This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2013 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.
CA Technologies Product References

This document refers to the following CA products:

- CA Anomaly Detector
- CA Event Manager
- CA NetVoyant
- CA Network Flow Analysis (ReporterAnalyzer)
- CA Application Delivery Analysis (SuperAgent)
- CA Unified Communications Monitor
Related Documentation

This guide provides background information, procedures, and best-practice recommendations to help you use CA Anomaly Detector effectively.

This guide contains the following sections:

- **Introduction to CA Anomaly Detector** (see page 11) -- Features and benefits of CA Anomaly Detector, how CA Anomaly Detector works with related software components, and an overview of what to do to get started.

- **Installation and Upgrade** (see page 29) -- Prerequisites, software versions supported, and instructions for installation and upgrade.

- **Post-Installation Tasks** (see page 29) -- Descriptions of CA Anomaly Detector-specific tasks to perform after the installation or upgrade.

- **CA Anomaly Detector Reports** (see page 49) -- How to view and customize the pre-defined report views, as well as descriptions of each view.

- **Sensors and Troubleshooting** (see page 59) -- Descriptions of the sensors and troubleshooting tips for the alerts from each sensor.

The documentation may have been updated since its release. To be sure you have the latest documentation updates, download the bookshelf and Readme files from CA Support.

The following convention is used in this guide: Syntax and literal examples are presented in a monotype font.
Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At [http://ca.com/support](http://ca.com/support), you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at [http://ca.com/docs](http://ca.com/docs).
Contents

Chapter 1: Introduction to CA Anomaly Detector 11
Overview of CA Anomaly Detector ................................................................. 11
Features and Benefits .................................................................................. 12
  Probability Thresholds .............................................................................. 13
  Correlated Anomalies .............................................................................. 14
CA Anomaly Detector Data Collection ......................................................... 14
  Scalability .................................................................................................. 15
Get