to address specific network security scenarios




How to Use this Guide

This guide presents the concepts, contents, and implementation guidelines for ArcSight's standard content. Use the table below to assist you in finding the information you need.

Chapter	Description
Preface	About this Guide. Describes the contents, properties, and audience for this book, and whom to contact for more information.
1	Standard Content for ESM v4.0. Describes the standard content, its structure, the ArcSight tools involved, and how the standard content addresses essential security monitoring scenarios in enterprise network environments.
2	Standard Content Installation, Upgrade, and Configuration. Describes how standard content is installed and provides general configuration instructions to set up the standard content for your network environment.
3	ArcSight System. Provides details about the core content infrastructure, and describes how to configure the resources that manage this infrastructure for your network environment.
4	Configuration Monitoring Foundation. Describes the configuration monitoring foundation, the devices that drive it, and configuration steps required. This foundation provides insight into the current configuration of your monitored hosts, applications and network infrastructure, monitors them for changes, and sends notifications as appropriate.
5	Intrusion Monitoring Foundation. Describes the intrusion monitoring foundation, the devices that drive it, configuration steps required, and run-time instructions. This foundation monitors everything to do with attacks, such as worms and viruses, and activity on protected assets.
6	Network Monitoring Foundation. Describes the network monitoring foundation, the devices that drive it, required configuration, and run-time instructions. This foundation monitors the status of the network and network infrastructure.
7	ArcSight Workflow Foundation. Describes the active channels and reports that support the investigation and incident response of daily security operations.
8	ArcSight Administration Foundation. Describes the content that manages ArcSight system monitoring, any configuration required, and run-time instructions. This foundation is essential for managing and tuning the performance of all ArcSight content and components.
Appendix A	Shared Package Inventory. This appendix lists the contents of the shared packages, Anti-Virus and Network Filters.
Appendix B	Default Access Permissions. This appendix lists the default permissions granted to all groups of content for the default ArcSight user groups.

Text Conventions

This book uses the following text conventions.

Text	Description and Example
Bold	<p>Bold is used to indicate an on-screen element that a user should click.</p> <ul style="list-style-type: none"> Enter a value and click OK.
<code>Code</code>	<p>Blue monospace text is used to indicate code elements.</p> <ul style="list-style-type: none"> If the name of your active list entries text file is "<code>AdministrativeUsers.txt</code>," the script would look like this:
<i>Italics</i>	<p><i>Italics</i> indicate emphasis or a book name:</p> <ul style="list-style-type: none"> <i>Do not</i> perform this procedure until you have backed up your data. For more information, see the <i>ArcSight Administrator's Guide</i>.
> angle brackets >	<p>Right angle brackets are used to indicate steps in a command sequence and online Help topic sequences.</p> <ul style="list-style-type: none"> command > subcommand > subcommand Authoring > Rules > Rule Actions > Updating Session Lists
Vertical bars	<p>Vertical bars are used to separate multilevel editor-tab sequences.</p> <ul style="list-style-type: none"> tab subtab subtab
/ Forward slash /	<p>Forward slashes are used to separate resource URI strings and other file paths.</p> <ul style="list-style-type: none"> All Reports/System Reports/Asset/All Assets
	<p>Tip. Tips provide helpful suggestions and best practices about how to get optimum results from a feature or procedure.</p>
	<p>Note. Notes provide additional information about a feature or procedure that might help you make decisions, or inform you about outcomes you can expect.</p>
	<p>Caution. Cautions indicate when a user error could cause system damage or data loss.</p>

Related Documentation

The following ArcSight documentation is installed with the ArcSight Manager. You can access this documentation from the ArcSight Console using the Browse Documentation link in the Help menu.

Document Title	Description
ArcSight 101: Concepts for ArcSight ESM™	ArcSight 101 introduces the underlying concepts behind how ArcSight works, and provides a road-map to the tools available in ArcSight depending on your role in security operations.
ArcSight Administrator's Guide	Describes how to configure ArcSight and its network interfaces, and maintain ArcSight for ongoing operations.
ArcSight SmartConnector Installation and Configuration Guide	Provides an overview of how to plan for and install an ArcSight SmartConnector.
Vendor-specific ArcSight Connector Configuration Guides	Provides vendor-specific instructions for how to install individual SmartConnectors and configure their associated devices.
ArcSight FlexConnector Configuration Guide	Describes how to design, create, and install custom SmartConnectors.
Using the ArcSight Console	Describes how to use the ArcSight Console. This is a printable version of the online Help contents.
ArcSight Console Online Help	Context sensitive help that contains information and procedures pertaining to the ArcSight Console user interface. To access online Help from the product user interface, click the question mark button in any screen.

In addition to the documents installed with the ArcSight Manager, you can find the following documents about this and other releases on ArcSight's Support web site: <https://support.arcsight.com/>. To view the documentation, obtain a user name and login from your ArcSight customer support representative.

Document Title	Description
Release Notes	Describes new product features, latest updates, known product issues and work-arounds, and technical support information.
ArcSight Installation and Configuration Guide	Describes how to install and configure ArcSight components in various enterprise network conditions.

ArcSight Customer Support

ArcSight Customer Support offers the following resources. A log-in user name and password are required, which you can obtain from your ArcSight customer support representative.

Resource	Description
Support web site	https://support.arcsight.com . Access to ArcSight incident reporting, knowledge base, software downloads, help, and new customer forum.
Customer forum	https://forum.arcsight.com . Offers a place for customers to share ArcSight tips and tricks.

What's Next

The next chapter provides a detailed overview of the standard content, its general architecture, the general use cases it addresses, and a synopsis of the types of devices that drive the content.

Chapter 1

Standard Content for ESM v4.0

ArcSight Enterprise Security Management 4.0 (ESM) comes with a series of coordinated resources that address common enterprise network security and ArcSight management tasks.

Some of these resources are installed automatically with ESM to provide essential system health and status operations. Others are presented as install-time options organized by category. These sets of resources are referred to collectively as *standard content*.

Upon installation, the standard content makes ArcSight ready to perform a wide range of security monitoring and reporting tasks. With some minor configuration, these standard tasks can be fine-tuned to provide immediate and detailed insight into the activity on your network and the security posture of your assets and network infrastructure.

This chapter describes the different areas of standard content: the functionality provided, interactions between resources, and how you can use and extend the standard content to address your essential security monitoring and remediation needs.

- [“Standard Content Overview” on page 8](#)
 - ◆ [“ArcSight Foundations” on page 9](#)
 - ◆ [“Shared Resources” on page 10](#)
 - ◆ [“ArcSight System” on page 11](#)
- [“Standard Content Special Features” on page 12](#)
 - ◆ [“Packages” on page 12](#)
 - ◆ [“Resource Locking” on page 13](#)
 - ◆ [“ArcSight System User” on page 14](#)
 - ◆ [“SANS Institute Top 5 Essential Log Reports” on page 15](#)

Standard Content Overview

The 4.0 standard content has been expanded and updated from previous versions to make use of new ESM features. Existing content has been streamlined and reorganized to provide a more comprehensive security management solution out of the box. Some resources that are no longer needed have been deprecated.

The new structure for the standard content introduces a framework that enables the content to be more effectively used and understood. The traditional functions the standard content addresses are organized into five major use cases, or "Foundations."

Several of the foundations rely on a series of common resources that provide core functions for common security scenarios. And resources that manage core ArcSight functions are expanded and locked to protect them from unintended damage.

All of the standard content is delivered in a series of portable bundles called packages. These packages are shown in figure 1-1, and are described in more detail on the following pages.

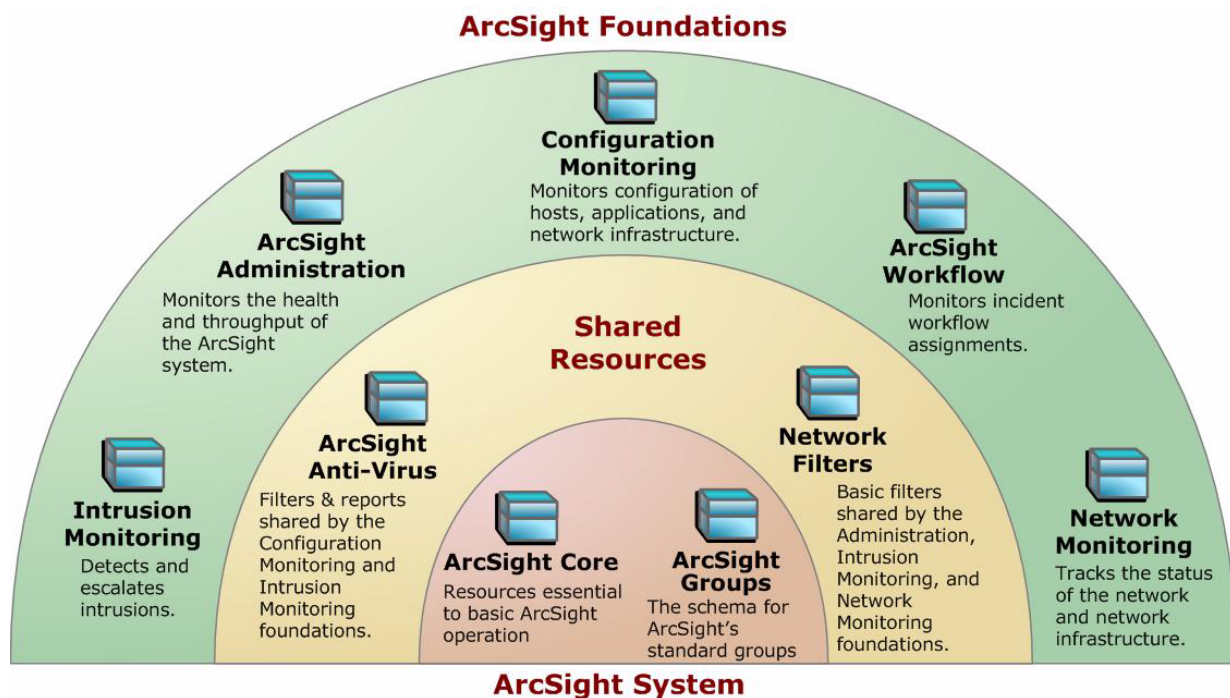


Figure 1-1 The ArcSight System packages at the center provide core content required for ArcSight operation. The packages in yellow in the second tier contain shared resources that support common security functions of the foundation packages. The packages in green in the outer layer are ArcSight Foundations that address common network security scenarios.

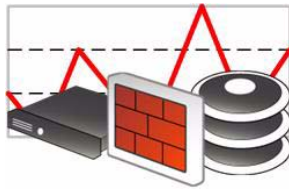
ArcSight Foundations

The five packages in the top layer deliver the ArcSight Foundations. Each foundation is a coordinated system of resources that provides real-time monitoring capabilities for its area of focus, as well as after-the-fact analysis in the form of reports, trends, and trend reports.

Each foundation makes use of new and enhanced capabilities introduced by ESM 4.0. These resources are intended to be used as the foundation for basic function in its area of focus, which you can extend with additional resources specific to your needs. The foundations can also be used as an example for how to build individual resources and whole coordinated use cases.

Dividing the content into these major functional areas makes it easier to understand and put to use right away. It also makes it easier for ArcSight to expand and update these resources in the future.

Configuration Monitoring



The Configuration Monitoring foundation identifies, analyzes, and remediates undesired modifications to systems, devices, and applications. This foundation helps IT and security staff to pinpoint and resolve problems quickly, and provides essential visibility into the network configuration so you understand the systems you have, where they are, what they host, and what vulnerabilities they expose.

Once you have this basic view, the configuration monitoring foundation helps you monitor how your networks change over time, measure daily statistics, understand the changes made, and know who's making them. Trends help you know what is normal and spot anomalies that should be investigated.

For more about the Configuration Monitoring foundation, see [“Configuration Monitoring Foundation” on page 71](#).

Intrusion Monitoring

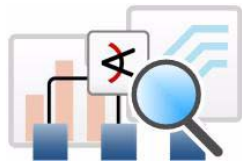


The focus of the Intrusion Monitoring foundation is to identify hostile activity and take appropriate action. This foundation provides statistics about intrusion-related activity, which can be used for incident investigation as well as routine monitoring and reporting. As with previous releases, the Intrusion Monitoring essential security monitoring functions make up the bulk of the ESM standard content.

The Intrusion Monitoring foundation targets generic intrusion types as well as specific types of attacks, such as worms, viruses, denial-of-service (DoS) attacks, and so on. This foundation also addresses several of the SANS top 20 list of vulnerable areas.

For more about the Intrusion Monitoring foundation, see [“Intrusion Monitoring Foundation” on page 121](#).

Network Monitoring



The Network Monitoring foundation monitors the status of network throughput and network infrastructure. This foundation provides statistics about traffic and bandwidth usage that helps you identify anomalies and areas of the network that need attention.

Network Monitoring also addresses the usage and traffic profiles that factor into a comprehensive security reporting strategy.

For more about the Network Monitoring foundation, see [“Network Monitoring Foundation” on page 243](#).

ArcSight Workflow



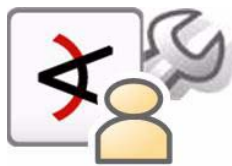
The ArcSight Workflow foundation is a system of active channels and reports that support incident response tracking using ArcSight's incident response system.

Qualifying events in the other ArcSight foundation packages trigger notifications and cases that get escalated through

ArcSight's incident response stages.

For more about the ArcSight Workflow foundation, see [“ArcSight Workflow Foundation” on page 307](#).

ArcSight Administration



The ArcSight Administration foundation provides statistics about the health and performance of ArcSight ESM and its components. This foundation is installed automatically, and is essential for managing and tuning the performance of ESM content and components.

For more about the ArcSight Administration foundation, see [“ArcSight Administration Foundation” on page 315](#).

Shared Resources



The ArcSight Anti-Virus and Network Filters packages shown in the yellow middle band of figure 1-1 provide common resources that support the five foundations. Dependencies between these packages and the foundation packages they support are managed by the Packages resource.

For details about the contents of the shared resources packages, see [“Shared Package Inventory” on page 361](#).

ArcSight System



The *ArcSight System* and *ArcSight Groups* packages shown in red at the center of figure 1-1 consist of resources that ESM requires for basic security processing functionality, such as threat escalation and priority calculations, and basic throughput channels required for out-of-the-box functionality.

This content is installed automatically with ArcSight ESM so that these functions and the infrastructure that supports them are immediately available. The core content infrastructure also serve the systems and solutions you deploy, and ArcSight content you create yourself. For more about the ArcSight system content, see [“ArcSight System” on page 47](#).

Standard Content Special Features

This section highlights special features of the standard content.

Packages



ArcSight ESM 4.0 delivers its standard content in a series of portable bundles called *packages*. A package is an ArcSight resource that acts as a container for other ArcSight resources, which enables blocks of resources to be easily backed up or transported among different ESM systems. Packages make the back-up and transfer capabilities of the ArcSight Archive tool available through the Console user interface.

Packages can be used to transport content for a family of use cases, and they can also be used to transport blocks of unrelated resources, or a core of common resources that can be leveraged by other use cases. Dependencies on resources located in other packages are managed by the Packages resource. For more about the Packages resource, see the topic *Managing Packages* in the Console online Help.

Resource Locking

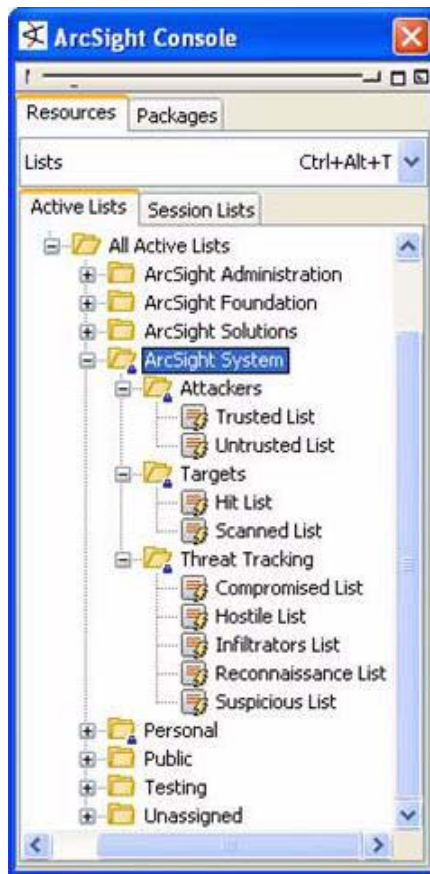


ESM v3.5 had the ability to lock cases to safeguard against one user overwriting another user's work. ESM 4.0 introduces the ability to lock any type of resource. Locking resources provides additional control to ArcSight's user permissions system to restrict access to what users can and cannot add to, modify, or delete.

The standard content makes use of resource locking to protect resources that are essential for ArcSight to function. This ensures that content required for essential ArcSight functions, such as the Priority Formula, are protected from accidental modification or deletion.

A locked *resource* cannot be deleted or its conditions modified. A locked *group* cannot be deleted, or have resources added to it or deleted from it. If the members of a *locked* group are *unlocked*, it means that the resource conditions *can* be modified. Essential core ArcSight resources that can be configured with values specific to your environment are presented as *unlocked* resources in a *locked* group.

An example of a locked group is the ArcSight System active lists: ([All Active Lists/ArcSight System/](#))



Locked group: The group is locked, which means that the group itself and its contents cannot be deleted, renamed, added to, or deleted from.

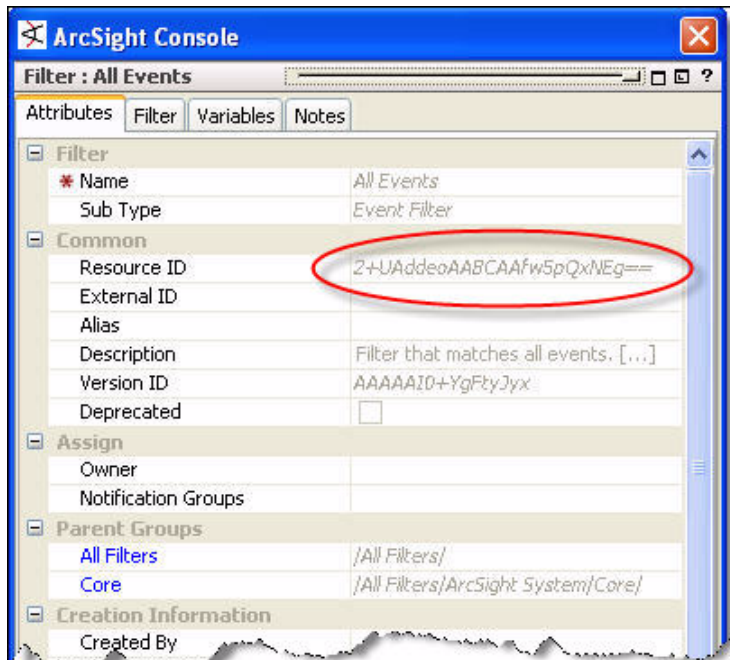
Unlocked contents: The contents of this locked group are *unlocked*, which means that their *conditions* can be modified, but the resources themselves cannot be moved, deleted or renamed.

With ESM 4.0, any resource type can be locked. When a resource is locked by a user, that user becomes the lock owner. Attempts to update a locked resource will fail if the user trying to change it is not the lock owner. Only the lock owner or a user with greater permissions can modify the resource or unlock it.

Resource IDs

The resource ID is an auto-generated 25-character string that uses a combination of numbers, letters, and symbols to internally identify resources.

Previous versions of ESM used the resource ID, but the value was not exposed. In v4.0, the resource ID is exposed in the resource editor in the Inspect/Edit panel. The example below shows the resource ID for the System Core filter *All Events*. The resource ID is a non-editable field.



ArcSight System User

The lock owner of ArcSight System content that is locked is the ArcSight System user. The System user is a special administrative account created for ESM 4.0 that is intended solely for specialized administration tasks.

For security purposes, the System User account is named by you at installation or upgrade time. Access to the account is managed only by ArcSight Customer Support. For contact information, see ["ArcSight Customer Support" on page 5](#).

SANS Institute Top 5 Essential Log Reports

Each foundation contains a set of reports that address the SANS Institute's list of recommendations of what every IT staff should know about their network at a minimum, based on the Top 5 Essential Log Reports (version 1.0, http://www.sans.org/resources/top5_logreports.pdf).

For a description of the SANS Top 5 content provided by each foundation, see the following sections:

- Configuration Monitoring: “SANS Top 5 Reports for Configuration Monitoring” on [page 118](#)
- Intrusion Monitoring: “SANS Top 5 Reports for Intrusion Monitoring” on [page 234](#)
- Network Monitoring: “SANS Top 5 Reports for Network Monitoring” on [page 301](#)

What's Next

Chapter 2 describes the installation and configuration process. The remaining chapters describe each of the standard content foundations, including additional configuration, implementation, and run-time details.

Standard Content Installation, Upgrade, and Configuration

The content required for basic ArcSight functionality is installed automatically with ArcSight ESM. The foundations are available optionally through the ESM installer. Once the content is installed, some basic configuration is recommended to tailor the content for your operating environment.

This chapter describes how the standard content is installed, or upgraded, and provides instructions for basic configuration. Depending on which foundation packages you install, additional configuration may be required, which is discussed in the individual foundation chapters to follow.

- [“How Standard Content is Installed and Upgraded” on page 17](#)
- [“Standard Content Package Overview” on page 25](#)
- [“Configuration Planning” on page 28](#)
- [“Network Modeling” on page 29](#)
- [“Configure Resources with Network-Specific Values” on page 35](#)
- [“Trends” on page 43](#)

How Standard Content is Installed and Upgraded

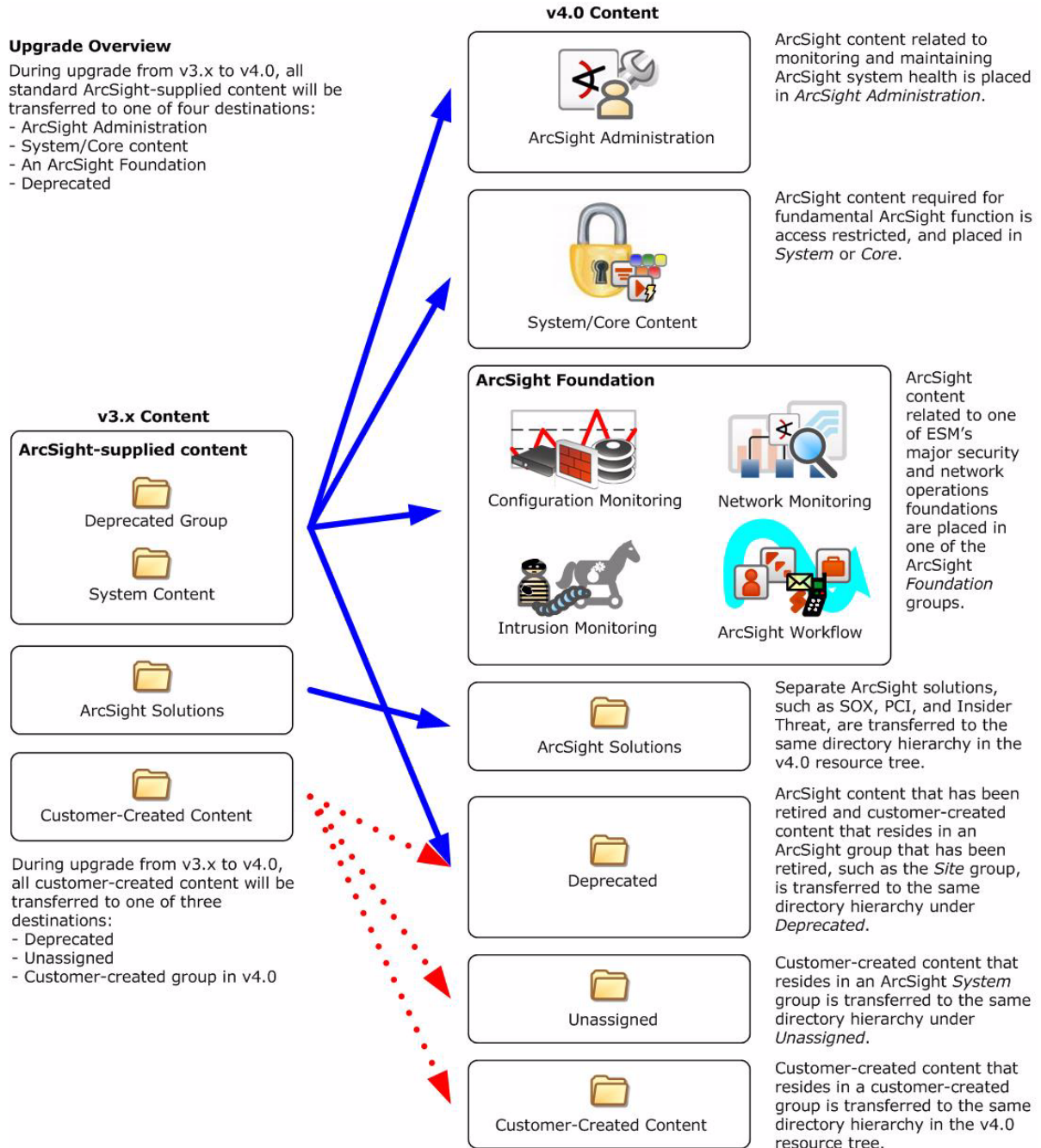
The ArcSight ESM v4.0 installer manages both fresh installs and upgrades from ESM versions 3.0 and 3.5.

The *Installation and Configuration Guide for ArcSight ESM v4.0* describes how to prepare for and install ArcSight ESM. Upgrade instructions are provided in the tech notes *Upgrading ArcSight™ ESM v3.5 SP2 to v4.0 GA* and *Upgrading ArcSight™ ESM v3.0 SP2 to v4.0 GA*.

This section provides more background about how the installer upgrades existing ArcSight-supplied content and customer-created content.

Standard Content Upgrade Overview

The resources that are installed with ESM have been updated, rearranged, or in some cases, deprecated (no longer in use) for ESM version 4.0. The diagram below illustrates how ArcSight-supplied content and customer-created content are migrated during the v3.x upgrade to v4.0.



ArcSight-supplied content is transferred to one of the active v4.0 foundations, ArcSight Solutions, or deprecated, as shown by the blue solid arrows. Customer-created content (resources created from scratch, or copied and modified from existing ArcSight content with a unique resource ID) is all preserved during the upgrade, and is migrated to different locations depending on where it was located in the v3.x structure, as indicated by the red dotted arrows:

- **Deprecated v3.x Group:** Customer-created content that resides in a v3.x group that has been deprecated is transferred to the same directory hierarchy in the v4.0 *Deprecated* group for that resource type. For more about deprecated resources, see the next section.
- **ArcSight System Group:** Customer-created content that resides in an ArcSight System group in v3.x is transferred to the same directory hierarchy in the v4.0 *Unassigned* group for that resource type.
- **Customer-Created Group:** Customer-created content that resides in a customer-created group in v3.x is transferred to the same directory hierarchy in the v4.0 resource tree.

Deprecated Resources and Resource Groups

Some of the v3.x resources and resource groups have been deprecated, meaning they are no longer needed. Resources are deprecated for several reasons:

- The resource was too product or vendor specific
- The resource was inefficient, or presented marginal value (for example, a collection of 10 reports was really one report with nine small variations)
- New v4.0 features accomplish the same goal more efficiently

During the upgrade, resources that have been deprecated are moved to a separate *Deprecated* group for that resource type. The resources that are moved into it retain the hierarchy they had in their original v3.x form. Resources moved to this folder are still active, so if you rely on any of these resources, they will still be present and operational.



If you have built resources that refer to a deprecated resource, or if you have modified a deprecated resource to refer to a resource that has not been deprecated, some connections could be broken during upgrade.

If you still need to use the deprecated resource, resolve the broken reference by moving the deprecated resource back into the active resource tree and changing the conditions as needed.

If you no longer need the deprecated resources, you can safely delete them after the upgrade.

If you still rely on a deprecated resource, you can move it back into an active resource tree and modify its conditions, as necessary, to repair any broken references.



Deprecated resources are no longer supported by ArcSight, so if you choose to restore a deprecated resource, you are responsible for its maintenance.



It is also recommended that you verify whether the new v4.0 resources address the same goal more efficiently. To determine this, refer to the *ArcSight System Content Reference Guide*.

After v4.0 is installed, you can generate a list of deprecated resources using the *Find Resource* function:

- 1 In the ArcSight Console, go to **Edit > Find Resource**
- 2 Enter the keyword “*deprecated*” in the *Search Query* field and click **Find**.

Preparing Existing Content for Upgrade




Every content situation is a unique blend of ArcSight-supplied resources in various states, and customer-supplied resources: those created from scratch, and those created by copying and modifying an existing ArcSight resource. When preparing existing content for upgrade, consider the following:

- **Back up v3.x resources.** Always back up all resources before upgrading. Instructions for how to do this are contained in the *Upgrading ArcSight™ ESM v3.x SP2 to v4.0 GA* tech notes. In some cases, modifications you have made to existing ArcSight resources may need to be reconfigured manually after the upgrade, and you can use the backup copy as a reference during reconfiguration.
-  **Assets Resource.** The Asset resource is part of ArcSight’s asset model, which helps ArcSight keep track of the network devices participating in the event flow. During upgrade, all v3.5 assets upgrade seamlessly, and all v3.0 assets that belong to only one zone upgrade seamlessly into the v4.0 asset structure. For 3.0 assets that belong to more than one zone:
 - ◆ A v3.0 asset that belongs to more than one zone will be disabled during upgrade, and stored in the Disabled group in the v4.0 Assets resource tree.
 - ◆ Likewise, if a v3.0 asset has an IP address that falls outside the upgraded 4.0 IP address range of the zone it is assigned to, it will also be moved to the Disabled group in the v4.0 Assets resource tree.
 - ◆ After upgrade, disabled assets can be restored by manually fixing their IP address ranges to match those of valid v4.0 zones.
-  **Zones Resource.** Zones are used by ArcSight to identify the network devices that contribute to the event stream by their IP addresses.
 - ◆ If you made customizations directly to the standard ArcSight zones (with the original resource ID), the customizations you made will be overwritten during the upgrade. Be sure to back up these customizations so you can restore them manually after the upgrade.
 - ◆ If you created your own zones, any that overlap standard ArcSight zones are disabled and placed in the v4.0 Disabled Zones group.
 - ◆ Before upgrade, manually note what zones you have where in v3.x, and manually verify the location and status of these zones after the upgrade.

Checking Existing Content After Upgrade

After the upgrade is complete, do the following checks to verify that all your content has been successfully transferred to the v4.0 structures. Manually fix any content that migrated to an unwanted location, or whose conditions are no longer valid.

- **Check for Unassigned resources.** After the upgrade, check the Unassigned group in the resource tree for all resource types. If you find resources in them, move them to other groups, as appropriate. ArcSight recommends against moving these resources into ArcSight standard content groups, as they will be moved to the Unassigned group again when future upgrades occur.

- **Restore customizations to resources with the original resource IDs.** If you had custom configurations to any resource with an original ArcSight resource ID, restore your configurations manually after upgrade is complete from the backed up version you saved before upgrade.
-  **Assets Resource.** The Disabled group in the assets resource tree is dynamic, which means it queries the Manager every two minutes for assets that have been disabled. After upgrade, check to see if any assets were disabled and moved to the Disabled group in the Assets resource tree.
 - ◆ If so, review the disabled asset to see the reason it was disabled and fix it as appropriate.
 - ◆ If the asset IP address is outside the range of the upgraded zone, either expand the range of the zone, or assign the asset to another zone.
 - ◆ You can also delete an asset that has become disabled if it is no longer needed (right-click the asset and select **Delete**).
-  **Users Resource.** Starting with v4.0, only the system user has access privileges to the `/All Users` resource tree (for more about the v4.0 system user, see [“ArcSight System User” on page 14](#)). Therefore, any users or groups you created in `/All Users` in the previous installation are now available under `Custom User Groups`.
 After upgrade, verify that your user ACLs are correct and make sense in light of how ArcSight standard content is organized for v4.0. For example, Administrator access should only be granted to those with authority to work with system-level content, such as ArcSight System and ArcSight Administration. Update user ACLs manually as appropriate.
-  **Zones Resource.** The zones resource tree is also a dynamic group that is regularly updated with new zone information from the Manager every two minutes. Check to see if any zones were invalidated during the upgrade process.
 - ◆ Fix zones that may have become invalid during upgrade that you want to keep.
 - ◆ Verify that the assets assigned to zones that have been moved or invalidated during the upgrade retain their connections to the appropriate v4.0 zones.
 - ◆ Delete any invalid zones that you no longer want to keep.
 - ◆ If you made customizations to the standard v3.x zones, manually edit the new resource to restore the customizations you made to the v3.x zone. Do not import the old zone.
- **Review and delete Deprecated resources.** The Deprecated groups in each resource type contain ArcSight resources that have been retired, and any customer-created resources that were located in a v3.x *Site* group. Review the resources located in these trees for any resources you still want. The resources in this group are still operational and evaluate the event stream until you delete them.
- **Review and move Unassigned resources.** The Unassigned groups in each resource type contain any customer-created resources that were located in a v3.x *System* group. Review these resources and relocate the ones you still need to active v4.0 groups.
- **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” on page 22](#).
- **Verify that customer-created content still behaves as expected.** Customer-created content that refers to ArcSight system content that has been significantly changed may not work as expected. Follow the pointers in [“Verify Proper Function of](#)

[Customer-Created Content](#) on page 23 to verify that your content still behaves as expected.

Fixing Invalid Resources



During the upgrade process, the content is run through a resource validator, which verifies that the values expressed in the resource's condition statement still apply to the resource in its new v4.0 format, and that any resources upon which it depends are still present and also valid. The resource validator is run on any resource that contains a condition statement, or populates the asset model:

- 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 customer-created or modified resource can become invalid. For example, if the schema of an ArcSight-supplied active list has changed from v3.x to v4.0, and a customer-created resource reads entries from this list, the condition statement in the customer-created resource will no longer match the schema of the v4.0 active list, and the logic will be invalid.

Persist Conflicts to the Database

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 gives you the choice to save the reason the resource was invalid in the database (**Persist conflicts to the database=TRUE**). If you choose this option, the upgrade installer:

- Saves the reason the resource was found to be invalid in the database, so you can generate a list of invalid resources, which you can use later to manually repair the problems.
- 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 was invalid in the database (**Persist conflicts to the database=FALSE**), the resources remain enabled, which means they try to evaluate the event stream in their invalid state.



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

Fixing and Re-Enabling Invalid Resources

To fix an invalid resource, use the report generated by the upgrade process to locate the resources and understand what needs to be fixed.

When the problem that makes the resource invalid is fixed, the system automatically re-validates the resource when the fix is applied. If the resource was disabled, the system automatically re-enables the resource.

Verify Proper Function of Customer-Created Content

It is also possible during upgrade that updates to the ArcSight standard content could cause resources you created to work in a way that is not intended. This case is harder to detect, because the resource condition is valid, but it may show more subtle symptoms, such as a rule getting triggered too often, or a rule that should be getting triggered is not getting triggered at all.

For example, this could happen if you have a rule that uses an ArcSight System filter whose conditions have been changed such that rule matches more events than you expect, or doesn't match the events you expect. Another example is a moving average data monitor whose threshold has been changed.

To verify that the resources you rely upon work as expected, go through the following checks:

- Send events that you know should trigger the content through the system using the Replay with Rules feature. For more about this feature and how it's been enhanced for v4.0, see the online Help topic *Verifying Rules with Events*.
- Check the Live or All Events active channel to verify if the correlation event is triggered, and check that data monitors you created are returning the expected output based on the test events you send through.
- Verify that notifications are sent to the recipients in your notification destinations as expected.
- Check that any active lists you have created to support your content are gathering the replay with rules data as expected.

Changes to Expect After the Upgrade

Beyond deprecated, unassigned, and invalid resources, some resource types themselves have been renamed, and thus have a new home in the v4.0 structure.

- **Active Lists are now part of Lists.** ESM v4.0 introduces the Session List, a new list resource that tracks session start and end data every time a user logs on and off the system as part of ESM v4.0's identity management feature. Active lists and Session lists share a spot on the resource tree under the heading Lists.
- **Agents are now Connectors.** To more accurately describe what they do, ArcSight SmartAgents are now called SmartConnectors, or Connectors for short in the ArcSight Console.

Core Customer-Configured Filters

There are several ArcSight standard filters that you may have configured to support auto-asset and device creation, SNMP trap forwarding, and network management as it applies in your situation. Any configurations you have made to these resources will be preserved, and the assets moved to the new 4.0 data structure as indicated in the table below.

Filter Name	3.x Location	4.0 Location
Agent Asset Auto Creation Events	/All Filters/ArcSight System Administration/Agent Asset Auto Creation Events	/All Filters/ArcSight System/Asset Auto Creation/Connector Asset Auto Creation Events
Device Asset Auto Creation Events	/All Filters/ArcSight System Administration/Device Asset Auto Creation Events	/All Filters/ArcSight System/Asset Auto Creation/Device Asset Auto Creation Events

Filter Name	3.x Location	4.0 Location
Network Management	/All Filters/Site Filters/Device Type Filters/Network Management	/All Filters/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Network Management
SNMP Trap Sender	/All Filters/System Filters/SNMP Trap Sender	/All Filters/ArcSight System/SNMP Forwarding/SNMP Trap Sender

For more about what these filters do and how to configure them, see [“Configure Asset Auto-Creation Filters”](#) on page 35.

Standard Content Package Overview

The standard content is presented as a set of packages during the configuration phase of the ArcSight Manager installation. In the configuration wizard, you will be prompted to select the packages you want to install.

Package	Description
ArcSight Administration (not shown in installer)	The ArcSight Administration foundation is a series of interactive resources that provide statistics about the health and performance of ArcSight ESM and its components. This package is required for ArcSight operation, and is installed automatically.
Anti-Virus	<p>This package contains a set of anti-virus resources, which is shared by the Configuration Monitoring and Intrusion Monitoring foundations. For example, the Configuration Monitoring <i>Anti-Virus Updates – All – Failed</i> and the Intrusion Monitoring <i>Anti-Virus Updates – Regulated Systems – Failed</i> both use the <i>AV – Failed Updates</i> filter, which is delivered as part of the anti-virus package).</p> <p>If installed by itself without the Configuration Monitoring or Intrusion Monitoring foundations, the anti-virus content will work independently.</p> <p>For more about the contents of the anti-virus package, see “Shared Package Inventory” on page 361.</p>
Configuration Monitoring	<p>Provides the ability to monitor configuration changes.</p> <p>The configuration monitoring foundation is an interactive suite of resources that provide insight into the current configuration of your monitored hosts, users, and network infrastructure, monitors them for changes, and sends notifications as appropriate.</p>
Intrusion Monitoring	<p>Provides the ability to monitor intrusions in the network.</p> <p>The intrusion monitoring foundation is an interactive suite of resources that provide statistics about intrusion-related activity on the network that can be used for monitoring and investigation as well as routine monitoring and reporting.</p>
Network Filters (required package, cannot be deselected)	<p>Set of filters required by the Intrusion Monitoring and Network Monitoring foundations.</p> <p>This package is required by the Configuration Monitoring, Intrusion Monitoring, and ArcSight Administration foundations, and is installed automatically.</p>
Network Monitoring	<p>Provides the ability to monitor traffic and network usage.</p> <p>The network monitoring foundation is an interactive suite of resources that monitor the status of the network and network infrastructure.</p> <p>For more about the contents of the network monitoring package, see “Shared Package Inventory” on page 361.</p>

Package	Description
Workflow	<p>The workflow foundation provides active channels for tracking events to be investigated, and reports that track notifications and cases, ArcSight ESM's built-in trouble-ticket system.</p> <p>The ArcSight Workflow foundation is a system of active channels and reports that support incident response tracking.</p>

By default, all the packages are selected. Some packages are required for ESM function and cannot be deselected, and others are optional, depending on how you want to use ESM. Deselect any packages you do not wish to install.

Package States: Imported and Installed

A package can exist in two states in the Console: imported and installed.

Package Installed 	 Package bundle imported to Manager	 Resources installed in database	 Resources available in resource tree
Package Imported (Package Not Installed or Uninstalled) 	 Package bundle imported to Manager	 Resources not installed in database	 Resources not available in resource tree

If you selected all the standard content packages to be *installed* at installation time, the packages and their resources will be installed in the ArcSight database and available in the Navigator panel resource tree. The package icon in the Navigator panel package view will appear blue.

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



If you do not plan to use the content in a particular package, it is recommended that you exclude it from the installation for system performance reasons.

For example, if you don't have a network traffic reporting device, most of the Network Monitoring content will not work, and having its rules, data monitors, and trends operating on the event stream will impact system performance.

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

Packages can also be used to share resources among multiple Managers. In this case, you can create, export, and import packages. When a package is imported from one Manager to another, it must also be installed to make its resources available in the Navigator panel resource tree.

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

- 1 In the Navigator panel Package view, navigate to the package you wish to install
- 2 Right-click the package and select **Install Package**. 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 wish to uninstall
- 2 Right-click the package and select **Uninstall Package**. 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 wish to delete
- 2 Right-click the package and select **Delete Package**. When you right-click a package and select **Delete Package**, there are two options:
 - a **Delete Resources**: this will delete the package *and* all the resources from that package (the package AND the resources in the navigator trees are gone)
 - b **Leave Resources**: this will only delete the package. The package will be removed from the package view, but the resources are still installed on the system and available in the resource tree.

For more about packages and how to use them, see the online Help topic *Managing Packages*.

Configuration Planning

To configure your installation, first model the network that will supply events to the foundation content.

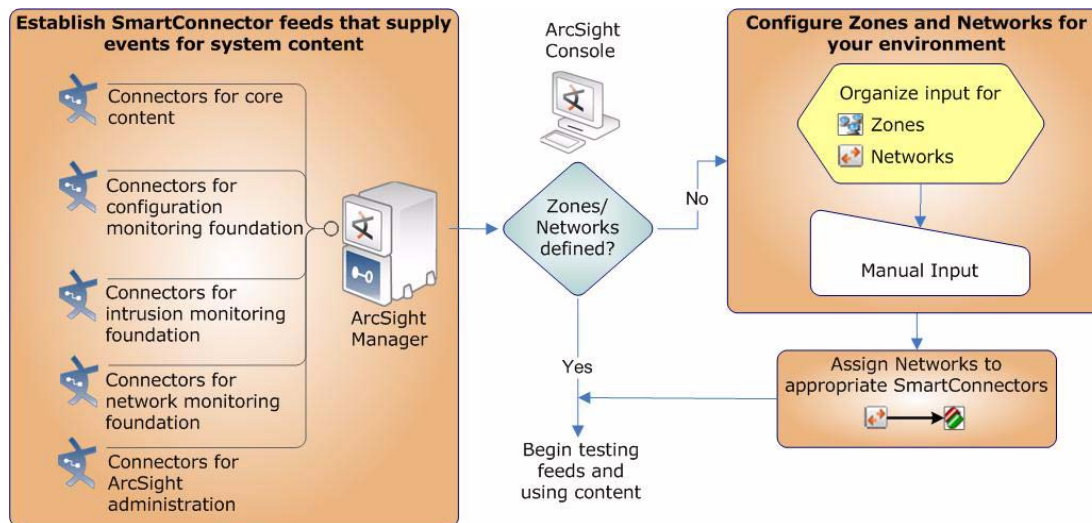


Figure 2-1 Configuring ESM standard content starts with installing SmartConnectors and configuring zones and networks for devices that report to ESM.

Standard Content-Related SmartConnectors


The standard content is designed to address event throughput, network health, and basic security-related scenarios. Depending on which packages you installed, verify that you have the minimum types of SmartConnectors reporting into ESM.


Package	Device Types
Anti-Virus (required by Configuration and Intrusion Monitoring foundations)	<ul style="list-style-type: none"> Anti-virus software
Configuration Monitoring	<ul style="list-style-type: none"> Operating systems Security applications (Network and host-based IDS, anti-virus) User management services (authentication, authorization, and accounting services) Basic network devices (firewalls, routers, switches, VPN)
Intrusion Monitoring	<ul style="list-style-type: none"> Network and host-based IDS Intrusion Prevention Systems (IPS) Anti-virus Firewalls
Network Monitoring	<ul style="list-style-type: none"> Real-time flow monitor (Qosient Argus)
Workflow	<ul style="list-style-type: none"> Trouble-ticket applications (such as BMC Remedy and HP OpenView)

Network Modeling

ArcSight ESM uses a model of the network to keep track of the network nodes participating in the event traffic.

Assets


 An asset is an ArcSight resource used to describe the network identity of an endpoint you consider significant enough to track using ArcSight.

 An asset range identifies a block of assets in a contiguous range of IP addresses where the individual identity of a particular endpoint in the range does not matter, such as a DHCP range.

The most common ways to populate your network model with assets is using output from a vulnerability or network scan, the Asset Import Connector (described in [“Assign Asset Categories Using the ArcSight Asset Import Connector” on page 33](#)), or custom transformation tools that take enterprise asset data and turn it into ArcSight Archive XML for import. Assets can also be modeled manually using the Asset editor in the ArcSight Console.

ESM automatically creates assets to model the network nodes that host ArcSight components. It also automatically creates assets for events received from device endpoints on your network that do not already have assets modeled in ArcSight. This auto-asset creation feature could require configuration, depending on the assets reporting in to ESM. For more about this feature and how to configure it, see [“Configure Asset Auto-Creation Filters” on page 35](#).

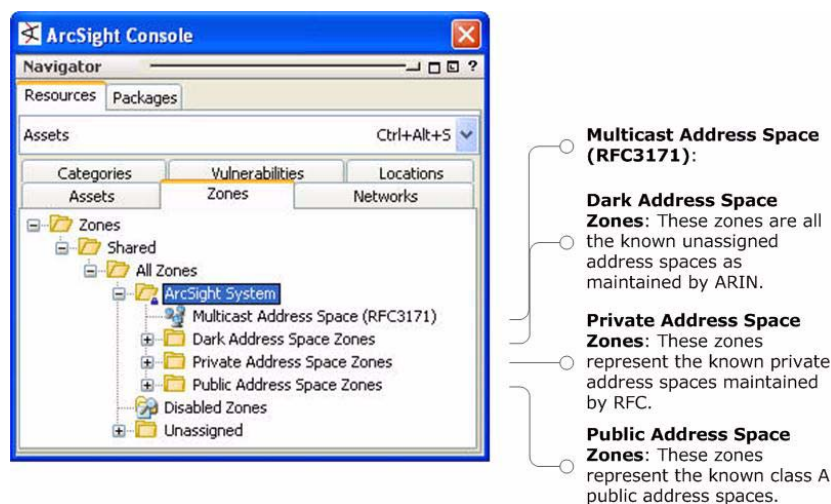
Zones

 Zones are ArcSight resources that represent parts of the network, and are identified by contiguous IP address ranges.

With ArcSight v4.0, every asset or address range is associated with a zone. ArcSight comes configured with the standard global IP address ranges already represented as zones, so if your network uses only these public IP addresses, ArcSight can resolve them without setting up any additional zones.


You would need to create your own zones if you have overlapping private networks. Private networks usually model a functional group within your network or a subnet, such as a wireless LAN, the engineering network, the VPN or the DMZ.

ESM comes with the following standard zones:



Use these zones, and create new zones, as necessary, to represent your overlapping private networks.

Networks

 Networks are ArcSight resources that are used to differentiate between zones whose IP ranges overlap, such as when branch locations assign the same private address spaces to resources in their locations.

Zones and networks only need to be configured if there are overlapping address ranges monitored by devices reporting into ArcSight agents

To learn more about ESM's network modeling tools and process, see Chapter 4, "ArcSight Network Model" in *ArcSight 101*. To find instructions for how to use the ArcSight Console to configure zones and networks, see the ESM Console online Help.

Asset Categories

Asset categories are ArcSight resources that describe the properties of an asset in terms of how it is used. Asset categories are one of the key ways that ESM adds differentiation, relevance, and context to the millions of events passing through your network.

Asset categories establish identity, ownership, and criticality of the assets on your network. Asset categories present an extensible schema that adds values to the business properties of your assets. The root of a particular category (for example, **Criticality** in the group [/All Asset Categories/System Asset Categories/Criticality](#)) defines the property itself, whereas the members of the category (for example, the criticality levels [Very High](#), [High](#), and so on) define the possible values for that property.

How ArcSight Determines the Protected Network

There is a set of filters in [All Filters/ArcSight Foundation/Common/Network Filters/Boundary Filters](#) that are used to determine whether a system is internal or external by checking to see if an asset or its zone is categorized with [/All Asset Categories/Site Asset Categories/Address Spaces/Protected](#).

By default, the Private Address Space Zones are categorized as *Protected*. Assets within a zone that has been categorized do not inherit categories from the zone. For example, an asset with an IP address of 192.168.0.1 is not automatically categorized as *Protected*, but it belongs to one of the Private Address Spaces zones, so it is considered *Internal* because it belongs to a zone categorized as *Protected*. This system provides a minimal structure to help discern between internal and external traffic if you do not have all your assets categorized.

Criticality Asset Categories for Priority Formula

The asset categories most essential to basic event processing are those used by the Priority Formula to calculate an event's criticality. Asset criticality is one of the 4 factors of the priority formula that combine to generate an overall event priority rating.

Asset criticality is based on one of the Criticality ratings assigned to the assets of your network using one of the following Criticality asset categories ([All Asset Categories/System Asset Categories/Criticality](#)):

- Very High
- High
- Medium
- Low
- Very Low
- Not categorized

Assigning criticality asset categories is not mandatory, but it is essential to activating features in the Foundation packages that enable ESM to provide its real-time evaluation of your network's security state. For more about the Priority Formula and how it leverages these asset categories to help assign priority to events, see *ArcSight 101*.

How to Assign Asset Categories

There are two main ways to assign asset categories:

- One by one or in groups using the Console UI
- In large batches using the ArcSight Asset Import Connector

Assign Asset Categories Using Console UI

Assign asset categories one by one using the Console UI if you have only a few assets to categorize as part of your monitoring program. One asset can be categorized in more than one asset category. You can also assign asset categories to groups of resources. This transfers the asset category onto all the members of the group and its sub-groups.

- 1 In the Navigator drop-down menu, go to **Assets**. Select the **Assets** tab. Go to [ArcSight System Administration/Agents](#), where you will find the agents installed for your environment.
- 2 Right-click the asset or asset group you wish to categorize and select **Edit Asset** (or **Edit Group**).
- 3 In the Inspect/Edit panel, click the **Categories** tab. Click the add icon (+) at the top of the screen.
- 4 In the Asset Categories Selector pop-up window, select the asset categories that apply to this asset and click **OK**. For example:
 - a The usage category that applies to the asset (for example, [/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Generates Financials](#))
 - b The criticality level that applies to the asset (for example, [/All Asset Categories/System Asset Categories/Criticality/Very High](#))
- 5 Repeat steps 3 and 4 for every asset or group of assets you wish to classify in one of the ESM asset categories.

Assign Asset Categories Using the ArcSight Asset Import Connector

If you have many assets that you want to track as part of your standard ESM monitoring program, you can configure them in a batch using the ArcSight Asset Import Connector. This connector can also create new assets as part of the batch function.

The ArcSight Asset Import Connector is available as part of ArcSight's connector download. For instructions about how to use this connector to configure your assets, see the *ArcSight Asset Import SmartConnector Configuration Guide*. The steps below outline the process involved.

- 1 Create a comma-separated value (CSV) file in a spreadsheet that contains the following data for each asset you wish to create and categorize in one or more asset category:

Header name	Data description
address	IP address of the asset
macAddress	Mac address of the asset with colons between the hexadecimals: 00:10:V6:VCO:CA:35
hostName	Fully qualified host name of the asset
location	ArcSight asset location. This is an ArcSight URI, and may not be applicable in all environments.
category:N	The complete ArcSight URI of the asset category in which you wish to categorize the asset. Replace N with the name of the asset category. Add a category column for every asset category that applies to the asset.

The CSV file must contain these columns, although each row need not contain a value. You can add as many Category columns as you need to, but there must be at least one. For details, see the *Asset Import Connector* guide.

- 2 Install the ArcSight Asset Import SmartConnector according to the instructions in the *ArcSight Asset Import SmartConnector Configuration Guide*.
- 3 Assign the SmartConnector to an ArcSight Network.
- 4 Copy the CSV file into the target directory on the Connector system. As soon as the CSV file is imported into the Connector's target directory, the Manager consumes the file and populates the asset model with your asset data.

Sample Asset Import Template

The table below shows the first five rows of a sample Asset Import table template, which you can use to populate your asset lists and asset categories. Your table can have as many **category:** rows as required to classify the asset in all the categories that apply.

address	mac Addr	hostName	location	category:Criticality	category:Business Role
10.0.0.1	00 00 00 11 11 11	servername1. customer.com	/All Assets/ CustomerX/ Support	/All Asset Categories/ System Asset Categories/Criticality/ High	/All Asset Categories/ Site Asset Categories/ Business Impact Analysis/Business Role/ Infrastructure/Network
10.0.0.2	00 00 00 11 11 12	servername2. customer.com	/All Assets/ CustomerX/ ArcSight	/All Asset Categories/ System Asset Categories/Criticality/ Very High	/All Asset Categories/ Site Asset Categories/ Business Impact Analysis/Business Role/ Security
10.0.0.3	00 00 00 11 11 13	servername3.c ustomer.com	/All Assets/ CustomerX/ E- mail	/All Asset Categories/ System Asset Categories/Criticality/ Medium	/All Asset Categories/ Site Asset Categories/ Business Impact Analysis/Business Role/ Security
10.0.0.4	00 00 00 11 11 14	servername4. customer.com	/All Assets/ CustomerX/ CorporateNet	/All Asset Categories/ System Asset Categories/Criticality/ High	/All Asset Categories/ Site Asset Categories/ Business Impact Analysis/Business Role/ Infrastructure/Network
10.0.0.5	00 00 00 11 11 15	servername5. customer.com	/All Assets/ CustomerX/ PS	/All Asset Categories/ System Asset Categories/Criticality/ Very High	/All Asset Categories/ Site Asset Categories/ Business Impact Analysis/Business Role/ Generates Financials

Configure Resources with Network-Specific Values

In order to work as expected, some standard resources should be configured with values specific to your network environment.

Configure Asset Auto-Creation Filters

A standard feature of ESM is that it automatically creates assets in the ArcSight asset model for events whose devices are not already modeled either manually or using an asset scanner.

Depending on what devices you have reporting to ArcSight and what devices report in to your network, however, this can potentially cause a lot of unnecessary individual assets to be added to your asset model. For example, laptops with the intrusion detection system BlackICE from ISS can generate a new asset ID for that device every time the laptop logs onto the network. This situation also applies to VPN and wireless networks every time a device logs onto a new subnet.

Likewise, if an ArcSight Connector reports from a DHCP subnet, every time a system is assigned a DHCP address, ESM would model a new Connector, which falsely clutters the network model with Connector nodes.

To limit how ESM automatically models assets in these cases, ArcSight provides two filters in the ArcSight System group that you can configure with the names of devices and Connectors that you need to include or exclude from the auto-creation feature.



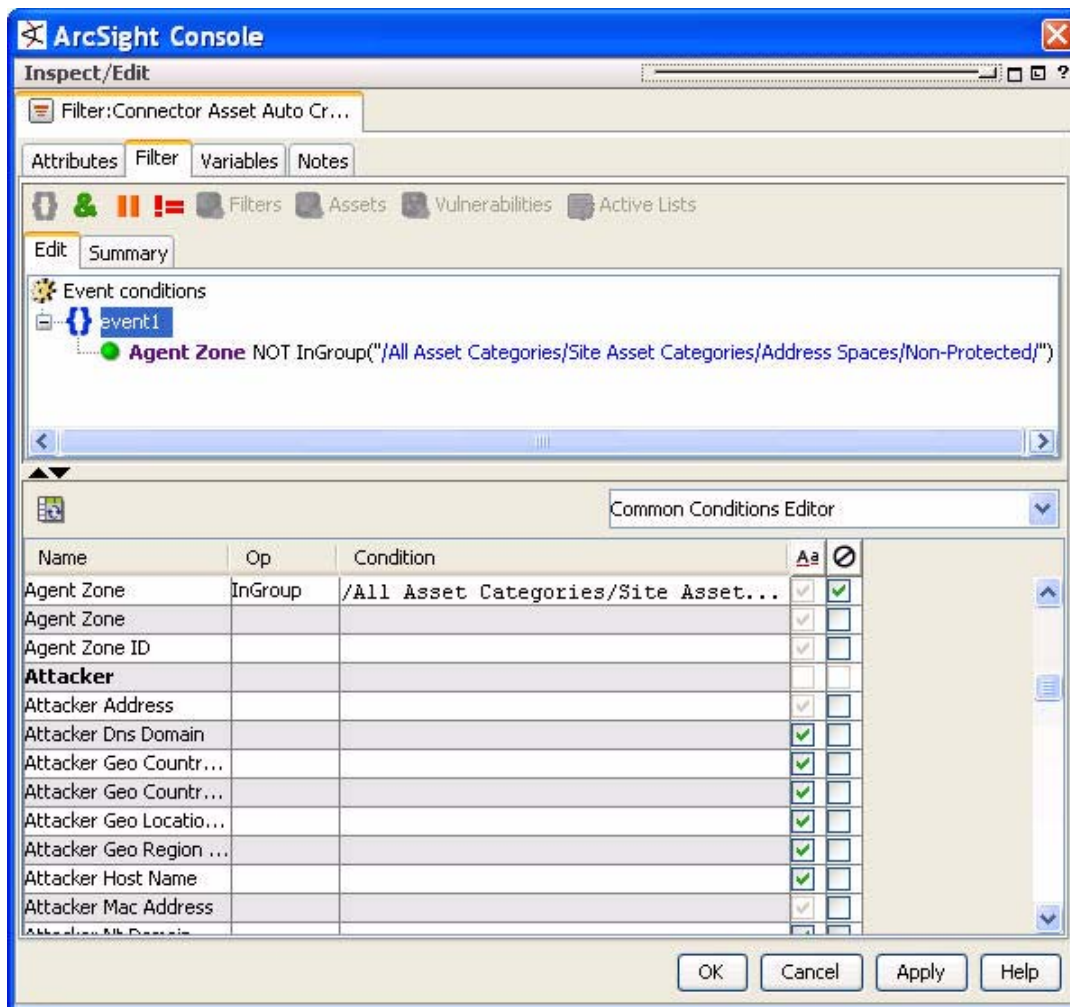
The Auto Asset Creation filters are part of the locked system content. The filters cannot be moved or renamed, but they can be configured by users who have write privileges to them, in this case, ArcSight Administrators and Analyzer Administrators.

Configure Connector Asset Auto-Creation Events Filter

By default, the *Connector Asset Auto Creation Events* filter is configured with the generic condition **True**, which matches all events. As necessary, you can configure this filter to specify assets to exclude from the asset auto creation feature.

One way to configure the filter is to exclude connectors from a specific zone, such as a VPN zone, where the asset already exists, but traffic is coming into the network from an alternate VPN interface. You can also exclude traffic from different types of Connectors, such as from a particular device and vendor.

The example below shows the *Connector Asset Auto Creation Events* filter configured to exclude Connector traffic coming from devices categorized as being in non-protected address spaces.



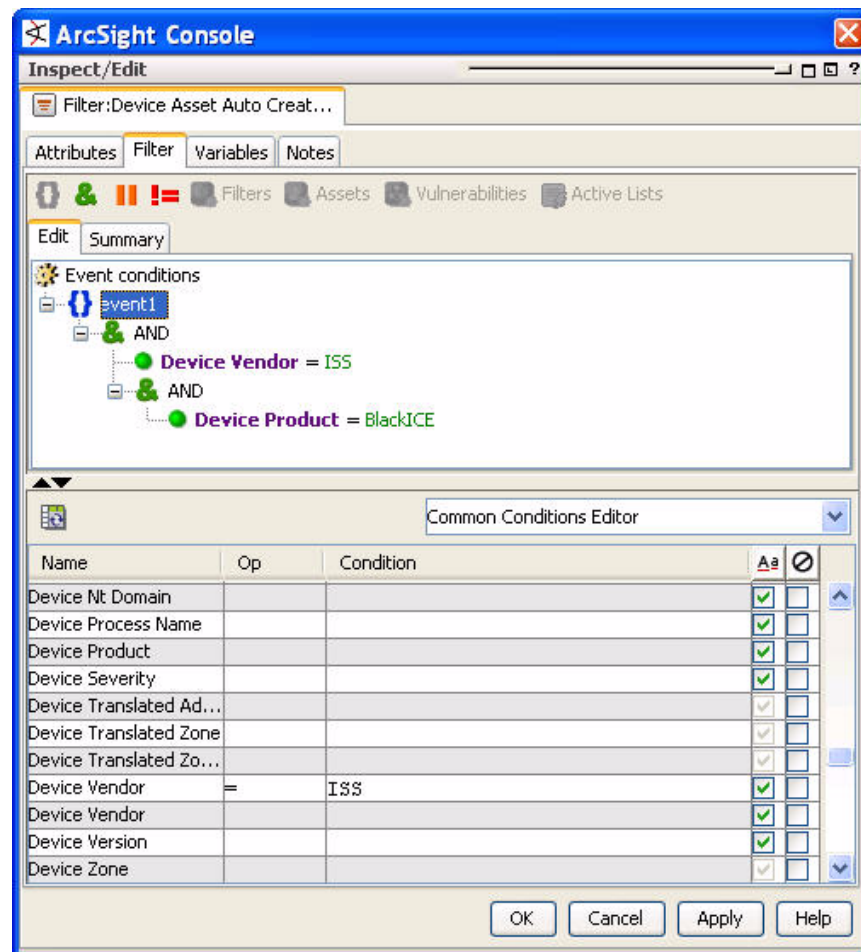
- 1 In the Navigator panel, navigate to the Connector Asset Auto Creation Events filter ([All Filters/ArcSight System/Asset Auto Creation](#)) and double-click it to open it in the Inspect/Edit panel.
- 2 In the Filter editor in the Inspect/Edit panel, select the **Filter** tab. Delete the default condition **True** (select the condition and press **Delete**).
- 3 In the event fields grid at the bottom of the pane, select **Agent Zone**.


- 4 In the Op column, select the **InGroup** operator.
- 5 In the Condition column, select the non-protected asset category from the drop-down menu.
- 6 Select the NOT checkbox (⊖).
- 7 Repeat steps 3 through 5 for every device and device vendor whose events you want to exclude from the auto asset creation feature.
- 8 Click **OK** to apply changes and close the Filter editor.

Configure Device Asset Auto Creation Events Filter

By default, the *Device Asset Auto Creation Events* filter is configured with the generic condition **True**, which matches all events. As necessary, you can configure this filter to specify traffic from specific devices and device vendors, or event categories, such as Hostile. When you specify an event category, the filter dictates that assets be created only for events with this severity.

The example below shows the *Device Asset Auto Creation Events* filter configured to only create assets for traffic coming from the ISS intrusion detection scanner BlackICE.



- 1 In the Navigator panel, navigate to the Connector Asset Auto Creation Events filter ([All Filters/ArcSight System/Asset Auto Creation](#)) and double-click it to open it in the Inspect/Edit panel.
- 2 In the Filter editor in the Inspect/Edit panel, select the Filter tab. Delete the default condition **True** (select the condition and press **Delete**).
- 3 Select **event1** and add an AND operator (click the AND icon .
- 4 Select **event1** and use the event fields grid to build the condition, or right-click **event1** and select **New Condition**. Navigate to **Device > Device Vendor**. In the Condition field, enter the vendor name, in this case **ISS**.
- 5 Add the device vendor and product you wish to include.

- a** If you are adding only one device vendor and product pair, select the Device Vendor condition and add another **AND** operator. Navigate to Device > Device Product. In the Condition field, enter the device name, in this case **BlackICE**.
- b** If you are adding more than one device vendor and product pair, select the Device Vendor condition and add an **OR** operator. Navigate to Device > Device Product. In the Condition field, enter the device name.

For example, the condition would look like this:

```
OR
  AND
    Device Vendor A
    Device Product 1
  AND
    Device Vendor B
    Device Product 2
  AND
    Device Vendor C
    Device Product 3
```

- 6** Repeat steps 3 through 6 for every device and device vendor whose events you want to exclude from the auto asset creation feature.
- 7** Click **OK** to apply changes and close the Filter editor.

Configure SNMP Trap Forwarding Filter

If you do not have SNMP traps enabled, you can skip this section and move on to [“Configure Active Lists” on page 41](#).

The System filters group contains an SNMP Trap Sender filter ([All Filters/ArcSight System/System/SNMP Forwarding/SNMP Trap Sender](#)). The SNMP Trap Sender filter only needs to be configured if you have the SNMP Trap Sender enabled to forward events via SNMP to a network management system, such as HP Openview.

By default, this filter is configured with the filter [/All Filters/ArcSight System/Event Types/ArcSight Correlation Events](#). If you leave this default setting and you have SNMP forwarding enabled, all ArcSight correlation events will be trapped and forwarded to the network management system.

To configure this filter to forward certain events as an SNMP trap, you can do either of the following:

- Change the default condition in the SNMP Trap Sender filter so it expresses which events should be forwarded as traps. You can express this condition directly in the SNMP Trap Forwarding filter, or you can create another filter that expresses these parameters and point to it in the SNMP Trap Sender filter.
- Change the server configuration (via [server.properties](#)) to point the SNMP trap sender to another filter, and set that filter up as per your convenience.

Change Default Condition in SNMP Trap Forwarding Filter

- 1 In the Navigator panel, navigate to [All Filters/ArcSight System/SNMP Forwarding/SNMP Trap Sender](#). Double-click the filter or right-click and select **Edit** to open it in the Filter editor in the Inspect/Edit panel.
- 2 At the Filter tab, change the default condition [/All Filters/ArcSight System/Event Types/ArcSight Correlation Events](#) to list the type(s) of events you want forwarded, or to point to another filter that expresses these parameters.

For example, you can create a filter that specifies all events with a priority greater than 8, or events from all Top Secret systems.

Change SNMP Trap Sender in server.properties

If you wish to use a filter other than the default [/All Filters/ArcSight System/SNMP Forwarding/SNMP Trap Sender](#), you must point the SNMP trap sender to the new filter in the Manager's `server.properties` file.



These instructions apply **only** if you have SNMP forwarding already enabled at the Manager, *and* if you are using a filter other than the default SNMP Trap Sender filter to forward events.

If the SNMP forwarding feature is not already enabled at the Manager, the `server.properties` file will not contain the string that needs to be modified.

- 1 On the ArcSight Manager machine at a command line, stop the Manager service.
 - ◆ Unix: `/etc/init.d/arcsight_manager stop`
 - ◆ Windows: Stop the ArcSight Manager service from the **Control Panel > Administrative Tools > Services** menu
- 2 Make a backup copy of the file `$ARCSIGHT_HOME/config/server.properties`.
- 3 In a text editor, open the file `$ARCSIGHT_HOME/config/server.properties` and look for the following lines:

```
# -----
# SNMP Trap Sender configuration.
# -----
# Configuration for the SNMP trapsender. Copy these properties into
# your server.properties file and remove the '#'s (comments). By
# default, the SNMP trap sender is disabled.
#
# set the following property to true to enable trap sending
snmp.trapsender.enabled=false

# Filter that determines what arcsight events will be sent out as traps
snmp.trapsender.uri=/All Filters/ArcSight System/SNMP Forwarding/SNMP
Trap Sender
```

- 4 Change the `snmp.trapsender.uri` from [/All Filters/ArcSight System/SNMP Forwarding/SNMP Trap Sender](#) to the URI for the filter you want to use.
- 5 Save and close the `server.properties` file.
- 6 Restart the Manager service.
 - ◆ Unix: `/etc/init.d/arcsight_manager start`
 - ◆ Windows: Start the ArcSight Manager service from the **Control Panel > Administrative Tools > Services** menu

To enable the SNMP trap sender, follow the instructions outlined in the *ArcSight Administrator's Guide* in chapter 4, *Configuration*.

Configure Active Lists

Several of the standard content foundations use static active lists, which retain specific data that you enter, which can be cross-referenced dynamically by resources that use conditions, such as active channels, filters, rules, reports, and data monitors. For details about active lists and how they are used by ESM, see *ArcSight 101* and the topic *Active Lists* in the online Help.

The static active lists that should be configured are:

- **Trusted/Untrusted** active lists in ArcSight Core (see [“Configure Asset Auto-Creation Filters” on page 35](#))
- **Local User Allowed Systems** in Configuration Monitoring (see [“Required Configuration” on page 74](#))

The active lists that store static data should be configured with data specific to your environment so the data can be evaluated by ESM rules. Active lists that are populated automatically with event data need not be configured before being used.

Static active lists can be populated two ways:

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

Configure Active Lists Using Console Active List Editor


For instructions about how to configure active lists, see the topic *Managing Active Lists* in the online Help.

Configure Active Lists from Imported CSV

- 1 In the Navigator panel, navigate to the active list you want to configure ([Lists > Active Lists](#)).
- 2 Generate a CSV file with the values with which you wish to populate the active list, and save it to a directory on the Console system.
- 3 Right-click the active list you wish to import the values into and select **Import CSV File...**
- 4 In the Open dialog box, navigate to and select the CSV file and click **Open**.

Configure Dynamic Active Lists

The Threat Tracking active lists in the ArcSight System group (described in [“Threat Tracking Active Lists” on page 57](#)) are dynamic, which means they are populated during run-time by threat escalation rules when events match the escalation conditions. You may, however, need to escalate or de-escalate a user or address manually from one list to the next. To add entries manually:

- 1 In the Navigator panel, go to [Lists/Active Lists/All Active Lists/Arc-Sight System/Threat Tracking/](#).
- 2 Right-click the active list you wish to populate with entries and select **Show Entries**.
- 3 In the active list details view in the Viewer panel, click the add icon () in the active list header.
- 4 In the ActiveListEntry Editor in the Inspect/Edit panel, add or edit entries for the appropriate columns and click **Add**. The *Creation time*, *Last seen time*, and *Count* columns should be left blank, as the system will fill them in at run-time.

Trends

ESM 4.0 introduces trends, a type of query 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 a snapshot of which devices report on the network over a series of days.

The standard content contains 34 trends that monitor long-term conditions among the ArcSight foundations, as outlined in the following sections.

Based on the volume of data generated by some of these queries, only 20 of the 34 trends are enabled by default at installation; 14 of the trends are disabled by default.

The enabled trends are scheduled to run on an alternating schedule between the hours of midnight and 7:00 a.m., when network traffic is usually slower than during normal business hours. These schedules can be customized to suit your needs using the Trend scheduler in the Console.

ESM's standard trends are listed below with their status on installation, and the time at which they are scheduled to run.

ArcSight Administration Trends

Both ArcSight Administration trends are enabled by default.

ArcSight Administration Trends	Status	Schedule
Trend Queries	Enabled	4:00 a.m.
ArcSight User Login Trends – Hourly	Enabled	5:00 a.m.

Configuration Monitoring Trends

Seven of the 13 Configuration Monitoring trends are enabled by default.

Configuration Monitoring Trends	Status	Schedule
Assets with Recent Configuration Modifications - Daily Trend	Enabled	12:40 a.m.
Asset Startup and Shutdown Events - Daily Trend	Enabled	2:40 a.m.
Critical System Startup and Shutdown Events - Daily Trend	Disabled	N/A
Most Common Account Login Attempts - Daily Trend	Enabled	3:40 a.m.
User Account Login Failures	Enabled	4:40 a.m.
AAA User Account Creation	Disabled	N/A
Accounts Deleted by Host	Disabled	N/A
Password Modifications	Disabled	N/A
User Account Creation	Enabled	5:40 a.m.

Configuration Monitoring Trends	Status	Schedule
User Account Modifications	Enabled	6:20 a.m.
VPN User Account Creation	Disabled	N/A
Vulnerability Exposure by Asset Criticality (Snapshot)	Enabled	1:40 a.m. once a week
Vulnerability Exposure of High and Very-High Criticality Assets by Zone - Daily Trend (Snapshot)	Disabled	N/A

Intrusion Monitoring Trends

Eight of the 16 Intrusion Monitoring trends are enabled by default.

Intrusion Monitoring (8/16)	Status	Schedule
SANS Top 20 (v6.01) Attacked Systems	Disabled	N/A
Prioritized Attack Counts by Service	Disabled	N/A
Prioritized Attack Counts by Target Zone	Disabled	N/A
Inbound DoS Events	Disabled	N/A
Environment Status Events	Disabled	N/A
Port Scanning	Enabled	1:20 a.m.
Port Scanning Daily Top 20	Enabled	2:20 a.m.
Reconnaissance Activity	Disabled	N/A
Reconnaissance Types Detected	Disabled	N/A
Zone Scanning Events by Priority	Enabled	4:20 a.m.
Resource Access	Disabled	N/A
Asset Counts by Vulnerability (Snapshot)	Enabled	12:20 a.m. once a week
Prioritized Vulnerability Events by Zone	Enabled	5:20 a.m.
Failed Logins per Hour	Enabled	6:00 a.m.
Top Users with Failed Logins per Day	Enabled	6:40 a.m.
Number of Vulnerabilities per Asset (Snapshot)	Enabled	3:20 a.m. once a week

Network Monitoring Trends

All three Network Monitoring trends are enabled by default.

Network Monitoring	Status	Schedule
Inbound Traffic by Application Protocol	Enabled	1:00 a.m.
Outbound Traffic by Application Protocol	Enabled	2:00 a.m.
Overall Traffic	Enabled	3:00 a.m.

How to Enable/Disable Trends



If you wish to enable a disabled trend, you must first **change the default start date** in the Trend editor, then enable it.

If the start date is not changed, the trend will take the default start date (which is derived from when the trend was first installed), and backfill the data from that time. For example, if you enable the trend 6 months after the first install, these trends will try to get all the data for the last 6 months, which would cause performance problems, overwhelm system resources, or cause the trend to fail if that event data is not available.

To enable a disabled trend:

- 1 Edit the trend to change the default start date.
 - a Double-click the trend, or right-click it and select **Edit Trend** to open it in the Trend Editor in the Inspect/Edit panel.
 - b In the Trend editor, click the **Parameters** tab. In the *Query Parameters* section, find Start Time and uncheck the **Use Default** checkbox.
 - c In the *Value* drop-down menu, select a start date appropriate for the frequency at which the trend is scheduled to run. For example, if the trend is scheduled to run daily, select a start date of a week or less earlier than today. Keep in mind the data partitioning schedule your Manager uses to make sure the time frame you have specified provides adequate online access to the events. Click **Apply**.
- 2 Enable the trend.
 - ◆ If the Trend editor is still open, click the Attributes tab and check the **Enabled** checkbox. Click **OK** to apply changes and close the Trend editor.
 - ◆ If the Trend editor is closed, right-click the trend in the Navigator panel and select **Enable Trend**.

To disable an enabled trend:

- In the Navigator panel, right-click the trend you want to enable and select **Disable Trend**.

How to Monitor Trend Performance

The ArcSight Administration foundation contains resources that enable you to monitor the performance of your enabled trends. The Trends Status dashboard (described in [“Resource Monitoring Data Monitors” on page 333](#)) shows the run-time status for all enabled trends. The Trend reports (described in [“Resource Monitoring Reports” on page 353](#)) show statistics about trend performance for all enabled trends.

What’s Next

The next chapter, ArcSight System, describes the essential ArcSight content required for ESM function.

Chapter 3

ArcSight System



The ArcSight System content consists of resources that ESM requires for basic security processing functionality, such as threat escalation and priority calculations, and basic throughput channels required for out-of-the-box functionality.

This content is installed automatically with ArcSight ESM so that these functions and the infrastructure that supports them are immediately available. The system content infrastructure also serves the systems and solutions you deploy, and ArcSight content you create yourself.

Some of the system content is intended to be configured by you during setup time; others are write protected.

System Content

Resources contained in the `/ArcSight System/` directories can be configured or modified as directed in [“Configure Resources with Network-Specific Values” on page 35](#).

Core Content

The `/ArcSight System/Core/` directories are locked, and cannot be deleted or renamed. Most of the Core content resources themselves are also locked. There are several filters in the Core content that can be configured as directed in [“Configure Asset Auto-Creation Filters” on page 35](#) and [“Configure SNMP Trap Forwarding Filter” on page 39](#).

This chapter describes all the system content that is automatically installed with ESM.

- [“System Content Overview” on page 48](#)
- [“Internal ArcSight Function” on page 48](#)
- [“Correlation Evaluation” on page 54](#)
- [“SOC Operations and Monitoring” on page 62](#)
- [“Benchmarking and Analysis” on page 66](#)

System Content Overview

The system content consists of a series of standard features and resources that support basic ESM function:

- Internal ArcSight Function
- Correlation Evaluation
- SOC Operations and Monitoring
- Benchmarking and Analysis

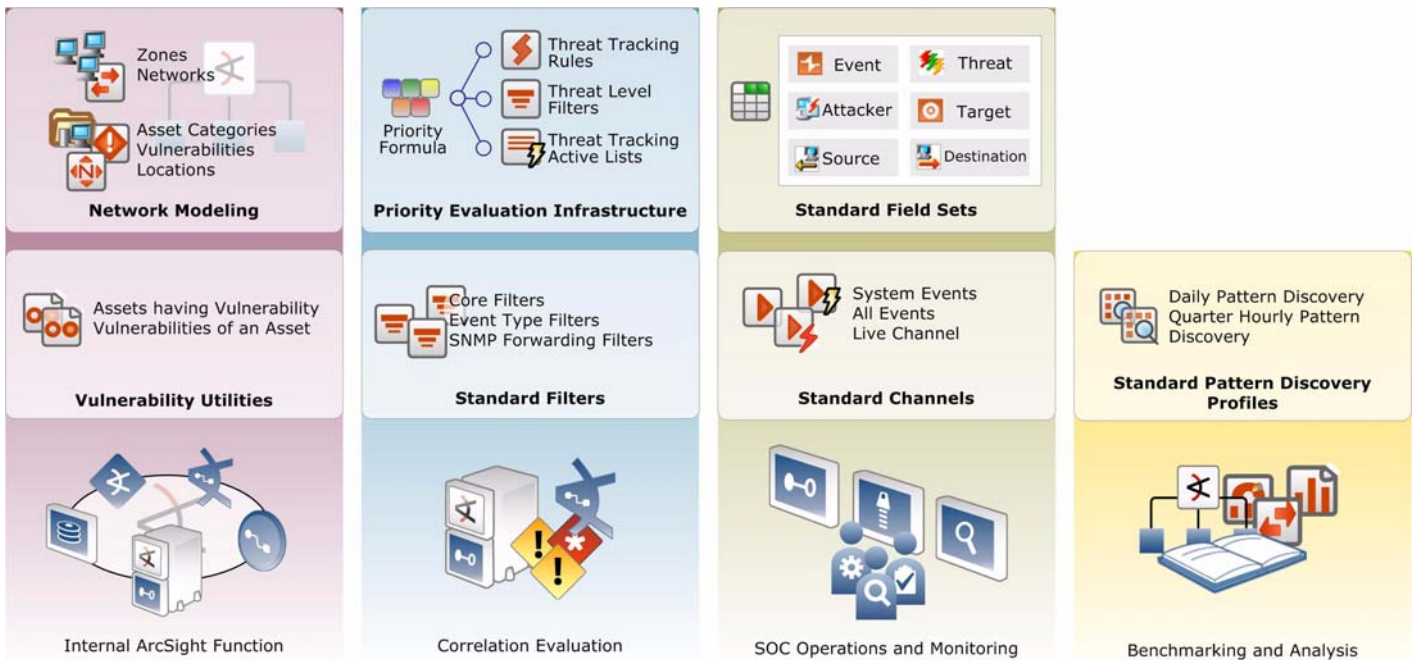


Figure 3-1 The standard features included in the core content support basic ESM function.

Internal ArcSight Function

The system content contains sets of resources that manage ESM's network modeling, vulnerability handling, and other internal ArcSight functions. These resources are leveraged by many basic systems and correlation use cases.

Network Modeling Standard Resources

The network model is a representation of the nodes on your network and certain characteristics of the network itself. For critical assets on the protected network, network modeling captures important facts that helps the system identify and classify the sources and destinations involved in your network traffic.

The ArcSight resources that make up the network model are assets, asset ranges, zones, and networks; assets, asset ranges, and zones are found in the Assets menu in the Console Navigator panel. For instructions about how to configure these for your environment, see [“Network Modeling” on page 29](#).

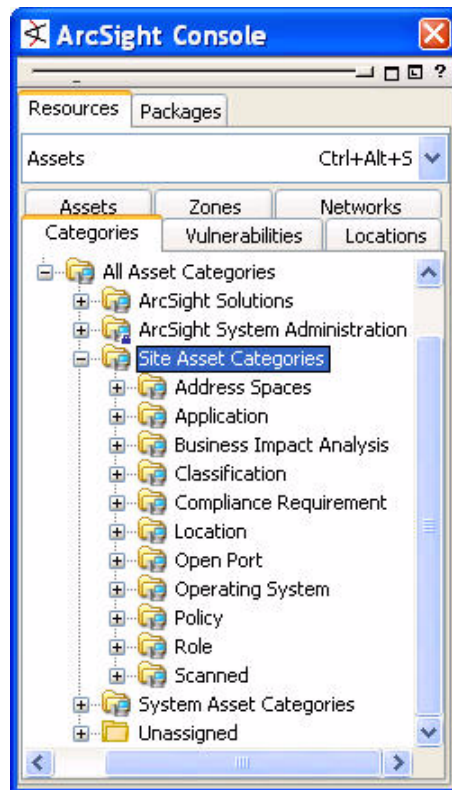
Asset Categories

Asset categories are an extensible classification system stored as ArcSight resources. These classifications describe properties of an asset, such as the operating system running on it, key applications it hosts, its role in the enterprise, and any other properties you want to consider when evaluating threats or behaviors associated with the asset.

ArcSight 4.0 comes with a library of asset categories used by the standard content.

Site Asset Categories

The Site asset categories provide a host of business-relevant categories, many of which are leveraged by the foundation packages.



The *Application*, *Open Port*, *Operating System* and *Scanned* asset categories are used by the scanner SmartConnector to automatically categorize assets. For example, Nessus can often identify the applications and operating systems a system runs, the vulnerabilities the system exposes, and keeps track of all the ports that were open on that system at the time of the last scan.

The foundations, such as the Intrusion Monitoring foundation, rely on the *Business Impact Analysis* categories, which includes the *Role* categories, the *Classification* category, and the *Compliance Requirements* categories.

ArcSight recommends that you add your own custom categories in the Site Asset Categories group. This group is specifically intended for you to extend with your own asset category system.



Although the Site Asset Categories group is not locked, you should retain the asset categories that are installed with ESM, since the foundations rely on many of them.

The Site Asset Categories are described below.

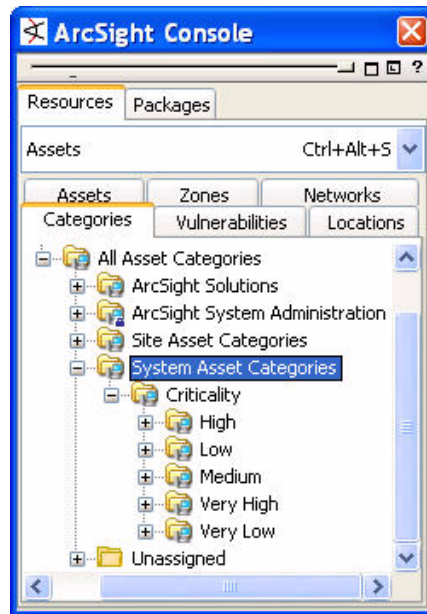
Asset Category	Description
Address Spaces	These categories include the Protected category, as well as some default categories used by zones (Dark for the Dark Address Space Zones, Protected for the Private Address Space Zones, etc.), and some potentially useful categories that can be attached to zones, like VPN and Wireless.
Application	These categories are maintained by scanner connectors.
Business Impact Analysis	This includes the Role categories and the Classification categories. This is used by the Intrusion Monitoring resources.
Location	Should be manually added to zones. For more about locations, see “Locations” on page 53 .
Open Ports	These categories are maintained by scanner connectors.
Operating System	These categories are maintained by scanner connectors.
Policy	This category should probably be manually added to systems that are significant relative to a company's computer use policy. Known malicious servers, porn, IRC servers, etc., could have assets created and have the disallowed servers category attached to them. Resources could then be written to notify or track connections to these servers.
Role	Common business and data roles, used by Business Impact Analysis.
Scanned	Maintained by scanner connectors. Each asset, when scanned, can be marked as scanned for open ports, scanned for vulnerabilities, or both. Note that the actual list of vulnerabilities found by a scanner are not listed under Asset Categories, but under Vulnerabilities. The Scanned asset category is used to determine whether, and what type of, a scan has (ever) been done.

System Asset Categories

The System asset categories contain the Criticality asset categories, which are leveraged by the Priority Formula. The priority formula is discussed in more detail in [“Priority Evaluation Infrastructure” on page 54](#).



The Criticality asset categories are locked, and cannot be moved, renamed, or modified.



The *Criticality* asset categories tell ESM which events involve the highest priority assets in your network. Prioritizing assets using this rating system is central to how much of the standard content sorts events. To make the most out of ArcSight's standard content, you should classify your assets in these asset categories at set-up time, especially those that qualify as *High* and *Very High* Criticality. Events whose asset criticality is not set are registered by the system as *Criticality Unknown*. For more about how to configure your assets with these asset categories, see [“Asset Categories” on page 30](#).

Vulnerabilities

A vulnerability is any hardware, firmware, or software state that leaves an asset open for potential exploitation. The *All Vulnerabilities* group provides a list of known vulnerabilities published by popular authorities.

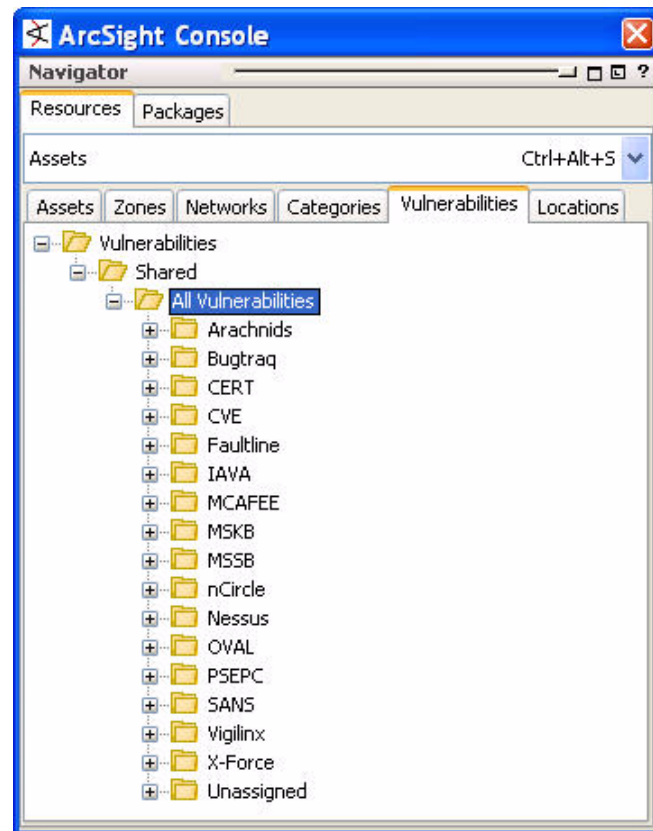
These vulnerabilities are updated by the scanner SmartConnectors every time a scan is run. Not every vulnerability possible will be listed, only those found on the network by the scanner or those used explicitly by some part of the system content (such as the SANS Top 20 rules).

Not every vulnerability scanner will report all the possible names of a vulnerability. Most of the vulnerability publishers use their own vulnerability names, CVE name, and possibly CERT name. For example, if you use Nessus, the whole host of nCircle vulnerabilities will not also appear, unless you also have nCircle. Scanners are updated just like IDS and anti-virus engines, so if your scanner is not updated with the latest vulnerability profiles, the vulnerability list also will not be updated.

Vulnerability scans don't directly use the Vulnerabilities, but the scanner SmartConnectors do attach the vulnerabilities to the appropriate assets, much like they attach *Open Ports* categories to assets.

If assets have vulnerabilities associated with them, the standard resources that reference these vulnerabilities make it possible to monitor and track systems that expose certain vulnerabilities over time, and track the number of assets with vulnerabilities. With these vulnerability identifiers, you can also create your own vulnerability tracking content.

For more about how ESM uses vulnerabilities, see ArcSight 101.



Locations

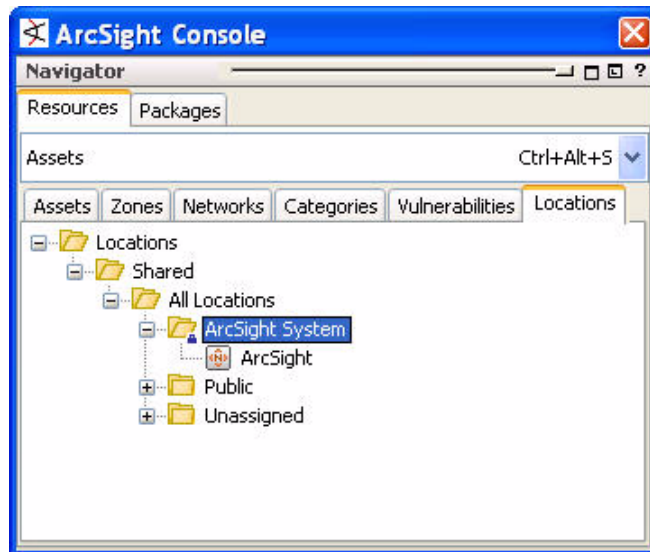
ArcSight provides a default location database that maps the IP addresses of event endpoints to its owning body for the block of IP addresses to which it belongs. This default location database is used by the Manager to find a latitude/longitude record (which also includes city, state, and country information) for each IP address in each endpoint reported by each event. This location data is used to populate the geographic map event graph available in the Viewer panel.

In some cases, the location mapping is inaccurate, or the IP address has no mapping at all, such as for private networks.

The location resource enables you to override the default location mapping provided automatically by the Manager by specifying the correct location for a known IP address whose mapping is wrong, and to specify locations for endpoints on private networks.

- If the override location is assigned to an **asset**, the location overrides the resolved longitude/latitude record from the internal database.
- If the location is assigned to a **zone**, it overrides the latitude/longitude record for all assets in that zone.
- If the location is assigned to a **network**, it overrides the latitude/longitude record for all zones in the network, and all the assets that belong on those zones.

If no override location is found, ESM uses the default location mapping, which is derived from ARIN records. The default ArcSight location is a placeholder.

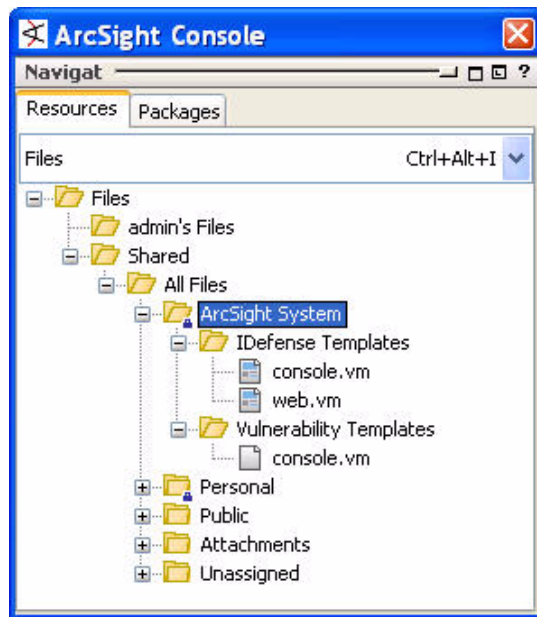


Files

The files contained in the ArcSight System group support Velocity template macros for vulnerability data and IDefense data. The `.vm` files contain the variable names that correspond with the event fields and reference pages related to qualifying events, and can be configured with the event fields you want to display for these features.

If you have IDefense set up, you can configure the event fields displayed in the event inspector for the ArcSight Console view and the ArcSight Web view. For more about IDefense setup, see the ArcSight Administrator's Guide Appendix A, *ArcSight Commands*.

The Vulnerability Template populates the reference pages and event inspector views with vulnerability mapping data. You can also configure the variables specified in these files to match the event fields you want to display for vulnerability mapping.



For more about how ESM uses velocity templates, see the topic *Velocity Templates* in ArcSight 101 and online Help.

Correlation Evaluation

System content active lists and filters help drive parts of ArcSight's correlation engine.

Priority Evaluation Infrastructure

Priority evaluation is an automatic feature of ESM that is always "on," and is applied to all the events received by the ArcSight Manager. Calculating an event's priority signals to security operations personnel which events warrant further notice and in what order.

An event's priority is calculated by the priority formula, also referred to as the threat level formula. The priority formula is an algorithm made up of five criteria that each event is evaluated against to determine its relative importance, or priority, to your security operations.

The priority formula itself is managed and maintained on the Manager, and is supported by an infrastructure of network model classifications, active lists, filters, and rules that track

an event's classification based on specific conditions. These conditions are expressed in the threat tracking and priority evaluation resources included in the core content.

The diagram on the next page shows the layers of ArcSight resources that influence the priority evaluation process. The sections that follow describe the priority evaluation resources in more detail.

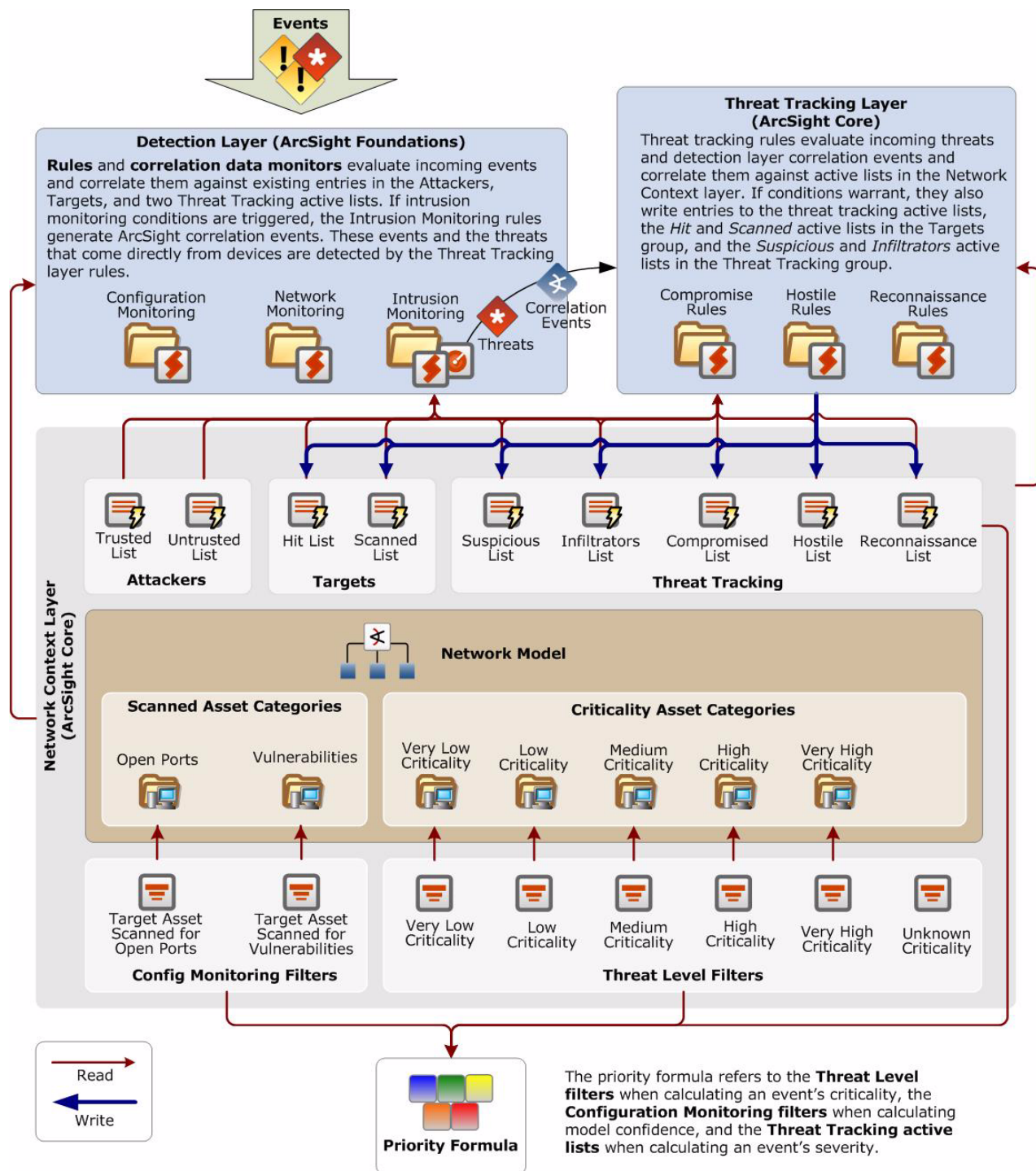
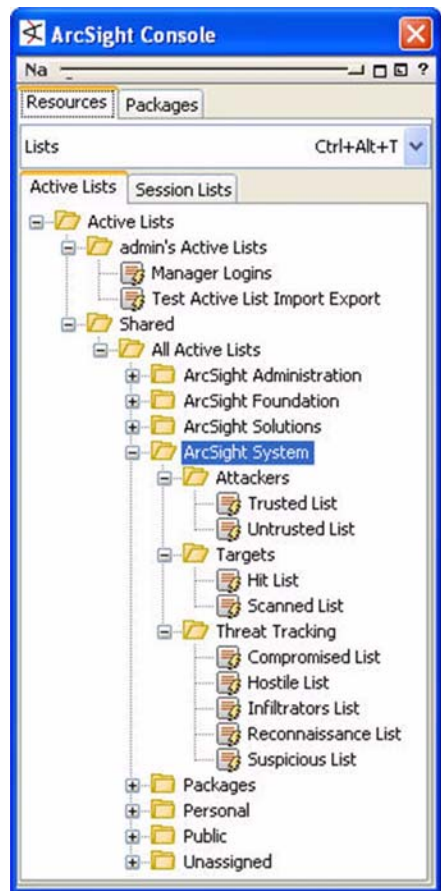


Figure 3-2 Threat tracking and evaluation is based on the priority formula and managed through a multi-tiered infrastructure that tracks events and their priority based on aggregated conditions.

Threat Escalation Active Lists

There are three groups of active lists that factor into priority evaluation:

- Attackers
- Targets
- Threat tracking



Attackers: These static active lists contain entries written to them manually during configuration to indicate systems that should be included or excluded from consideration by ArcSight conditions expressed in rules, filters, and other resources.

Targets: These dynamic active lists contain entries written to them by the Threat Tracking rules, which look for events from systems that perform scans on protected network assets.

Threat Tracking: These dynamic active lists contain entries written to them by the Threat Tracking rules, which look for events from systems that exhibit compromised characteristics, either directly, or via correlation events generated by the Intrusion Monitoring foundation suite.

Attackers Active Lists

The static active lists in the Attackers group, *Trusted* and *Untrusted*, act as a way to include or exclude the systems listed there in a condition statement, whether the condition is in a rule, filter, active list, report query, or other resource. These active lists should be configured during system setup. For instructions about how to configure active lists, see [“Configure Active Lists”](#) on page 41.

Active List	Description
Trusted List	-This is a list of systems (include the IP Address and Zone) that are trusted to perform activity, such as network mapping, vulnerability scans, port scans, etc., that would be considered suspicious or hostile from any other source. This can include permanent internal scanner devices or IP addresses of security consultants who are under contract to scan your network.

Active List	Description
Untrusted List	-This is a list of systems that are known to be hostile or compromised. An ArcSight user could insert an external system that has successfully attacked internal assets, external systems that are known to be hostile based on a third-party blacklists, or internal systems that are known to be compromised (by an attacker, a worm, or some insider threat), and have not yet been recovered and cleaned up.

Target Active Lists

The dynamic active lists in the Targets group, *Hit List* and *Scanned List*, act as a way to include or exclude the systems listed there in a condition statement, whether the condition is in a rule, filter, active list, report query, or other resource. These dynamic active lists are populated during run-time by rules triggered by qualifying events.

Active List	Description
Hit List	-This list holds target asset data for assets that have been attacked, whether successfully or not. An asset's presence in this list does not mean that it has been compromised, but that a compromise attempt has been made.
Scanned List	-This list holds target asset data for assets that have been scanned. Usually, the scanning system will be listed in the Reconnaissance List under Threat Tracking.

Threat Tracking Active Lists

The threat tracking active lists correspond directly with the threat tracking rules *Compromise*, *Hostile*, and *Reconnaissance*. The threat tracking active list group also contains two active lists whose entries are read by rules in the intrusion monitoring foundation.

The threat tracking active lists are described below. These active lists are dynamically populated by rules, so no configuration is required, although you can manually configure the active lists with systems you know are compromised. For example, you might want to populate one or more of these lists manually during system testing. For instructions, see [“Configure Dynamic Active Lists” on page 42](#).

Active List	Description
Compromised List	-This list contains assets that have been successfully compromised.
Hostile List	-This list contains attacker information on systems that have attempted to or successfully attack an asset.
Infiltrators List	-This list contains attacker information on systems that have successfully attacked an asset.
Reconnaissance List	-This list contains attacker information on systems that have exhibited reconnaissance activity against one or more assets on the network.
Suspicious List	-This list contains attacker information on systems exhibiting suspicious behavior, such as attempting to open connections to other systems that shouldn't exist (systems with addresses in Dark Address Space), or systems that have been performing brute force logon attacks.

System Filters

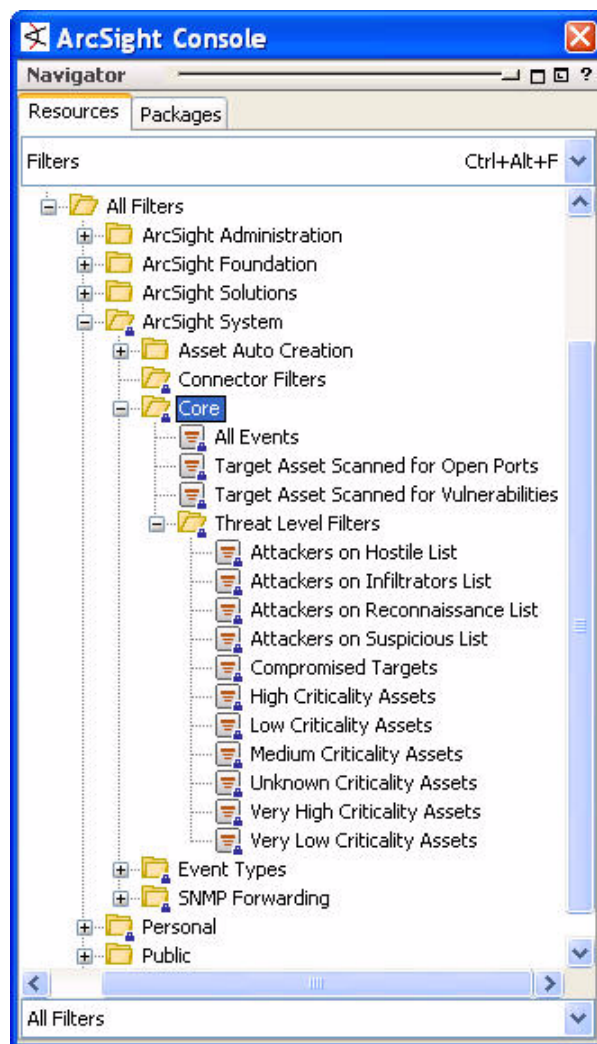
The filters contained in the ArcSight System filters group support various essential ArcSight functions.

Core Filters

The Core filters group contains a series of filters used by essential out-of-the-box features, such as the ArcSight System, All Events, and Core active channels, and features of the priority formula.



All the filters in the Core filters group are locked, which means they cannot be modified, moved, or deleted.



The core filters are described in more detail below:

Filter	Description
All Events	Filter that matches all events.
Target Asset Scanned for Open Ports	This filter selects events where the Target Asset ID is categorized as scanned and showing open ports. This filter is used by the prioritization formula.
Target Asset Scanned for Vulnerabilities	This filter selects events where the Target Asset ID is categorized as scanned and showing vulnerabilities. This filter is used by the prioritization formula.
Attackers on Hostile List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.
Attackers on Infiltrators List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.
Attackers on Reconnaissance List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.
Attackers on Suspicious List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.
Compromised Targets	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.

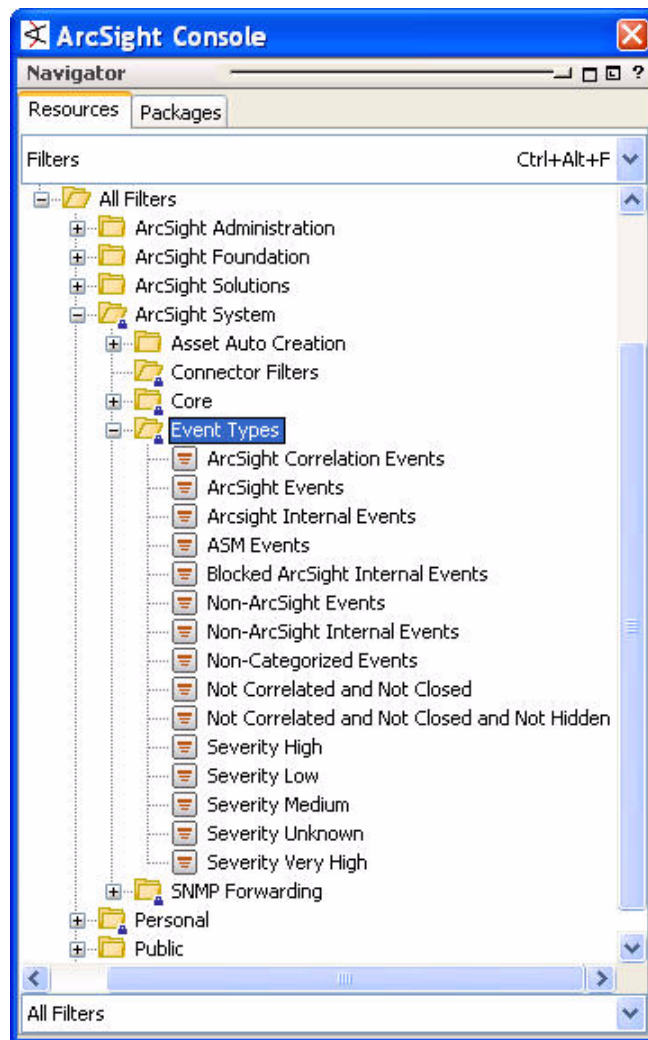
Event Type Filters

The Event Type filters include all the different types of events that ArcSight identifies. These are used by the Priority Formula, the correlation engine, ArcSight administrative function, and many of the foundation resources.

For example, the Event Privileges tab in the User Groups access control list editor uses the All Events filter to set the Event Privileges that the different user groups, such as Operators and Analyzer Administrators. The Event Types filters are used to populate this list.



The Event Types filter group is locked, which means the group and its contents cannot be moved, added to, or deleted.



SNMP Forwarding Filters

The System filters group also has a group that contains an SNMP Trap Sender filter. This filter is only needed if you have SNMP traps that forward events to a network management system, such as HP OpenView.

If you have SNMP forwarding enabled, this filter should be configured with the name of the filter whose events match the SNMP Trap Sender filter to forward events to the network management system. For instructions about how to configure this filter, see [“Configure SNMP Trap Forwarding Filter” on page 39](#).

For instructions about how to enable the SNMP trap sender on the ArcSight Manager, follow the instructions outlined in the *ArcSight Administrator's Guide* in chapter 4, *Configuration*.

SOC Operations and Monitoring

The system content provides standard field sets and active channels to provide basic operations and monitoring functions out of the box.

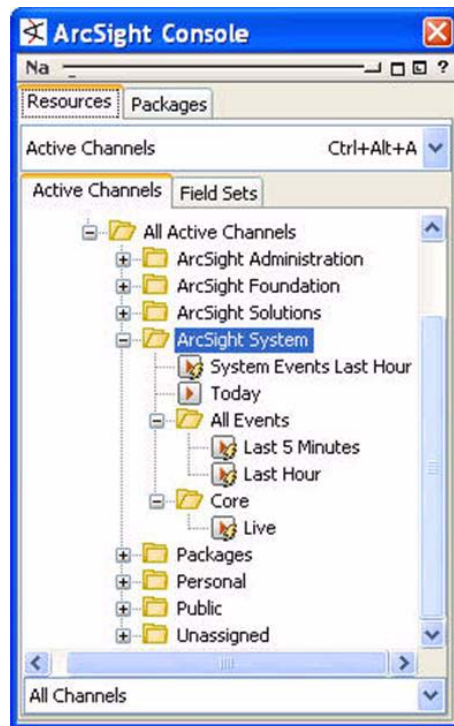
System Active Channels

The system channels are a basic set of active channels that support out-of-the-box monitoring functionality.

At installation, these active channels verify feeds coming in from network devices through ArcSight SmartConnectors, and verify that the SmartConnector settings are correct.

During SOC operations and monitoring, these views can be a first place to start to observe the flow of events from the monitored devices on the network.

During incident investigation, these channels can provide a contextual launching place for drill-down and investigation into an event or series of events.



ArcSight System: These active channels show all ArcSight internal events.

All Events: These active channels are the default monitoring grids that display the flow of all events through the ArcSight system.

Core: The Live channel shows events received from devices during the last two hours. It filters out internal events and those that contributed to correlation events.

ArcSight System Active Channels

Active Channel	Description
System Events Last Hour	Channel showing all events generated by ArcSight during the last hour. A filter prevents the channel from showing events that contributed to the firing of a rule, commonly referred to as correlated events.
Today	Channel showing events received today since midnight. A filter prevents the channel from showing events that contributed to the firing of a rule, commonly referred to as correlated events.

All Events Active Channels

The All Events active channels show all events: those generated by devices, and all those generated internally by ArcSight.

During installation, these channels are helpful to verify the complete throughput of events from devices as well as ArcSight internal events to verify that all feeds are being received as expected.

When an ArcSight admin creates new users, this channel can also be effective to test that the access control levels (ACLs) set for the user are showing the intended event data. Only event data that the user has permission to view should be available.

During content development, you can use this channel to test that your conditions find the intended event data and/or initiate the intended actions.

Active Channel	Description
Last 5 Minutes	Channel showing events received during the last five minutes. The channel includes a sliding window that always displays exactly the last five minutes of event data.
Last Hour	Channel showing events received during the last hour. The channel includes a sliding window that always displays exactly the hour of event data.

Core Active Channels

The Core group contains the *Live* active channel, which shows a sliding window of the last two hours' events. To maximize performance and throughput, the channel shows aggregated events and correlation events generated by triggered rules rather than all the raw events that led up to them.

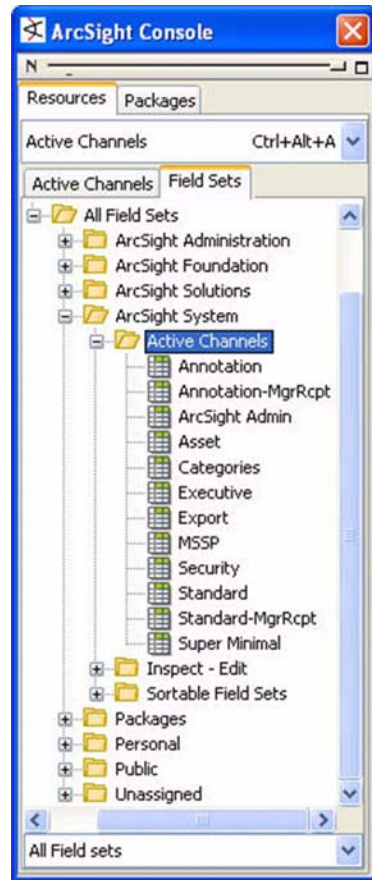
Active Channel	Description
Live	Live Channel showing events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data. A filter prevents the channel from showing events that contributed to the firing of a rule, commonly referred to as correlated events.

System Field Sets

Field sets are collections of event fields stored as ArcSight resources that narrow the number of event fields displayed in certain situations, such as active channels and the common conditions editor in the Inspect/Edit panel.

Active Channels

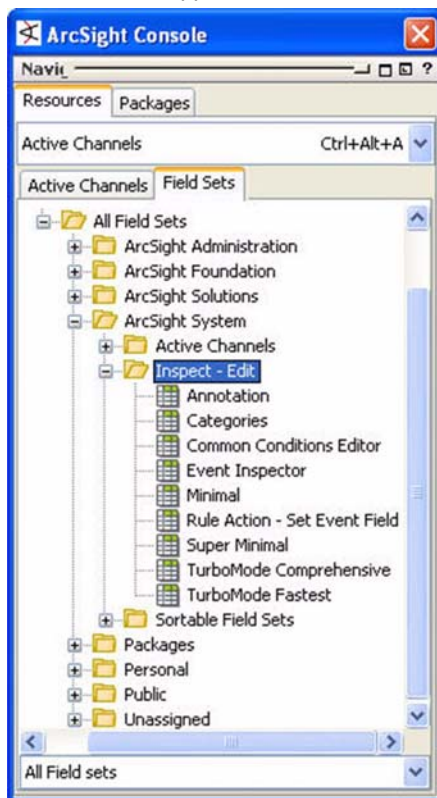
Event fields are displayed in active channels as column headers, for example *AssetID*, *Event Name*, and *Target User Name*. The standard field sets designed for active channels narrow the number of event fields displayed to those that are most pertinent to certain types of monitoring.



Active Channels: These field sets provide a set of event fields limited to those that are most relevant to certain types of monitoring.

Inspect - Edit Field Sets

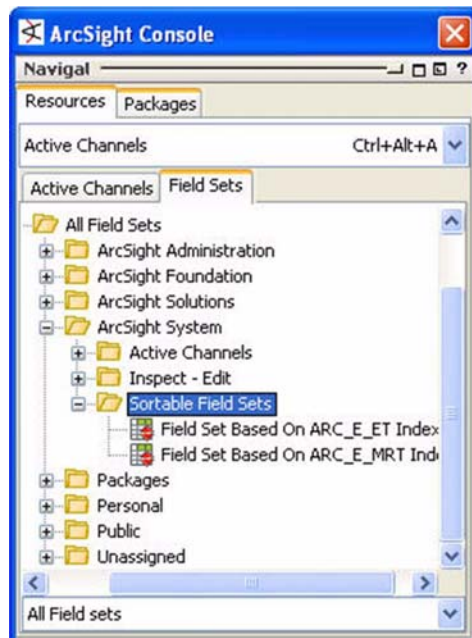
Event fields are also presented in groups in the Common Conditions Editor in the Inspect/ Edit panel. The field sets designed for this use narrow the number of fields displayed to those that are applicable to certain kinds of correlation.



Inspect - Edit: These field sets provide a collection of event fields limited to those that are most relevant to certain types of correlation activities.

Sortable Field Sets

Indexed sortable field sets are used in both active channels and the Common Conditions Editor.



Sortable Field Sets: These field sets are limited to those event field that are indexed, which enable an active channel column to be sorted by the entries in that column.

Benchmarking and Analysis

ArcSight provides several benchmarking and analysis tools as add-on modules. As part of the system content, ArcSight includes two Pattern Discovery profiles. These profiles will be active only if you have the Pattern Discovery module installed.

Pattern Discovery Profiles

Pattern Discovery is ArcSight's separately licensed data mining module. Pattern Discovery automatically identifies patterns that occur in an event flow that you didn't know to look for. Pattern Discovery can be used for benchmarking, that is, identifying patterns of normal activity that you can then filter out, and it can be used as a regular diligence check on historical data flows to ensure you're not missing anything in your daily operations.

To support these functions, the system content provides the following two Pattern Discovery profiles:

- Daily Pattern Discovery
- Quarter Hourly Pattern Discovery

The Daily Pattern Discovery profile can be used as a daily check for any patterns of activity that may have been overlooked during real-time operations.

The Quarter Hourly Pattern Discovery can be used as an investigation tool.

Both profiles can be used for benchmarking to find normal activity patterns that can be filtered out when building your own correlation content.

For more about Pattern Discovery, see the *ArcSight Pattern Discovery Guide* or call Customer Support (see ["ArcSight Customer Support" on page 5](#)).

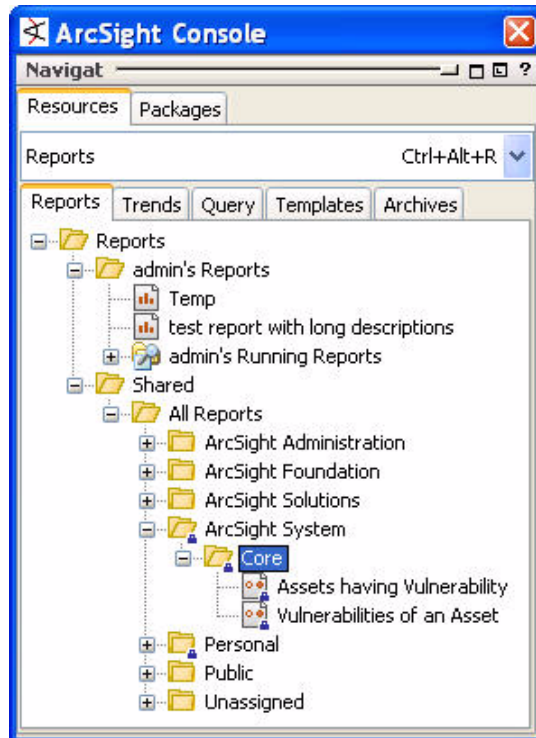
Core Reports

The Core reports group contains two special reports that are used internally by the ArcSight vulnerability update structure.



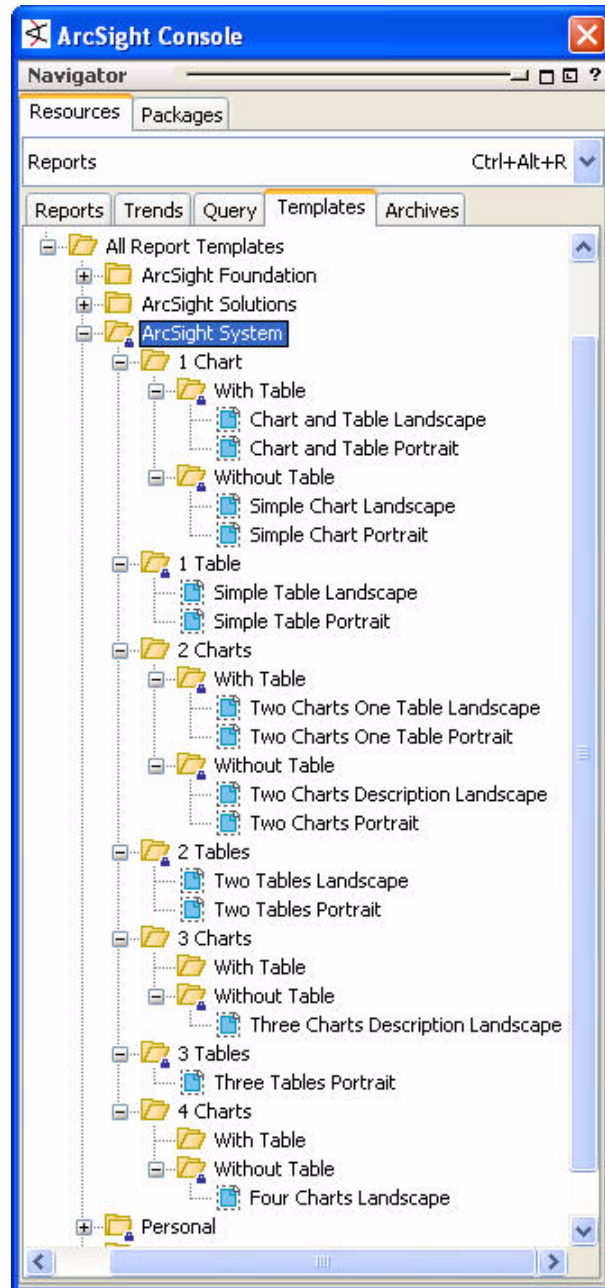
These reports cannot be scheduled, and are not intended to be run as stand-alone reports.

The Assets Having Vulnerability report lists all the assets that expose a particular vulnerability. The Vulnerabilities of an Asset report lists all the vulnerabilities exposed by a particular asset.



Standard Report Templates

ESM 4.0 is installed with a series of standard report templates, which define the layout of the reports contained in the System and Foundation content. These templates are also available for you to use for reports you create.



The report templates' parent groups are locked, which means you cannot move, rename, or delete the report templates. You can perform some minimal customizations, however, as directed in the following sections.

Customize Branding in Standard Templates

By default, the standard ArcSight report templates are branded with the ArcSight logo. You can customize this branding with your own corporate logo.

To change the company logo branding:

- 1 Right-click the standard report template you wish to customize and select **Edit Template**.
- 2 In the Report Template editor in the Inspect/Edit panel, click **Open in Designer**.
- 3 In the Report Designer, select, then right-click the ArcSight logo and select **Properties**.
- 4 In the Image Properties dialog, select the Image tab and click **Browse**.
- 5 Browse to the image file you wish to use and click **Open**, then **OK**.
- 6 Save and close the report template (**File > Save**, or **Ctrl + S**).

Making Custom Modifications to Standard Templates

It is possible to make other custom modifications to a standard template. Before you do however, be aware of the following:



- If you remove an element (such as a chart, table, text box for title) in the report template, all the reports using this template will also lose their link to that element. The report will not be broken, but the link between the query and the deleted chart, table, or text box, will be broken.
- If you add an element (such as a chart or table) to the report template, all the reports using this template will need to be modified or updated to make use of the new element. If they are not updated, the element will appear empty. If you add a new text box to the template, the default text is set in the report template, so any reports linked to the template will automatically display the new text box and the default text.
- Renaming an element in a report template will also break the links between the queries and the elements they are linked to (charts and tables).

The things you can safely change without breaking any report elements include:

- Move, resize elements (such as the size of the chart)
- Change the default parameters of an element (such as default text in a text box, colors for the charts, default font sizes for tables, and so on)

Follow these tips when modifying a standard template.

- Make a copy of the template you want to customize and make modifications to the copy.
- Use a resource graph to view what reports the template supports.
- After making modifications to the copy, go to the reports the template supports and point the report to the new modified template.

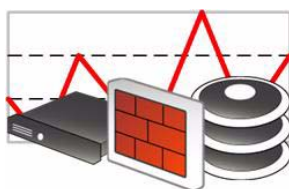


Note that any changes made directly to a standard template will likely be overridden during future upgrades.

What's Next

The next chapter, Configuration Monitoring, describes the Configuration Monitoring foundation.

Configuration Monitoring Foundation



The Configuration Monitoring foundation identifies, analyzes, and remediates undesired modifications to systems, devices, and applications. This foundation helps IT and security staff to pinpoint and resolve problems quickly, and provides essential visibility into the network configuration so you understand the systems you have, where they are, what they host, and what vulnerabilities they expose.

Once you have this basic view, the Configuration Monitoring foundation helps you monitor how your networks change over time, measure daily statistics, understand the changes made, and know who's making them. Trends help you know what is normal and spot anomalies that should be investigated.

Because the configuration of network assets is mostly of interest to network and security analysts and IT personnel, most of the content is geared toward the operational and detailed views. The foundation also contains a basic set of executive-level summary reports that give managers and executives the information they need to understand the health of the monitored network.

- ["Configuration Monitoring Foundation Overview" on page 72](#)
- ["Configuration Summary" on page 74](#)
- ["Configuration Monitoring Filters" on page 75](#)
- ["Configuration Monitoring Active Channels" on page 86](#)
- ["Configuration Monitoring Active Lists" on page 88](#)
- ["Configuration Monitoring Dashboards and Data Monitors" on page 89](#)
- ["Configuration Monitoring Rules" on page 119](#)
- ["Configuration Monitoring Reports" on page 93](#)

Configuration Monitoring Foundation Overview

Configuration monitoring is concerned mainly with monitoring hosts and user accounts for configuration-related activity, such as installing new applications, adding new systems to the network, anti-virus/network scanner/IDS engine and signature updates, asset vulnerability postures, and so on.

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

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

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

Uptime

Monitoring system uptime is an important part of assuring that critical revenue-based systems and the infrastructure that supports them is up and available when it should be.

For ESM 4.0, the Configuration Monitoring foundation addresses system uptime by monitoring system restarts. For example, if a system has multiple restarts in a short period, it may indicate a problem.

The importance of a system restart can be determined by the asset's criticality. Systems that are considered critical to operations and the infrastructure that supports them should be categorized in the Criticality: High and Very High asset categories.

User Configuration Monitoring

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

For ESM 4.0, the Configuration Monitoring foundation addresses user Configuration Monitoring by identifying and monitoring user accounts and the hosts/addresses associated with them. This ties a user to certain IP addresses, MAC addresses, host-names, zones, and so on. The reports cover user account additions, modifications to those accounts, and account removal.

Network Configuration Monitoring

Configuration Monitoring focuses on the changes to the network hosts and infrastructure. For example, hosts and network devices appearing randomly on a network could be an indication that there is a network connection or access point that could expose the network to threats that should have been mitigated by network perimeter defense devices. Likewise, random changes to network infrastructure, such as routers and firewalls, could indicate misconfigurations or malicious actions from within the network, which could expose the network to more threats.

Network Configuration Monitoring content is concerned with providing visibility into the configuration and configuration changes to the network.

Device Reporting

The Configuration Monitoring foundation contains resources that monitor the network devices reporting into ArcSight and provides reports that summarize that activity.

Some of the device monitoring content is a simple summary of the events being generated by device. Others summarize activity from blocks of similar devices in particular zones of the network.

Host Networking

Network change monitoring for hosts is concerned with ports opened to the network. This is a combination of detecting when services are run, and if the firewall configuration is changed to accommodate these services. This content also detects and reports when a firewall is enabled or disabled.

Security Applications (Anti-Virus)

Anti-virus Configuration Monitoring is concerned with verifying how effectively the anti-virus solutions on your network are deployed and functioning. The content is concerned with questions such as what hosts have anti-virus coverage and what percentage of hosts in each Zone have coverage, and whether the AV configurations (DAT files) up to date.

Supported Devices

The Configuration Monitoring content works on feeds from many network devices and hosts. Devices that report user account changes and authorization checks (usually operating systems, via syslog or Windows logs), and device configuration changes (router logs, firewall logs, etc.) and application logs of various types provide useful Configuration Monitoring events.

- Operating systems
- Security applications
 - ◆ Network and host-based IDS
 - ◆ Anti-virus
- User management services
 - ◆ Authentication, authorization, and accounting services
- Basic network devices
 - ◆ Firewalls
 - ◆ Routers
 - ◆ Switches
 - ◆ VPN

Configuration Summary

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

Required Configuration

The Configuration Monitoring foundation contains the following resource that requires configuration to be functional:

Active List	Configuration required
Local User Allowed Systems	Configure with the IP address, zone, and customer (if applicable) of systems that allow local users to be created. These would likely be systems operated by IT or network development groups.

This is a static active list whose entries are looked up by the rules *Local Windows User Creation - Disallowed Host* and *Local Windows User Creation - Allowed Host*. If this active list is not configured, or is not relevant to your operating environment, the rules will not yield results from the look-up. This does not affect overall foundation functionality.

- 1 In the Navigator panel, go to [Active Lists/All Active Lists/ArcSight Foundation/Configuration Monitoring/](#).
- 2 Right-click the active list you wish to populate and select **Show Entries**. The active list details are displayed in the Viewer panel.
- 3 To add an entry to the list, click the add icon (+) in the active list header.
- 4 In the Active List Entry Editor in the Inspect/Edit panel, enter the following values and click **Add**.

Name	Value
Target Address	Enter the IP address of the system that allows local users.
Target Zone	Enter the name of the ArcSight zone the system is located in from the drop-down tree selector.
Customer	If applicable, enter the name of the customer the system belongs to from the drop-down tree selector.
Creation Time	Timestamp of when this entry was created. This value is supplied by the system and cannot be edited.
Last Modified	This field is reserved for active lists that are populated dynamically by rule actions. This value is supplied by the system and cannot be edited.
Count	This field is reserved for active lists that are populated dynamically by rule actions. This value is supplied by the system and cannot be edited.

- 5 Repeat steps 3 and 4 for every system that allows local users to be created.

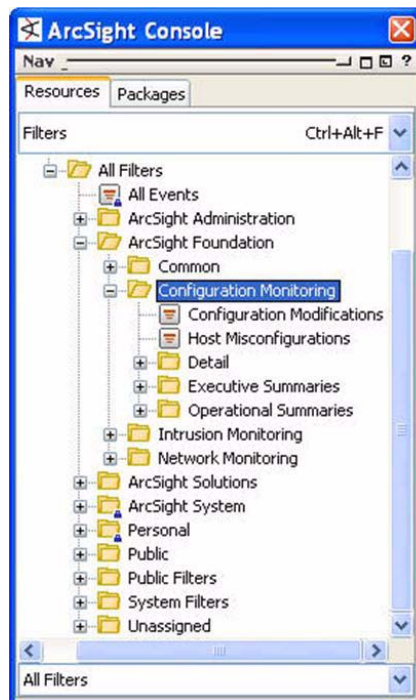
Verify Asset Model

The Configuration Monitoring foundation works best if your asset model is populated: you have assets, they are located in zones, and they have been scanned, so ESM knows what ports are open, what vulnerabilities are exposed, and what applications are running.

It is also important to have the criticality asset categories assigned to your high and very high criticality assets. An asset's criticality is used to evaluate trends and vulnerability exposure, and focuses on systems categorized as high and very high criticality.

Configuration Monitoring Filters

The Configuration Monitoring filters express conditions that are used by the other Configuration Monitoring and reporting resources.

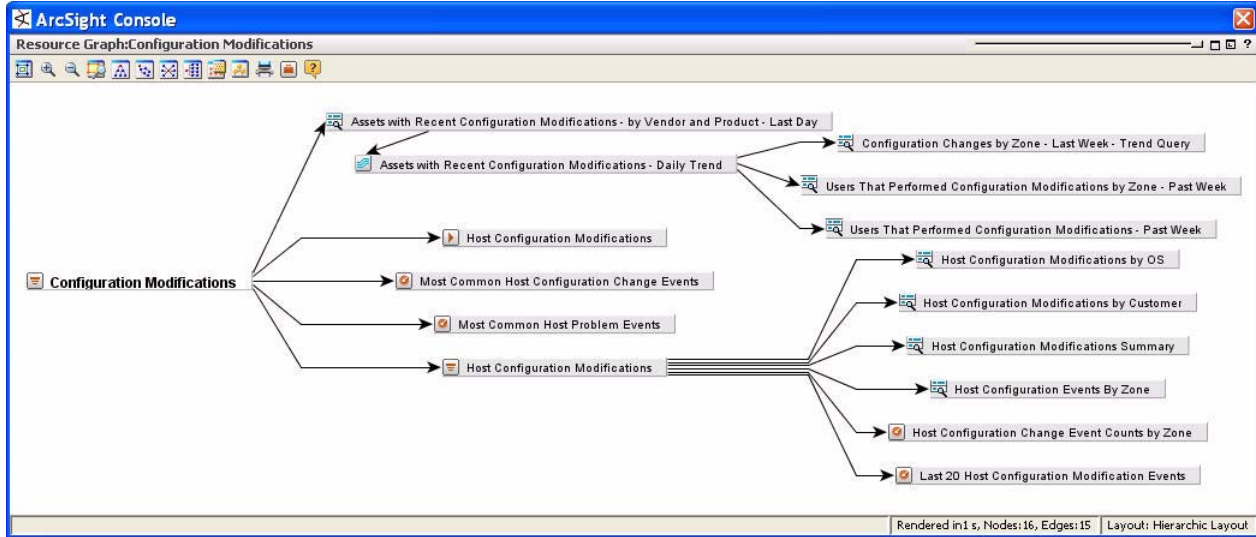


Configuration Monitoring:
These filters identify all configuration modification behaviors, and are leveraged as base filters for many configuration monitoring resources.

These filters are described in more detail below:

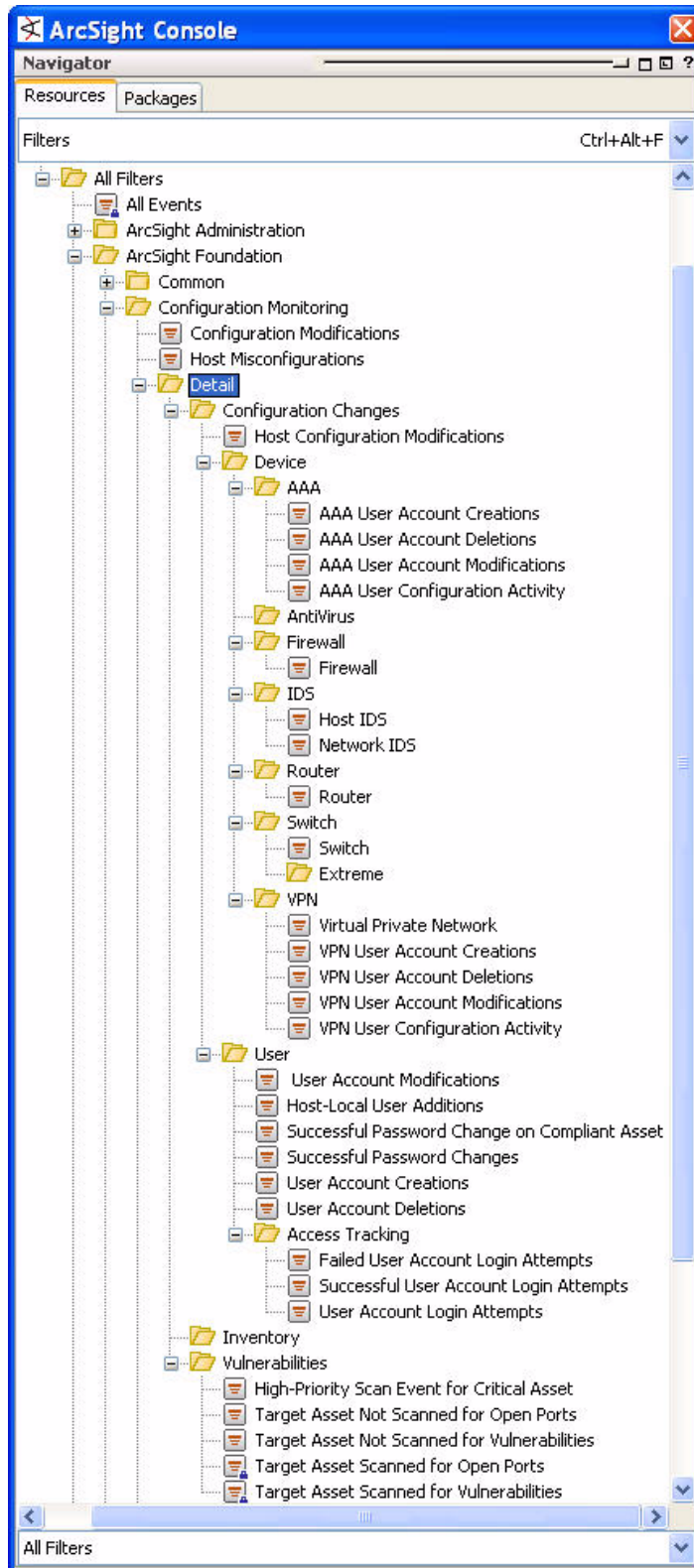
Filter	Description
Configuration Modifications	This is a base filter used to identify configuration modifications on any system or device. This resource is a part of the Configuration Monitoring content.
Host Misconfigurations	This filter is used to detect events indicating misconfigurations on hosts. This filter is a part of the Configuration Monitoring content.

The Configuration Modifications filter supplies conditions for the following Configuration Monitoring resources:



Detail Filters

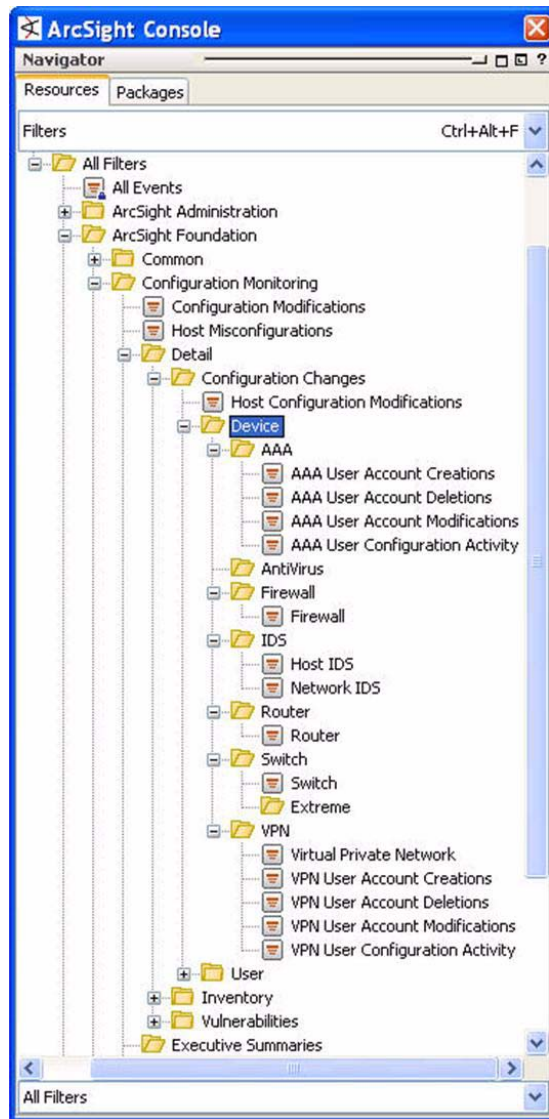
The detail filters provide conditions for many Configuration Monitoring detail-level resources that focus on data for detailed analysis.



The two main filter groups within Detail are *Configuration Changes* and *Vulnerabilities*. The *Configuration Changes* filters focus on events related to specific network devices, such as firewalls, routers, switches, VPNs, IDSs, and hosts, and user management and access tracking. The vulnerabilities detail filters focus on assets that are not covered by network vulnerability/mapping scanners and related scanner events for critical assets.

Configuration Changes by Device

The Configuration Changes by Device filters supply conditions for resources that track configuration changes by device.

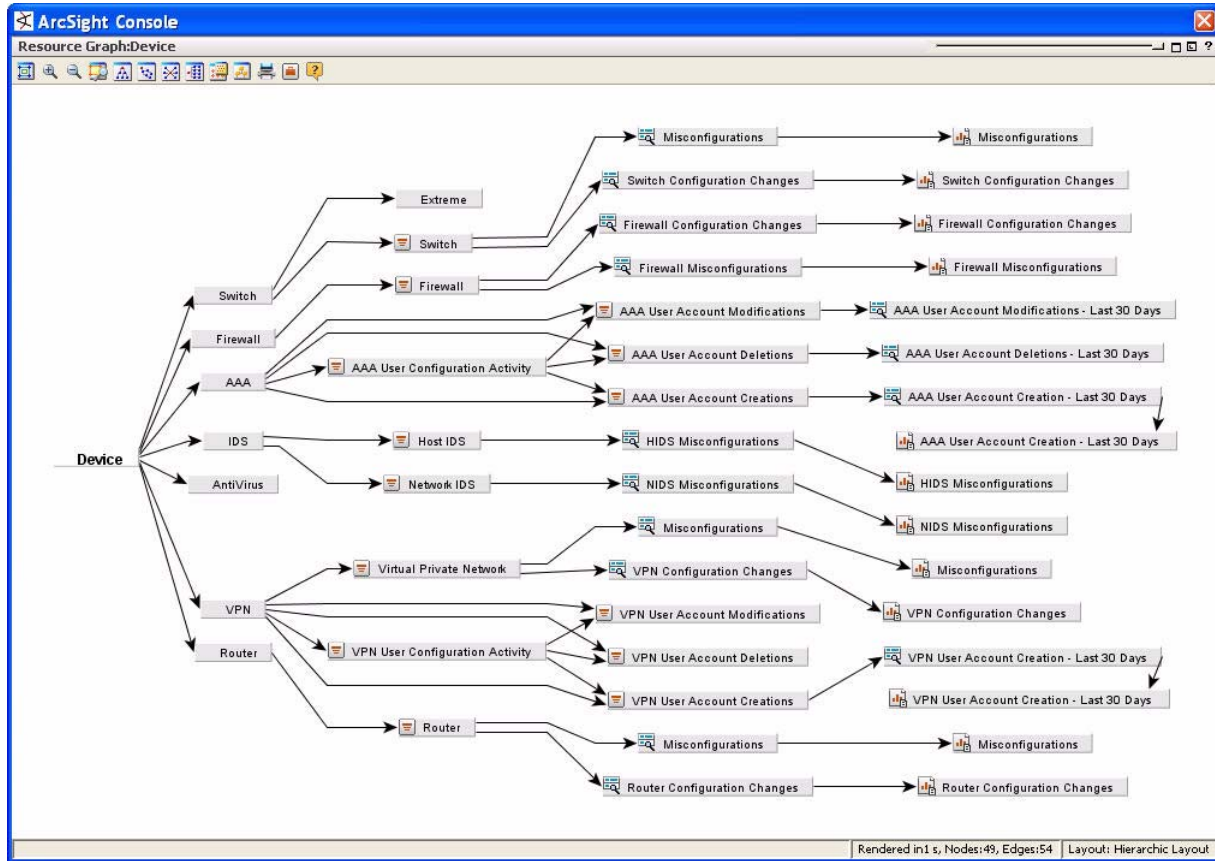


Device: These filters find events that involve the indicated devices and transactions.

The Configuration Changes by Device filters are discussed in more detail below.

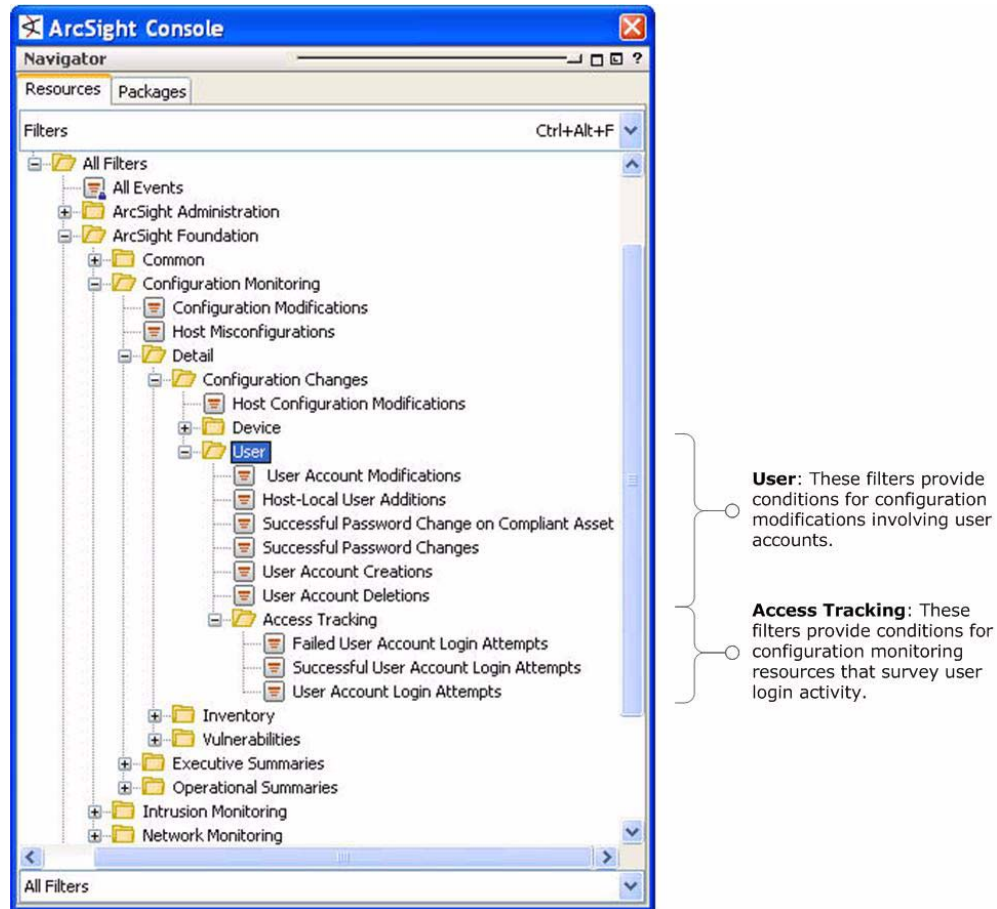
Filter	Description
AAA User Account Creations	This filter identifies user account creation activity on AAA systems. This filter is part of the Configuration Monitoring content.
AAA User Account Deletions	This filter identifies user account deletion activity on AAA systems. This filter is part of the Configuration Monitoring content.
AAA User Account Modifications	This filter identifies user account modification activity on AAA systems. This filter is part of the Configuration Monitoring content.
AAA User Configuration Activity	This filter is used to identify user configuration activity on AAA systems. This filter is a part of the Configuration Monitoring content.
VPN User Account Creations	This Filter is looking for events showing VPN user account creation information. This Filter uses the "VPN User Configuration Activity" Filter and looks for the "/Authentication/Add" category behavior.
VPN User Account Deletions	This Filter is looking for events showing VPN user account deletion information. This Filter uses the "VPN User Configuration Activity" and "User Account Deletions" Filters.
VPN User Account Modifications	This Filter is looking for events showing VPN user account modification information. This Filter uses the "VPN User Configuration Activity" and "User Account Modifications" Filters.
VPN User Configuration Activity	This filter is used to identify user configuration activity on VPN systems. This filter is a part of the Configuration Monitoring content.

The Configuration Monitoring filters by device provide conditions for the following Configuration Monitoring resources:



Configuration Changes by User

The Configuration Changes by User filters supply conditions for resources that track configuration changes to user accounts.

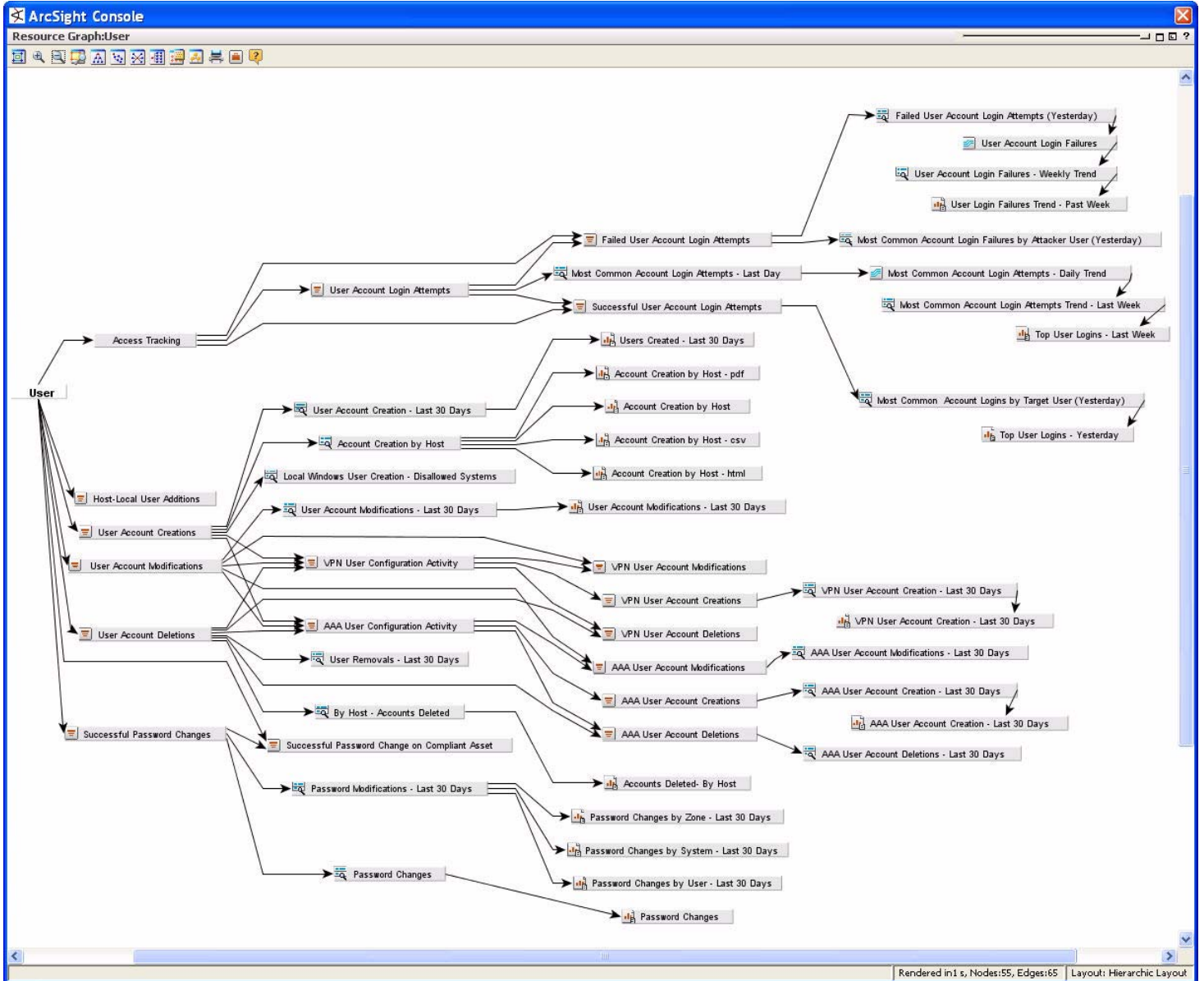


The Configuration Changes by User filters are described in more detail below.

Filter	Description
User Account Modifications	This filter identifies user account modification events. This filter is a part of the Configuration Monitoring content.
Host-Local User Additions	This Filter is looking for events showing local user account additions.
User Account Creations	This filter identifies user account addition events. This filter is a part of the Configuration Monitoring content.
User Account Deletions	This filter identifies user account deletion events. This filter is a part of the Configuration Monitoring content.
Failed User Account Login Attempts	This filter uses the ArcSight event categories to identify failed user account login attempts.
Successful User Account Login Attempts	This filter uses the ArcSight event categories to identify successful user account login attempts.

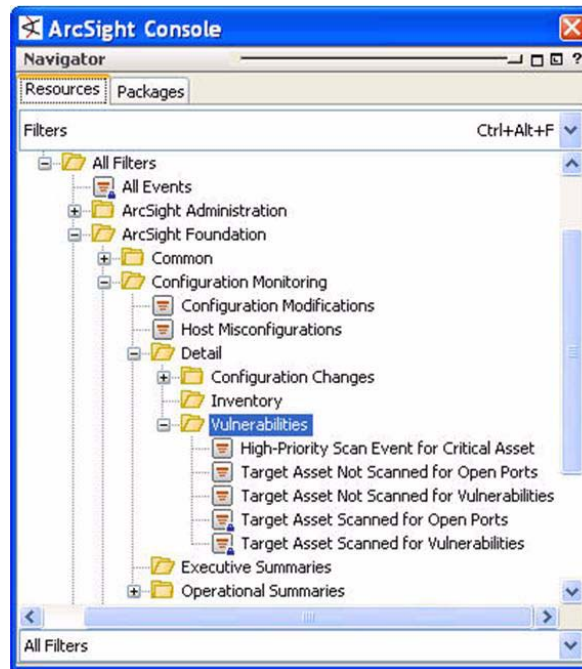
Filter	Description
User Account Login Attempts	This filter uses ArcSight categories to choose events that indicate user login attempts. These may be successful or failures.

These filters provide conditions for the following Configuration Monitoring resources:



Vulnerability Filters

The vulnerability filters provide conditions for Configuration Monitoring resources that evaluate vulnerability scan events.

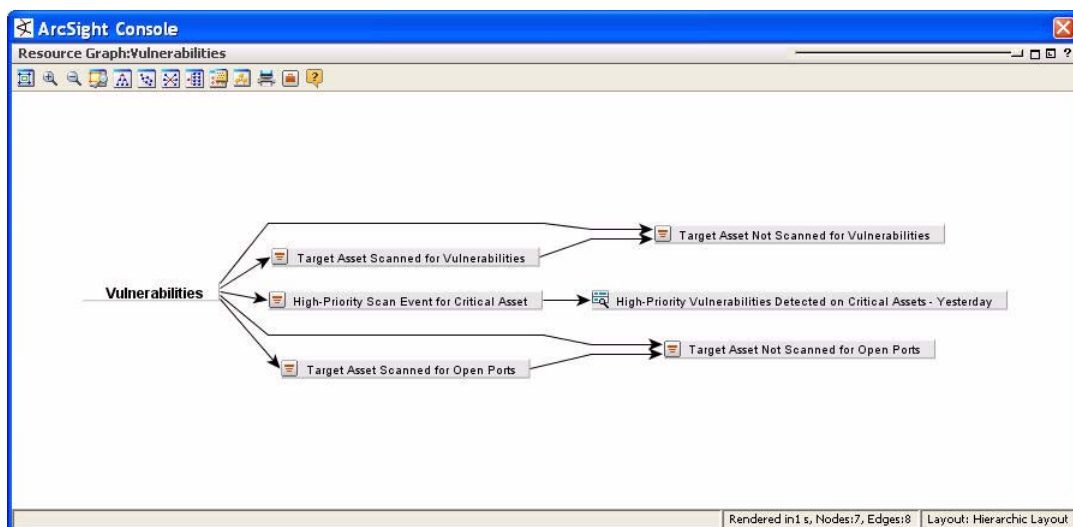


Vulnerabilities: These filters provide conditions for configuration monitoring resources that survey vulnerability scan events. The two locked filters are used for internal ESM function, and cannot not be modified or deleted.

The Vulnerability filters are described in more detail below:

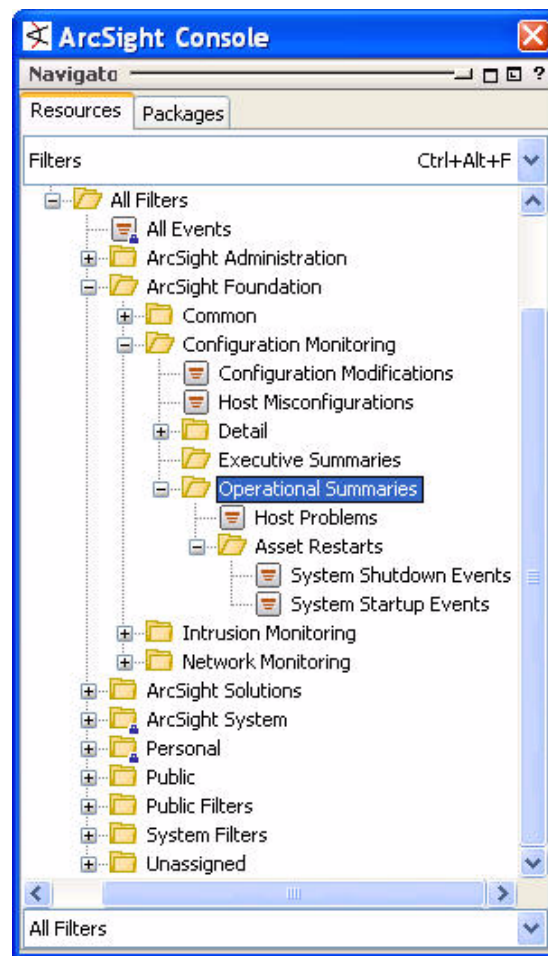
Filter	Description
High-Priority Scan Event for Critical Asset	This filter identifies vulnerability scan events that indicate that a high-priority vulnerability was detected on a system you have marked with high or very-high criticality.

The vulnerability filters provide conditions for the following Configuration Monitoring resources:



Operational Summaries Filters

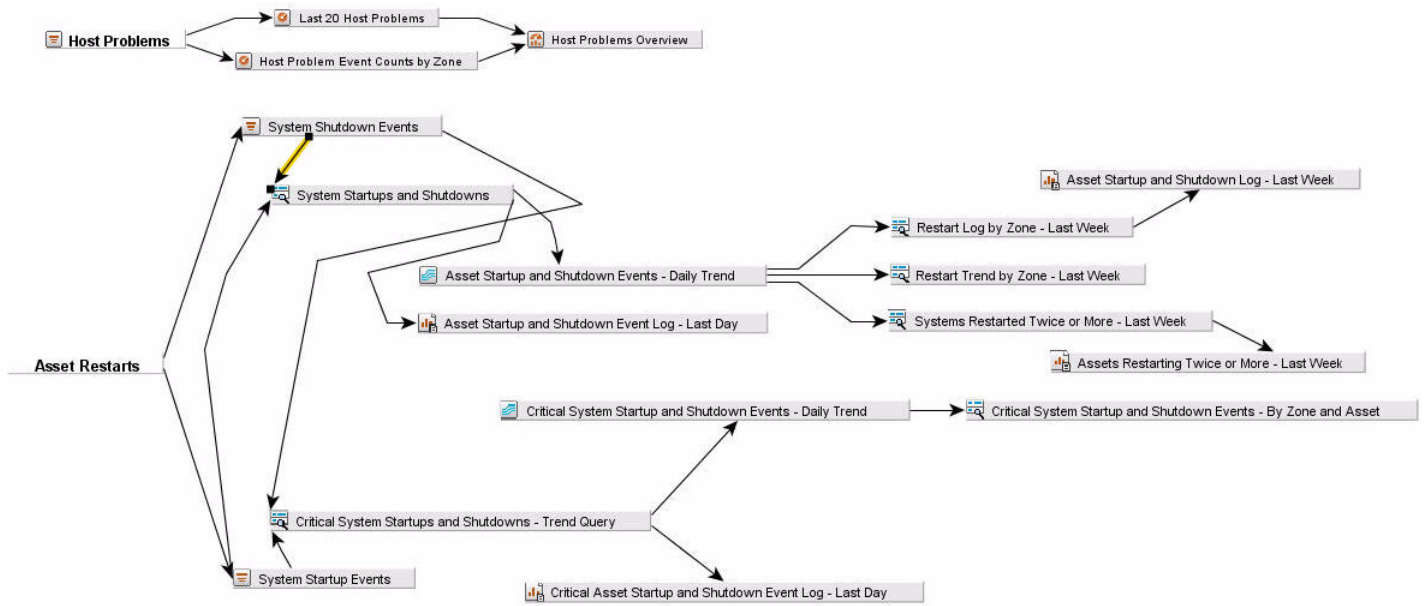
The operational summary filters focus on events related to host problems and startup/shutdown events for monitored devices and hosts.



The Operational Summary filters are described in more detail below.

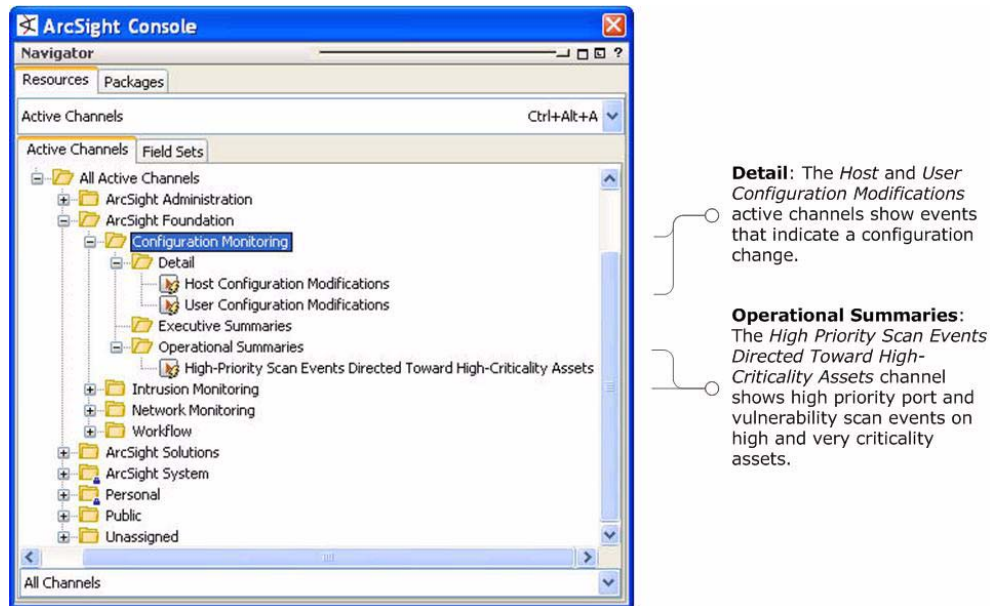
Filter	Description
Host Problems	This filter is used to identify host-related problems and errors. This filter is part of the Configuration Monitoring content.
System Shutdown Events	This filter identifies events that indicate a system has shut-down. This is often indicative of a reboot.
System Startup Events	This filter identifies events that indicate a system has started up. This is often indicative of a reboot.

The Operational Summary filters supply conditions for the following operational summary resources



Configuration Monitoring Active Channels

The Configuration Monitoring foundation contains the following active channels:

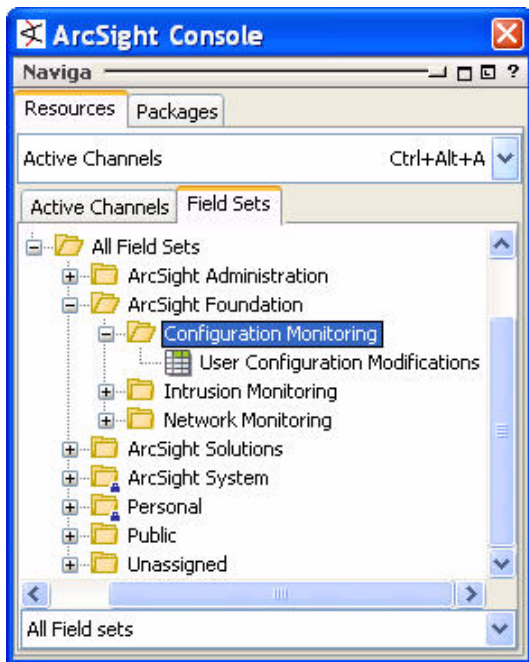


These active channels are described in more detail below:

Active Channel	Description
Host Configuration Modifications	This channel provides a view of the last day of configuration modification events related to hosts. This channel is a part of the host-specific Configuration Monitoring content.
User Configuration Modifications	This channel provides a view of the last day of configuration modification events related to users. This channel is a part of the user-specific Configuration Monitoring content.
High-Priority Scan Events Directed Toward High-Criticality Assets	This channel can be used to view scan results in real-time if you would like a view into any high-priority vulnerabilities detected on highly-critical assets.

Configuration Monitoring Field Sets

The Network Monitoring foundation comes with one field set, which focuses on fields that indicate when a configuration change has been made.

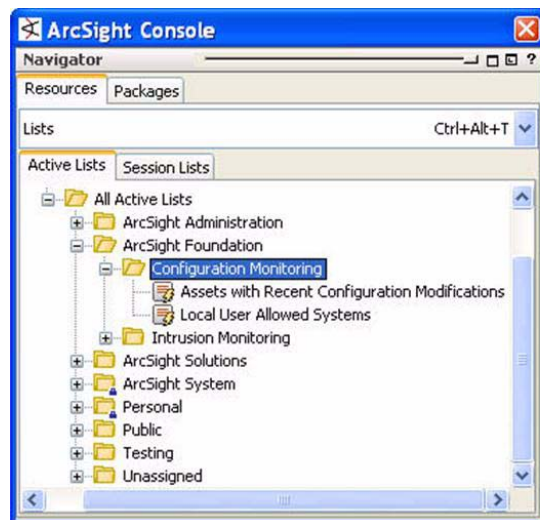


- End time
- Customer
- Target user name
- Attacker user name
- Name
- Target zone name
- Attacker zone name

This field set is used by the *User Configuration Modification* active channel.

Configuration Monitoring Active Lists

The Configuration Monitoring foundation contains two active lists, a static active list that should be configured with the systems that allow local users to be created, such as development and testing environment systems, and a dynamic active list that maintains a list of systems with modification changes.



Configuration Monitoring:
These active lists keep track of events involving systems with recent configuration modifications and that allow local user accounts.

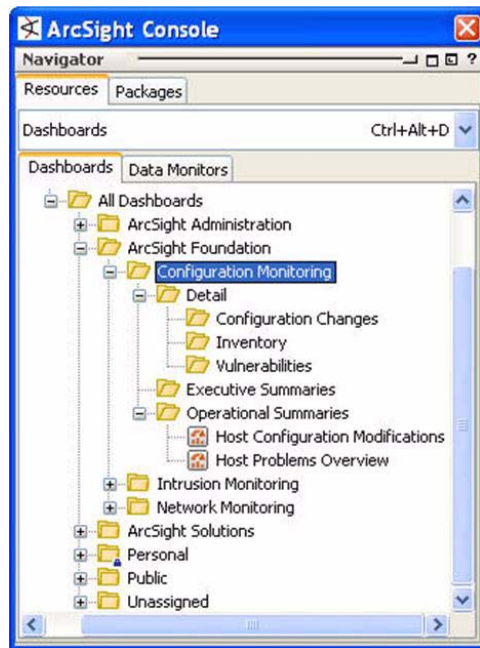
These active lists are described in more detail below.

Active List	Description
Assets with Recent Configuration Modifications	This active list is intended to track devices and hosts that have had some sort of configuration modification in the past 7 days.
Local User Allowed Systems	This active list is used to specify systems on which local user creation activity is allowed. This active list is part of the Configuration Monitoring content.

The Local User Allowed Systems active list should be configured with the network identification of the systems on which local user accounts are allowed. For configuration instructions, see [“Required Configuration” on page 74](#).

Configuration Monitoring Dashboards and Data Monitors

The Configuration Monitoring dashboards give real-time insight into host modifications.

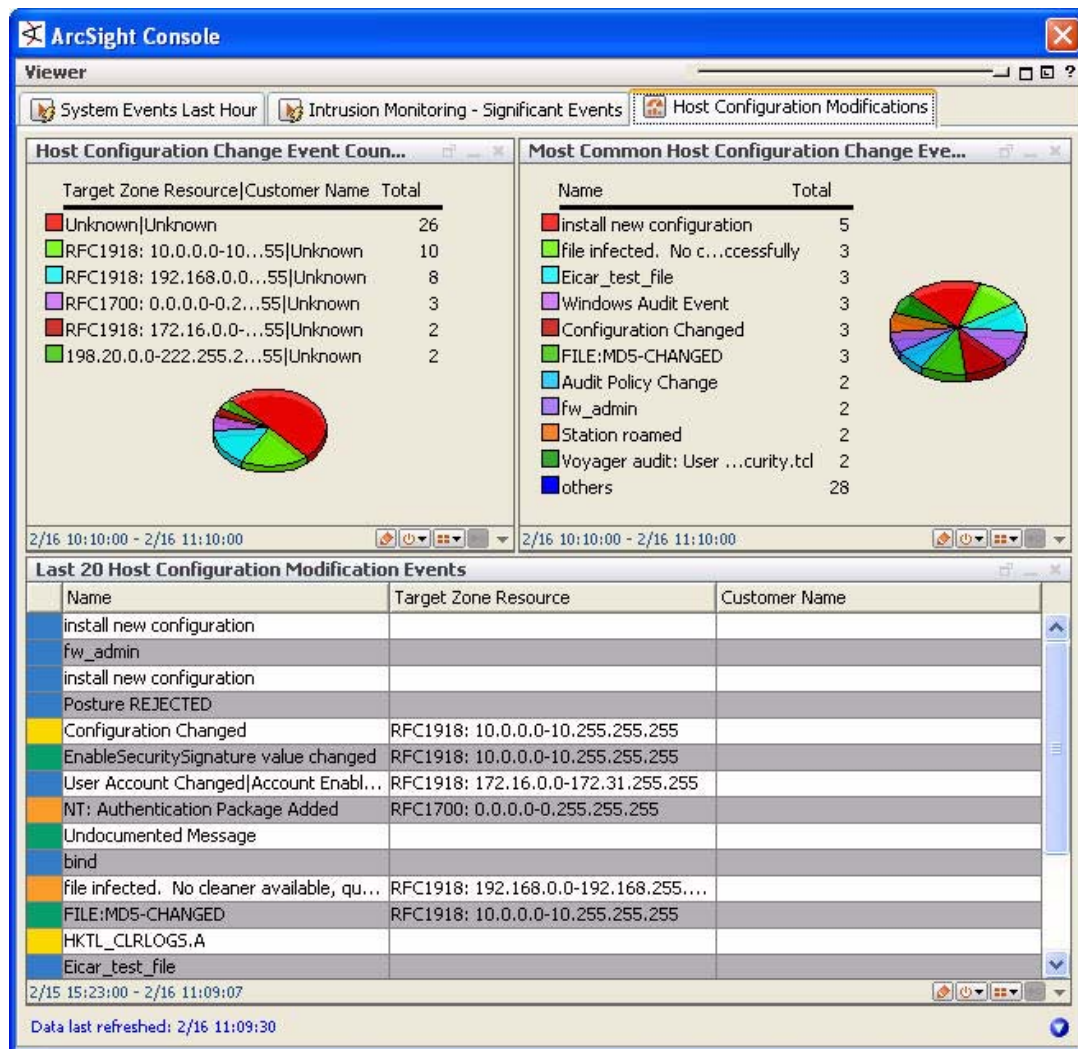


Operational Summaries:
These dashboards show real-time summaries of host modification activity.

These dashboards are described in more detail below.

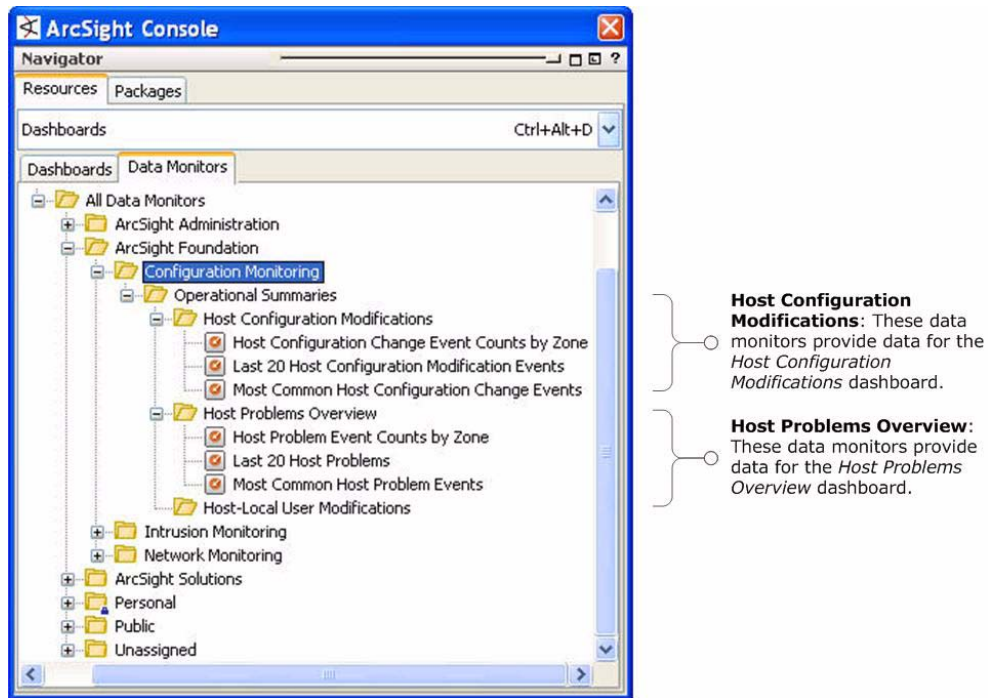
Dashboard	Description
Host Configuration Modifications	This dashboard shows three data monitors focusing on host configuration change events. The two Top Value Counts (Bucketized) data monitors show charts of the event counts by zone or the most common events. The Last N Events data monitor shows the last 20 events.
Host Problems Overview	This dashboard shows three data monitors focusing on host problem events. The two Top Value Counts (Bucketized) data monitors show charts of the event counts by zone or the most common events. The Last N Events data monitor shows the last 20 events.

The Host Configuration Modification dashboard shows two pie-charts, one with configuration changes events focused on zones, the other with the most common configuration change events, and a table of the last 20 modification events.



Configuration Monitoring Data Monitors

The Configuration Monitoring dashboards are supported by the following data monitors:



These data monitors are described in more detail below.

Data Monitor	Description
Host Configuration Change Event Counts by Zone	This data monitor provides a view of the top 10 Zones with configuration changes. By default, the data monitor displays a pie chart. This data monitor is a part of the Configuration Monitoring content.
Last 20 Host Configuration Modification Events	This data monitor provides a scrolling list of the last 20 host configuration events seen by the system. Events are noted by customer and zone in addition to the change type information. This data monitor is part of the Configuration Monitoring content.
Most Common Host Configuration Change Events	This data monitor provides a view of the top 10 most common host configuration changes. By default, the data monitor displays a pie chart. This data monitor is a part of the Configuration Monitoring content.
Host Problem Event Counts by Zone	This data monitor provides a graphical summary view of host-specific problems noted by ArcSight, by Zone. By default this data monitor displays a pie chart of the top 10 Zones by problem event volume. This data monitor is a part of the Configuration Monitoring content.
Last 20 Host Problems	This data monitor provides a table view of the last 20 host issues noted by ArcSight. This data monitor is used in the Host Problems Overview data monitor and these resources are part of the Configuration Monitoring content.

Data Monitor	Description
Most Common Host Problem Events	This data monitor shows graph of the top 10 most common problems seen on your monitored hosts. This data monitor is a part of the Host Problems Overview dashboard and is a part of the Configuration Monitoring content.

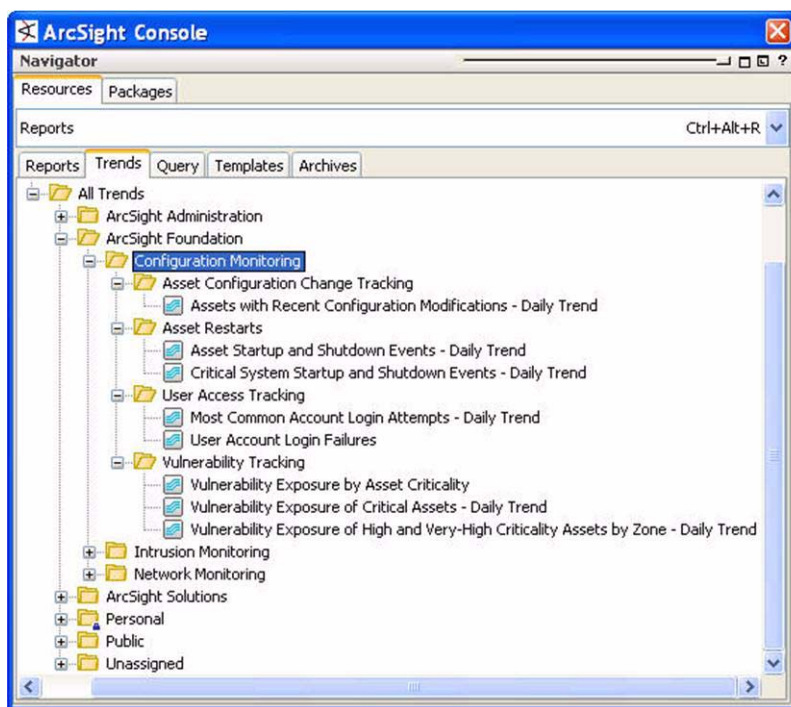
Configuration Monitoring Reports

The Configuration Monitoring foundation provides a system of reporting tools that together provide a comprehensive summary of activity that indicate configuration modifications on the network. These views are organized into groups depending on what level of detail you need to see:

- **Executive Summaries.** Executive summary reports provide high-level analysis of Configuration Monitoring activity for management reports. These views show overall trends and long-term summaries.
- **Operational Summaries.** The operational summary reports are intended for SOC operators and analysts for daily network monitoring and triage-level investigation.
- **Details.** The detailed reports are intended for incident responders and analysts who need access to relevant event details in order to investigate situations that arise from monitoring reports in the operational summaries.
- **SANS Top 5 Reports.** The SANS Top 5 reports that are relevant to Configuration Monitoring are those that address SANS section 3.

Configuration Monitoring Trends

The Configuration Monitoring foundation contains the following trends that gather data about various types of network configuration changes. This data is used by several Configuration Monitoring queries and reports.



Asset Configuration Change Tracking: This trend gathers data about configuration modifications by the day.

Asset Restarts: These trends gather data about asset start-ups and shutdowns.

User Access Tracking: These trends gather data about user log-ins.

Vulnerability Tracking: These trends gather data about vulnerabilities exposed on assets with various criticality levels.

Trends are useful for identifying spikes in behavior that could indicate a problem. For the user access tracking trends, for example, one user trying to log in 50 times is probably unusual unless the user is a sysadmin. A spike in failed logins could indicate a terminated employee who is trying to log in, or someone trying to gain unauthorized access data or systems.

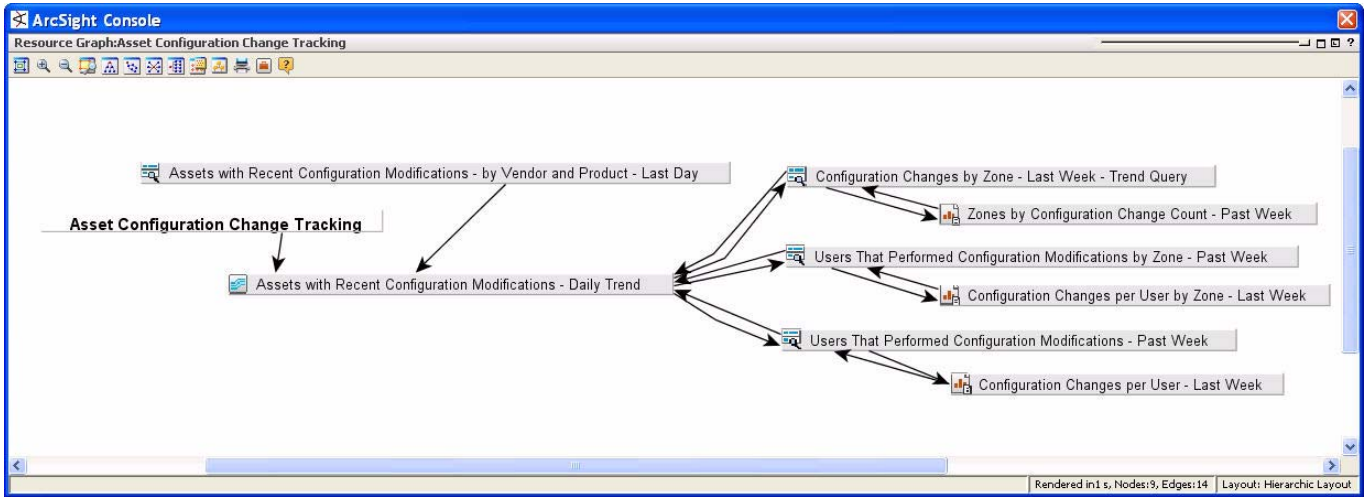
The three vulnerability trends gather statistics for exposed vulnerabilities. *Vulnerability Exposure by Asset Criticality* produces more granular results for all assets. *Vulnerability Exposure of Critical Assets* focuses on all assets categorized as critical.

The *Assets by Zone* trend summarizes vulnerability exposure by zone. These trends can help you keep track of software patch levels and remediation from organization to organization.

These trends are described in more detail below:

Trend	Description
Assets with Recent Configuration Modifications - Daily Trend	This daily trend picks up all changes to assets within the last day and stores information about the change itself as well as who made the change.
Asset Startup and Shutdown Events - Daily Trend	This trend collects daily statistics on shutdown and startup events from your different assets. The trend query includes information on the device product and vendor in case you wish to query the trend for stats by OS.
Critical System Startup and Shutdown Events - Daily Trend	This trend collects daily statistics about critical system startup and shutdown events. The startup events typically indicate a system restart, but may not be reliably matched with shutdown events. This trend is a more focused view (assets modeled with criticality categorization) of the Asset Startup and Shutdown Events - Daily Trend.
Most Common Account Login Attempts - Daily Trend	This trend collects daily statistics about User Account Login Attempts to track the most frequent user logins.
User Account Login Failures	This trend collects aggregate information about failed user account login attempts. It also collects other information including the target zone as well as the target device vendor and product.
Vulnerability Exposure by Asset Criticality	This trend provides a daily snapshot of the vulnerability counts of assets marked as high or very high criticality.
Vulnerability Exposure of Critical Assets - Daily Trend	This trend collects daily statistics on the vulnerability exposure of your assets that have been categorized as highly or very-highly critical. The trend includes information about the asset and a count of the number of vulnerabilities it currently exposes.
Vulnerability Exposure of High and Very-High Criticality Assets by Zone - Daily Trend	This trend collects a weekly snapshot of the assets to be used for tracking of how many vulnerabilities highly and very-highly critical systems have over time, by zone. This trend only collects a count of the number of vulnerabilities in these zones, not the full list of vulnerabilities, as this would result in much larger storage requirements.

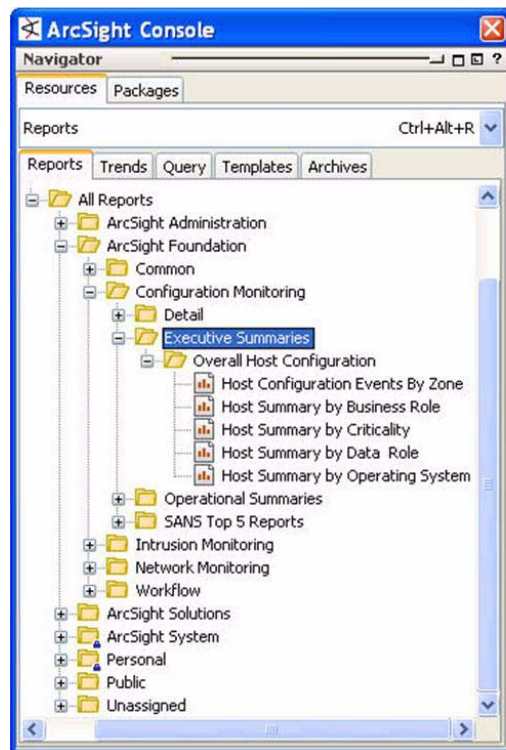
Once the trend data is stored in the trend table, the data is available to be queried for reports. The following Configuration Monitoring queries and reports consume data from these trends:



You can also build your own reports based on the data gathered in these trends. These trends do not support minute-by-minute details, but they can be used to extract summaries that span an hour or more.

Executive Summary Reports

The executive summary reports show summaries by zone of configuration changes. This can confirm the health of IT operations, and can also be used to track expected flurries of activity, such as when Microsoft releases a patch.



For these reports to be populated with data, your network assets must be categorized in the Business Role, Criticality, Data Role, and Operating System asset categories.

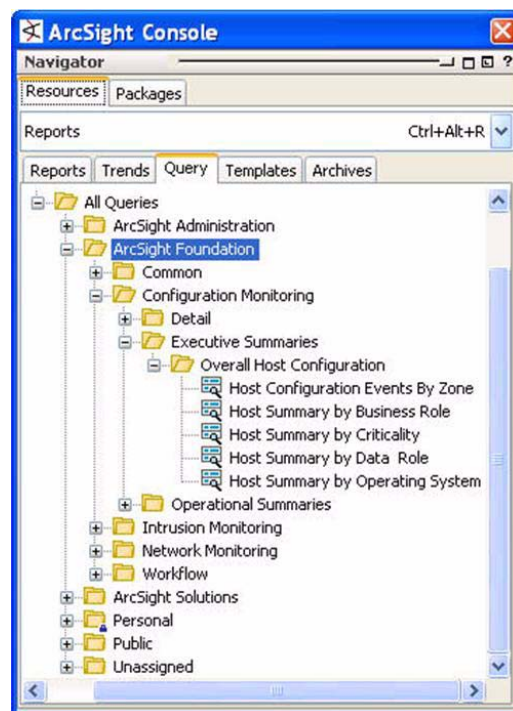
These reports are described in more detail below.

Report	Description
Host Configuration Events By Zone	This report provides a summary pie chart showing the breakdown of host configuration events by Zone. This chart and others are combined to produce an overview of the Asset configurations. This report is a part of the Configuration Monitoring content.
Host Summary by Business Role	This report provides a summary pie chart showing the breakdown of Assets by Business Role. This chart and others are combined to produce an overview of the Asset configurations. This report is a part of the Configuration Monitoring content.
Host Summary by Criticality	This report provides a summary pie chart showing the breakdown of Assets by Criticality. This chart and others are combined to produce an overview of the Asset configurations. This report is a part of the Configuration Monitoring content.

Report	Description
Host Summary by Data Role	This report provides a summary pie chart showing the breakdown of Assets by Data Role. This chart and others are combined to produce an overview of the Asset configurations. This report is a part of the Configuration Monitoring content.
Host Summary by Operating System	This report provides a summary pie chart showing the breakdown of Assets by Operating System. This chart and others are combined to produce an overview of the Asset configurations. This report is a part of the Configuration Monitoring content.

Executive Summary Queries

The data for the executive summary reports is gathered by the following queries:



Executive Summaries:
These queries poll the event stream to supply the data for the executive summary reports.

The Executive Summary queries are described in more detail below:

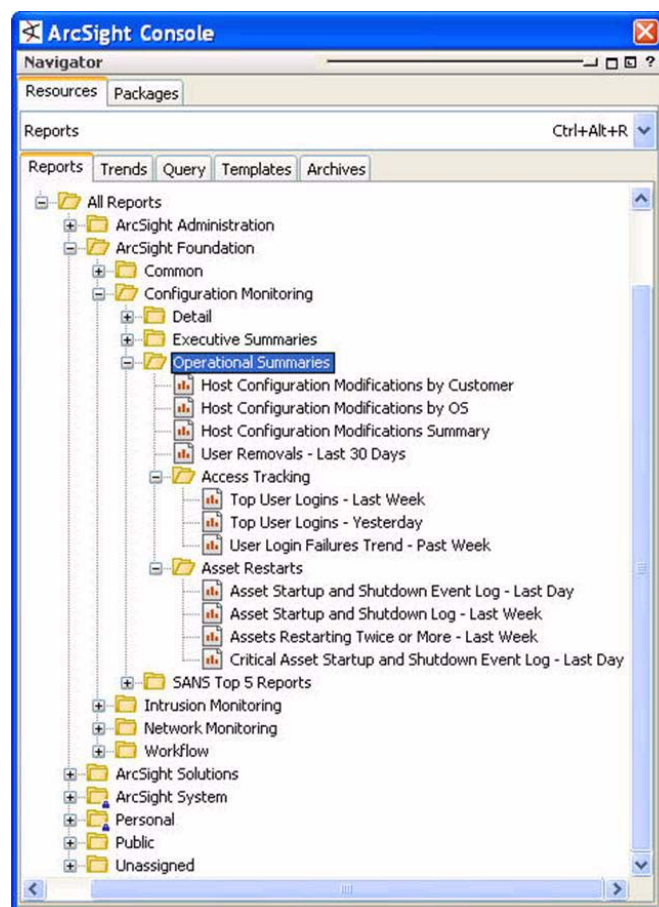
Query	Description
Host Configuration Events By Zone	This query selects information regarding the breakdown of host configuration events by Zone. This query is a part of the Configuration Monitoring content.
Host Summary by Business Role	This query selects data regarding the breakdown of Assets by Business Role. This query is a part of the Configuration Monitoring content.
Host Summary by Criticality	This query selects data to show the breakdown of Assets by Criticality. This query is a part of the Configuration Monitoring content.

Query	Description
Host Summary by Data Role	This query selects data to show the breakdown of Assets by Data Role. This query is a part of the Configuration Monitoring content.
Host Summary by Operating System	This query selects data to show the breakdown of Assets by Operating System. This query is a part of the Configuration Monitoring content.

Operational Summary Reports

The Configuration Monitoring operational summary reports provide medium-detail summaries of configuration modifications for hosts by customer and OS, and lists user accounts removed over the last 30 days. You can corroborate these lists with review these, why were these accounts removed, does it correlate with quits and terminations?

The access tracking reports Access tracking stuff, who's been logging in most when, where; from trend, login failures trend over time. reports on asset restarts, listing of all, list of those restarted more than twice; list of critical assets rebooted.



Operational Summaries:

These reports show a summary of host configurations in the last week from a number of perspectives.

Access Tracking: These reports show a summary of user log-in activity over a series of timeframes.

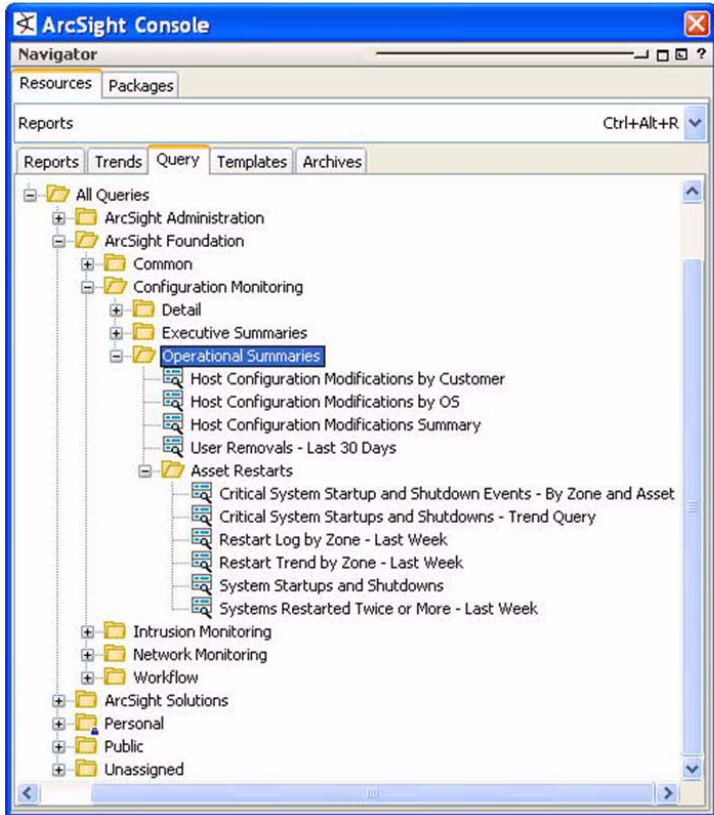
Asset Restarts: These reports show a profile of system startups and shutdowns over the last day or week.

The Operational Summary reports are described in more detail below:

Report	Description
Host Configuration Modifications Summary	This report provides a summary of the host configuration modification activity seen over the preceding week. This report should be focused on a certain Zone to provide a manageable and useful data set. This report is a part of the Configuration Monitoring content.
Host Configuration Modifications by Customer	This report will show the host configuration modifications by customer.
Host Configuration Modifications by OS	This report will show the host configuration modifications by OS.
User Removals - Last 30 Days	This report will show the user removals for the past 30 days.
Top User Logins - Last Week	This report gives an overview of the top users attempting logins over the past week.
Top User Logins - Yesterday	This summary report provides a chart summary of the top user logins that occurred yesterday and a table listing the login counts by user.
User Login Failures Trend - Past Week	This report provides aggregate information about what user accounts are experiencing failed logins most often over the past 7 days.
Asset Startup and Shutdown Event Log - Last Day	This report provides a listing of the system startup and shutdown events seen over the past day.
Asset Startup and Shutdown Log - Last Week	This report queries a trend table to retrieve a listing of all system startup and shutdown events seen over the past week.
Assets Restarting Twice or More - Last Week	This report provides you with a list of assets that appear to be restarting twice or more per week. Depending on the function of these assets, these events may indicate a problem and should be investigated.
Critical Asset Startup and Shutdown Event Log - Last Day	This report provides a listing of the critical system startup and shutdown events seen over the past day.

Operational Summary Queries

The data for the operational summary reports are provided by the following queries:



The screenshot shows the ArcSight Console interface. The 'Navigator' pane on the left displays a tree structure under 'All Queries'. The 'Operational Summaries' folder is selected, showing a list of queries: Host Configuration Modifications by Customer, Host Configuration Modifications by OS, Host Configuration Modifications Summary, User Removals - Last 30 Days, Asset Restarts, Critical System Startup and Shutdown Events - By Zone and Asset, Critical System Startups and Shutdowns - Trend Query, Restart Log by Zone - Last Week, Restart Trend by Zone - Last Week, System Startups and Shutdowns, and Systems Restarted Twice or More - Last Week. To the right of the screenshot, two callout boxes provide descriptions:

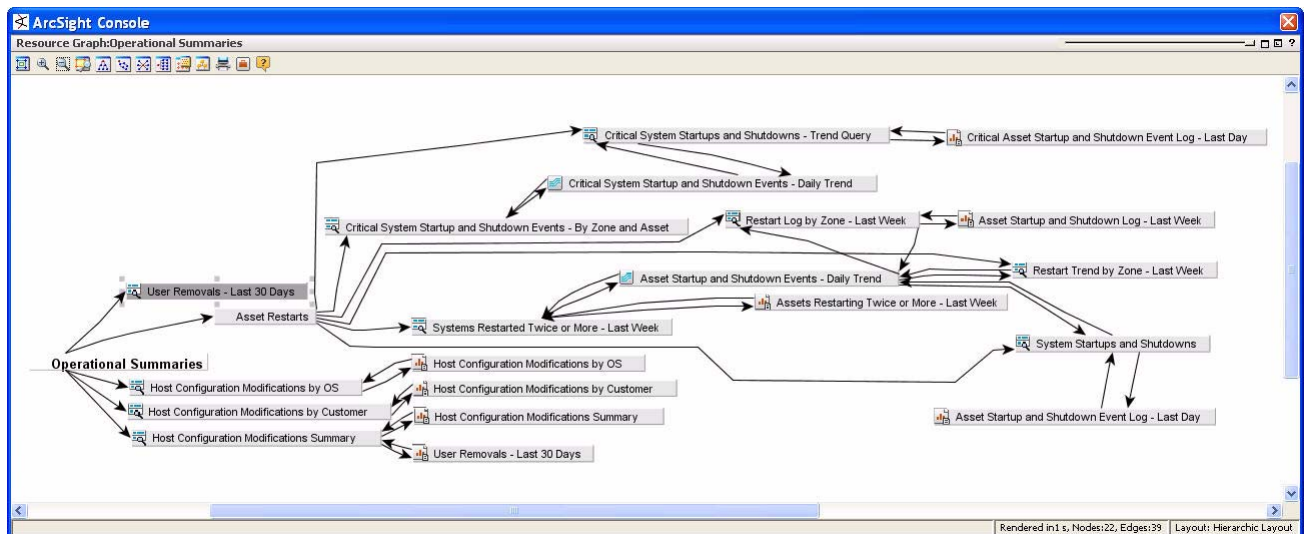
- Operational Summaries:** These queries leverage configuration monitoring filters to gather data for the Operational Summary reports.
- Asset Restarts:** These queries express conditions and leverage filters to gather data for the asset restart reports and trends.

These queries are described in more detail below:

Query	Description
Host Configuration Modifications Summary	This query selects data to provide a summary of the host configuration modification activity. This report is a part of the Configuration Monitoring content.
Host Configuration Modifications by Customer	This query selects host configuration modification data (restricted by the Host Configuration Modifications filter), grouped by customer.
Host Configuration Modifications by OS	This query selects host configuration modification data (restricted by the Host Configuration Modifications filter), grouped by Operating System.
User Removals - Last 30 Days	This query selects user account deletion data (restricted by the User Account Deletions filter), grouped by customer.
Critical System Startup and Shutdown Events - By Zone and Asset	This query collects summary data from a trend table to provide a count of how often your critical systems startup or shut down.
Critical System Startups and Shutdowns - Trend Query	This query is used to collect information about critical system startup and shutdown events that occurred yesterday. The startup events typically indicate a system restart, but may not be reliably matched with shutdown events.

Query	Description
Restart Log by Zone - Last Week	This query retrieves a list of all asset startup and shutdown events over the past week.
Restart Trend by Zone - Last Week	This query checks the system startup and shutdown trend table and retrieves a count of the number of restarts per zone, per day, for the last week. This is useful for creating charts and tables of stats for your different zones.
System Startups and Shutdowns	This query is used to collect information about system startup and shutdown events that occurred yesterday. The startup events typically indicate a system restart, but may not be reliably matched with shutdown events.
Systems Restarted Twice or More - Last Week	This query checks the system startup and shutdown trend table and retrieves a list of the systems that have restarted more than once in the past week. It shows the restart history for each system each day.

These queries support the following Configuration Monitoring reports and trends:



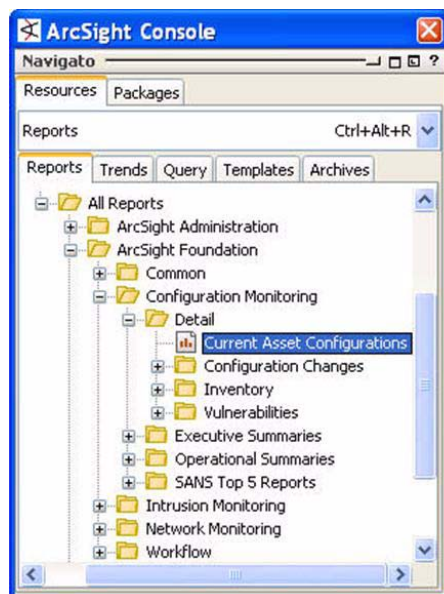
Detail Reports

The detail reports contain numerous perspectives divided into four major categories:

- Current configuration
- Configuration changes
- Inventory
- Vulnerabilities

Current Configuration Report

The current configuration report provides a snapshot of the current configurations of all devices reporting to ArcSight.



Current Asset Configurations: This report shows the current configuration of all devices reporting to ArcSight.

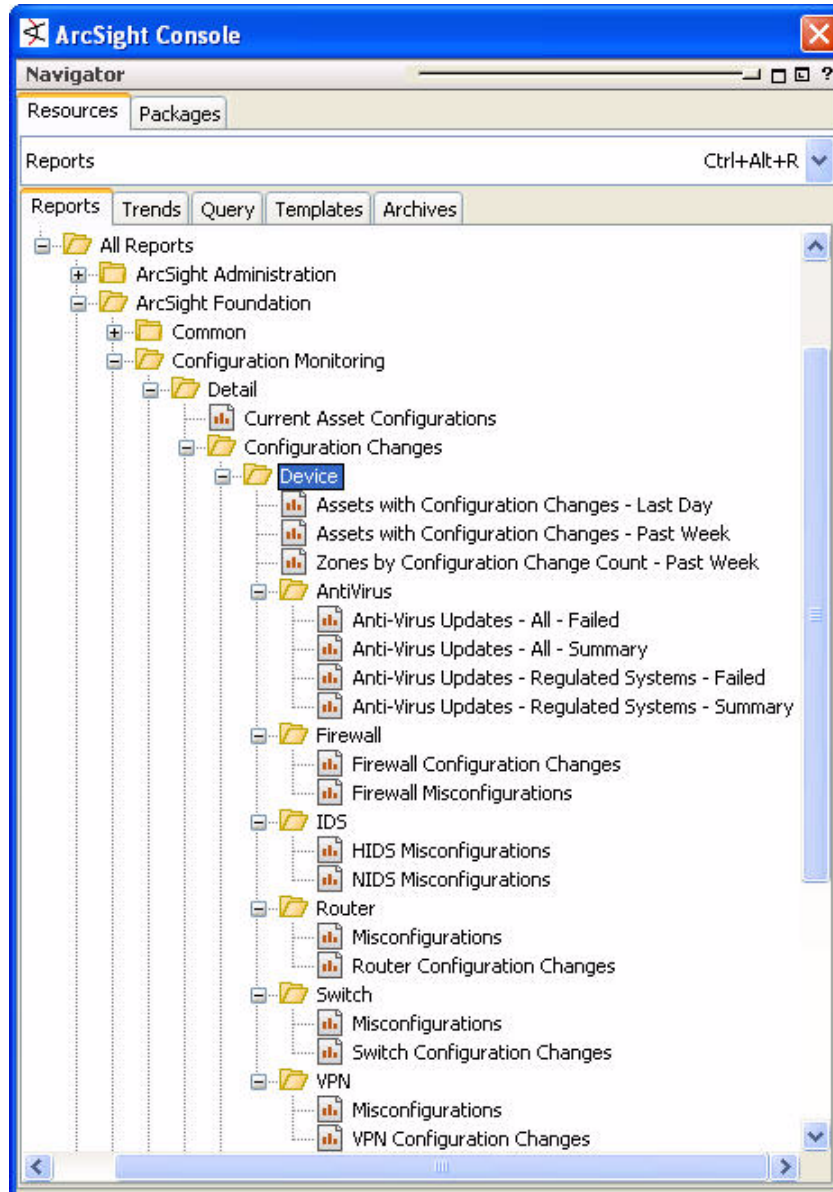
This report is described in more detail below:

Report	Description
Current Asset Configurations	This report provides a listing of the assets modeled in and monitored by the ArcSight system and the current configuration information available to the system regarding those assets. This report will primarily provide information on the operating system and services running on the selected set of hosts. For information on vulnerabilities, see the reports in the Detail/Vulnerabilities section. This report is a part of the host-specific Configuration Monitoring content.

The current configuration report is supported by the current configuration query.

Configuration Changes by Device Reports

The configuration changes by device reports concentrate on configuration changes on the devices reporting into ArcSight ESM from ArcSight SmartConnectors. The views start out with a summary of activity per device and per zone over the past day and week. The reports then expand into a breakdown of activity from the different major types of network devices. You can review these to verify that anti-virus definitions are being updated regularly, and that appropriate changes are being made to other network devices by appropriate users on appropriate timetables.

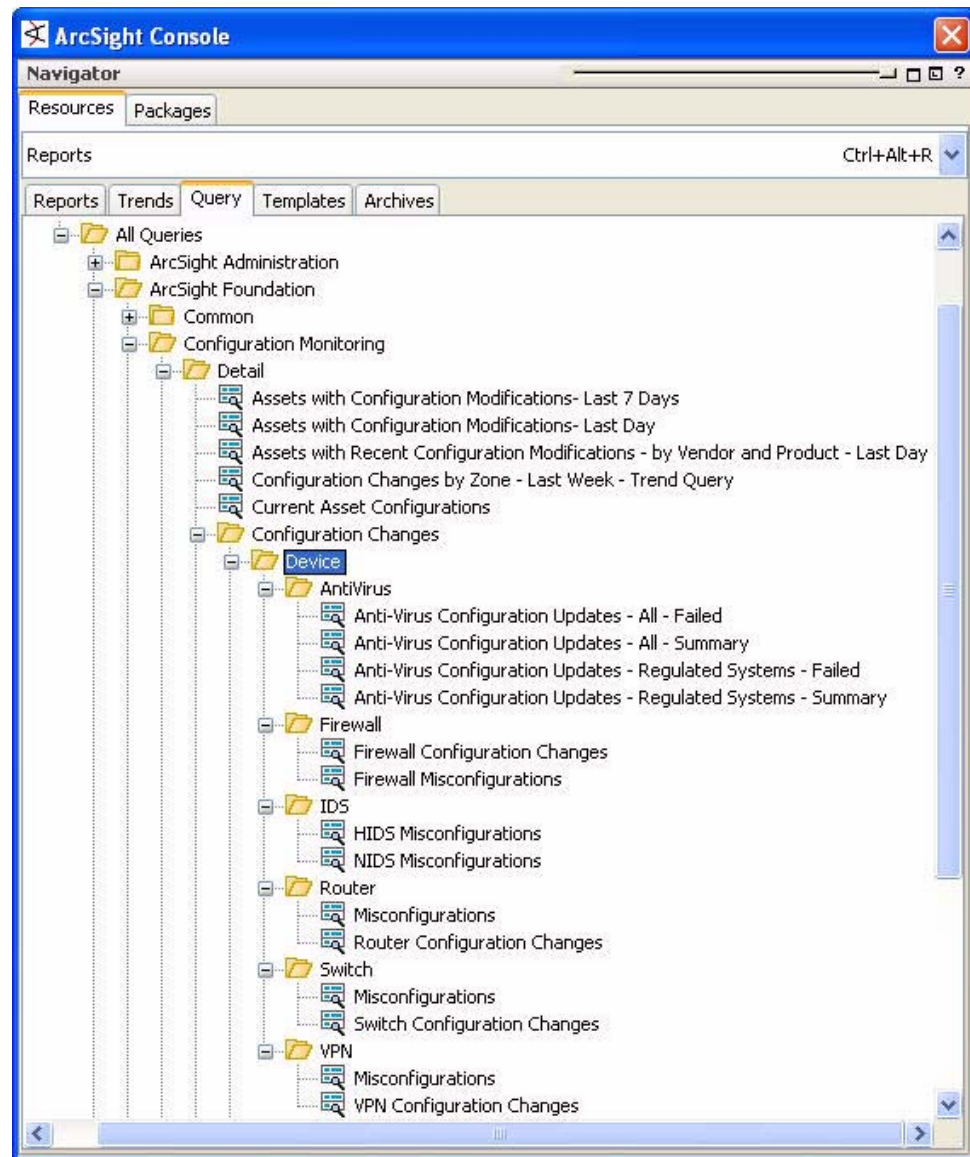


The Configuration Changes by Device reports are described in more detail below:

Report	Description
Assets with Configuration Changes - Last Day	This report provides a listing of the assets that have been modified over the course of the last day and who modified them. The listing is sorted first by zone, then by asset name.
Assets with Configuration Changes - Past Week	This report provides a listing of the assets that have been modified over the course of the last week and who modified them. The listing is sorted first by zone, then by asset name.
Zones by Configuration Change Count - Past Week	This report provides a summary chart and table to show what zones had the most configuration changes over the past week.

Configuration Changes by Device Queries

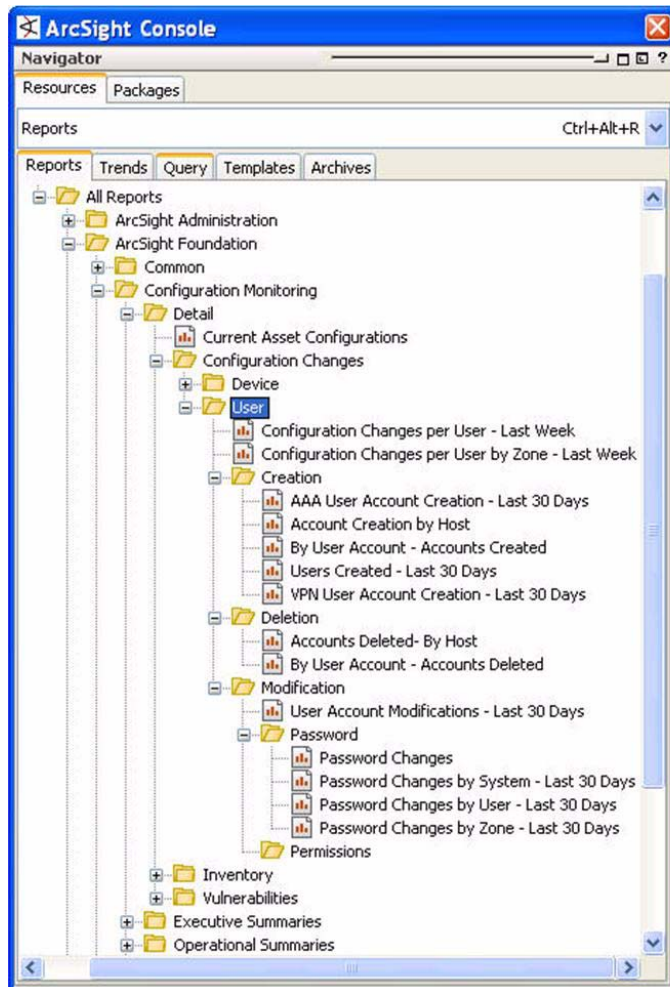
The configuration changes by device reports are supported by the following queries:



Configuration Changes by User Reports

The configuration changes by user reports concentrate on configuration changes made to user accounts. If you are using a AAA system, such as RSA ACE, these reports help monitor activity, such as whether accounts have been created, deleted, or modified in the last 30 days.

Keeping track of VPN users is important, because they are gaining remote access to the network. Keeping track of user account deletion and modifications, such as password changes, helps you keep track of how password policies are being applied and carried out.



User: These reports summarize activity from all users over the past week.

Creation: These reports provide detailed summaries of user account creations in a variety of systems over the past 30 days.

Deletion: These reports provide detailed summaries of user account deletions.

Modification: This report summarizes user account modifications over the past 30 days.

Password: These reports provide summaries of user password changes over the past 30 days.

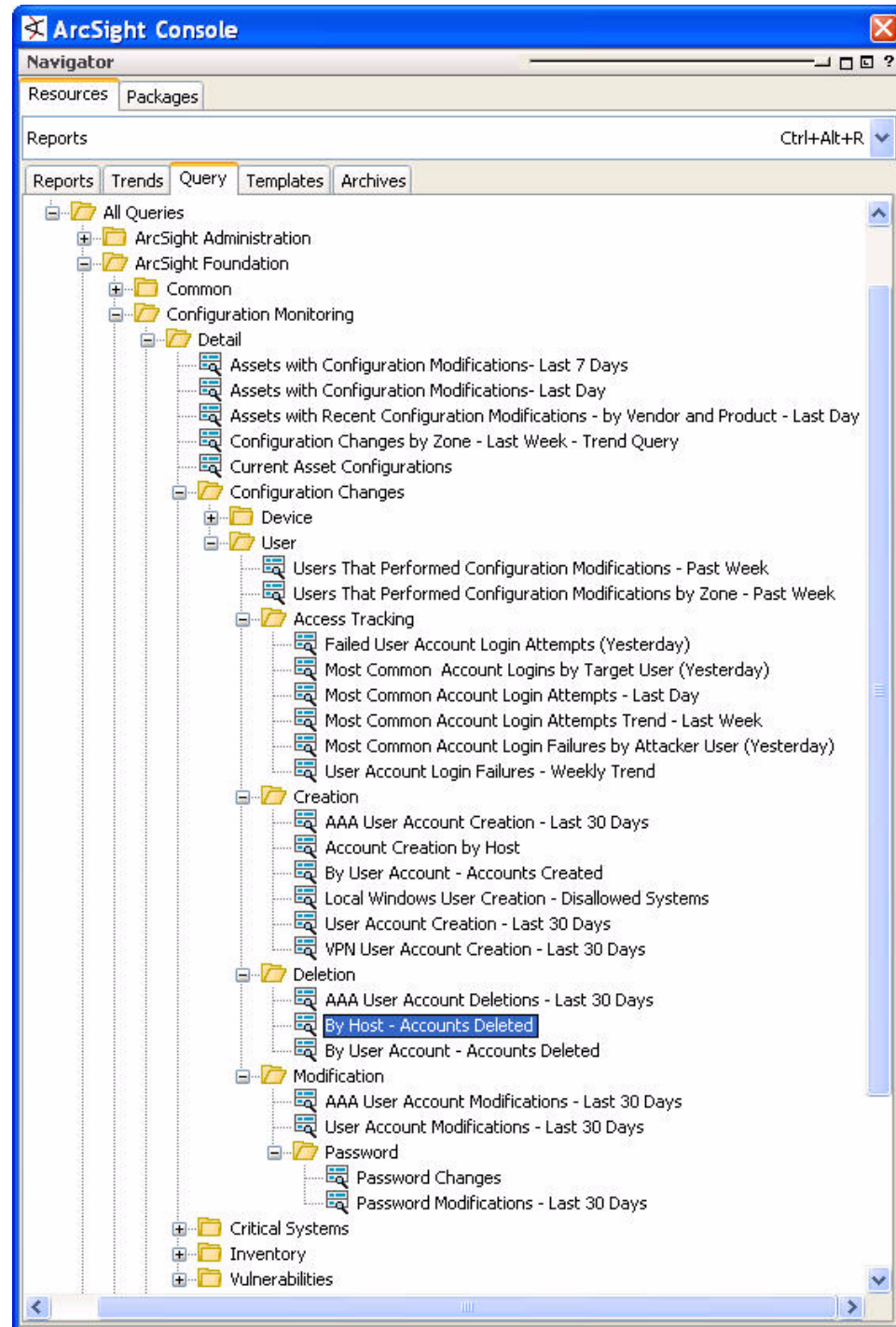
The Configuration Changes by User reports are described in more detail below:

Report	Description
Configuration Changes per User - Last Week	This report provides a view of users that have made configuration changes over the past week, sorted by the number of changes each user made.
Configuration Changes per User by Zone - Last Week	This report provides a view of users that have made configuration changes over the past week, sorted by zone and the number of changes each user made.
AAA User Account Creation - Last 30 Days	This report contains one table showing all the AAA user account creation for the past 30 days.

Report	Description
Account Creation by Host	This report provides a listing of the account creation events seen over the past week on your monitored assets. Note that this report looks for host-local user account creations, rather than authentication service account creations. This means that this report will not pick up user additions in Active Directory, for instance. This report is a part of the Configuration Monitoring content.
By User Account - Accounts Created	
Users Created - Last 30 Days	
VPN User Account Creation - Last 30 Days	This report contains one table showing all the VPN user account creation for the past 30 days.
Accounts Deleted- By Host	This report provides a listing of user deletions over the previous 30 days, ordered by Customer, Zone, and System. This report is a part of the Configuration Monitoring content.
User Account Modifications - Last 30 Days	This report shows an overview of the user account modifications for the past 30 days. It contains one pie chart and a table. The pie chart shows the total number of user account modifications per user account and the table shows all the details.
Password Changes by System - Last 30 Days	This report provides a listing of the password changes for the past 30 days. It contains one pie chart and a table. The pie chart shows the total number of password changes by system and the table shows the details of the password changes.
Password Changes by User - Last 30 Days	This report provides a listing of the password changes for the past 30 days. It contains one pie chart and a table. The pie chart shows the total number of password changes by user and the table shows the details of the password changes.
Password Changes by Zone - Last 30 Days	This report provides a listing of the password changes for the past 30 days. It contains one pie chart and a table. The pie chart shows the total number of password changes by zone and the table shows the details of the password changes.

Configuration Changes by User Queries

The configuration changes by user reports are supported by the following queries:

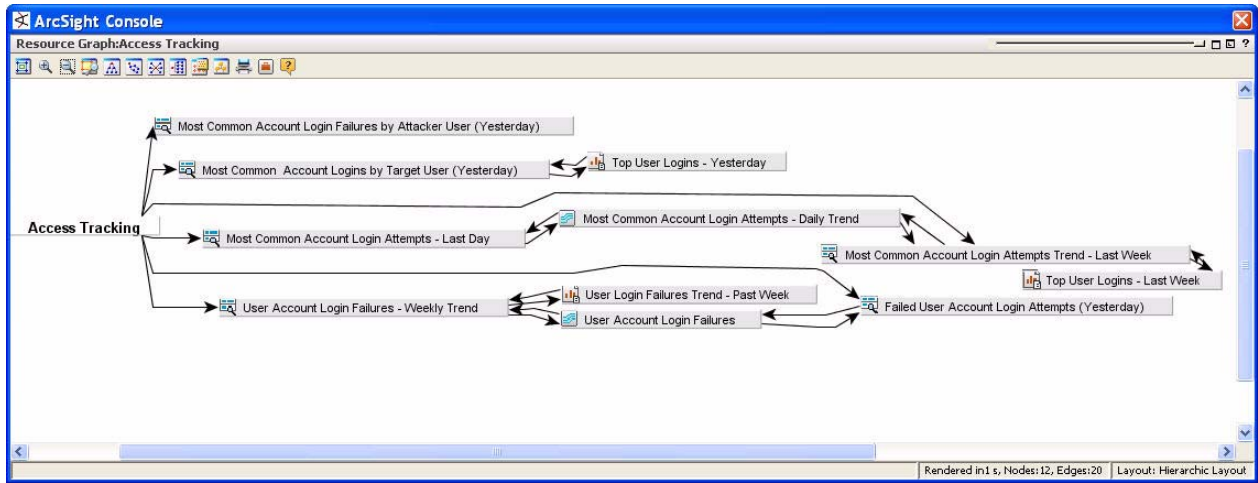


The Configuration Changes by User queries are described in more detail below:

Query	Description
Users That Performed Configuration Modifications - Past Week	This query retrieves a list of the users that performed configuration modifications to assets in the past week.
Users That Performed Configuration Modifications by Zone - Past Week	This query retrieves a list of the users that performed configuration modifications to assets in the past week, by zone.
Failed User Account Login Attempts (Yesterday)	This query selects events passed by the Failed User Account Login Attempts filter, selecting Category Object, Target Address, Target Asset ID, Target Asset Name, Target Nt Domain, Target User ID, Target User Name, Target Zone, Event ID and End Time for the User Account Login Failures trend.
Most Common Account Logins by Target User (Yesterday)	This query selects events passed by the Successful User Account Login Attempts filter, selecting Category Object, Target Address, Target Asset ID, Target Asset Name, Target Nt Domain, Target User ID, Target User Name, Target Zone and the Count of Event ID for the Top User Logins - Yesterday report.
Most Common Account Login Attempts - Last Day	This query selects events passed by the User Account Login Attempts filter, selecting Category Object, Target Address, Target Asset ID, Target Asset Name, Target Nt Domain, Target User ID, Target User Name, Target Zone, Attacker Address, Attacker Asset Name, Attacker Nt Domain, Attacker User ID, Attacker User Name, Attacker Zone and Category Outcome for the Most Common Account Login Attempts - Daily Trend.
Most Common Account Login Attempts Trend - Last Week	This query retrieves a listing of the count of target user account logins by zone for the last 7 days.
User Account Login Failures - Weekly Trend	This query retrieves aggregated information about failed logins over the past week from a trend table.
AAA User Account Creation Trend	This query selects events passed by the AAA User Account Creations filter, selecting Customer, Attacker User Name, Attacker Zone, Target Address, Target Asset Name, Target Host Name, Target Nt Domain, Target User ID, Target User Name and Target Zone for the AAA User Account Creation trend.
Account Creation by Host	This query provides a listing of the account creation events seen over the past week on your monitored assets. Note that this query looks for host-local user account creations, rather than authentication service account creations. This means that this query will not pick up user additions in Active Directory, for instance. This query is a part of the Configuration Monitoring content.
By User Account - Accounts Created	This query selects events meeting the conditions Category Behavior = /Authentication/Add and Category Outcome = /Success, selecting End Time, Target User Name, Attacker User Name, Name, Target Zone Name and Target Host Name for the By User Account - Accounts Created report.

Query	Description
Trend on AAA User Account Creation	This query on the AAA User Account Creation trend selects Customer Name, Attacker User Name, Attacker Zone Name, Target Address, Target Asset Name, Target Host Name, Target Nt Domain, Target User ID, Target User Name and Target Zone Name for the AAA User Account Creation report.
Trend on User Account Creation	This query on the User Account Creation trend selects Customer, Attacker User Name, Attacker Zone, Target Address, Target Asset Name, Target Host Name, Target Nt Domain, Target User ID, Target User Name and Target Zone for the User Account Creation report.
Trend on VPN User Account Creation	This query on the VPN User Account Creation trend selects Customer, Target Zone Name, Target User ID and Attacker User Name for the VPN User Account Creation report. The fields Target Zone Name, Target User ID and Attacker User Name are renamed Zone, New Account and Creator, respectively, in the report.
User Account Creation Trend	This query on events restricted by the User Account Creations filter selects Customer, Attacker User Name, Attacker Zone, Target Address, Target Asset Name, Target Host Name, Target Nt Domain, Target User ID, Target User Name and Target Zone for the User Account Creation trend.
VPN User Account Creation Trend	This query on events restricted by the VPN User Account Creations filter selects Customer, Attacker User Name, Attacker Zone, Target Address, Target Asset Name, Target Host Name, Target Nt Domain, Target User ID, Target User Name and Target Zone for the VPN User Account Creation trend.
Accounts Deleted by Host Trend	This query on events restricted by the User Account Deletions filter provides a listing of the users deleted over the time interval by System & Zone for the Accounts Deleted by Host trend.
By Host - Accounts Deleted	This query on the Accounts Deleted by Host trend provides a listing of the users deleted over the past 30 days by System & Zone.
Trend on User Account Modifications	This query on the User Account Modifications trend selects data for use in the User Account Modifications report. This query is used as both the chart and table data sources.
User Account Modifications Trend	The query on events restricted by the User Account Modifications filter to select Customer, Target Zone, Target Address, Target Asset ID, Target Asset Name Target User ID, Target User Name, Aggregated Event Count and End Time for the User Account Modifications trend.
Password Modifications Trend	This query on events restricted by the Successful Password Changes filter selects Attacker User ID, Attacker User Name, Attacker Zone, Target Address, Target Asset ID, Target Asset Name, Target Nt Domain, Target User ID, Target User Name, Target Zone and sums Aggregated Event Count for use in the Password Modifications trend.
Trend on Password Modifications	This query selects data from the Password Modifications trend for use in the Password Changes by System/User/Zone; reports.

The access tracking queries support the following Configuration Monitoring reports and trends.

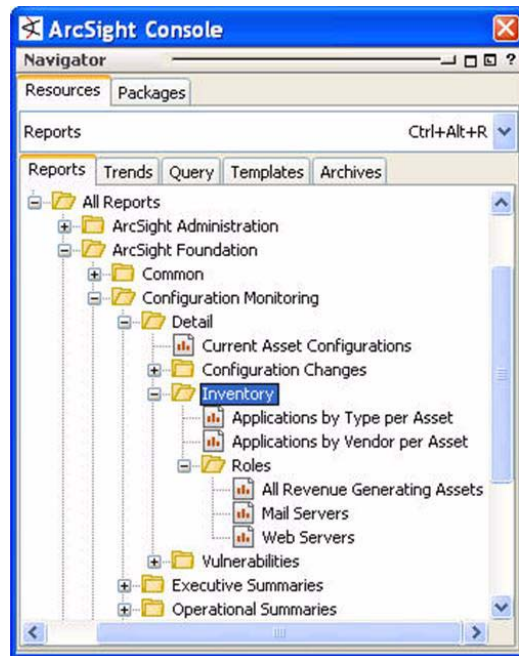


Inventory Reports

The inventory reports provide statistics about the applications running on your network systems sorted by application, application type, vendor, and business role.



For these reports to be active, your network devices should be categorized in the application and role asset categories.



Inventory: These reports provide an accounting of applications running on your network systems sorted by type and vendor.

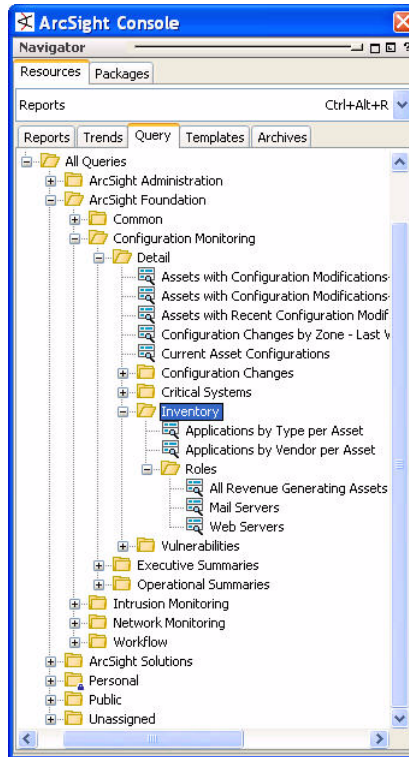
Roles: These reports provide a complete list of assets serving in these business roles.

These reports are described in more detail below.

Report	Description
Applications by Type per Asset	This report gives a listing of all Assets that have been scanned for Applications or that have been manually categorized with Applications and shows the Applications by Type. This report is a part of the Configuration Monitoring content.
Applications by Vendor per Asset	This report gives a listing of all Assets that have been scanned for Applications or that have been manually categorized with Applications and shows the Applications by Vendor. This report is a part of the Configuration Monitoring content.

Inventory Queries

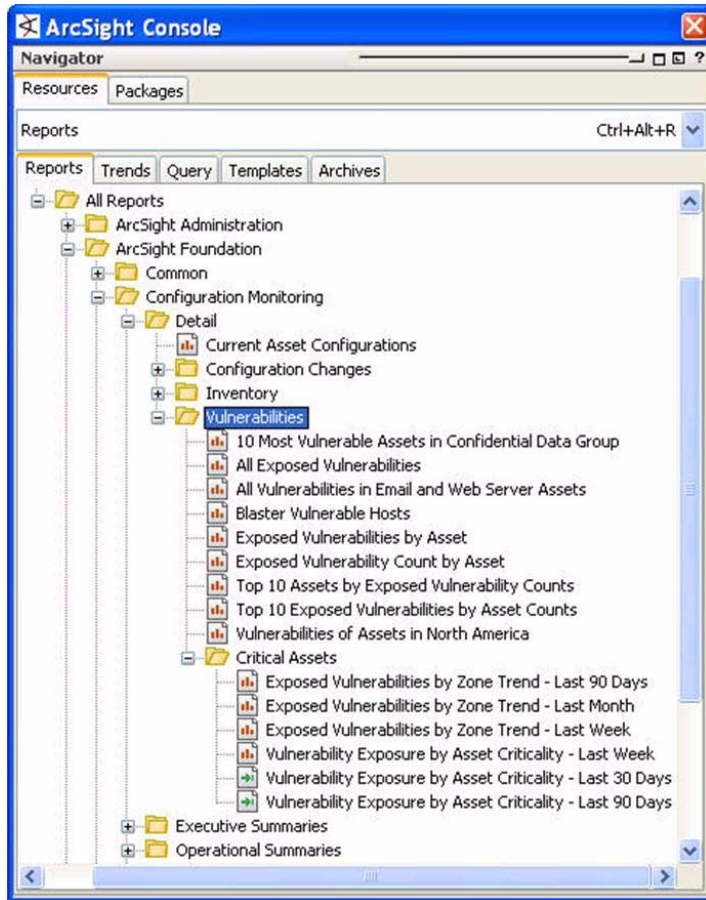
The inventory queries supply the conditions for the inventory reports.



Vulnerability Reports

The vulnerability reports provide a series of statistical views about the vulnerabilities exposed on your network assets. These reports are presented in a variety of perspectives to provide a comprehensive view of the network's vulnerability profile. These views are a starter set; you can add to these, focus them on a particular asset, zone, business role, or other distinction to make the reports reveal more insight about your network's vulnerability profile.

The critical asset reports leverage trends that span over one week, 30 days, and 90 days to provide a long-term look at exposed vulnerability patterns. These reports can also be focused on an asset criticality category over a 30 or 90-day time frame.



Vulnerabilities: These reports provide an accounting of vulnerabilities exposed on the network from various perspectives.

Critical Assets: These reports leverage trends to provide a long-term view of vulnerability management on your network.

These reports are described in more detail below.

Report	Description
Exposed Vulnerabilities by Zone Trend - Last 90 Days	This report provides a chart view of the exposed vulnerabilities across your top vulnerable zones over the course of a week. If you patch on a monthly or longer basis this report may not provide much value for you and you should consult the reports for longer periods.

Report	Description
Exposed Vulnerabilities by Zone Trend - Last Month	This report provides a chart view of the exposed vulnerabilities across your top vulnerable zones over the course of a month. If you patch on a monthly or longer basis this report may not provide much value for you and you should consult the reports for longer periods.
Exposed Vulnerabilities by Zone Trend - Last Week	This report provides a chart view of the exposed vulnerabilities across your top vulnerable zones over the course of a week. If you patch on a monthly or longer basis this report may not provide much value for you and you should consult the reports for longer periods.
Vulnerability Exposure by Asset Criticality - Last Week	This report provides a weekly view into the vulnerability exposure trend of your high and very high criticality assets.



To create a focused report that focuses on another time period:

- 1 Right-click the focusable report *Vulnerability Exposure by Asset Criticality - Last Week* ([All Reports/ArcSight Foundation/Configuration Monitoring/Detail/Vulnerabilities/Critical Assets/Vulnerability Exposure by Asset - Last Week](#)) and select **New Focused Report**.
- 2 In the Focused Report Editor in the Inspect/Edit panel on the Attributes tab, fill in the following values and click **Apply**:

Field	Value
Name	Enter a name for the focused report that differentiates it from the parent report and indicates what the report is focused on.
Source Report	This field is automatically filled in by the parent report and is not editable.
Description	Add a description of the report to clarify what it does for other users.

You can add more details to the focused report to help you keep track of it in your own system, such as external ID, alias, owner, and creation details.

- 3 At the Parameters tab, you can change any of the values by removing the checkmark from the *Use Default* column. To specify the time period you want the report to focus on, scroll down to the chart section in the Query Parameters section and do the following:

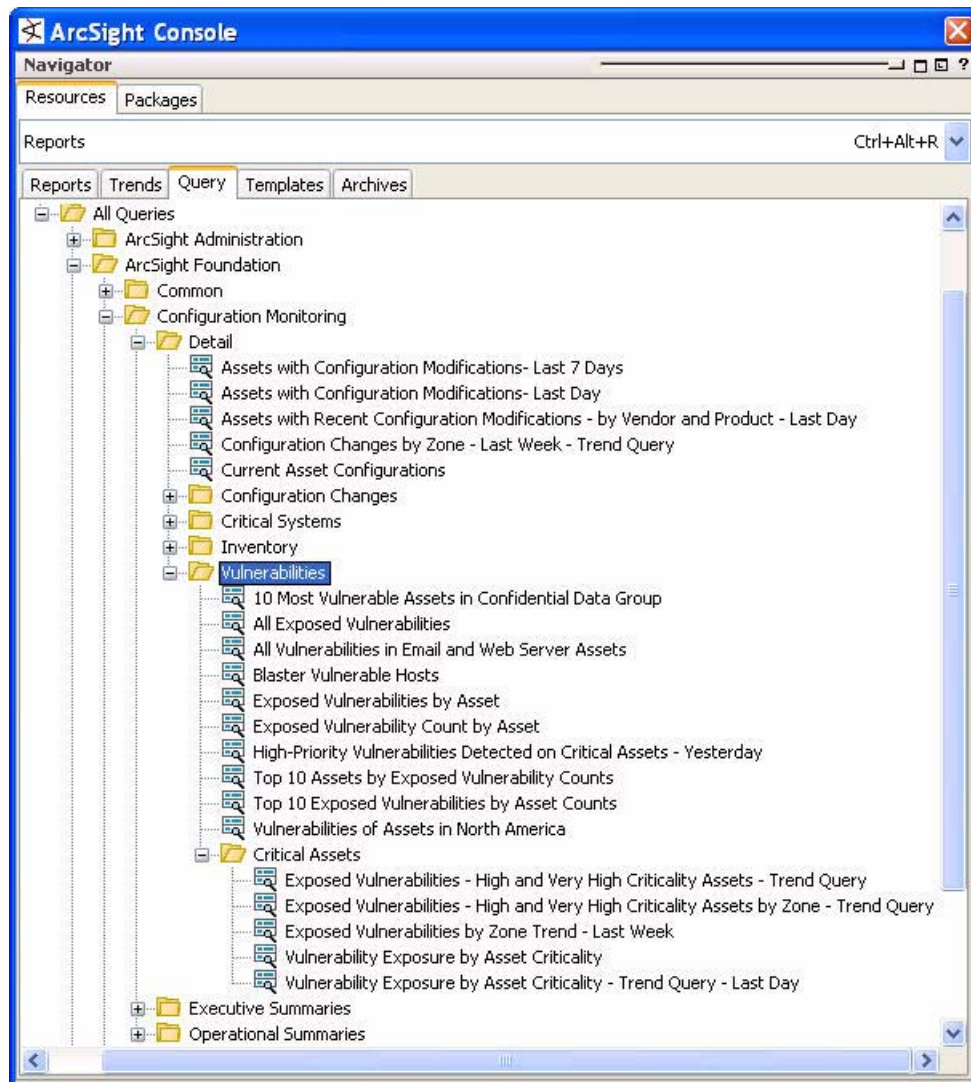
Field	Value
StartTime	To change the time range over which the data is gathered, remove the "Use Default" checkmark and either select a new start time from the drop-down menu, or enter a new start time manually from the  menu.
EndTime	To change the data end time, remove the "Use Default" checkmark and either select a new end time from the drop-down menu, or enter a new end time manually from the  menu.
Title	If present, remove the "Use Default" checkmark and enter a report title that will appear in the report output.

To run a focused report:

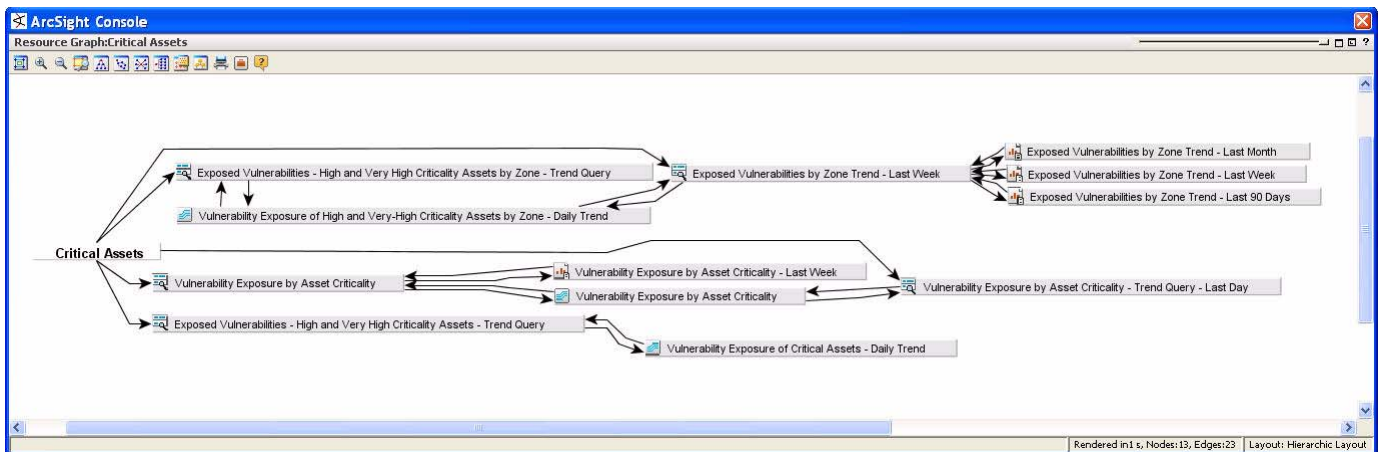
- 1 Right-click the focused report and select **Run > Report with defaults**.
- 2 In the ArcSight Console dialog box, click **Open** to view the report in a browser on screen, or click **Save** to save the report output to the default reports directory.

Vulnerability Queries

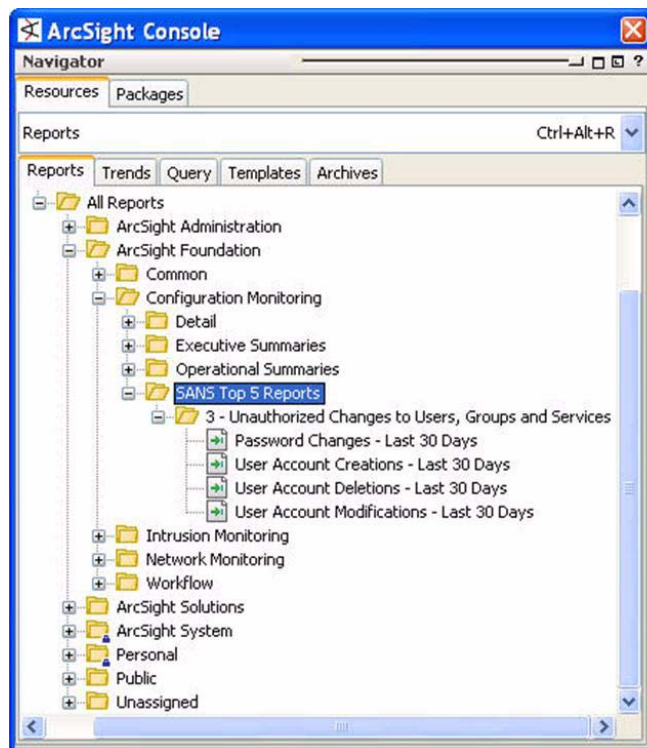
The vulnerability queries supply the conditions for the vulnerability reports.



The Vulnerability queries support the following reports and trends:



SANS Top 5 Reports for Configuration Monitoring



SANS Top 5 Reports:
These focused reports use several Detail reports to provide a SANS-relevant profile of unauthorized changes to users, groups, and services.

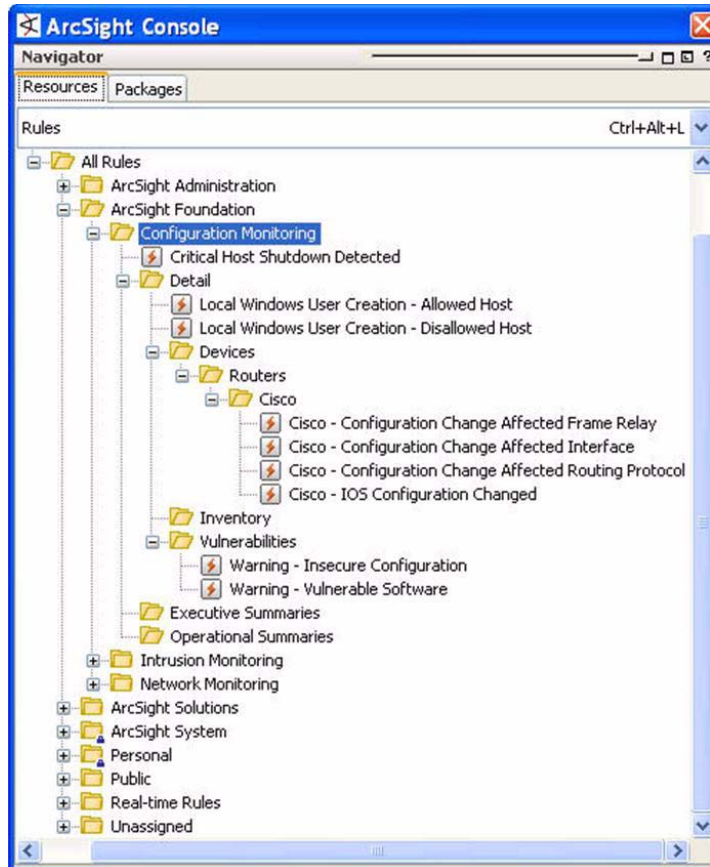
The SANS top 5 reports address SANS section 3, unauthorized access by users. The reports featured are focused reports derived corresponding parent reports in the Detail branch:

Report	Parent Report
Password changes - Last 30 Days	Password Changes
User Account Creations - Last 30 Days	Users Created - Last 30 Days
User Account Deletions - Last 30 Days	By User Account - Accounts Deleted
User Account Modifications - Last 30 Days	User Account Modifications - Last 30 Days

For instructions about how to create new focused reports that focus on other parameters or time frames, see [“To create a focused report that focuses on another time period:” on page 115.](#)

Configuration Monitoring Rules

The Configuration Monitoring rules detect a number of host-based conditions, such as when a user is created on allowed and disallowed hosts (listed in the *Local User Allowed Systems* active list), and Cisco router configuration changes. The vulnerability rules detect scan events that indicate that an insecure configuration exists on a software, host, or network device, such as a router.



Configuration Monitoring: The Critical Host Shutdown Detected rule supports the Asset Restarts reports in the Operational Summaries reports section.

Detail: These rules detect when a new local windows user is created. They reference the *Local User Allowed Systems* active list.

Devices: These rules detect configuration changes to your Cisco network infrastructure.

Vulnerabilities: These rules detect insecure configurations and vulnerable software.

These rules are described in more detail below:

Rule	Description
Critical Host Shutdown Detected	This rule detects when a host with high or very high criticality is shut down. This rule is a part of the Configuration Monitoring content.
Cisco - Configuration Change Affected Frame Relay	This rule detects when an IOS configuration change affected the frame relay. This rule looks for an IOS configuration change followed by a frame relay error, having both the same target IP and the same target zone resource. This rule only requires 1 such event, and the time frame is set to 1 minute. This rule will be triggered by events generated by CISCO NDC rules.

Rule	Description
Cisco - Configuration Change Affected Interface	This rule detects when a configuration change affected the interface. This rule looks for a configuration change followed by an interface change or a line state change that have both the same target IP and target zone resource. This rule only requires 1 such event, and the time frame is set to 1 minute. This rule will be triggered by events generated by CISCO NDC rules.
Cisco - Configuration Change Affected Routing Protocol	This rule detects when a configuration change affected the routing protocol. This rule looks for a configuration change followed by a routing protocol error that have both the same target IP and the same target zone resource. This rule only requires 1 such event, and the time frame is set to 1 minute. This rule will be triggered by events generated by CISCO NDC rules.
Cisco - IOS Configuration Changed	This rule detects an IOS configuration change. This rule looks for event names containing the string 'SYS-5-CONFIG'. This rule only requires 1 such event, and the time frame is set to 1 minute. After this rule is triggered, the "agentSeverity" event field will be set to medium. This rule will be triggered by events generated by CISCO routers.
Local Windows User Creation - Allowed Host	This rule detects the creation of a local user on a Windows system. If this rule triggers, the system on which the user has been created is present in the Local User Allowed Systems active list and this alert should be treated as normal activity. This rule is a part of the Configuration Monitoring content.
Local Windows User Creation - Disallowed Host	This rule detects the creation of a local user on a Windows system. If this rule triggers, the system on which the user has been created is not present in the Local User Allowed Systems active list and this alert should be treated as suspicious or hostile activity to be investigated immediately. This rule is a part of the Configuration Monitoring content.
Warning - Insecure Configuration	This rule looks for an insecure configuration of an object. The rule fires whenever an insecure object is found or a security check fails. On first event, a notification is sent to SOC operators.
Warning - Vulnerable Software	This rule looks for vulnerable software. The rule fires whenever a vulnerable application or operating system is found. The vulnerability should not be a scan vulnerability. On first event, a notification is sent to SOC operators.

What's Next

The next chapter describes the Intrusion Monitoring foundation.

Intrusion Monitoring Foundation



The Intrusion Monitoring foundation is a coordinated set of resources whose focus is to identify hostile activity and take appropriate action.

This foundation provides statistics about intrusion-related activity, which can be used for incident investigation as well as routine monitoring and reporting. As with previous releases, the Intrusion Monitoring essential security monitoring functions make up the bulk of the ESM standard content.

The Intrusion Monitoring foundation targets generic intrusion types as well as specific types of attacks, such as worms, viruses, denial-of-service (DoS) attacks, and so on. This foundation also addresses several of the SANS top 20 list of vulnerable areas.

- [“Intrusion Monitoring Foundation Overview” on page 121](#)
- [“Configuration Summary” on page 125](#)
- [“Intrusion Monitoring Filters” on page 127](#)
- [“Intrusion Monitoring Active Channels” on page 150](#)
- [“Intrusion Monitoring Active Lists” on page 155](#)
- [“Intrusion Monitoring Dashboards and Data Monitors” on page 156](#)
- [“Intrusion Monitoring Rules” on page 177](#)
- [“Intrusion Monitoring Reports” on page 192](#)

Intrusion Monitoring Foundation Overview

The bulk of the Intrusion Monitoring foundation is presented in The Intrusion Monitoring foundation is grouped into the following major use cases. These use cases are presented for real-time monitoring through the Intrusion Monitoring dashboards. Comprehensive Intrusion Monitoring statistics are supplied by a large collection of reports and trends.

Anti-Virus

The Anti-Virus content uses resources from the Anti Virus package. The resources in the Anti Virus package include the Virus dashboard and its data monitors and some reports at the Operational Summary and Detail level.

The Virus dashboard shows virus activity using two moving average data monitors that track increases in virus activity either by zone or by host, and the Virus Activity event graph.

Some reports in the Anti Virus package are also shared with the Configuration Monitoring foundation.

Attack Monitoring

The Attack Monitoring group is divided into more specific use cases. Resources in these use cases compile statistics for various types of hostile activity.

Attack Rates

These resources focus on changes in attack activity by either service or target zone.

The reports are driven by moving average data monitors. The dashboards display the appropriate data monitors for a view of the areas (services and target zones), to assist in determining whether the network is being attacked in a general sense, or if the attacks focus on specific network areas.

The dashboard and data monitors are replicated under the group "By Customer" for MSSPs. These modified duplicates are disabled by default.

DoS

The Denial of Service resources use moving average data monitors and categorized events with the technique set to [/DoS](#) to help determine when a DoS is taking place. The data monitors highlight high-volume activity that could result in a DoS. The categorized events (mostly from IDSs) can show DoS events that do not require exceeding bandwidth or processing limitations.

SANS Top 20

The SANS Top 20 Vulnerabilities list provides the context for a series of e-mail and operating system rules that look for specific events that relate to the vulnerabilities. The Intrusion Monitoring SANS Top 20 reports show assets with these vulnerabilities that have been compromised.

ArcSight releases updates to this content whenever practical when new SANS vulnerability lists are available.

Attackers

The Attackers group focuses on information about the attacker, such as the attacker address, zone and port.

Attacker Counts

The Attacker Counts content provides statistics about attackers, such as reporting device, target host, target port, ArcSight priority, and so on. This content was also provided in previous versions of ArcSight ESM.

By Port or Protocol

The port or protocol content provides views of attackers by attacker port and, when available, by protocol.

Top and Bottom 10

The Top and Bottom 10 content provides statistics about the top and bottom 10 a view of attackers by way of top and bottom 10 lists. The bottom 10 lists can be useful for tracking the attackers who are trying to avoid detection by the low-and-slow method (low volume over a long period of time).

Business Impact Analysis/Business Roles

The business and data role asset categories, along with the classification asset category, provide the focus for the Business Impact Analysis content. This is primarily a group of active channels, dashboards with data monitors, and reports to show which business areas are showing up as victims of the most attack activity.

Environment State

The Environment State content shows activity that reflects the state of the overall network, and provides details about applications, operating systems and services.

Reconnaissance

The Reconnaissance use case expands on the ArcSight Core reconnaissance rules, and provides insight into the different types of reconnaissance directed at the network or parts of the network.

This content breaks down reconnaissance activity by type. Dashboards show what parts of the network are being scanned and how.

Regulated Systems

The Regulated Systems resources focus on events related to assets that have been categorized as one of the compliance requirement asset categories (HIPAA, Sarbanes-Oxley, FIPS-199, and so on).

Resource Access

The Resource Access content focuses on access events, broken down by resource types (database, e-mail, files, and so on) and tracks this access by user. The brute force resource activity is included here. There are session lists that track the duration of an access session by user, as well as tracking the duration of access sessions that were accessed after a brute force login attack.

Revenue Generating Systems

The Revenue Generating Systems content is a group of reports that focus on attacked or compromised systems that have been categorized with the Revenue Generation category under Business Impact Analysis/Business Roles.

Targets

The Target content provides statistics about targets in the Compromised, Scanned, and Hit lists generated by evaluations from the priority formula.

By Port or Protocol

The By Port or Protocol content provides views of targets by target port. The protocol information can often be derived by the port number.

Target Counts

The Target Counts content gives views of attackers from various perspectives: reporting device, the target host, the target port, the ArcSight priority, and so on.

Targets in Lists

The Targets in Lists content gives a view of targets that are in one or more of the ArcSight Core Priority Formula lists, which specify hit, scanned or compromised.

Top and Bottom 10

The Top and Bottom 10 content gives views of targets by way of top and bottom 10 lists. The bottom 10 lists can be useful for tracking the attackers who are trying to avoid detection by the low-and-slow method (low volume over a long period of time), gunning for a particular target.

User Accounts

The User Accounts content shows activity related to compromised user accounts and the activity associated with those accounts.

Vulnerability View

This use case addresses assets and their vulnerabilities, with an active channel that focuses on vulnerability scanner reports. This use case presents two major reports that are a variation on the list of assets and the list of vulnerabilities.

Running these reports can produce reams of output. Scanner reports (the source of the scanner events) are considered sensitive, so not every user of ArcSight should have access to these resources. See [“Restrict Access to Vulnerability View Reports” on page 125](#) for tips about how to restrict access to these resources.

Worm Outbreak

The Worm Outbreak use case uses a collection of data monitors and rules to display worm activity and generate reports showing the affect a worm has had on the network.

User-Relevant Views

As with the other foundation packages, the Intrusion Monitoring content is presented in the following groups, according to how much a user audience needs to know:

- **Detail:** provides granular detail for operations center personnel who need to investigate incident activity.
- **Executive:** high-level summaries to provide system status information to management-level users.
- **Operational Summary:** medium-level summaries for operations personnel to use for daily monitoring and reporting.

Supported Devices

The Intrusion Monitoring content works primarily on feeds from the following security application devices.

- Network and host-based Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- Anti-virus

Connectors sending operating system or application log information (such as for user management devices) contribute details to the network's security posture. Information from other devices, such as network routing devices, VPN, and network management devices, can clarify or give further insight into the conditions surrounding an interesting event.

Configuration Summary

The Intrusion Monitoring foundation itself does not contain any resources that require configuration, although there are some optional resource customizations that will improve the quality of analysis. The Intrusion Monitoring foundation also relies on the following system-level configurations being made:

- Verify that the active list Trusted List set up to support priority formula calculations. For details, see [“Configure Active Lists” on page 41](#).
- Have vulnerability scanner running regularly.
- Categorize assets for business role, data role, criticality, and any application that you are interested in tracking. Major services, such as OS and application, will be filled in by the scanner. If it's not, then configure this manually.

Restrict Access to Vulnerability View Reports

The Vulnerability View detail reports (described in [“Vulnerability View Detail Reports” on page 208](#)) display a list of vulnerabilities generated by scanner report events, and are thus 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.

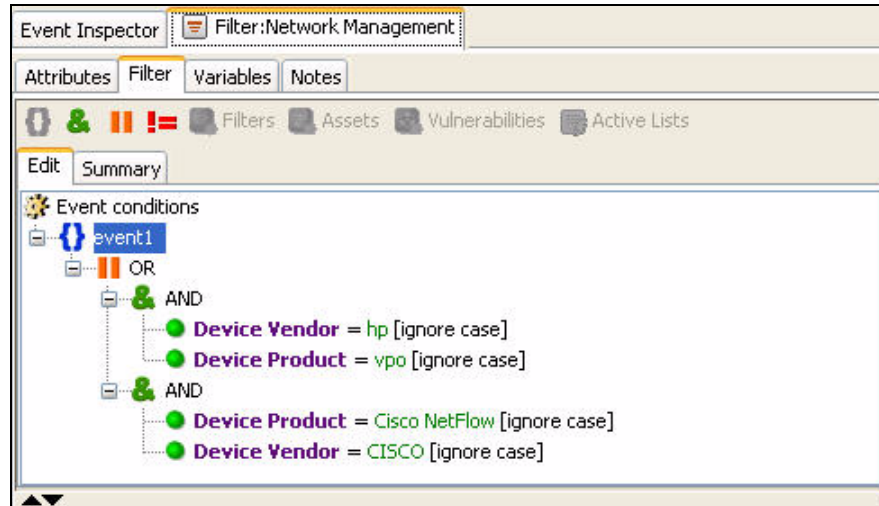
A fair amount of effort is required to eliminate these events from view without creating a special filter and applying it to the appropriate users groups. Before deciding whether to restrict access to the Vulnerability View reports, be aware of the following:

- Since 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**).

Configure Network Management Filter

The Network Management filter ([/All Filters/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Network Management](#)) identifies events from two network management devices: HP VPO, and Cisco NetFlow. If you use a network management device other than these, modify this filter with the Device Vendor and Device

Product name of the device you use. The example below shows the default conditions in the Network Management filter.

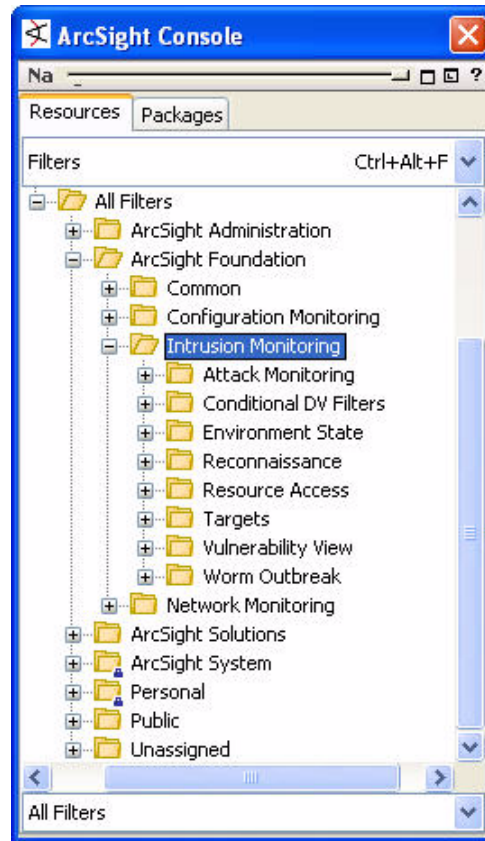


You can add to these conditions, or remove the existing ones, and create new ones.

This filter is required by the Event Counts by Hour data monitor ([/All Data Monitors/ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/Event Counts by Hour](#)).

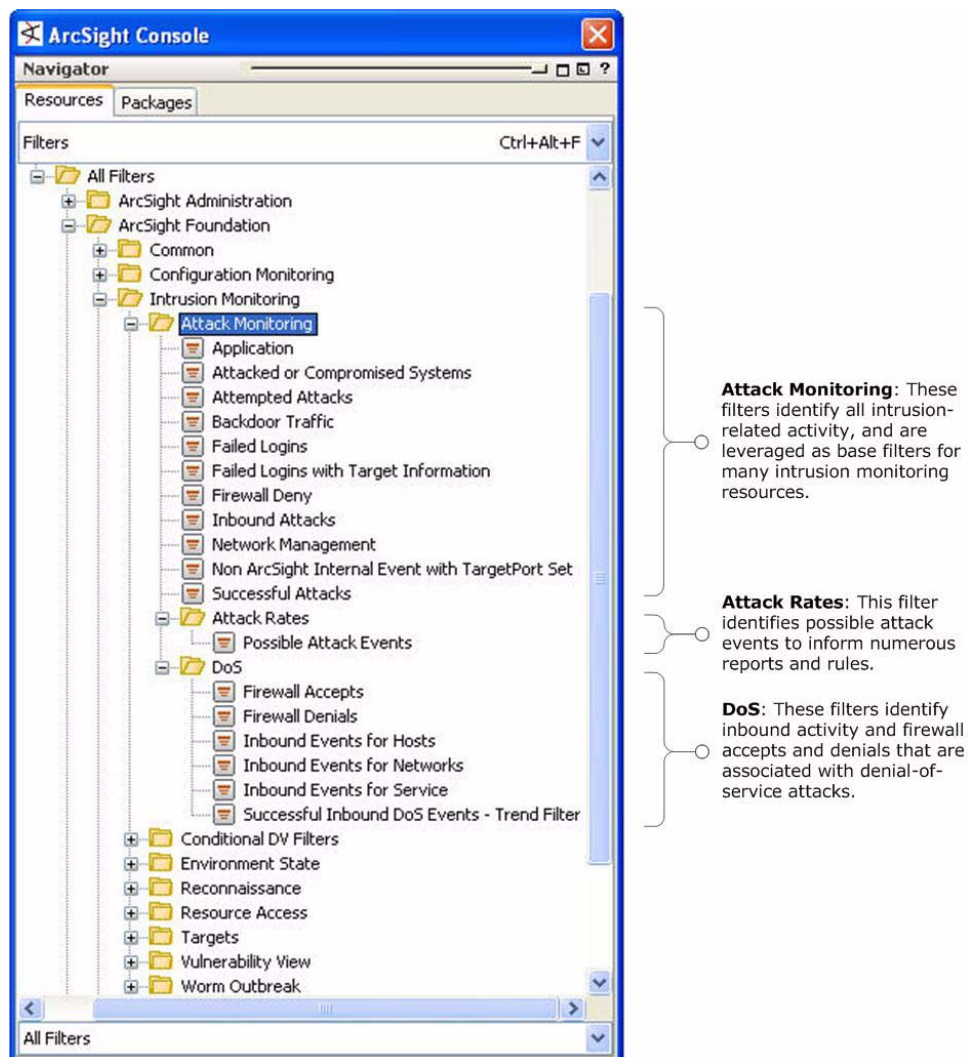
Intrusion Monitoring Filters

The Intrusion Monitoring filters express conditions that are used by the other Intrusion Monitoring and reporting resources.



Attack Monitoring Filters

The Attack Monitoring filters are divided into more specific use cases. Resources in these use cases compile statistics for various types of hostile activity.



These filters are described in more detail below.

Filter	Description
Attacked or Compromised Systems	This filter passes events that have one of the following names: Compromise - Success Compromise - Attempt Hostile - Success Hostile - Attempt These events are generated by the rules of that name for use in the Attacked or Compromised Systems data monitor.
Inbound Attacks	This filter passes events that have a significance of compromise or hostile and an outcome of success that are passing into the network.
Non ArcSight Internal Event with TargetPort Set	This filter passes events that have a Category Significance entry and a Target Port.

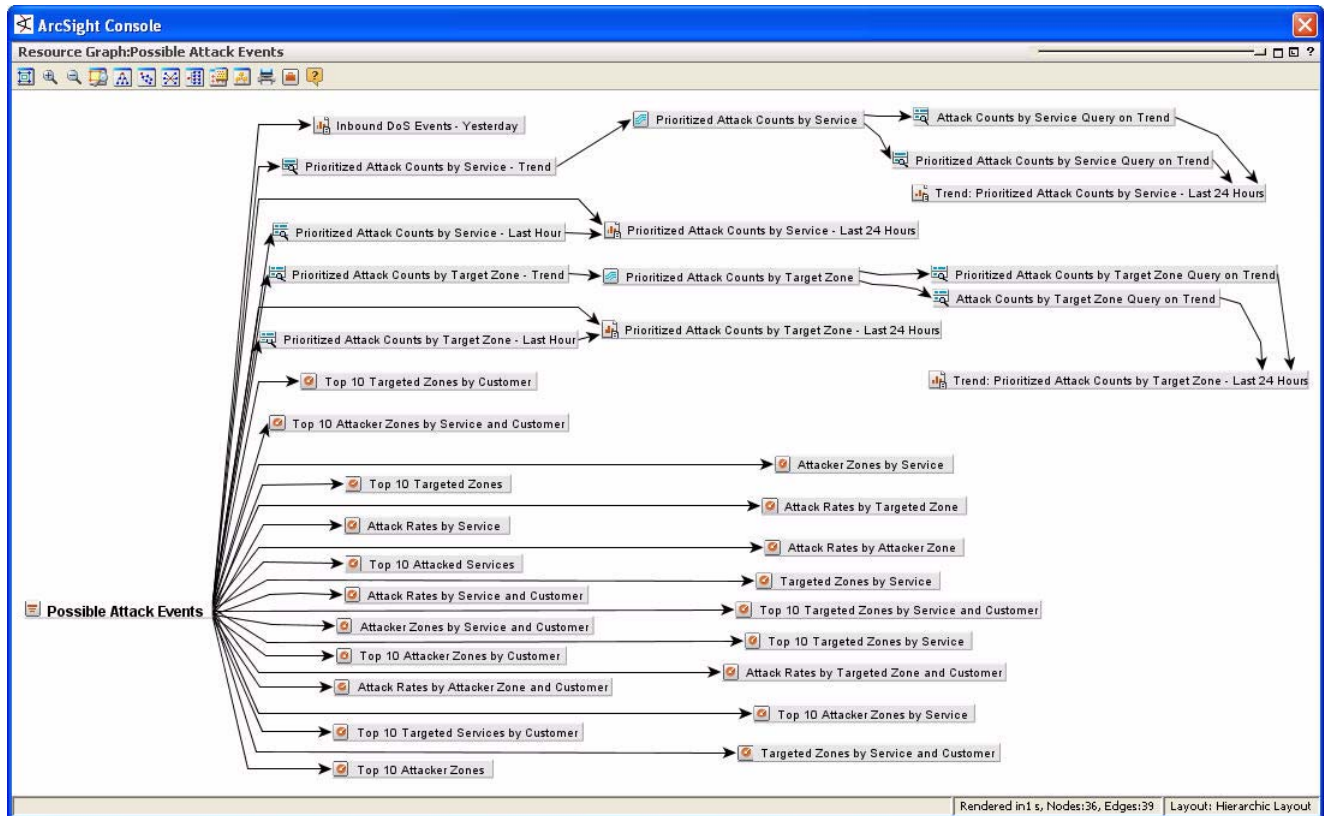
Filter	Description
Successful Attacks	This filter passes events that have a significance of compromise or hostile and an outcome of success.

Attack Rates Filter

The Attack Rates filter finds Compromise, Hostile, and Suspicious events for Intrusion Monitoring resources that provide attack rate statistics.

Filter	Description
Possible Attack Events	This filter passes events where the category significance is / Compromise, /Hostile or /Suspicious. Note that there is no restriction on whether the target is an internal or external system.

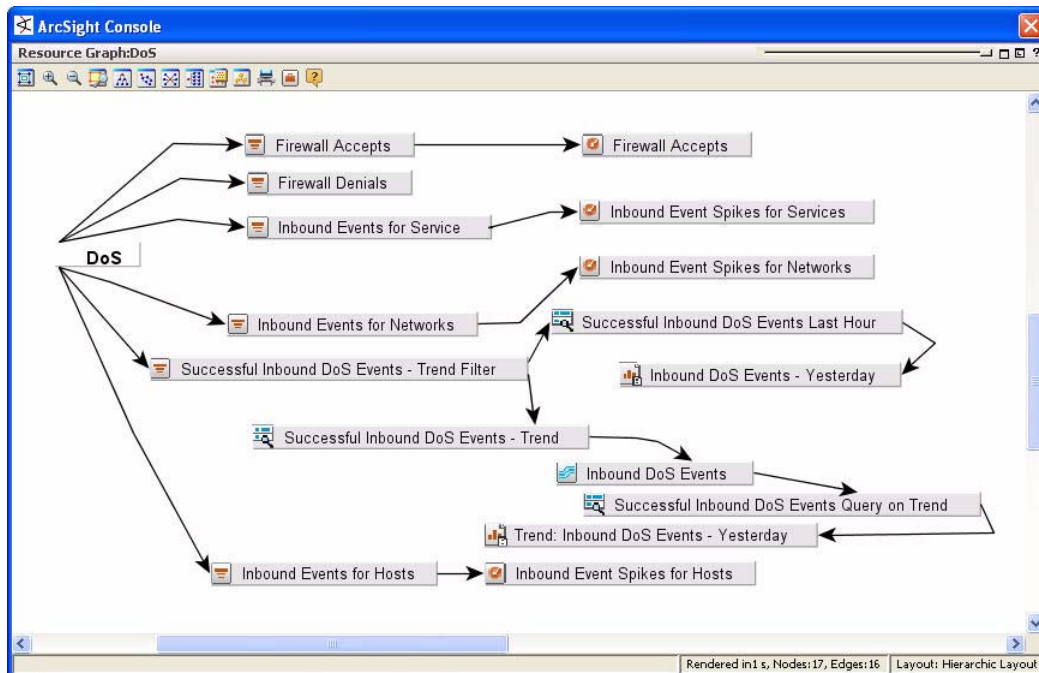
This filter supplies conditions for the following Intrusion Monitoring resources:



DoS Filters

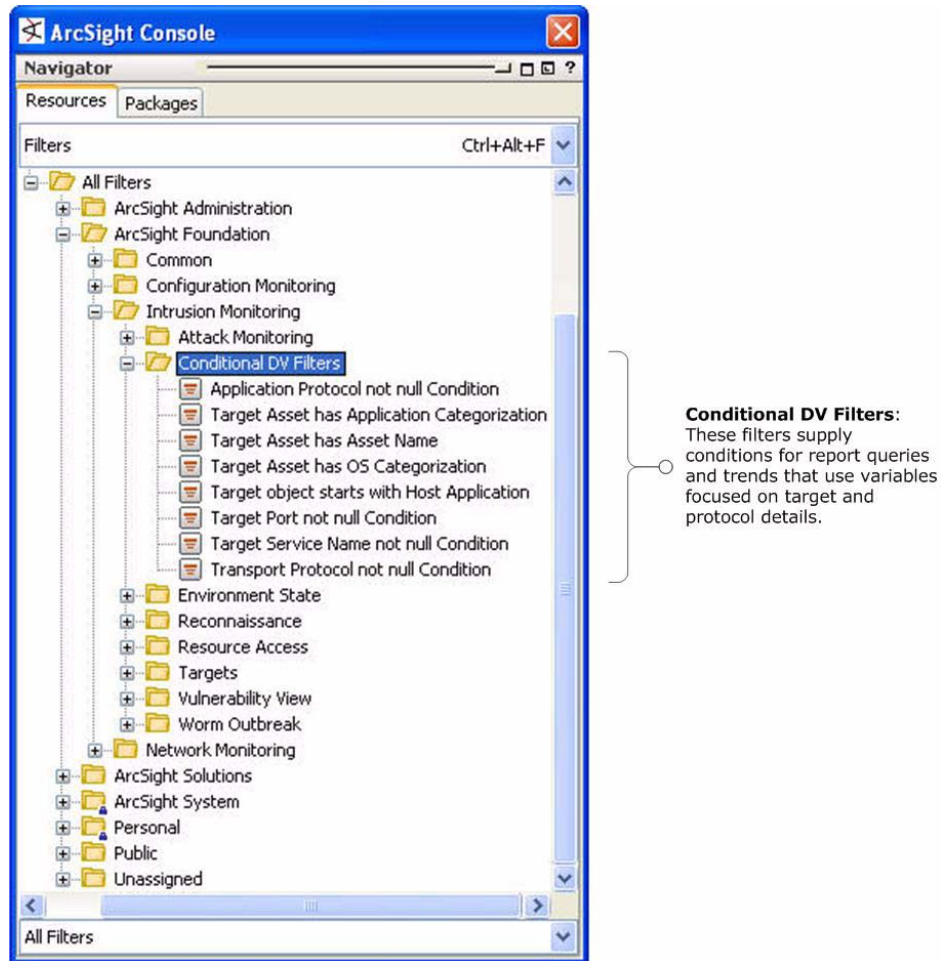
Filter	Description
Inbound Events for Hosts	This filter passes request or access events targeting internal hosts on the network as a whole, with the exception of trusted attackers (i.e., approved internal vulnerability scanners) and ArcSight administrative assets.
Inbound Events for Networks	This filter passes request or access events targeting the network as a whole, with the exception of trusted attackers (i.e., approved internal vulnerability scanners) and ArcSight administrative assets.
Inbound Events for Service	This filter passes request or access events targeting internal services, with the exception of trusted attackers (i.e., approved internal vulnerability scanners) and ArcSight administrative assets.
Successful Inbound DoS Events - Trend Filter	This filter passes events that are related to successful Denial of Service attacks on internal targets, with the exception of trusted attackers (i.e., approved internal vulnerability scanners). This filter is used to select events by a query for a trend on Denial of Service attacks affecting the network, but can also be used for filtering events for a standard event report (not a trend report).

The DoS filters provide conditions for the following Intrusion Monitoring rules and report queries and trends:



Conditional Variable Filters

The Conditional Variable Filters supply conditions for report queries and trends that focus on details about targets and application and transport protocols.

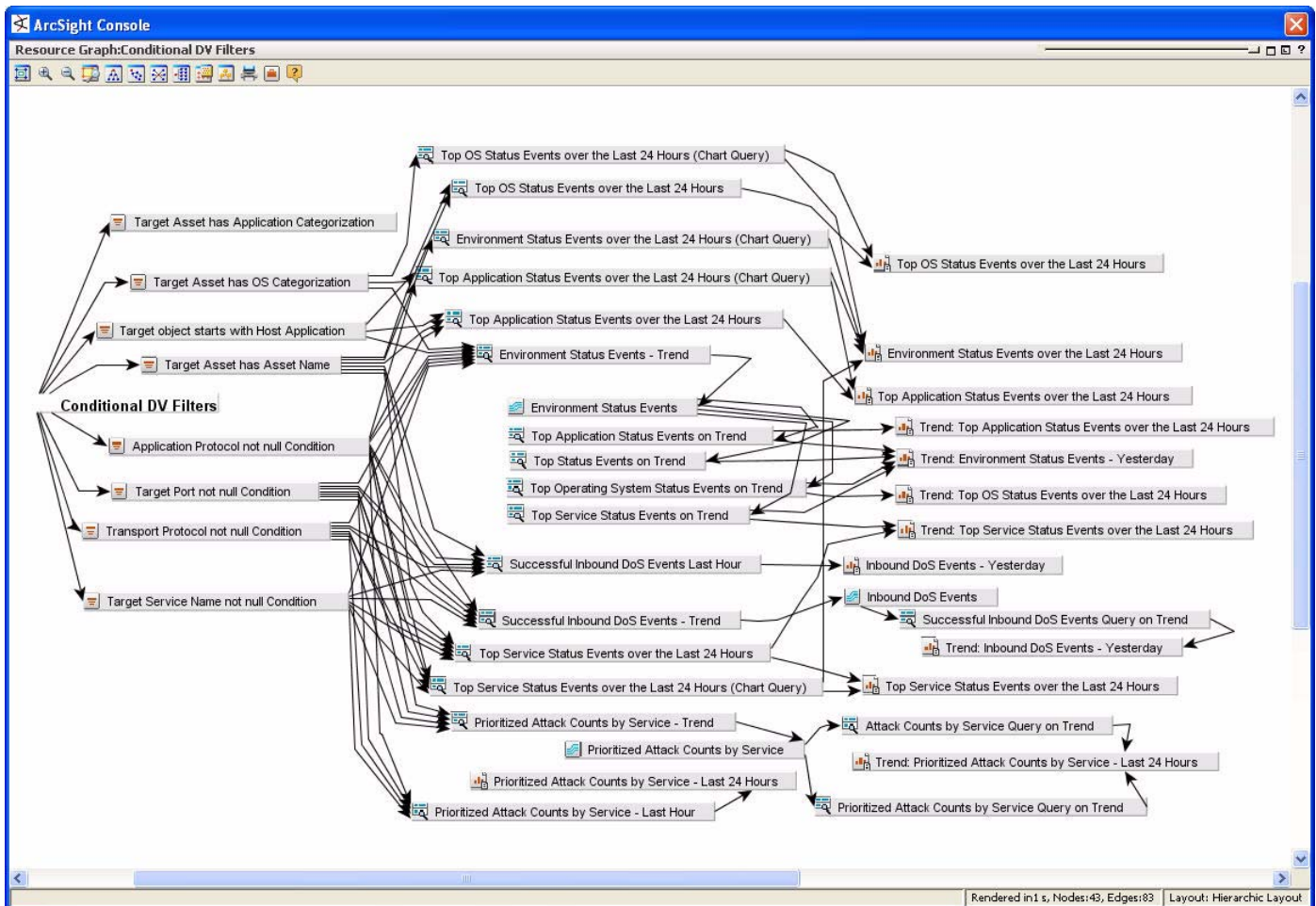


The Conditional Variable filters are described in more detail below:

Filter	Description
Application Protocol not null Condition	This filter is used by some of the query dependent variables to determine whether an event has an entry for the Application Protocol field.
Target Asset has Application Categorization	This filter is used by some of the query dependent variables to determine whether the target of an event has an Asset Category within /Site Asset Categories/Application.
Target Asset has Asset Name	This filter is used by some of the query dependent variables to determine whether an event has an entry for the Target Asset Name field.
Target Asset has OS Categorization	This filter is used by some of the query dependent variables to determine whether the target of an event has an Asset Category within /Site Asset Categories/Operating System.

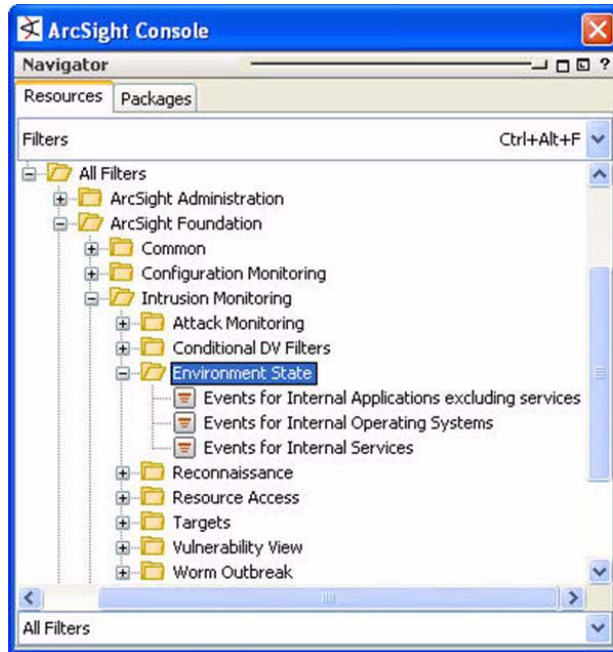
Filter	Description
Target Port not null Condition	This filter is used by some of the query dependent variables to determine whether an event has an entry for the Target Port field.
Target Service Name not null Condition	This filter is used by some of the query dependent variables to determine whether an event has an entry for the Target Service Name field.
Target object starts with Host Application	This filter is used by some of the query dependent variables to determine whether an event is a Category Object within /Host/ Application.
Transport Protocol not null Condition	This filter is used by some of the query dependent variables to determine whether an event has an entry for the Transport Protocol field.

The Conditional Variable filters supply conditions to the following Intrusion Monitoring report queries and trends.



Environment State Filters

The Environment State filters express conditions for resources that report the intrusion status of applications, operating systems and services.

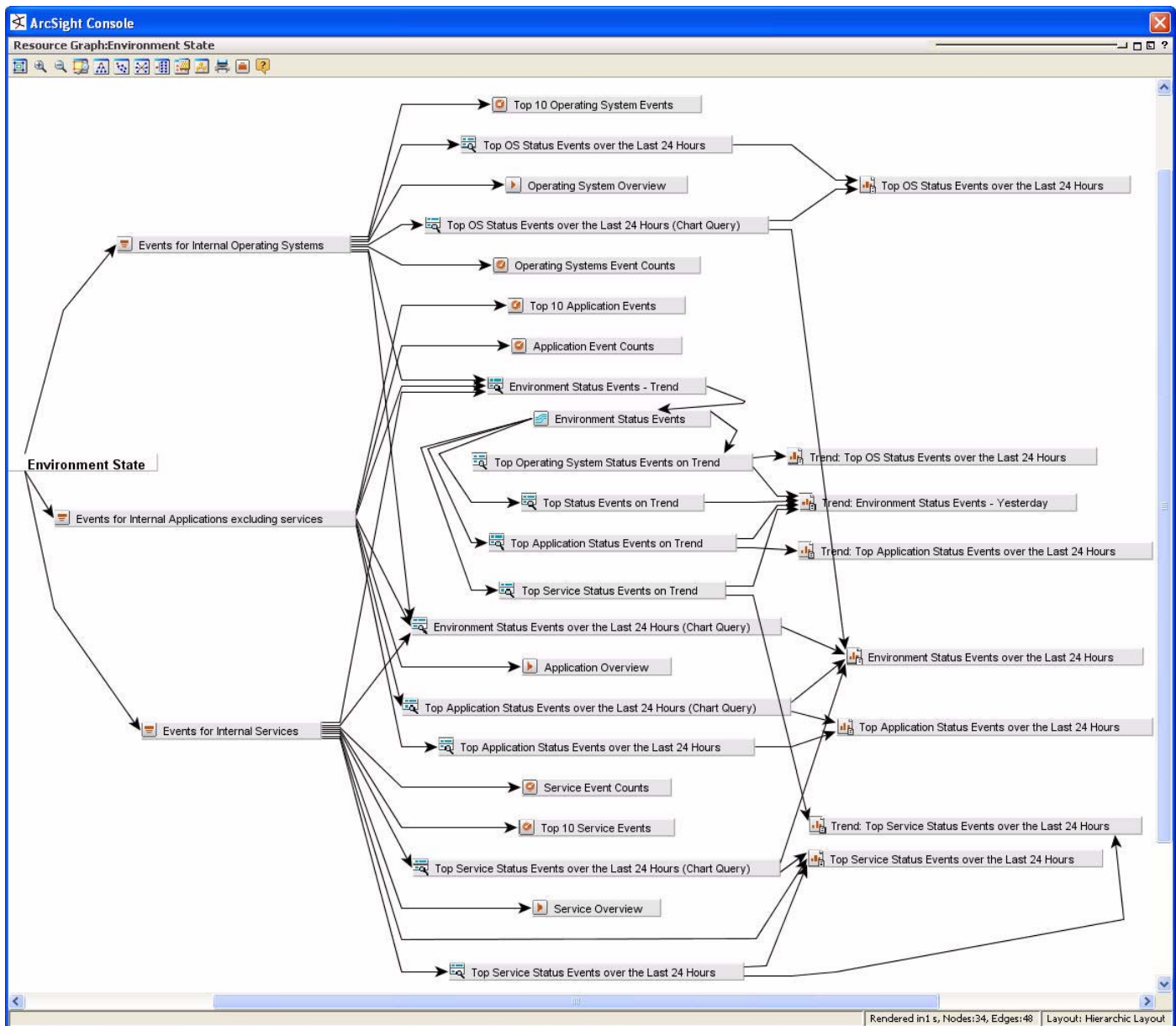


Environment State: These filters supply conditions for resources that report the intrusion status of systems on the network.

These filters are described in more detail below.

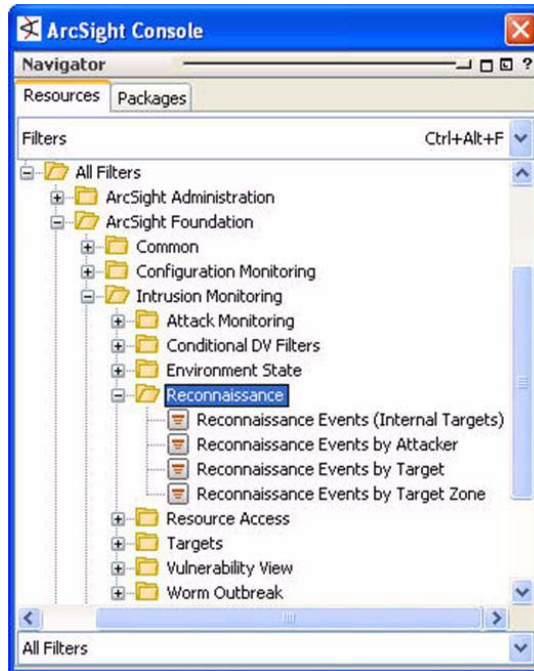
Filter	Description
Events for Internal Applications excluding services	This filter passes events that are not ArcSight internal events and that are related to an internal destination. The events are further limited to being in the Category Device Group /Application or being a Category Object of /Host/Application, but not a Category Object of /Host/Application/Service.
Events for Internal Operating Systems	This filter passes events that are not ArcSight internal events and that are related to an internal destination. The events are further limited to being in the Category Device Group /Operating System or being a Category Object of /Host/Operating System.
Events for Internal Services	This filter passes events that are not ArcSight internal events and that are related to an internal destination. The events are further limited to having a port set or being a Category Object of /Host/Application/Service.

The Environment State filters provide conditions for the following Intrusion Monitoring resources:



Reconnaissance Filters

The Reconnaissance filters provide conditions for the ArcSight Core reconnaissance rules, and Intrusion Monitoring resources that detect reconnaissance activity directed at the network.

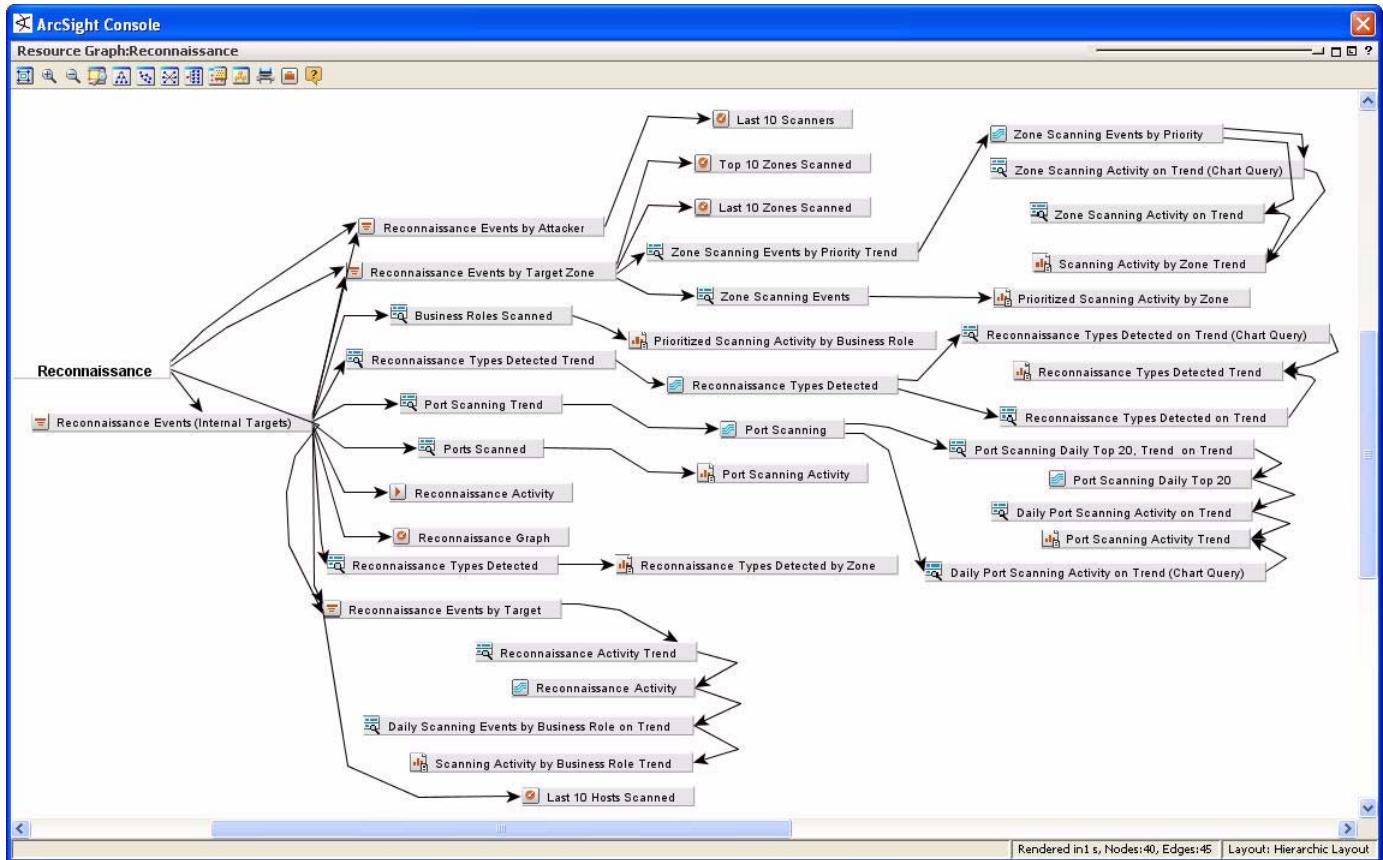


Reconnaissance: These filters supply conditions for resources that report on reconnaissance activity of systems on the network.

The Reconnaissance filters are described in more detail below.

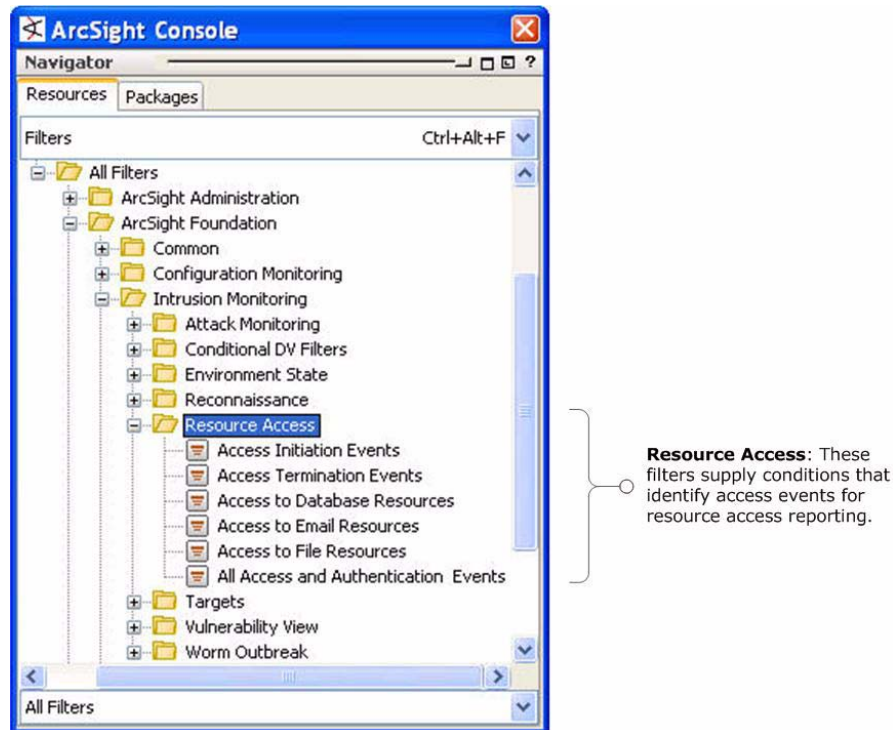
Filter	Description
Reconnaissance Events (Internal Targets)	This filter selects events that match the ".../Boundary Filters/Internal Target," ".../Event Types/Not Correlated and Not Closed and Not Hidden," and ".../Event Types/Non-ArcSight Internal Events" filters and one or more conditions where the event name starts with Reconnaissance, the category significance is /Recon or the category technique starts with /Scan. This is the foundation filter for the other Reconnaissance filters, Reconnaissance Events by Attacker, Reconnaissance Events by Target and Reconnaissance Events by Target Zone.
Reconnaissance Events by Attacker	This filter matches events where the attacker address is provided and the event matches the Reconnaissance Events (Internal Targets) filter.
Reconnaissance Events by Target	This filter matches events where the target address is provided and the event matches the Reconnaissance Events (Internal Targets) filter.
Reconnaissance Events by Target Zone	This filter matches events where the target zone is provided and the event matches the Reconnaissance Events (Internal Targets) filter.

The Reconnaissance filters supply conditions for the following Intrusion Monitoring resources:



Resource Access Filters

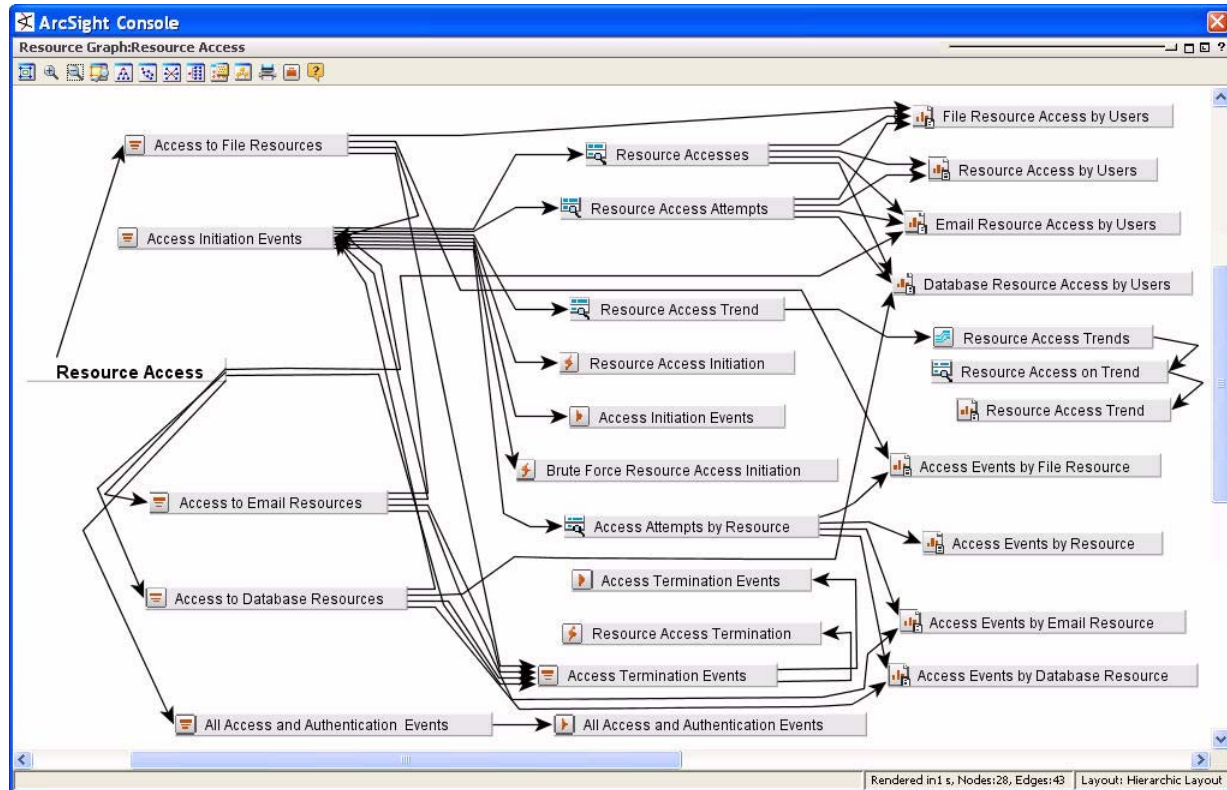
The Resource Access filters express conditions to find access events to inform resources that report on access events, broken down by major device type.



The Resource Access filters are described in more detail below.

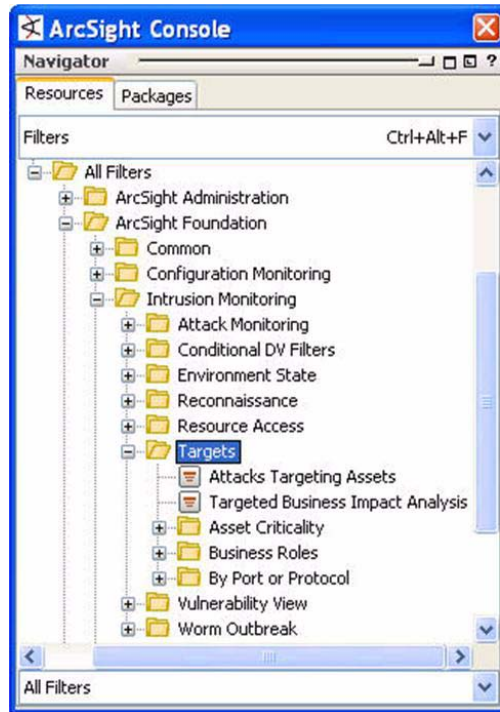
Filter	Description
Access Initiation Events	This filter selects events where the Category Behavior is one of: /Access/Start /Authentication/Verify /Authorization/Verify and the event also matches one of the filters: Access to Database Resources Access to Email Resources Access to File Resources
Access Termination Events	This filter selects events where the Category Behavior is /Access/Stop, and the event also matches one of the filters: Access to Database Resources Access to Email Resources Access to File Resources
Access to Database Resources	This filter select events where the Category Object is /Host/Application/Database. It is designed to focus on specific events selected by the Access Initiation Events filter.
Access to Email Resources	This filter select events where the Category Object is /Host/Application/Service/Email. It is designed to focus on specific events selected by the Access Initiation Events filter.
Access to File Resources	This filter select events where the Category Object is /Host/Resource/File. It is designed to focus on specific events selected by the Access Initiation Events filter.
All Access and Authentication Events	This filter selects events where the Category Behavior is one of: /Access, /Authentication, and the event also matches one of the filters: Access to Database Resources, Access to Email Resources, Access to File Resources

The Resource Access filters supply conditions for the following Intrusion Monitoring resources:



Targets Filters

The Target filters express conditions that focus on targets in the Compromised, Scanned, and Hit lists generated by evaluations from the priority formula.

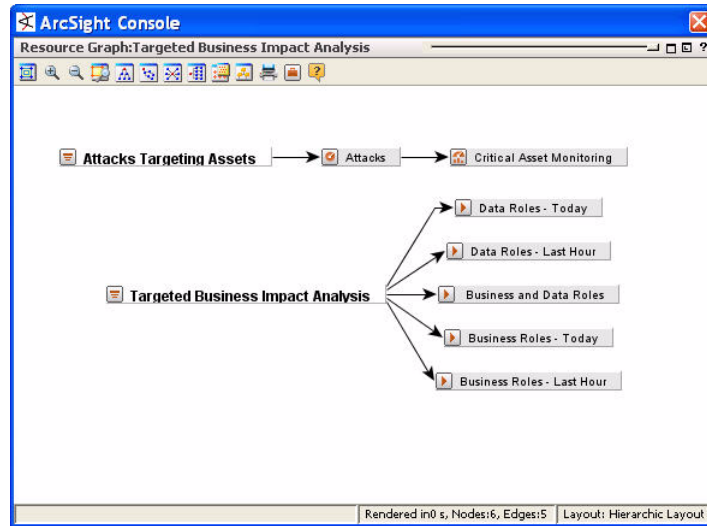


Targets: The top-level filters supply conditions for the Business Impact Analysis active channels and the Target/Critical Asset Monitoring dashboard and data monitor in the detail view.

The Targets filters are described in more detail below.

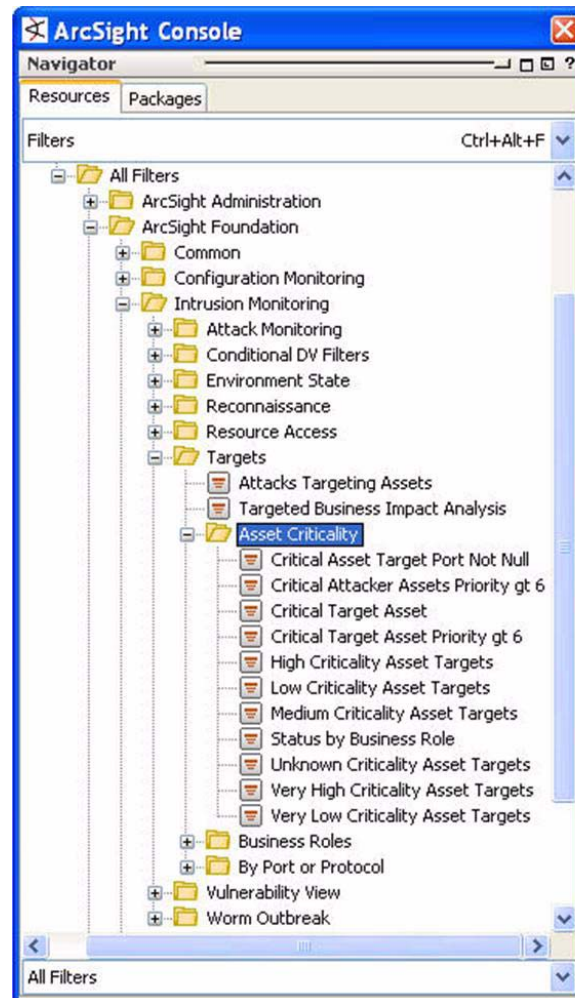
Filter	Description
Targeted Business Impact Analysis	This filter passes hostile & compromise events relating to target assets within the Business Role, Data Role or Classification categories. The events match: - Non-ArcSight Internal Event - Target asset has a Business Impact Analysis Category - Priority > 5 - Category Significance StartsWith /Compromise or /Hostile. The Business Role, Data Role and Classification categories are sub-categories of /All Asset Categories/Site Asset Categories/Business Impact Analysis.

The top-level Targets filters supply conditions for the following Intrusion Monitoring dashboards and active channels:



Asset Criticality Filters

The Asset Criticality filters leverage the asset categories set for the devices reporting to ESM. For these filters to work, your assets should be categorized in the relevant asset categories.



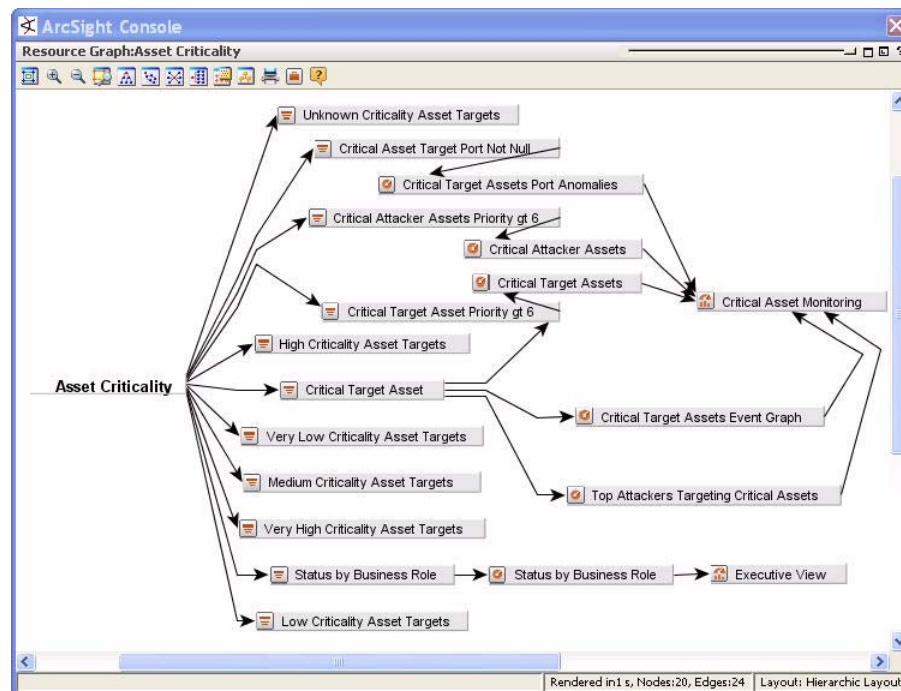
Asset Criticality: These filters supply conditions for events that relate to asset criticality levels set for the devices reporting to ESM.

The Asset Criticality filters are described in more detail below.

Filter	Description
High Criticality Asset Targets	This filter selects Target Asset IDs that are in the System Asset Categories/Criticality/High Criticality Asset list.
Low Criticality Asset Targets	This filter selects Target Asset IDs that are in the System Asset Categories/Criticality/Low Criticality Asset list.
Medium Criticality Asset Targets	This filter selects Target Asset IDs that are in the System Asset Categories/Criticality/Medium Criticality Asset list.
Unknown Criticality Asset Targets	This filter selects Target Asset IDs that have no associated asset category within the System Asset Categories/Criticality asset category hierarchy.
Very High Criticality Asset Targets	This filter selects Target Asset IDs that are in the System Asset Categories/Criticality/Very High Criticality Asset list.

Filter	Description
Very Low Criticality Asset Targets	This filter selects Target Asset IDs that are in the System Asset Categories/Criticality/Very Low Criticality Asset list.
Status by Business Role	This filter selects events with the names Compromise/Attempt, Compromise/Success, Hostile/Attempt or Hostile/Success with Target Asset IDs that are associated with the Site Asset Categories/Business Impact Analysis/Business Role asset category hierarchy.

The Asset Criticality filters supply conditions for the following Intrusion Monitoring resources:

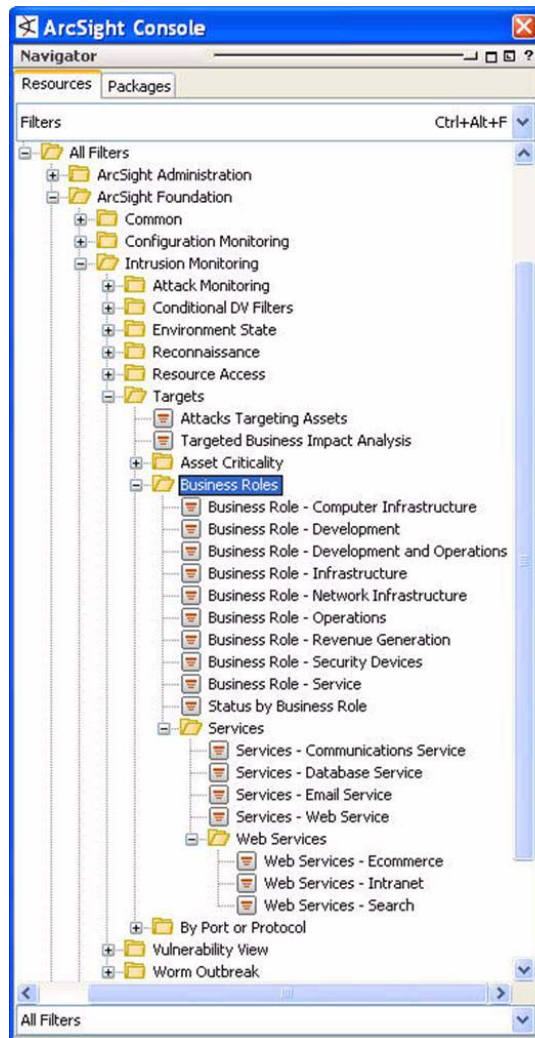


Business Roles Filters

The Business Roles filters supply conditions for the Executive and Detail view Targets dashboards and data monitors.



For these filters to work, your assets must be categorized in the business role, services, and/or web services asset categories. These filters will remain dormant if your assets are not categorized in these asset categories.



Business Roles: These filters supply conditions that identify the business role represented in an event.

Services: These filters supply conditions that identify the service represented in an event.

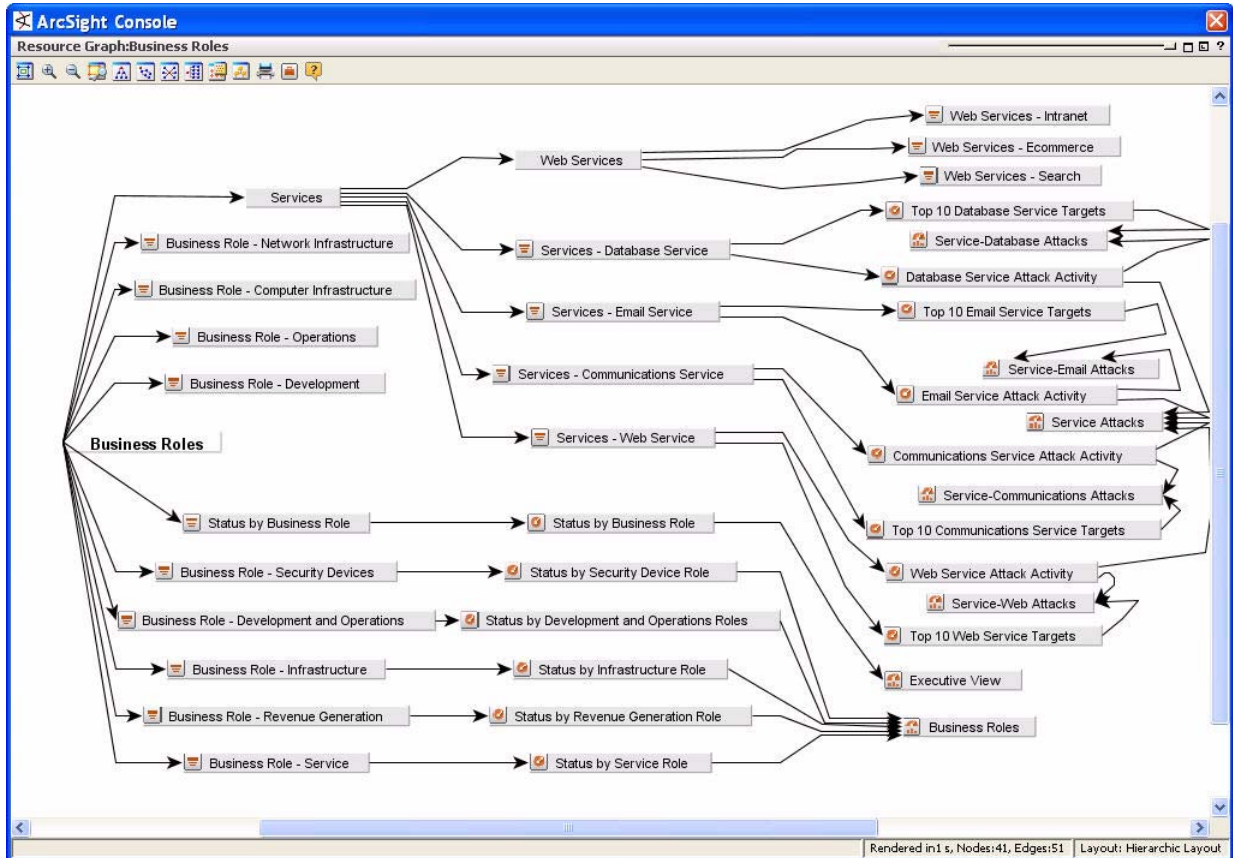
Web Services: These filters supply conditions to identify events that are web-services related.

The Business Roles filters are described in more detail below.

Filter	Description
Business Role - Computer Infrastructure	This filter selects Target Asset IDs that are in the Site Asset Categories/Business Impact Analysis/Business Role/Infrastructure/Computer Asset list.
Business Role - Development	This filter selects Target Asset IDs that are in the Site Asset Categories/Business Impact Analysis/Business Role/Development Asset list.

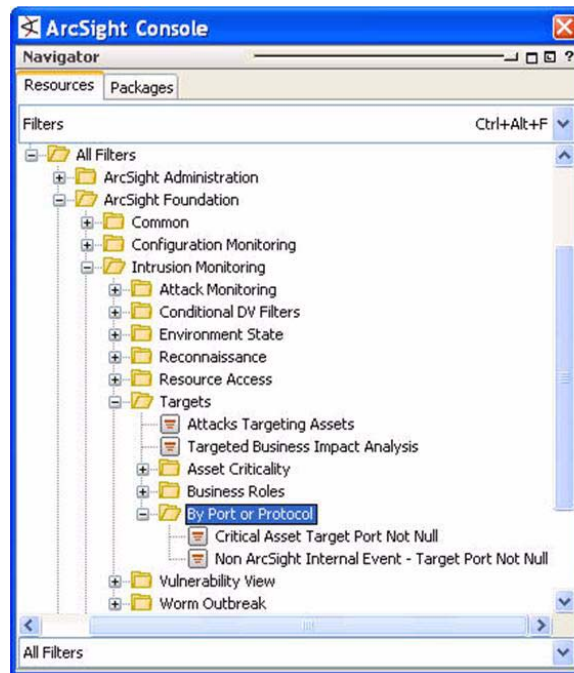
Filter	Description
Business Role - Development and Operations	This filter selects Target Asset IDs that are in the Site Asset Categories/Business Impact Analysis/Business Role/Development or the Site Asset Categories/Business Impact Analysis/Business Role/Operations Asset list.
Business Role - Infrastructure	This filter selects Target Asset IDs that have the Site Asset Categories/Business Impact Analysis/Business Role/Infrastructure/Computer or the Site Asset Categories/Business Impact Analysis/Business Role/Network Infrastructure asset categories associated with them.
Business Role - Network Infrastructure	This filter selects Target Asset IDs that are in the Site Asset Categories/Business Impact Analysis/Business Role/Network Infrastructure Asset list.
Business Role - Operations	This filter selects Target Asset IDs that are in the Site Asset Categories/Business Impact Analysis/Business Role/Operations Asset list.
Business Role - Revenue Generation	This filter selects Target Asset IDs that are in the Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation Asset list.
Business Role - Security Devices	This filter selects Target Asset IDs that are in the Site Asset Categories/Business Impact Analysis/Business Role/Security Devices Asset list.
Business Role - Service	This filter selects Target Asset IDs that are in the Site Asset Categories/Business Impact Analysis/Business Role/Service Asset list.

The Business Role filters supply conditions for the following Intrusion Monitoring dashboards and data monitors:



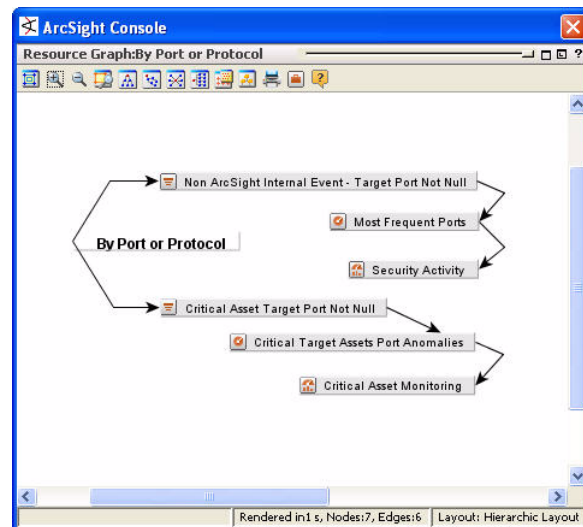
By Port or Protocol Filters

The port or protocol filters identify attackers by identifying target ports. These filters rely on the System/Event Type filters.



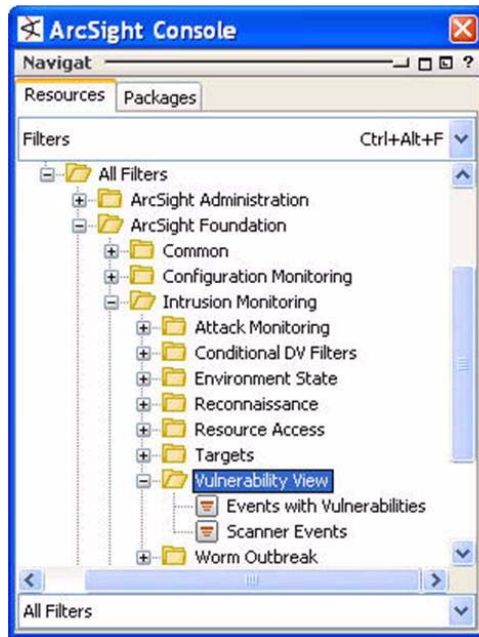
By Port or Protocol: These filters supply conditions that identify events by target port. These filters rely on System/Event Type filters.

The By Port or Protocol filters supply conditions for the following Intrusion Monitoring dashboards and data monitors:



Vulnerability View Filters

The Vulnerability View filters express conditions used by resources that focus on assets and their vulnerabilities.

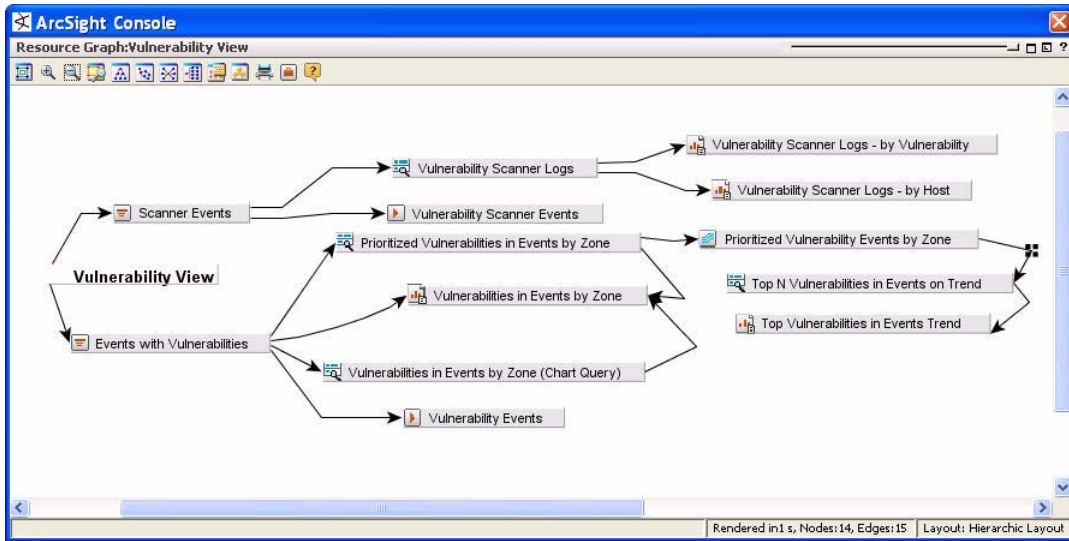


Vulnerability View: These filters supply conditions for vulnerability and scanner-related events that are consumed by vulnerability reports and active channels.

The Vulnerability View filters are described in more detail below.

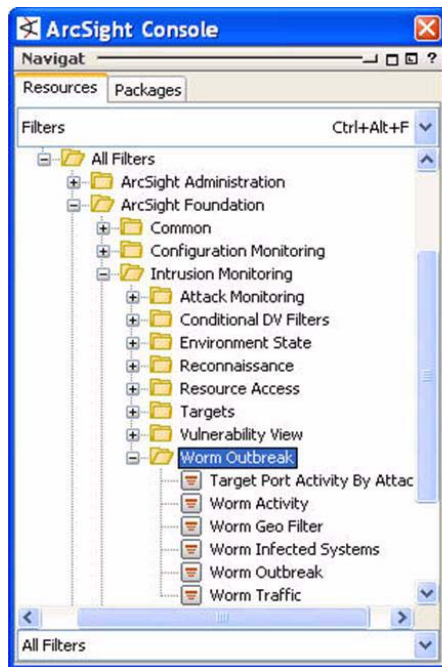
Filter	Description
Events with Vulnerabilities	This filter selects events where the vulnerability field has been populated. The vulnerability field is populated when an event that attempts to exploit the vulnerability targets an asset that has had that vulnerability reported by a security scanner.
Scanner Events	This filter selects events from network vulnerability scanners, where the events are defined as: Category Behavior = /Found/Vulnerable, Category Device Group = /Assessment Tools, Category Technique StartsWith /Scan, Category Technique Contains vulnerability. It is used by the Vulnerability Scanner Events active channel.

The Vulnerability View filters supply conditions for the following Intrusion Monitoring resources:



Worm Outbreak Filters

The Worm Outbreak filters express conditions that identify event activity consistent with worm activity for the worm outbreak resources.

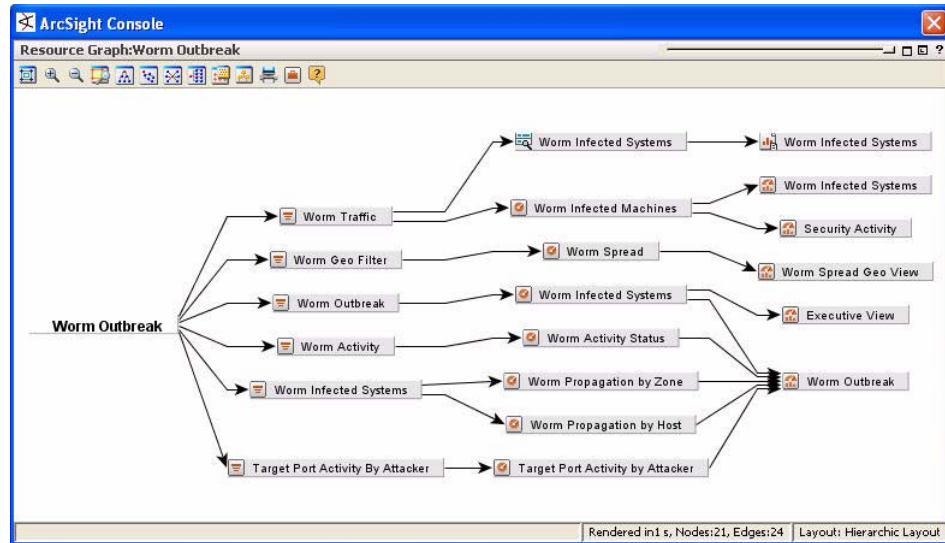


Worm Outbreak: These filters supply conditions that identify events associated with a worm outbreak.

The Worm Outbreak filters are described in more detail below.

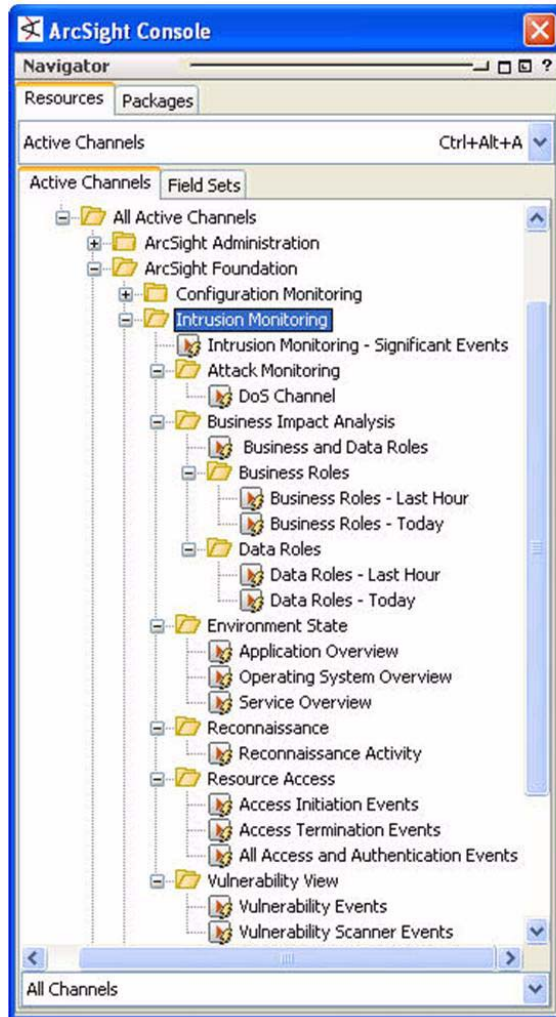
Filter	Description
Worm Geo Filter	The Worm Geo Filter is used by the Worm Spread data monitor in the Worm Spread Geo View dashboard to graph worm related events between systems on a world map. Worm related events are defined here as a category object of /Vector/Worm or /Host/Infection/Worm, or a category technique of /Code/Worm. For the event to be graphed, either the attacker or the target systems need to have their geographic longitudes and latitudes set (i.e., they must be NOT NULL).
Worm Outbreak	This filter only passes events with a name of Worm Outbreak Detected and the type Correlation.

The Worm Outbreak filters supply conditions for the following Intrusion Monitoring resources:



Intrusion Monitoring Active Channels

The Intrusion Monitoring active channels provide a series of live views



Intrusion Monitoring: This active channel shows intrusion-relevant events categorized as Hostile, Compromise, and Priority 8 or greater.

DoS Channel: This active channel shows DoS-relevant events targeting internal assets.

Business and Data Roles: This active channel shows Compromise and Hostile events relating to assets within the Business Role, Data Role or Classification asset categories.

Business Roles: These active channels show events that match the Targeted Business Impact Analysis filter for assets categorized with a Business Role.

Data Roles: These active channels show events that match the Targeted Business Impact Analysis filter for assets categorized with a Data Role.

Environment State: These active channels show application related events, non-ArcSight Internal events and events for internal applications excluding services.

Reconnaissance: This live active channel shows reconnaissance-related activity.

Resource Access: These live active channels show access and authentication-related activity.

Vulnerability View: These live active channels show vulnerability and scanner-related events.

The Intrusion Monitoring active channels are described in more detail below:

Active Channel	Description
Intrusion Monitoring - Significant Events	"Overview of hostile, compromise or high priority events. Continuously monitors events matching: - Not ArcSight Internal Events - Priority > 8 or Category Significance StartsWith /Compromise or /Hostile - Uses the Business Impact Analysis Field Set (End Time, Business Role, Data Role, Attacker Zone Name, Target Host Name, Category Significance, Category Outcome and Priority)."

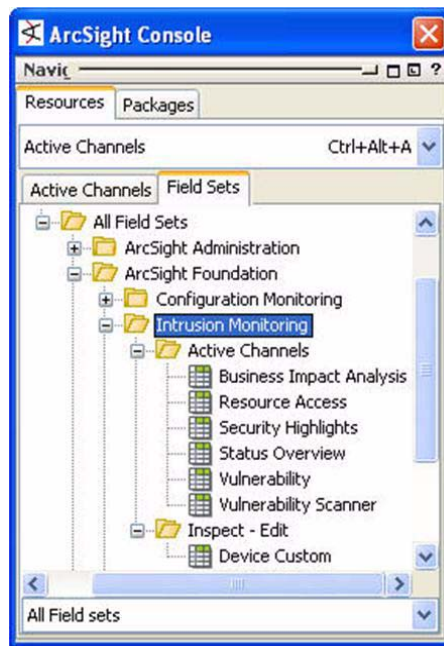
Active Channel	Description
DoS Channel	Live Channel showing events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data. - The channel uses its own filter to limit the view to Denial of Service related events where the Category Technique = /DoS, the Category Significance = /Compromise, the Category Outcome = /Success and the event MatchesFilter(Internal Target).
Business and Data Roles	Live Channel showing events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data, showing an overview of hostile & compromise events relating to assets within the Business Role, Data Role or Classification categories. The events match the Targeted Business Impact Analysis filter. - The Business Role, Data Role and Classification categories are sub-categories of /All Asset Categories/Site Asset Categories/Business Impact Analysis. - Uses the Business Impact Analysis Field Set (End Time, Business Role, Data Role, Attacker Zone Name, Target Host Name, Category Significance, Category Outcome and Priority).
Business Roles - Last Hour	Live Channel showing events received during the last hour. The channel includes a sliding window that always displays exactly the last hour of event data, showing events matching the Targeted Business Impact Analysis filter, with the further restriction that the target asset has a Business Role. - The Business Role category is a sub-category of /All Asset Categories/Site Asset Categories/Business Impact Analysis. - Uses the Business Impact Analysis Field Set (End Time, Business Role, Data Role, Attacker Zone Name, Target Host Name, Category Significance, Category Outcome and Priority). -
Business Roles - Today	Live Channel showing events received since midnight today. The channel includes a sliding window that always displays event data since midnight, showing events matching the Targeted Business Impact Analysis filter, with the further restriction that the target asset has a Business Role. - The Business Role category is a sub-category of /All Asset Categories/Site Asset Categories/Business Impact Analysis. - Uses the Business Impact Analysis Field Set (End Time, Business Role, Data Role, Attacker Zone Name, Target Host Name, Category Significance, Category Outcome and Priority). -
Data Roles - Last Hour	Live Channel showing events received during the last hour. The channel includes a sliding window that always displays exactly the last hour of event data, showing events matching the Targeted Business Impact Analysis filter, with the further restriction that the target asset has a Data Role. - The Data Role category is a sub-category of /All Asset Categories/Site Asset Categories/Business Impact Analysis. - Uses the Business Impact Analysis Field Set (End Time, Business Role, Data Role, Attacker Zone Name, Target Host Name, Category Significance, Category Outcome and Priority). -

Active Channel	Description
Data Roles - Today	Live Channel showing events received since midnight today. The channel includes a sliding window that always displays event data since midnight, showing events matching the Targeted Business Impact Analysis filter, with the further restriction that the target asset has a Data Role. - The Data Role category is a sub-category of /All Asset Categories/ Site Asset Categories/Business Impact Analysis. - Uses the Business Impact Analysis Field Set (End Time, Business Role, Data Role, Attacker Zone Name, Target Host Name, Category Significance, Category Outcome and Priority). -
Application Overview	Live Channel showing events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data. - The channel uses two filters to limit the view to application related events, Non-ArcSight Internal Events and Events for Internal Applications excluding services. For more information on the application related events, please see this latter filter.
Operating System Overview	Live Channel showing events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data. - The channel uses two filters to limit the view to operating system related events, Non-ArcSight Internal Events and Events for Internal Operating Systems. For more information on the service related events, please see this latter filter.
Service Overview	Live Channel showing events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data. - The channel uses two filters to limit the view to service related events, Non-ArcSight Internal Events and Events for Internal Services. For more information on the service related events, please see this latter filter.
Reconnaissance Activity	Live Channel showing reconnaissance events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data.
Access Initiation Events	Live Channel showing events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data. A selection of three filters restricts the events shown in the channel only to those related to access initiation, authentication verification or authorization verification for database, email and file resources.
Access Termination Events	Live Channel showing events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data. A selection of three filters restricts the events shown in the channel only to those related to access termination for database, email and file resources.
All Access and Authentication Events	Live Channel showing events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data. A selection of three filters restricts the events shown in the channel only to those related to access and authorization for any resource.

Active Channel	Description
Vulnerability Events	Live Channel showing events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data. A filter prevents the channel from showing events that contributed to the firing of a rule, commonly referred to as correlated events.
Vulnerability Scanner Events	This active channel shows the events selected by the Scanner Events filter over the last hour, using the Vulnerability Scanner field set, which shows the description of the scanner event, the zone and address of the asset for which the vulnerability is being reported, and the scanner information, vendor, product and scanning host, reporting the vulnerability for that asset.

Intrusion Monitoring Field Sets

Several field sets accompany Intrusion Monitoring to define relevant subsets of event fields for its active channels.



Active Channels: These field sets provide relevant subsets of event fields to facilitate monitoring and investigating intrusion-related events.

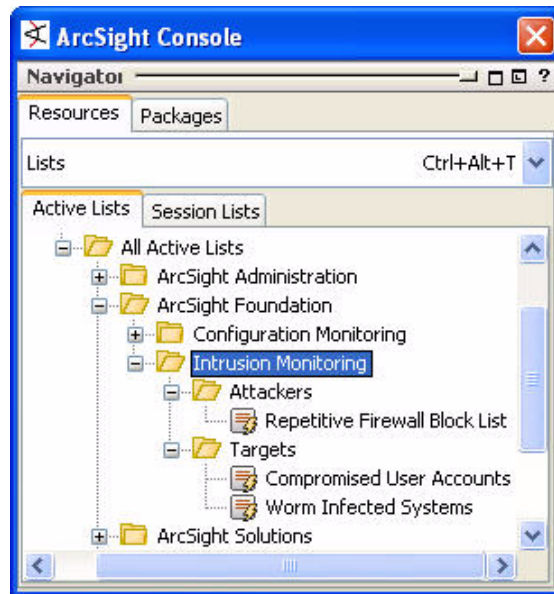
Inspect - Edit: The Device Custom field set presents fields that support events that contain custom fields for the conditions editor in the Inspect/Edit panel.

Field Set	Description
Business Impact Analysis	Field set including: - End Time - Business Role - Data Role - Attacker Zone Name - Target Host Name - Category Significance - Category Outcome - Priority

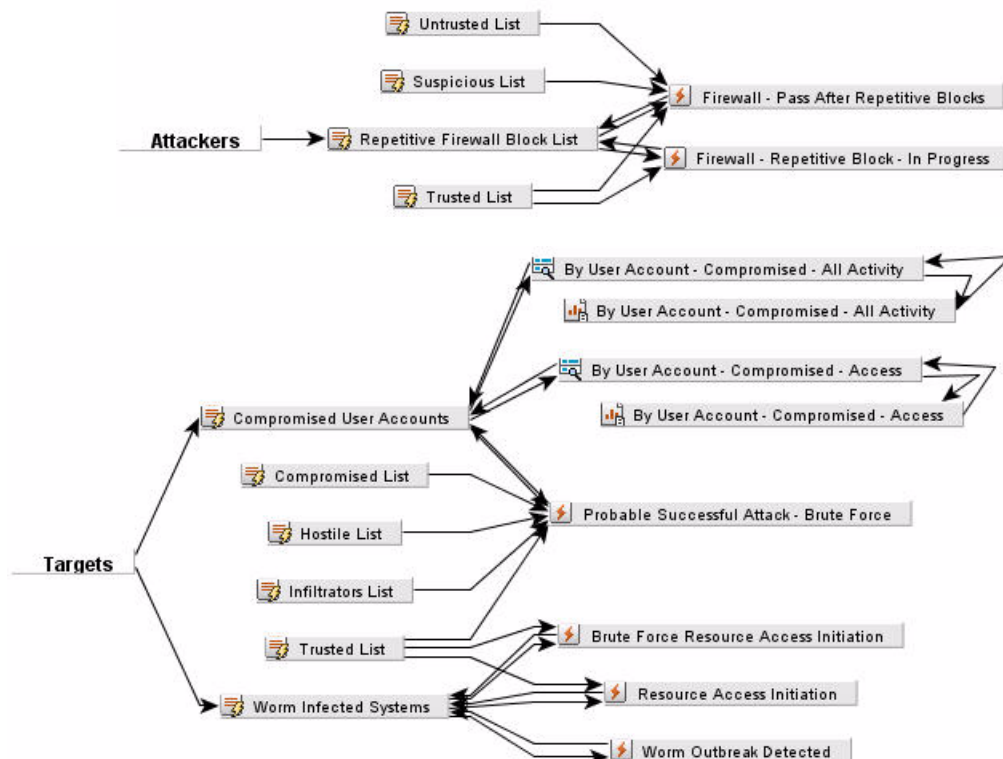
Field Set	Description
Resource Access	This field set is designed to show the fields of interest when monitoring resource access events. It includes the following fields: - End Time - Name - Resource Type * - User ID * - User Name * - Resource Zone Name * - Resource Address * - Device Vendor - Device Product - Access Outcome * - Priority - Agent Name - Attacker Zone Name - Attacker Address - * These fields are aliased by means of dependent variables, where: - Resource Type = Category Object - User ID = Target User ID - User Name = Target User Name - Resource Zone Name = Target Zone Name - Resource Address = Target Address - Access Outcome = Category Outcome
Security Highlights	This field set is a modification to the Security field set with the custom Event Name field replaced with the (sortable) Name field.
Status Overview	Field set including: - End Time - Name - Category Object - Category Device Group - Attacker Target - Priority - Device Vendor - Device Product
Vulnerability	This field set shows the following columns: - End Time - Name - Attacker Address - Target Address - Priority - Vulnerability Resource - Device Vendor - Device Product
Vulnerability Scanner	This field set shows the following columns: - End Time - Name - Target Zone Resource - Target Address - Priority - Device Vendor - Device Product - Device Host Name
Device Custom	Field set including: End Time - Name - Attacker Address - Target Host Name - Target Address - Target Port - Device Custom Date1 - Device Custom Date1 Label - Device Custom Date2 - Device Custom Date2 Label - Device Custom Number1 - Device Custom Number1 Label - Device Custom Number2 - Device Custom Number2 Label - Device Custom Number3 - Device Custom Number3 Label - Device Custom String1 - Device Custom String1 Label - Device Custom String2 - Device Custom String2 Label - Device Custom String3 - Device Custom String3 Label - Device Custom String4 - Device Custom String4 Label - Device Custom String5 - Device Custom String5 Label - Device Custom String6 - Device Custom String6 Label - Note: In an active channel, there will be a column for each field listed above. In the Event Inspector, the column header will display the text in the Label variation of the field name as part of the field name (e.g., Device Custom String1.labelname).

Intrusion Monitoring Active Lists

The Attackers and Targets active lists are dynamic active lists that are populated by rules that detect intrusion-relevant behavior. The contents of the lists are in turn read by other rules and reports.



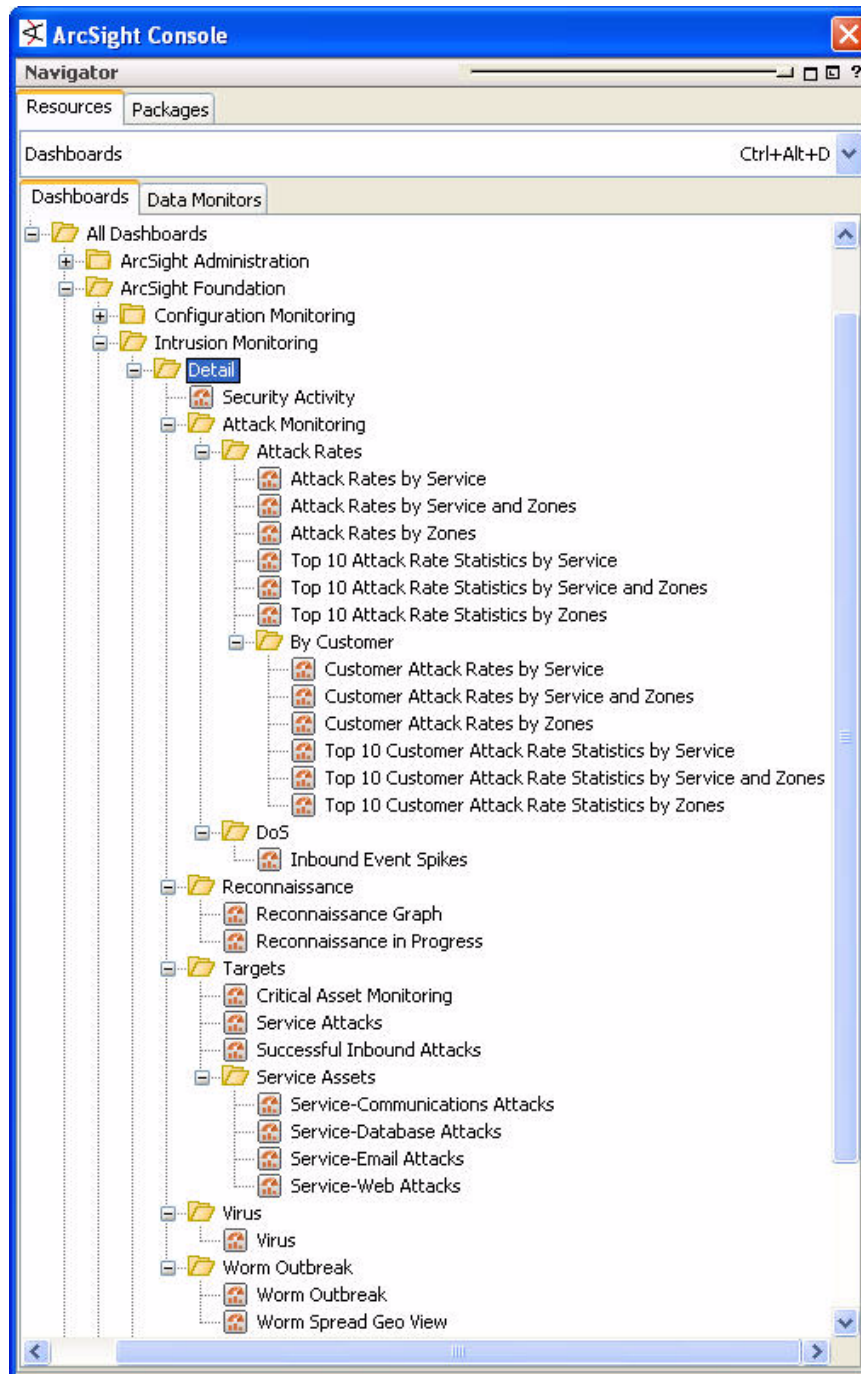
The Intrusion Monitoring active lists are written to and read by the following Intrusion Monitoring resources:



Intrusion Monitoring Dashboards and Data Monitors

Intrusion monitoring dashboards display real-time intrusion-related activity. They provide summarized views of activity across your network, and are intended to be used in daily operations and incident investigation.

Detail Dashboards



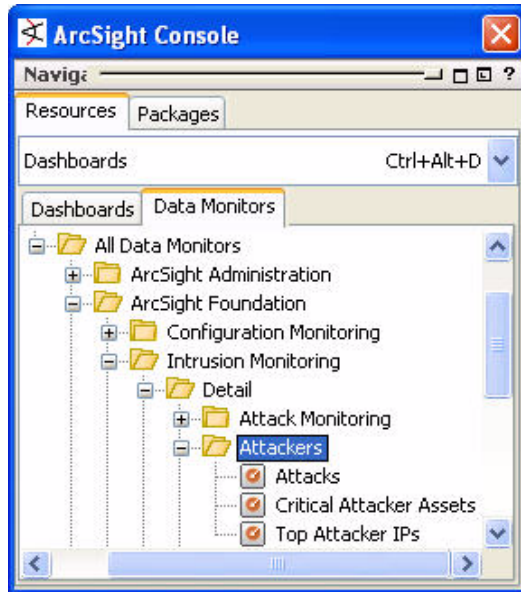
These dashboards are described in more detail below.

Dashboard	Description
Attack Rates by Service	This dashboard gives an overview of the attack rates by service. The three areas covered are the target service (defined as the service name and port), the target services broken down by target zones and the target services broken down by attacker zones.
Attack Rates by Service and Zones	This dashboard gives an overview of the attack rates by service. The three areas covered are the target service (defined as the service name and port), the target services broken down by target zones and the target services broken down by attacker zones.
Attack Rates by Zones	This dashboard gives a broad overview of the attack rates in two areas, target zones and attacker zones.
Top 10 Attack Rate Statistics by Service	This dashboard gives a top 10 view of the attack rates by service. The three areas covered are the target services (defined as the service name and port), the target services broken down by target zones and the target services broken down by attacker zones.
Top 10 Attack Rate Statistics by Service and Zones	This dashboard gives a top 10 view of the attack rates by service. The three areas covered are the target services (defined as the service name and port), the target services broken down by target zones and the target services broken down by attacker zones.
Top 10 Attack Rate Statistics by Zones	This dashboard gives a top 10 view of the attack rates in two areas, target zones and attacker zones.
Customer Attack Rates by Service	This dashboard gives an overview of the attack rates by service. The three areas covered are the target service (defined as the service name and port), the target services broken down by target zones and the target services broken down by attacker zones. Each of the areas is also broken down by customer.
Customer Attack Rates by Service and Zones	This dashboard gives an overview of the attack rates by service. The three areas covered are the target service (defined as the service name and port), the target services broken down by target zones and the target services broken down by attacker zones. Each of the areas is also broken down by customer.
Customer Attack Rates by Zones	This dashboard gives a broad overview of the attack rates in two areas, target zones and attacker zones. Each zone is also broken down by customer.
Top 10 Customer Attack Rate Statistics by Service	This dashboard gives a top 10 view of the attack rates by service. The three areas covered are the target services (defined as the service name and port), the target services broken down by target zones and the target services broken down by attacker zones. Each of the areas is also broken down by customer.
Top 10 Customer Attack Rate Statistics by Service and Zones	This dashboard gives a top 10 view of the attack rates by service. The three areas covered are the target services (defined as the service name and port), the target services broken down by target zones and the target services broken down by attacker zones. Each of the areas is also broken down by customer.

Dashboard	Description
Top 10 Customer Attack Rate Statistics by Zones	This dashboard gives a top 10 view of the attack rates in two areas, target zones and attacker zones. Each zone is also broken down by customer.
Inbound Event Spikes	This dashboard includes four moving average data monitors that measure event activity looking for suspicious spikes in activity. These data monitors create events that can be used to determine if a Denial of Service attack is starting. The data monitors cover activity reported by firewalls, activity related to the protected network, activity related to protected host and activity related to the services on the protected network.
Reconnaissance Graph	This dashboard displays the Reconnaissance Graph data monitor to provide operators and analysts a view into how reconnaissance events are probing the network.
Reconnaissance in Progress	This dashboard displays the Top 10 Zones Scanned, the last 10 Zones Scanned, the Last 10 Hosts Scanned and the Last 10 Scanners data monitors to give an overview of the reconnaissance activity against the network.
Service Attacks	This dashboard gives a overview on service attack activity for web, email, database and communications services. More detailed information is available from the follow-on dashboards in the Detail/ Targets/ Service Assets group: Service-Communications Attacks, Service-Database Attacks, Service-Email Attacks, Service-Web Attacks. This dashboard uses the following data monitors: Web Service Attack Activity, Email Service Attack Activity, Communications Service Attack Activity, Database Service Attack Activity.
Service-Communications Attacks	This dashboard gives a focused view on communications service attack activity. This dashboard uses the following data monitors: Top 10 Communications Service Targets, Communications Service Attack Activity.
Service-Database Attacks	This dashboard gives a focused view on database attack activity. This dashboard uses the following data monitors: Top 10 Database Service Targets, Database Service Attack Activity.
Service-Email Attacks	This dashboard gives a focused view on email attack activity. This dashboard uses the following data monitors: Top 10 Email Service Targets, Email Service Attack Activity.
Service-Web Attacks	This dashboard gives a focused view on web attack activity. This dashboard uses the following data monitors: Top 10 Web Service Targets, Web Service Attack Activity.
Virus	The Virus dashboard displays data monitors describing virus activity from three perspectives. The Virus Activity data monitor shows a graph view of the viruses, their relationships to the infected systems and the relationships of the infected systems to the network zones. The Virus Activity by Zone and Virus Activity by Host data monitors are moving average graphs grouping by the name of the virus, the target's zone resource and address and the customer resource. This dashboard uses the Virus Activity, Virus Activity by Zone and Virus Activity by Host data monitors.

Attackers Data Monitors

The Attackers data monitors define the views for the Attackers detail dashboards.



These data monitors are described in more detail below.

Data Monitor	Description
Attacks	Note: This Data Monitor will not work properly when running in Turbo Mode Fastest!
Critical Attacker Assets	Note: This Data Monitor will not work properly when running in Turbo Mode Fastest!

Attack Monitoring Data Monitors

The Attack Monitoring data monitors define the views for the Attack Monitoring dashboards.



By default, the data monitors in the By Customer group are disabled. If you have Customers (different cost centers) set up in your ESM environment, you can activate these data monitors to gather data on your different Customer cost centers. If you do not have Customers enabled, you can leave these data monitors disabled, so they do not use up system resources unnecessarily.

The attack monitoring data monitors are described in more detail below:

Data Monitor	Description
Attack Rates by Service	This moving average data monitor follows the possible attack counts for up to 20 target services (service here is defined as the transport protocol, service name and port), at five minute intervals over an hour. It will send alerts at no more than ten minute intervals, and refreshes its display every 30 seconds.
Attacker Zones by Service	This moving average data monitor follows the possible attack counts for up to 20 target services (service here is defined as the transport protocol, service name and port) by attacker zone, at five minute intervals over an hour. It will send alerts at no more than ten minute intervals, and refreshes its display every 30 seconds.
Targeted Zones by Service	This moving average data monitor follows the possible attack counts for up to 20 target services (service here is defined as the transport protocol, service name and port) by target zone, at five minute intervals over an hour. It will send alerts at no more than ten minute intervals, and refreshes its display every 30 seconds.
Attack Rates by Attacker Zone	This moving average data monitor follows the possible attack counts for up to 20 target services by attacker zones (service here is defined as the service name and port), at five minute intervals over an hour. It will send alerts at no more than ten minute intervals, and refreshes its display every 30 seconds.
Attack Rates by Targeted Zone	This moving average data monitor follows the possible attack counts for up to 20 target services by target zones (service here is defined as the service name and port), at five minute intervals over an hour. It will send alerts at no more than ten minute intervals, and refreshes its display every 30 seconds.
Attack Rates by Service and Customer	This moving average data monitor follows the possible attack counts for up to 20 target services (service here is defined as the transport protocol, service name and port), at five minute intervals over an hour. It will send alerts at no more than ten minute intervals, and refreshes its display every 30 seconds. The services are also broken down by customer.
Attacker Zones by Service and Customer	This moving average data monitor follows the possible attack counts for up to 20 target services (service here is defined as the transport protocol, service name and port) by attacker zone, at five minute intervals over an hour. It will send alerts at no more than ten minute intervals, and refreshes its display every 30 seconds. The services are also broken down by customer.

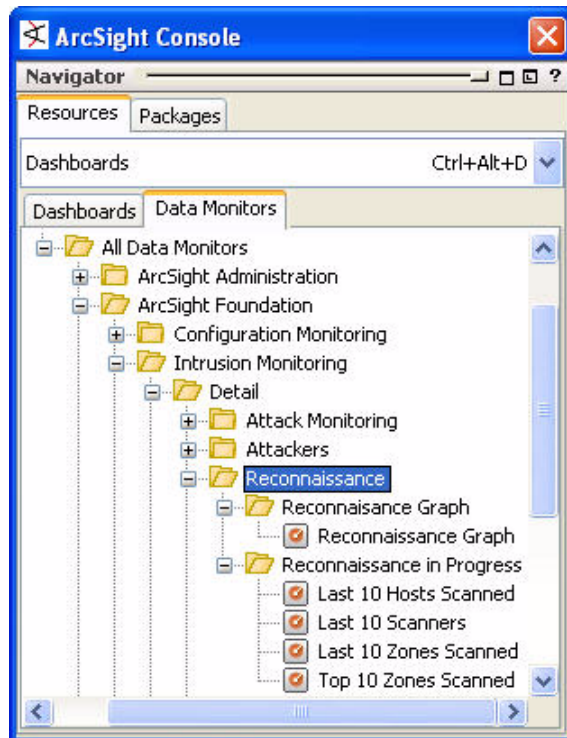
Data Monitor	Description
Targeted Zones by Service and Customer	This moving average data monitor follows the possible attack counts for up to 20 target services (service here is defined as the transport protocol, service name and port) by target zone, at five minute intervals over an hour. It will send alerts at no more than ten minute intervals, and refreshes its display every 30 seconds. The services are also broken down by customer.
Attack Rates by Attacker Zone and Customer	This moving average data monitor follows the possible attack counts for up to 20 target services by attacker zones (service here is defined as the service name and port), at five minute intervals over an hour. It will send alerts at no more than ten minute intervals, and refreshes its display every 30 seconds. The services are also broken down by customer.
Attack Rates by Targeted Zone and Customer	This moving average data monitor follows the possible attack counts for up to 20 target services by target zones (service here is defined as the service name and port), at five minute intervals over an hour. It will send alerts at no more than ten minute intervals, and refreshes its display every 30 seconds. The services are also broken down by customer.
Top 10 Targeted Services by Customer	This top value counts data monitor follows the possible attack counts for the top 10 targeted services (service here is defined as the transport protocol, service name and port), at five minute intervals over an hour. It will refresh its display every 30 seconds. The services are also broken down by customer.
Top 10 Attacker Zones by Service and Customer	This top value counts data monitor follows the possible attack counts for the top 10 attacker zones and targeted services (service here is defined as the transport protocol, service name and port), at five minute intervals over an hour. It will refresh its display every 30 seconds. The services are also broken down by customer.
Top 10 Targeted Zones by Service and Customer	This top value counts data monitor follows the possible attack counts for the top 10 targeted zones and targeted services (service here is defined as the transport protocol, service name and port), at five minute intervals over an hour. It will refresh its display every 30 seconds. The services are also broken down by customer.
Top 10 Attacker Zones by Customer	This top value counts data monitor follows the possible attack counts for the top 10 targeted services by attacker zones (service here is defined as the service name and port), at five minute intervals over an hour. It will refresh its display every 30 seconds. The services are also broken down by customer.
Top 10 Targeted Zones by Customer	This top value counts data monitor follows the possible attack counts for the top 10 targeted services by targeted zones (service here is defined as the service name and port), at five minute intervals over an hour. It will refresh its display every 30 seconds. The services are also broken down by customer.

Data Monitor	Description
Top 10 Attacked Services	This top value counts data monitor follows the possible attack counts for the top 10 attacker zones and targeted services (service here is defined as the transport protocol, service name and port), at five minute intervals over an hour. It will refresh its display every 30 seconds.
Top 10 Attacker Zones by Service	This top value counts data monitor follows the possible attack counts for the top 10 targeted services (service here is defined as the transport protocol, service name and port), at five minute intervals over an hour. It will refresh its display every 30 seconds.
Top 10 Targeted Zones by Service	This top value counts data monitor follows the possible attack counts for the top 10 targeted zones and targeted services (service here is defined as the transport protocol, service name and port), at five minute intervals over an hour. It will refresh its display every 30 seconds.
Top 10 Attacker Zones	This top value counts data monitor follows the possible attack counts for the top 10 targeted services by attacker zones (service here is defined as the service name and port), at five minute intervals over an hour. It will refresh its display every 30 seconds.
Top 10 Targeted Zones	This top value counts data monitor follows the possible attack counts for the top 10 targeted services by targeted zones (service here is defined as the service name and port), at five minute intervals over an hour. It will refresh its display every 30 seconds.
Firewall Accepts	This moving average data monitor sums the count of events constrained by the Inbound Events for Networks filter. The data monitor checks the up to 5 firewalls (the 5 firewalls reporting the most request or access activity) over five minute intervals over a period of an hour. It sends an alarm event if the moving average changes by 50%. - This data monitor is looking for sudden increases in request or access activity related to the protected network.
Inbound Event Spikes for Hosts	This moving average data monitor sums the count of events constrained by the Inbound Events for Hosts filter. The data monitor checks the up to 10 hosts (zone/host, the 10 most frequently accessed hosts) over thirty second intervals over a period of a half-hour. It sends an alarm event if the moving average changes by 300%. - This data monitor is looking for sudden increases in request or access activity related to the protected hosts. The alarm threshold is set high to detect significant spikes in the related event flow. The discard threshold is also set high (average 100 events per second) to filter out low event rates where an event spike of 10 or so packets with an average of 1 would be a false positive.

Data Monitor	Description
Inbound Event Spikes for Networks	This moving average data monitor sums the count of events constrained by the Inbound Events for Networks filter. The data monitor checks the up to 10 zones (the 10 most frequently accessed zones) over one minute intervals over a period of an hour. It sends an alarm event if the moving average changes by 300%. - This data monitor is looking for sudden increases in request or access activity related to the protected network. The alarm threshold is set high to detect significant spikes in the related event flow. The discard threshold is also set high (average 100 events per second) to filter out low event rates where an event spike of 10 or so packets with an average of 1 would be a false positive.
Inbound Event Spikes for Services	This moving average data monitor sums the count of events constrained by the Inbound Events for Service filter. The data monitor checks the up to 10 services (zone/address/port, the 10 most accessed hosts/services) over fifteen second intervals over a fifteen minute period. It sends an alarm event if the moving average changes by 300%. - This data monitor is looking for sudden increases in activity related to services on the protected network. The alarm threshold is set high to detect significant spikes in the related event flow. The discard threshold is also set high (average 100 events per second) to filter out low event rates where an event spike of 10 or so packets with an average of 1 would be a false positive.

Reconnaissance Data Monitors

The Reconnaissance data monitors supply the views for the Reconnaissance detail dashboards.

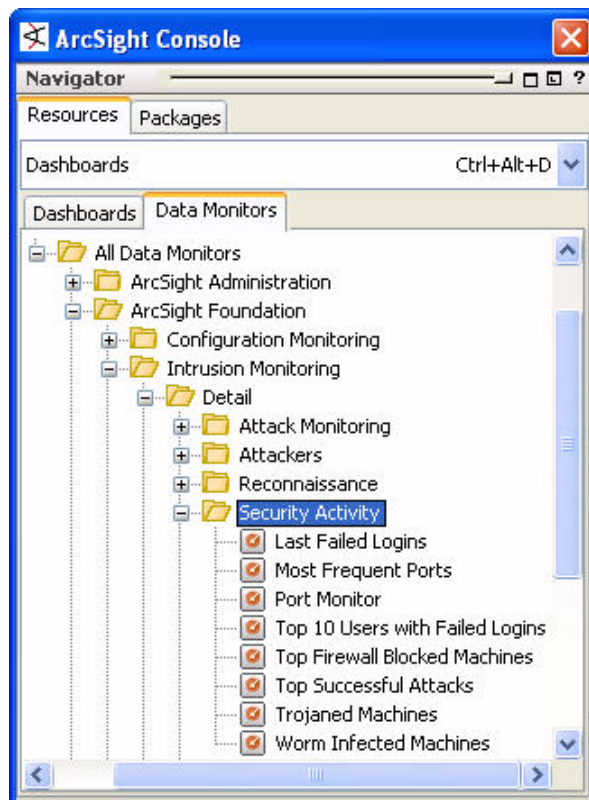


The reconnaissance data monitors are described in more detail below:

Data Monitor	Description
Reconnaissance Graph	This data monitor provides operators and analysts a view into how reconnaissance events are probing the network.
Last 10 Hosts Scanned	This data monitor shows the target zone and address, along with the time, of the last 10 reconnaissance events to give an overview of the most recent scanning activity against specific hosts.
Last 10 Scanners	This data monitor shows the attacker zone and address, along with the time, of the last 10 reconnaissance events to give an overview of the most recent scanning activity against the network.
Last 10 Zones Scanned	This data monitor shows the time and the target zone of the last 10 reconnaissance events to give an overview of the most recent scanning activity against the network.
Top 10 Zones Scanned	This data monitor shows the target zone of the 10 most frequent reconnaissance events within the last hour to give an overview of the most recent scanning activity against the network.

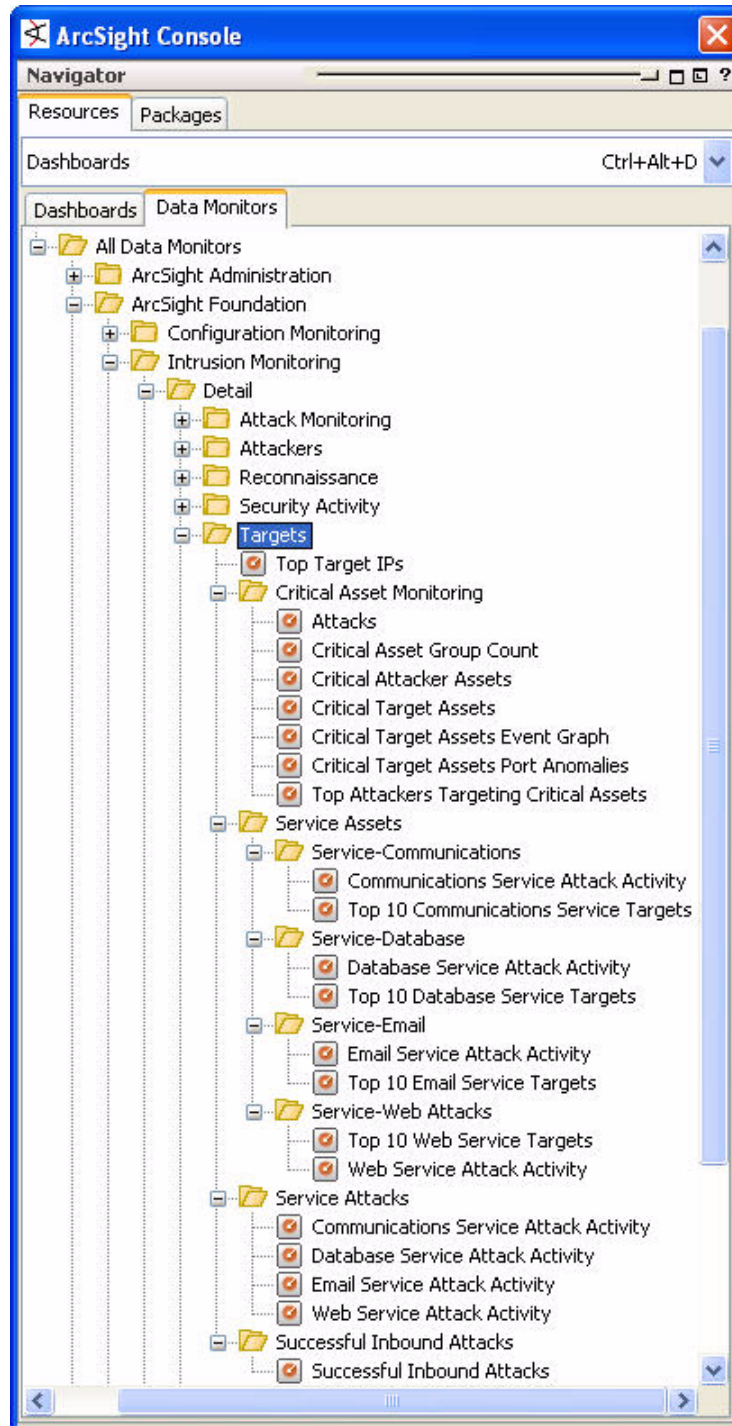
Security Activity Data Monitors

The Security Activity data monitors supply the views for the security activity detail dashboards.



Targets Data Monitors

The target data monitors supply views for the Targets detail dashboards.

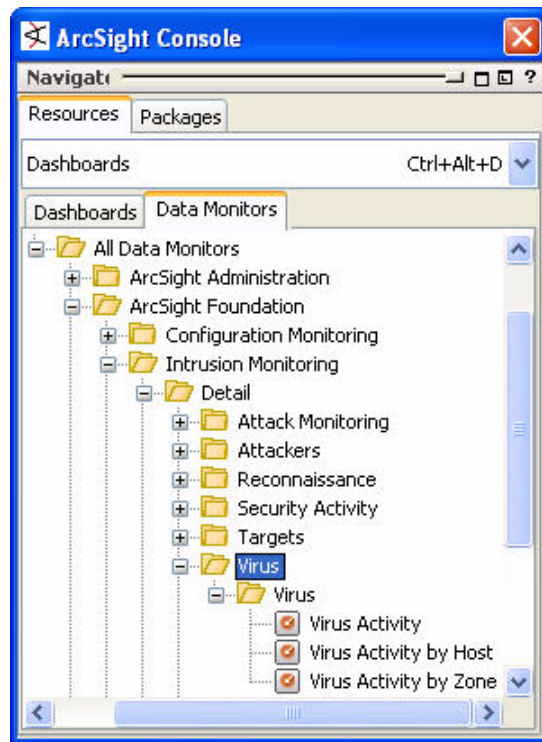


The Target data monitors are described in more detail below:

Data Monitor	Description
Critical Asset Group Count	Note: This Data Monitor will not work properly when running in Turbo Mode Fastest!
Critical Target Assets	Note: This Data Monitor will not work properly when running in Turbo Mode Fastest!
Critical Target Assets Event Graph	Note: This Data Monitor will not work properly when running in Turbo Mode Fastest!
Critical Target Assets Port Anomalies	Note: This Data Monitor will not work properly when running in Turbo Mode Fastest!
Top Attackers Targeting Critical Assets	Note: This Data Monitor will not work properly when running in Turbo Mode Fastest!
Top 10 Communications Service Targets	This Top Value Counts (Bucketized) Data Monitor displays the number of events affecting the top 10 Targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Communications Asset List.
Communications Service Attack Activity	This Asset Category Count Data Monitor displays the number of events affecting Targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Communications Asset List
Top 10 Database Service Targets	This Top Value Counts (Bucketized) Data Monitor displays the number of events affecting the top 10 Targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Database Asset List.
Database Service Attack Activity	This Asset Category Count Data Monitor displays the number of events affecting Targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Database Asset List
Top 10 Email Service Targets	This Top Value Counts (Bucketized) Data Monitor displays the number of events affecting the top 10 Targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Email Asset List.
Email Service Attack Activity	This Asset Category Count Data Monitor displays the number of events affecting Targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Email Asset List
Top 10 Web Service Targets	This Top Value Counts (Bucketized) Data Monitor displays the number of events affecting the top 10 Targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Web Asset List.
Web Service Attack Activity	This Asset Category Count Data Monitor displays the number of events affecting Targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Web Asset List: - Ecommerce - Intranet - Search

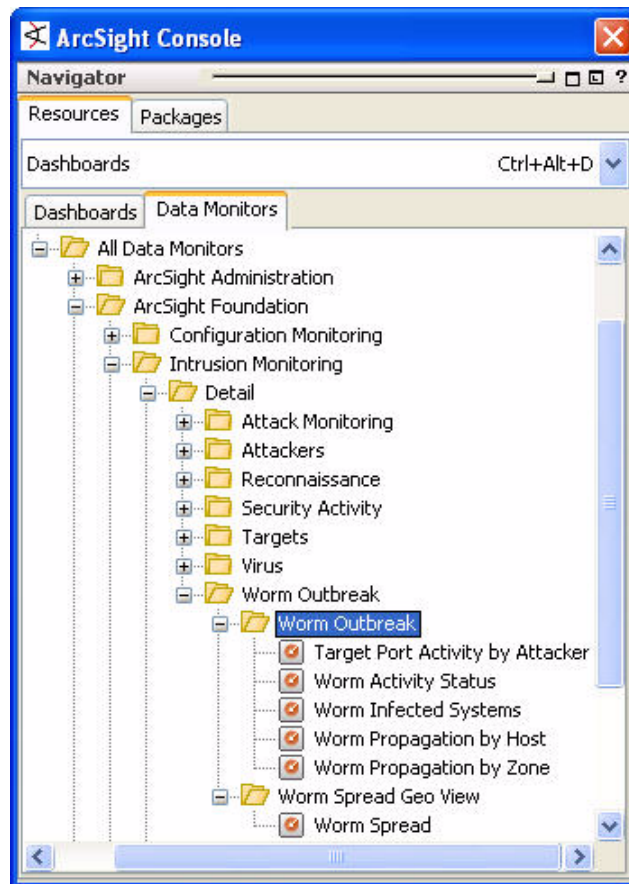
Virus Data Monitors

The Virus data monitors supply the views for the Virus detail dashboards.



Worm Outbreak Data Monitors

The Worm Outbreak data monitors supply the views for the Worm Outbreak detail dashboards.

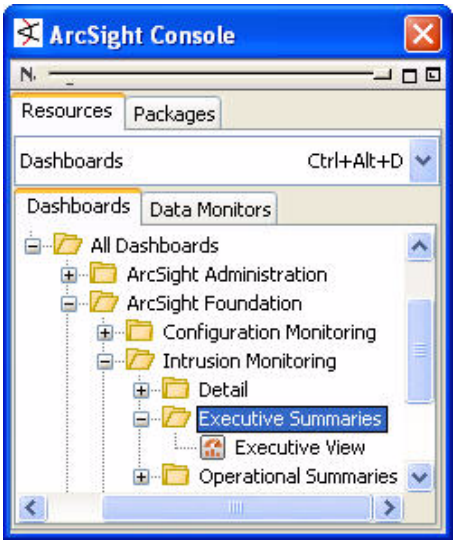


The Worm Outbreak data monitors are described in more detail below:

Data Monitor	Description
Target Port Activity by Attacker	This Data monitor is used in conjunction with the Worm Outbreak detected rule and the possible network sweep rule to detect worm outbreaks before an IDS signature is released.
Worm Infected Systems	This Last State data monitor displays the status of systems that have been infected in the course of a worm outbreak.

Executive Summary Dashboards

The Executive Summary dashboards show real-time high-level summaries of intrusion-related activity.

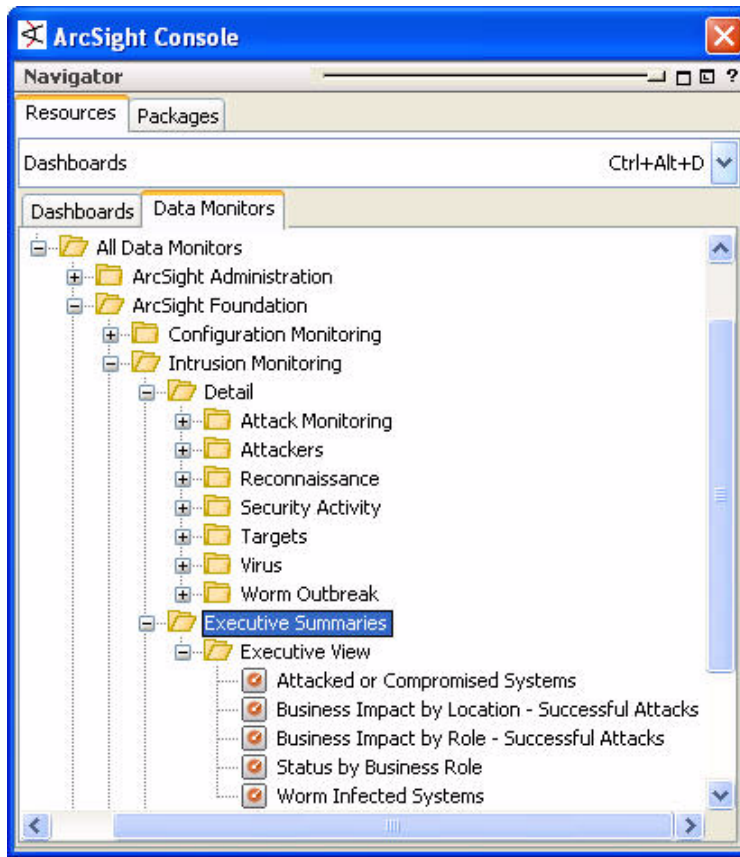


The Executive View dashboard is described in more detail below.

Dashboard	Description
Executive View	The Executive View dashboard gives an overview of the network with respect to attacked systems status by asset location, business role and worm activity. More detailed information is available from the follow-on dashboards in the Operational Summaries/ Executive View Details group: Attacked or Compromised Systems, Business Impact by Location, Business Impact by Role, Business Roles, Worm Infected Systems. This dashboard uses the following data monitors: Business Impact by Role - Successful Attacks, Business Impact by Location - Successful Attacks, Status by Business Role, Worm Infected Systems.

Executive Summary Data Monitors

The Executive Summary data monitors supply the views in the Executive Summary dashboards.

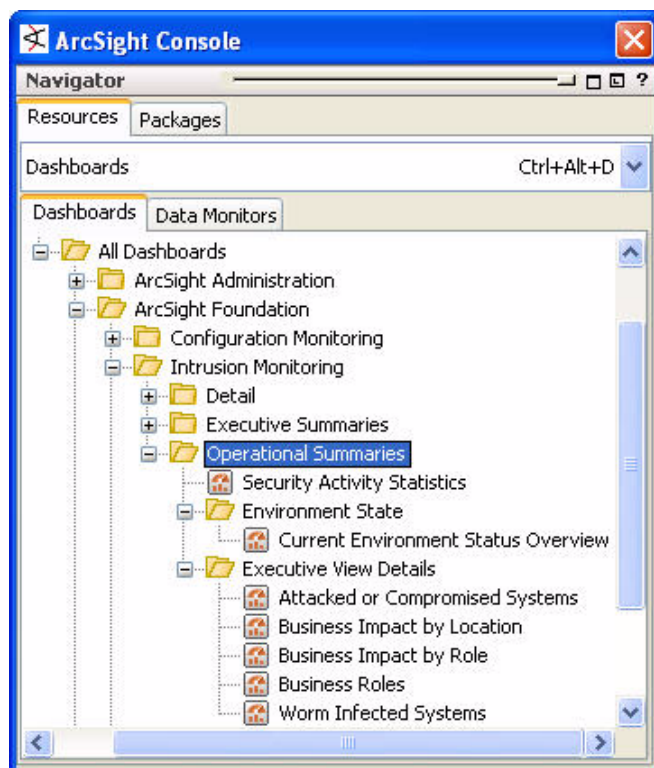


These data monitors are described in more detail below.

Data Monitor	Description
Attacked or Compromised Systems	This Last State Data Monitor displays the status of attacked or compromised systems.
Status by Business Role	This Last State Data Monitor displays the status of systems by Business Role, showing whether the target system has been attacked or compromised.
Business Impact by Location - Successful Attacks	This Asset Category Count data monitor displays a chart showing the number of successful attacks on systems within each asset location.
Business Impact by Role - Successful Attacks	This Asset Category Count Data Monitor displays a count and priority of the systems attacked by Business and Data Role.

Operational Summary Dashboards

The Operational Summary dashboards show real-time summaries of intrusion-related events. These views are optimal for identifying intrusions as they happen, and provide direction into the detail views for further investigation.



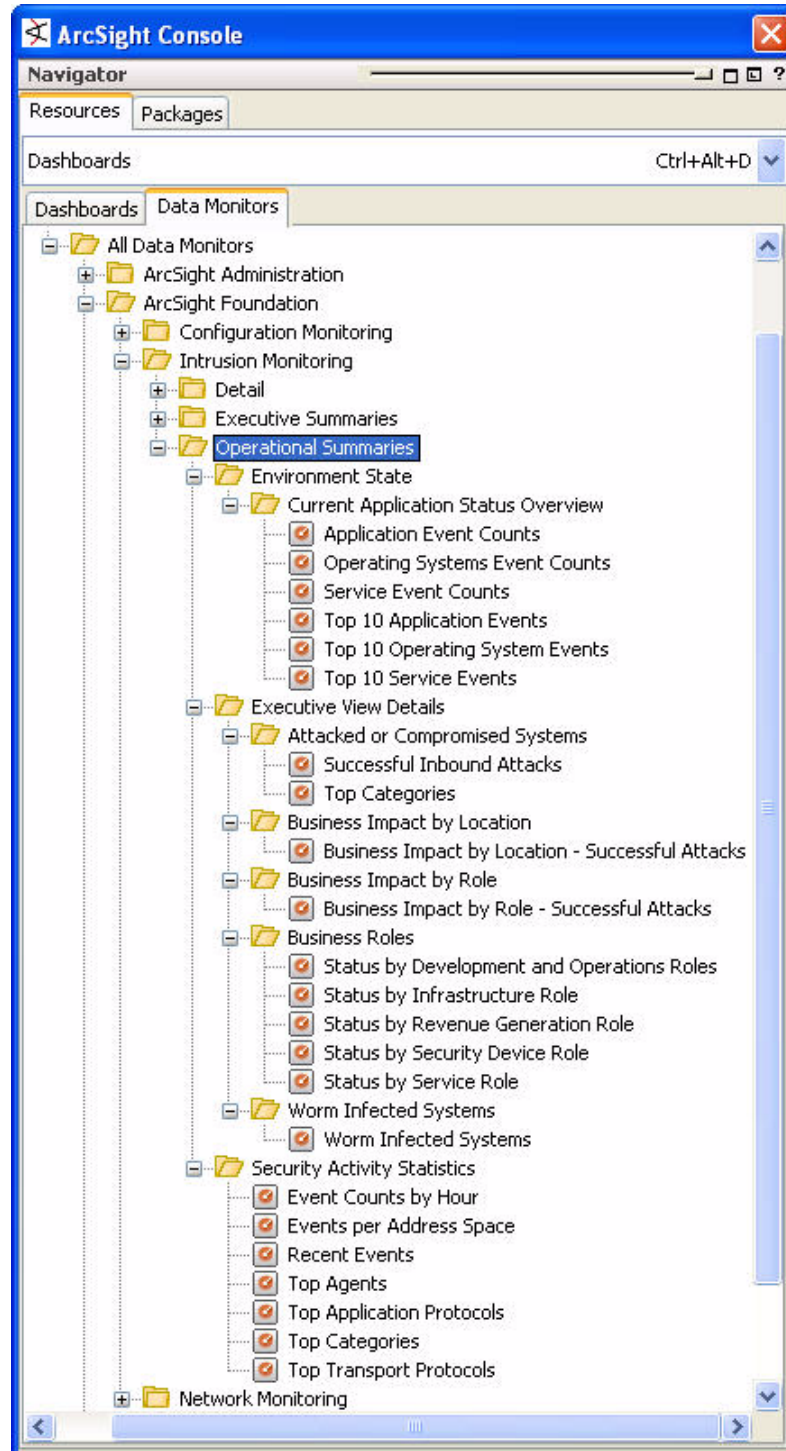
The Operational Summary dashboards are discussed in more detail below.

Dashboard	Description
Current Environment Status Overview	This dashboard shows an overview of the current environment based on application events, operating system events and service events. There are two data monitors for each area, a moving average data monitor and a top 10 events data monitor. The goal is to show changes in network activity related to these areas and provide some indication of what the most frequent events affecting these areas are.
Attacked or Compromised Systems	This dashboard shows a data monitor graph of targets and attackers with the attacks as nodes, and a data monitor showing the top 10 categories, by volume, of the event stream.
Business Impact by Location	This dashboard shows a chart of the successful attacks on systems by asset location.
Business Impact by Role	This dashboard shows a chart of the successful attacks on systems by asset category (business and data roles).

Dashboard	Description
Business Roles	The Business Roles dashboard displays the status of systems by their business roles: Security Device, Revenue Generation, Infrastructure, Development & Operations and Service. More detailed information is available from the follow-on dashboards in the Detail/Targets groups: Development Assets, Infrastructure Assets, Operations Assets, Revenue Generation Assets, Security Device Assets, Service Assets. This dashboard uses the following data monitors: Status by Security Device Role, Status by Infrastructure Role, Status by Development and Operations Role, Status by Revenue Generation Role, Status by Service Role
Worm Infected Systems	The Worm Infected Systems dashboard displays the number of systems infected by worms. More detailed information is available from the follow-on dashboards in the Detail/Attackers/Worm Outbreak group: Worm Outbreak and Worm Spread Geo View. This dashboard uses the Worm Infected Machines data monitor.

Operational Summary Data Monitors

The Operational Summary data monitors provide the views for the Operational summary dashboards.



These Operational Summary data monitors are described in more detail below:

Data Monitors	Description
Application Event Counts	This moving average data monitor sums the count of events constrained by the Events for Internal Applications excluding services filter. The data monitor checks the up to 20 Category Objects/Category Device Groups (the 20 most frequent events related to that object/device) over five minute intervals over a two hour period. It sends an alarm event if the moving average changes by 50%. - This data monitor is looking for sudden increases or decreases in activity related to applications on the protected network.
Operating Systems Event Counts	This moving average data monitor sums the count of events constrained by the Events for Internal Operating Systems filter. The data monitor checks the up to 20 Category Objects/Category Device Groups (the 20 most frequent events related to that object/device) over five minute intervals over a two hour period. It sends an alarm event if the moving average changes by 50%. - This data monitor is looking for sudden increases or decreases in activity related to operating systems on the protected network.
Service Event Counts	This moving average data monitor sums the count of events constrained by the Events for Internal Services filter. The data monitor checks the up to 20 Category Objects (the 20 most frequent events related to that object) over five minute intervals over a two hour period. It sends an alarm event if the moving average changes by 50%. - This data monitor is looking for sudden increases or decreases in activity related to services on the protected network.
Top 10 Application Events	This top 10 data monitor shows events constrained by the Events for Internal Applications excluding services filter. The data monitor check 1,000 distinct events in five minute intervals over the period of an hour.
Top 10 Operating System Events	This top 10 data monitor shows events constrained by the Events for Internal Operating Systems filter. The data monitor check 1,000 distinct events in five minute intervals over the period of an hour.
Top 10 Service Events	This top 10 data monitor shows events constrained by the Events for Internal Services filter. The data monitor check 1,000 distinct events in five minute intervals over the period of an hour.
Top Categories	
Status by Development and Operations Roles	This Last State Data Monitor displays the last state (Compromised, Attacked or Resolved) of Targets in the Site Asset Categories/Business Impact Analysis/Business Role/Development and the Site Asset Categories/Business Impact Analysis/Business Role/Operations asset lists.
Status by Infrastructure Role	This Last State Data Monitor displays the last state (Compromised, Attacked or Resolved) of Targets in the Site Asset Categories/Business Impact Analysis/Business Role/Infrastructure/Computer and the Site Asset Categories/Business Impact Analysis/Business Role/Infrastructure/Network asset lists.

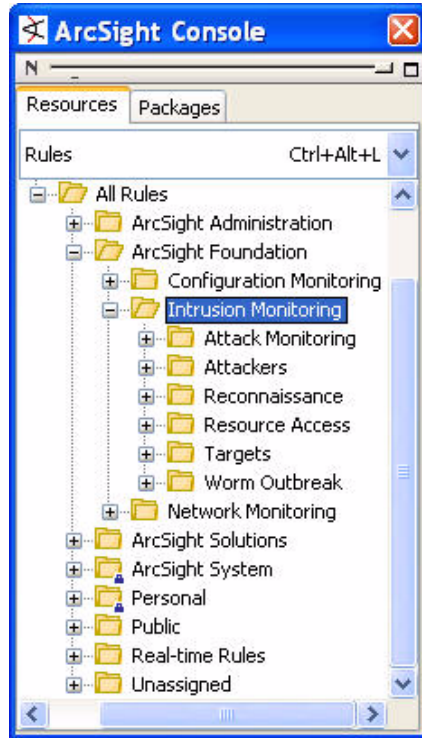
Data Monitors	Description
Status by Revenue Generation Role	This Last State Data Monitor displays the last state (Compromised, Attacked or Resolved) of Targets in the Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation Asset List.
Status by Security Device Role	This Last State Data Monitor displays the last state (Compromised, Attacked or Resolved) of Targets in the Site Asset Categories/Business Impact Analysis/Business Role/Security Device Asset List.
Status by Service Role	This Last State Data Monitor displays the last state (Compromised, Attacked or Resolved) of Targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service Asset List.

Last-State Data Monitors - Usage Instructions

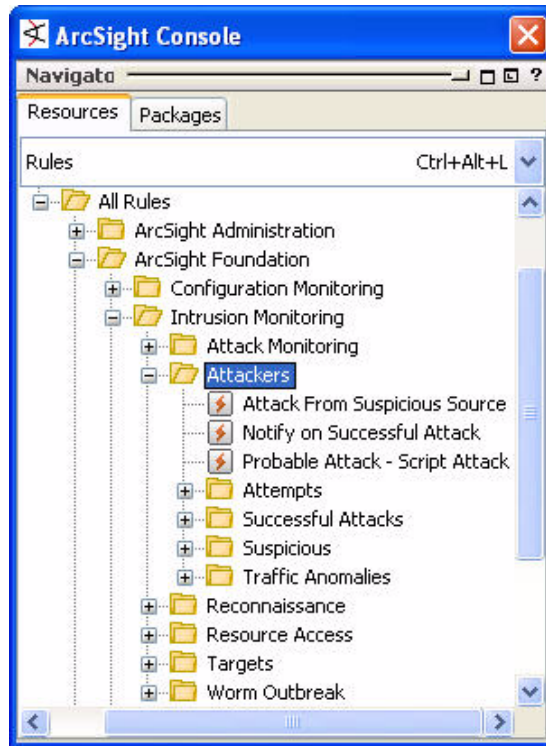
The last state data monitors will reset themselves automatically after the period of time set in the data monitor's History Time Range field. The device the data monitor is reporting on may not be online after a compromise, however; the detail reports can be one of the ways that you identify what systems are offline after a compromise so you can restore it to service appropriately.

Intrusion Monitoring Rules

The Intrusion Monitoring rules correlate conditions among intrusion-related events that support the Attack Monitoring, Attackers, Reconnaissance, Resource Access, Targets, and Worm Outbreak use cases.



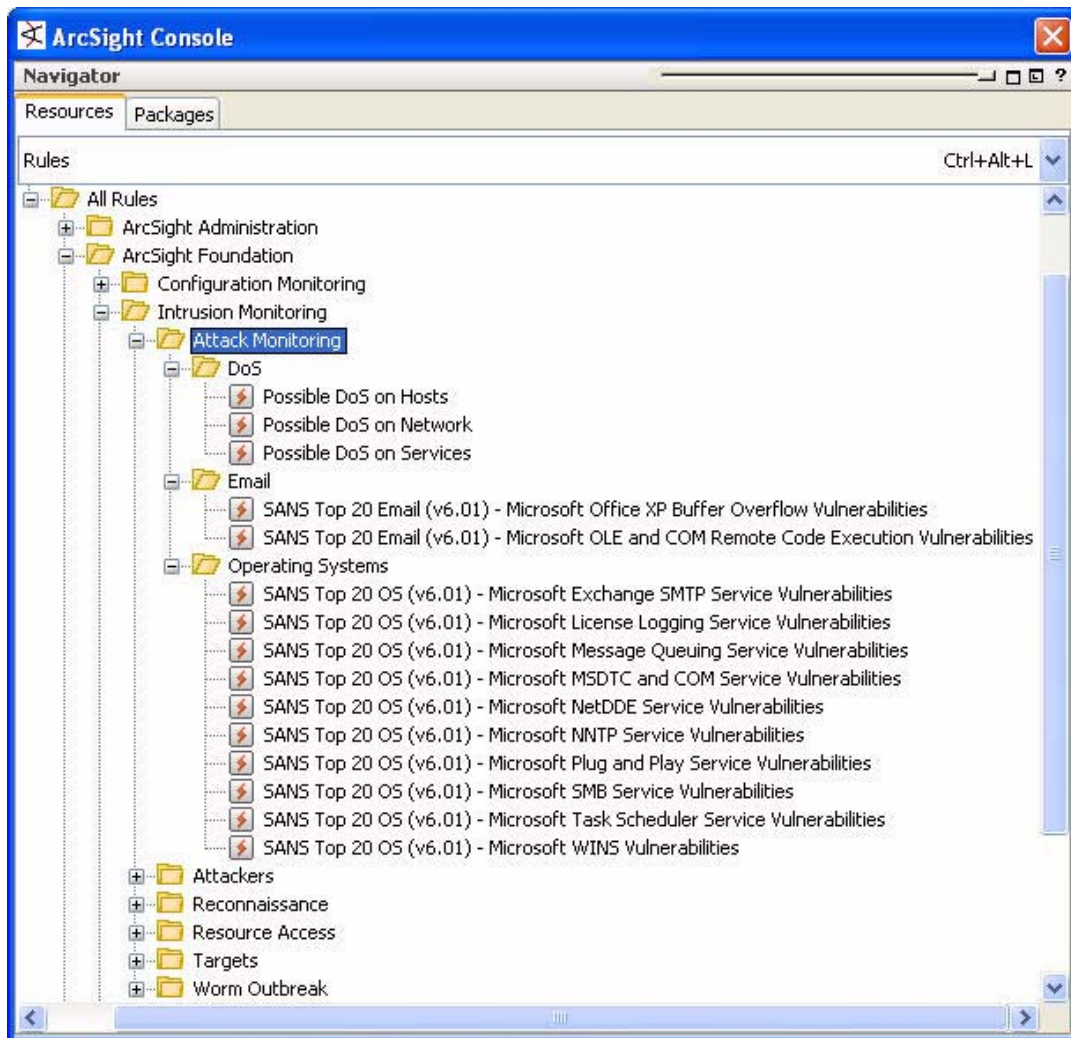
Attackers Rules



The Attacker rules are described in more detail below.

Rule	Description
Attack From Suspicious Source	This rule looks for attacks coming from a source categorized as suspicious or untrusted and does not belong to Attackers/Trusted List. It fires whenever an event coming from a source belonging to suspicious or untrusted active list but not to Attackers/Trusted List has category significance hostile and compromise. On first event, the source address is added to the /Hostile active list and event severity is set to high.
Notify on Successful Attack	This rule detects successful attacks. This rule looks for high priority (= 8) successful attacks for which the attacker is not in the Attackers/Trusted List. This rule only requires 1 such event, and the time frame is set to 10 minutes. After this rule is triggered, a new Case will be created and a notification will be sent to the CERT team.
Probable Attack - Script Attack	This rule looks for multiple executions of scripts, (http, cgi, and so on) that have the same event name, attacker address, and target address within a short period of time. The rule monitors any attempts to start or execute a script that target an application, a service or an operating system. The rule fires when 10 events occur in 1 minute with the same event name, attacker address, and target address. On first threshold, the attacker address is added to the /Hostile active list, and the target address is added to the /Hit active list. ***Note: This rule will not fire when running in Turbo Mode Fastest!

Attack Monitoring Rules



The Attack Monitoring rules are described in more detail below.

Rule	Description
Possible DoS on Hosts	This rule looks for two conditions, one is a spike in events detected by the Inbound Event Spikes for Hosts data monitor, and the other is for an event describing either failure to communicate with the host mentioned in the first event or an event describing the shutting down of the host.; The rule looks for two such events within three minutes. This aggregation is used to keep the rule from firing too often if a host reboots or restarts its affected service quickly.; On the first event, the rule will fire an event describing a successful Denial of Service compromise on the affected host.

Rule	Description
Possible DoS on Network	This rule looks for two conditions, one is a spike in events detected by the Inbound Event Spikes for Networks data monitor, and the other is for an event describing either failure to communicate with hosts on the network zone mentioned in the first event.; The rule looks for six such events within one minute with six different hosts. This aggregation is used to determine whether the spike is for a specific host on the network or a possible Denial of Service attack against the entire network.; On the first threshold (six such events), the rule will fire an event describing a successful Denial of Service compromise on the affected network zone.
Possible DoS on Services	This rule looks for two conditions, one is a spike in events detected by the Inbound Event Spikes for Services data monitor, and the other is for an event describing either failure to communicate with a service on a host mentioned in the first event or an event describing the shutting down of the service.; The rule looks for two such events within three minutes. This aggregation is used to keep the rule from firing too often if a host reboots or restarts its affected service quickly.; On the first event, the rule will fire an event describing a successful Denial of Service compromise on the affected network zone.
SANS Top 20 Email (v6.01) - Microsoft OLE and COM Remote Code Execution Vulnerabilities	This rule checks for the SANS Top 20 vulnerabilities in W4 Microsoft Office and Outlook Express for the Microsoft OLE and COM Remote Code Execution vulnerabilities (see http://www.sans.org/top20/2005/#w4 for details).; There is a buffer overflow error in the way that Exchange (2000 and Server 2003) handles an SMTP extension that could allow a remote attacker to execute arbitrary code or cause a denial of service.; The rule checks for base events related to outbound traffic from an application with behavior categorized as Communicate/Query or starting with Access, with an outcome of no failure, from source systems with a Microsoft operating system.; If the above conditions are met, the following actions are taken: An event is sent with the following additional settings:; name = SANS Top 20 Email (v6.01) - Microsoft OLE and COM Remote Code Execution Vulnerability Exploit Attempt; agentSeverity = Medium; categoryBehavior = /Communicate/Query; categoryObject = /Host/Operating System; categoryOutcome = /Attempt; categorySignificance = /Compromise; categoryTechnique = /Exploit/Vulnerability; deviceCustomString1Label = Rule Type; deviceCustomString1 = SANS Top 20 (v6.01); deviceCustomString2Label = Vulnerability Area; deviceCustomString2 = Email; deviceCustomString3Label = Vulnerability Name; deviceCustomString3 = Microsoft OLE and COM Remote Code Execution Vulnerability Exploit Attempt. The relevant Microsoft Security Bulletins and CVE identifiers are MSSB MS05-012, CVE CAN-2005-0044 and CVE CAN-2005-0047.

Rule	Description
SANS Top 20 Email (v6.01) - Microsoft Office XP Buffer Overflow Vulnerabilities	<p>This rule checks for the SANS Top 20 vulnerabilities in W4 Microsoft Office and Outlook Express for the Microsoft OLE and COM Remote Code Execution vulnerabilities (see http://www.sans.org/top20/2005/#w4 for details).; There is a buffer overflow error in Microsoft Office XP that could allow an attacker to gain full control of a system where the user is tricked into clicking on a link to a malicious file, either from an email message or through Internet Explorer.; The rule checks for base events related to outbound traffic from an application with behavior categorized as Communicate/Query or starting with Access, with an outcome of no failure, from source systems with a Microsoft operating system.; If the above conditions are met, the following actions are taken: An event is sent with the following additional settings:; name = SANS Top 20 Email (v6.01) - Microsoft Office XP buffer overflow vulnerability Exploit Attempt; agent Severity = Medium; category Behavior = /Communicate/Query; category Object = /Host/Operating System; category Outcome = /Attempt; category Significance = /Compromise; category Technique = /Exploit/Vulnerability; deviceCustomString1Label = Rule Type; deviceCustomString1 = SANS Top 20 (v6.01); deviceCustomString2Label = Vulnerability Area; deviceCustomString2 = Email; deviceCustomString3Label = Vulnerability Name; deviceCustomString3 = Microsoft Office XP buffer overflow vulnerability Exploit Attempts relevant Microsoft Security Bulletins and CVE identifiers are MSSB MS05-005, and CVE CAN-2004-0848.</p>
SANS Top 20 OS (v6.01) - Microsoft Exchange SMTP Service Vulnerabilities	<p>This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see tap://www.sans.org/top20/2005/#w1 for details) for the Exchange SMTP Service vulnerability.; There is a buffer overflow error in the way that Exchange (2000 and Server 2003) handles an SMTP extension that could allow a remote attacker to execute arbitrary code or cause a denial of service.; The rule checks for events related to inbound traffic categorized as hostile or compromise, with an outcome of no failure, to target systems with a Microsoft operating system on port 25.; It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group. If the target system is not in the Microsoft operating system Asset Group, the asset ID should either be NULL or not in any Operating System group.; If the above conditions are met, the following actions are taken: An event is sent with the following additional settings:; name = SANS Top 20 (v6.01) - Microsoft Exchange SMTP Service Vulnerability Exploited; agentSeverity = Very High; categoryBehavior = /Communicate/Query; categoryObject = /Host/Operating System; categoryOutcome = /Success; categorySignificance = /Compromise; categoryTechnique = /Exploit/Vulnerability. The targeted machine is placed in the SANS Top 20 Vulnerabilities - OS - Exploited machines" active list.; The relevant Microsoft Security Bulletins and CVE identifiers are MSSB MS05-021 and CVE CAN-2005-0560.</p>

Rule	Description
SANS Top 20 OS (v6.01) - Microsoft License Logging Service Vulnerabilities	This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see http://www.sans.org/top20/2005/#w1) for the Microsoft License Logging Service vulnerabilities.; The Microsoft License Logging service has an unchecked buffer that could allow an attacker to remotely execute arbitrary code.; The rule checks for events related to inbound traffic on TCP ports 139 or 445, categorized as hostile or compromise, with an outcome of no failure. It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group.; If the above conditions are met, the following actions are taken: An event is sent with the following additional settings:; name: SANS Top 20 (v6.01) - Microsoft License Logging Service Vulnerability Exploited; agent Severity: Very-High; category Behavior: /Execute; category Object: /Host/Operating System; category Outcome: /Success; category Significance: /Compromise; category Technique: /Exploit/Vulnerabilities targeted machine is placed in the SANS Top 20 Vulnerabilities (v6.01) - OS - Exploited machines" active list.; The relevant Microsoft Security Bulletins and CVE identifiers are MSSB MS05-010 and CVE CAN-2005-0050.;
SANS Top 20 OS (v6.01) - Microsoft MSDTC and COM Service Vulnerabilities	This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see tap://www.sans.org/top20/2005/#w1) for the Microsoft MSDTC and COM+ Services vulnerabilities.; The Microsoft Distributed Transaction Coordinator (MSDTC), COM+, Transaction Internet Protocol (TIP) and Distributed TIP services have flaws that could allow an attacker to execute arbitrary code, elevate local privileges or cause a denial of service.; The rule checks for events related to inbound traffic on TCP ports 135, 139, 445, 593, 1025 or 3372, or UDP ports 135, 137, 138 or 445, categorized as hostile or compromise, with an outcome of no failure. It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group.; If the above conditions are met, the following actions are taken: An event is sent with the following additional settings:; name: SANS Top 20 (v6.01) - Microsoft MSDTC or COM+ Services Vulnerability Exploited; agentSeverity: Very-High; categoryBehavior: /Execute; categoryObject: /Host/Operating System; categoryOutcome: /Success; categorySignificance: /Compromise; categoryTechnique: /Exploit/Vulnerability; The targeted machine is placed in the SANS Top 20 Vulnerabilities (v6.01) - OS - Exploited machines" active list.; The relevant Microsoft Security Bulletins and CVE identifiers are MSSB MS05-051, CVE CAN-2005-1978, CVE CAN-2005-1979, CVE CAN-2005-1980 and CVE CAN-2005-2119.;

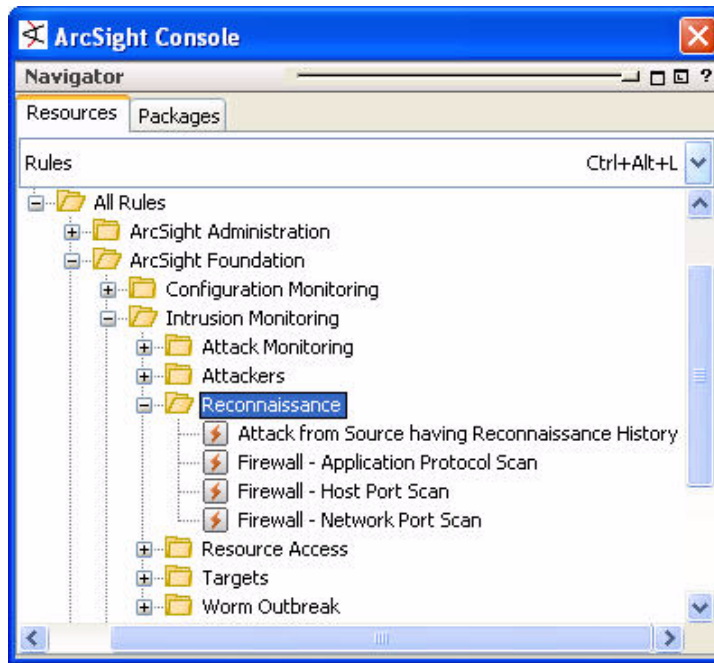
Rule	Description
SANS Top 20 OS (v6.01) - Microsoft Message Queuing Service Vulnerabilities	This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see http://www.sans.org/top20/2005/#w1) for the Microsoft Message Queuing Service vulnerabilities.; The Microsoft Message Queuing service has an unchecked buffer that could allow an attacker to remotely execute arbitrary code.; The rule checks for events related to inbound traffic on TCP ports 135, 139, 445, 593, 1801, 2101, 2103, 2105 or 2107, or UDP ports 135, 137, 138, 445, 1801 or 3527, categorized as hostile or compromise, with an outcome of no failure. It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group.; If the above conditions are met, the following actions are taken: An event is sent with the following additional settings:; name: SANS Top 20 (v6.01) - Microsoft Message Queuing Service Vulnerability Exploited; agent Severity: Very-High; categoryBehavior: /Execute; categoryObject: /Host/Operating System; categoryOutcome: /Success; categorySignificance: /Compromise; categoryTechnique: /Exploit/Vulnerability; The targeted machine is placed in the SANS Top 20 Vulnerabilities (v6.01) - OS - Exploited machines" active list.; The relevant Microsoft Security Bulletins and CVE identifiers are MSSB MS05-017 and CVE CAN-2005-0059.
SANS Top 20 OS (v6.01) - Microsoft NNTP Service Vulnerabilities	This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see http://www.sans.org/top20/2005/#w1) for the Microsoft NNTP Service vulnerability.; The Microsoft Network News Transport Protocol (NNTP) Service in Internet Information Services (IIS) has several flaws in the way the NNTP component handles the parsing of user search patterns for the XPAT command. A remote, unauthenticated attacker could execute arbitrary code with administrative privileges on a vulnerable system.; The rule checks for events related to inbound traffic on ports 119 or 563 (TCP or UDP), categorized as hostile or compromise, with an outcome of no failure, to assets with the vulnerability category MSSB MS04-036 or CVE CAN-2004-0574. It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group.; If the above conditions are met, the following actions are taken:; An event is sent with the following additional settings:; name: SANS Top 20 (v6.01) - Microsoft NNTP Service Vulnerability Exploited; agent Severity: Very-High; categoryBehavior: /Execute; categoryObject: /Host/Operating System; categoryOutcome: /Success; categorySignificance: /Compromise; categoryTechnique: /Exploit/Vulnerability; The targeted machine is placed in the SANS Top 20 Vulnerabilities (v6.01) - OS - Exploited machines" active list.; The relevant Microsoft Security Bulletins and CVE identifiers are MSSB MS04-036 and CVE CAN-2004-0574.

Rule	Description
SANS Top 20 OS (v6.01) - Microsoft NetDDE Service Vulnerabilities	This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see http://www.sans.org/top20/2005/#w1) for the Microsoft NetDDE Service vulnerability.; The Microsoft Network Dynamic Data Exchange (NetDDE) protocol has a buffer management flaw in the way malformed messages are handled that exposes a vulnerability that could allow an attacker to compromise the vulnerable system.; The rule checks for events related to inbound traffic on TCP ports 135, 139, 445 or 593, or UDP port 135, 137, 138 or 445, categorized as hostile or compromise, with an outcome of no failure. It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group.; If the above conditions are met, the following actions are taken:; An event is sent with the following additional settings:; name: SANS Top 20 (v6.01) - Microsoft NetDDE Service Vulnerability Exploited; agentSeverity: Very-High; categoryBehavior: /Execute; categoryObject: /Host/Operating System; categoryOutcome: /Success; categorySignificance: /Compromise; categoryTechnique: /Exploit/Vulnerability; The targeted machine is placed in the SANS Top 20 Vulnerabilities (v6.01) - OS - Exploited machines" active list.; The relevant Microsoft Security Bulletins and CVE identifiers are MSSB MS04-031 and CVE CAN-2004-0206.;
SANS Top 20 OS (v6.01) - Microsoft Plug and Play Service Vulnerabilities	This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see http://www.sans.org/top20/2005/#w1) for the Microsoft Plug and Play Service vulnerability.; The Microsoft Plug and Play Service contains buffer overflows that can allow a remote user to execute arbitrary code.; The rule checks for events related to inbound traffic on TCP ports 139 or 445, categorized as hostile or compromise, with an outcome of no failure, to assets with the vulnerability category MSSB MS05-039 or MSSB MS05-047. It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group.; If the above conditions are met, the following actions are taken:; An event is sent with the following additional settings:; name: SANS Top 20 (v6.01) - Microsoft Plug and Play Service Vulnerability Exploited; agentSeverity: Very-High; categoryBehavior: /Execute; categoryObject: /Host/Operating System; categoryOutcome: /Success; categorySignificance: /Compromise; categoryTechnique: /Exploit/Vulnerability; The targeted machine is placed in the SANS Top 20 Vulnerabilities (v6.01) - OS - Exploited machines" active list.; The relevant Microsoft Security Bulletins and CVE identifiers are MSSB MS05-039, MSSB MS05-047, CVE CAN-2005-1983 and CVE CAN-2005-2120.;

Rule	Description
SANS Top 20 OS (v6.01) - Microsoft SMB Service Vulnerabilities	This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see http://www.sans.org/top20/2005/#w1) for the Microsoft SMB Service vulnerability.; The Microsoft Server Message Block (SMB) protocol allows sharing of files, printers, serial ports, etc. There are flaws in SMB packet validation that could result in a buffer receiving inappropriate data.; The rule checks for events related to inbound traffic on TCP ports 139 or 445, categorized as hostile or compromise, with an outcome of no failure, to assets with the vulnerability category MSSB MS05-011 or MSSB MS05-027. It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group.; If the above conditions are met, the following actions are taken:; An event is sent with the following additional settings:; name: SANS Top 20 (v6.01) - Microsoft SMB Service Vulnerability Exploited; agentSeverity: Very-High; categoryBehavior: /Execute; categoryObject: /Host/Operating System; categoryOutcome: /Success; categorySignificance: /Compromise; categoryTechnique: /Exploit/Vulnerability; The targeted machine is placed in the SANS Top 20 Vulnerabilities (v6.01) - OS - Exploited machines" active list.; The relevant Microsoft Security Bulletins and CVE identifiers are MSSB MS05-011, MSSB MS05-027, CVE CAN-2005-0045 and CVE CAN-2005-1206.
SANS Top 20 OS (v6.01) - Microsoft Task Scheduler Service Vulnerabilities	This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see http://www.sans.org/top20/2005/#w1) for the Microsoft Task Scheduler vulnerability.; The Microsoft Windows Task Scheduler is an ActiveX control that schedules arbitrary commands to be run on a system. There is a buffer overflow in the scheduler due to not properly checking attributes of the command names tasked within the scheduler.; The rule checks for events related to inbound traffic categorized as hostile or compromise, with an outcome of no failure, to assets with the vulnerability category MSSB MS04-022 or CVE CAN-2004-0212. It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group.; If the above conditions are met, the following actions are taken:; An event is sent with the following additional settings:; name: SANS Top 20 (v6.01) - Microsoft Task Scheduler Service Vulnerability Exploited; agentSeverity: Very-High; categoryBehavior: /Execute; categoryObject: /Host/Operating System; categoryOutcome: /Success; categorySignificance: /Compromise; categoryTechnique: /Exploit/Vulnerability; The targeted machine is placed in the SANS Top 20 Vulnerabilities (v6.01) - OS - Exploited machines" active list.; The relevant Microsoft Security Bulletins and CVE identifiers are MSSB MS04-022 and CVE CAN-2004-0212.;

Rule	Description
SANS Top 20 OS (v6.01) - Microsoft WINS Vulnerabilities	<p>This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see http://www.sans.org/top20/2005/#w1) for WINS vulnerabilities.; The Windows Internet naming Service (WINS) provides a mapping between NETBIOS computer names and IP addresses. Incoming WINS packets are not sufficiently validated on the name parameter, allowing a buffer overflow. Additionally, there is a heap-based buffer overflow in the server-to-server replication protocol due to not properly validating the association context data structure.; The rule checks for events related to inbound traffic on port 42 (UDP or TCP), categorized as hostile or compromise, with an outcome of no failure, to assets with the vulnerability category MSSB MS04-045, CVE CAN-2004-0567 or CVE CAN-2004-1080. It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group.; If the above conditions are met, the following actions are taken:; An event is sent with the following additional settings:; name: SANS Top 20 (v6.01) - Microsoft WINS Vulnerability Exploited; agentSeverity: Very-High; categoryBehavior: /Execute; categoryObject: /Host/Operating System; categoryOutcome: /Success; categorySignificance: /Compromise; categoryTechnique: /Exploit/Vulnerability; The targeted machine is placed in the SANS Top 20 Vulnerabilities (v6.01) - OS - Exploited machines" active list.; The relevant Microsoft Security Bulletins and CVE identifiers are MSSB MS04-045, CVE CAN-2004-0567 and CVE CAN-2004-1080;</p>

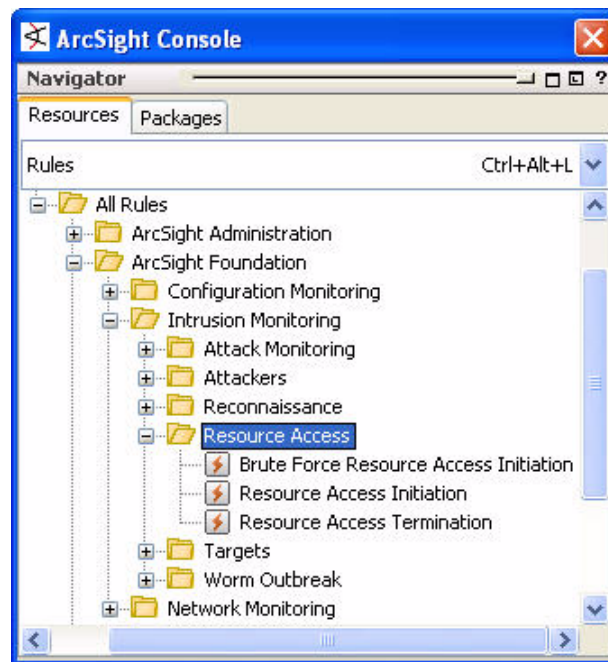
Reconnaissance Rules



The Reconnaissance rules are described in more detail below.

Rule	Description
Attack from Source having Reconnaissance History	This rule looks for attack from sources that have already performed reconnaissance. This rule fires whenever the attacker is in the Reconnaissance or Untrusted active list and the event has hostile and compromise significance. On first event, the attacker is added to the /Hostile active list.
Firewall - Application Protocol Scan	This rule looks for application protocol scans. The rule monitors failure access detected by a firewall. The rule fires when 3 events occur in 3 minutes with the same attacker/target pair with different application protocols each time. On first threshold, the attacker address is added to the /Reconnaissance active list and the target address is added to the /Scanned active list.
Firewall - Host Port Scan	This rule looks for port scan on a host. The rule monitors failure access detected by a firewall. The rule fires when 3 events occur in 3 minutes with the same attacker/target pair with different target ports each time. On first threshold, the attacker address is added to the /Reconnaissance active list and the target address is added to the /Scanned active list.
Firewall - Network Port Scan	This rule looks for a network port scan. The rule monitors failure access detected by a firewall. The rule fires when 5 events occur in 3 minutes with the same port for each attacker/target pair, but with different target addresses each time. On first threshold, the attacker address is added to the /Suspicious active list and the target address is added to the /Scanned active list.

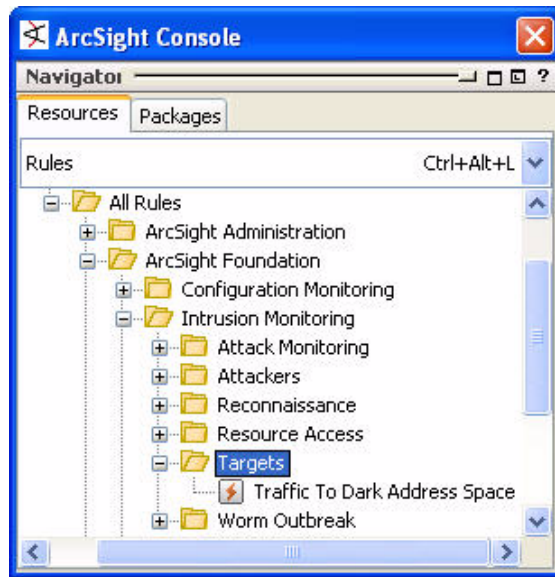
Resource Access Rules



The Resource Access rules are described in more detail below.

Rule	Description
Brute Force Resource Access Initiation	This rule looks for brute force resource access initiation events (defined by the Access Initiation Events filter) and terminates the sessions in the Resource Access session list. It also sets the categoryDeviceGroup field to /Security Information Manager and the categorySignificance to /Informational.
Resource Access Initiation	This rule looks for resource access initiation events as defined by the Access Initiation Events filter and terminates the sessions in the Resource Access session list. It also sets the categoryDeviceGroup field to /Security Information Manager and the categorySignificance to /Informational.
Resource Access Termination	This rule looks for resource access termination events as defined by the Access Termination Events filter and terminates the sessions in the following session lists: Brute Force Resource AccessResource Access. It also sets the categoryDeviceGroup field to /Security Information Manager and the categorySignificance to /Informational.

Targets Rule

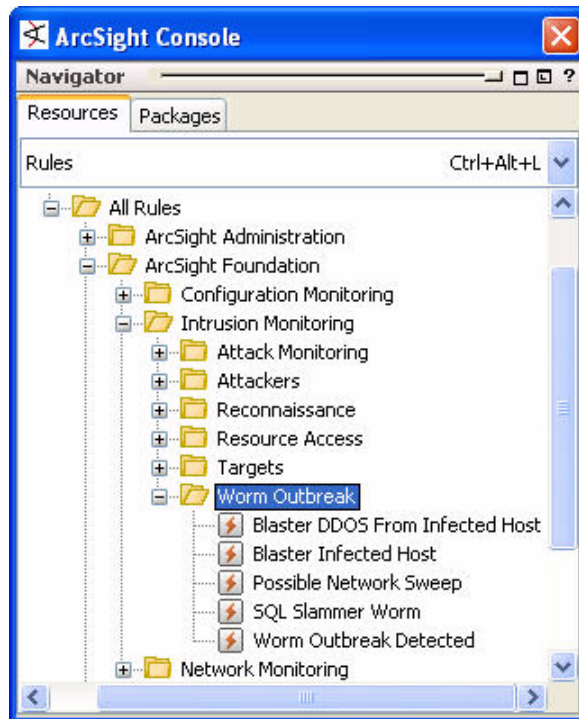


The Targets rule is described in more detail below.

Rule	Description
Traffic To Dark Address Space	This rule looks for any traffic that targets the Dark address space and adds the attacker address to the /Suspicious active list.

Worm Outbreak Rules

The Worm Outbreak rules look for conditions associated with known and suspected worm activity.



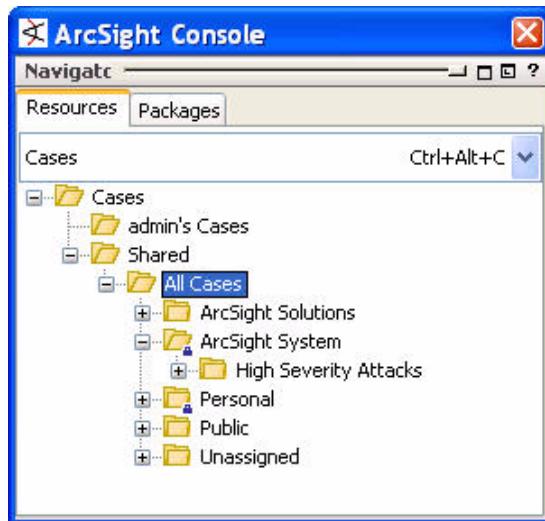
The Worm Outbreak rules are described in more detail below.

Rule	Description
Blaster DDOS From Infected Host	This rule detects a Distributed Denial Of Service (DDOS) attack (Blaster) coming from an infected host. This rule looks for DoS events targeting a windowsupdate.com host, either coming from a host in the 'Attackers/Untrusted List' active list or from a host in the 'Targets/Compromised List' active list. This means that a compromised target could be acting as an attacker. In this case, this host is infected. This rule only requires 1 such event, and the time frame is set to 2 minutes. After this rule is triggered, the 'categoryOutcome' field is set to /Success and the 'categorySignificance' field is set to /Hostile.
Blaster Infected Host	This rule detects infected hosts by a Blaster worm. This rule looks for 2 events. The first event targets one of the following ports: 135, 139 or 445. The second event targets the port 69 and uses UDP. Neither event comes from a host in the 'Attackers/Trusted List' Active List. In order to have a matching event, the two events have to be chronologically ordered and the Attacker-Target pair in the first event should match the Target-Attacker pair in the second event. This rule requires 1 matching occurrence, and the time frame is set to 2 minutes. On the first occurrence, a notification will be sent to the Analysts, the target of the first event will be added in the 'Targets/Compromised List' active list and the attacker of the first event will be added in the 'Attackers/Hostile List' active list.

Rule	Description
Possible Network Sweep	This rule is looking for a single host trying to communicate with at least 10 other hosts on the same target port. This rule, combined with a spike in target port activity by the same host, will result in the worm outbreak detected rule being triggered.
SQL Slammer Worm	This rule detects a SQL Slammer worm. The SQL Slammer worm uses a vulnerability of Microsoft SQL Server by sending an executable code to random IP addresses. If the host is vulnerable, it will send again the code to another random IP address. This rule looks for 2 events. The two events are targeting the port 1433 or 1434 using UDP and the attacker is not in the 'Attackers/Trusted List' active list. An event matches if the target of the first event is the attacker of the second event. This rule requires 1 matching occurrence and the time frame is set to 1 minute. On Time Window Expiration, the target of the first event will be added to the 'Targets/Compromised List' active list.
Worm Outbreak Detected	This rule is looking for both the Possible Network Sweep rule to fire and the Target Port Activity by Attacker data monitor to trigger a correlation event that indicates an increase in target port activity by one attacker of more than 100%. Joining the attackers and target ports from these two correlation events determines that the attacker has shown an increase in target port traffic to multiple hosts, not just a two-way communication with a single host. This behavior is indicative of a worm infected system.

Cases

The Intrusion Monitoring foundation contains several rules that generate a case when a high severity attack is detected. If a high severity attack occurs, the cases opened are stored in the high severity attack group.



Intrusion Monitoring Reports

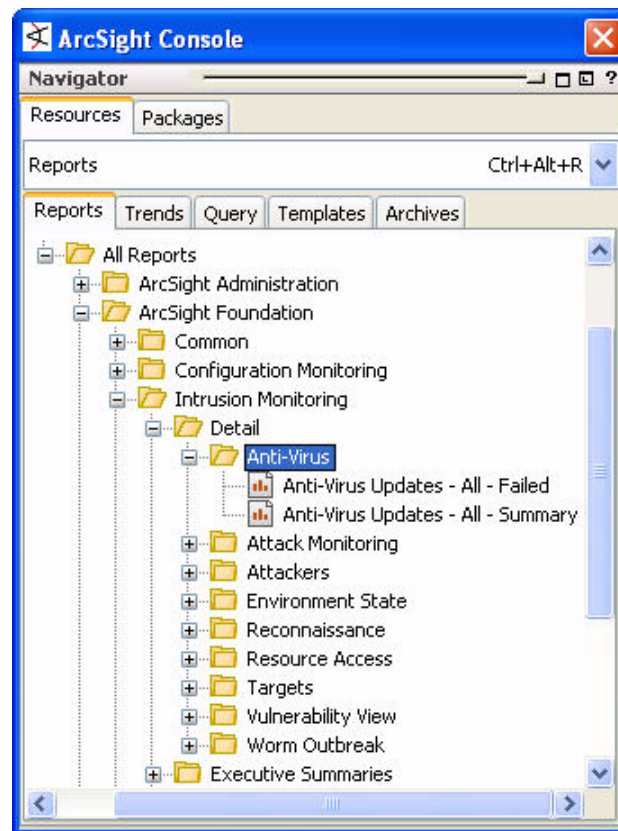
Intrusion monitoring reports display historical summaries of intrusion-related activity over varying time periods with varying detail for the major Intrusion Monitoring use cases. They are intended to be used for daily operational reporting and statistics gathering, as well as executive-level reporting.

Detail Reports

The Detail reports provide granular statistics (often hourly) of intrusion-related activity on the network.

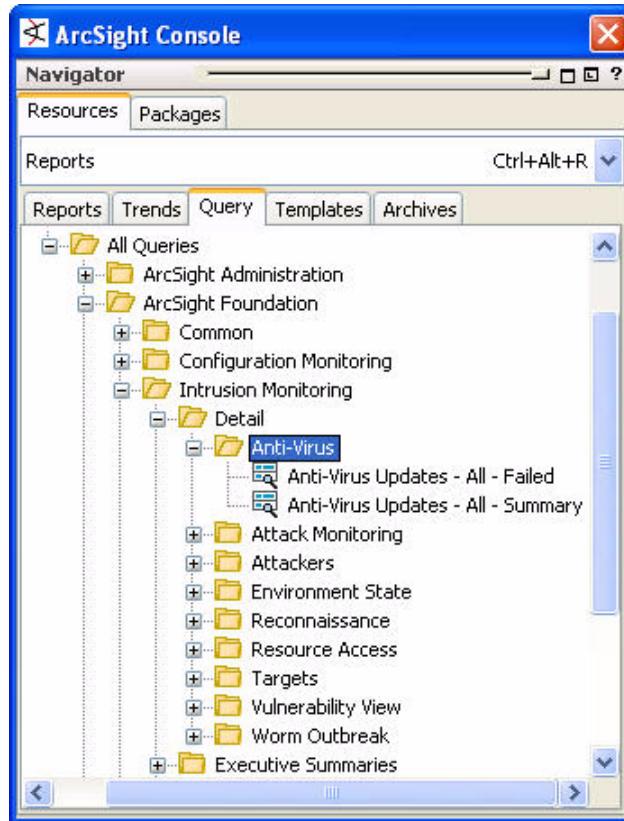
Anti-Virus Detail Reports

The Anti-Virus reports provide statistics about virus scans: those that failed, and a summary of virus scan activity.



Anti-Virus Detail Queries

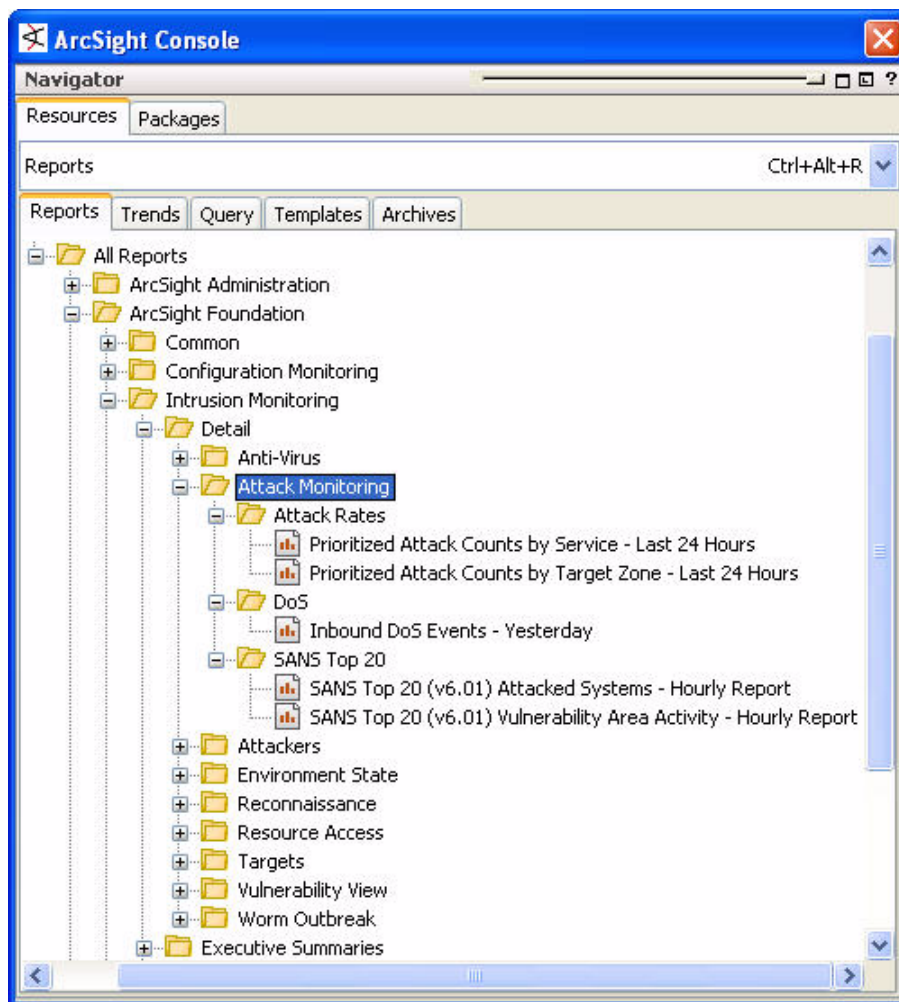
The Anti-Virus queries supply conditions for the Anti-Virus reports.



Attack Monitoring Detail Reports

The attack monitoring content compiles statistics for various types of attack-related activity. DoS reports are things you would monitor as they happen. The reports are hourly reports, although they can be edited to run over longer periods of data.

The Detail reports are designed to be reviewed hourly to get an idea of where intrusion weaknesses might be, especially if there has been a lot of compromise activity.



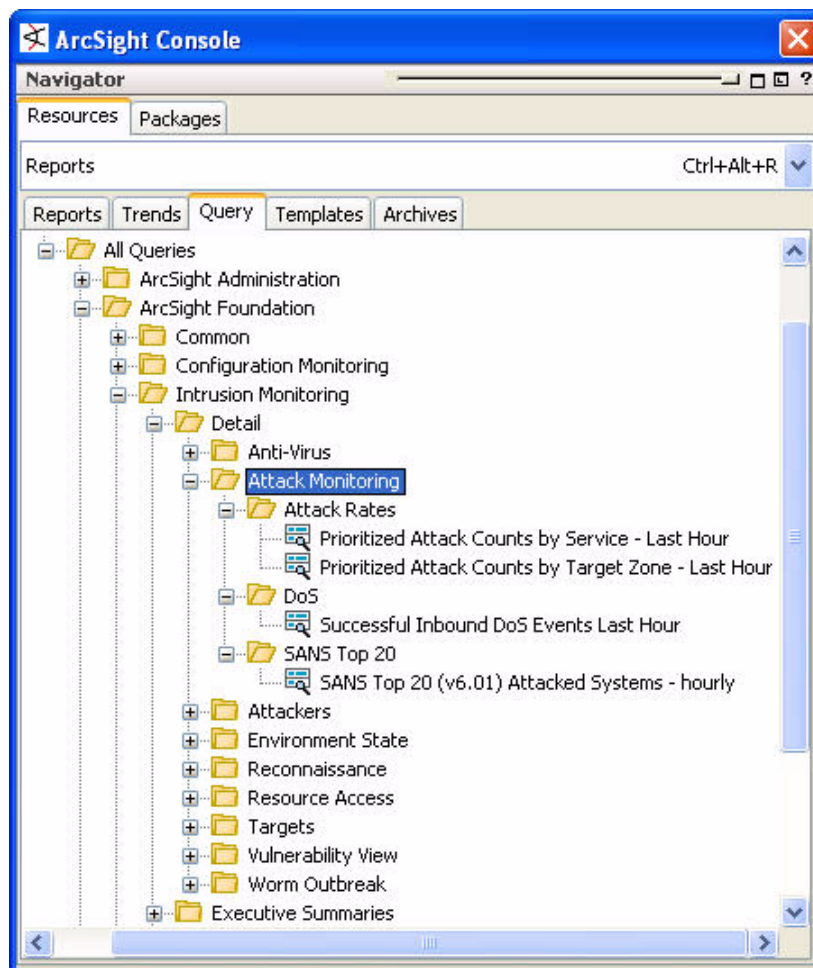
The Attack Monitoring Detail reports are described in more detail below:

Report	Description
Prioritized Attack Counts by Service - Last 24 Hours	This report displays a stacking bar chart of the target services by priority and the associated number of attack events for the previous day. The service displayed is a combination of the Transport Protocol, the Application Protocol and the Port number. A detailed table follows showing each target service and the number of attack events associated with it by priority for the same time period.

Report	Description
Prioritized Attack Counts by Target Zone - Last 24 Hours	This report displays a 3D stacking bar chart showing each target zone with the counts of the events separated by priority. A detailed table follows the chart, with the event counts for each zone subtotalled for each zone, with a total for all zones at the end.
Inbound DoS Events - Yesterday	This report displays a 3D stacking bar chart showing each target zone with the counts of the DoS events separated by service. A detailed table follows the chart, with the DoS event counts for each zone subtotalled for each zone, with a total for all zones at the end.
SANS Top 20 (v6.01) Attacked Systems - Hourly Report	This report is designed to give a view of the different SANS Top 20 Vulnerabilities and how many attacks for each vulnerability have occurred in the last 60 minutes. This report has a 3D Bar Chart showing the number of machines that have been attacked using one of the SANS Top 20 (v6.01) vulnerabilities. It also has a table with the same information, but with a grouping of vulnerabilities by area (Operating System, Email, RDBMS, etc.). The data used is generated by events from the SANS Top 20" rules.
SANS Top 20 (v6.01) Vulnerability Area Activity - Hourly Report	This report is designed to give a view of the different SANS Top 20 Vulnerability areas (Operating System, Email, etc.), and how many attacks for each area have occurred in the last 60 minutes. This report has a 3D Bar Chart showing the number of machines that have been attacked using one of the SANS Top 20 (v6.01) vulnerabilities in each area. It also has a table with more detailed information (the area, the vulnerability name and the number of attacks). The data used is generated by events from the SANS Top 20" rules.

Attack Monitoring Detail Queries

The Attack Monitoring queries supply conditions for the Attack Monitoring detail reports.



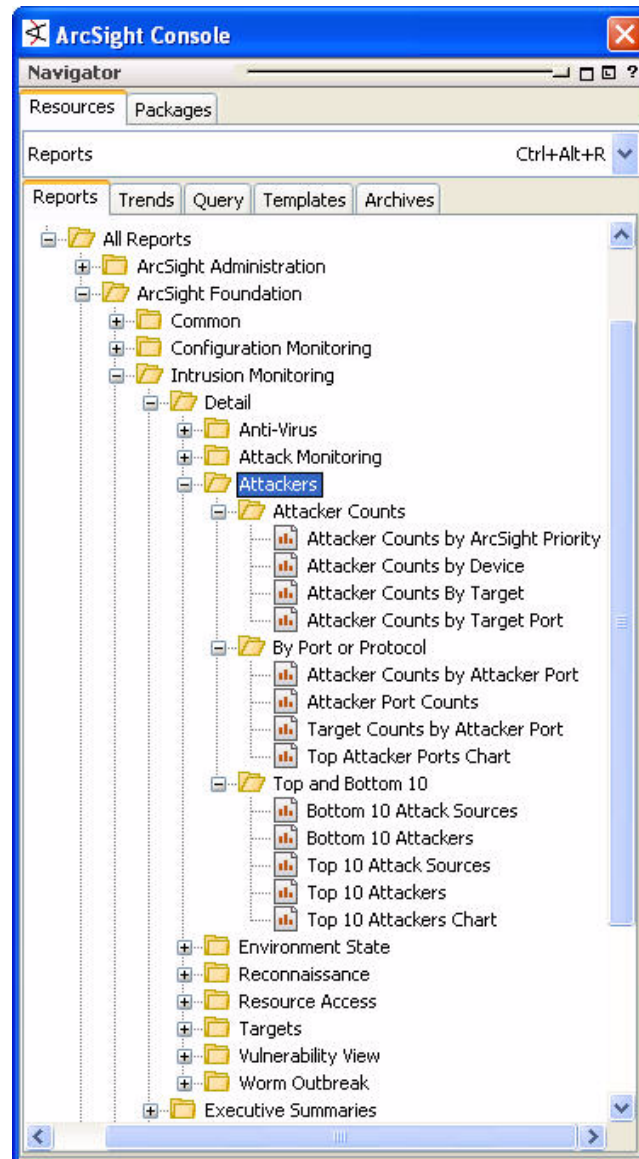
The Attack Monitoring Detail queries are described in more detail below:

Query	Description
Attack Counts by Service Query on Trend	This query on the Prioritized Attack Counts by Service trend selects the hour, the service name (Application Protocol Name/Transport Protocol Name: Target Port) and sums the number of events for that service for the Trend: Prioritized Attack Counts by Service - Last 24 Hours report.
Attack Counts by Target Zone Query on Trend	This query on the Prioritized Attack Counts by Target Zone trend selects the hour, the Target Zone Name and sums the number of events for that service for the Trend: Prioritized Attack Counts by Target Zone - Last 24 Hours report.
Prioritized Attack Counts by Service Query on Trend	This query on the Prioritized Attack Counts by Service trend selects the hour, the service name (Application Protocol Name/Transport Protocol Name: Target Port), the priority and sums the number of events for that service for the Trend: Prioritized Attack Counts by Service - Last 24 Hours report.

Query	Description
Prioritized Attack Counts by Target Zone Query on Trend	This query on the Prioritized Attack Counts by Target Zone trend selects the hour, the Target Zone Name, the priority and sums the number of events for that service for the Trend: Prioritized Attack Counts by Target Zone - Last 24 Hours report.
Prioritized Attack Counts by Service - Trend	This query is used to populate the trend Prioritized Attack Counts by Service. It selects the Hour (a DV based on the event's end time), the Service (a DV based on the service name or application protocol, the transport protocol and the port, e.g., HTML/TCP:80), the Priority and Sums the Aggregated Event Count. The Hour DV is used so that the data can be plotted based on the hour in which the event occurred, not the trend timestamp (the time the event data was stored in the trend).
Prioritized Attack Counts by Target Zone - Trend	This query is used to populate the trend Prioritized Attack Counts by Target Zone. It selects the Hour (a DV based on the event's end time), the Target Zone Name, the Priority and Sums the Aggregated Event Count. The Hour DV is used so that the data can be plotted based on the hour in which the event occurred, not the trend timestamp (the time the event data was stored in the trend).
Successful Inbound DoS Events Query on Trend	This query on the Inbound DoS Events trend selects the Target Zone Name, the Target Asset Name (or its IP address), the service name (Application Protocol Name/ Transport Protocol Name: Target Port), a timestamp and sums the number of Denial so Service events against the services on that asset during the time-period (hourly), for the Trend: Inbound DoS Events - Yesterday report.
Successful Inbound DoS Events - Trend	This query selects the data for reporting the target zone name, the asset name (or IP address), the service name and a summary of event counts. This data is used to populate the Inbound DoS Events trend.
SANS Top 20 (v6.01) Attacked Systems - daily trend	This trend collects information about the SANS Top 20 vulnerability areas and vulnerability names and the number of attacks for each vulnerability on an hourly basis. The data used is generated by events from the SANS Top 20 rules.

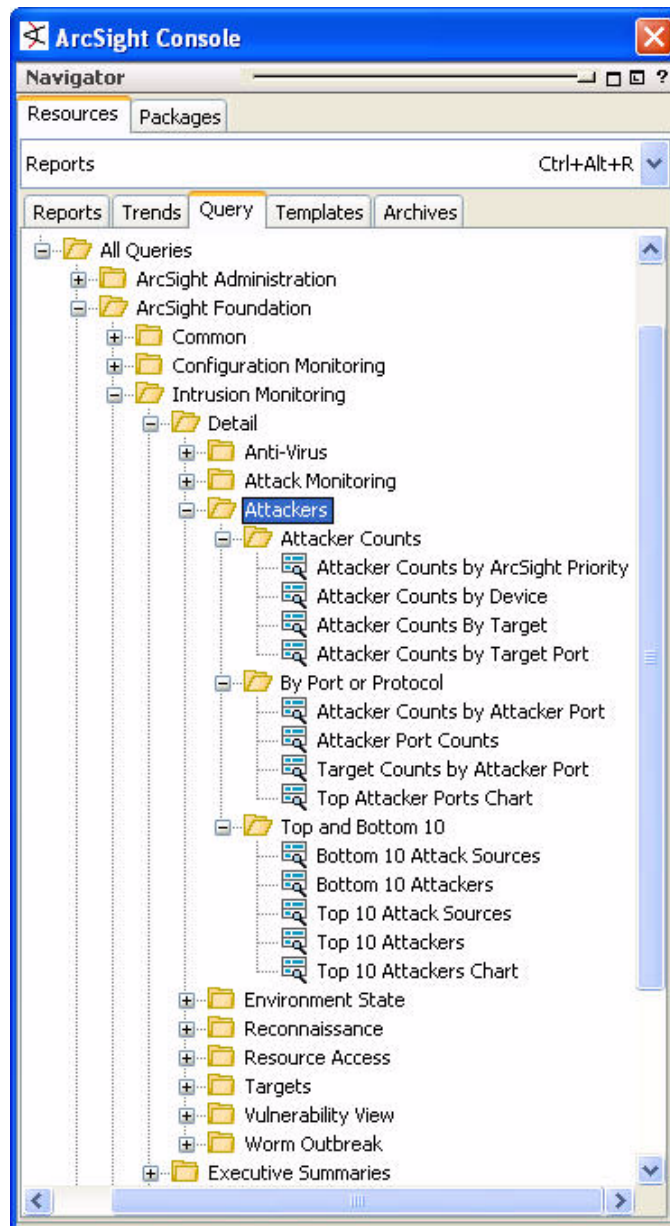
Attackers Detail Reports

The Attackers detail reports provide statistics about attacks, including counts, top and bottom activity, ports, and protocols.



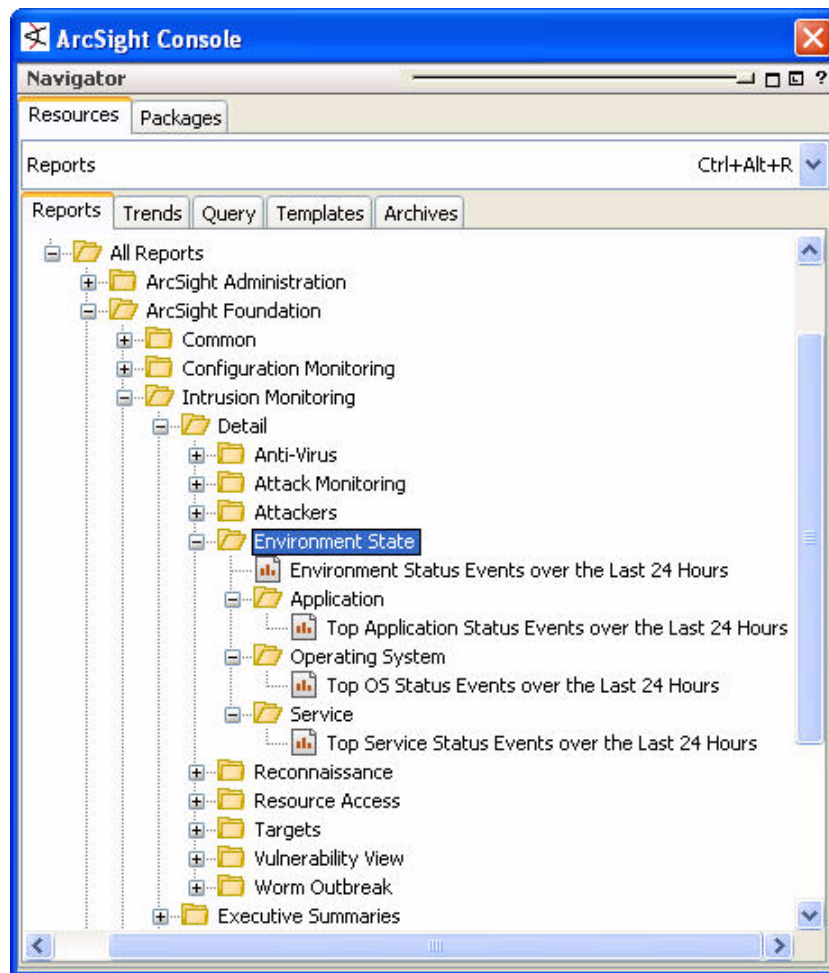
Attackers Detail Queries

The Attackers queries provide the conditions for the Attackers detail reports.



Environment State Detail Reports

The environment state detail reports provide summaries about the state of the overall network, and statistics about applications, operating systems and services.



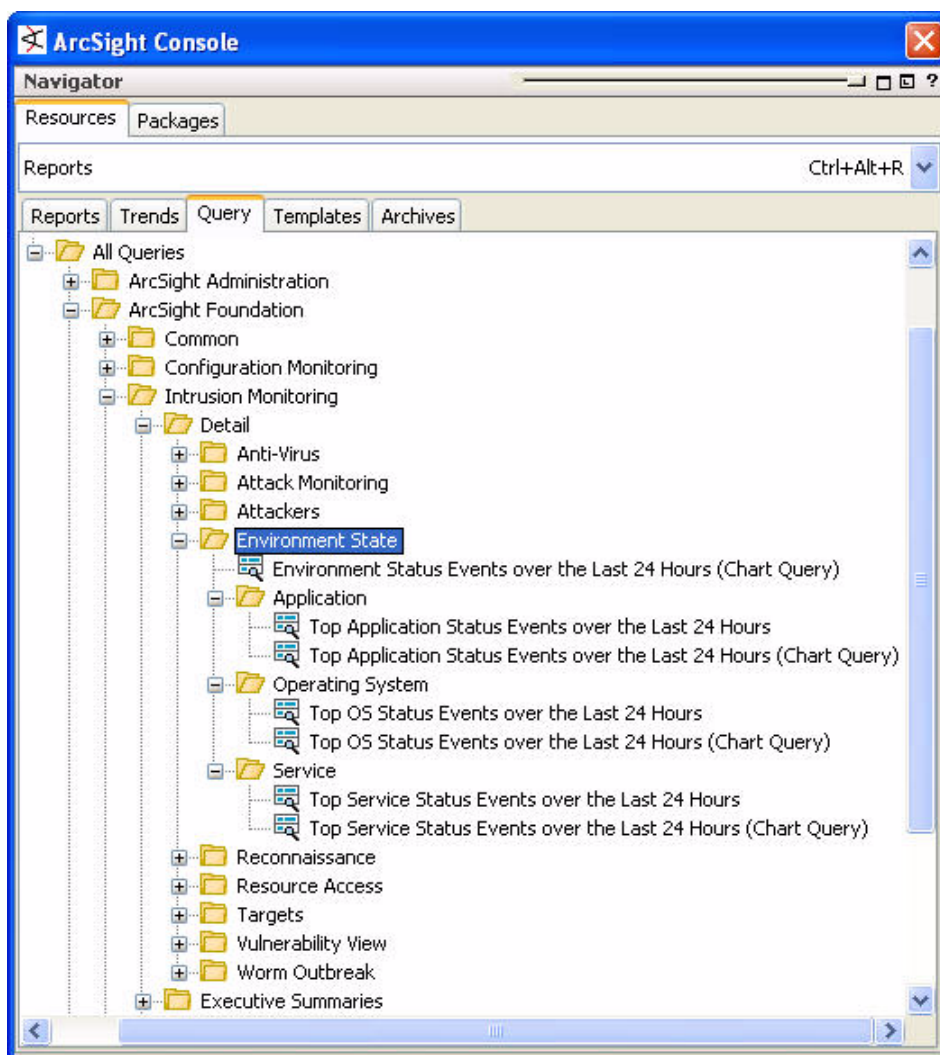
The Environment State Detail reports are described in more detail below:

Report	Description
Environment Status Events over the Last 24 Hours	This report displays four 3D stacked bar charts. The first shows each target zone with the event counts for the network. The remaining charts show the application, operating system or service events separated by zones.
Top Application Status Events over the Last 24 Hours	This report displays a 3D stacked bar chart showing each target zone with the event counts separated by application. A detailed table follows the chart, with each application and host in descending order by the event counts.
Top OS Status Events over the Last 24 Hours	This report displays a 3D stacked bar chart showing each target zone with the event counts separated by operating system. A detailed table follows the chart, with each OS and host in descending order by the event counts.

Report	Description
Top Service Status Events over the Last 24 Hours	This report displays a 3D stacked bar chart showing each target zone with the event counts separated by service. A detailed table follows the chart, with each service and host in descending order by the event counts.

Environment State Detail Queries

The Environment State Detail Queries provide conditions for the Environment State detail reports.

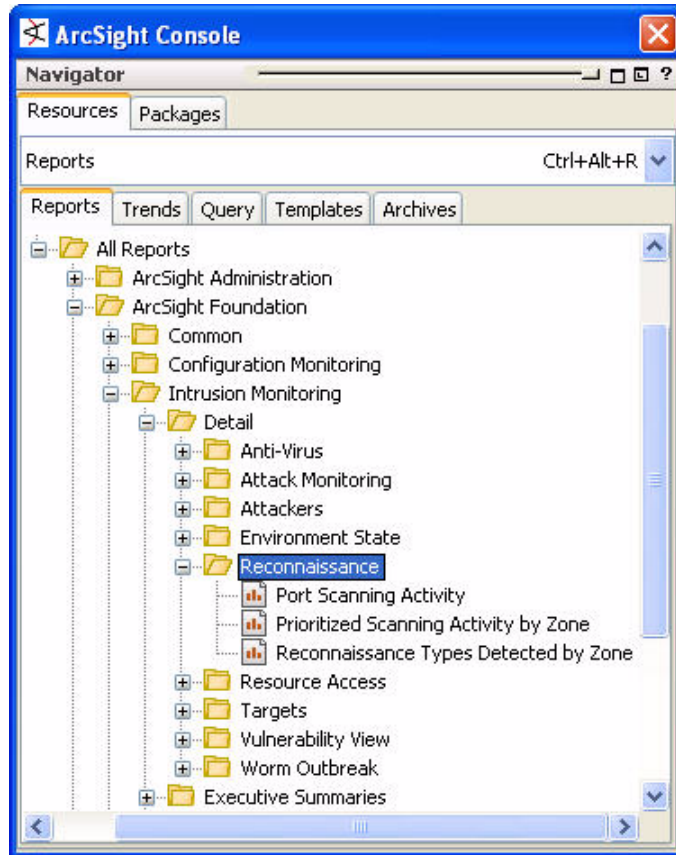


The Environment States Detail queries are described in more detail below:

Query	Description
Top Application Status Events on Trend	This query on the Environment Status Events trend selects the Target Zone Name, the trend type name (dvLabel-Name), the time and sums the number of events for that zone in the time-range for the Trend: Top Application Status Events over the Last 24 Hours report.
Top Status Events on Trend	This query on the Environment Status Events trend selects the Target Zone Name, the trend type (application, operating system, service), the time and sums the number of events for that zone in the time-range for the Trend: Environment Status Events - Yesterday report.
Environment Status Events - Trend	This query selects the data for reporting the Target Zone Name, the time (expressed within a dependent variable), the service, operating system or application name (another dependent variable field) and a summary of the event counts for overview information to populate the trend Environment Status Events. This query uses the Events for Internal Operating Systems, Events for Internal Applications excluding services and Events for Internal Services filters to limit events to those relating to the network environment state.
Top Operating System Status Events on Trend	This query on the Environment Status Events trend selects the Target Zone Name, the trend type name (dvLabel-Name), the time and sums the number of events for that zone in the time-range for the Trend: Top OS Status Events over the Last 24 Hours report.
Top Service Status Events on Trend	This query on the Environment Status Events trend selects the Target Zone Name, the trend type name (dvLabel-Name), the time and sums the number of events for that zone in the time-range for the Trend: Top Service Status Events over the Last 24 Hours report.

Reconnaissance Detail Reports

The Reconnaissance detail reports provide statistics about reconnaissance-type activity.

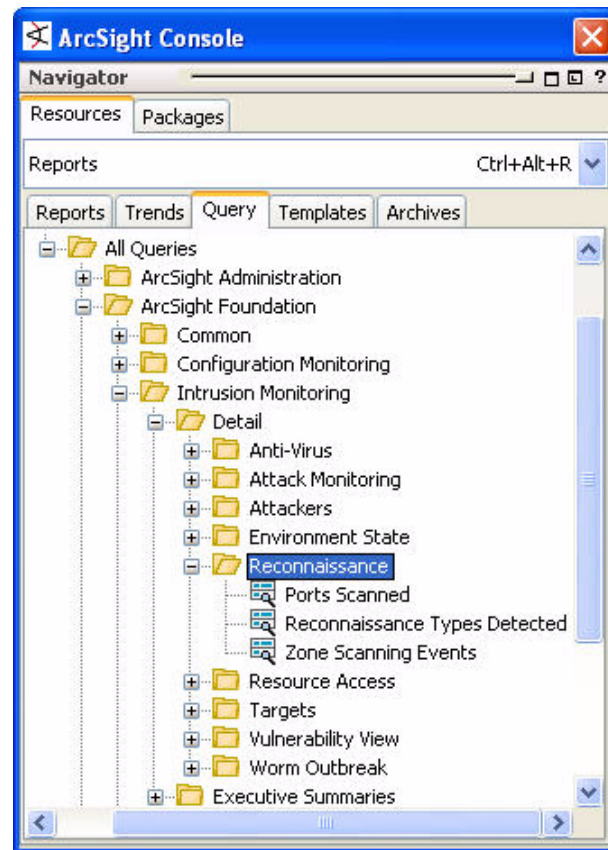


The Reconnaissance Detail reports are described in more detail below:

Report	Description
Port Scanning Activity	This report presents a chart of the most frequently occurring events for transport protocol/target port pairs by zone, and a table with more data points for additional information beyond that presented in the chart.
Prioritized Scanning Activity by Zone	This report presents a chart and table showing the numbers of events, by priority and target zone, over the past hour. The table shows the zones in order of highest event counts by the priority of the events (from highest priority to lowest).
Reconnaissance Types Detected by Zone	This report presents a chart with the event activity over the past hour of the different reconnaissance types (based on the ArcSight System rules with names beginning with "Reconnaissance - " and differentiated by the type names Distributed Host Port Scan, Distributed Network Host Scan, Multiple Host Scan, Network Service Scan, Script Scan, Stealthy Host Port Scan and Vulnerability Scan), and a table showing the breakdown and zone information charted.

Reconnaissance Detail Queries

The Reconnaissance detail queries provide conditions for the Reconnaissance detail reports.

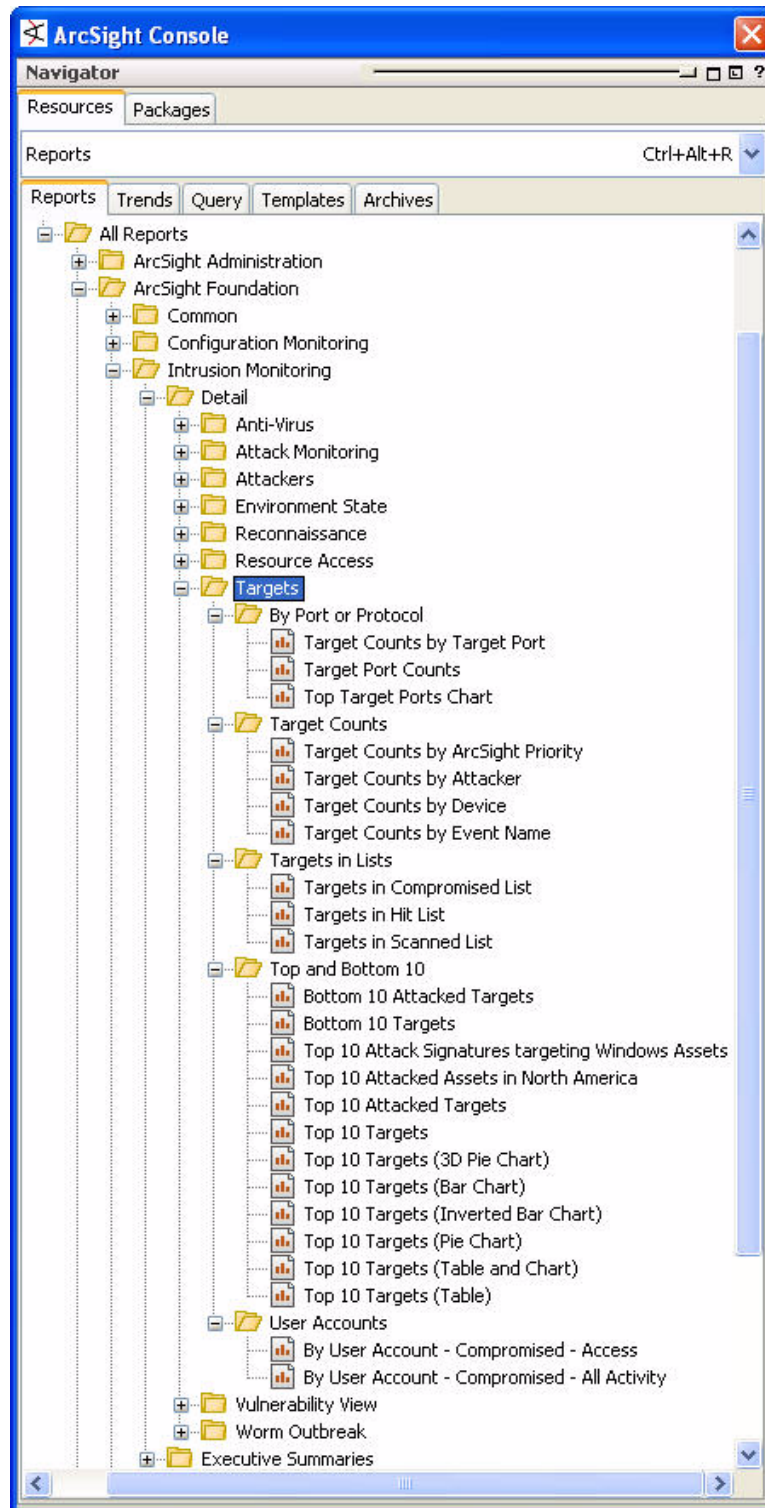


The Reconnaissance Detail queries are described in more detail below:

Query	Description
Business Roles Scanned	This query selects the business role via a dependent variable (dvBusinessRole), the priority, and sums the aggregated event count of events matching the Reconnaissance Events (Internal Target) filter targeting assets categorized by the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/ category.
Daily Port Scanning Activity on Trend	This query selects the date via a dependent variable (dvDate), the target zone resource, the priority, the transport protocol, the target port, and sums the aggregated event count from the summary provided by the Port Scanning Daily Top 20 trend for the Daily Top 20 Protocol and Ports by Zone table in the Port Scanning Activity Trend report.
Daily Port Scanning Activity on Trend (Chart Query)	This query selects the date via a dependent variable (dvDate), the target zone resource, the priority, the transport protocol, the target port, and sums the aggregated event count from the summary provided by the Port Scanning trend for the Top 20 Protocol and Ports by Count from MM-DD-YYYY to MM-DD-YYY-HH:MM:SS chart in the Port Scanning Activity Trend report.
Daily Scanning Events by Business Role on Trend	This query selects the date via a dependent variable (dvMonthDay), the business role via a dependent variable (dvBusinessRole), and sums the aggregated event count of the data from the Reconnaissance Activity trend. This query provides both chart and table data for the Scanning Activity by Business Role Trend report.
Reconnaissance Types Detected on Trend	This query selects the date via a dependent variable (dvMonthDay), the target zone resource, the event name and the sum of the aggregated event count from the summary of the Reconnaissance Types Detected trend for the Daily Breakdown of Reconnaissance Types Detected table in the Reconnaissance Types Detected Trend report.
Reconnaissance Types Detected on Trend (Chart Query)	This query selects the date via a dependent variable (dvMonthDay), the reconnaissance type (event name), and a sum of the aggregated event count from summary information in the Reconnaissance Types Detected trend. This query provides data for the Daily Reconnaissance Types Detected chart in the Reconnaissance Types Detected Trend report.
Port Scanning Daily Top 20, Trend on Trend	This query selects the target zone resource, priority, transport protocol, target port, and sums the aggregated event count for the summary data from the Port Scanning trend to populate the Port Scanning Daily Top 20 trend.

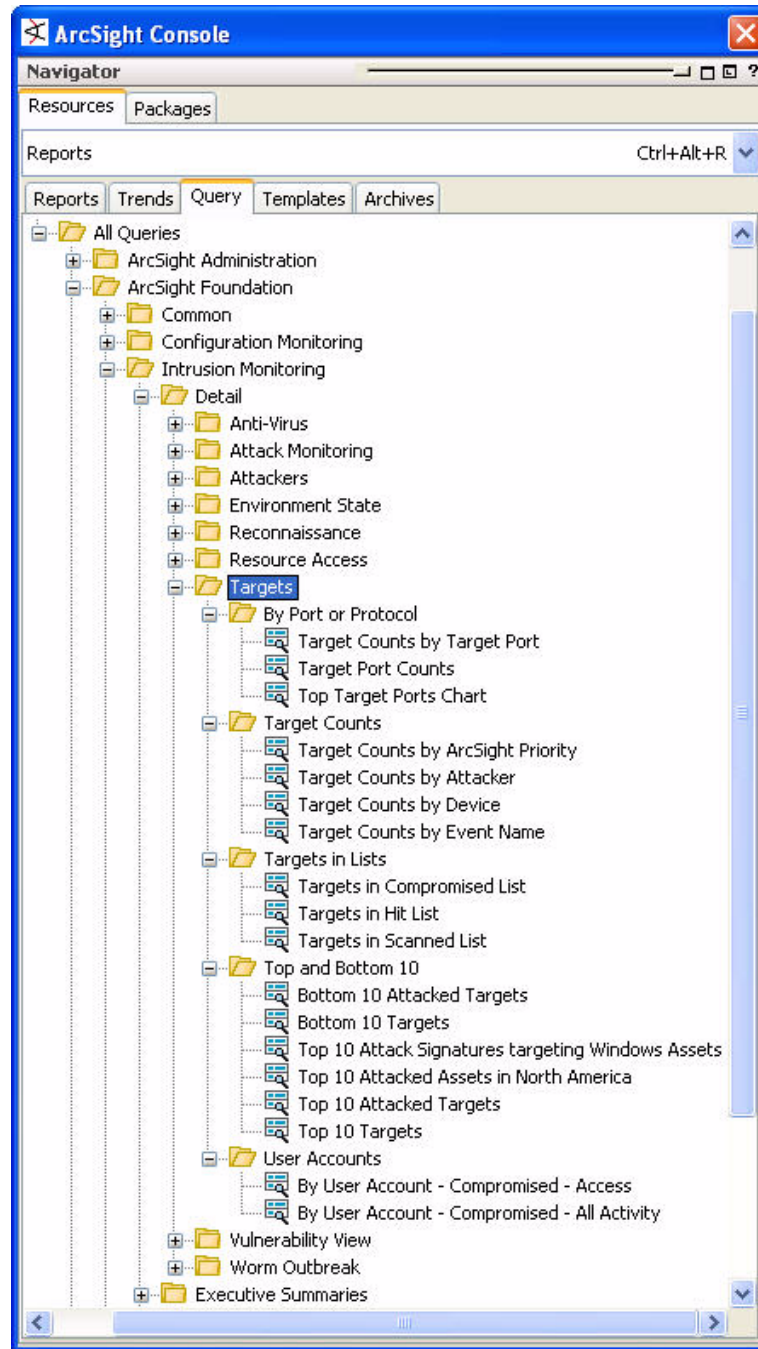
Target Detail Reports

The Target detail reports provide statistics about targets.



Target Detail Queries

The Target detail queries provide conditions for the Targets reports.



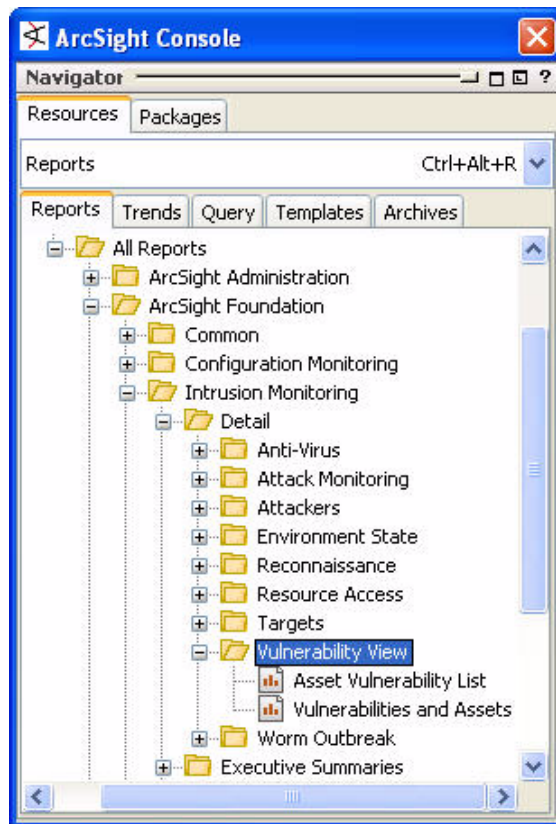
Vulnerability View Detail Reports

These reports provide a list of all assets with vulnerabilities and all vulnerabilities and the asset they are associated with.

Scanner reports (the source of the scanner events) are considered sensitive, so access to these reports should be restricted. Read, and in some cases, write, access to these reports should be restricted. For instructions about how to set this up, see [“Restrict Access to Vulnerability View Reports” on page 125](#).



Depending on how many assets you have scanned into your asset model and how up-to-date their vulnerability profiles, running these reports can produce a large volume of output. Before running the report, ensure that the system has adequate processing power, and check the page count before sending the report to a printer.

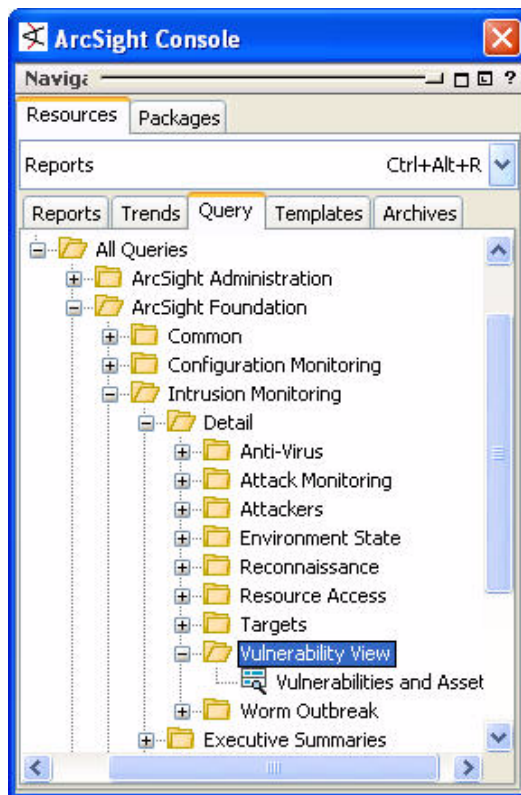


The Vulnerability View Detail reports are described in more detail below:

Report	Description
Asset Vulnerability List	This report presents a table of each asset, by zone, and all the vulnerabilities that have been reported for the asset. This is an exhaustive list that can get extremely large, so beware printing it if there are hundreds or thousands of assets in the network!
Vulnerabilities and Assets	This report presents a table of each vulnerability that has been reported for any asset and all the assets, by zone, affected by the vulnerability. This is an exhaustive list that can get extremely large, so beware printing it if there are hundreds or thousands of assets in the network!

Vulnerability View Detail Query

This query supplies conditions for the Vulnerability View reports.

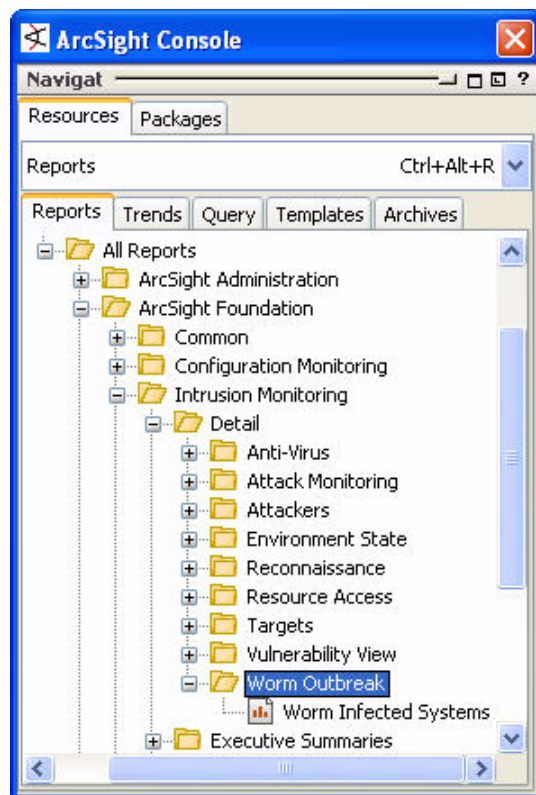


The Vulnerability View Detail query is described in more detail below:

Query	Description
Vulnerabilities and Assets	This is an asset query that selects the vulnerability, the asset's zone, the asset's address, the asset's ID, the asset's host name and the count of the asset's ID to get an exhaustive list of the assets and associated vulnerabilities. The asset ID count is used to retrieve assets that may not yet have any vulnerabilities reported. The asset ID is included for future expansion should it be necessary to modify or create a report to display the asset ID along with the other data for verification or investigation purposes. This query is used by two reports, the Asset Vulnerability Lists report and the Vulnerabilities and Assets report, to give two different views of the assets and vulnerabilities. Note that this is an asset query and that as vulnerability reports come in and assets are added or removed from the network, the data will change. It only takes a snapshot of the assets and vulnerabilities reported to the system at the time the report query is run. It is not possible to run this query to see what the status was at any point in the past. For that, we recommend scheduling the report to run periodically for tracking these changes. The efficacy of this will also depend on the number of assets involved.

Worm Outbreak Detail Report

The Worm Outbreak detail report shows worm-infected systems.

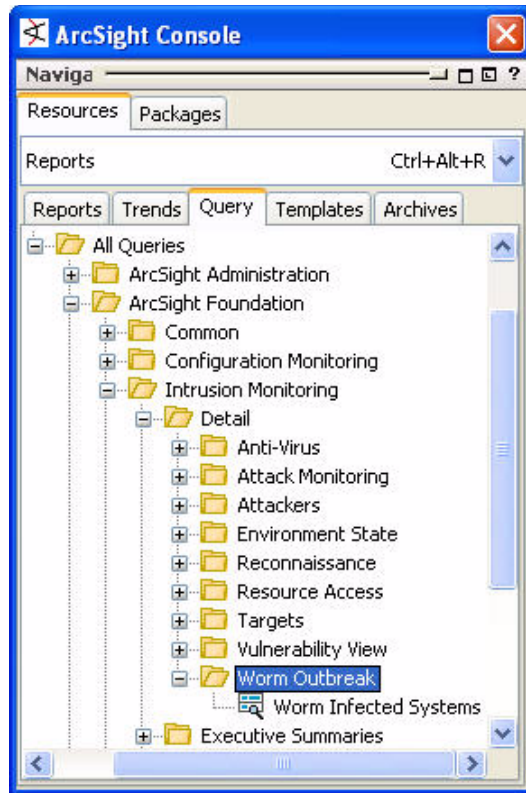


The Worm Outbreak Detail report is described in more detail below:

Report	Description
Worm Infected Systems	This report presents a table of systems that have been infected by a worm. The table is sorted by the Attacker Zone Name, then by the Attacker Host Name and finally by the Attacker Address (for cases where the system does not have a host name). The parameters are set so that the user can change the start and end times of the event query. The row limit is also modifiable, so that more or fewer systems are shown. Also, the FilterBy parameter is available so that the user can create an additional filter to limit the report to specific systems (i.e., filter by zone, asset criticality, etc.). Changing the FilterBy parameter will cause the query to select events that match both the selected filter and the Worm Traffic filter (Worm Traffic AND selected filter).

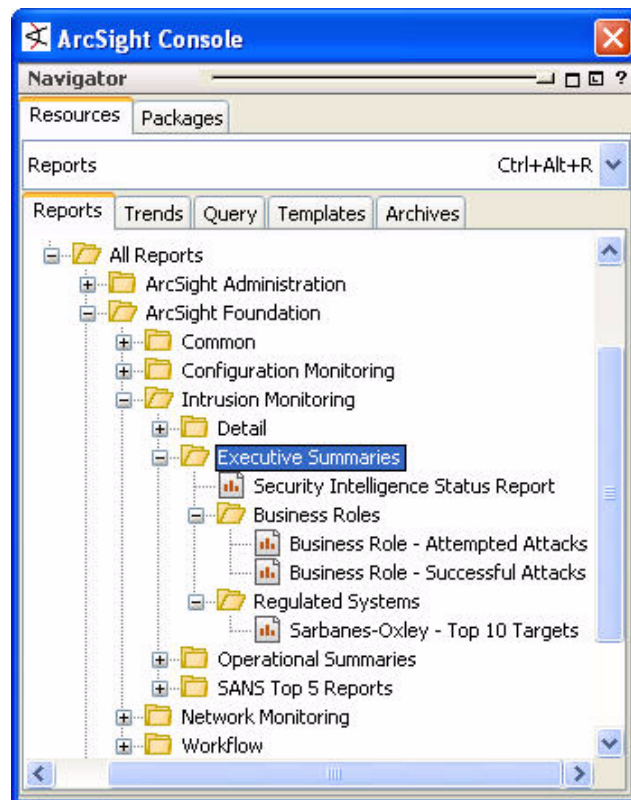
Worm Outbreak Detail Query

The Worm Outbreak query provides conditions for the Worm Outbreak report.



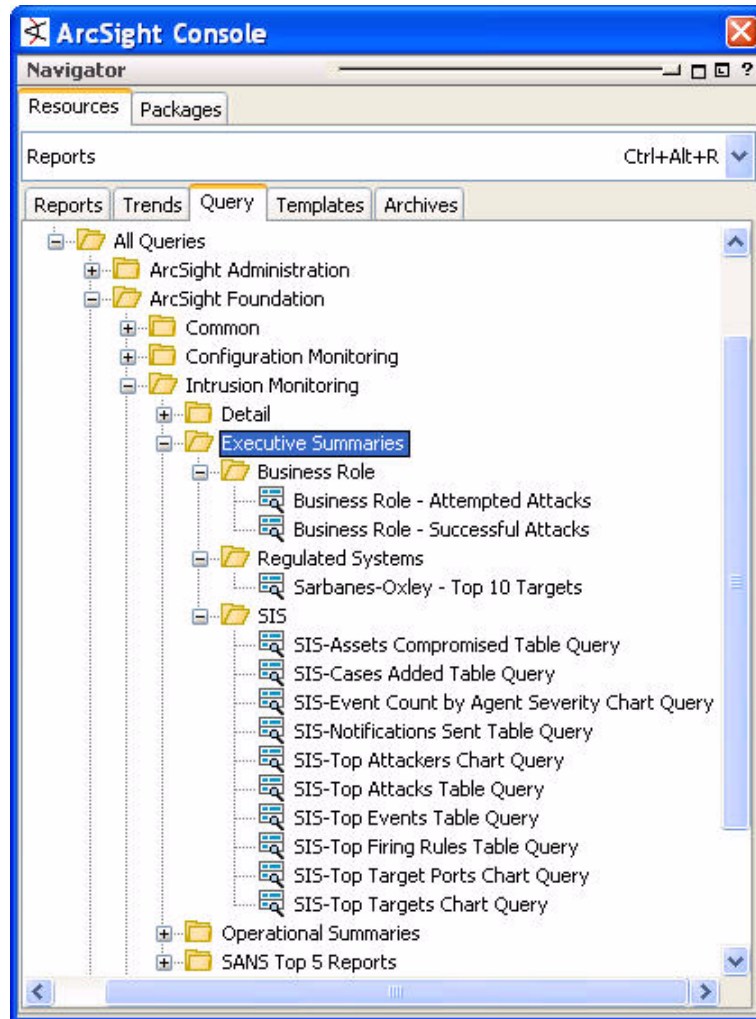
Executive Summary Reports

The Executive Summary reports show high-level summaries of the Intrusion Monitoring statistics for your network.



Executive Summary Queries

The Executive Summary queries supply conditions for the Executive Summary reports.



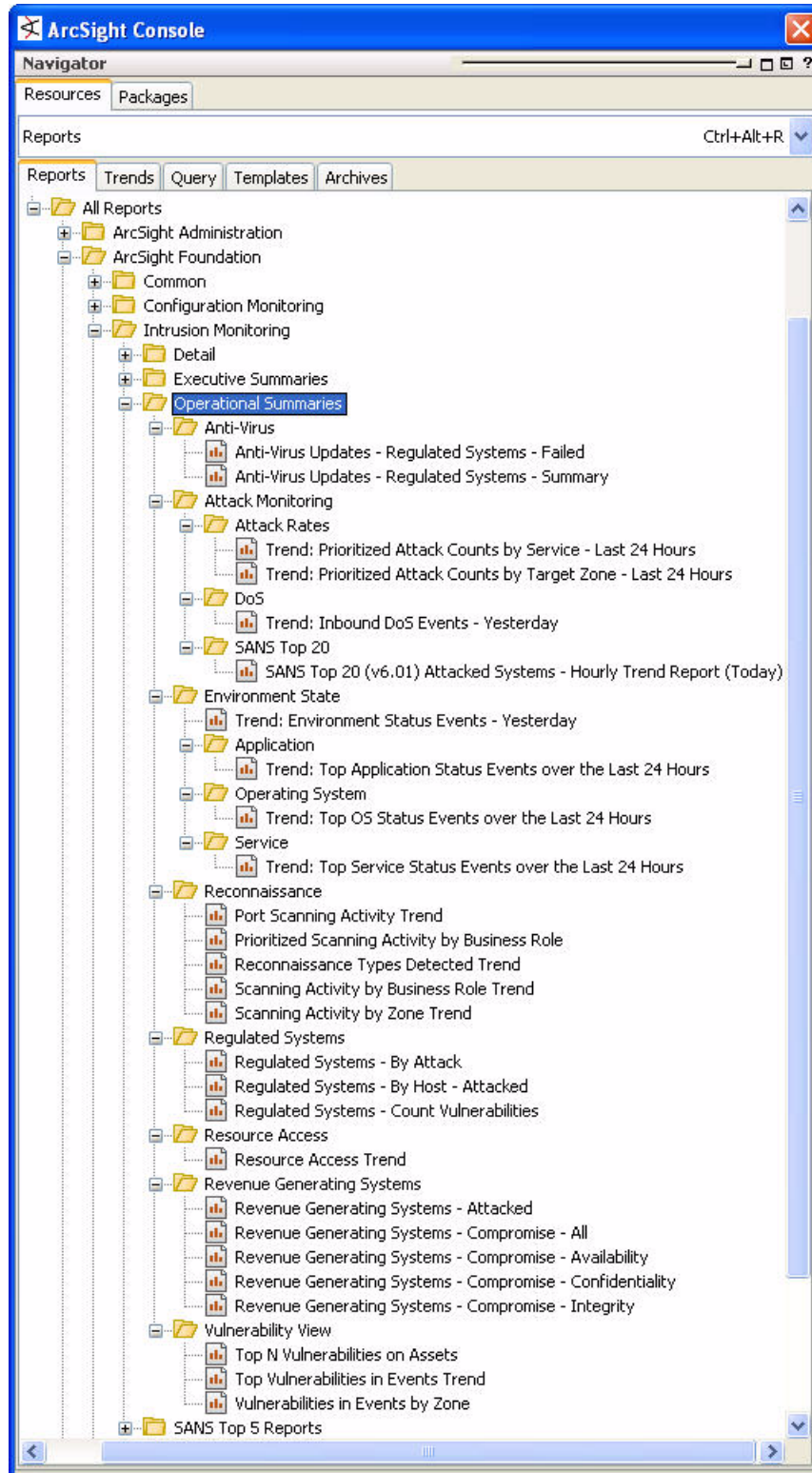
These queries are described in more detail below:

Query	Description
Business Role - Attempted Attacks	
Business Role - Successful Attacks	
Sarbanes-Oxley - Top 10 Targets	
SIS-Assets Compromised Table Query	This query on events selects the Target Asset Name, the Vulnerability External ID (the vulnerability name), and a sum of the number of events reported for that asset/vulnerability pair for use in the Security Intelligence Status Report.
SIS-Cases Added Table Query	This query on cases selects the Stage, the Consequence Severity and a count of the cases with that pairing for use in the Security Intelligence Status Report.

Query	Description
SIS-Event Count by Agent Severity Chart Query	This query on events selects the date (Dependent Variable - dvDayHour), the Agent Severity and the number of events for each agent severity level for that day/hour for use in the Security Intelligence Status Report.
SIS-Notifications Sent Table Query	This query on notifications selects the Group Name, the Escalation Level, the Acknowledgement Status and a count of the notifications for these conditions for use in the Security Intelligence Status Report.
SIS-Top Attackers Chart Query	This query on events selects the Attacker Zone Name, the Attacker address and sums the Aggregated Event Count for use in the Security Intelligence Status Report.
SIS-Top Attacks Table Query	This query on events selects the event Name and sums the Aggregated Event Count that have a category significance of / Compromise or /Hostile for use in the Security Intelligence Status Report.
SIS-Top Events Table Query	This query on events selects the event Name and sums the Aggregated Event Count for use in the Security Intelligence Status Report.
SIS-Top Firing Rules Table Query	This query on events selects the event Name and sums the Aggregated Event Count where the type is Correlation for use in the Security Intelligence Status Report.
SIS-Top Target Ports Chart Query	This query on events selects the Target Port and sums the Aggregated Event Count for use in the Security Intelligence Status Report.
SIS-Top Targets Chart Query	This query on events selects the Target Zone Name, the Target Address and sums the Aggregated Event Count for use in the Security Intelligence Status Report.

Intrusion Monitoring Operational Summary Reports

The Intrusion Monitoring Operational Summary reports show medium-level summaries of Intrusion Monitoring activity on your network.



The Operational Summary reports are described in more detail below.

Report	Description
Trend: Prioritized Attack Counts by Service - Last 24 Hours	This report displays a 3D stacking bar chart of the target zones and the associated number of service events per hour. Each line of the chart represents a target zone (see the legend for the zone names). A detailed table follows showing each target zone and the number of attack events associated with it by hour and priority.
Trend: Prioritized Attack Counts by Target Zone - Last 24 Hours	This trend report displays a line chart of the target zones and the associated number of attack events per hour. Each line of the chart represents a target zone (see the legend for the zone names). A detailed table follows showing each target zone and the number of attack events associated with it by hour and priority.
Trend: Inbound DoS Events - Yesterday	This trend report displays a line chart of the target zones and the associated number of DoS events per hour. Each line of the chart represents a target zone (see the legend for the zone names). A detailed table follows showing each target zone and the number of DoS events associated with it by hour and service.
SANS Top 20 (v6.01) Attacked Systems - Hourly Trend Report (Yesterday)	
Trend: Environment Status Events - Yesterday	This report displays four 3D stacked bar charts. The first shows each target zone with the event count trend for the network. The remaining charts show the application, operating system or service event trends separated by zones.
Trend: Top Application Status Events over the Last 24 Hours	This report displays a 3D stacked bar chart showing each target zone with a trend of the event counts separated by application. A detailed table follows the chart, with each application and host in descending order by the event counts.
Trend: Top OS Status Events over the Last 24 Hours	This report displays a 3D stacked bar chart showing each target zone with a trend of the event counts separated by operating system. A detailed table follows the chart, with each OS and host in descending order by the event counts.
Trend: Top Service Status Events over the Last 24 Hours	This report displays a 3D stacked bar chart showing each target zone with a trend of the event counts separated by service. A detailed table follows the chart, with each service and host in descending order by the event counts.
Port Scanning Activity Trend	This trend report presents a chart showing the top transport protocol and target port pairs (Protocol - Port) by target zone over the last 7 days based on summary data from the Port Scanning trend. It also presents a table showing the daily summary of the top 20 prioritized event counts from each zone for the protocol - port pairs from the Port Scanning Daily Top 20 trend.
Prioritized Scanning Activity by Business Role	This report presents a chart and a table showing the activity levels and priorities of reconnaissance events directed at assets within the various business role categories.

Report	Description
Reconnaissance Types Detected Trend	This report presents a chart with the daily event activity summary of the different reconnaissance types (based on the ArcSight System rules with names beginning with "Reconnaissance - " and differentiated by the type names Distributed Host Port Scan, Distributed Network Host Scan, Multiple Host Scan, Network Service Scan, Script Scan, Stealthy Host Port Scan and Vulnerability Scan), over the past 7 days, and a table showing the daily breakdown and zone information charted.
Scanning Activity by Business Role Trend	This report displays a daily trend of scanning events related to business roles over the past 7 days, and a table giving a simple breakdown of the activity charted.
Scanning Activity by Zone Trend	This trend report shows a chart plotting the daily trend of the most frequent reconnaissance events, and a daily prioritized breakdown of those events by zone over the last 7 days. This report uses two separate queries, one for the table and a simpler one for the chart, on the Zone Scanning Events by Priority trend.
Regulated Systems - By Attack	
Regulated Systems - By Host - Attacked	
Regulated Systems - Count Vulnerabilities	
Resource Access Trend	This report displays a chart and a table of unusual resource access attempt trends for each of the past seven days. The chart presents a breakdown of the access attempt counts for the resource types by outcome. The table presents the top events, defined as the resource, user and outcome combinations occurring most frequently. The resource type, outcome, the user ID and name, resource zone and address, and count of attempts for that resource are shown. The range of outcomes are failure, attempt or success. An outcome of attempt means that there was not sufficient information to determine whether or not the attempt succeeded. Also note that an outcome of success means that there was enough information to know that the resource was indeed accessed, but something about the access initiation did not fit in the normal access initiation pattern.
Revenue Generating Systems - Attacked	
Revenue Generating Systems - Compromise - All	
Revenue Generating Systems - Compromise - Availability	
Revenue Generating Systems - Compromise - Confidentiality	

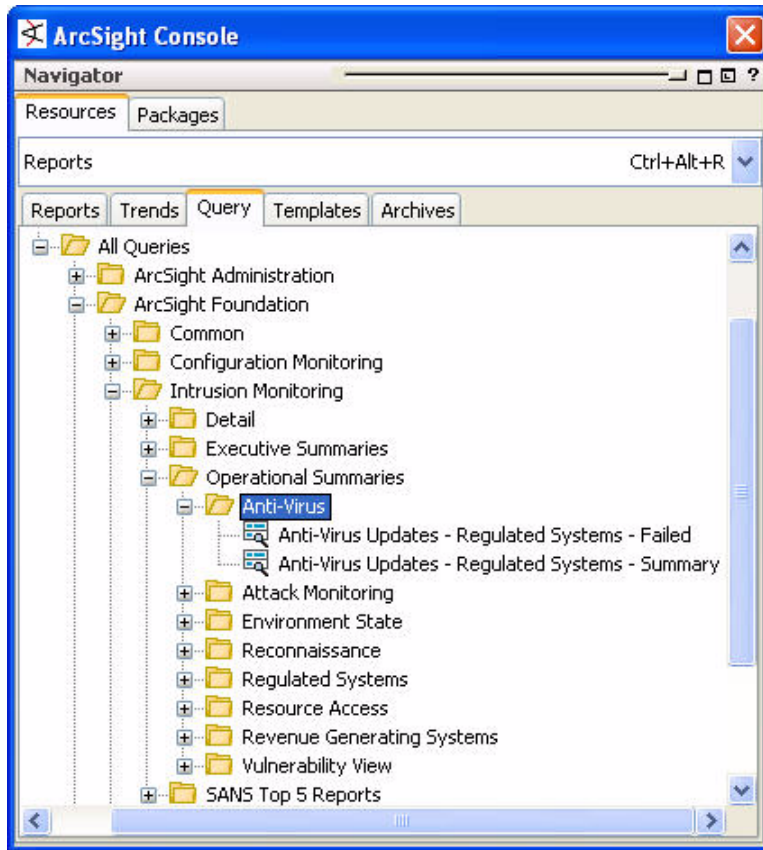
Report	Description
Revenue Generating Systems - Compromise - Integrity	
Top N Vulnerabilities on Assets	This report displays a table showing the most frequent vulnerability exploit attempts against the network. This data is collected from the Asset Counts by Vulnerability trend. This trend is a snapshot trend of the assets taken once per week.
Top Vulnerabilities in Events Trend	This trend report presents a chart and table showing the most frequent vulnerability exploit attempts on the network. The goal of this report is to show the vulnerabilities that are being targeted across the network in the last day or so to gain a better understanding of what the threat activity currently is. The chart gives the top few vulnerability exploit attempts (default is 10), and the number of times these attempts have been detected over the past day. The table gives a longer list (default is 25) of the trend data covered by the same period.
Vulnerabilities in Events by Zone	This report presents a chart and a table. The chart shows the vulnerability event counts seen on the network, by zone. The table shows the breakdown of the charted events by priority.

Operational Summary Queries

The Operational Summary queries provide conditions for the Operational Summary reports by use case.

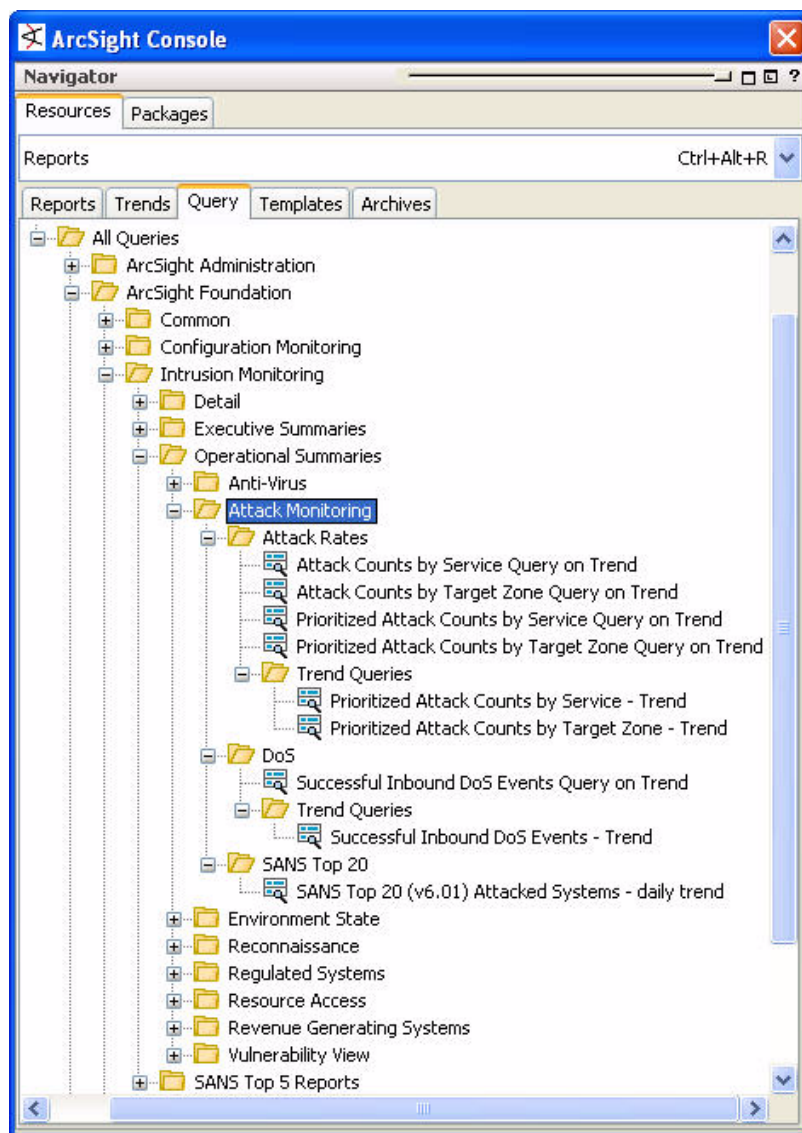
Anti-Virus Operational Summary Queries

The Anti-Virus Operational Summary queries supply conditions for the Anti-Virus Operational Summary reports.



Attack Monitoring Operational Summary Queries

The Attack Monitoring Operational Summary queries supply conditions for the Attack Monitoring Operational Summary reports.



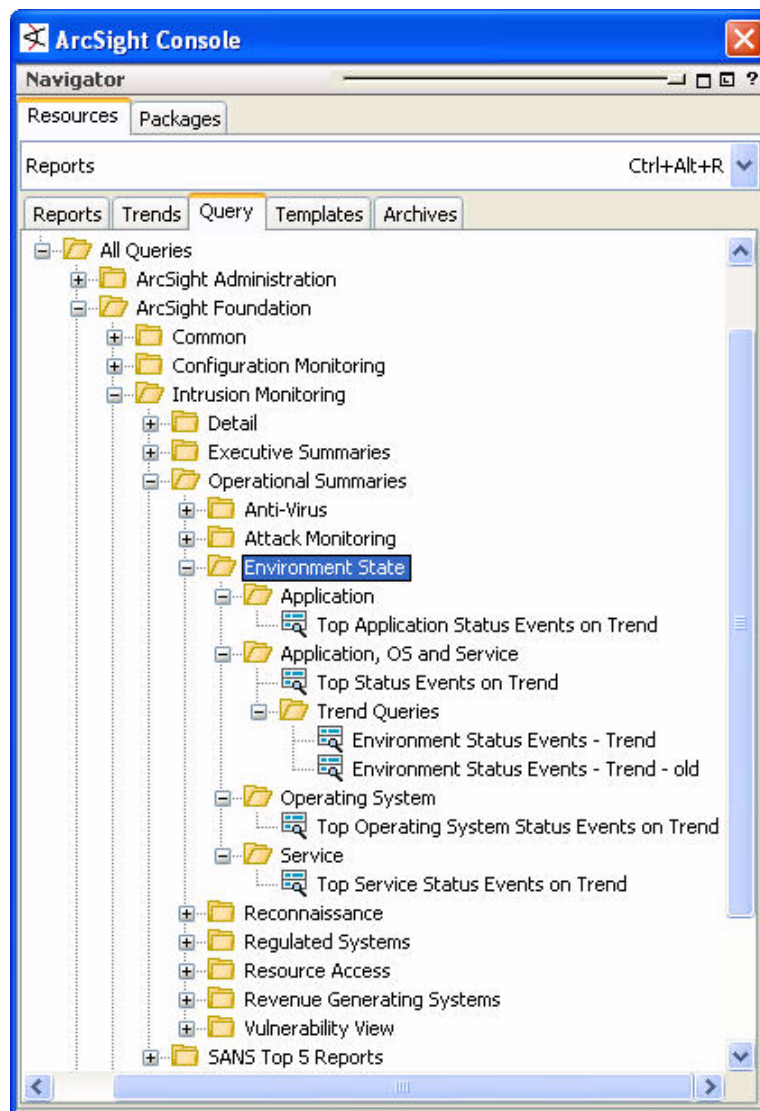
The Attack Monitoring Operational Summary queries are described in more detail below.

Query	Description
Attack Counts by Service Query on Trend	This query on the Prioritized Attack Counts by Service trend selects the hour, the service name (Application Protocol Name/ Transport Protocol Name: Target Port) and sums the number of events for that service for the Trend: Prioritized Attack Counts by Service - Last 24 Hours report.
Attack Counts by Target Zone Query on Trend	This query on the Prioritized Attack Counts by Target Zone trend selects the hour, the Target Zone Name and sums the number of events for that service for the Trend: Prioritized Attack Counts by Target Zone - Last 24 Hours report.

Query	Description
Prioritized Attack Counts by Service Query on Trend	This query on the Prioritized Attack Counts by Service trend selects the hour, the service name (Application Protocol Name/Transport Protocol Name: Target Port), the priority and sums the number of events for that service for the Trend: Prioritized Attack Counts by Service - Last 24 Hours report.
Prioritized Attack Counts by Target Zone Query on Trend	This query on the Prioritized Attack Counts by Target Zone trend selects the hour, the Target Zone Name, the priority and sums the number of events for that service for the Trend: Prioritized Attack Counts by Target Zone - Last 24 Hours report.
Prioritized Attack Counts by Service - Trend	This query is used to populate the trend Prioritized Attack Counts by Service. It selects the Hour (a DV based on the event's end time), the Service (a DV based on the service name or application protocol, the transport protocol and the port, e.g., HTML/TCP:80), the Priority and Sums the Aggregated Event Count. The Hour DV is used so that the data can be plotted based on the hour in which the event occurred, not the trend timestamp (the time the event data was stored in the trend).
Prioritized Attack Counts by Target Zone - Trend	This query is used to populate the trend Prioritized Attack Counts by Target Zone. It selects the Hour (a DV based on the event's end time), the Target Zone Name, the Priority and Sums the Aggregated Event Count. The Hour DV is used so that the data can be plotted based on the hour in which the event occurred, not the trend timestamp (the time the event data was stored in the trend).
Successful Inbound DoS Events Query on Trend	This query on the Inbound DoS Events trend selects the Target Zone Name, the Target Asset Name (or its IP address), the service name (Application Protocol Name/Transport Protocol Name: Target Port), a timestamp and sums the number of Denial so Service events against the services on that asset during the time-period (hourly), for the Trend: Inbound DoS Events - Yesterday report.
Successful Inbound DoS Events - Trend	This query selects the data for reporting the target zone name, the asset name (or IP address), the service name and a summary of event counts. This data is used to populate the Inbound DoS Events trend.
SANS Top 20 (v6.01) Attacked Systems - daily trend	This trend collects information about the SANS Top 20 vulnerability areas and vulnerability names and the number of attacks for each vulnerability on an hourly basis. The data used is generated by events from the SANS Top 20 rules.

Environment State Operational Summary Queries

The Environment State Operational Summary queries supply conditions for the Environment State Operational Summary reports.



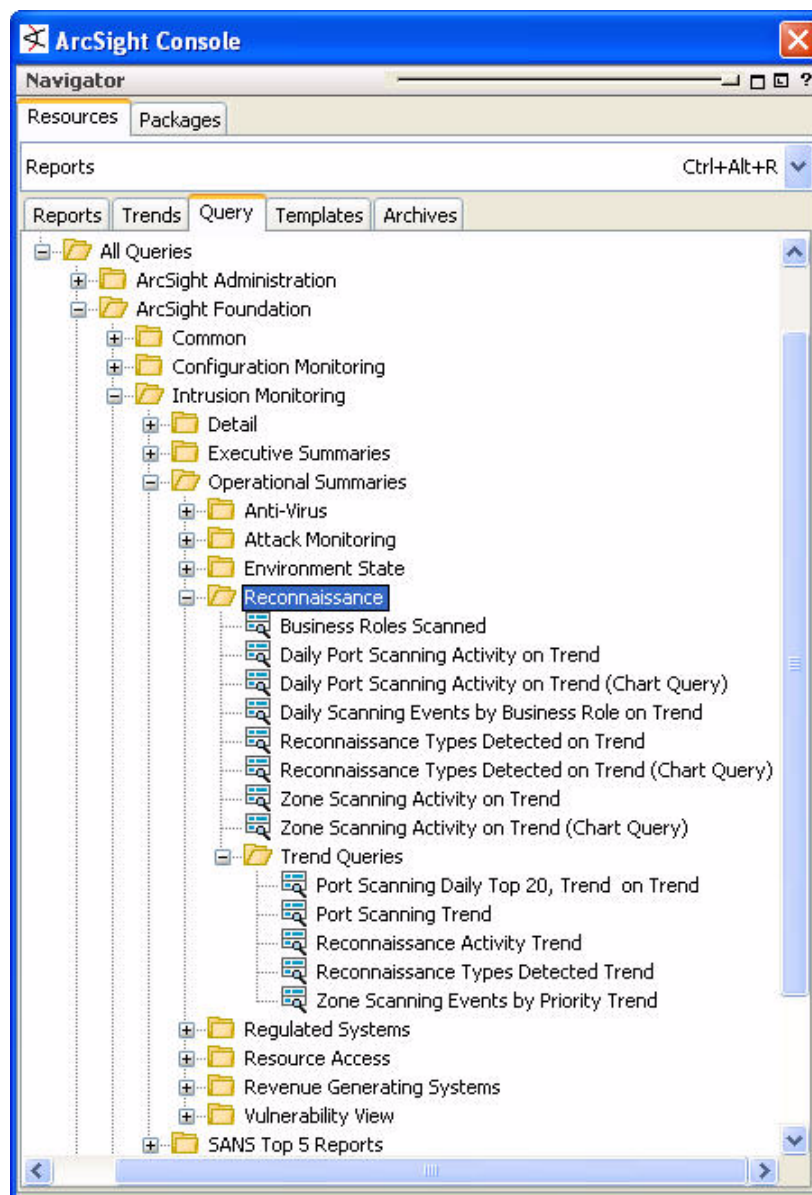
The Environment State queries are described in more detail below.

Query	Description
Top Application Status Events on Trend	This query on the Environment Status Events trend selects the Target Zone Name, the trend type name (dvLabelName), the time and sums the number of events for that zone in the time-range for the Trend: Top Application Status Events over the Last 24 Hours report.
Top Status Events on Trend	This query on the Environment Status Events trend selects the Target Zone Name, the trend type (application, operating system, service), the time and sums the number of events for that zone in the time-range for the Trend: Environment Status Events - Yesterday report.

Query	Description
Environment Status Events - Trend	This query selects the data for reporting the Target Zone Name, the time (expressed within a dependent variable), the service, operating system or application name (another dependent variable field) and a summary of the event counts for overview information to populate the trend Environment Status Events. This query uses the Events for Internal Operating Systems, Events for Internal Applications excluding services and Events for Internal Services filters to limit events to those relating to the network environment state.
Top Operating System Status Events on Trend	This query on the Environment Status Events trend selects the Target Zone Name, the trend type name (dvLabelName), the time and sums the number of events for that zone in the time-range for the Trend: Top OS Status Events over the Last 24 Hours report.
Top Service Status Events on Trend	This query on the Environment Status Events trend selects the Target Zone Name, the trend type name (dvLabelName), the time and sums the number of events for that zone in the time-range for the Trend: Top Service Status Events over the Last 24 Hours report.

Reconnaissance Operational Summary Queries

The Reconnaissance Operational Summary queries supply conditions for the Reconnaissance Operational Summary reports.



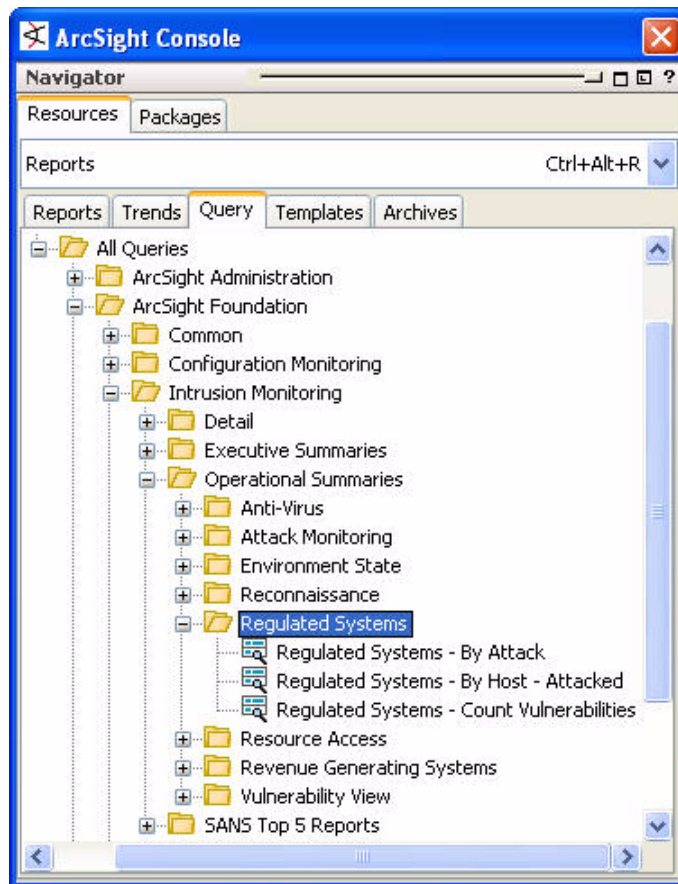
The Reconnaissance queries are described in more detail below.

Query	Description
Business Roles Scanned	This query selects the business role via a dependent variable (dvBusinessRole), the priority, and sums the aggregated event count of events matching the Reconnaissance Events (Internal Target) filter targeting assets categorized by the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/ category.

Query	Description
Daily Port Scanning Activity on Trend	This query selects the date via a dependent variable (dvDate), the target zone resource, the priority, the transport protocol, the target port, and sums the aggregated event count from the summary provided by the Port Scanning Daily Top 20 trend for the Daily Top 20 Protocol and Ports by Zone table in the Port Scanning Activity Trend report.
Daily Port Scanning Activity on Trend (Chart Query)	This query selects the date via a dependent variable (dvDate), the target zone resource, the priority, the transport protocol, the target port, and sums the aggregated event count from the summary provided by the Port Scanning trend for the Top 20 Protocol and Ports by Count from MM-DD-YYYY to MM-DD-YYY-HH:MM:SS chart in the Port Scanning Activity Trend report.
Daily Scanning Events by Business Role on Trend	This query selects the date via a dependent variable (dvMonth-Day), the business role via a dependent variable (dvBusiness-Role), and sums the aggregated event count of the data from the Reconnaissance Activity trend. This query provides both chart and table data for the Scanning Activity by Business Role Trend report.
Reconnaissance Types Detected on Trend	This query selects the date via a dependent variable (dvMonth-Day), the target zone resource, the event name and the sum of the aggregated event count from the summary of the Reconnaissance Types Detected trend for the Daily Breakdown of Reconnaissance Types Detected table in the Reconnaissance Types Detected Trend report.
Reconnaissance Types Detected on Trend (Chart Query)	This query selects the date via a dependent variable (dvMonth-Day), the reconnaissance type (event name), and a sum of the aggregated event count from summary information in the Reconnaissance Types Detected trend. This query provides data for the Daily Reconnaissance Types Detected chart in the Reconnaissance Types Detected Trend report.
Port Scanning Daily Top 20, Trend on Trend	This query selects the target zone resource, priority, transport protocol, target port, and sums the aggregated event count for the summary data from the Port Scanning trend to populate the Port Scanning Daily Top 20 trend.

Regulated Systems Operational Summary Queries

The Regulated Systems Operational Summary queries supply conditions for the Regulated Systems Operational Summary reports. Regulated systems are those categorized in the Compliance Requirement asset categories.

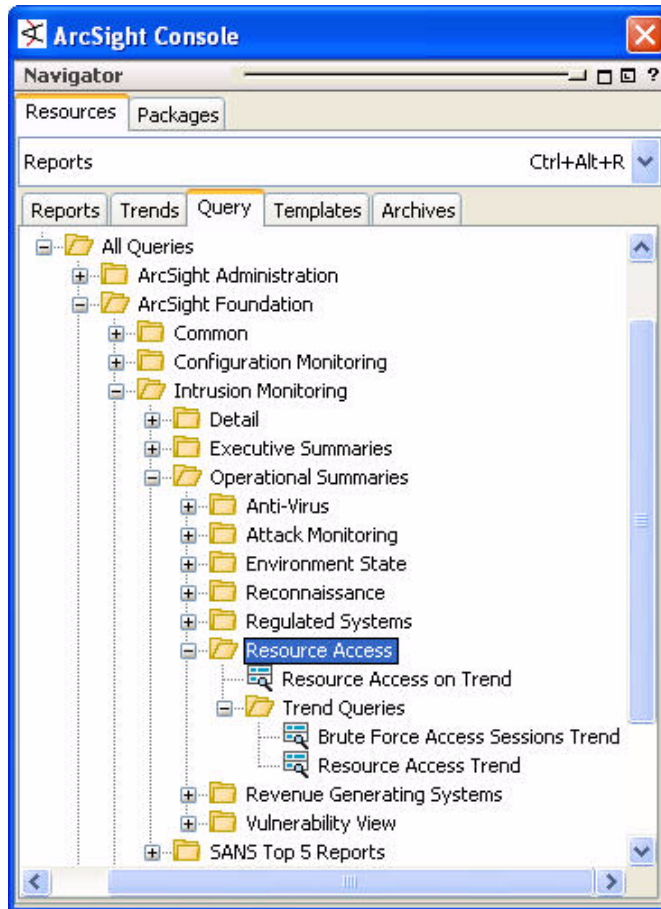


These queries are described in more detail below.

QueryDescription

Resource Access Operational Summary Queries

The Resource Access Systems Operational Summary queries supply conditions for the Resource Access Operational Summary reports.

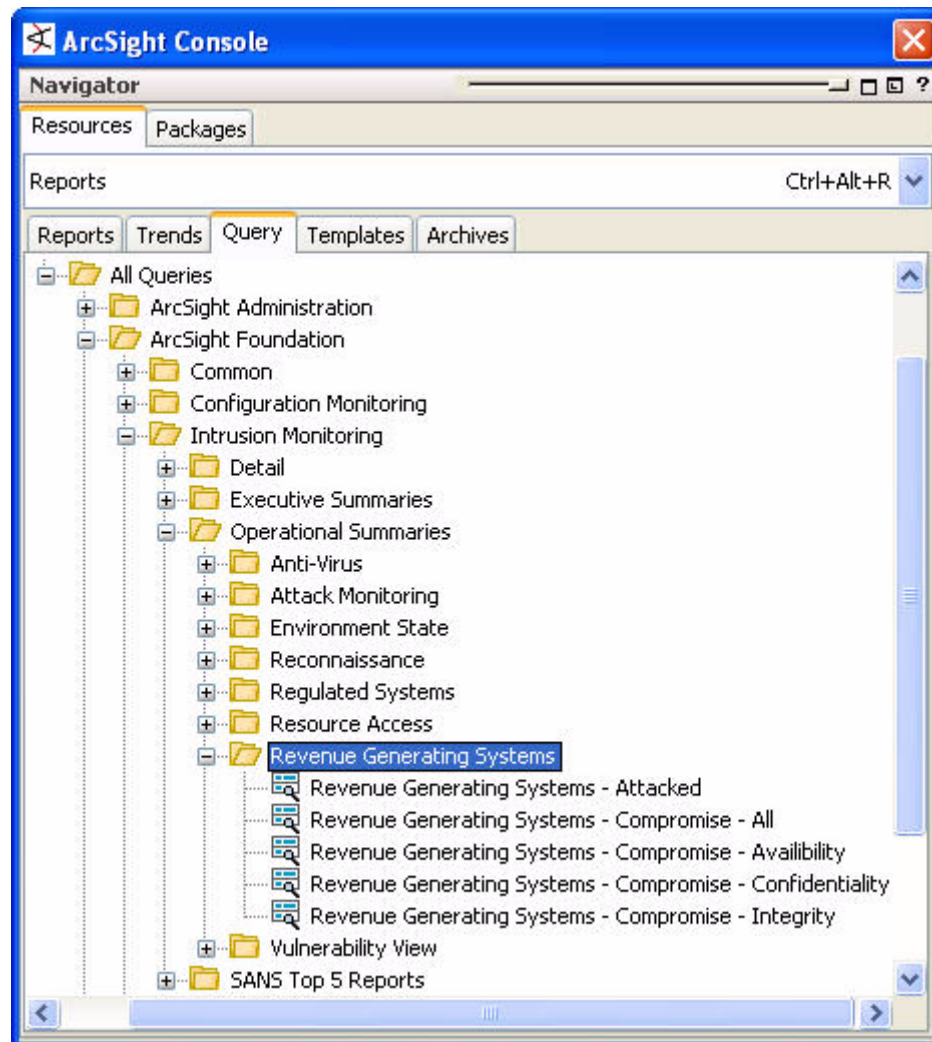


These queries are described in more detail below.

Query	Description
Resource Access on Trend	This query selects the Date, Resource Type, Outcome, User ID, User Name, Resource Zone, Resource Address and the count of events for these events from the Resource Access Trends trend.
Brute Force Access Sessions Trend	This query selects data from the Brute Force Resource Access session list to collect data for the Brute Force Access Sessions trend.
Resource Access Trend	This query selects event data for the Resource Access Trends trend. The event data fields collected are: Category ObjectCategory OutcomeTarget User IDTarget User NameTarget Zone ResourceTarget Address and the count of the number of times the events occurred for that resource.

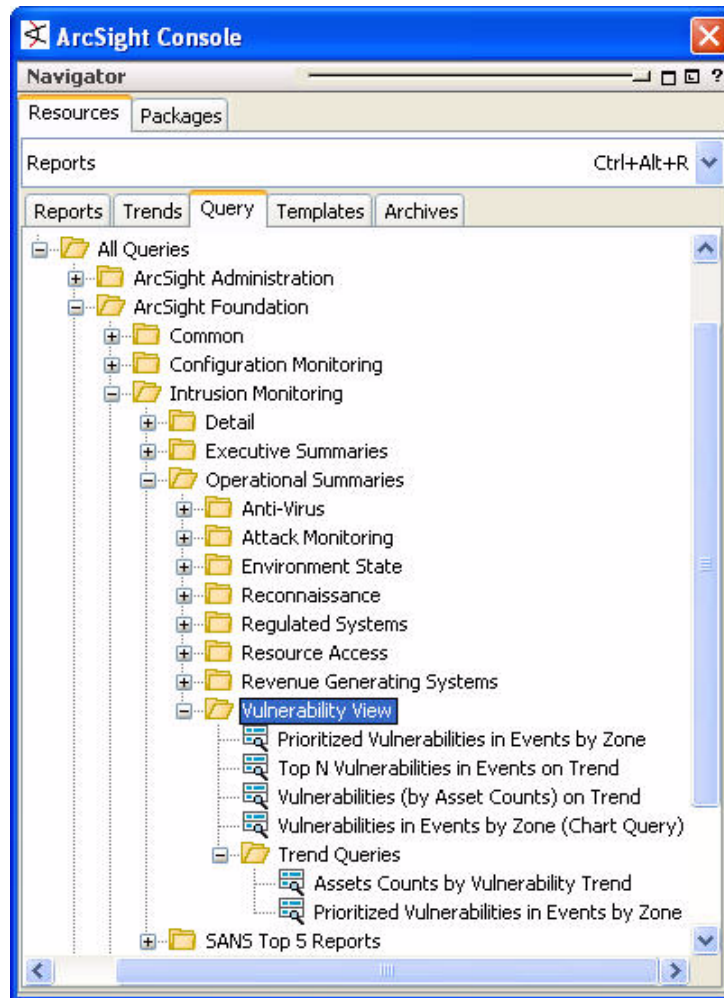
Revenue Generating Operational Summary Systems Queries

The Revenue Generating Systems queries supply conditions for systems that are categorized as revenue-generating systems.



Vulnerability View Operational Summary Queries

The Vulnerability View Systems Operational Summary queries supply conditions for the Vulnerability View Operational Summary reports.



These queries are described in more detail below.

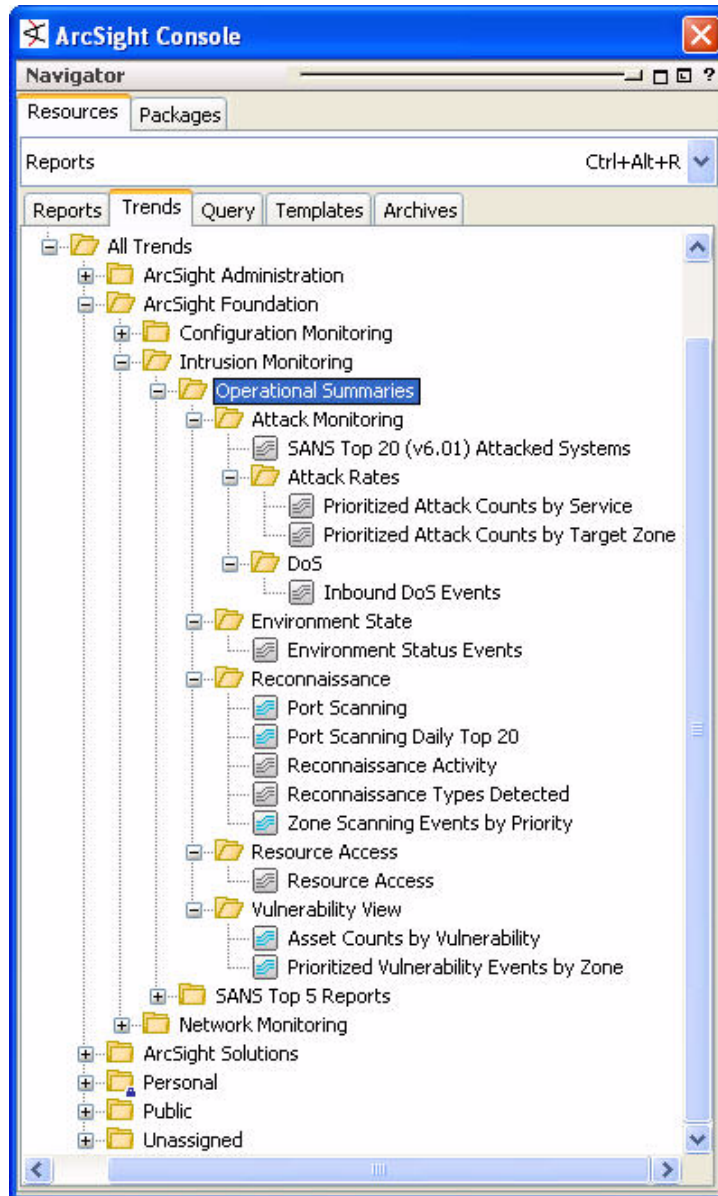
Query	Description
Top N Vulnerabilities in Events on Trend	This trend query polls the Prioritized Vulnerability Events by Zone trend, selecting the vulnerability name and the sum of the aggregated event count for use in the Top Vulnerabilities in Events Trend report.
Vulnerabilities (by Asset Counts) on Trend	This query on the Asset Counts by Vulnerability trend selects the vulnerability and the sum of the assets affected by the vulnerability for the Top N Vulnerabilities on Assets report.
Vulnerabilities in Events by Zone (Chart Query)	This query selects the zone, vulnerability name and sums the aggregated event count for events matching the Events with Vulnerabilities filter to provide data for the Top N Vulnerabilities by Zone chart in the Vulnerabilities in Events by Zone report.

Query	Description
Prioritized Vulnerabilities in Events by Zone	This query selects the zone, vulnerability name, priority and sums the aggregated event count for events matching the Events with Vulnerabilities filter to provide data for the Top N Vulnerabilities by Zone with Priority table in the Vulnerabilities in Events by Zone report. This query also provides data for the Prioritized Vulnerability Events by Zone trend.
Assets Counts by Vulnerability Trend	This query on assets populates the Asset Counts by Vulnerability trend. It collects the vulnerability and the number of assets for which the vulnerability was reported. The query selects the most widely reported vulnerabilities in descending order, to show the most common vulnerabilities exposed on the network.

Operational Summary Trends

These trends supply conditions that consolidate data for the Operational Summary trend reports for Attack Monitoring, Environment State, Reconnaissance, Resource Access, and Vulnerability View.

The blue icons indicate trends that are enabled by default. For more about enabling and disabling trends, see [“Trends” on page 43](#).



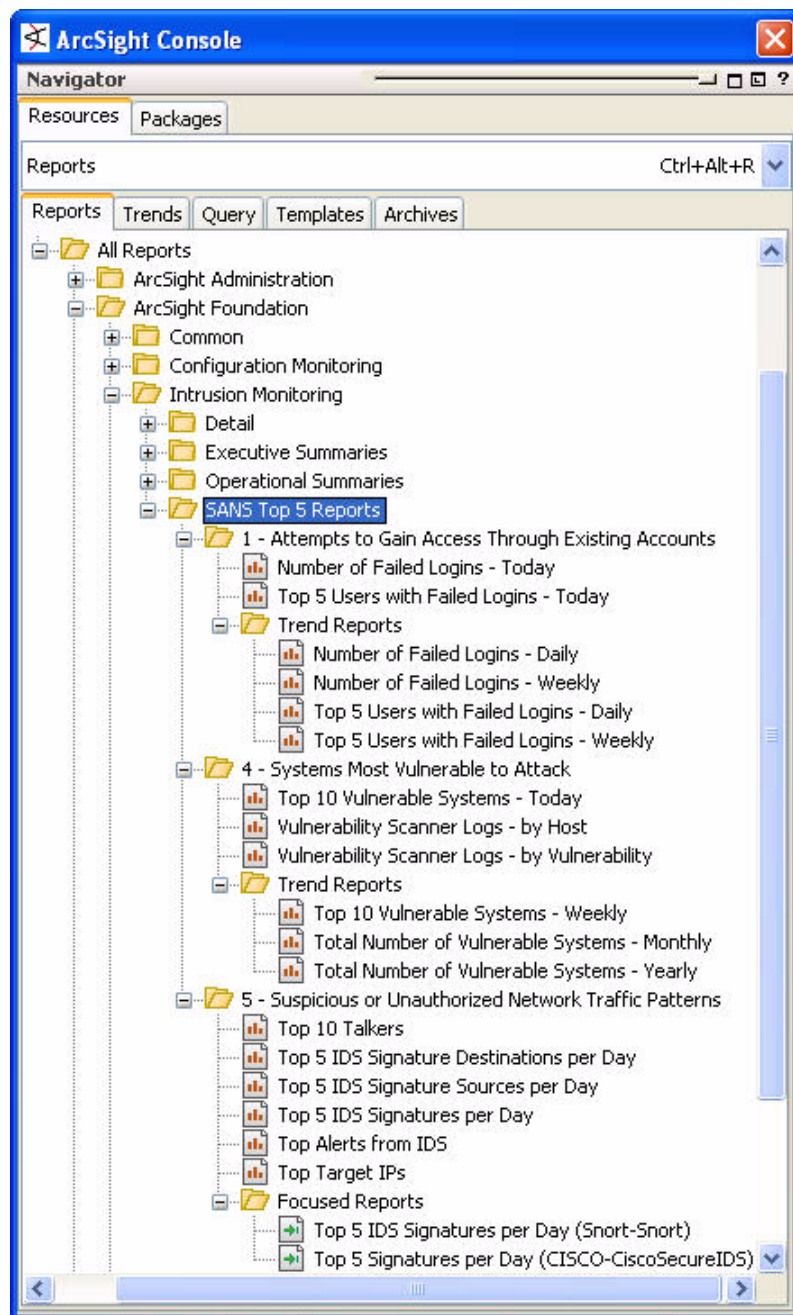
These Operational Summary trends are described in more detail below:

Trend	Description
SANS Top 20 (v6.01) Attacked Systems	This trend collects information about the SANS Top 20 vulnerability areas and vulnerability names and the number of attacks for each vulnerability on an hourly basis. The data used is generated by events from the "SANS Top 20" rules.
Prioritized Attack Counts by Service	This trend contains data selected by the query Prioritized Attack Counts by Service - Trend, which selects the Hour (a DV based on the event's end time), the Service (a DV based on the service name or application protocol, the transport protocol and the port, e.g., HTML/TCP:80), the Priority and Sums the Aggregated Event Count. The Hour DV is used so that the data can be plotted based on the hour in which the event occurred, not the trend timestamp (the time the event data was stored in the trend).
Prioritized Attack Counts by Target Zone	
Inbound DoS Events	
Environment Status Events	This trend collects summary counts of events, storing the target zone, the time, the service, application or operating system names and a marker field that can be used by queries to extract data for any one or all of the related areas. Note the use of dependent variables in the Environment Status Events - Trend query that is used to populate the trend, and the filtering conditions of the queries used by the reports to extract specific data.
Port Scanning	This trend collects a daily snapshot of the top 1,000 events in 6 hour intervals for use as detailed daily information in the Port Scanning Activity Trend report. The Port Scanning trend collects the top events for the day and the Port Scanning Daily Top 20 trend (a trend on this trend), follows up and collects summary information.
Port Scanning Daily Top 20	This is a trend on a trend that collects a daily snapshot of the top events in the Port Scanning trend. Up to 20 events per day are collected for use as detailed daily information in the Port Scanning Activity Trend. The Port Scanning trend collects the top events for the day and this trend follows up and collects summary information.
Reconnaissance Activity	This trend collects a daily snapshot of events in 6 hour intervals using the Reconnaissance Activity Trend query. Up to 1,000 events per interval are collected (4,000 per day) to collect data for the Scanning Activity by Business Role Trend.
Reconnaissance Types Detected	This trend collects a daily snapshot of events in 6 hour intervals using the Reconnaissance Types Detected Trend query. Up to 1,000 events per interval are collected (4,000 per day) to collect the most common reconnaissance types. This data is used by the Reconnaissance Types Detected Trend report.
Zone Scanning Events by Priority	This trend collects a daily snapshot of events in 6 hour intervals using the Zone Scanning Events by Priority Trend query. Up to 1,000 events per interval are collected (4,000 per day) to collect the top reconnaissance events per zone by priority. The data is used by the Scanning Activity by Zone Trend report.

Trend	Description
Resource Access	This trend tracks unusual resource access attempts, including the outcome of the access attempt. This trend runs daily, broken up into 6 queries running in 4-hour blocks, covering a full day.
Asset Counts by Vulnerability	This trend collects a snapshot of the vulnerabilities that have been reported for assets on a weekly basis. The goal of this trend is to collect the top 1,000 vulnerabilities reported affecting the most assets on the network to give a view of which vulnerabilities represent the highest risk, by vulnerability exposure, on a weekly basis. This is assuming that the vulnerability scanner is scanning once per week. For more or less frequent scans, the timing of this trend and the report time range should be adjusted to give a more accurate picture. When viewing the data for this trend, you may notice a count with a blank vulnerability. This means that number of assets did not have any vulnerabilities associated with them. You should be able to locate them by reviewing the Vulnerabilities and Assets report (go to the end of the report and the blank vulnerability should have the zones, addresses and host names of the assets with no reported vulnerabilities).
Prioritized Vulnerability Events by Zone	This trend stores the target zone name, the vulnerability name, the priority and the sum of the aggregated event count to determine the top vulnerability events in a given time period. The trend runs four 6-hour interval queries once a day, collecting the top 1,000 events per interval. This allows the determination of the top 10 most frequent vulnerability exploit attempts per day, and can give a reasonable view of the top 10 attempts for the past week, or possibly the last month.

SANS Top 5 Reports for Intrusion Monitoring

The SANS Top 5 reports provide summaries that pertain to SANS sections 1, 4, and 5.



The SANS Top 5 reports are described in more detail below.

Report	Description
Number of Failed Logins - Today	This Report shows the number of failed logins per hour for the last day.
Top 5 Users with Failed Logins - Today	This Report shows the top 5 users with the biggest number of failed logins attempts.

Report	Description
Number of Failed Logins - Daily	This Trend Report shows the number of failed logins per hour for a given day.
Number of Failed Logins - Weekly	This Trend Report shows the number of failed logins per day for a given week.
Top 5 Users with Failed Logins - Daily	This Trend Report shows the top 5 users with the biggest number of failed login attempts for a given day.
Top 5 Users with Failed Logins - Weekly	This Trend Report shows the top 5 users with the biggest number of failed login attempts for a given week.
Top 10 Vulnerable Systems - Today	This Report shows the top 10 current vulnerable systems. This Report contains a bar chart and a table. The chart shows the top 10 vulnerable systems with the number of associated vulnerabilities. The table provides some more details for the top 10 systems, such as IP address, Host Name, and Zone Name.
Vulnerability Scanner Logs - by Host	This Report shows Vulnerability Scanner Logs grouped by Zone and Host IP Address. This Report can be focused by Device Vendor and Device Product.
Vulnerability Scanner Logs - by Vulnerability	This Report shows Vulnerability Scanner Logs grouped by Vulnerability IDs and Names. This Report can be focused by Device Vendor and Device Product.
Top 10 Vulnerable Systems - Weekly	This Trend Report shows the top 10 vulnerable systems for a given week. This Trend Report contains a bar chart and a table. The chart shows the top 10 vulnerable systems with the number of associated vulnerabilities. The table provides some more details for the top 10 systems, such as IP address, Host Name, and Zone Name.
Total Number of Vulnerable Systems - Monthly	This Trend Report shows the total number of vulnerable systems by week for a given month.
Total Number of Vulnerable Systems - Yearly	This Trend Report shows the total number of vulnerable systems by week for a given year.
Top 10 Talkers	This Report contains a chart and a table. The chart shows the Top 10 Talkers and the table shows a detailed list of the Top Talkers.
Top 5 IDS Signature Destinations per Day	This Report shows the Top 5 IDS Signature Destinations per Day. The Report contains a chart showing the Top 5 IDS Signature Destination IP Addresses, and a table showing the Top Signature Destination IP Address and Zone, as well as the Device Vendor and Product of the reporting device.
Top 5 IDS Signature Sources per Day	This Report shows the Top 5 IDS Signature Sources per Day. The Report contains a chart showing the Top 5 IDS Signature Source IP Addresses, and a table showing the Top Signature Source IP Address and Zone, as well as the Device Vendor and Product of the reporting device.
Top 5 IDS Signatures per Day	This Report shows the Top 5 IDS Signatures per Day in a chart. This Report can be focused by Device Vendor and Product.
Top Alerts from IDS	This Report shows the Top Alerts coming from Intrusion Detection Systems. The Report contains a chart and a table. The chart shows the Top 10 Alerts (Signature ID), and the table shows the details of the Top Alerts.

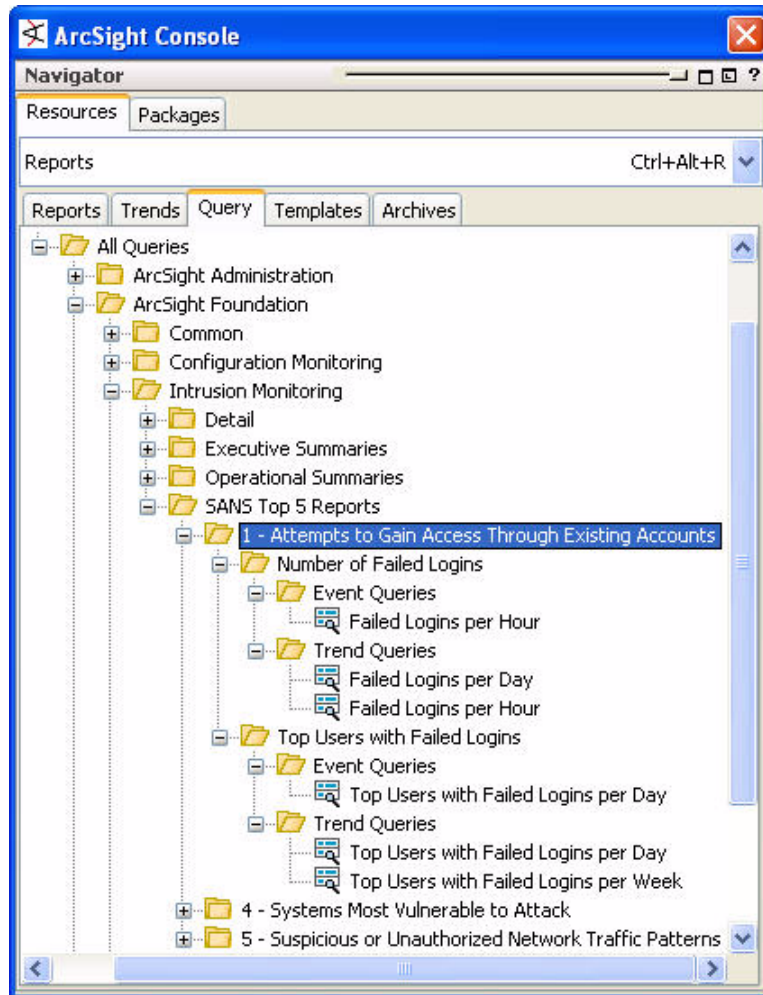
Report	Description
Top Target IPs	This Report contains a chart and a table. The chart shows the Top 10 Target IPs and the table shows a detailed list of the Top Targets.

SANS Top 5 Queries

The SANS Top 5 queries supply conditions for the SANS Top 5 reports and trends.

1 - Attempts to Gain Access Through Existing Accounts

These queries supply conditions for the SANS section 1 reports and trends.



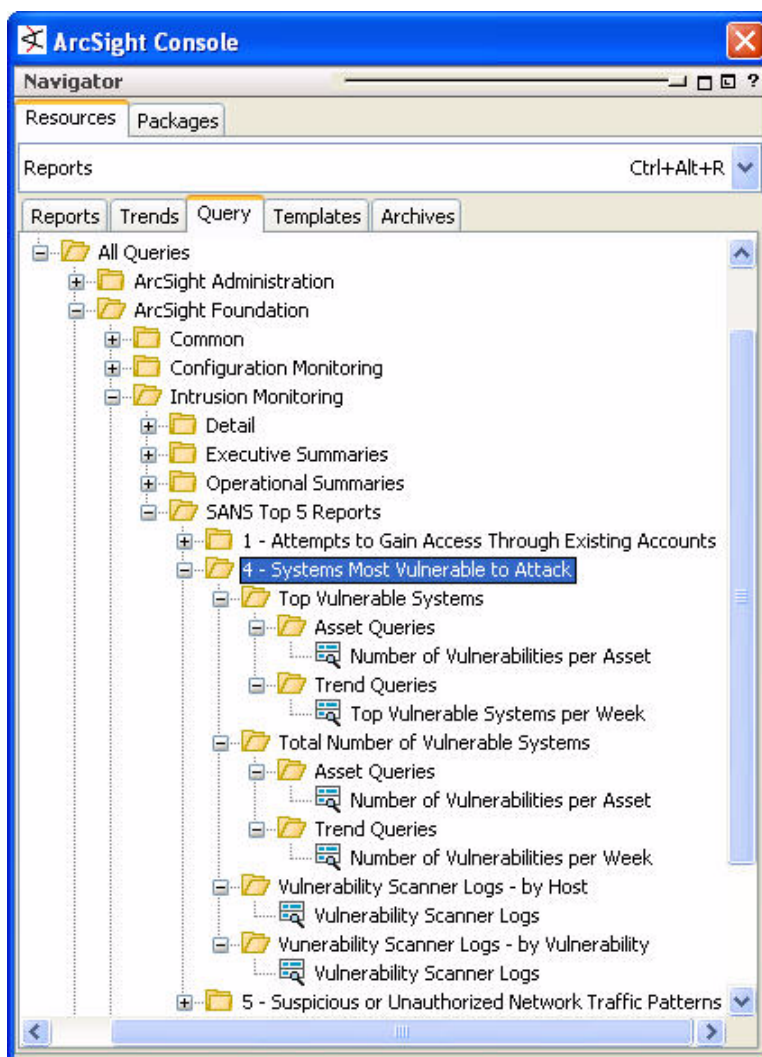
The SANS Top 5 section 1 queries are described in more detail below.

Query	Description
Failed Logins per Hour	This query selects the Hour and the number of occurrences for failed authentication verifications.
Failed Logins per Day	This query on the Top Users with Failed Logins per Hour trend provides the sum of the number of failed logins for the day.

Query	Description
Failed Logins per Hour	This query on the Top Users with Failed Logins per Hour trend provides the sum of the number of failed logins for each hour.
Top Users with Failed Logins per Day	This query selects the day, the Target User Name and the number of occurrences for failed authentication verifications.
Top Users with Failed Logins per Day	This query on the Top Users with Failed Logins per Day trend provides the sum of the number of failed logins for each user-name by hour.
Top Users with Failed Logins per Week	This query on the Top Users with Failed Logins per Day trend provides the sum of the number of failed logins for each user-name within the week.

4 - Systems Most Vulnerable to Attack

The Systems Most Vulnerable to Attack queries supply conditions for the SANS section 4 reports and trends.

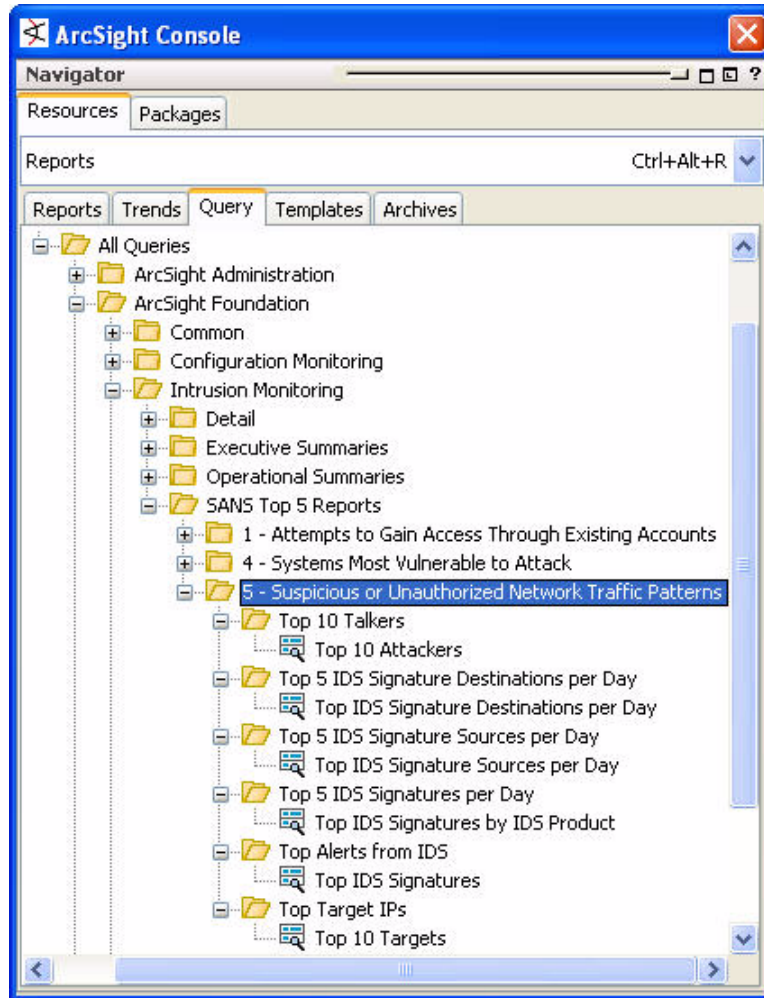


The SANS section 4 queries are described in more detail below.

Query	Description
Number of Vulnerabilities per Asset	This query on assets selects the asset name, its IP address, its host name and its device zone name and counts the number of vulnerabilities associated with that device.
Top Vulnerable Systems per Week	This query on the Number of Vulnerabilities per Asset trend selects the asset name, its IP address, its host name and its device zone name and averages the number of vulnerabilities associated with that device per week.
Number of Vulnerabilities per Week	This query on the Number of Vulnerabilities per Asset trend selects the asset name, its IP address, its host name and its device zone name and averages the number of vulnerabilities associated with that device per week.
Vulnerability Scanner Logs	This query scans events for scanner events (defaulting to the Foundstone FoundScan scanner) and selects the target address, the target zone name, the device event class ID and the event (vulnerability) name.

5 - Suspicious or Unauthorized Network Traffic Patterns

The Suspicious or Unauthorized Network Traffic Patterns queries supply conditions for the SANS Top 5 reports.

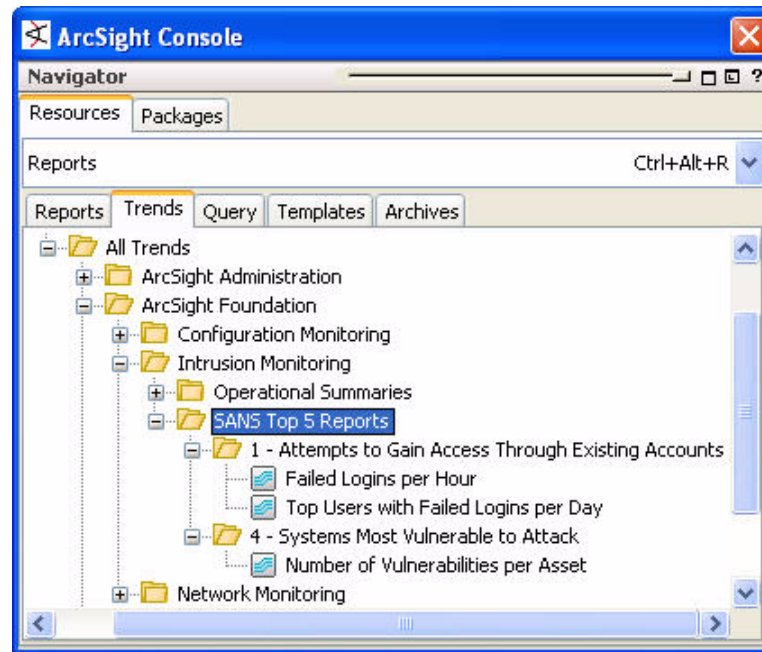


The SANS Top 5 section 5 queries are described in more detail below.

Query	Description
Top IDS Signature Destinations per Day	This query over base IDS/Network events selects the target address, the target zone name, the device vendor, the device product and the count of the events within the query's time-frame.
Top IDS Signature Sources per Day	This query over base IDS/Network events selects the attacker address, the attacker zone name, the device vendor, the device product and the count of the events within the query's time-frame.
Top IDS Signatures by IDS Product	This query on base /IDS/Network events for the device product and vendor Short, Short (default setting, selectable by the user running the report...), selects the device event class ID and the count based on the end time.
Top IDS Signatures	This query looks for base /IDS/Network events, selecting the device event class ID, the device vendor, the device product and a count on the end time of the event.

SANS Top 5 Trends

The SANS Top 5 trends define trend frameworks for the SANS top 5 section 1 and 4 trend reports.

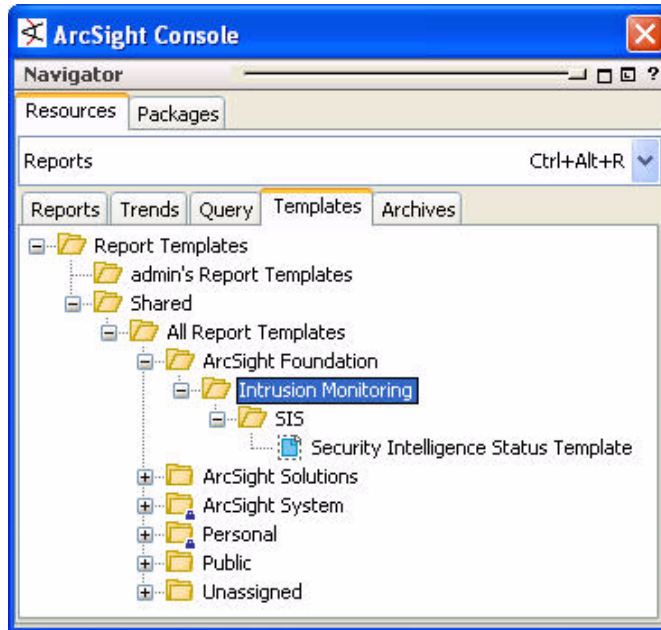


These trends are described in more detail below.

Trend	Description
Failed Logins per Hour	This Trend stores the number of failed logins per hour and is scheduled for a daily run.
Top Users with Failed Logins per Day	This Trend stores the Top 1000 users with the highest number of failed logins per day.
Number of Vulnerabilities per Asset	This Snapshot Trend stores the number of vulnerabilities associated to an Asset on a weekly basis.

SIS Report Template

The Security Intelligence Status template supports the four charts and six tables of the Security Intelligence Status report, required by the IRRC.



For instructions about how to customize this template with your company logo, see [“Customize Branding in Standard Templates” on page 69](#).

What's Next

The next chapter, Network Monitoring, describes the Network Monitoring foundation.

Network Monitoring Foundation



The Network Monitoring foundation monitors the status of network throughput and network infrastructure. This foundation provides statistics about traffic and bandwidth usage that helps you identify anomalies and areas of the network that need attention.

Network Monitoring also addresses the usage and traffic profiles that factor into a comprehensive security reporting strategy.

- [“Network Monitoring Foundation Overview” on page 243](#)
- [“Configuration Overview” on page 246](#)
- [“Network Monitoring Filters” on page 250](#)
- [“Network Monitoring Active Channel” on page 257](#)
- [“Network Monitoring Dashboards and Data Monitors” on page 259](#)
- [“Network Monitoring Reports” on page 269](#)
- [“Network Monitoring Rules” on page 305](#)

Network Monitoring Foundation Overview

By monitoring and analyzing the bandwidth usage and traffic patterns on your network, the system content’s network monitoring content is intended to:

- Keep the network up and running
- Ensure maximum availability of mission-critical server applications and vital network resources
- Validate the existence and availability of any network object
- Observe and detect any object in error state
- Monitor common and custom TCP/IP ports
- Evaluate network productivity and utilization of network resources
- Assess impact of changes to the network
- Track network anomaly and security vulnerabilities

Supported Devices

The Network Monitoring content is built around feeds from the ArcSight SmartConnector that collects events from Qosient Argus, which is a real-time flow monitor. It monitors all network transactions seen in a data network traffic stream (<http://www.qosient.com/argus/>).

The Argus device will see a transaction from point A to point B and keep the information in the following Argus-specific fields:

Argus event field	Description
lasttime	record last time
srcaddr	source IP address
dstaddr	destination IP address
sport	source port number
dport	destination port number
bytes	total transaction bytes
srcbytes	source-to-destination transaction bytes
dstbytes	destination-to-source transaction bytes

The ArcSight Argus Connector maps this information to the correct fields in the ArcSight event schema, for example:

Argus event field	ArcSight event field
srcaddr	Attacker Address
dstaddr	Target Address
srcbytes	Bytes in
dstbytes	Bytes out

Calculating Bytes In and Bytes Out

One of the goals of the network monitoring foundation is to analyze how much traffic volume is coming into and going out of the network. Calculating this bandwidth usage involves keeping track of bytes in and bytes out of the network, from what sources, at and what rates.

Argus counts any request as “bytes in” and any response as “bytes out” regardless of where the requestor is located in relation to your protected network. For example, in the illustration below, Point A initiates the request to Point B, and Point C initiates the request to Point A. Both are considered by Argus to be “bytes in.”

But as a network administrator, you're also interested in traffic volume outbound *from* and inbound *to* your protected network, illustrated by the blue and red arrows in the example below.

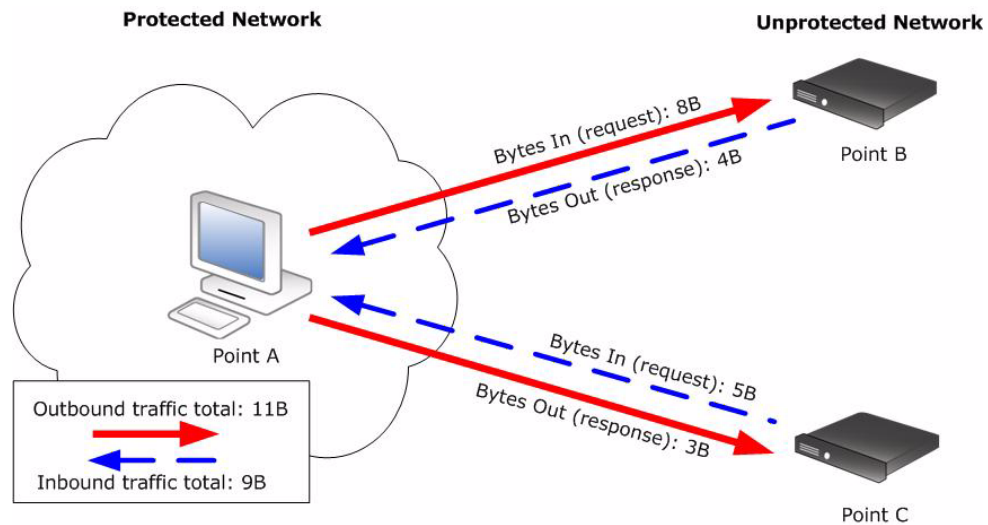


Figure 6-1 ArcSight variables ensure that Argus' byte counts for "bytes in" and "bytes out" correspond with the network's notion of inbound traffic and outbound traffic.

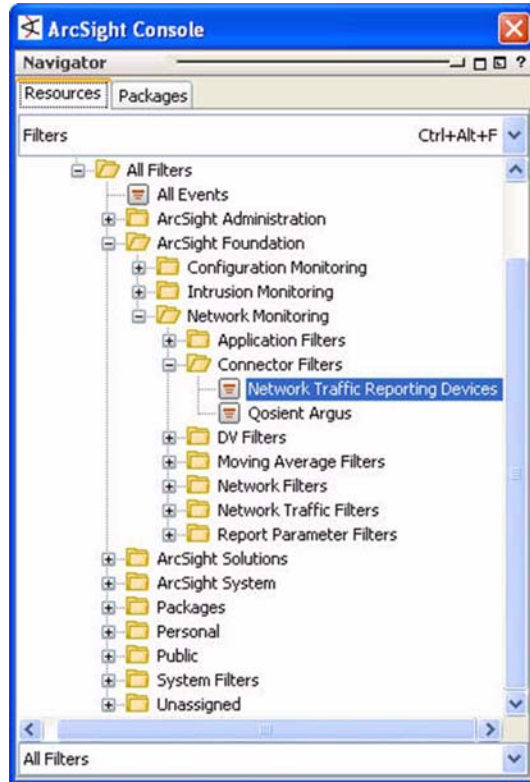
To make sure that the byte counts for Argus' "bytes in" and "bytes out" correspond with your network's notion of outbound traffic and inbound traffic, ArcSight has constructed a system of variables and filters that translate Argus' "bytes in" and "bytes out" to traffic inbound to and outbound from your network.

The ArcSight `IncomingBytes` and `OutgoingBytes` variables take the Argus byte count of activity on the way out of the protected network and counts it as outbound traffic, and activity coming into the protected network as inbound traffic. In the A-to-B case, it considers the byte count for Argus' "bytes in" to be outbound traffic and considers the byte count for Argus' "bytes out" to be inbound traffic. The A-to-C case would match: bytes in are counted as inbound traffic, and bytes out are counted as outbound traffic.

In our example, if you add the total bytes out from the network's perspective (after the values have been normalized by the ArcSight variables), you would add the byte counts for the two red arrows, in this case, $8 + 3$, or 11. And the byte total for the inbound traffic would be the sum of the two blue arrows: $4 + 5$, or 9.

Configuration Overview

The events that trigger the network monitoring content are controlled by the filters in the Connector Filters group ([\All Filters\ArcSight Foundation\Network Monitoring\Connector Filters](#)).



Connector Filters: These filters determine what devices drive the content for the network monitoring content. By default, it is set for devices reported by the Argus network flow monitoring system.

If you use another real-time flow monitoring device besides Argus, that device must also report Attacker, Target, Ports, Bytes in and Bytes out. You can then configure the Smart-Connector filters to operate on events from that device.

If you use only Argus, you do not have to do this procedure, and can skip to the next section, [“Advanced Connector Configuration” on page 248](#).



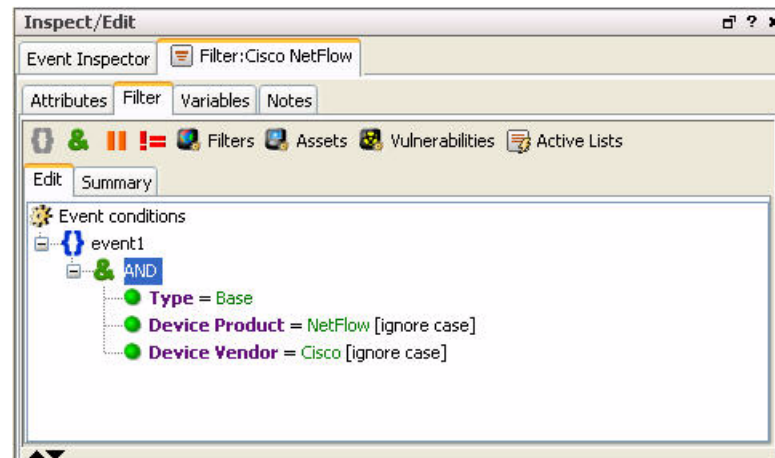
If you have multiple network reporting devices, verify that any overlapping address spaces are defined through their own ArcSight network.

This configuration procedure creates a new filter based on the *Qosient Argus* filter for each reporting device relevant to your network environment.

- 1 Copy the *Qosient Argus* filter: click and drag the filter into the same group; when prompted “Do you want to make a copy of this resource?” select **Yes**.
- 2 Modify the copy to reflect your network monitoring device and vendor.
 - a Open the copy in the Inspect/Edit panel. At the Attributes tab, rename the copy to indicate the name of your network reporting device, for example, [Cisco Net-Flow](#).
 - b At the Filter tab in the Event conditions window, double-click the condition `Device Product = Argus [ignore case]`. Delete `Argus` and type in the

name of your device as your device reports it to the ArcSight Connector, for example, `NetFlow`. Click **OK**.

- c In the Event conditions window, double-click the condition `Device Vendor = Qosient [ignore case]`. Delete `Qosient` and type in the name of your device as your device reports it to the ArcSight Connector, for example, `Cisco`. Click **OK** in the condition. The condition should look like this:



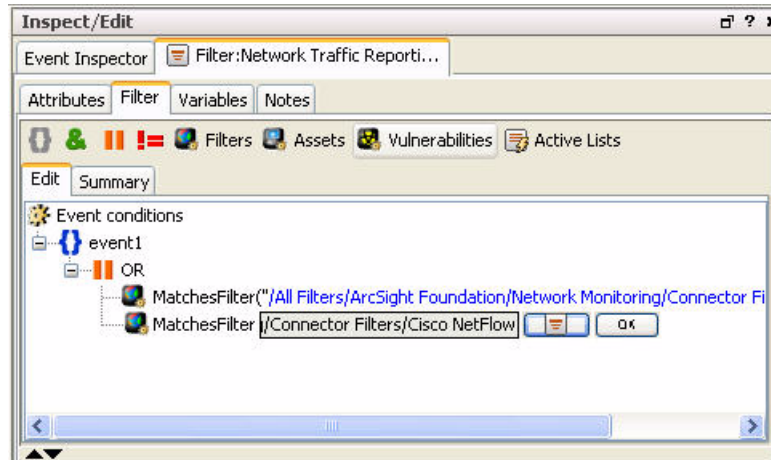
- d Repeat steps a through c for however many network monitoring devices you have.
- e Click **OK** to apply changes and close the filter editor.



Depending on how you want to organize your content, you can also express all your network reporting devices in a single filter. When adding vendors and products to the expression, add an **OR** clause to the `event1` base.

- 3 Modify the *Network Traffic Reporting Devices* filter to point to the filter(s) you created in step 2.
 - a Open the *Network Traffic Reporting Devices* filter in the Inspect/Edit panel.
 - b At the Filter tab in the Event conditions window, select `event1` and click the OR operator (||).
 - c Select the first condition, `MatchesFilter("/All Filters/ArcSight Foundation/Network Monitoring/Connector Filters/Qosient Argus")`, and select **Copy** from the Edit menu.
 - d Select the OR operator and select **Paste** from the Edit menu.
 - e Double-click the second condition, `MatchesFilter("/All Filters/ArcSight Foundation/Network Monitoring/Connector Filters/Qosient Argus")`, and double-click it. Click the filter button () and

navigate to the filter you created in step 2. Click **OK**. The condition should look like this:



- f** Repeat step 3 for however many network monitoring filters you want to add. If you do not have Argus, you can remove the Qosient Argus filter from the **OR** statement (select it and press the **Delete** key).
- g** Click **OK** to apply changes and close the filter editor.

Advanced Connector Configuration

As an option to reduce the number of raw events that get sent from your network monitoring device to ArcSight, you can aggregate groups of events with the same characteristics using the **group by** option at the SmartConnector. You can do this configuration from the ArcSight Console in the Connectors portion of the navigator panel.

For example, the attacker port (Argus **srcPort**) is often less interesting than the target port (**destPort**). If there are many events with the same target port and different attacker ports, you can aggregate the events, which combines the values that are the same, and nulls out the values that are different.

In the example below, the attacker ports are different, but the target ports, attacker IPs, and target IPs are the same for each event. In this case, the value in the attacker port column is null, and the values in the *Bytes in* column are summed.

Attacker port	Target port	Attacker IP	Target IP	Bytes in
3331	80	1.1.1.1	2.2.2.2	2
3332	80	1.1.1.1	2.2.2.2	3
3333	80	1.1.1.1	2.2.2.2	15
3334	80	1.1.1.1	2.2.2.2	9
NULL	80	1.1.1.1	2.2.2.2	29

This reduces the number of individual events that the system has to process, which improves performance and efficiency.



As an option, you can perform this aggregation on the Argus device itself using a RAGATOR script and a configuration file that specifies the fields you wish to aggregate, those you wish to nullify, and those you wish to sum. This configuration should be done by the Argus administrator.

Required Asset Modeling

The network monitoring content relies upon assets being created in the ArcSight asset model to represent what is internal to and external from the protected network. Some content also relies on e-mail and web servers being categorized.



If this network modeling is not performed, ESM will still function, but some network monitoring content will contain no data.

Assets

ESM knows that an asset is internal only if an asset is created for it in a known internal address space. The content that reports on internal and external traffic requires that the assets it reports on be present in the ArcSight asset model.

For instructions about how to configure assets, see [“Configure Resources with Network-Specific Values” on page 35](#).

Asset Categories

In order to activate content that references e-mail and web servers, your e-mail and web servers must be categorized in the *Email* asset category group ([All Asset Categories/Site Asset Categories/Application/Type/Email](#)), and your web servers must be categorized in the *Web Server* asset category group ([All Asset Categories/Site Asset Categories/Application/Type/Web Server](#)). For tips about how to categorize groups of assets, see [“Asset Categories” on page 30](#).

If you have created your own asset categories that are relevant to the top traffic dashboards, you can add those asset categories to the corresponding filter ([All Filters/ArcSight Foundation/Network Monitoring/Application Filters](#)).

How to Interact with the Network Monitoring Content

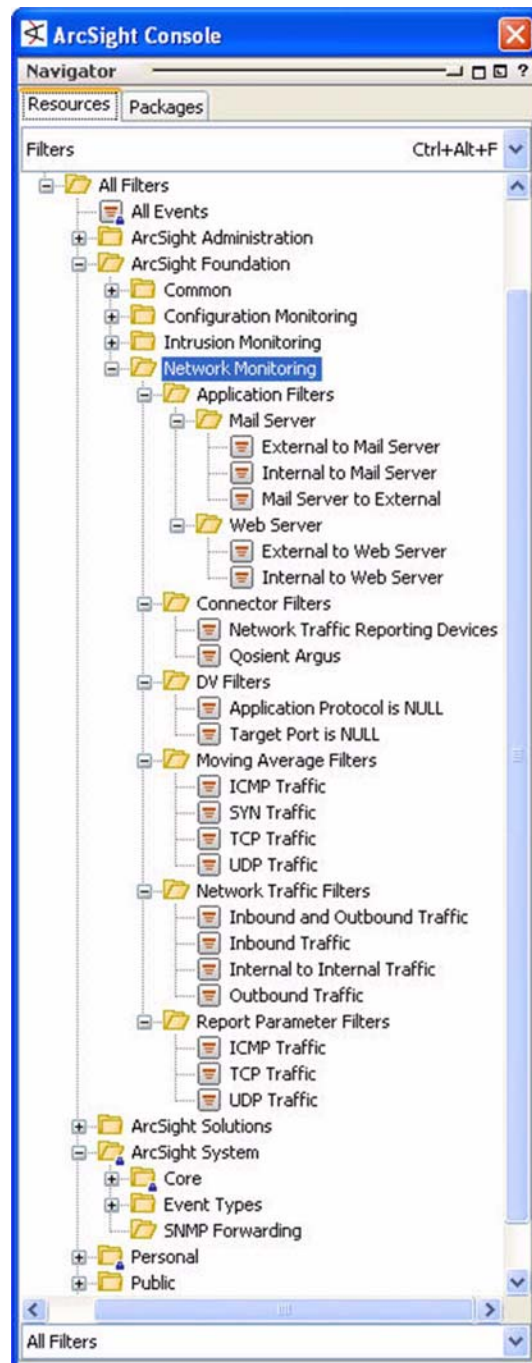
The content in the Network Monitoring foundation all support three main sets of monitoring and reporting tools:

- **Filters:** conditions that support functions in the other network monitoring resource layers.
- **Active Channel:** the flow of live events from network monitoring device(s).
- **Dashboards:** statistical summaries of live events from network monitoring device(s).
- **Reports:** summaries of historical event data from network monitoring device(s).

The remaining sections describe the content that makes up these views and explains how to use it.

Network Monitoring Filters

The network monitoring filters express conditions that are used by the other network monitoring and reporting resources.



Application Filters: These filters capture traffic to and from mail servers and web servers.

Connector Filters: These filters define what network flow device activates the network monitoring content.

DV Filters: These filters supply conditions for variables that promote consistent event statistics.

Moving Average Filters: These filters define events that use specific protocols. The results are consumed by moving average data monitors.

Network Traffic Filters: These filters define activity involving inbound and outbound traffic for bandwidth monitoring and reports.

Report Parameter Filters: These filters support the SANS Top 5 Traffic Moving Average Report.

The sections below describe these filters. How the filters are used is discussed in the remaining Network Monitoring sections, as indicated.

Application Filters

The Application Filters capture traffic to and from mail servers and web servers. They are consumed by the General dashboards and data monitors described in [“General Dashboards” on page 262](#).

These filters use two conditions. The first condition determines if the traffic is inbound or outbound. The second condition determines if the source or the target is a Mail or a Web server.

For example, External to Mail Server means External source to Internal target (i.e. inbound) and target is a Mail Server.

Mail Server Filters

Filter	Description
External to Mail Server	This filter is looking for Argus events coming from the outside network targeting internal hosts categorized as mail servers.
Internal to Mail Server	This filter is looking for Argus events coming from inside the company network targeting internal hosts categorized as mail servers.
Mail Server to External	This filter is looking for Argus events coming from internal hosts categorized as mail servers targeting the outside network.

Web Server Filters

Filter	Description
External to Web Server	This filter is looking for Argus events coming from the outside network targeting internal hosts categorized as web servers.
Internal to Web Server	This filter is looking for Argus events coming from inside the company network targeting internal hosts categorized as web servers.

Connector Filters

These filters define what network flow device activates the network monitoring content. By default, the Network Monitoring foundation operates on events from the Qosient Argus network flow system. For instructions about how to configure these filters for other network flow systems, see [“Configuration Overview” on page 246](#).

Filter	Description
Network Traffic Reporting Devices	This Filter is used to select your Network Traffic Reporting Devices. The default Network Traffic Reporting Device is Qosient Argus.
Qosient Argus	This filter is looking for events coming from the Argus connectors.

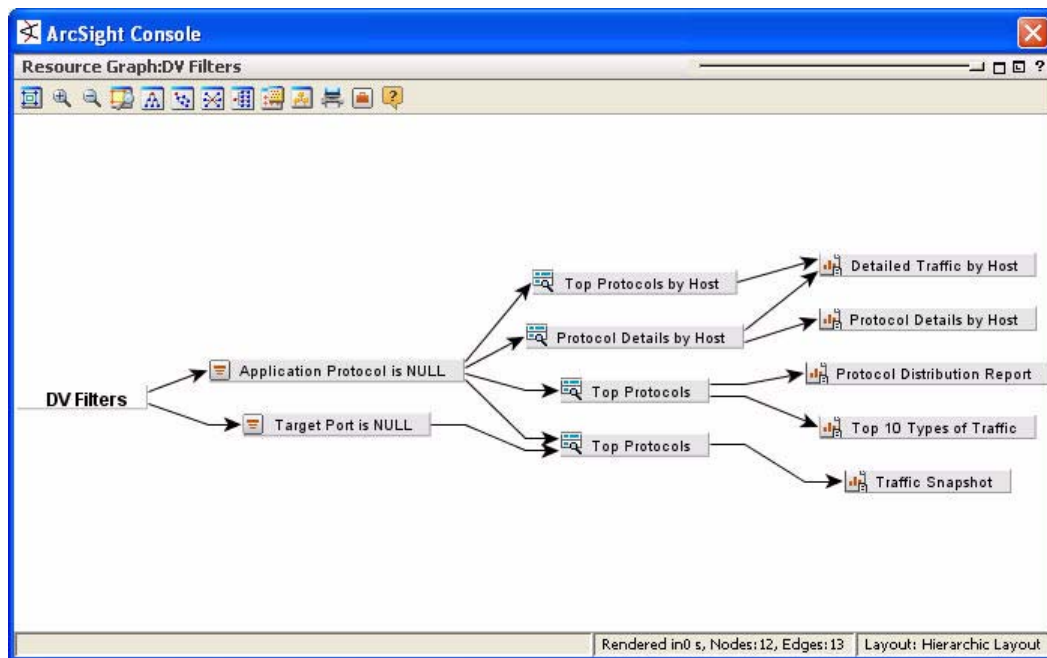
DV Filters

These filters supply conditions for variables that promote consistent event statistics in report queries. Because all devices don't report the same types of event data, these filters help ESM sort events with missing information with a consistent identifier.

Filter	Description
Application Protocol is NULL	This filter is used by a dependent variable to check whether the event target has an application protocol associated with it.
Target Port is NULL	This filter is used by a dependent variable to check whether the event target has a port number associated with it.

For example, if an event does not have a value in the application protocol field, the *Application Protocol is NULL* filter informs the variable set in the report *Protocol Details by Host*, which will then use the event's target port and append the transport protocol (1234/TCP).

These two filters inform variables for the following reports:



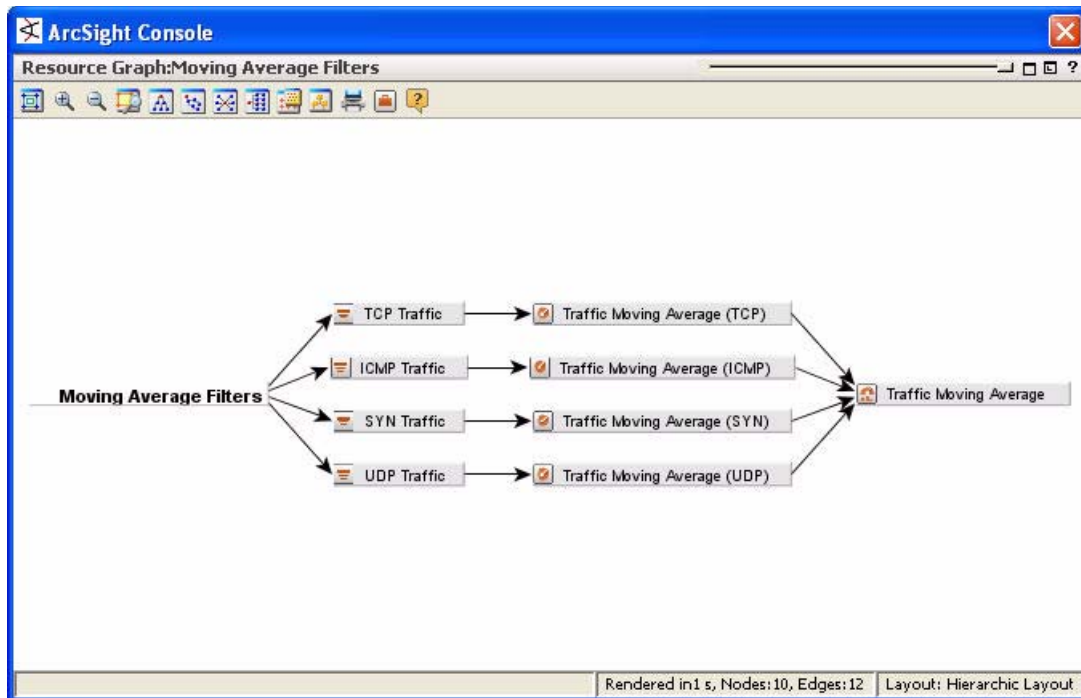
For more about the report queries these filters support, see [“Network Monitoring Reports” on page 269](#).

Moving Average Filters

These filters define events from network reporting devices (by default, Argus) that use specific transport protocols. The results are consumed by the moving average data monitors.

Filter	Description
ICMP Traffic	This filter is looking for ICMP traffic.
SYN Traffic	This filter is looking for SYN (TCP transaction request) traffic.
TCP Traffic	This filter is looking for TCP traffic.
UDP Traffic	This filter is looking for UDP traffic.

These filters are consumed by the data monitors that support the Traffic Moving Average dashboard:



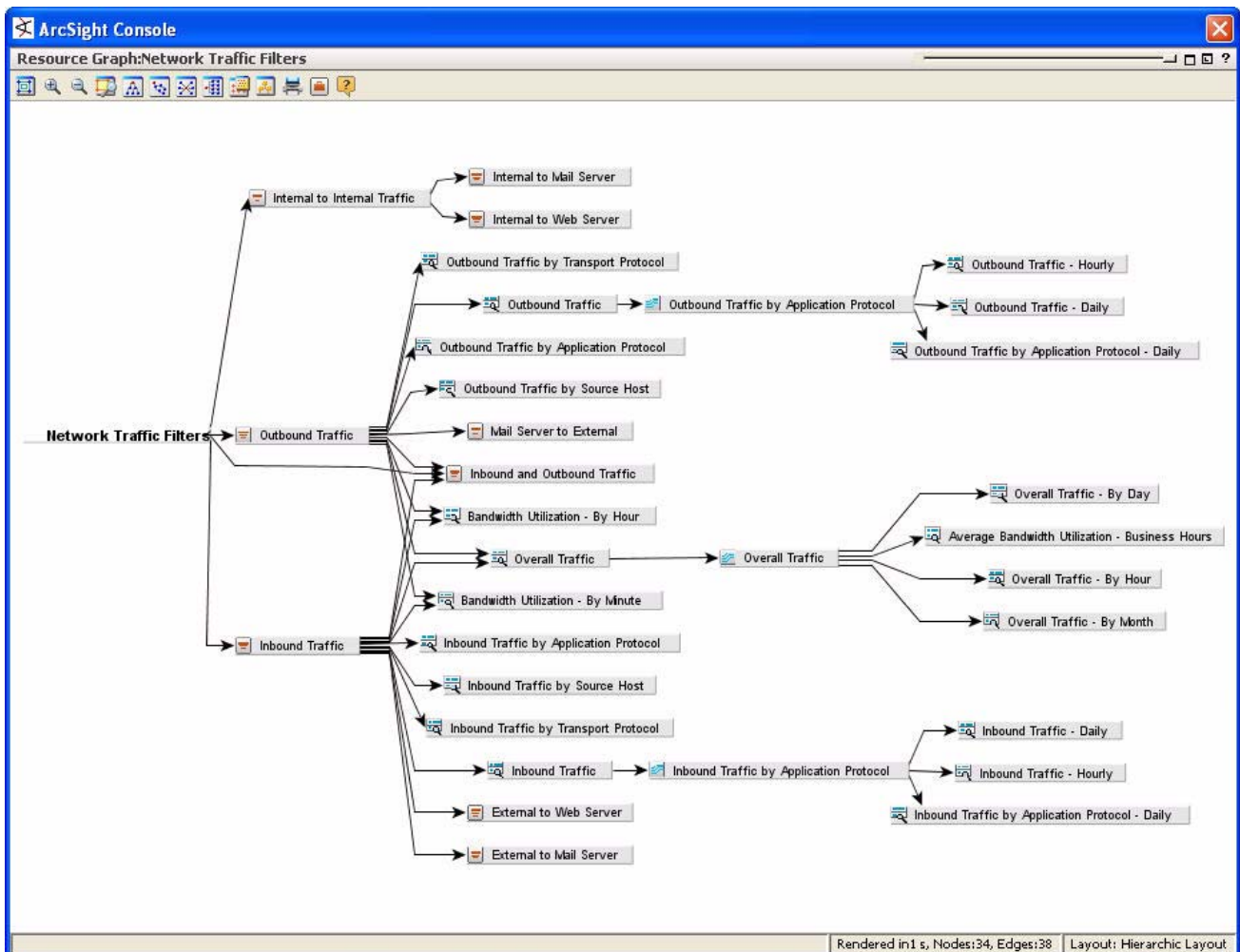
For more about how these filters are used by the various moving average data monitors, see ["Network Monitoring Dashboards and Data Monitors" on page 259](#).

Network Traffic Filters

These Filters are used by almost all the Data Monitors and Report Queries to catch the Argus events and the inbound/outbound conditions. These Filters use the Network Filters (*Inbound events*, *Outbound events*) and the *Network Traffic Reporting Devices* filter. These filters are also used by resources in other foundation suites.

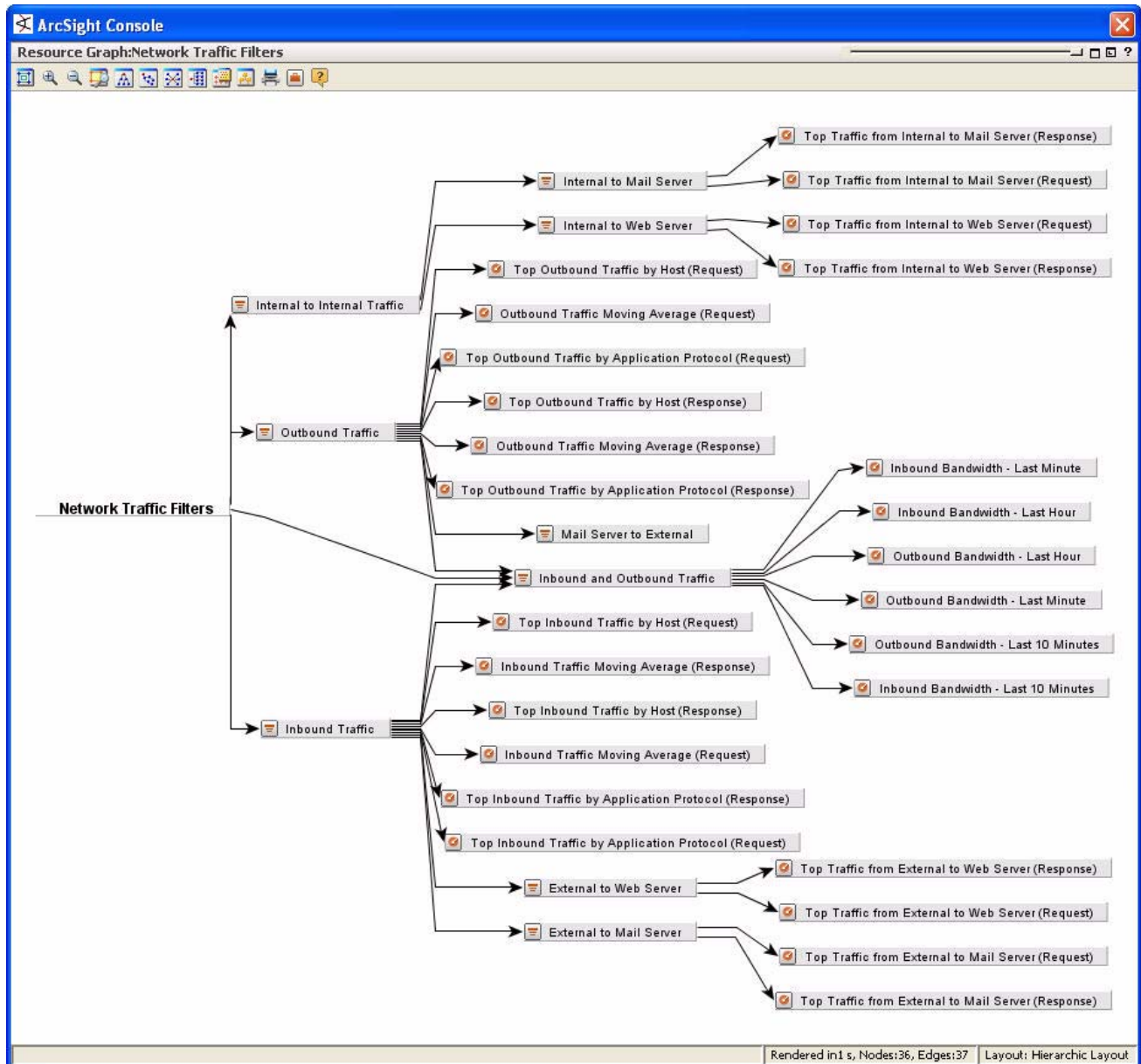
Filter	Description
Inbound Traffic	This filter is looking for Argus events coming from the outside network targeting inside the company network.
Inbound and Outbound Traffic	This filter is looking for Argus inbound events (external to internal) and Argus outbound events (internal to external). This filter is used by all the bandwidth-related Moving Average Data Monitors.
Internal to Internal Traffic	This filter is looking for Argus events internal to the company network.
Outbound Traffic	This filter is looking for Argus events coming from inside the company network targeting the outside network.

The network traffic filters are consumed by the following report queries and trends:



For more about how these filters are used by network monitoring trends and queries, see [“Network Monitoring Reports” on page 269](#).

They are also consumed by the following top traffic and bandwidth monitoring data monitors:



For more about how these filters are used by network monitoring dashboards, see [“Bandwidth Usage Dashboards” on page 260](#), and [“General Dashboards” on page 262](#).

Report Parameter Filters

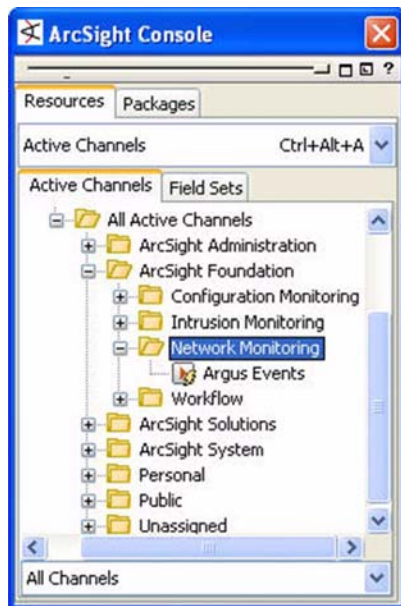
The Report Parameter Filters are used only in the “SANS Top 5 Traffic Moving Average” Report as parameter filters.

Filter	Description
ICMP Traffic	This Filter is used by a Report Parameter to select ICMP Traffic.
TCP Traffic	This Filter is used by a Report Parameter to select TCP Traffic.
UDP Traffic	This Filter is used by a Report Parameter to select UDP Traffic.

These filters look for at all the correlation events generated by the TCP, UDP, and ICMP Moving Average Data Monitors when the Moving Average goes up by 50% or more. When a 50% spike occurs, the filters find the correlation events named “ICMP Traffic Spike”, “TCP Traffic Spike”, or “UDP Traffic Spike”. The result sets are then read by the “SANS Top 5 Traffic Moving Average” report.

Network Monitoring Active Channel

The Network Monitoring foundation contains one active channel to monitor events from the Qosient Argus network monitoring device.



Active Channel: The Argus Events active channel displays the events coming from the Argus network monitoring device.

This active channel shows all the events coming from the Argus SmartConnectors for the last 24 hours.



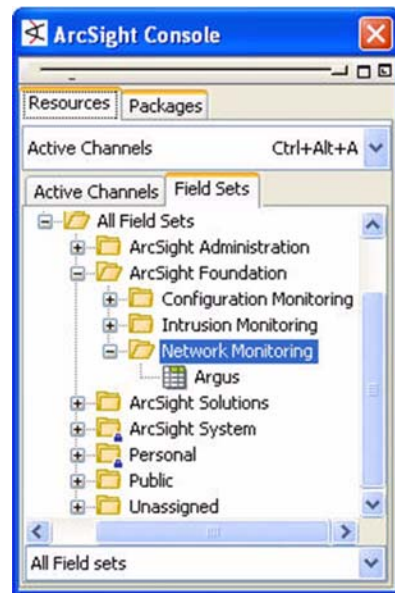
If you use a network monitoring device other than Qosient Argus and you created a filter other than the Qosient Argus filter (as outlined in ["Configuration Overview" on page 246](#)), you should modify the Filter condition on the Argus Events active channel to point to the new filter(s).

How to Use the Network Monitoring Active Channel

Use this active channel to verify that events are being received from Argus as expected. This verifies that Connector configuration is correct.

Network Monitoring Field Sets

The Network Monitoring foundation comes with one field set that focuses on the required fields from Qosient Argus.



Argus Field Set: This field set concentrates on the Qosient Argus event fields that are relevant to ArcSight.

- Attacker
- Target
- Ports
- Bytes in
- Bytes out

This field set is used by the Network Monitoring Active Channel.



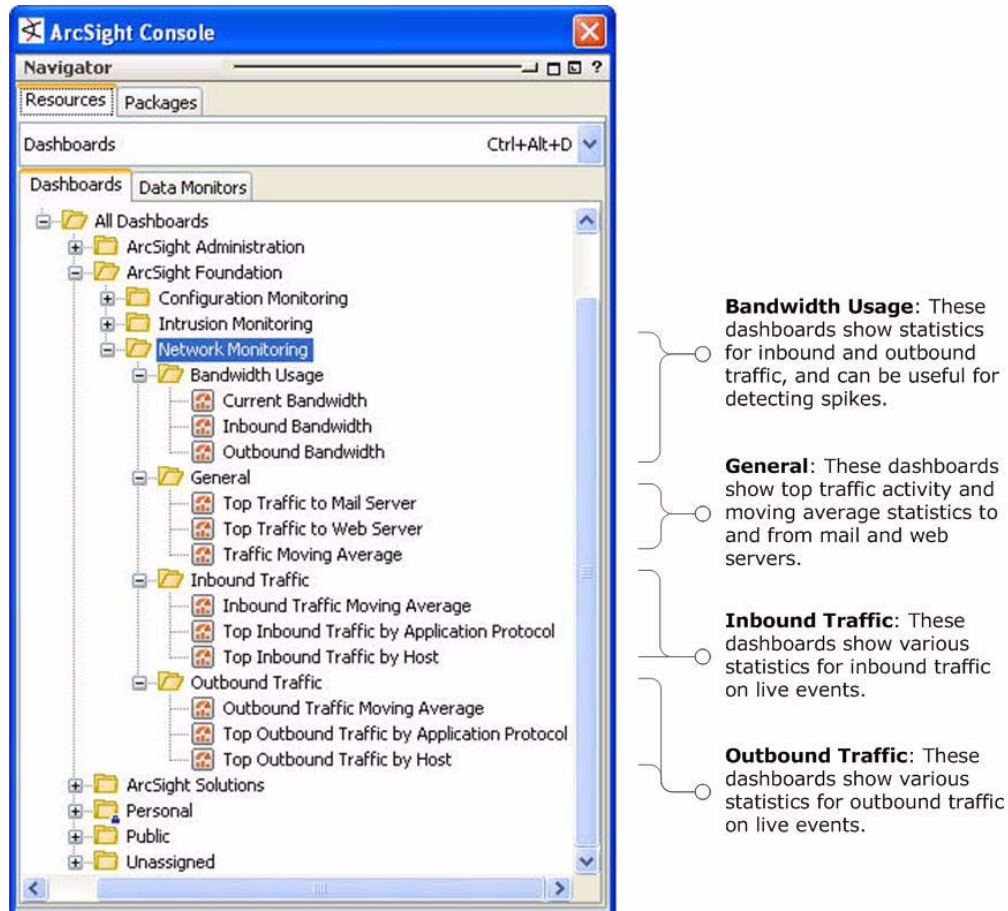
If you have configured your system to use a network flow device other than Argus, it is recommended that you:

1. make a copy of the Argus field set and rename the copy
2. change any of the fields as appropriate for your network flow device
3. use the field set with a copy of the Network Monitoring active channel.

Network Monitoring Dashboards and Data Monitors

Dashboards are made up of individual data monitors in a variety of graphical and tabular formats that summarize the live event flow and communicate the effect of event traffic on specific network systems. Like the instrument panel of a car, dashboards communicate the state of your enterprise from the various key systems that indicate network health.

Dashboards display live event data, and are part of regular daily monitoring and investigation. The Network Monitoring foundation operates on events from Argus (or whatever network flow device you configured in [“Configuration Overview” on page 246](#)), and contains four main groups of dashboards:



Each dashboard in these groups is made up of one or more data monitors, which express the event conditions and specify the display format viewed in the dashboard. This section introduces each group of dashboards, their intended purpose, and how to interact with them. It also introduces the data monitors that make up the dashboard, and the other resources that support them.

Bandwidth Usage Dashboards

Bandwidth measures bytes in and bytes out per second. A sustained spike could indicate something wrong, such as a device not working or a user making a large request that might not be authorized.

For example, the inbound bandwidth dashboard shows three views: Inbound bandwidth in the last 10 minutes, the last hour, and last minute.

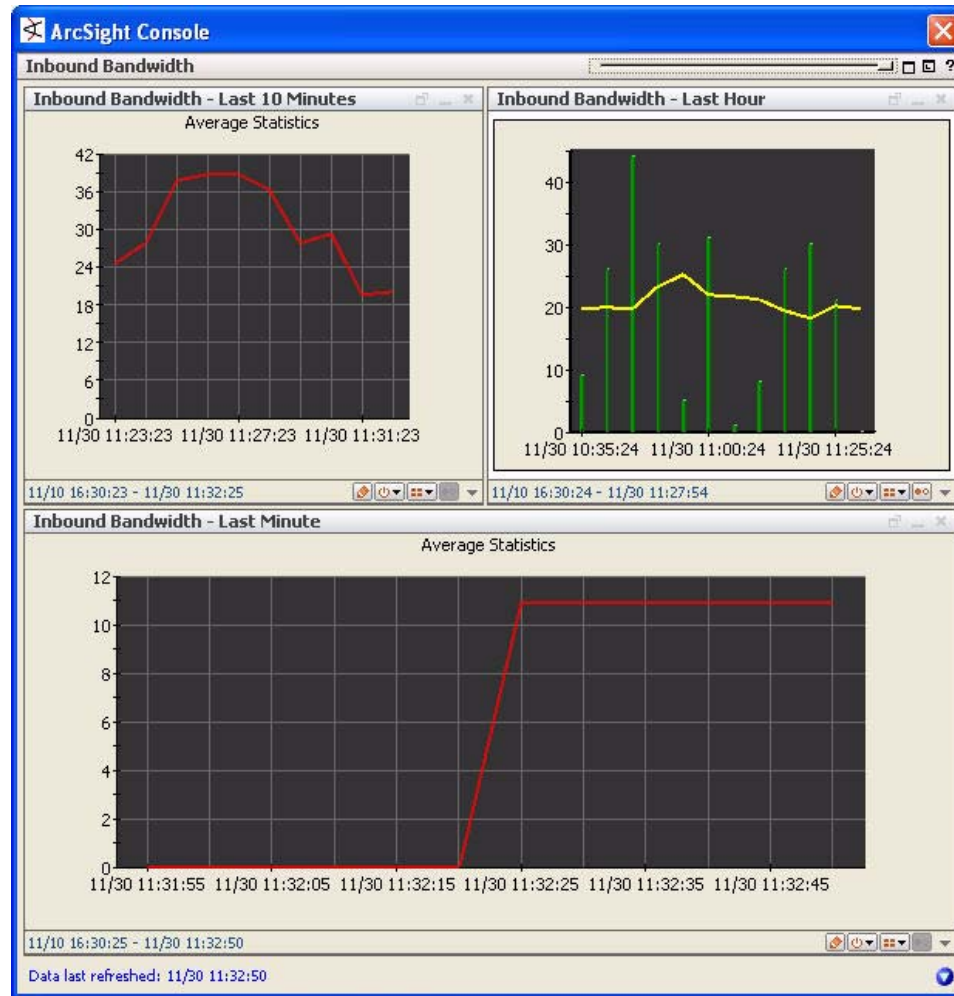


Figure 6-2 Check the bandwidth usage dashboards regularly to monitor bytes in and bytes out, and to detect unwarranted spikes.

Dashboard	Description
Current Bandwidth	This dashboard shows an overview of the current bandwidth usage. This dashboard contains two data monitors: "Inbound Bandwidth - Last Minute" and "Outbound Bandwidth - Last Minute".
Inbound Bandwidth	This dashboard shows an overview of the Inbound Bandwidth. This dashboard contains 3 data monitors: "Inbound Bandwidth - Last 10 Minutes", "Inbound Bandwidth - Last Hour", and "Inbound Bandwidth - Last Minute".

Dashboard	Description
Outbound Bandwidth	This dashboard shows an overview of the Outbound Bandwidth. This dashboard contains 3 data monitors: "Outbound Bandwidth - Last 10 Minutes", "Outbound Bandwidth - Last Hour", and "Outbound Bandwidth - Last Minute".

Bandwidth Usage Data Monitors

The following data monitors contribute to the bandwidth usage dashboards:

Current Bandwidth: The current bandwidth data monitors show bytes per second in a moving average over the last minute.

Inbound Bandwidth: These data monitors show bytes per second for inbound traffic in a moving average over three different timeframes.

Outbound Bandwidth: These data monitors show bytes per second for outbound traffic in a moving average over three different timeframes.

These data monitors are described in more detail below:

Data Monitor	Description
Inbound Bandwidth - Last Minute	This Moving Average Data Monitor shows the inbound bandwidth (bytes/sec) for the last minute. The bandwidth values are updated every 5 seconds.
Outbound Bandwidth - Last Minute	This Moving Average Data Monitor shows the outbound bandwidth (bytes/sec) for the last minute. The bandwidth values are updated every 5 seconds.
Inbound Bandwidth - Last 10 Minutes	This Moving Average Data Monitor shows the average inbound bandwidth (bytes/sec) for the last 10 minutes. The values are updated every 30 seconds.

Data Monitor	Description
Inbound Bandwidth - Last Hour	This Moving Average Data Monitor shows the average inbound bandwidth (bytes/sec) for the last hour. The values are updated every 5 minutes.
Outbound Bandwidth - Last 10 Minutes	This Moving Average Data Monitor shows the average outbound bandwidth (bytes/sec) for the last 10 minutes. The values are updated every 30 seconds.
Outbound Bandwidth - Last Hour	This Moving Average Data Monitor shows the average outbound bandwidth (bytes/sec) for the last hour. The values are updated every 5 minutes.

General Dashboards

The General dashboards show the top traffic to mail and web servers, and traffic moving average for TCP, UDP, ICMP, and SYN protocols.



Configuration Tip: The Top Traffic to Mail and Web Servers dashboards monitor traffic that targets internal assets. In order to activate these dashboards, your mail servers must be categorized in the Email asset category group ([All Asset Categories/Site Asset Categories/Application/Type/Email](#)), and your web servers must be categorized in the Web Server asset category group ([All Asset Categories/Site Asset Categories/Application/Type/Web Server](#)). For tips about how to categorize groups of assets, see ["Asset Categories" on page 30](#).

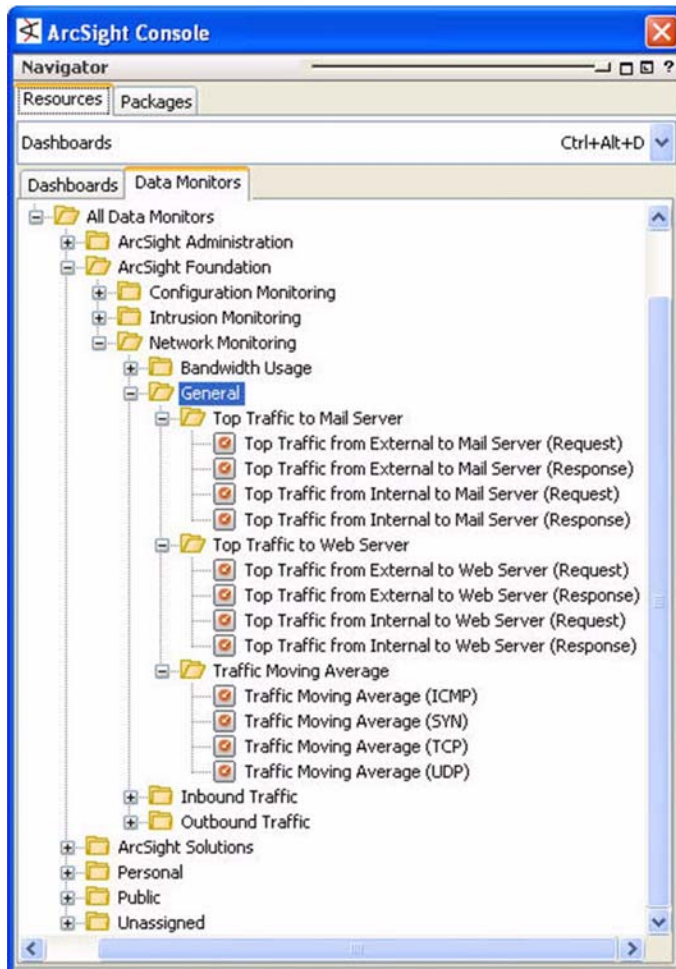
If you have created your own asset categories that are relevant to the top traffic dashboards, you can add those asset categories to the corresponding filter ([All Filters/ArcSight Foundation/Network Monitoring/Application Filters](#)).

The General dashboards are described in more detail below:

Dashboard	Description
Top Traffic to Mail Server	This dashboard shows an overview of the traffic targeting internal hosts categorized as mail servers. This dashboard contains 4 data monitors: "Top Traffic from External to Mail Server (Request)", "Top Traffic from External to Mail Server (Response)", "Top Traffic from Internal to Mail Server (Request)", and "Top Traffic from Internal to Mail Server (Response)".
Top Traffic to Web Server	This dashboard shows an overview of the traffic targeting internal hosts categorized as web servers. This dashboard contains 4 data monitors: "Top Traffic from External to Web Server (Request)", "Top Traffic from External to Web Server (Response)", "Top Traffic from Internal to Web Server (Request)", and "Top Traffic from Internal to Web Server (Response)".
Traffic Moving Average	This dashboard a moving average of the ICMP, SYN, and UDP traffic. This dashboard contains 3 data monitors: "Traffic Moving Average (ICMP)", "Traffic Moving Average (SYN)", and "Traffic Moving Average (UDP)".

General Data Monitors

The General data monitors calculate the top traffic to and from mail and web servers.



Top Traffic to Mail Server:
These data monitors provide statistics on the top traffic to and from mail servers.

Top Traffic to Web Server:
These data monitors provide statistics on the top traffic to and from web servers.

Traffic Moving Average:
These data monitors show moving average statistics for events using various transfer protocols.

The Traffic Moving Average data monitors send a correlation event called "ICMP Traffic Spike", "TCP Traffic Spike", or "UDP Traffic Spike" if the average number of packets goes up by 50% or more in a 5-minute time frame. The correlation events are detected by the Report Parameter Filters and the Network Monitoring rules, and are consumed by the *SANS Top 5 Traffic Moving Average* report.

These data monitors are described in more detail below:

Data Monitor	Description
Top Traffic from External to Mail Server (Request)	This data monitor shows the 10 external source hosts with the highest amount of traffic targeting internal hosts categorized as mail servers. This data monitor focuses on the total number of bytes contained in the requests the external source hosts are sending to the mail servers.
Top Traffic from External to Mail Server (Response)	This data monitor shows the 10 external source hosts with the highest amount of traffic targeting internal hosts categorized as mail servers. This data monitor focuses on the total number of bytes contained in the responses the external source hosts are sending to the mail servers.

Data Monitor	Description
Top Traffic from Internal to Mail Server (Request)	This data monitor shows the 10 internal source hosts with the highest amount of traffic targeting internal hosts categorized as mail servers. This data monitor focuses on the total number of bytes contained in the requests the internal source hosts are sending to the mail servers.
Top Traffic from Internal to Mail Server (Response)	This data monitor shows the 10 internal source hosts with the highest amount of traffic targeting internal hosts categorized as mail servers. This data monitor focuses on the total number of bytes contained in the response the internal source hosts get from the mail servers.
Top Traffic from External to Web Server (Request)	This data monitor shows the 10 external source hosts with the highest amount of traffic targeting internal hosts categorized as web servers. This data monitor focuses on the total number of bytes contained in the requests the external source hosts are sending to the web servers.
Top Traffic from External to Web Server (Response)	This data monitor shows the 10 external source hosts with the highest amount of traffic targeting internal hosts categorized as web servers. This data monitor focuses on the total number of bytes contained in the responses the external source hosts are sending to the web servers.
Top Traffic from Internal to Web Server (Request)	This data monitor shows the 10 internal source hosts with the highest amount of traffic targeting internal hosts categorized as web servers. This data monitor focuses on the total number of bytes contained in the requests the internal source hosts are sending to the web servers.
Top Traffic from Internal to Web Server (Response)	This data monitor shows the 10 internal source hosts with the highest amount of traffic targeting internal hosts categorized as web servers. This data monitor focuses on the total number of bytes contained in the response the internal source hosts get from the web servers.
Traffic Moving Average (ICMP)	This data monitor shows a moving average of the incoming ICMP traffic. This data monitor shows the moving average of the number of ICMP packets per minute for the last hour using twelve 5-minutes buckets.
Traffic Moving Average (SYN)	This data monitor shows a moving average of the incoming SYN traffic (TCP connection requests). This data monitor shows the moving average of the number of SYN packets per minute for the last hour using twelve 5-minutes buckets.
Traffic Moving Average (TCP)	This data monitor shows a moving average of the incoming UDP traffic. This data monitor shows the moving average of the number of UDP packets per minute for the last hour using twelve 5-minutes buckets.
Traffic Moving Average (UDP)	This data monitor shows a moving average of the incoming UDP traffic. This data monitor shows the moving average of the number of UDP packets per minute for the last hour using twelve 5-minutes buckets.

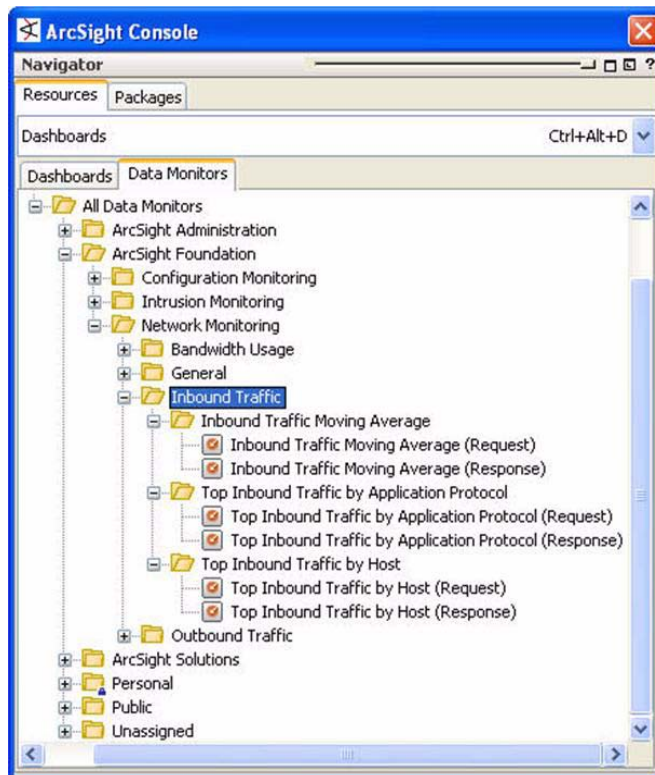
Inbound Traffic Dashboards

The Inbound Traffic dashboards show various statistics for inbound traffic.

Dashboard	Description
Inbound Traffic Moving Average	This dashboard shows a moving average of the inbound traffic (i.e. external network to internal network) for the last hour. This dashboard contains 2 data monitors: "Inbound Traffic Moving Average (Request)" and "Inbound Traffic Moving Average (Response)".
Top Inbound Traffic by Application Protocol	This dashboard shows an overview of the inbound traffic (i.e. external network to internal network) by application protocol. This dashboard contains 2 data monitors: "Top Inbound Traffic by Application Protocol (Request)" and "Top Inbound Traffic by Application Protocol (Response)".
Top Inbound Traffic by Host	This dashboard shows an overview of the inbound traffic (i.e. external network to internal network) by source host. This dashboard contains 2 data monitors: "Top Inbound Traffic by Host (Request)" and "Top Inbound Traffic by Host (Response)".

Inbound Traffic Data Monitors

The Inbound Traffic Data Monitors track bytes in for bandwidth-related dashboards. To get consistent statistics, Variables track requests as bytes in and responses as bytes out.



Top Inbound Traffic Moving Average: These data monitors track bytes in and bytes out per application protocol for bandwidth-related dashboards.

Top Inbound Traffic by Application Protocol: These data monitors track bytes in and bytes out per application protocol for bandwidth-related dashboards.

Top Inbound Traffic by Host: These data monitors track bytes in and bytes out per host name for bandwidth-related dashboards.

These data monitors are described in more detail below.

Data Monitor	Description
Inbound Traffic Moving Average (Request)	This data monitor shows a moving average of the inbound traffic (i.e. external network to internal network). This data monitor focuses on the bytes contained in the requests the external hosts are sending to the internal hosts. This data monitor shows the average amount of bytes/sec for the last hour using twelve 5-minutes buckets.
Inbound Traffic Moving Average (Response)	This data monitor shows a moving average of the inbound traffic (i.e. external network to internal network). This data monitor focuses on the bytes contained in the responses the external hosts get from the internal hosts. This data monitor shows the average amount of bytes/sec for the last hour using twelve 5-minutes buckets.
Top Inbound Traffic by Application Protocol (Request)	This data monitor shows the 10 application protocols with the highest amount of inbound traffic (i.e. external network to internal network). This data monitor focuses on the total number of bytes by application protocol contained in the requests the external hosts are sending to the internal hosts.
Top Inbound Traffic by Application Protocol (Response)	This data monitor shows the 10 application protocols with the highest amount of inbound traffic (i.e. external network to internal network). This data monitor focuses on the total number of bytes by application protocol contained in the responses the external hosts get from the internal hosts.
Top Inbound Traffic by Host (Request)	This data monitor shows the 10 source hosts with the highest amount of inbound traffic (i.e. external network to internal network). This data monitor focuses on the total number of bytes contained in the requests the host is sending to the internal network.
Top Inbound Traffic by Host (Response)	This data monitor shows the 10 source hosts with the highest amount of inbound traffic (i.e. external network to internal network). This data monitor focuses on the total number of bytes contained in the responses the host gets from the external network.

Outbound Traffic Dashboards

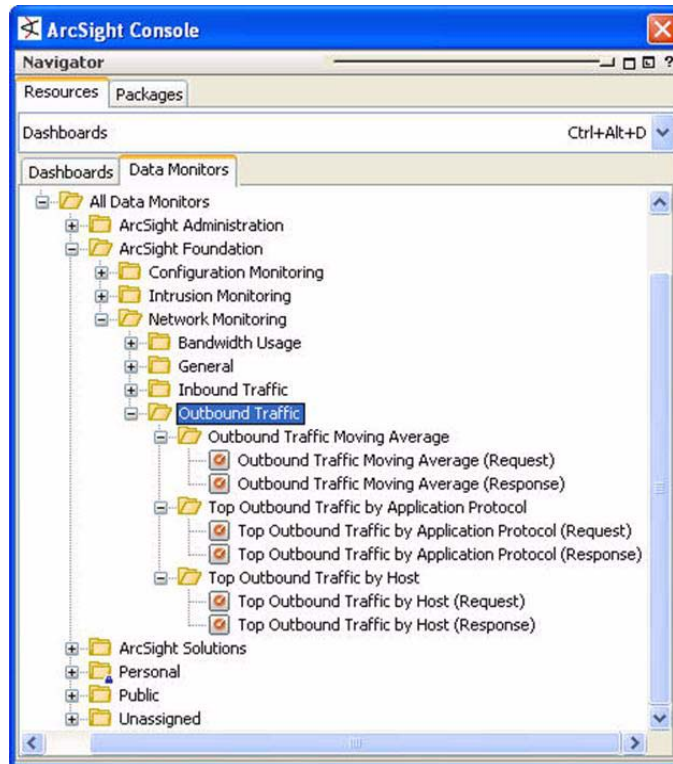
The Outbound Traffic dashboards show various statistics for outbound traffic.

Dashboard	Description
Outbound Traffic Moving Average	This dashboard shows a moving average of the outbound traffic (i.e. internal network to external network) for the last hour. This dashboard contains 2 data monitors: "Outbound Traffic Moving Average (Request)" and "Outbound Traffic Moving Average (Response)".
Top Outbound Traffic by Application Protocol	This dashboard shows an overview of the outbound traffic (i.e. internal network to external network) by application protocol. This dashboard contains 2 data monitors: "Top Outbound Traffic by Application Protocol (Request)" and "Top Outbound Traffic by Application Protocol (Response)".

Dashboard	Description
Top Outbound Traffic by Host	This dashboard shows an overview of the outbound traffic (i.e. internal network to external network) by source host. This dashboard contains 2 data monitors: "Top Outbound Traffic by Host (Request)" and "Top Outbound Traffic by Host (Response)".

Outbound Traffic Data Monitors

The outbound traffic data monitors track bytes out for bandwidth-related dashboards.



Outbound Traffic Moving Average: These data monitors track bytes in and bytes out in a moving average over the last hour.

Top Outbound Traffic by Application Protocol: These data monitors track bytes in and bytes out per application protocol for bandwidth-related dashboards.

Top Outbound Traffic by Host: These data monitors track bytes in and bytes out per host name for bandwidth-related dashboards.

These data monitors are described in more detail below.

Data Monitor	Description
Outbound Traffic Moving Average (Request)	This data monitor shows a moving average of the outbound traffic (i.e. internal network to external network). This data monitor focuses on the bytes contained in the requests the internal hosts are sending to the external hosts. This data monitor shows the average amount of bytes/sec for the last hour using twelve 5-minutes buckets.
Outbound Traffic Moving Average (Response)	This data monitor shows a moving average of the outbound traffic (i.e. internal network to external network). This data monitor focuses on the bytes contained in the responses the internal hosts get from the external hosts. This data monitor shows the average amount of bytes/sec for the last hour using twelve 5-minutes buckets.

Data Monitor	Description
Top Outbound Traffic by Application Protocol (Request)	This data monitor shows the 10 application protocols with the highest amount of outbound traffic (i.e. internal network to external network). This data monitor focuses on the total number of bytes by application protocol contained in the requests the internal hosts are sending to the external hosts.
Top Outbound Traffic by Application Protocol (Response)	This data monitor shows the 10 application protocols with the highest amount of outbound traffic (i.e. internal network to external network). This data monitor focuses on the total number of bytes by application protocol contained in the responses the internal hosts get from the external hosts.
Top Outbound Traffic by Host (Request)	This data monitor shows the 10 source hosts with the highest amount of outbound traffic (i.e. internal network to external network). This data monitor focuses on the total number of bytes contained in the requests the internal host is sending to the external network.
Top Outbound Traffic by Host (Response)	This data monitor shows the 10 source hosts with the highest amount of outbound traffic (i.e. internal network to external network). This data monitor focuses on the total number of bytes contained in the responses the internal host gets from the external network.

Network Monitoring Reports

The reporting tools for ESM 4.0 have been significantly expanded and improved to be more robust, more configurable, and more flexible.

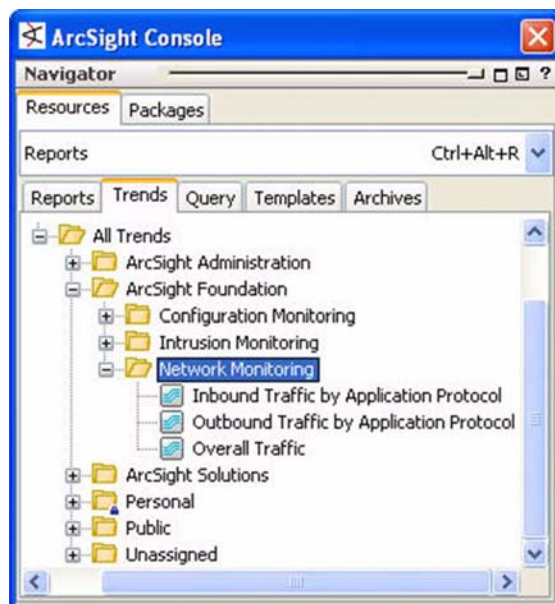
The Network Monitoring foundation provides a system of reporting tools that together provide a comprehensive summary of activity from network flow devices. These views are organized into groups depending on what level of detail you need to see:

- **Executive Summaries.** Executive summary reports provide high-level analysis of network monitoring activity for management reports. These views show overall trends and
- **Operational Summaries.** The operational summary reports are intended for SOC operators and analysts for daily network monitoring and triage-level investigation.
- **Details.** The detailed reports are intended for incident responders and analysts who need access to relevant event details in order to investigate situations that arise from monitoring reports in the operational summaries.
- **SANS Top 5 Reports.** The SANS Top 5 reports that are relevant to network monitoring are those that address SANS section 5. Other SANS Top 5 reports are contained in other system content foundation suites.

Network Monitoring Trends

Trends are ArcSight resources that define how and over what time period data will be aggregated and evaluated for trends. A trend gathers data on a defined schedule and time duration, which can then be queried in order to show specific trends in data over time.

The Network Monitoring foundation contains four trends that gather data about inbound and outbound traffic. This data is used by several Network Monitoring reports.



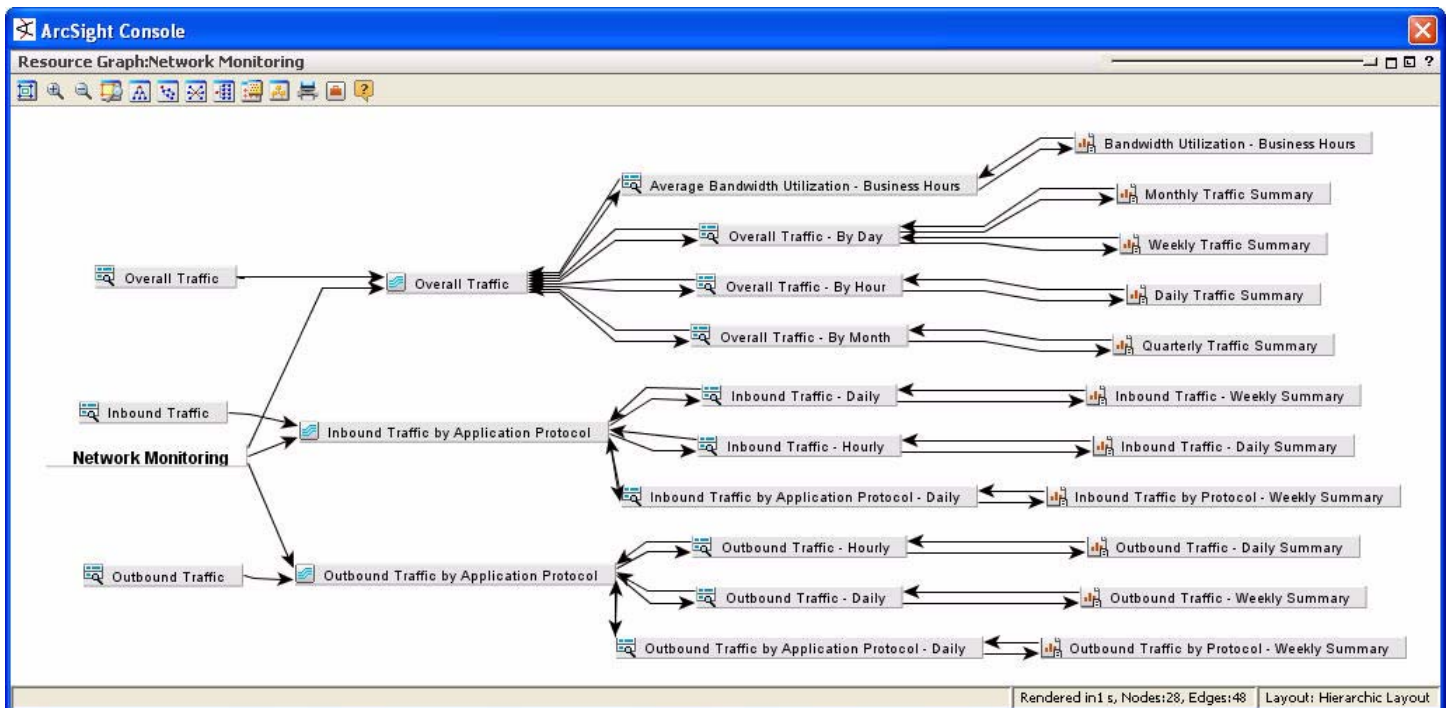
Network Monitoring Trends: These trends gather data about inbound and outbound traffic at specific time intervals, which can be queried in reports.

These trends are described in more detail below:

Trend	Description
Inbound Traffic by Application Protocol	This trend runs every hour using the "Inbound Traffic" query. The trend table stores the total number of bytes contained in the requests and responses and group them by application protocol, target port, and hour.
Outbound Traffic by Application Protocol	This trend runs every hour using the "Outbound Traffic" query. The trend table stores the total number of bytes contained in the requests and responses and group them by application protocol, target port, and hour.
Overall Traffic	This trend runs every day using the "Overall Traffic" query. The trend table stores the total number of Incoming Bytes and Outgoing Bytes per hour.

These trends store values by the hour. For example, the *Overall Traffic* trend calculates the total number of incoming bytes and outgoing bytes in the past hour. Once the trend data is stored in the trend table, the data is available to be queried for reports.

The following Network Monitoring queries and reports consume data from these trends:



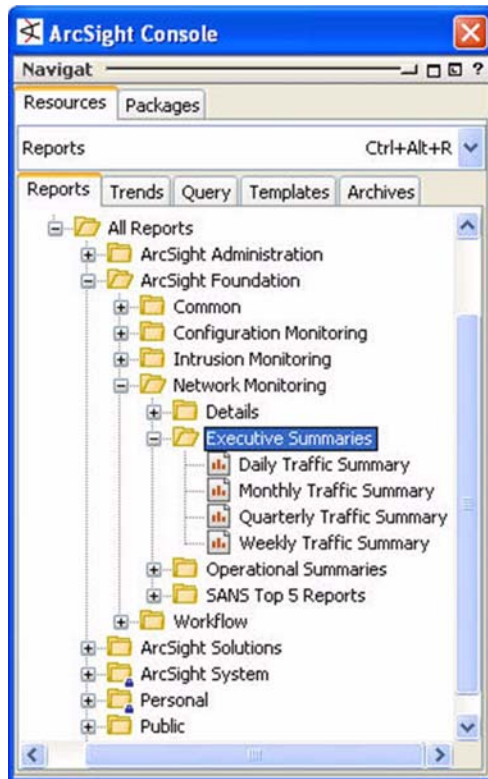
You can also build your own reports based on the data gathered in these trends. You can build any report that requires data over a 24-hour, weekly, or monthly time frame. You can even build a yearly report that shows a sum of activity over the last 12 months.

For a yearly summary report, you only have to query on 24 x 365 (~10,000) rows instead of all the events in the database for the last year.

These trends do not support minute-by-minute details, but they can be used to extract summaries that span an hour or more.

Executive Summaries Reports

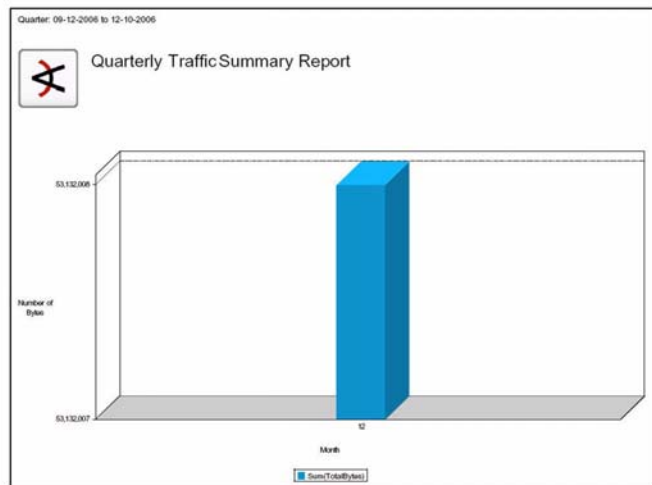
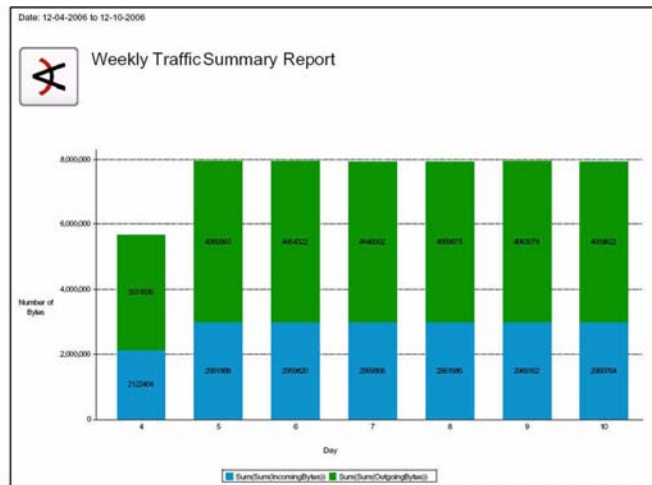
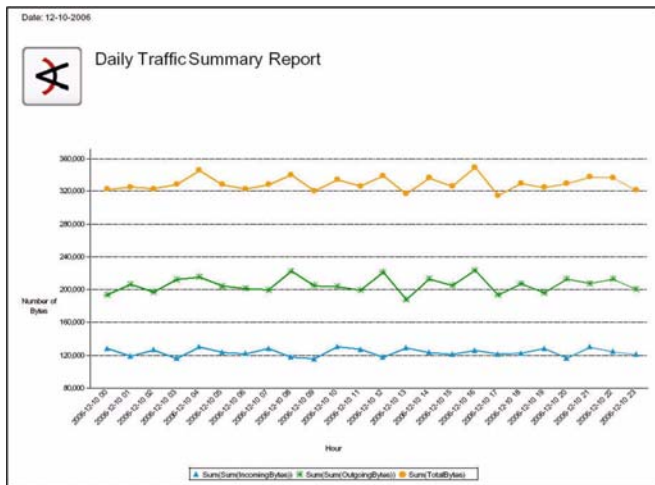
The executive summary reports show high-level views of network inbound and outbound traffic on a daily, weekly, monthly, and quarterly basis.



Executive Summaries:

These reports provide summaries of network flow activity over the indicated time periods.

These summaries show general summaries of traffic over daily, weekly, monthly, and quarterly time frames that can be used for regular operational reporting.



Report	Description
--------	-------------

Daily Traffic Summary	This Report shows a daily traffic summary. The Report contains one line chart showing the number of BytesIN, BytesOUT, and total number of Bytes (BytesIN + BytesOUT).
-----------------------	--

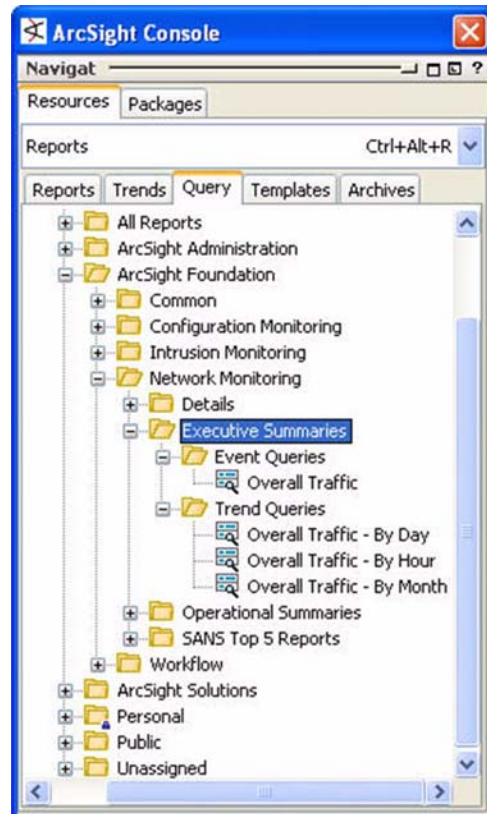
Monthly Traffic Summary	This report shows an executive summary of the traffic for the last month. The Report contains one line chart with two set of values. The first set of values is the total number of bytes for the incoming traffic, and the second set of values is the total number of bytes for the outgoing traffic. These values are grouped by week.
-------------------------	---

Quarterly Traffic Summary	This report shows an executive summary of the traffic for the last quarter. The Report contains one line chart with two set of values. The first set of values is the total number of bytes for the incoming traffic, and the second set of values is the total number of bytes for the outgoing traffic. These values are grouped by week.
---------------------------	---

Report	Description
Weekly Traffic Summary	This report shows an executive summary of the traffic for the last week. The Report contains one line chart with two set of values. The first set of values is the total number of bytes for the incoming traffic, and the second set of values is the total number of bytes for the outgoing traffic. These values are grouped by day.

Executive Summary Queries

These queries supply the data for the executive summaries reports.



Event Queries: The Overall Traffic query supplies the inbound and outbound event data for the Overall Traffic trend.

Trend Queries: These queries poll the trend data gathered by the Network Monitoring trends ([All Trends/ArcSight Foundation/Trends/Network Monitoring](#)).

These queries are described in more detail below.

Query	Description
Overall Traffic	This query is used by the "Overall Traffic" trend. This query looks for the overall number of incoming bytes and outgoing bytes. The incoming bytes are the sum of the number of bytes in the requests in the inbound events (i.e. external network to internal network) and the number of bytes in the responses in the outbound events (i.e. internal network to external network). The outgoing bytes are the sum of the number of bytes in the requests in the outbound events (i.e. internal network to external network) and the number of bytes in the responses in the inbound events (i.e. external network to internal network).

Query	Description
Overall Traffic - By Day	This Query selects the number of Incoming Bytes, Outgoing Bytes, and Total Bytes (Incoming Bytes + Outgoing Bytes) in the "Overall Traffic" Trend Table and groups the values by day.
Overall Traffic - By Hour	This Query selects the number of Incoming Bytes, Outgoing Bytes, and Total Bytes (Incoming Bytes + Outgoing Bytes) in the "Overall Traffic" Trend Table and groups the values by hour.
Overall Traffic - By Month	This Query selects the number of Incoming Bytes, Outgoing Bytes, and Total Bytes (Incoming Bytes + Outgoing Bytes) in the "Overall Traffic" Trend Table and groups the values by month.

Operational Summaries Reports

Operational summaries show more detail about inbound/outbound traffic, and provide statistics, such as top protocols and top source hosts.

Basic reports usually cover the last hour of events. Summaries provide an overview of daily and weekly activity.

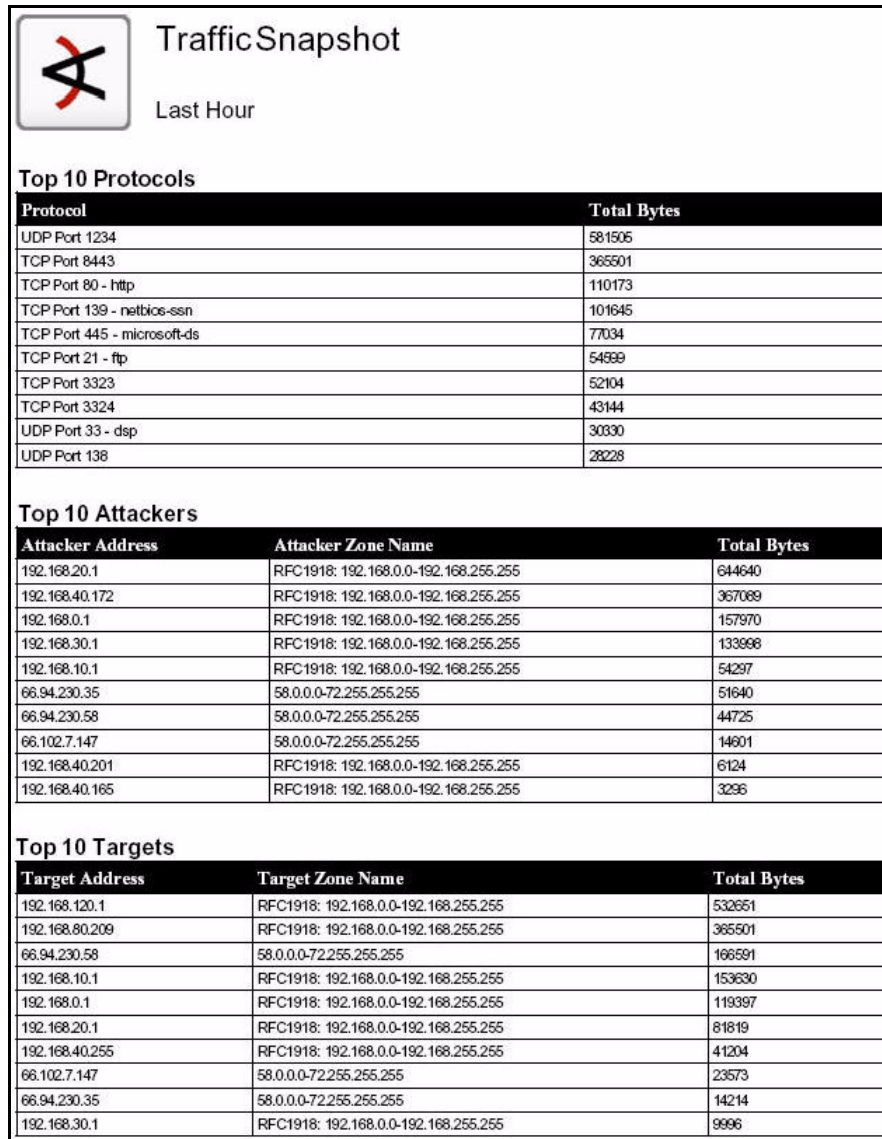
The operational summaries also contain focused reports. A focused report is a query that can be run multiple times on the same set of data with a focus on one parameter variable. For example, the report *Inbound Traffic by Protocol* can show a summary of all transport protocols used in a given data set, or it can be focused on a particular transport protocol, such as HTTP.

The operational summaries reports are divided into the following groups, which are discussed in more detail in the sections that follow:

- Traffic Snapshot
- Bandwidth Utilization
- Inbound Traffic
- Outbound Traffic

Traffic Snapshot Report

The top 10 attackers, targets, and protocols are rolled up in the Traffic Snapshot report.



Report

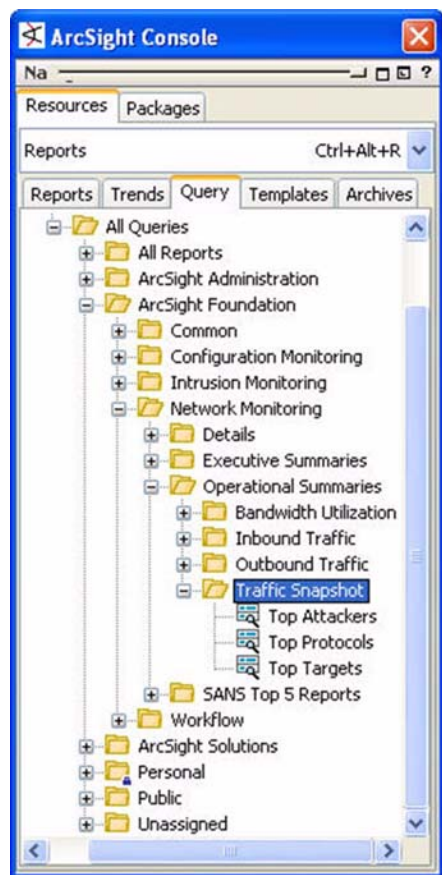
Description

Traffic Snapshot

This Report contains three tables. The first table shows the Top 10 Protocols, the second chart shows the Top 10 Attackers, and the third chart shows the Top 10 Targets.

Traffic Snapshot Queries

The traffic snapshot queries find the current values for the top 10 protocols, attackers, and targets, and consolidate them into one report.



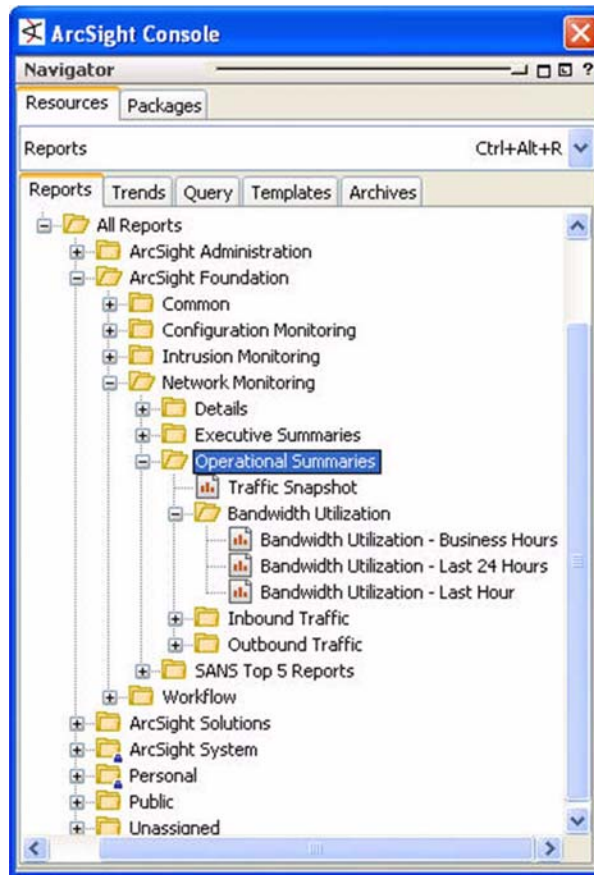
Traffic Snapshot: These queries gather data on the top 10 attackers, targets, and protocols and consolidates it into the *Traffic Snapshot* report.

These queries are described in more detail below:

Query	Description
Top Attackers	This Query selects the Attacker Address/Zone with the highest number of Total Bytes (Bytes In + Bytes Out) in the last hour.
Top Protocols	This Query selects the Protocol with the highest number of Total Bytes (Bytes In + Bytes Out) in the last hour.
Top Targets	This Query selects the Target Address/Zone with the highest number of Total Bytes (Bytes In + Bytes Out) in the last hour.

Bandwidth Utilization Reports

The bandwidth utilization reports provide statistics about bytes in and bytes out.

**Operational Summaries:**

The traffic snapshot report shows a roll-up of the top 10 attackers, targets, and protocols.

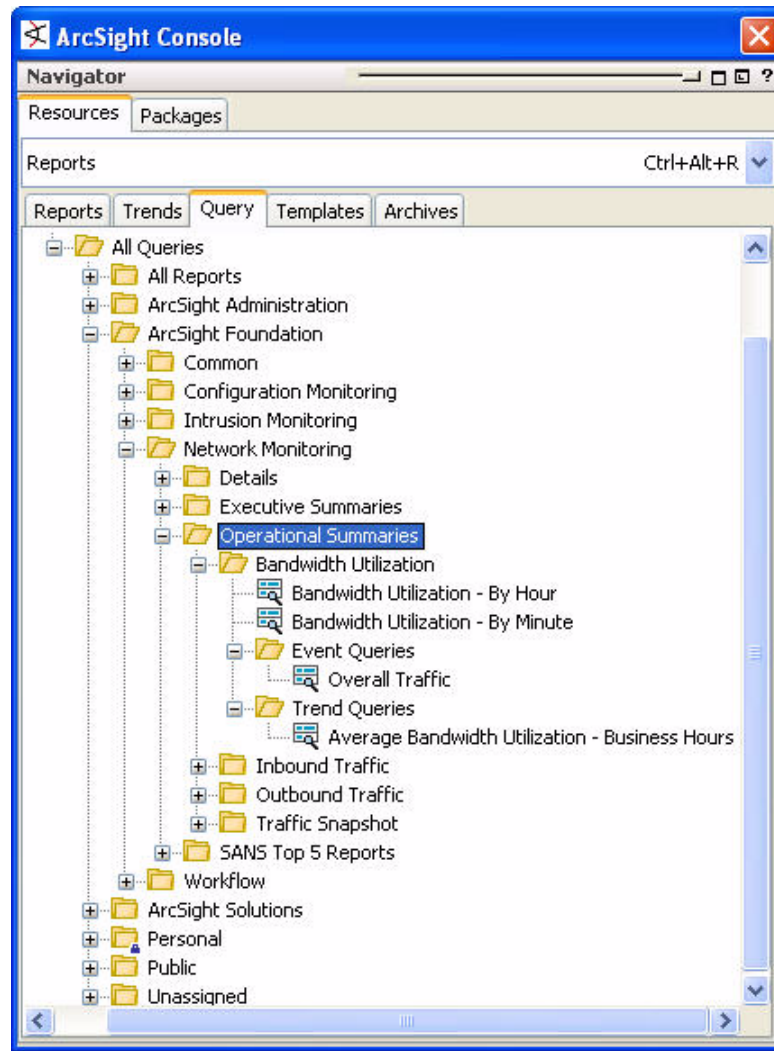
Bandwidth Utilization:

These reports show cumulative bytes in and bytes out during different timeframes.



Bandwidth Utilization Queries

The Bandwidth Utilization queries supply conditions for the Bandwidth Utilization reports.

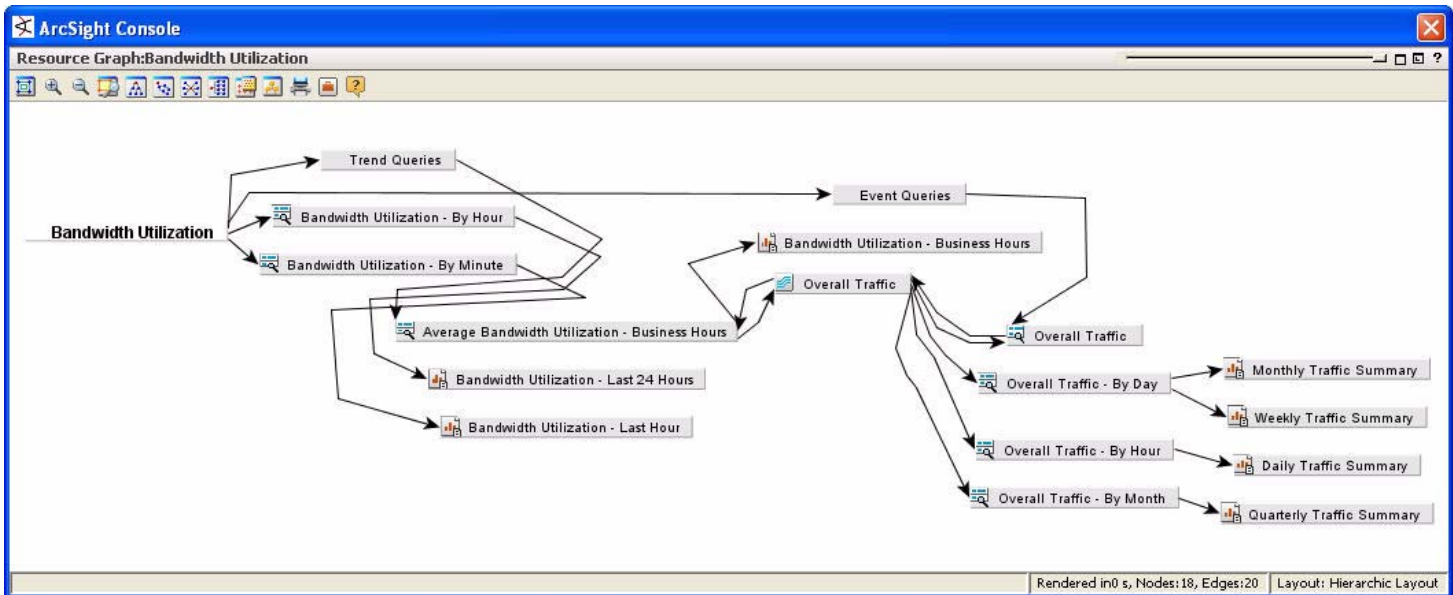


The Bandwidth Utilization queries are described in more detail below.

Query	Description
Bandwidth Utilization - By Hour	This Query selects the average number of Bytes In and Bytes Out per second for the inbound and outbound traffic and groups the values by hour.
Bandwidth Utilization - By Minute	This Query selects the average number of Bytes In and Bytes Out per second for the inbound and outbound traffic and groups the values by minute.

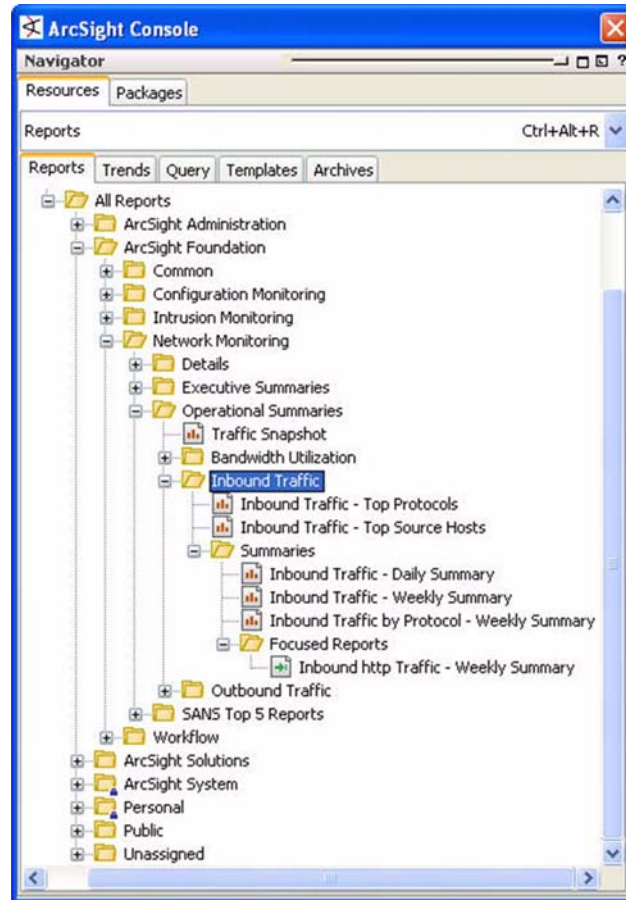
Query	Description
Overall Traffic	This Query is used by the "Overall Traffic" Trend. This Query looks for the overall number of incoming bytes and outgoing bytes. The incoming bytes are the sum of the number of bytes in the requests in the inbound events (i.e. external network to internal network) and the number of bytes in the responses in the outbound events (i.e. internal network to external network). The outgoing bytes are the sum of the number of bytes in the requests in the outbound events (i.e. internal network to external network) and the number of bytes in the responses in the inbound events (i.e. external network to internal network).

These queries are used by the following network monitoring queries and reports:



Inbound Traffic Reports

Inbound traffic reports provide statistics about traffic inbound to your network.



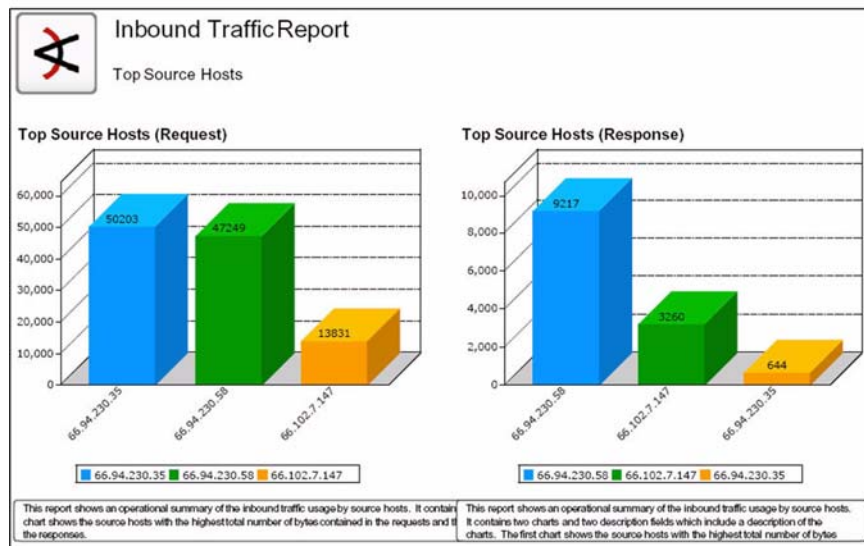
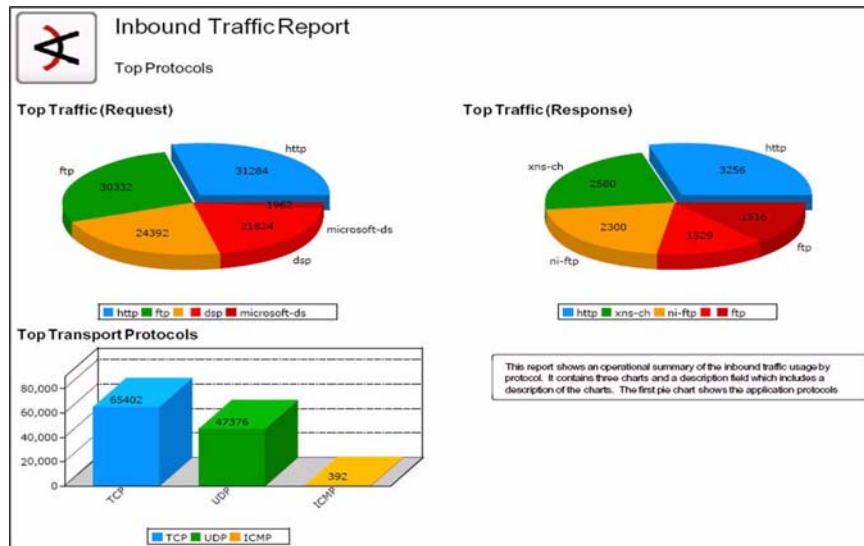
Inbound Traffic: These reports show the top protocols and top source hosts representing bytes in.

Summaries: These reports show daily and weekly summaries of bytes in. The Inbound Traffic by Protocol can be focused on activity involving a particular application protocol.

Focused Reports: The Inbound http Traffic - Weekly Summary is a sample focused report that reports on inbound HTTP traffic.

Inbound Traffic Reports

The Top Protocols and Top Source Hosts provide a profile of the traffic coming into your network. From these views, you can get a profile of regular inbound traffic, and be able to spot spikes and trends.

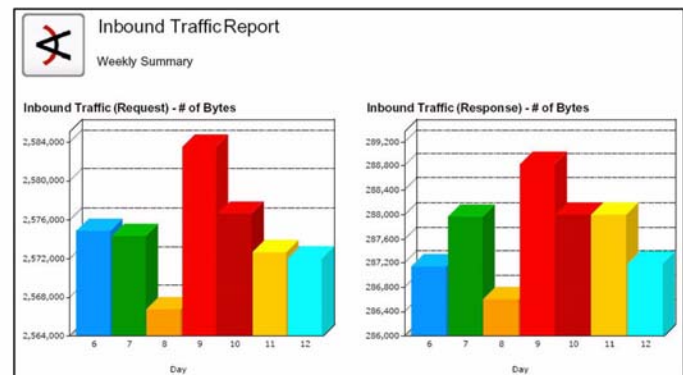
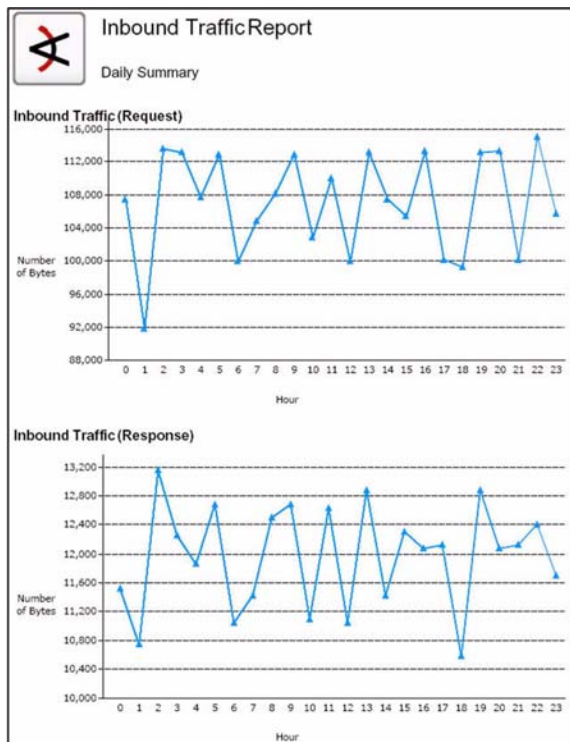


Report	Description
Inbound Traffic - Top Protocols	This report shows an operational summary of the inbound traffic usage by protocol. It contains three charts and a description field which includes a description of the charts. The first pie chart shows the application protocols with the highest total number of bytes contained in the requests, the second pie chart shows the application protocols with the highest total number of bytes contained in the responses, and the bar chart shows the repartition of the inbound traffic by transport protocol (only includes the requests).


Report	Description
Inbound Traffic - Top Source Hosts	This report shows an operational summary of the inbound traffic usage by source hosts. It contains two charts and two description fields which include a description of the charts. The first chart shows the source hosts with the highest total number of bytes contained in the requests and the second chart shows the source hosts with the highest total number of bytes contained in the responses.

Inbound Traffic Summaries

These reports show operational summaries of inbound traffic by the day and by the week. The daily summary graphs bytes in and bytes out for each hour of the day. The weekly summary shows a tally of bytes in and bytes out of the network for each day of the week.



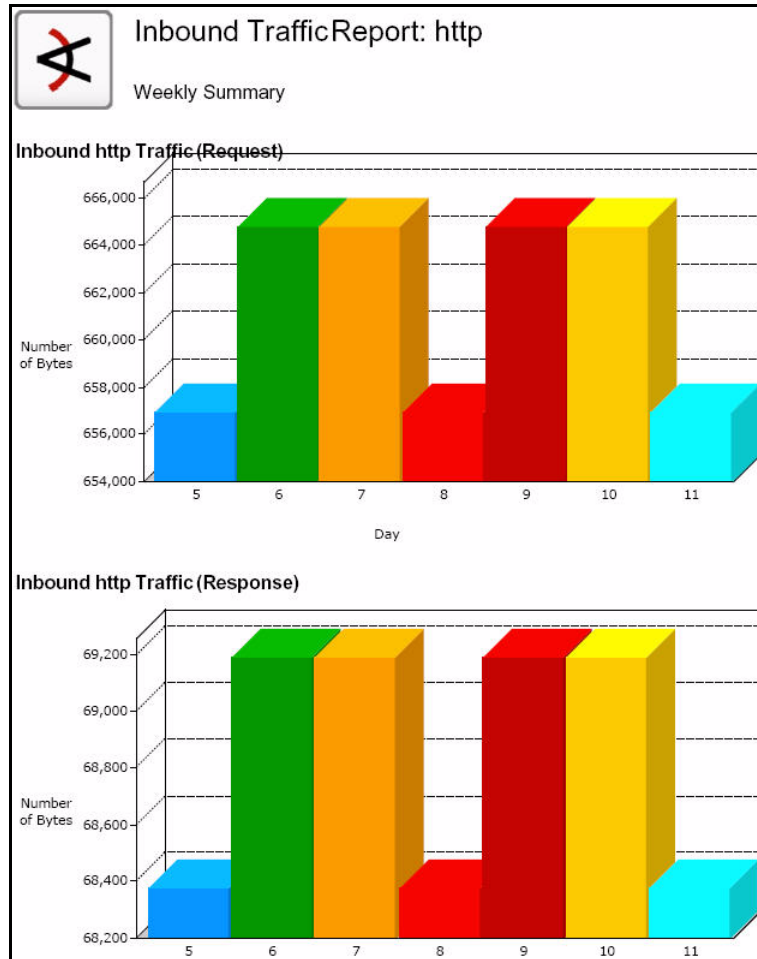
Report	Description
Inbound Traffic - Daily Summary	This report shows an operational summary of the inbound traffic usage for the last day. The first chart shows the total number of bytes contained in the requests by hour. The second chart shows the total number of bytes contained in the responses by hour.
Inbound Traffic - Weekly Summary	This report shows an operational summary of the inbound traffic usage for the last week. The first chart shows the total number of bytes contained in the requests by day. The second chart shows the total number of bytes contained in the responses by day.

Report	Description
 Inbound Traffic by Protocol - Weekly Summary (focusable report)	This report shows an operational summary of the inbound traffic usage for the last week. The first chart shows the total number of bytes contained in the requests by day. The second chart shows the total number of bytes contained in the responses by day. This is a focusable report which allows a user to specify the application protocol he wants to focus on.

Inbound Traffic Focused Reports

This group contains one focused report definition generated from the *Inbound Traffic by Protocol - Weekly Summary* focusable report. This definition focuses on inbound traffic that uses HTTP. Because it's likely that you might run this particular focused report more than once, this focused report definition is saved.

As needed, you can use the *Inbound Traffic by Protocol - Weekly Summary* report to create additional focused reports for other application protocols.



Report	Description
Inbound http Traffic - Weekly Summary	This focused report shows an operational summary of the inbound http traffic usage for the last week. The first chart shows the total number of bytes contained in the requests by day. The second chart shows the total number of bytes contained in the responses by day. This is a focused report depending on the "Inbound Traffic by Protocol - Weekly Summary" Report.

To create a focused report that focuses on another protocol:



- 1 Right-click the focusable report *Inbound Traffic by Protocol - Weekly Summary* ([All Reports/ArcSight Foundation/Network Monitoring/Operational Summaries/Inbound Traffic/Summaries/Inbound Traffic by Protocol - Weekly Summary](#)) and select **New Focused Report**.

- 2 In the Focused Report Editor in the Inspect/Edit panel on the Attributes tab, fill in the following values and click **Apply**:

Field	Value
Name	Enter a name for the focused report, such as Inbound TCP Traffic by
Source Report	This field is automatically filled in by the parent report and is not editable.
Description	Add a description of the report to clarify what it does for other users.

You can add more details to the focused report to help you keep track of it in your own system, such as external ID, alias, owner, and creation information.

- 3 At the Parameters tab, you can change any of the values by removing the checkmark from the *Use Default* column. To specify the parameter you want the report to focus on, scroll down to Custom Parameters in the Reports Parameters section and do the following:

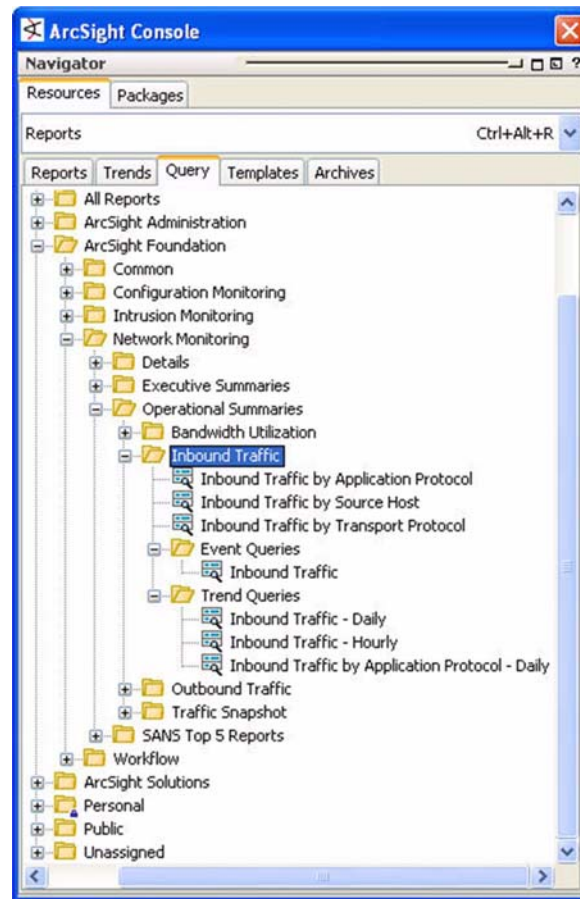
Field	Value
StartTime	To change the time range over which the data is gathered, remove the "Use Default" checkmark and either select a new start time from the drop-down menu, or enter a new start time manually from the  menu.
EndTime	To change the data end time, remove the "Use Default" checkmark and either select a new end time from the drop-down menu, or enter a new end time manually from the  menu.
Application Protocol	Remove the "Use Default" checkmark and enter the application protocol you want to report on, such as <code>ftp</code> .

To run a focused report:

- 1 Right-click the focused report and select **Run > Report with defaults**.
- 2 In the ArcSight Console dialog box, click **Open** to view the report in a browser on screen, or click **Save** to save the report output to the default reports directory.

Inbound Traffic Queries

The Inbound Traffic queries gather the data about inbound bytes that is consumed by the Inbound Traffic reports.



Inbound Traffic: These queries gather data on inbound bytes by application protocol, source host, and transport protocol.

Event Queries: The *Inbound Traffic* query gathers event data that is consumed by the *Inbound Traffic by Application Protocol* trend.

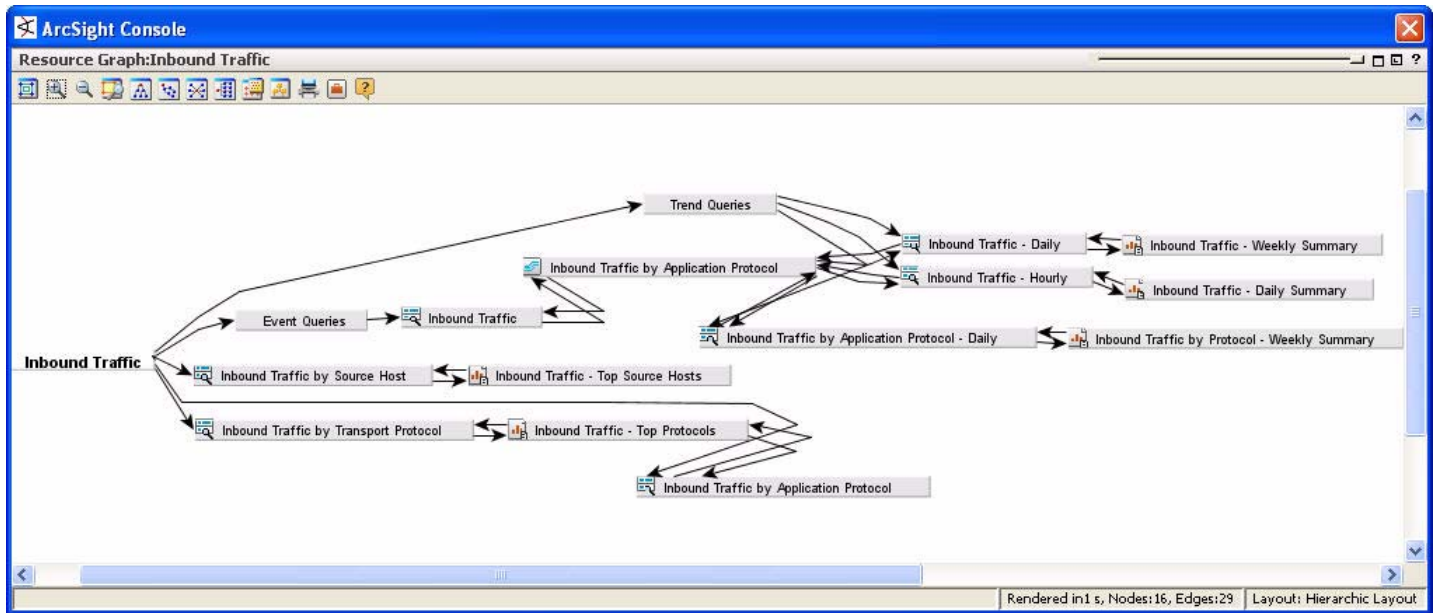
Trend Queries: These queries poll the trend data gathered by the *Inbound Traffic by Application Protocol* trend.

These queries are described in more detail below:

Query	Description
Inbound Traffic by Application Protocol	This query looks for inbound events (i.e. external network to internal network) and groups them by application protocol. The query returns the application protocol and the corresponding sums of bytesIn (request) and bytesOut (response).
Inbound Traffic by Source Host	This query looks for inbound events (i.e. external network to internal network) and groups them by attacker address and attacker zone name. The query returns the attacker address, the attacker zone name, and the corresponding sums of bytesIn (request) and bytesOut (response).
Inbound Traffic by Transport Protocol	This query looks for inbound events (i.e. external network to internal network) and groups them by transport protocol. The query returns the transport protocol and the corresponding sums of bytesIn (request) and bytesOut (response).

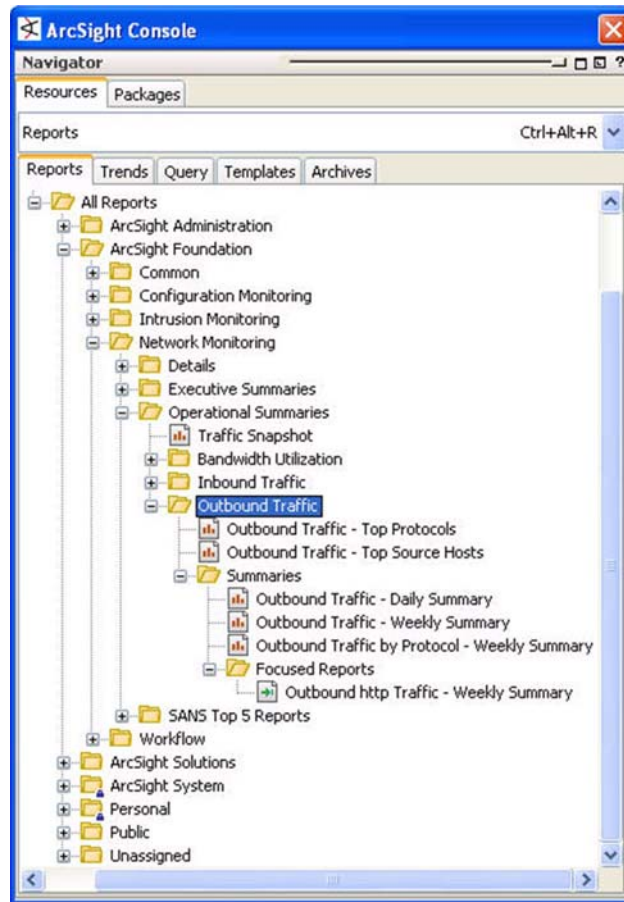
Query	Description
Inbound Traffic	This query is used by the Inbound Traffic by Application Protocol trend. This query looks for inbound events (i.e. external network to internal network) and returns the sums of bytesIn (request) and bytesOut (response) grouped by target port, application protocol, and hour.
Inbound Traffic - Daily	This query retrieves the information stored in the Inbound Traffic by Application Protocol trend. The query returns the sums of bytesIn (request) and bytesOut (response) and groups them by day.
Inbound Traffic - Hourly	This query retrieves the information stored in the Inbound Traffic by Application Protocol trend. The query returns the sums of bytesIn (request) and bytesOut (response) and groups them by hour.
Inbound Traffic by Application Protocol - Daily	This query retrieves the information stored in the Inbound Traffic by Application Protocol trend. The query returns the sums of bytesIn (request) and bytesOut (response) and groups them by day. This query also allows the user to choose a specific application protocol in order to create a focused report such as the Inbound http Traffic Last Week report.

The Inbound Traffic queries are used by the following network monitoring queries and reports:



Outbound Traffic Reports

Outbound traffic reports provide statistics about traffic going out from your network.



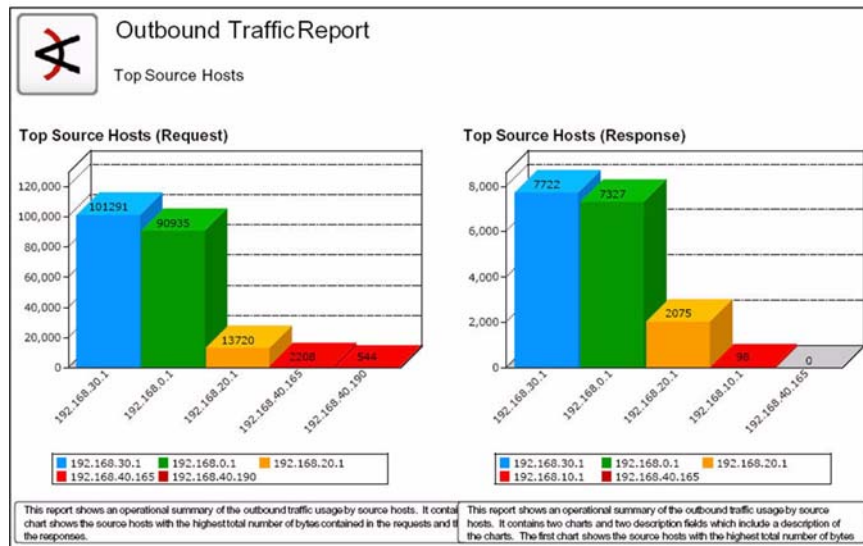
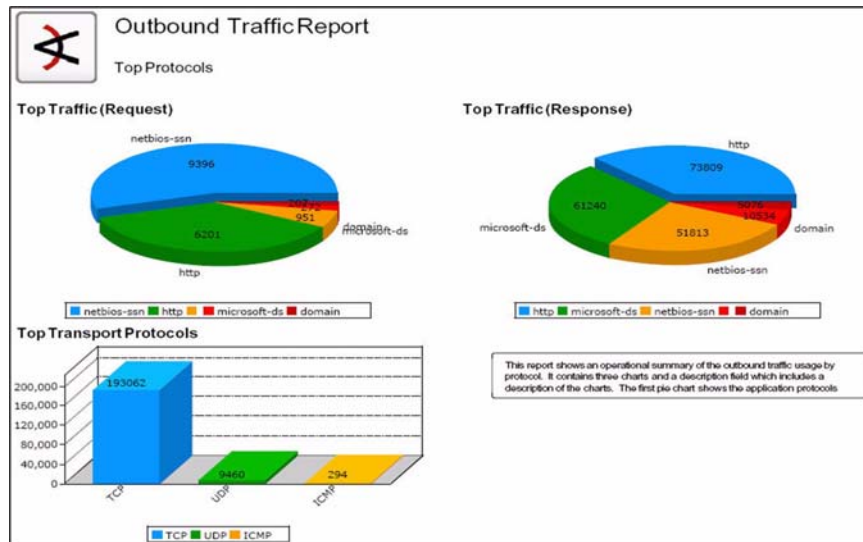
Outbound Traffic: These reports show the top protocols and top source hosts representing bytes out.

Summaries: These reports show daily and weekly summaries of bytes out. The *Outbound Traffic by Protocol* report can be focused on activity involving a particular application protocol.

Focused Reports: The *Outbound http Traffic - Weekly Summary* is a sample focused report that reports on outbound HTTP traffic.

Outbound Traffic Reports

The Top Protocols and Top Source Hosts provide a profile of the traffic going out of your network. From these views, you can get a profile of regular outbound traffic, and be able to spot spikes and trends.



Report

Description

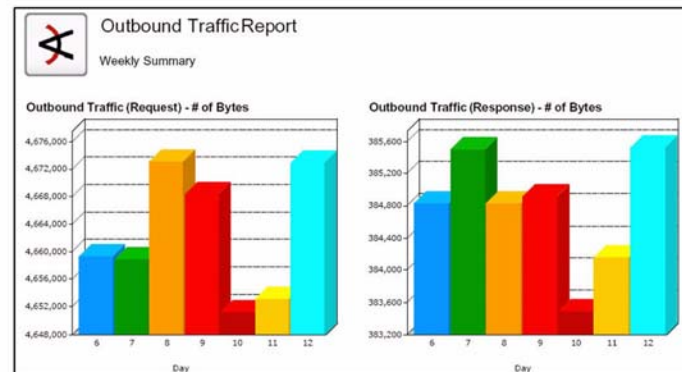
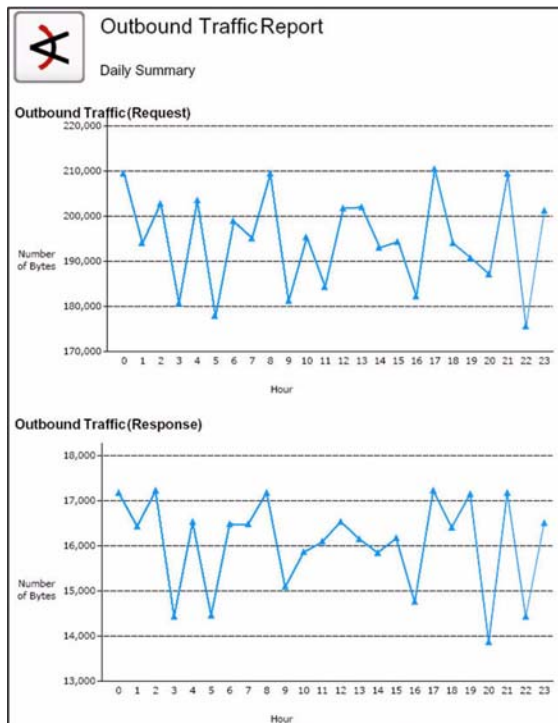
Outbound Traffic - Top Protocols

This report shows an operational summary of the outbound traffic usage by protocol. It contains three charts and a description field which includes a description of the charts. The first pie chart shows the application protocols with the highest total number of bytes contained in the requests, the second pie chart shows the application protocols with the highest total number of bytes contained in the responses, and the bar chart shows the repartition of the outbound traffic by transport protocol (only includes the requests).


Report	Description
Outbound Traffic - Top Source Hosts	This report shows an operational summary of the outbound traffic usage by source hosts. It contains two charts and two description fields which include a description of the charts. The first chart shows the source hosts with the highest total number of bytes contained in the requests and the second chart shows the source hosts with the highest total number of bytes contained in the responses.

Outbound Traffic Summaries

These reports show operational summaries of outbound traffic by the day and by the week. The daily summary graphs bytes in and bytes out for each hour of the day. The weekly summary shows a tally of bytes in and bytes out of the network for each day of the week.



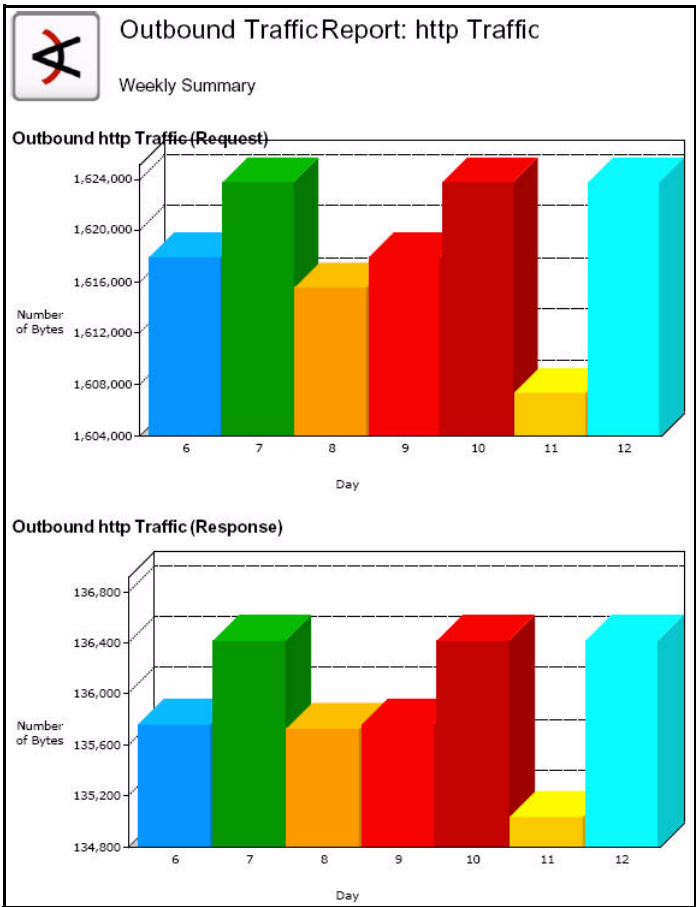
Report	Description
Outbound Traffic - Daily Summary	This report shows an operational summary of the outbound traffic usage for the last day. The first chart shows the total number of bytes contained in the requests by hour. The second chart shows the total number of bytes contained in the responses by hour.
Outbound Traffic - Weekly Summary	This report shows an operational summary of the outbound traffic usage for the last week. The first chart shows the total number of bytes contained in the requests by day. The second chart shows the total number of bytes contained in the responses by day.

Report	Description
 Outbound Traffic by Protocol - Weekly Summary	This report shows an operational summary of the outbound traffic usage for the last week. The first chart shows the total number of bytes contained in the requests by day. The second chart shows the total number of bytes contained in the responses by day. This is a focusable report which allows a user to specify the application protocol he wants to focus on.

Outbound Traffic Focused Reports

This group contains one focused report definition generated from the *Outbound Traffic by Protocol - Weekly Summary* focusable report. This definition focuses on outbound traffic that uses HTTP. Because it's likely that you might run this particular focused report more than once, this focused report definition is saved.

As needed, you can use the *Outbound Traffic by Protocol - Weekly Summary* report to create additional focused reports for other application protocols.

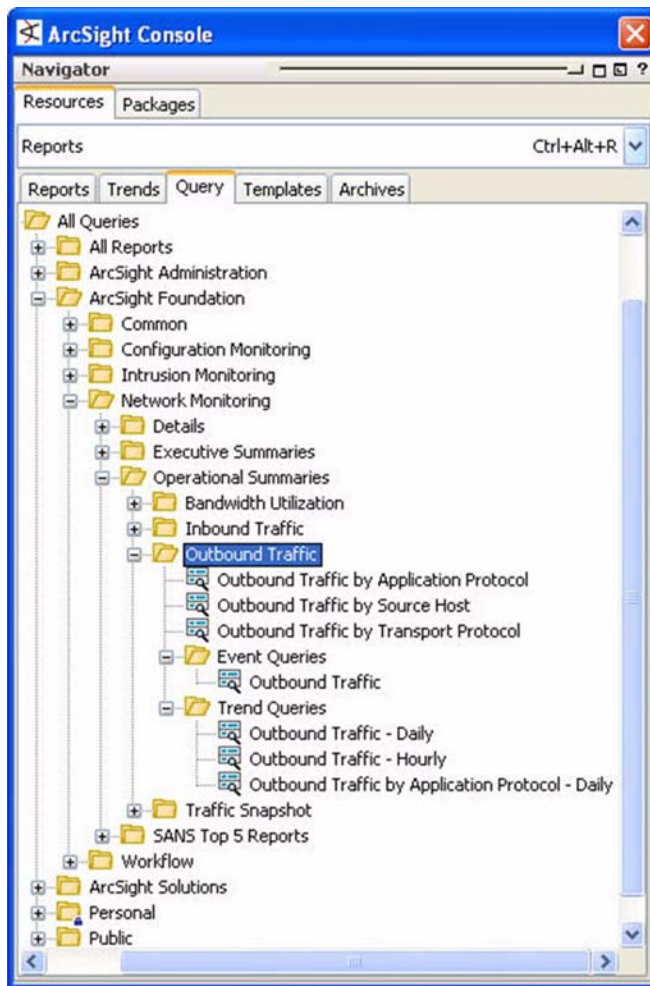


Report	Description
Outbound http Traffic - Weekly Summary	This focused report shows an operational summary of the outbound http traffic usage for the last week. The first chart shows the total number of bytes contained in the requests by day. The second chart shows the total number of bytes contained in the responses by day. This is a focused report depending on the "Outbound Traffic by Protocol - Weekly Summary" Report.

For instructions about how to create new focused reports based on the *Outbound Traffic by Protocol* focusable report, see ["To create a focused report that focuses on another protocol:"](#) on page 285.

Outbound Traffic Queries

The Outbound Traffic queries gather the data about outbound bytes that is consumed by the Outbound Traffic reports.



Outbound Traffic: These queries gather data on outbound bytes by application protocol, source host, and transport protocol.

Event Queries: The *Outbound Traffic* query gathers event data that is consumed by the *Outbound Traffic by Application Protocol* trend.

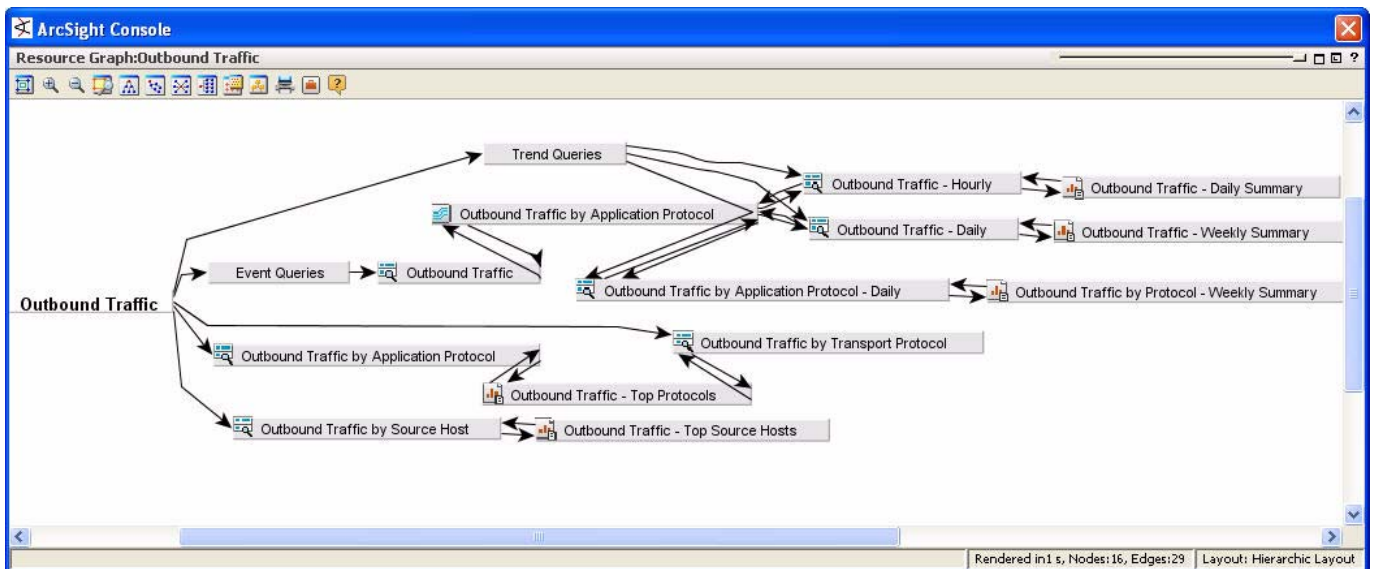
Trend Queries: These queries poll the trend data gathered by the *Outbound Traffic by Application Protocol* trend.

These queries are described in more detail below:

Query	Description
Outbound Traffic by Application Protocol	This query looks for outbound events (i.e. internal network to external network) and groups them by application protocol. The query returns the application protocol and the corresponding sums of bytesIn (request) and bytesOut (response).
Outbound Traffic by Source Host	This query looks for outbound events (i.e. internal network to external network) and groups them by attacker address and attacker zone name. The query returns the attacker address, the attacker zone name, and the corresponding sums of bytesIn (request) and bytesOut (response).

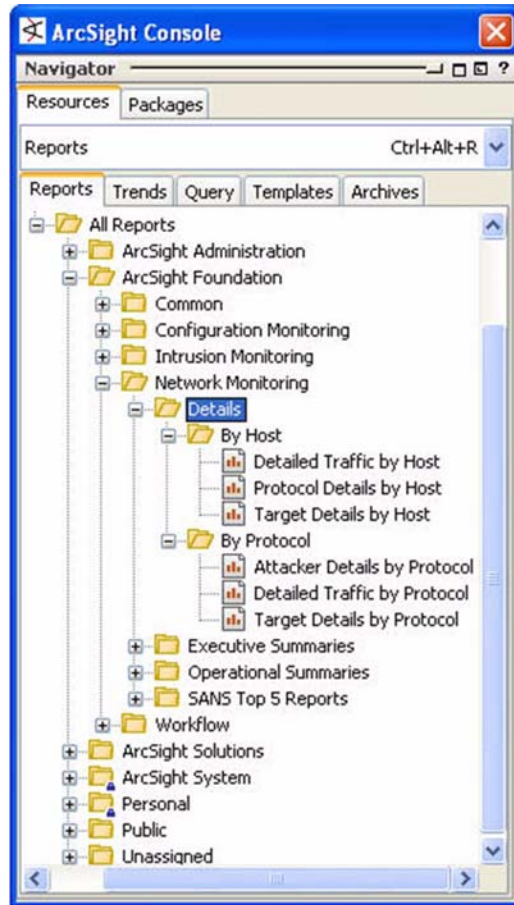
Query	Description
Outbound Traffic by Transport Protocol	This query looks for outbound events (i.e. internal network to external network) and groups them by transport protocol. The query returns the transport protocol and the corresponding sums of bytesIn (request) and bytesOut (response).
Outbound Traffic	This query is used by the Outbound Traffic by Application Protocol trend. This query looks for outbound events (i.e. internal network to external network) and returns the sums of bytesIn (request) and bytesOut (response) grouped by target port, application protocol, and hour.
Outbound Traffic - Daily	This query retrieves the information stored in the Outbound Traffic by Application Protocol trend. The query returns the sums of bytesIn (request) and bytesOut (response) grouped by day.
Outbound Traffic - Hourly	This query retrieves the information stored in the Outbound Traffic by Application Protocol trend. The query returns the sums of bytesIn (request) and bytesOut (response) and groups them by hour.
Outbound Traffic by Application Protocol - Daily	This query retrieves the information stored in the Outbound Traffic by Application Protocol trend. The query returns the sums of bytesIn (request) and bytesOut (response) and groups them by day. This query also allows the user to choose a specific application protocol in order to create a focused report such as the Outbound http Traffic Last Week report.

The Inbound Traffic queries are used by the following network monitoring queries and reports:



Detail Reports

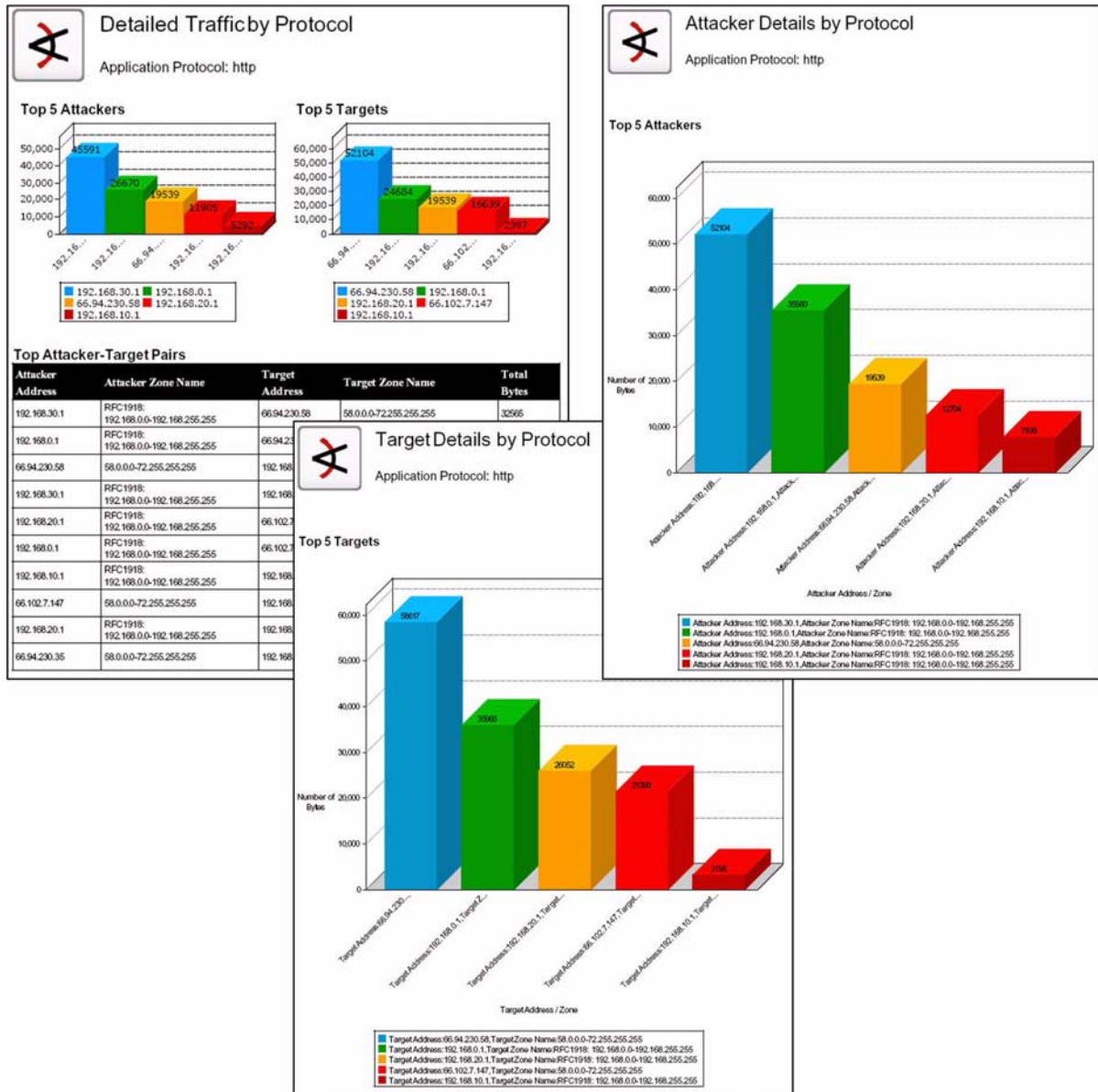
The Detail report groups contain a series of reports that provide traffic details by host and by application protocol. All of the reports are focusable, which means you can run the statistics for one particular host or IP address range or application protocol.



By Host: These reports show detailed traffic by host. The Protocol and Target reports can be focused on specific transport protocols and target IPs.

By Protocol: These reports show detailed traffic by protocol. They can each be focused respectively on attacker, target, or application protocol details.

The samples below show the Details by Protocol reports.

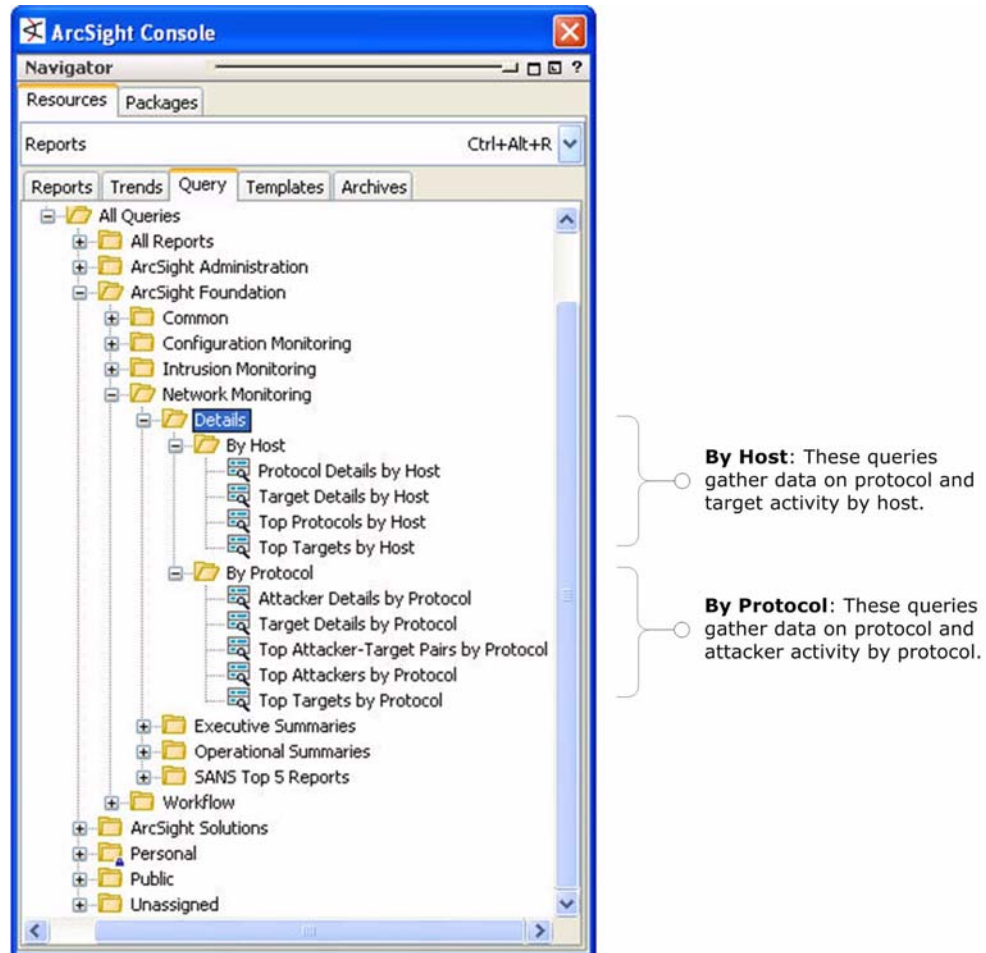


The Details reports are described in more detail below:

Report	Description
Detailed Traffic by Host	This report shows a chart of the total bytes (in and out) by host, a second chart of the total bytes by protocol and a detailed table showing the bytes in, bytes out and total bytes for each protocol by host.
Protocol Details by Host	This Focusable Report shows the Application Protocol repartition for a specific Host. The Report contains one chart and one table. The chart shows the Top 5 Protocols with the total number of Bytes (BytesIN + BytesOUT). The table shows the details for the Top Protocols (BytesIN, BytesOUT, and Total Number of Bytes).
Target Details by Host	This Focusable Report shows the Top Targets for a specific host. This Report contains one chart and one table. The chart shows the Top 5 Targets and the table shows the details of the Top Targets.
Attacker Details by Protocol	This Focusable Report shows the Top Attackers for a specific Application Protocol. This Report contains one chart and one table. The chart shows the Top 5 Attackers and the table shows the details of the Top Attackers.
Detailed Traffic by Protocol	This Focusable Report shows the Traffic for a specific Application Protocol. The Report contains two charts and one table. The first chart shows the Top 5 Attackers, the second chart shows the Top 5 Targets, and the table shows the Top Attacker-Target Pairs.
Target Details by Protocol	This Focusable Report shows the Top Targets for a specific Application Protocol. This Report contains one chart and one table. The chart shows the Top 5 Targets and the table shows the details of the Top Targets.

Detail Reports Queries

These queries supply the data for the Detail reports.

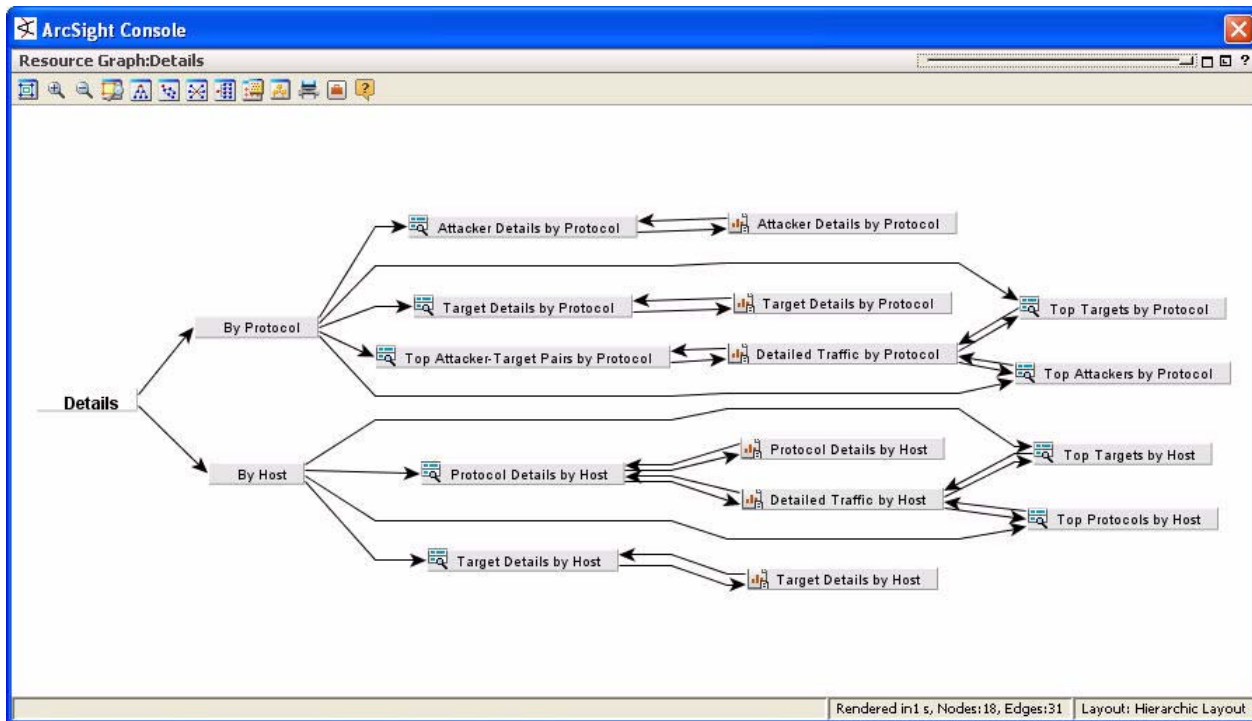


The Detail by Host and by Protocol queries are described in more detail below:

Query	Description
Protocol Details by Host	This Query selects the number of Bytes In, Bytes Out, and Total Bytes (Bytes In + Bytes Out) for a specific Attacker Address/Zone and groups the values by Protocol, Target Address, and Target Zone.
Target Details by Host	This Query selects the number of Bytes In, Bytes Out, and Total Bytes (Bytes In + Bytes Out) for a specific Attacker Address/Zone and groups the values by Target Address and Target Zone.
Top Protocols by Host	This Query selects the Protocols with the highest number of Total Bytes (Bytes In + Bytes Out) for a specific Attacker Address/Zone.
Top Targets by Host	This Query selects the Target Address/Zone with the highest number of Total Bytes (Bytes In + Bytes Out) for a specific Attacker Address/Zone.

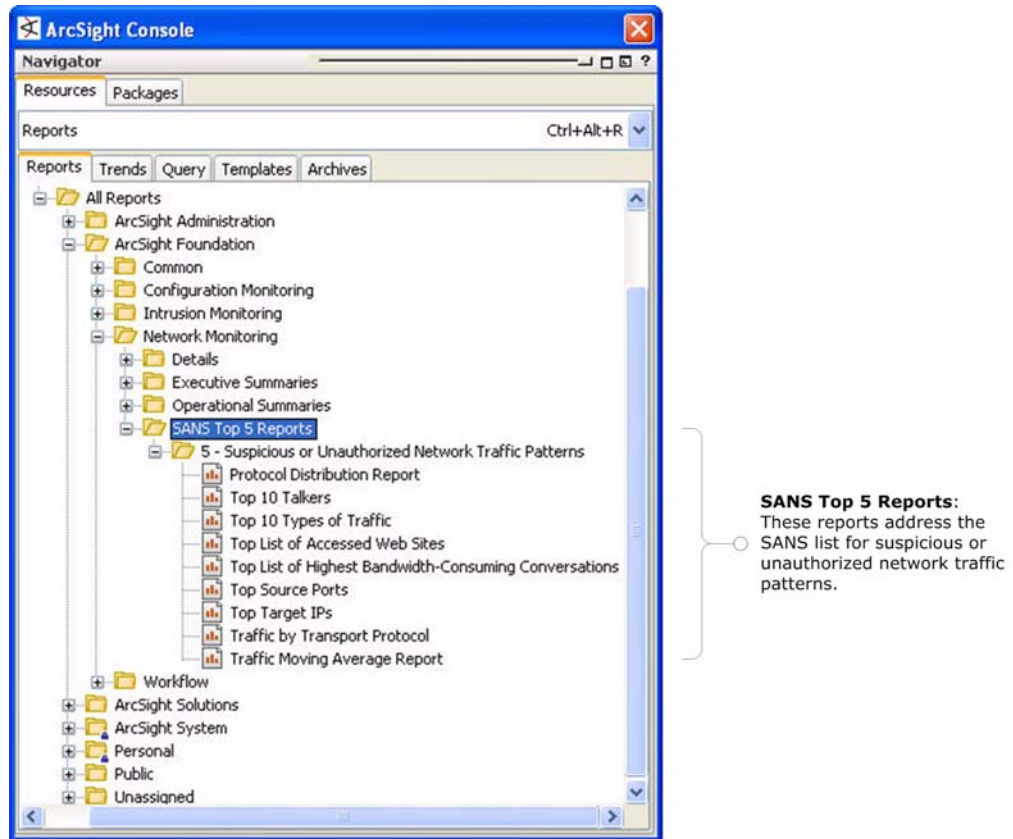
Query	Description
Attacker Details by Protocol	This Query selects the number of Bytes In, Bytes Out, and Total Bytes (Bytes In + Bytes Out) for a specific Application Protocol and groups them by Attacker Address and Attacker Zone.
Target Details by Protocol	This Query selects the number of Bytes In, Bytes Out, and Total Bytes (Bytes In + Bytes Out) for a specific Application Protocol and groups them by Target Address and Target Zone.
Top Attackers by Protocol	This Query selects the Attacker/Zone with the highest number of Total Bytes (Bytes In + Bytes Out) for a specific Application Protocol.
Top Attacker-Target Pairs by Protocol	This Query selects the Attacker-Target pairs with the highest number of Total Bytes (Bytes In + Bytes Out) for a specific Application Protocol and groups them by Attacker Address, Attacker Zone, Target Address and Target Zone.
Top Targets by Protocol	This Query selects the Target/Zone with the highest number of Total Bytes (Bytes In + Bytes Out) for a specific Application Protocol.

The Detail by Host and by Protocol queries support the following Network Monitoring reports:



SANS Top 5 Reports for Network Monitoring

The SANS Top 5 Reports for Network Monitoring focus on SANS section 5, Suspicious or Unauthorized Network Traffic.



A good place to start is the *Traffic Moving Average* report. This report uses the *Traffic Spike Rule Fired Events* query, which looks for correlation events from the Network Monitoring rules (described in “[Network Monitoring Rules](#)” on page 305). Then each of the 3 tables in the report will look at either TCP, UDP, or ICMP using the *Report Parameters Filters* (described in “[Report Parameter Filters](#)” on page 256).

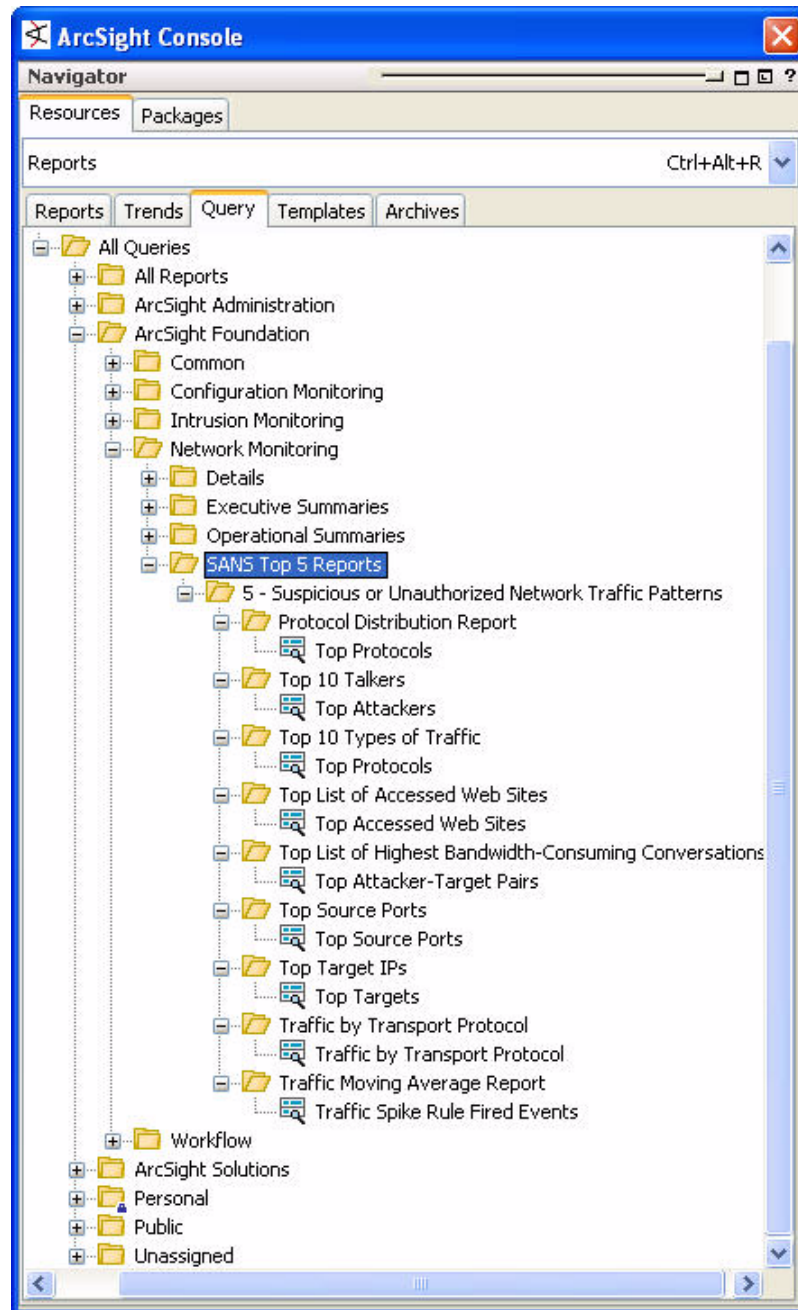
The SANS Top 5 reports are described in more detail below.

Report	Description
Protocol Distribution Report	This Report shows the top busiest protocols. This Report contains a pie chart and a table. The pie chart shows the top 10 busiest protocols and the table shows the list of all the protocols, sorted by the total number of bytes IN and bytes OUT.
Top 10 Talkers	This Report shows a bar chart with the top 10 talkers.
Top 10 Types of Traffic	This Report shows a bar chart with the top 10 types of traffic.
Top List of Accessed Web Sites	This Report shows the top accessed web sites. This Report contains a bar chart and a table. The chart shows the top 10 accessed web sites and the table shows the list of all the accessed web sites.

Report	Description
Top List of Highest Bandwidth-Consuming Conversations	This Report shows the highest bandwidth-consuming conversations. This Report contains a bar chart and a table. The chart shows the top 10 highest conversations and the table shows the list of the highest conversations.
Top Source Ports	This Report shows the busiest source ports. The Report contains a bar chart and a table. The chart shows the top 10 source ports and the table shows the list of the top source ports.
Top Target IPs	This Report shows the top target IP addresses. The Report contains a bar chart and a table. The chart shows the top 10 target IP addresses and the table shows the list of the target IP addresses.
Traffic Moving Average Report	This Report shows the moving average of ICMP, UDP, and TCP Traffic for the last hour. The Report contains 3 tables. The first table shows the moving average for ICMP traffic, the second table shows the moving average for UDP traffic, and the third table shows the moving average for TCP traffic.
Traffic by Transport Protocol	This Report shows the traffic repartition by transport protocol by minute for the last hour.

SANS Top 5 Reports Queries

These queries supply the data for the SANS Top 5 reports.

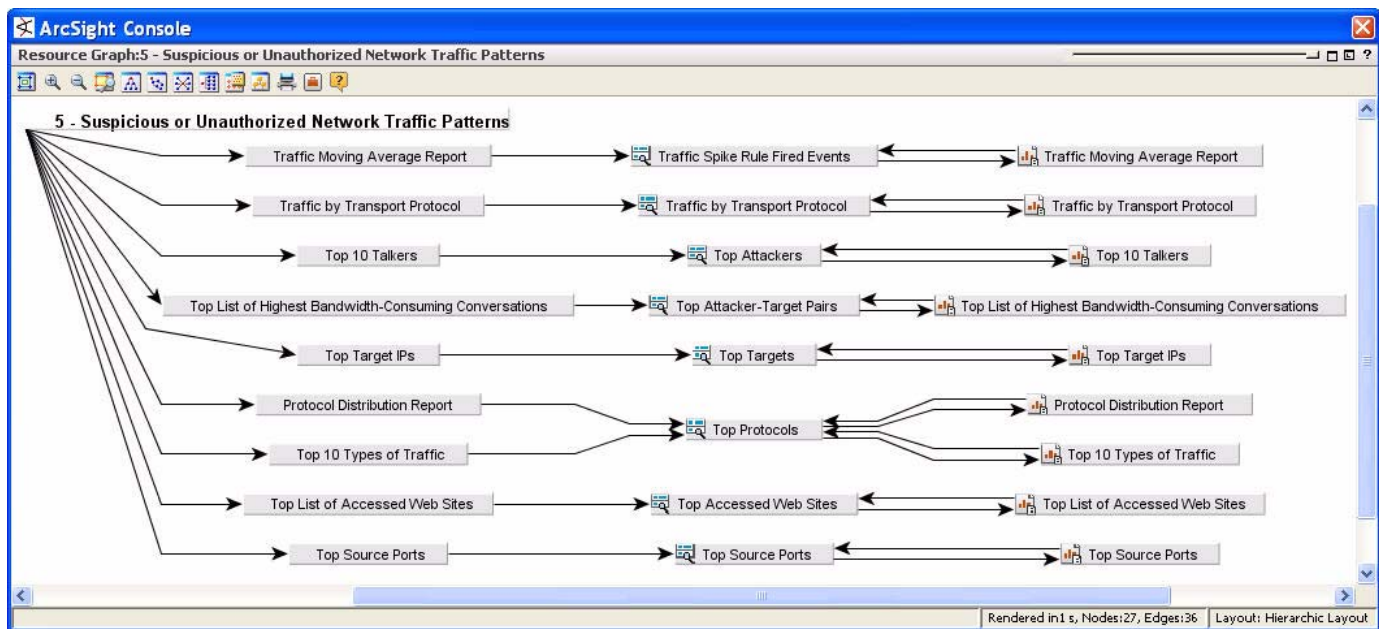


The SANS Top 5 Report queries are described in more detail below:

Query	Description
Top Protocols	This Query selects the Protocol with the highest number of Total Bytes (Bytes In + Bytes Out) in the last hour.
Top Attackers	This Query selects the Attacker/Zone with the highest number of Total Bytes (Bytes In + Bytes Out) in the last hour.

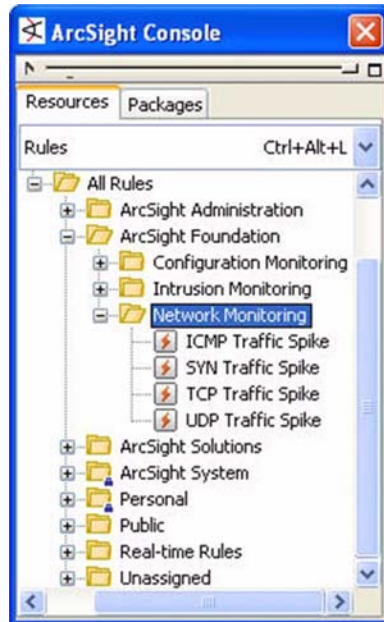
Query	Description
Top Accessed Web Sites	This Query selects the Target Address/Zone of the Web Sites with the highest number of Total Bytes (Bytes In + Bytes Out) in the last hour.
Top Attacker-Target Pairs	This Query selects the Attacker-Target pairs with the highest number of Total Bytes (Bytes In + Bytes Out) in the last hour.
Top Source Ports	This Query selects the Attacker Ports with the highest number of Total Bytes (Bytes In + Bytes Out) in the last hour.
Top Targets	This Query selects the Target Ports with the highest number of Total Bytes (Bytes In + Bytes Out) in the last hour.
Traffic by Transport Protocol	This Query selects the number of Total Bytes (Bytes In + Bytes Out) by Transport Protocol in the last hour.
Traffic Spike Rule Fired Events	This Query looks for correlation events generated by Moving Average Data Monitors looking for TCP, UDP, and ICMP spikes in the last hour.

The SANS Top 5 Report queries support the following Network Monitoring SANS Top 5 reports:



Network Monitoring Rules

The Network Monitoring rules support the SANS Top 5 reports. They trigger a correlation event whenever a spike occurs for traffic involving any of the following transport protocols: ICMP, SYN, TCP and UDP. These rules detect alarms from the moving average data monitors ([All Data Monitors/ArcSight Foundation/Network Monitoring/Traffic Moving Average](#)) caused by traffic spikes. A spike is considered a 50-packet variation from the average over a 5-minute timeframe.



Network Monitoring

Rules: These rules look for spike warnings generated by the Traffic Moving Average data monitors. When a spike of 50% or greater occurs, these rules trigger a correlation event that is consumed by Network Monitoring filters and reports.

These rules are described in more detail below.

Rule	Description
ICMP Traffic Spike	This rule monitors the moving average of inbound ICMP events (i.e. external network to internal network). It fires whenever the number of ICMP packets per minute goes up by 50% or more.
SYN Traffic Spike	This rule monitors the moving average of inbound SYN events (i.e. external network to internal network). It fires whenever the number of SYN packets per minute goes up by 50% or more.
TCP Traffic Spike	This rule monitors the moving average of inbound UDP events (i.e. external network to internal network). It fires whenever the number of UDP packets per minute goes up by 50% or more.
UDP Traffic Spike	This rule monitors the moving average of inbound UDP events (i.e. external network to internal network). It fires whenever the number of UDP packets per minute goes up by 50% or more.

What's Next

Next, we describe the ArcSight Administration resources, all the tools you need to monitor and tune the inner workings of ArcSight ESM.

ArcSight Workflow Foundation



The ArcSight Workflow foundation is a system of active channels and reports that support incident response tracking using ArcSight's incident response system.

ArcSight ESM uses notifications and cases to enable security operators to coordinate and prioritize response to security events. Qualifying events in the other ArcSight foundation packages trigger notifications and cases that get escalated through ArcSight's incident response stages. The Workflow foundation active channels and reports show the status of cases and notifications generated by these qualifying event.

For a complete overview about ESM's notifications, cases, and incident response workflow, see "Phase 4: Monitoring, Investigation, and Workflow" in *ArcSight 101*.

- ["WorkFlow Foundation Overview" on page 307](#)
- ["Configuration Summary" on page 308](#)
- ["Workflow Active Channels" on page 309](#)
- ["Workflow Reports" on page 311](#)

WorkFlow Foundation Overview

The Workflow foundation provides two ways to view and track events that have been routed for follow-up.

Active Channels

The active channels provide a live view of events that have been routed for follow up. The Workflow group shows events for the user currently logged in to ESM, and the Incident Tracking group shows events that are queued during different shifts of the day.

Reports

The reports provide a historical summary of events that have been routed for follow-up. The Cases reports show events for which cases have been opened in ESM's incident tracking system. The Notification reports show events that have generated notifications.

Qualifying Events

The Intrusion Monitoring, Configuration Monitoring, and ArcSight Administration foundations contain rules whose actions generate notifications or cases when qualifying events occur. Notifications can also be sent by the Manager, such as database notifications or other internal conditions that may warrant a notification.

For example, the action triggered by a qualifying event in the Intrusion Monitoring rule **Notify on Successful Attack** is to send a notification to [/All Destinations/CERT Team](#) and create a case that is put in [/All Cases/ArcSight System/High Severity Attacks](#).

The rules that open cases and send notifications are:

Foundation	Rule	Notification Group
ArcSight Administration	/All Rules/Real-time Rules/ArcSight Administration/Connector and Device Monitoring/Connector Connection Down	SOC Operators
ArcSight Administration	/All Rules/Real-time Rules/ArcSight Administration/Connector and Device Monitoring/Device Connection Down	SOC Operators
ArcSight Administration	/All Rules/Real-time Rules/ArcSight Administration/ESM Status/Excessive Rule Recursion	SOC Operators
ArcSight Administration	/All Rules/Real-time Rules/ArcSight Administration/ESM Status/Rule Matching Too Many Events	SOC Operators
Configuration Monitoring	/All Rules/ArcSight Foundation/Configuration Monitoring/Detail/Vulnerabilities/Warning - Insecure Configuration	SOC Operators
Configuration Monitoring	/All Rules/ArcSight Foundation/Configuration Monitoring/Detail/Vulnerabilities/Warning - Vulnerable Software	SOC Operators
Intrusion Monitoring	/All Rules/ArcSight Foundation/Intrusion Monitoring/Attackers/Notify on Successful Attack	CERT Team

Configuration Summary

The Workflow foundation itself contains no resources that require configuration, however, the foundation does rely on the following system-level configurations be made:

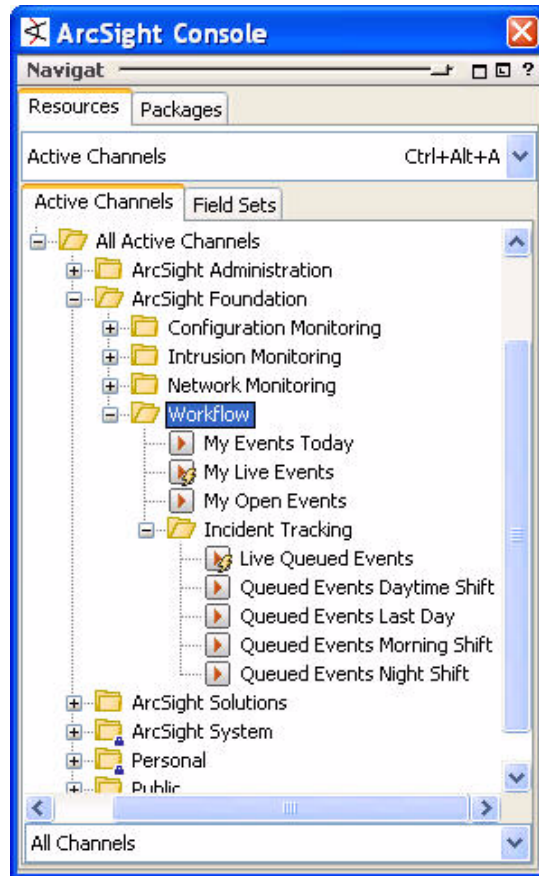
- Users should be assigned to the Notification Destination groups listed in [/All Destinations](#) groups, as appropriate for your company organization.

Workflow Active Channels

The Workflow active channels show events that have been routed for follow up in two groups: Workflow and Incident Tracking.

Workflow Active Channels

The Workflow group shows events assigned to the user who is currently logged in to ESM.



The Workflow active channels are described in more detail below.

Active list	Description
My Events Today	Live Channel showing events assigned to me today. The channel includes a sliding window that always displays events occurring since midnight today. A filter prevents the channel from showing correlated events. It shows only events that are not in closed stage and are assigned to the current user.
My Live Events	Events assigned to me over the last two hours.
My Open Events	Live Channel showing events received since the beginning of the week. The channel includes a sliding window that always displays events received since the beginning of the week. A filter prevents the channel from showing correlated events. It shows only events that are not in closed stage and are assigned to the current user.

Incident Tracking Active Channels

The Incident Tracking active channels provide views of events that are at various stages in the follow-up routing system.

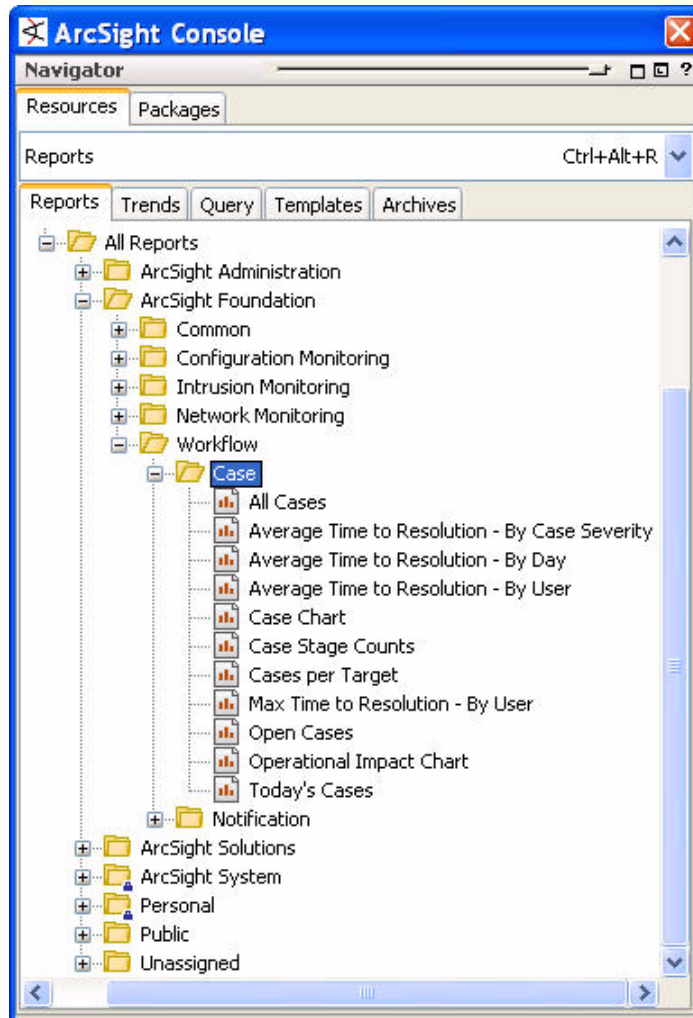
Active Channel	Description
Live Queued Events	Events received within the last two hours that have not been reviewed.
Queued Events Day-time Shift	Channel showing events received today between 8am and 4pm. A filter prevents the channel from showing correlated events. It shows only events that are in queued stage.
Queued Events Last Day	Channel showing events received during the last 24 hours. The channel includes a sliding window, showing exactly the events generated during the last 24 hours. A filter prevents the channel from showing correlated events. It shows only events that are in queued stage.
Queued Events Morning Shift	Channel showing events received today between 12am and 8am. A filter prevents the channel from showing correlated events. It shows only events that are in queued stage.
Queued Events Night Shift	Channel showing events received today between 4pm and midnight. A filter prevents the channel from showing correlated events. It shows only events that are in queued stage.

Workflow Reports

The reports show a historical view of cases and notifications triggered by qualifying events.

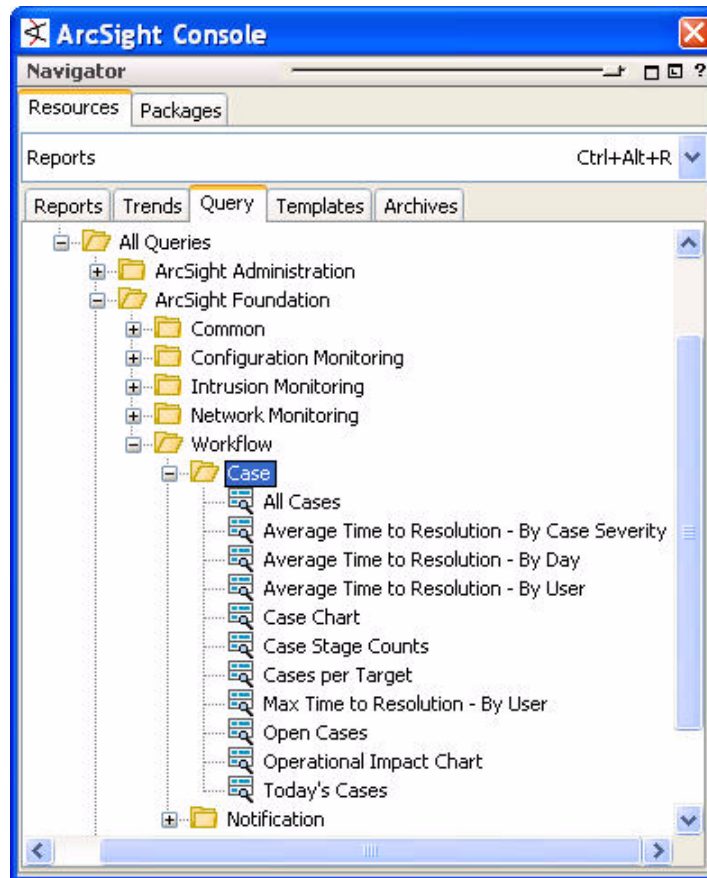
Case Reports

The Case reports show statistics about cases opened in ESM's case management system. Cases can be automatically created and assigned by standard content rules, such as [Notify on Successful Attack](#) in the Intrusion Monitoring foundation, or by rules written by ESM users, or even manually created by ESM users while investigating events, such as those that might be displayed in the [My Live Events](#) active channel.



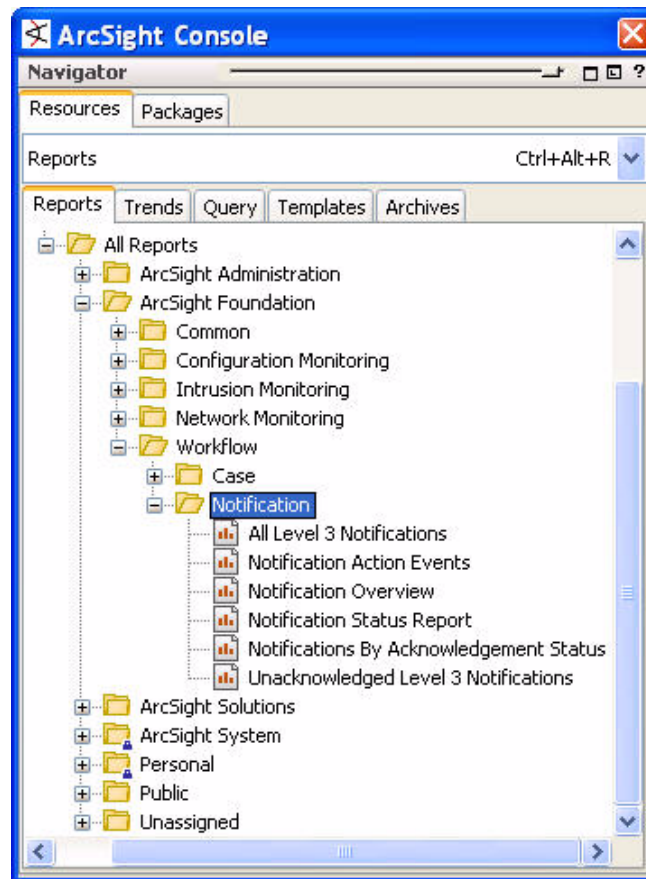
Case Queries

The Case queries supply conditions for the Case reports.



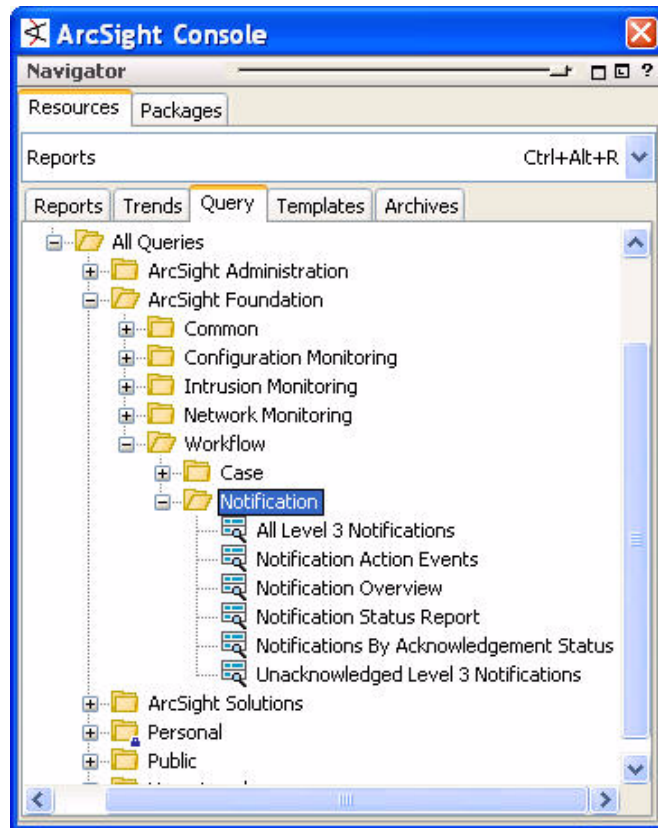
Notification Reports

The Notification reports provide statistics about notifications generated by rules and by the ArcSight Manager.



Notification Queries

The Notification queries supply conditions for the Notification reports.



What's Next

The next chapter describes how to monitor and tune ArcSight components in the ArcSight Administration foundation.

ArcSight Administration Foundation



The ArcSight Administration foundation is a coordinated set of resources that provide statistics about the health and performance of ArcSight ESM and its components. This foundation is essential for managing and tuning the performance of ESM content and components.

- ["ArcSight Administration Overview" on page 315](#)
- ["Configuration Summary" on page 316](#)
- ["ArcSight Administration Filters" on page 317](#)
- ["ArcSight Administration Active Channels" on page 325](#)
- ["ArcSight Administration Active List" on page 327](#)
- ["ArcSight Administration Dashboards and Data Monitors" on page 328](#)
- ["ArcSight Administration Rules" on page 335](#)
- ["ArcSight Administration Reports" on page 343](#)

ArcSight Administration Overview

The Administration foundation active channels, dashboards and reports provide insight into various aspects of ArcSight function and performance.

Agent/Connector

The Agent/Connector content provides statistics about events being sent from the Connectors reporting in to ESM environment. This content also monitors the status of the Connectors.

Device

The Device dashboards provide statistical data about the devices reporting in to ESM.

Configuration Change Monitoring

The first part of the Configuration Change Monitoring content monitors changes (creations, updates, and deletions) made to ArcSight resources. The second part of the content monitors the performance of ArcSight Rules (top firing rules, partial matches, rule errors, and so on).

Event Flow

The Event Flow content provides a profile of and statistics about the events flowing into ESM from the Connectors, such as time-based statistics, re-partition of the events by priority or Connector type, the latest "important" events, and so on.

ESM Status

The ESM Status dashboards provide statistics about ArcSight ESM components, such as Consoles status, Database performance statistics, and ESM system information.

Licensing

The licensing report shows what IP address and zones have been used to run an ArcSight Console or ArcSight SmartConnector connected to an ArcSight Manager, and the user information associated with these connections.

The report query selects the address from which the ArcSight Console is connecting, which means the Console could be running on the same physical machine, but using different IP addresses (such as a VPN or DHCP situation). These reports should be used to see where ArcSight licensed activity is happening. Manual analysis may provide data leading to the discovery of unusual or unauthorized accesses.

Resource Monitoring

The Resource Monitoring content provides statistics about the ArcSight resources operating in the ESM environment, such as statistics about Active List and Session List access, number of correlation events, Trend status, and so on. This content is helpful to troubleshoot performance issues with content configuration.

User

The User content provides statistics about users logging into and out of ESM.

Configuration Summary

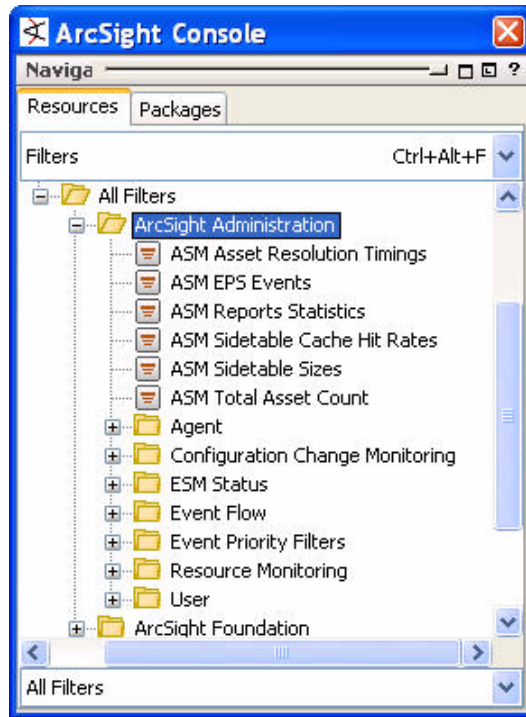
Beyond the initial setup outlined in [“Standard Content Installation, Upgrade, and Configuration” on page 17](#), no additional configuration is required for the ArcSight Administration foundation.

ArcSight Administration Filters

The Administration filters support all the ArcSight administration use cases.

ArcSight Administration Filters

The ArcSight Administration filters provide general event statistics for events and ESM components.



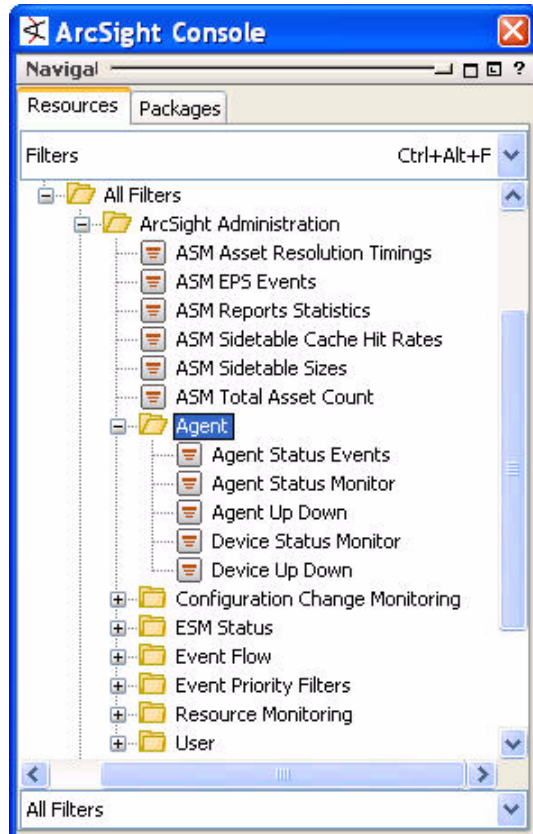
The top-level ArcSight Administration filters are described in more detail below.

Filter	Description
ASM Asset Resolution Timings	This Filter is looking for ArcSight Status Monitor events containing asset resolution timings information. The asset resolutions average time is the average time in milliseconds taken to resolve an end-point in an event to an asset.
ASM EPS Events	This Filter is looking for ArcSight Status Monitor events containing EPS (Events Per Second) information. There are 2 types of EPS events: the first event type provides the count of events that have passed through the flow since the manager started and the second event type provides the count of correlated events generated by the rule engine.
ASM Reports Statistics	This Filter is looking for ArcSight Status Monitor events containing report statistics information. These events provide statistics about the current number of reports querying the database or being rendered.

Filter	Description
ASM Sidetable Cache Hit Rates	This Filter is looking for ArcSight System Monitor events containing side table cache hit rates information. Side tables are tables held in-memory and in the database to retain common and relatively static information such as geographical information, categorization information, connector information, device information, and labels for custom strings and numbers. The cache hit rate identifies how many successful attempts to find entries occurred in the past two hours.
ASM Sidetable Sizes	This Filter is looking for ArcSight System Monitor events containing side table size information. Side tables are tables held in-memory and in the database to retain common and relatively static information such as geographical information, categorization information, connector information, device information, and labels for custom strings and numbers. The side table size identifies how many entries are presently in the cache.
ASM Total Asset Count	This Filter is looking for ArcSight System Monitor events containing the current total number of assets.

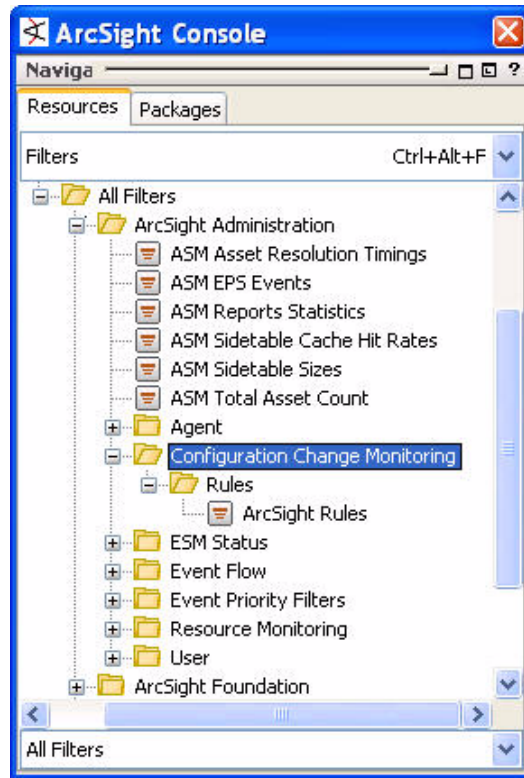
Agent Filters

The Agent filters support the Connector statistics use case.



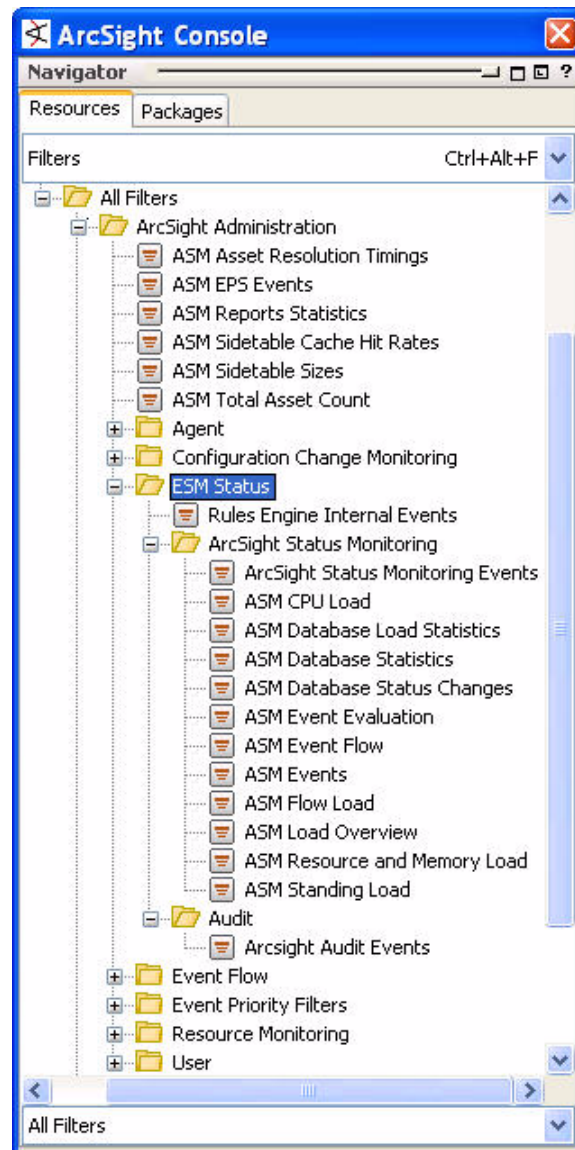
Configuration Change Monitoring Filter

The Configuration Change Monitoring filter supports the content that provides statistics about configuration changes made to ArcSight resources and rule status.



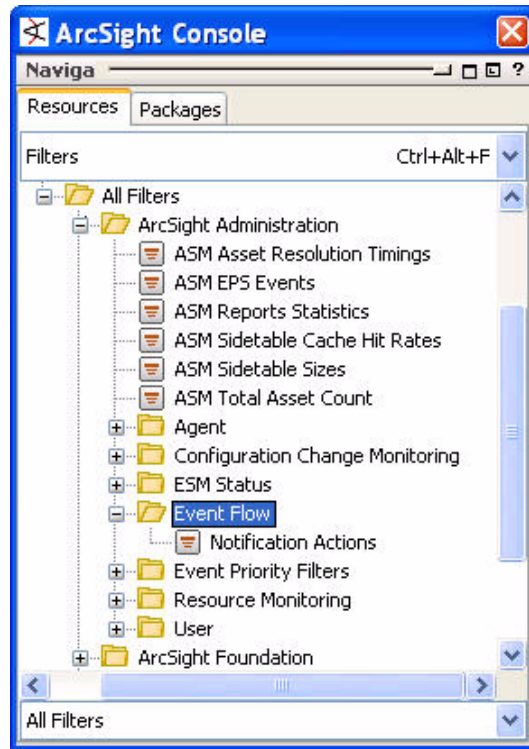
ESM Status Filters

The ESM Status filters provide conditions for the content that reports on ArcSight Status Monitoring (ASM) and audit events.



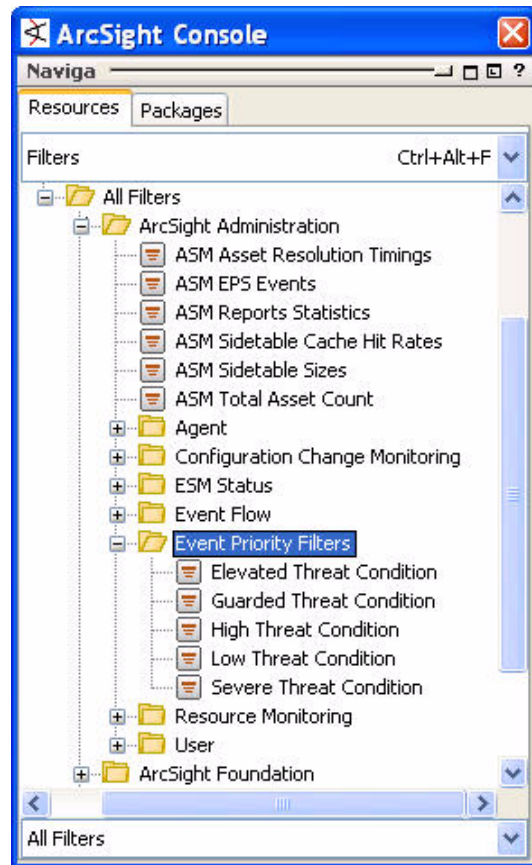
Event Flow Filter

The Event Flow filter provides conditions about notification actions for the ESM Event Flow resources.



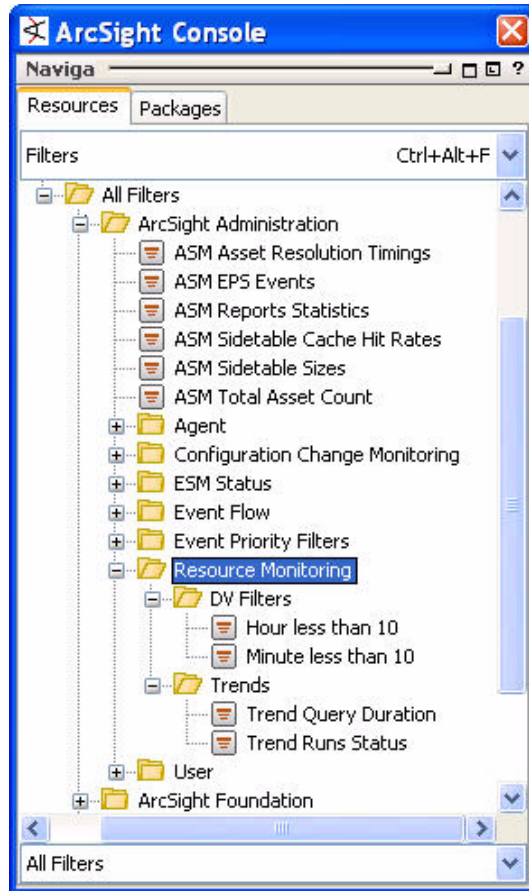
Event Priority Filters

The Event Priority filters provide priority level conditions for the event priority content.



Resource Monitoring Filters

The Resource Monitoring DV filters provide conditions used by variables, also referred to as dependent variables or DVs. The Trends filters provide conditions used by the Resource Monitoring trend reports.

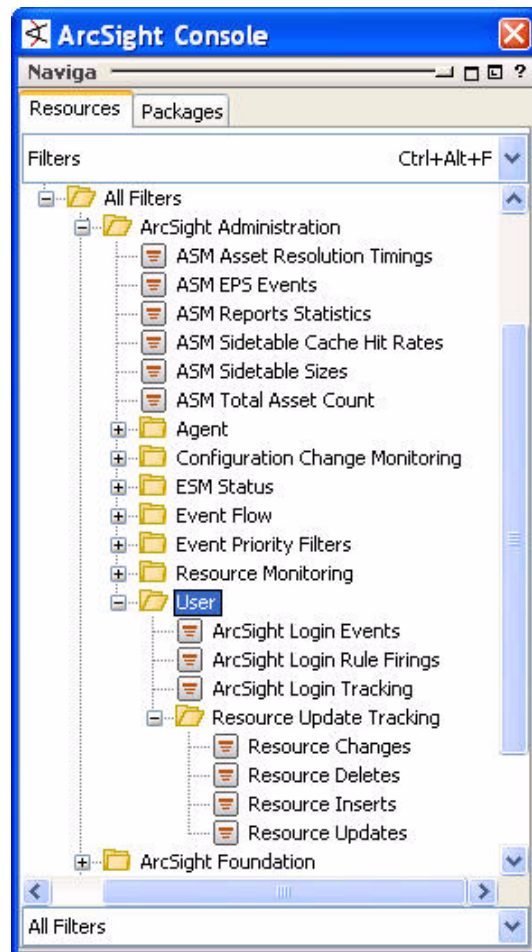


The Resource Monitoring filters are described in more detail below.

Filter	Description
Hour less than 10	This Filter is used by a Conditional DV. The condition in the Filter is "Hour(EndTime) is less than 10".
Minute less than 10	This Filter is used by a Conditional DV. The condition in the Filter is "Minute(EndTime) is less than 10".
Trend Query Duration	This Filter is looking for successful Trend query runs events.
Trend Runs Status	This Filter is looking for Trend query runs events.

User Filters

The User filters provide conditions for the resources that report on ESM user log-on and log-off activity. The Resource Update Tracking filters provide conditions that report on changes to ArcSight resources.

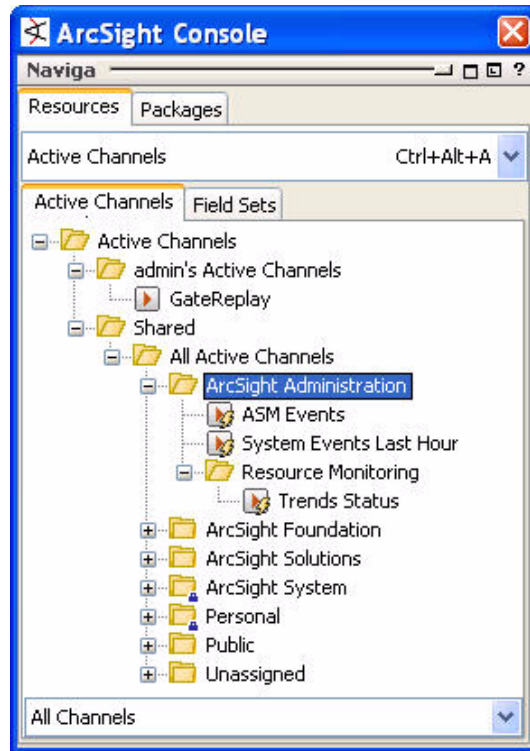


The User filters are described in more detail below:

Filter	Description
ArcSight Login Events	
ArcSight Login Rule Firings	This filter is looking for events containing ArcSight login rule firing information. The deviceEventCategory used in this filter is generated by the "ArcSight User Login" rule and the filter is used by a trend that tracks hourly login stats.\n
ArcSight Login Tracking	This filter is looking for events containing ArcSight login and logout information. The deviceEventCategory used in this filter are generated by the "ArcSight User Login", "ArcSight User Login Timeout", and "ArcSight User Logout" rules.

ArcSight Administration Active Channels

The ArcSight Administration active channels provide real-time views into internal ArcSight ASM and System-level events.

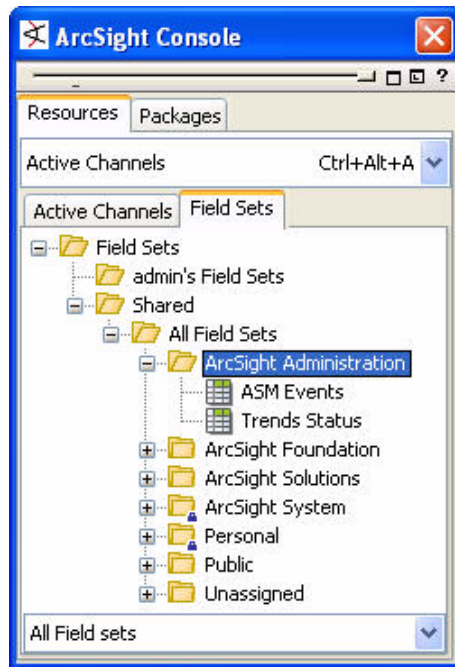


The ArcSight Administration active channels are described in more detail below.

Active Channel	Description
ASM Events	
System Events Last Hour	Channel showing all events generated by ArcSight during the last hour. A filter prevents the channel from showing events that contributed to the firing of a rule, commonly referred to as correlated events.
Trends Status	This Active Channel shows all the trend-related events in the last 2 hours. The "Trend Name" Field shows the name of the Trend and its URI. The "Trend Infos" Field shows some information on the Trend event.

ArcSight Administration Field Sets

The ArcSight Administration field sets define the event fields displayed in the ArcSight Administration active channels and condition editors.

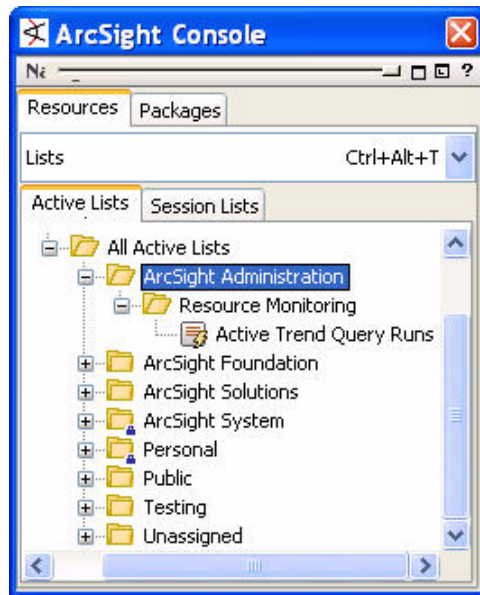


The ArcSight Administration field sets are described in more detail below.

Field Set	Description
ASM Events	
Trends Status	This Field Set is used by the "Trends Status" Active Channel. The Field Set contains the following fields: "End Time", "Name", "Trend Name", and "Trend Infos".

ArcSight Administration Active List

The Resource Monitoring active list stores event entries whenever an active trend query is run for Resource Monitoring use case rules and reports.

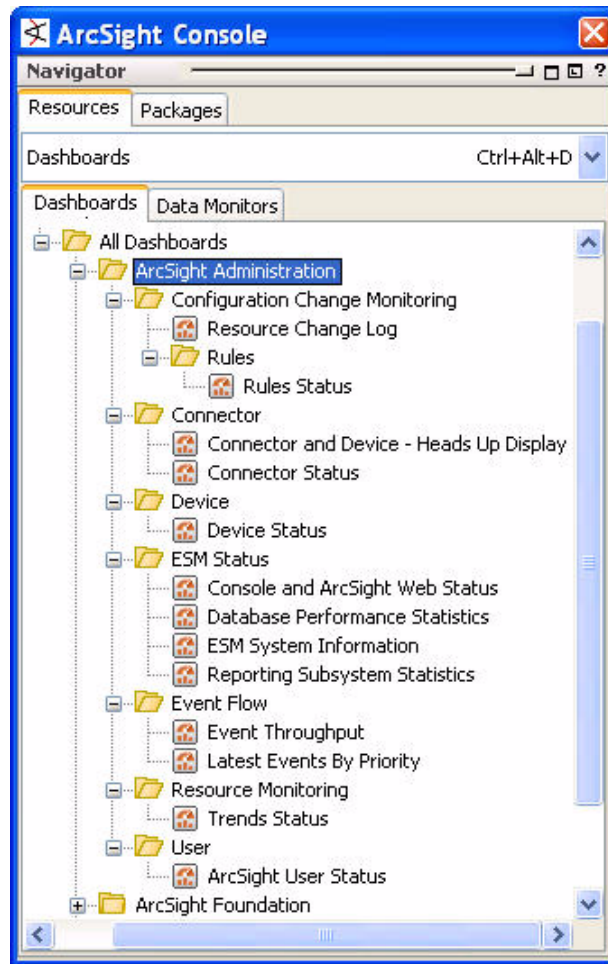


The Resource Monitoring active list is described in more detail below.

Active List	Description
Active Trend Query Runs	This active list stores running query information including the name of the trend, the URI of the trend, and the time the query started. It is used by the Active Trend Queries query to determine the duration of the trend runs for the Active Trend Queries report.

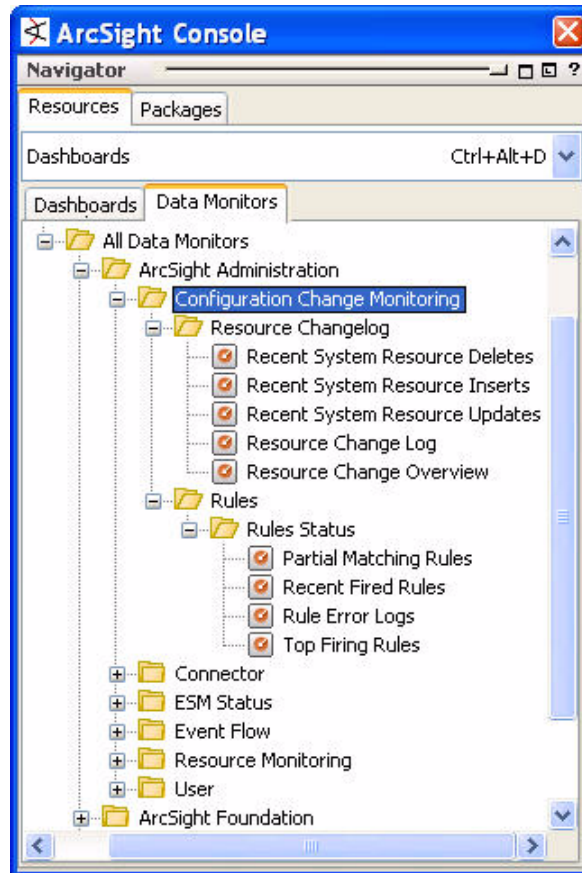
ArcSight Administration Dashboards and Data Monitors

The ArcSight Administration dashboards display real-time statistics for ESM internal activity based on events expressed in ArcSight Administration data monitors.



Configuration Change Monitoring Data Monitors

The Configuration Change Monitoring data monitors define the views shown in the Configuration Change Monitoring dashboards.

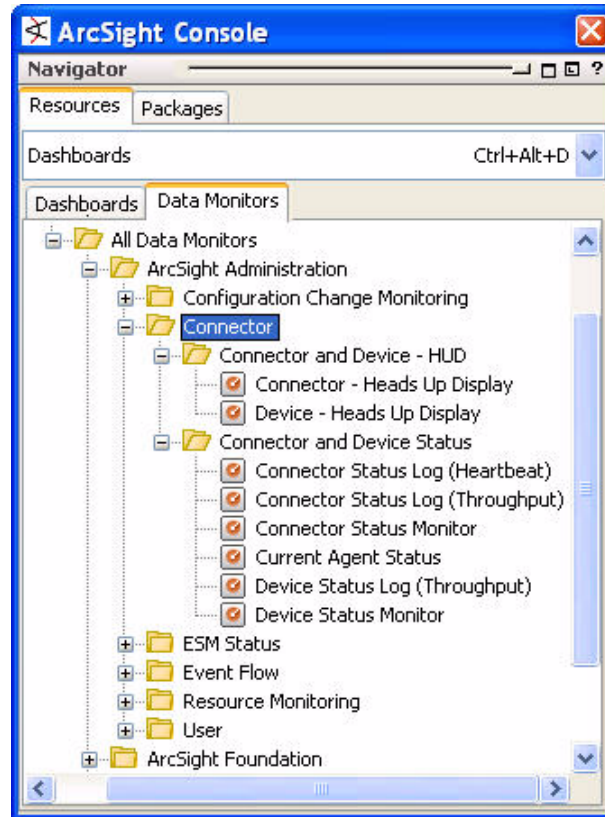


The Configuration Change Monitoring data monitors are described in more detail below.

Data Monitor	Description
Recent System Resource Deletes	Note: This Data Monitor will not populate all values when running in Turbo Mode Fastest!
Recent System Resource Inserts	Note: This Data Monitor will not populate all values when running in Turbo Mode Fastest!
Recent System Resource Updates	Note: This Data Monitor will not populate all values when running in Turbo Mode Fastest!
Resource Change Log	Note: This Data Monitor will not populate all values when running in Turbo Mode Fastest!
Resource Change Overview	This data monitor shows an overview of the ArcSight resource changes. The data monitor shows the total number of changes by type for the last hour.

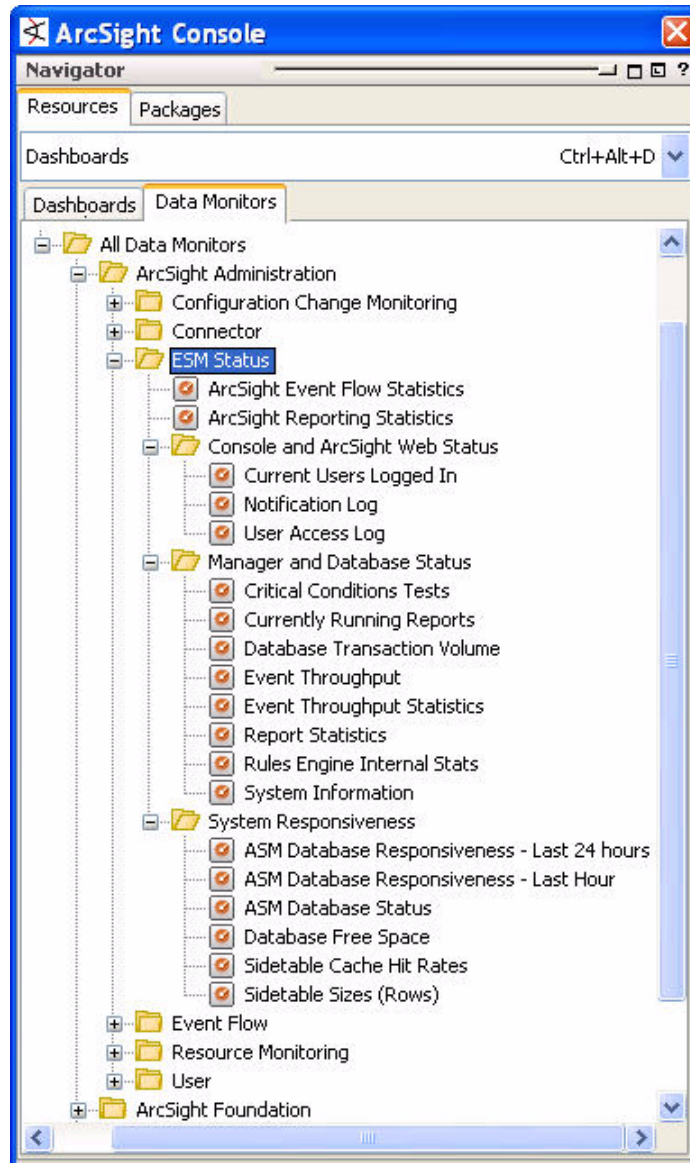
Connector Data Monitors

The Connector data monitors define the views shown in the Connector dashboards.



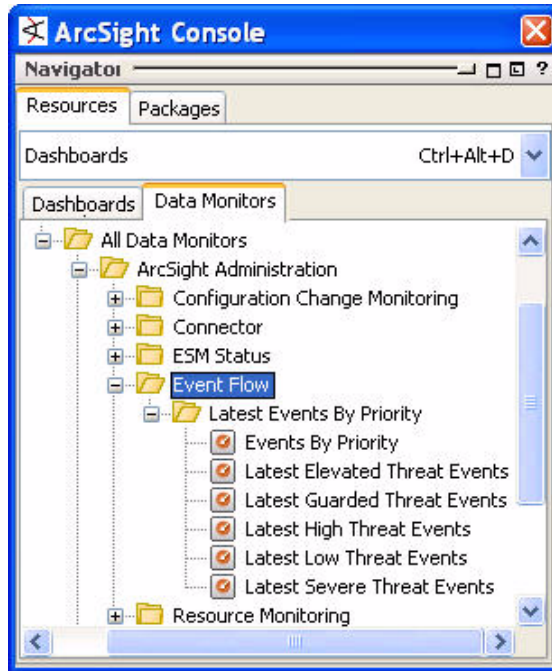
ESM Status Data Monitors

The ESM Status data monitors define the views shown in the ESM Status dashboards.



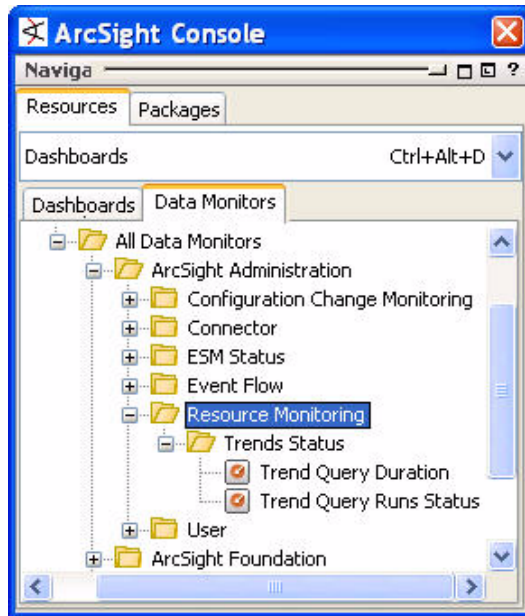
Event Flow Data Monitors

The Event Flow data monitors define the views shown in the Event Flow dashboards.



Resource Monitoring Data Monitors

The Resource Monitoring data monitors define the views shown in the Resource Monitoring dashboards.

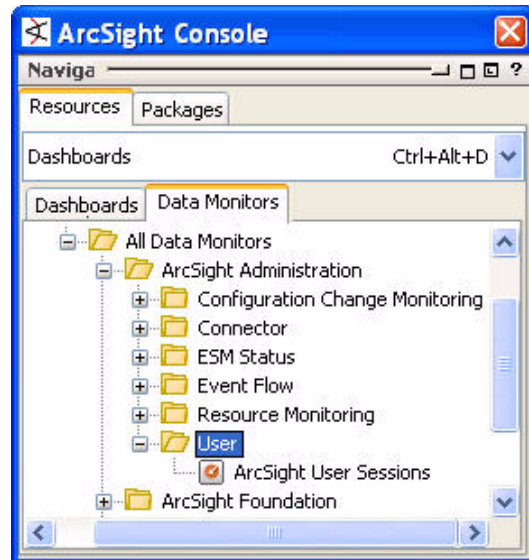


The Resource Monitoring data monitors are described in more detail below.

Data Monitor	Description
Trend Query Duration	This "Last N Events" Data Monitor shows the duration of the last 20 successful Trend queries. This Data Monitor is used in the "Trends Status" Dashboard.
Trend Query Runs Status	This "Last State" Data Monitor shows the status of the last Trend queries. When a Trend query starts the Trend state will be set to "Running". If the Trend query is successful the Trend state will be changed to "Successful". If an error occurs and the Trend query fails the Trend state will be set to "Failed". This Data Monitor is used by the "Trends Status" Dashboard.

User Monitoring Data Monitor

The User Monitoring data monitor defines the user session data shown in the ArcSight User Status dashboard.



The User Monitoring data monitor is described in more detail below.

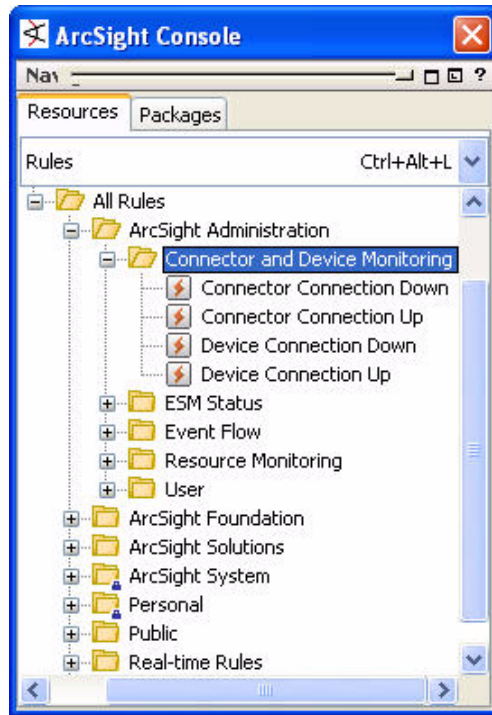
Data Monitor	Description
ArcSight User Sessions	This last state data monitor shows the status of the ArcSight user sessions to the manager. The data monitor shows the user-name, the IP address of the machine he's connecting from, and the status of the connection. The status of the connection can be "Logged in", "Logged out", or "Login Timed Out".

ArcSight Administration Rules

The ArcSight Administration rules correlate conditions that support the ArcSight Administration use cases.

Connector and Device Monitoring Rules

The Connector and Device Monitoring rules



The Connector and Device Monitoring rules are described in more detail below.

Rule	Description
Connector Connection Down	"This rule monitors the moving average of events on a per agent basis. It fires whenever the volume of events received from an agent goes down by 80% or more. The change threshold and the other moving average parameters are defined in the Moving Average dashboard for Agent and Device Status and the Agent Status data monitor. By default, this rule gets triggered whenever there is an 80% drop in the moving average of events. The rule firing indicates that the agent has failed or that the connection between the manager and agent is down. The time frame is 5 minutes. After this rule is triggered, a notification will be sent to SOC Operators. ***Note: This Rule will not fire when running in Turbo Mode Fastest!"

Rule	Description
Connector Connection Up	"This rule monitors the moving average of events on a per agent basis. It fires whenever the monitoring threshold drastically goes up (80%), indicating that the agent connection is alive again after being down. The monitoring threshold and the moving average parameters are defined in the Moving Average data monitor Agent StatusMonitor on the dashboard for Agents and Devices. This rule is triggered whenever there is an 80% increase in the moving average of events, indicating that the event flow restarted from that agent. The time frame is 5 minutes. ***Note: This rule will not fire when running in Turbo Mode Fastest!
Device Connection Down	"This rule monitors the moving average of events across all event-collecting devices. It fires whenever the volume of events received from a sensor goes down drastically (80%). The change threshold and the other moving average parameters are defined in the Moving Average dashboard for Sensors Data Monitor. By default, this rule gets triggered whenever there is an 80% drop in the moving average of events. The rule firing indicates that either the agent or sensor have failed, or that the connection between either the Manager and agent or the agent and device (sensor) is down. The time frame is 1 minute. After this rule is triggered, a notification will be sent to SOC Operators. ***Note: This rule will not fire when running in Turbo Mode Fastest!
Device Connection Up	This rule monitors the moving average of events across all event-collecting devices. It fires whenever the monitoring threshold drastically goes up (80%), indicating that the device connection is alive again after being down. The monitoring threshold and the moving average parameters are defined in the Moving Average dashboard for sensors. This rule gets triggered whenever there is an 80% increase in the moving average of events, indicating that the event flow restarted from that sensor. The time frame is 1 minute. ***Note: This rule will not fire when running in Turbo Mode Fastest!

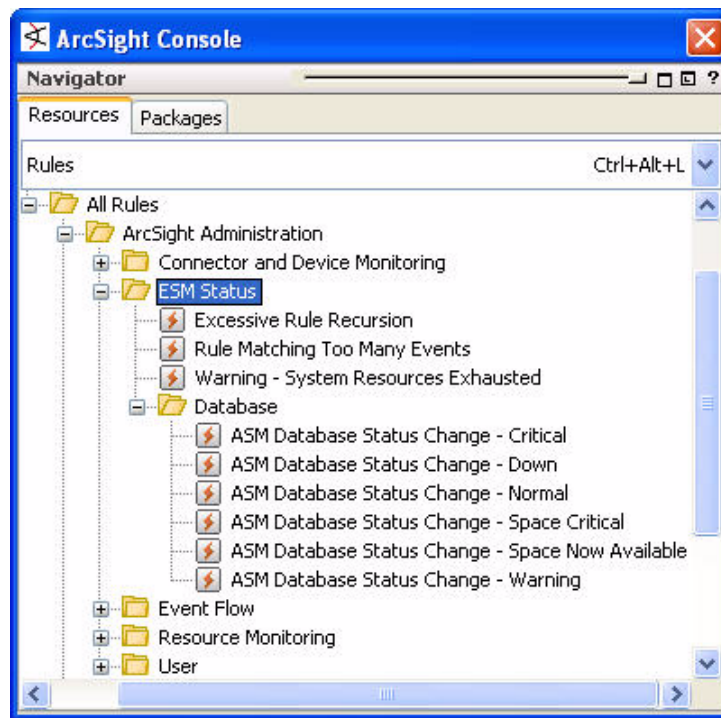
ESM Status Rules

The ESM Status rules correlate conditions for internal ESM and ArcSight database activity to detect potential problems.

Excessive rule recursion is when one rule triggers a succession of several other rules in a repetitive loop in a short time frame. In the case of the ESM status rules, excessive is considered when one rule triggers up to two other rules in a repetitive loop totalling 9 correlation events in a 5-minute time frame. Excessive rule recursion indicates that the rule conditions need to be modified so they are not triggered so easily.

Excessive rule recursion and other conditions can also lead to excessive rule matches. A rule is considered to match too many events when the system reaches 10,000 matches per minute.

System resource exhaustion checks for no response, error, and resource check failures from ArcSight components.



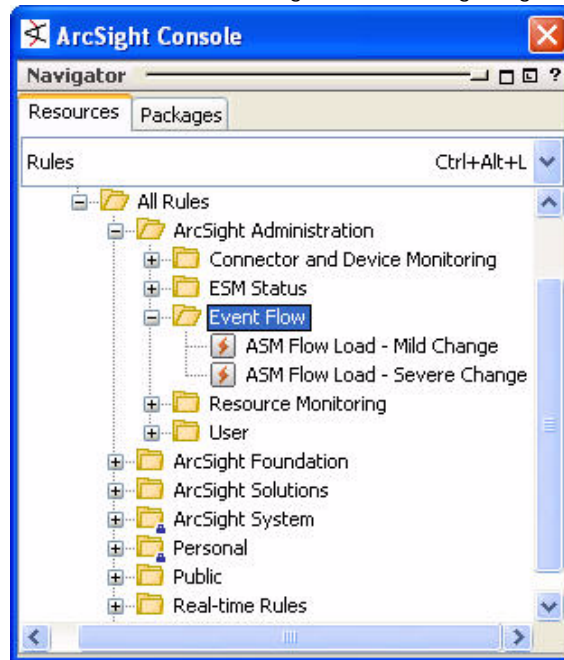
The ESM Status rules are described in more detail below.

Rule	Description
Excessive Rule Recursion	This rule detects excessive rule recursion. This rule looks for events coming from the ArcSight Security Manager with the 'Device Event Category' set to "/Rule/Warning/Loop". This rule only requires 1 such event in a time frame of 5 minutes. After this rule is triggered, a notification will be sent to SOC Operators."

Rule	Description
Rule Matching Too Many Events	"This rule detects rules that are matching too many events. This rule looks for events coming from the ArcSight Security Manager with the 'Device Event Category' set to '/Rule/Error/Deactivate/Unsafe'. This rule only requires 1 such event in a time frame of 5 minutes. After this rule is triggered, a notification will be sent to SOC Operators.
Warning - System Resources Exhausted	"This rule indicates that a device has detected a system resource issue. The rule fires whenever a resource is exhausted or a resource check fails. On first event, a notification is sent to SOC operators.***Note: This rule will not produce completely accurate results when running in Turbo Mode Fastest!
ASM Database Status Change - Critical	This rule detects if the database status is critical. This rule looks for an event's insert and retrieval time, and the status is considered critical when the 'EventInsertTimeNanos' field is greater than or equal to 50,000. This rule requires 2 such events in a time frame of 3 minutes. After the first event, the "agentSeverity" event field will be set to very-high.
ASM Database Status Change - Down	This rule detects if the database status is down. This rule looks for event's insert and retrieval time, and the status is considered critical when the 'EventInsertTimeNanos' field is equal to 0. This rule requires 2 such events in a time frame of 3 minutes. After the first event, the "agentSeverity" event field will be set to unknown.
ASM Database Status Change - Normal	This rule detects if the database status is normal. This rule looks for event's insert and retrieval time, and the status is considered critical when the 'EventInsertTimeNanos' field is less than or equal to 20,000. This rule requires 2 such events in a time frame of 3 minutes. After the first event, the "agentSeverity" event field will be set to low.
ASM Database Status Change - Space Critical	This rule detects if the database status is critical due to storage concerns. This rule looks for a base event saying that the database storage space is low. This rule only requires 1 such event to fire. After the first event, the "agentSeverity" event field will be set to very-high.
ASM Database Status Change - Space Now Available	This rule detects if the database status has returned to normal because storage space has been freed or added. This rule looks for a base event saying that database storage space is available. This rule only requires 1 such event to fire. After the first event, the "agentSeverity" event field will be set to Low.
ASM Database Status Change - Warning	This rule detects if the database status is at a warning level. This rule looks for event's insert and retrieval time, and the status is considered critical when the 'EventInsertTimeNanos' field is between 20,000 and 50,000. This rule requires 2 such events in a time frame of 3 minutes. After the first event, the "agentSeverity" event field will be set to medium.

Event Flow Rules

The Event Flow rules focus on mild and severe changes in ArcSight Status Monitor event loads. These detect when the ArcSight database is getting flooded with ASM events.

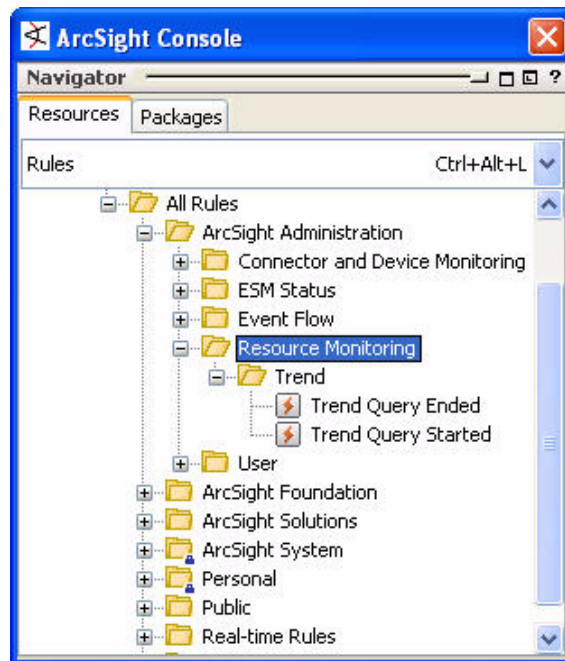


The Event Flow rules are described in more detail below.

Rule	Description
ASM Flow Load - Mild Change	This rule detects if there are mild changes in the flow load. This rule looks for 'ASM Flow Load' events that have a change greater than or equal to 33%. This rule requires 2 such events in a time frame of 2 minutes. After this rule is triggered, the "agentSeverity" event field will be set to low.
ASM Flow Load - Severe Change	This rule detects if there are severe changes in the flow load. This rule looks for 'ASM Flow Load' events that have a change greater than or equal to 66%. This rule requires 2 such events in a time frame of 3 minutes. After this rule is triggered, the "agentSeverity" event field will be set to medium.

Resource Monitoring Rules

The Resource Monitoring rules write entries to the Trend Queries active list, which tracks when trend queries start and end in order to report on trend performance.

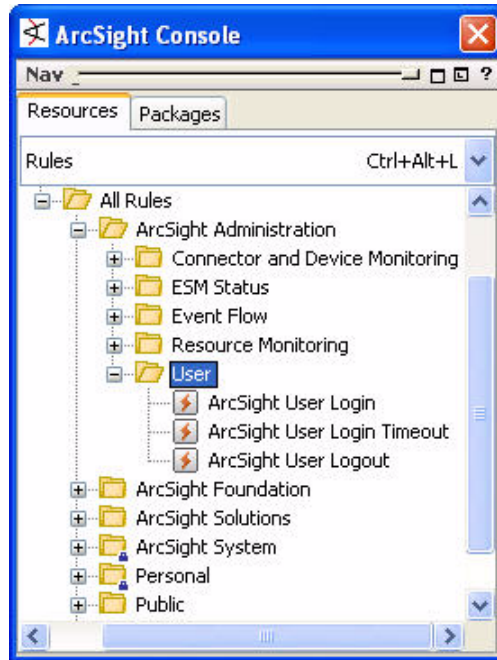


The Resource Monitoring rules are described in more detail below.

Rule	Description
Trend Query Ended	This rule fires when a Trend Query ends (success or failure) and remove the corresponding entry in the "Trend Queries" Active List.
Trend Query Started	This rule fires when a Trend Query starts and adds a new entry in the "Trend Queries" Active List containing the name of the Trend, the URI of the Trend, and the time the Query started.

User Rules

The User rules work with the ArcSight Administration session lists to track ESM user activity.

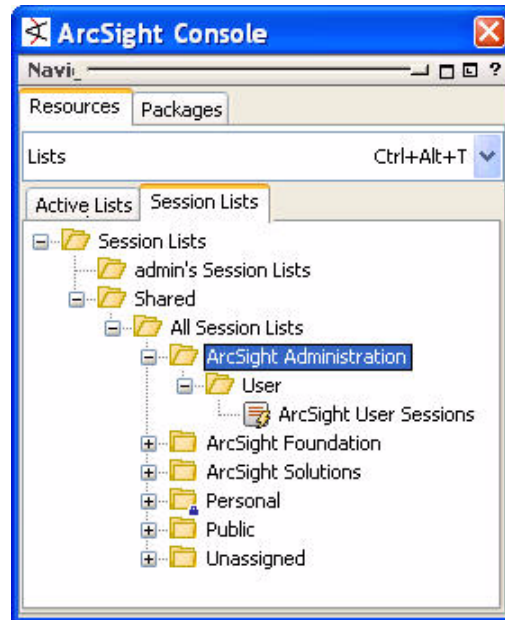


The User rules are described in more detail below.

Rule	Description
ArcSight User Login	This rule looks for ArcSight user login events. This rule will add the user name, the attacker address, the attacker zone, and the login time in the "ArcSight User Sessions" session list.
ArcSight User Login Timeout	This rule looks for ArcSight user login timeout events. This rule will terminate the ArcSight user session in the "ArcSight User Sessions" session list when an ArcSight user login timeout occurs.
ArcSight User Logout	This rule looks for ArcSight user logout events. This rule will terminate the ArcSight user session in the "ArcSight User Sessions" session list when an ArcSight user logout occurs.

ArcSight Administration Session List

The ArcSight Administration foundation contains a session list that is used to track ESM user activity. You can right-click on the Session List and select **Show entries** to view all the ArcSight Sessions with start time and end time for a username, client address and zone.



The User session list is described in more detail below.

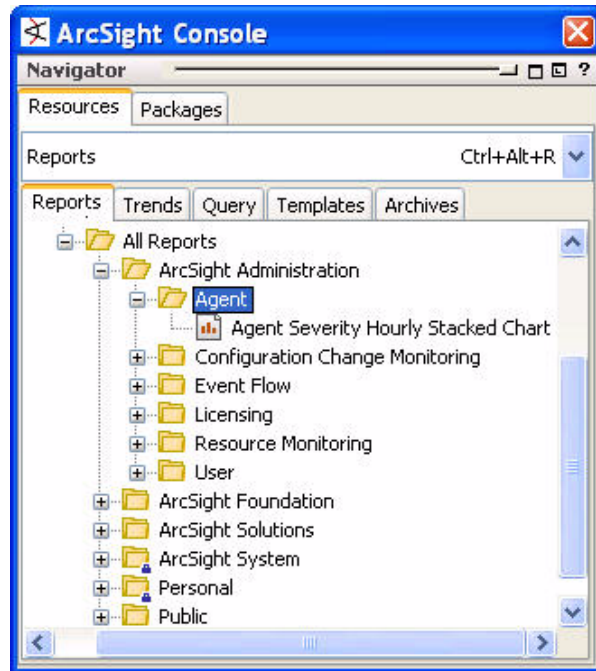
Session List	Description
ArcSight User Sessions	This session list stores the client username, client address and zone used by an ArcSight user to access the ArcSight manager in order to monitor the login times, logout times or console timeouts to determine who had access to the system over specific time periods.

ArcSight Administration Reports

The ArcSight Administration reports, queries, and trends provide historical statistics about the internal ArcSight activity use cases.

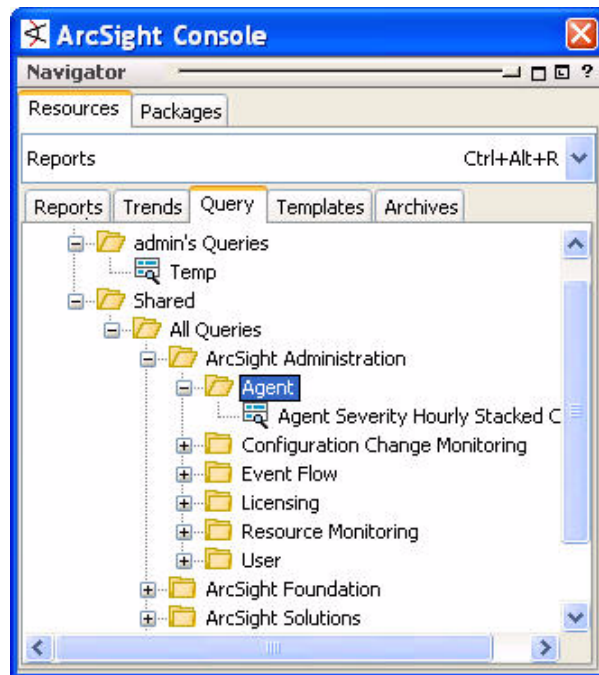
Agent Reports

The Agent reports provide statistics about Connector event activity.



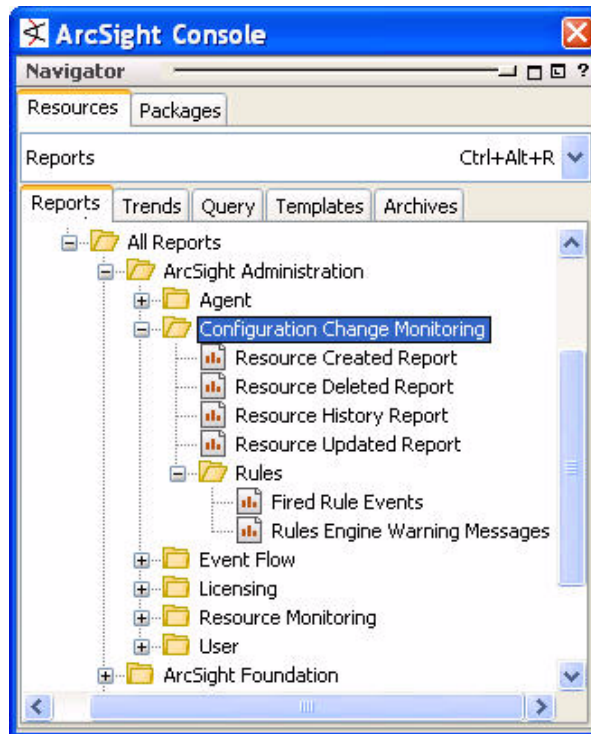
Agent Queries

The Agent queries provide the conditions for the Agent reports.



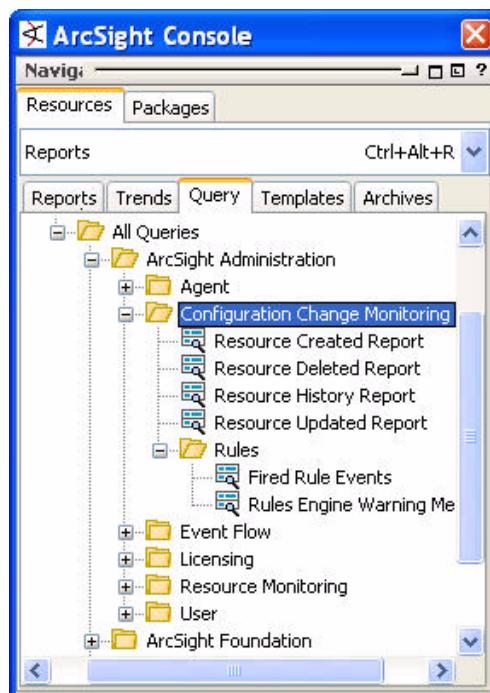
Configuration Change Monitoring Reports

The Configuration Change Monitoring reports provide statistics about configuration changes made to ArcSight resources.



Configuration Change Monitoring Queries

The Configuration Change Monitoring queries provide conditions for the Configuration Change Monitoring reports.

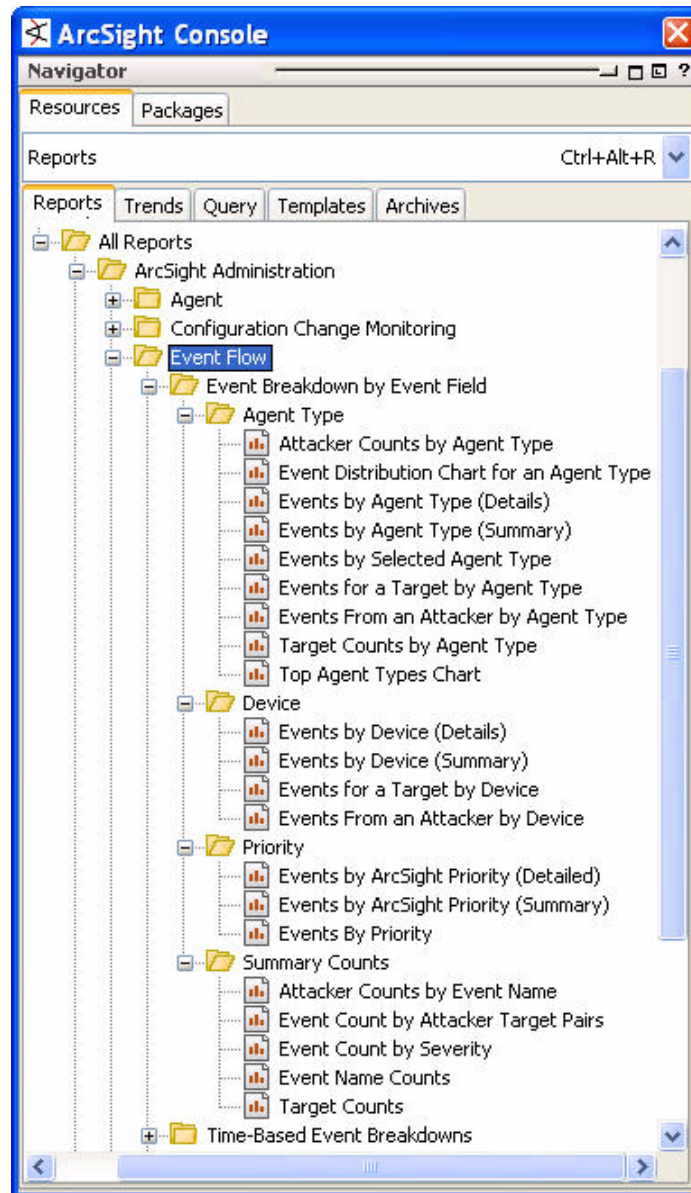


Event Flow Reports

The Event Flow reports provide statistics about events flowing in from ArcSight Connectors.

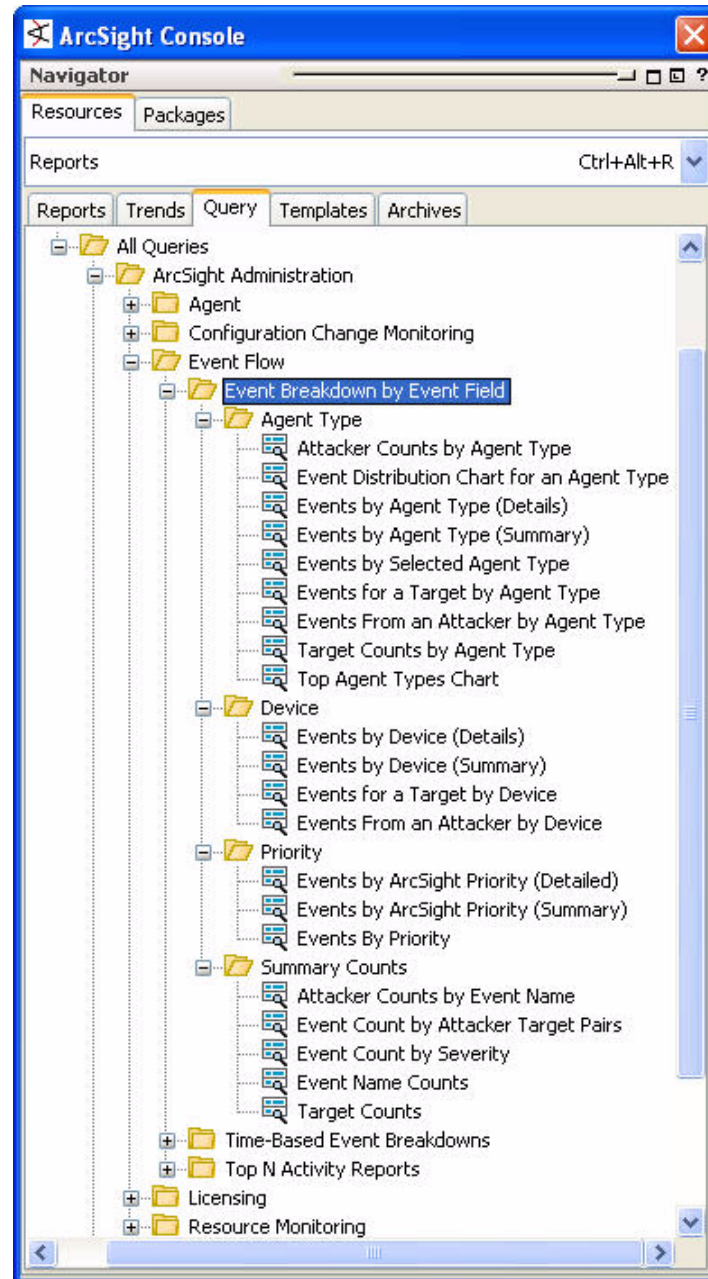
Event Breakdown by Event Field Reports

The Event Breakdown by Event Field reports provide statistics about events flowing in from ArcSight Connectors, sorted by relevant event field.



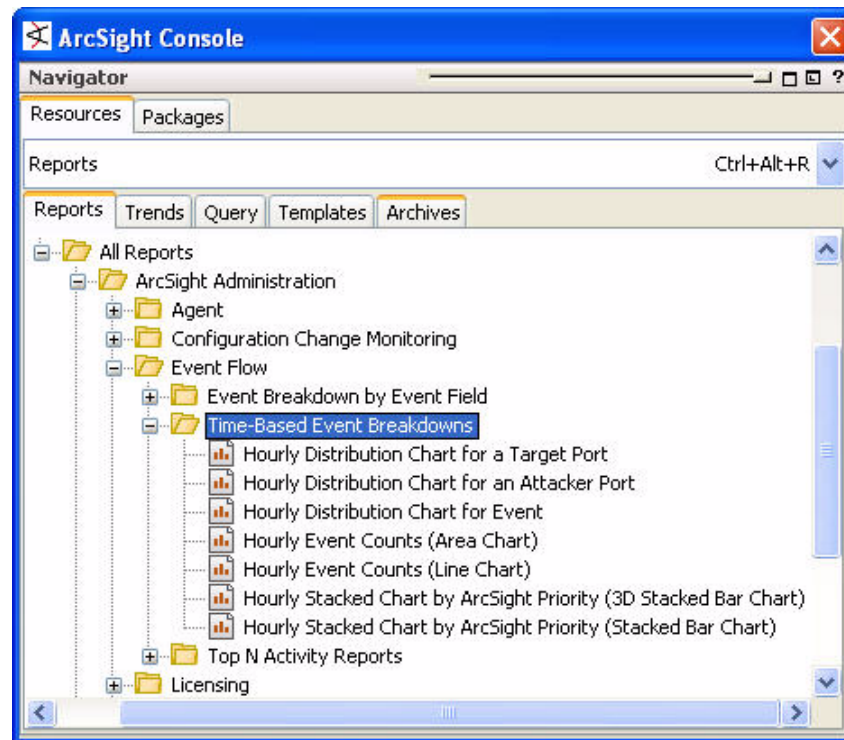
Event Breakdown by Event Field Queries

The Event Flow queries supply conditions for the Event Breakdown by Event Field reports.



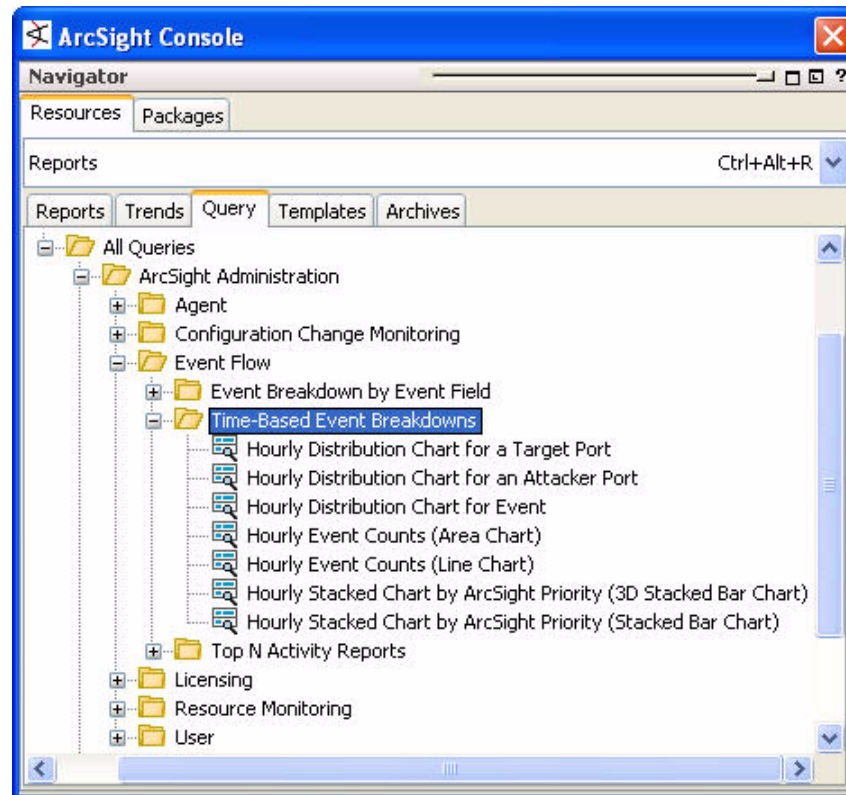
Time-Based Event Breakdown Reports

The Time-Based Event Breakdown reports provide various views of hourly statistics about events flowing in from ArcSight Connectors.



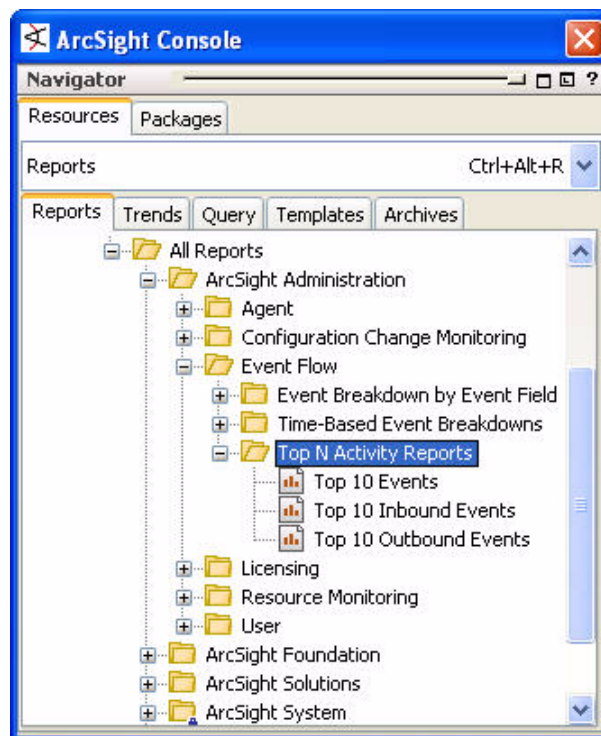
Time-Based Event Breakdown Queries

The Time-Based Event Breakdown queries supply conditions for the Time-Based Event Breakdown reports.



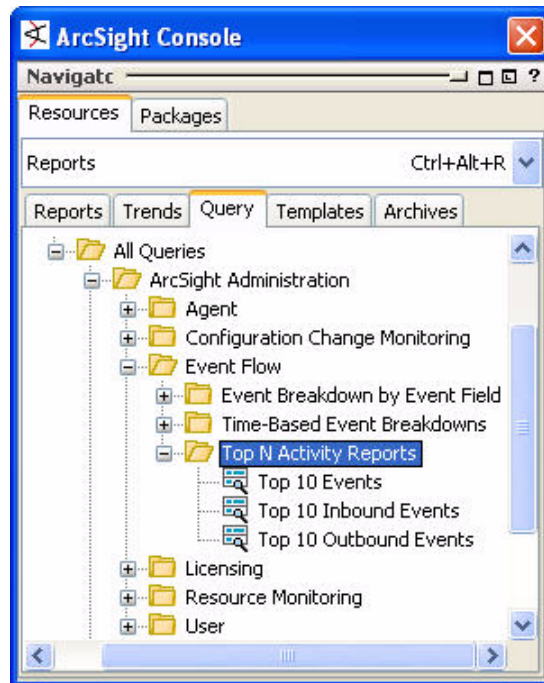
Top N Activity Reports

The Top N Activity Reports reports provide top 10 statistics about the most common events running through the ESM system.



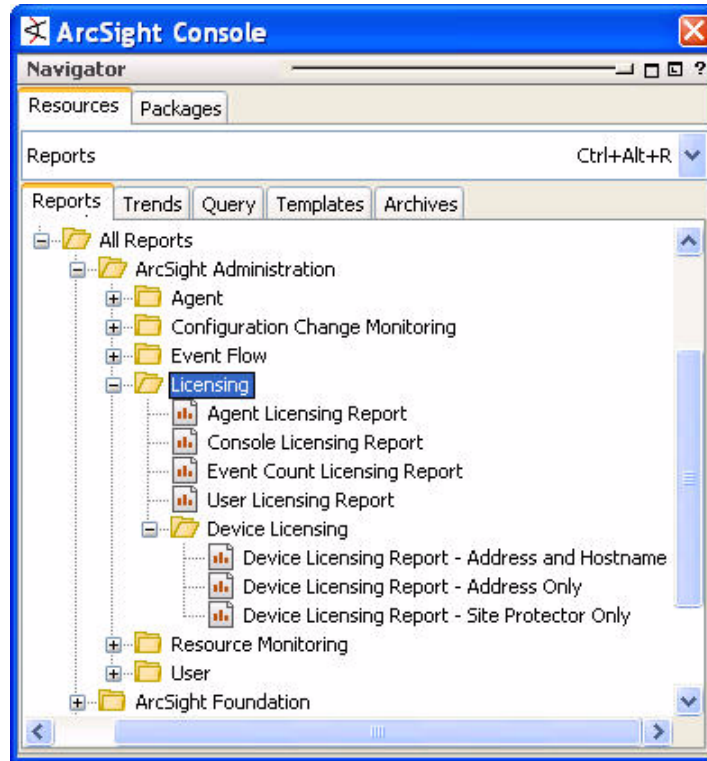
Top N Activity Reports Queries

The Top N Activity Reports queries supply conditions for the Top N Activity Reports reports.



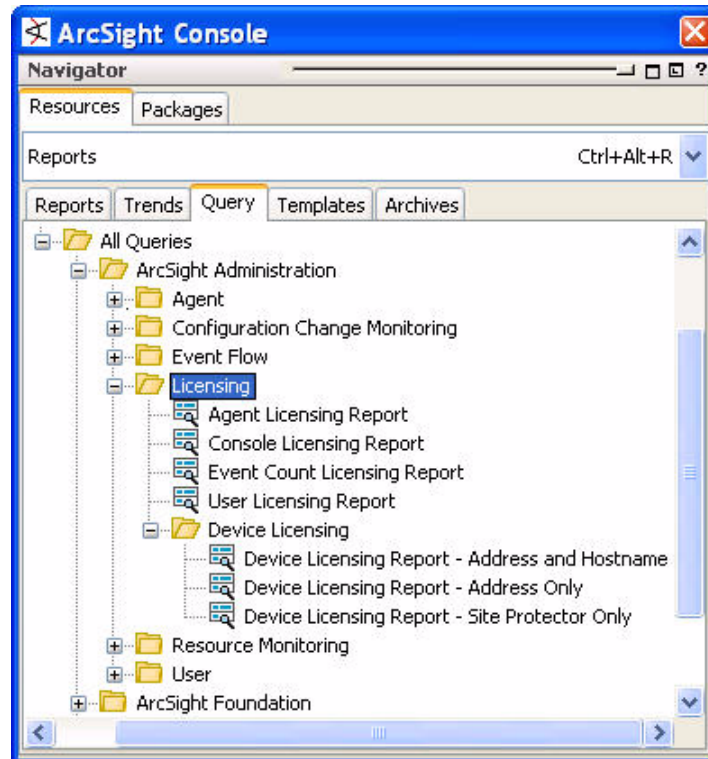
Licensing Reports

The licensing reports show what IP Addresses and Zones have been used to run ArcSight Consoles and SmartConnectors communicating with an ArcSight Manager. The User Licensing Report shows ArcSight user licensing information. These reports should be used to see where ArcSight-licensed activity is happening.



Licensing Queries

The Licensing queries supply conditions for the Licensing reports.



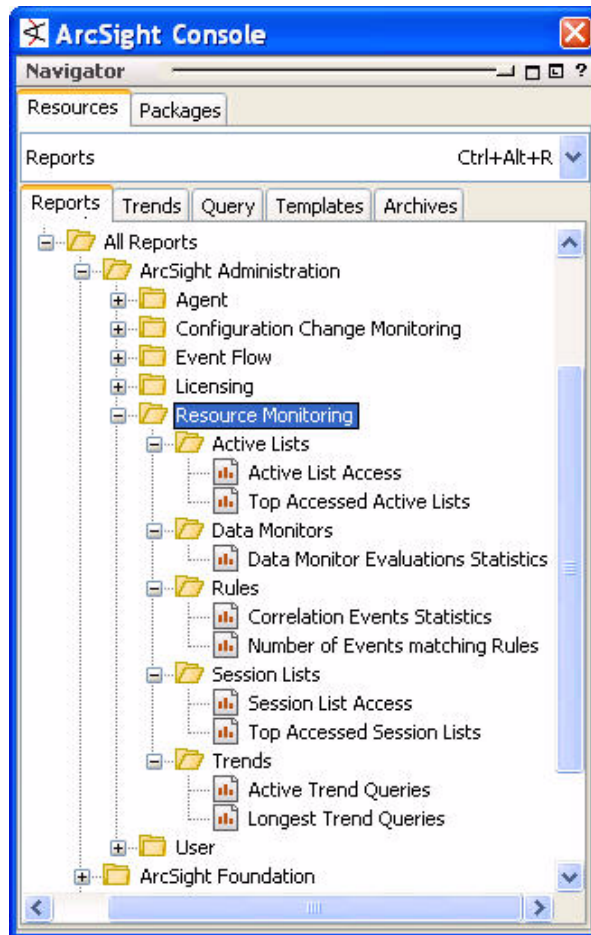
Resource Monitoring Reports

The Resource Monitoring reports provide statistics about active lists, data monitors, rules, session lists and trends.

The active list reports show statistics, such as how often the lists are modified, updated, and which are the most used active lists. This data can be used to see if there is any configuration issue where an active list would be updated too often, for example.

The rule reports show statistics about correlation events in the last hour.

The trend reports show statistics about the different trends in the system, such as which ones take a long time to run. This data can be useful to evaluate trend performance, and decide to disable costly trends that are not used.



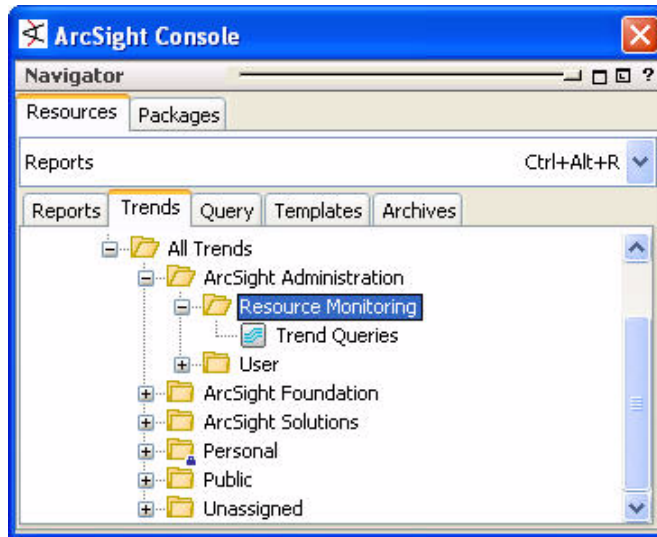
The Resource Monitoring reports are described in more detail below.

Report	Description
Active List Access	This Report shows Active List access statistics. This Report contains a curve chart and a table. The chart shows the number of added, deleted, and updated Active List entries in the last hour, grouping the counts by 10 minutes intervals. The table shows the details of the Active List Access grouping the number by time interval and Active List name.

Report	Description
Top Accessed Active Lists	This Report shows the Top 10 accessed Active Lists. This Report contains a 3d bar chart and a table. The chart shows the Top 10 accessed Active Lists in the last hour, grouping the counts by 10 minutes intervals. The table shows the details of the Active List Access grouping the number by Active List name and time interval.
Data Monitor Evaluations Statistics	This Report shows a chart with the average number of Data Monitor evaluations per second.
Correlation Events Statistics	This Report shows Correlation Events statistics. This Report contains a 3d bar chart and a table. The chart shows the number of Correlation Events in the last hour, grouping them by 10 minutes intervals. The table shows the details of the number of Correlation Events grouping them by Rule name and time interval.
Number of Events matching Rules	This Report shows the total number of events matching Rules in the last hour grouping them by 10 minutes intervals. This Report contains a line chart. The chart shows the number of events matching Filter Rules, Join Rules, and the total of both types of Rules.
Session List Access	This Report shows Session List access statistics. This Report contains a curve chart and a table. The chart shows the number of added, deleted, and updated Session List entries in the last hour, grouping the counts by 10 minutes intervals. The table shows the details of the Session List Access grouping the number by time interval and Active List name.
Top Accessed Session Lists	This Report shows the Top 10 accessed Session Lists. This Report contains a 3d bar chart and a table. The chart shows the Top 10 accessed Session Lists in the last hour, grouping the counts by 10 minutes intervals. The table shows the details of the Session List Access grouping the number by Active List name and time interval.
Active Trend Queries	This Report shows the list of all the currently running Trend Queries and their durations.
Longest Trend Queries	This Report shows the status of the longest Trend Queries for the last day. The chart shows the top 10 longest Trend Queries and the table shows the details for the top 20 Trend Queries.

Resource Monitoring Trend

The Resource Monitoring Trend supplies trend data for the Resource Monitoring trend reports.

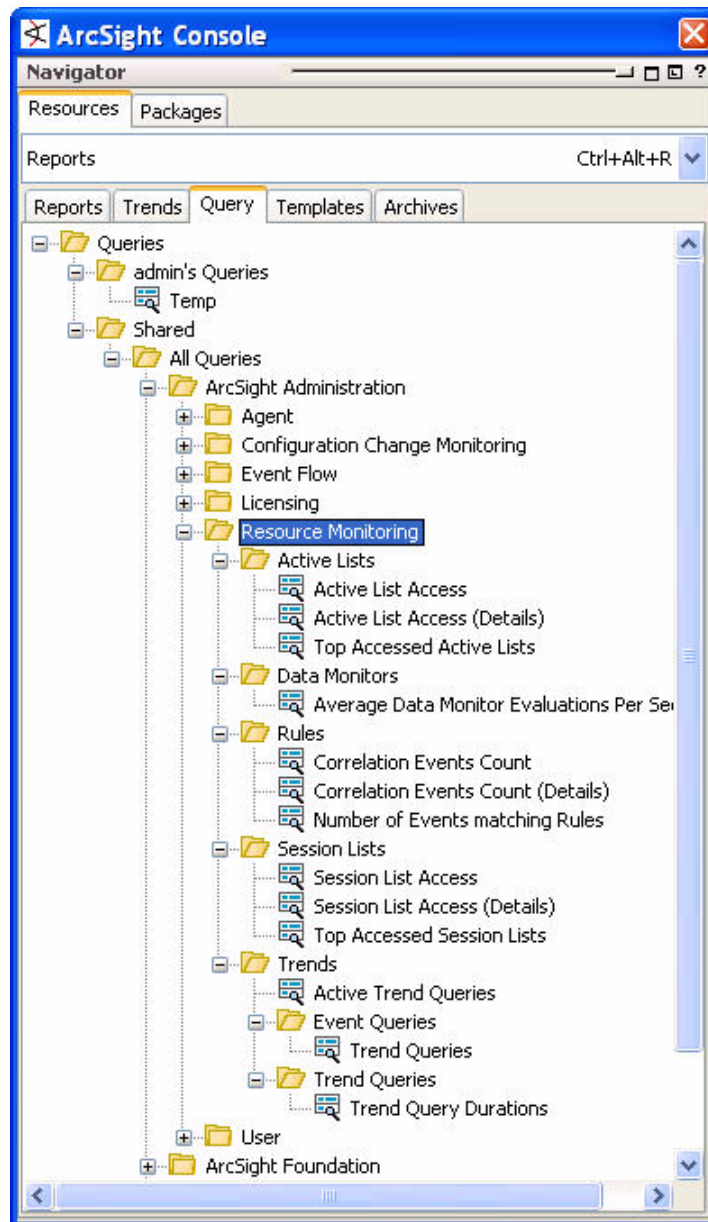


The Resource Monitoring trend is described in more detail below.

Trend	Description
Trend Queries	This Trend stores all the successful Trend Queries runs. It will store the name of the Trend, the URI of the Trend, the start time of the Trend Query, the number of rows inserted in the Trend table, and the duration of the Trend Query run.

Resource Monitoring Queries

The Resource Monitoring queries express conditions for the Resource Monitoring reports.

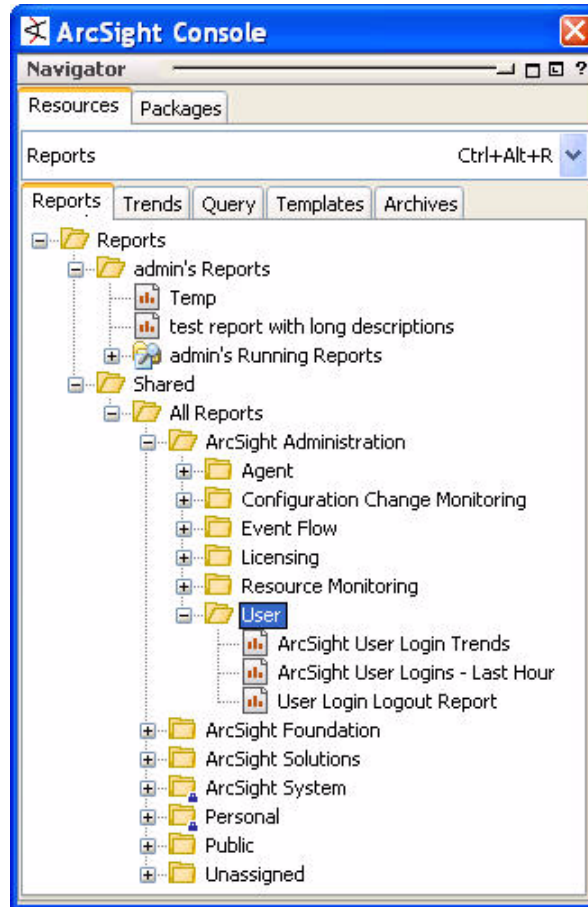


The Resource Monitoring Trend Queries are described in more detail below.

Query	Description
Active Trend Queries	This Query queries the "Active Trend Query Runs" Active List. The Query will return the list of all the currently running Trends.
Trend Queries	This Query uses the "Trend Query Duration" Filter to return all the successful Trend Query runs events.
Trend Query Durations	This Query queries the "Trend Queries" Trend and returns the duration of all the successful Trend Queries in the last day.

User Reports

The User reports provide statistics about ESM user activity.

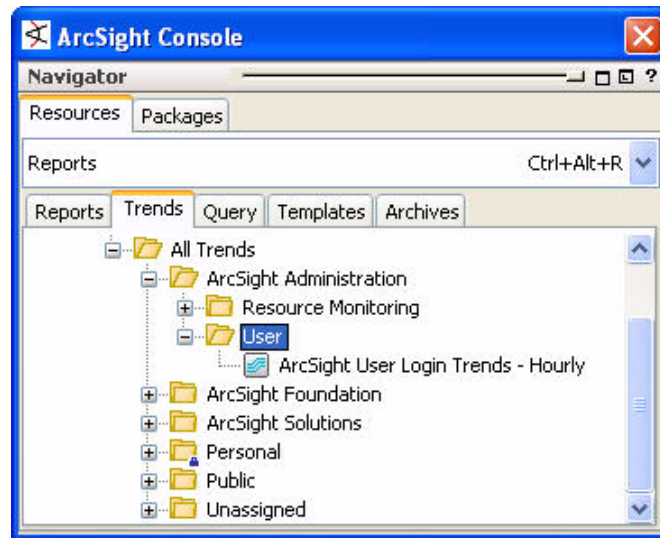


The User reports are described in more detail below.

Report	Description
ArcSight User Login Trends	This report shows a summary of the number of ArcSight user logins in the previous 24 hours. It contains a bar chart and a table. The bar chart shows the total number of logins by user and the table shows the number of logins by user per hour.
ArcSight User Logins - Last Hour	This report shows the details for all the ArcSight user logins in the past 24 hours. It contains a table showing the source host, the username, and the login time.
User Login Logout Report	

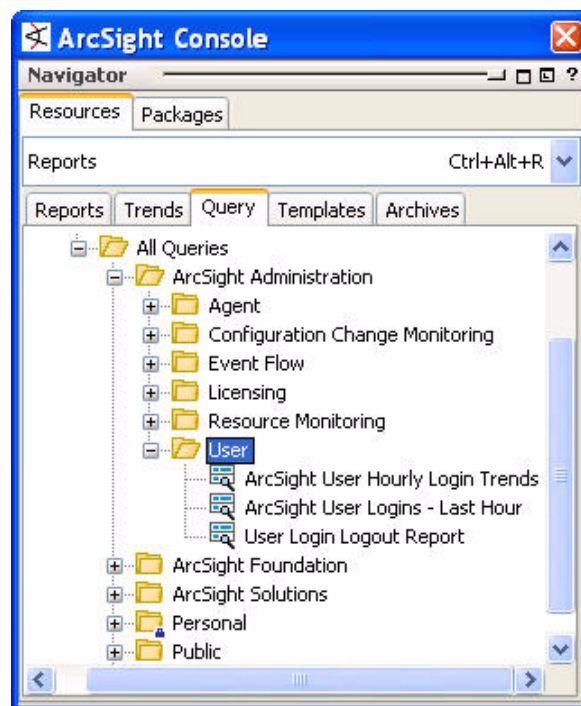
User Trend

The User trend collects ESM user login and logout data over time.



User Queries

The User queries supply conditions for the User reports.



The User queries are described in more detail below.

Query	Description
ArcSight User Hourly Login Trends	This query on the ArcSight User Login Trends - Hourly trend selects Target User Name, Attacker Zone, Attacker Address and the Hour of each console login for the ArcSight User Login Trends report.
ArcSight User Logins - Last Hour	This query tracks the counts of how many users logged into ArcSight over the previous hour. It checks for firings of the login tracking rule that is used to populate a data monitor with currently logged in users.

Shared Package Inventory



This appendix contains a list of the resources contained in the shared resource packages, *Anti-Virus* and *Network Filters*. These packages contain resources that are used by one or more of the other foundation packages. Dependencies between these packages and the foundation packages they support are managed by the Packages resource.

- [“Anti-Virus Package” on page 362](#)
- [“Network Filters Package” on page 363](#)

Anti-Virus Package

This package is a set of anti-virus content required by the Configuration Monitoring and Intrusion Monitoring packages. The Anti-Virus package is installed automatically.

Anti-Virus Filters

- AV - All
- AV - Clean or Quarantine Failed
- AV - Failed Updates
- AV - Found Infected
- Virus Activity

Anti-Virus Reports

- Anti-Virus Updates - All - Failed
- Anti-Virus Updates - All - Summary
- Anti-Virus Updates - Regulated Systems - Failed
- Anti-Virus Updates - Regulated Systems - Summary

Anti-Virus Queries

- Anti-Virus Configuration Updates - All - Failed
- Anti-Virus Configuration Updates - All - Summary
- Anti-Virus Configuration Updates - Regulated Systems - Failed
- Anti-Virus Configuration Updates - Regulated Systems - Summary
- Anti-Virus Updates - All - Failed
- Anti-Virus Updates - All - Summary
- Anti-Virus Updates - Regulated Systems - Failed
- Anti-Virus Updates - Regulated Systems - Summary
- Anti-Virus Updates - All - Failed
- Anti-Virus Updates - All - Summary
- Anti-Virus Updates - Regulated Systems - Failed
- Anti-Virus Updates - Regulated Systems - Summary
- Anti-Virus Updates - Regulated Systems - Summary

Network Filters Package

This package contains a set of filters required by the Intrusion Monitoring and Network Monitoring packages. It is installed automatically with ESM.

Network Filters

Filter	Description
External Source	This filter is looking for events coming from outside the company network.
External Target	This filter is looking for events targeting the outside network.
Internal Source	This filter is looking for events coming from inside the company network.
Internal Target	This filter is looking for events targeting inside the company network.
External to External Events	This filter is looking for events external to the company network.
Inbound Events	This filter is looking for events coming from the outside network targeting inside the company network.
Internal to Internal Events	This filter is looking for events internal to the company network.
Outbound Events	This filter is looking for events coming from inside the company network targeting the outside network.

Default Access Permissions

By default, access to the following resource trees is granted to the following standard ArcSight user groups.

Resource Group	Administrators Read	Default User Groups Read	Operators Read	Analyst Read	Analyzer Administrators Read	Administrators Write	Default User Groups Write	Operators Write	Analyst Write	Analyzer Administrators Write
/All Active Channels/	X					X				
/All Active Channels/ArcSight Foundation/		X								X
/All Active Channels/ArcSight Solutions/		X								X
/All Active Channels/ArcSight System/		X								X
/All Active Channels/Packages/					X					X
/All Active Channels/Public/		X					X			
/All Active Lists/	X					X				
/All Active Lists/ArcSight Foundation/		X								X
/All Active Lists/ArcSight Solutions/		X								X
/All Active Lists/ArcSight System/		X								X
/All Active Lists/Packages/					X					X
/All Active Lists/Public/		X					X			
/All Agents/	X					X				
/All Agents/Site Connectors/					X					
/All Archived Reports/	X					X				
/All Archived Reports/Packages/					X					X
/All Archived Reports/Public/		X					X			

Resource Group	Administrators Read	Default User Groups Read	Operators Read	Analyst Read	Analyzer Administrators Read	Administrators Write	Default User Groups Write	Operators Write	Analyst Write	Analyzer Administrators Write
/All Asset Categories/	X				X	X				X
/All Asset Categories/ArcSight Foundation/		X								X
/All Asset Categories/ArcSight Solutions/		X								X
/All Asset Categories/Packages/					X					X
/All Asset Categories/Site Asset Categories/		X					X			
/All Asset Categories/System Asset Categories/		X								X
/All Assets/	X	X				X				X
/All Cases/All Cases/	X					X				
/All Cases/All Cases/ArcSight Solutions/			X							
/All Cases/All Cases/ArcSight System/			X						X	
/All Cases/All Cases/Public/		X					X			
/All Customers/	X	X				X				X
/All Dashboards/	X					X				
/All Dashboards/ArcSight Administration/					X					
/All Dashboards/ArcSight Foundation/		X								X
/All Dashboards/ArcSight Solutions/		X								X
/All Dashboards/Packages/					X					X
/All Dashboards/Public/		X					X			
/All Data Monitors/	X					X				
/All Data Monitors/ArcSight Administration/					X					
/All Data Monitors/ArcSight Foundation/		X								X
/All Data Monitors/ArcSight Solutions/		X								X
/All Data Monitors/Packages/					X					X
/All Data Monitors/Public/		X					X			
/All Destinations/	X				X	X				X
/All Field Sets/	X					X				
/All Field Sets/ArcSight Foundation/		X								X

Resource Group	Administrators Read	Default User Groups Read	Operators Read	Analyst Read	Analyzer Administrators Read	Administrators Write	Default User Groups Write	Operators Write	Analyst Write	Analyzer Administrators Write
/All Field Sets/ArcSight Solutions/		X								X
/All Field Sets/ArcSight System/		X								X
/All Field Sets/Packages/					X					X
/All Field Sets/Public/		X					X			
/All Fields/	X	X				X	X			
/All Files/	X					X				
/All Filters/	X					X				
/All Filters/ArcSight Foundation/		X								X
/All Filters/ArcSight Solutions/		X								X
/All Filters/ArcSight System/		X								X
/All Filters/Packages/					X					X
/All Filters/Public/		X					X			
/All Knowledge Base Articles/	X					X				
/All Knowledge Base Articles/Public/		X					X			
/All Locations/	X					X				
/All Locations/ArcSight System/		X								X
/All Locations/Public/		X					X			
/All Networks/	X					X				
/All Networks/ArcSight System/		X								X
/All Networks/ArcSight System/Core/		X								
/All Networks/Public/		X					X			
/All Packages/	X					X				
/All Packages/ArcSight Foundation/		X								
/All Packages/ArcSight Solutions/		X								
/All Packages/ArcSight System/		X								
/All Partitions/	X					X				
/All Partitions/System Partitions/					X					X

Resource Group	Administrators Read	Default User Groups Read	Operators Read	Analyst Read	Analyzer Administrators Read	Administrators Write	Default User Groups Write	Operators Write	Analyst Write	Analyzer Administrators Write
/All Patterns/	X					X				
/All Patterns/ArcSight Solutions/		X								
/All Patterns/Public/		X						X		X
/All Profiles/	X					X				
/All Profiles/ArcSight Solutions/		X								
/All Profiles/ArcSight System/		X								X
/All Profiles/Public/		X					X			
/All Queries/	X					X				
/All Queries/ArcSight Administration/					X					
/All Queries/ArcSight Foundation/		X								X
/All Queries/ArcSight Solutions/		X								
/All Queries/Packages/					X					X
/All Queries/Public/		X					X			
/All Report Templates/	X					X				
/All Report Templates/ArcSight Foundation/		X								X
/All Report Templates/ArcSight Solutions/		X								X
/All Report Templates/ArcSight System/		X								X
/All Report Templates/Packages/					X					X
/All Report Templates/Public/		X					X			
/All Reports/	X					X				
/All Reports/ArcSight Administration/					X					
/All Reports/ArcSight Foundation/		X								X
/All Reports/ArcSight Solutions/		X								X
/All Reports/ArcSight System/		X								X
/All Reports/Packages/					X					X
/All Reports/Public/		X					X			
/All Rules/	X					X				

Resource Group	Administrators Read	Default User Groups Read	Operators Read	Analyst Read	Analyzer Administrators Read	Administrators Write	Default User Groups Write	Operators Write	Analyst Write	Analyzer Administrators Write
/All Rules/ArcSight Administration/					X					
/All Rules/ArcSight Foundation/		X								X
/All Rules/ArcSight Solutions/		X								X
/All Rules/ArcSight System/		X								X
/All Rules/Packages/					X					X
/All Rules/Public/		X					X			
/All Rules/Real-time Rules/		X								X
/All Scanner Reports/	X					X				
/All Scheduled Tasks/										
/All Session Lists/	X					X				
/All Session Lists/ArcSight Administration/					X					
/All Session Lists/ArcSight Foundation/		X								X
/All Session Lists/ArcSight Solutions/		X								X
/All Session Lists/Packages/					X					X
/All Session Lists/Public/		X					X			
/All Snapshots/	X					X				
/All Snapshots/ArcSight Solutions/					X					
/All Snapshots/Public/		X					X			
/All Stages/	X	X				X				X
/All Trends/	X					X				
/All Trends/ArcSight Administration/					X					
/All Trends/ArcSight Foundation/		X								X
/All Trends/ArcSight Solutions/		X								X
/All Trends/Packages/					X					X
/All Trends/Public/		X					X			
/All Users/Administrators/	X					X				
/All Users/Custom User Groups/	X					X				

Resource Group	Administrators Read	Default User Groups Read	Operators Read	Analyst Read	Analyzer Administrators Read	Administrators Write	Default User Groups Write	Operators Write	Analyst Write	Analyzer Administrators Write
/All Users/Default User Groups/	X					X				
/All Vulnerabilities/	X	X				X				X
/All Zones/	X	X				X				X

Index

A

Active Channels

- ArcSight Administration Foundation 325
- Configuration Monitoring Foundation 86
- Intrusion Monitoring Foundation 150
- Network Monitoring Foundation 257
- System Active Channels 62
- Workflow Foundation 309

Active Lists

- ArcSight Administration Foundation 327
- Configuration Monitoring Foundation 88
- General Configuration 41
- Intrusion Monitoring Foundation 155

ArcSight Administration Foundation

- Active Channels 325
- Active Lists 327
- Configuration Summary 316
- Dashboards 328
- Data Monitors 329, 330, 331, 332, 333, 334
- Field Sets 326
- Filters 317
- Foundations
 - ArcSight Administration Foundation 315
- Overview 315
- Queries 344, 345, 347, 349, 350, 352, 356, 358
- Reports 343
- Rules 335
- Session Lists 342
- Trends 355

Asset Categories 30

- Assigning 31
- Criticality 31

Asset Modeling

- Protected Network 31

Assets 29

C

Cases

- Intrusion Monitoring Foundation 191

Configuration

- Active Lists 41
- ArcSight Administration Foundation 316
- Asset Auto-Creation Filters 35
- Configuration Monitoring Foundation 74
- Connector Asset Auto-Creation Filter 36
- Device Asset Auto-Creation Filter 38
- General Configuration 17, 35
- General Configuration Planning 28
- Intrusion Monitoring Foundation 125
- Report Templates 69

- SNMP Trap Forwarding Filter 39
- Configuration Monitoring Foundation 71
- Active Channels 86
- Active Lists 88
- Configuration 74
- Dashboards 89
- Data Monitors 91
- Field Sets 87
- Filters 75
- Focused Reports 114
- Overview 72
- Queries 97, 100, 105, 108, 113, 116
- Reports 93
- Rules 119
- Supported Devices 73
- Trends 93
- Core Content
 - About 47

D

Dashboards

- ArcSight Administration Foundation 328
- Configuration Monitoring Foundation 89
- Intrusion Monitoring Foundation 156, 170, 172
- Network Monitoring Foundation 259

Data Monitors

- ArcSight Administration Foundation 329, 330, 331, 332, 333, 334
- Configuration Monitoring Foundation 91
- Intrusion Monitoring Foundation 159, 160, 164, 165, 166, 168, 169, 171, 174
- Last State Data Monitors 176
- Network Monitoring Foundation 261, 263, 265, 267

E

- Event Type Filters 60

F

Field Sets

- ArcSight Administration Foundation 326
- Configuration Monitoring Foundation 87
- Intrusion Monitoring Foundation 153
- Network Monitoring Foundation 258

Files 54

Filters

- ArcSight Administration Foundation 317
- Configuration Monitoring Foundation 75
- Intrusion Monitoring Foundation 127

- Network Monitoring Foundation 250
- Focused Reports
 - Changing Focus of 115
 - Configuration Monitoring Foundation 114
 - Network Monitoring Foundation 284
- Foundations
 - ArcSight Workflow Foundation 307
 - Configuration Monitoring Foundation 71
 - Intrusion Monitoring Foundation 121
 - Network Monitoring Foundation 243
 - Overview 8, 9
 - What are 8

I

- Imported Package 26
- Installation 17
- Installed Package 26
- Intrusion Monitoring Foundation 121
 - Active Channels 150
 - Active Lists 155
 - Cases 191
 - Configuration 125
 - Dashboards 156, 170, 172
 - Data Monitors 159, 160, 164, 165, 166, 168, 169, 171, 174
 - Last State Data Monitors 176
 - Field Sets 153
 - Filters 127
 - Overview 121
 - Queries 196, 199, 201, 204, 207, 209, 211, 213, 218, 219, 220, 222, 224, 226, 227, 228, 229
 - Reports 192
 - Rules 177
 - Trends 231
- Invalid Resources 22

L

- Locations 53
- Locking
 - What is 13

N

- Network Modeling
 - Asset Categories 30
 - Assets 29
 - Networks 30
 - What is 29
 - Zones 29
- Network Monitoring Foundation 243
 - Active Channels 257
 - Dashboards 259
 - Data Monitors 261, 263, 265, 267
 - Field Sets 258
 - Filters 250
 - Focused Reports 284
 - Changing Focus of 285
 - Overview 243
 - Queries 273, 276, 279, 287, 294, 299, 303
 - Reports 269
 - Rules 305
 - Supported Devices 243

- Trends 269
- Networks 30

P

- Packages
 - Delete 27
 - Installation Overview 25
 - Overview 8
 - Package States 26
 - Uninstall 27
 - What are 12
- Pattern Discovery Profiles 66
- Priority Formula 54
 - Criticality Asset Categories 31

Q

- Queries
 - ArcSight Administration Foundation 344, 345, 347, 349, 350, 352, 356, 358
 - Configuration Monitoring Foundation 97, 100, 105, 108, 113, 116
 - Intrusion Monitoring Foundation 196, 199, 201, 204, 207, 209, 211, 213, 218, 219, 220, 222, 224, 226, 227, 228, 229
 - Network Monitoring Foundation 273, 276, 279, 287, 294, 299, 303
 - Workflow Foundation 312, 314

R

- Report Templates 68
 - Customize Branding in 69
- Reports
 - ArcSight Administration Foundation 343
 - Configuration Monitoring Foundation 93
 - Intrusion Monitoring Foundation 192
 - Network Monitoring Foundation 269
 - Workflow Foundation 311
- Resource ID 14
- Rules
 - ArcSight Administration Foundation 335
 - Configuration Monitoring Foundation 119
 - Intrusion Monitoring Foundation 177
 - Network Monitoring Foundation 305

S

- SANS Top 5
 - Configuration Monitoring Foundation 118
 - Intrusion Monitoring Foundation 234
 - Network Monitoring Foundation 301
 - Overview 15
- Session Lists
 - ArcSight Administration Foundation 342
- SmartConnectors
 - For Standard Content 28
- SNMP Forwarding Filters 61
- System Content
 - About 47
 - Active Channels 62
 - Field Sets 64
 - Asset Categories 49
 - Site Asset Categories 49

- System Asset Categories 51
- Files 54
- Filters 58
 - Event Type Filters 60
 - SNMP Forwarding Filters 61
- Locations 53
- Overview 48
- Priority Formula 54
- Reports
 - Core Reports 66
 - Vulnerabilities 51
- System User 14
- Sytsem Content
 - Reports
 - Report Templates 68

T

- Threat Level Formula. See Priority Formula
- Trends
 - About 43
 - ArcSight Administration Foundation 355
 - Configuration Monitoring Foundation 93
 - Enabling and Disabling 45
 - Intrusion Monitoring Foundation 231
 - Network Monitoring Foundation 269

U

- Upgrade 17

- After Upgrade 20
 - Verify Customer Content 23
- Asset Auto-Creation Filters 23
- Before Upgrade 20
- Deprecated Resources 19
- Invalid Resources 22
- Network Management Filter 23
- Overview 17
- SNMP Trap Sender Filter 23

V

- Vulnerabilities 51

W

- What's New in v4.0 8, 23
 - Deprecated Resources 19
 - Upgrade Overview 18
- Workflow Foundation 307
 - Active Channels 309
 - Configuration Summary 308
 - Overview 307
 - Queries 312, 314
 - Reports 311

Z

- Zones 29

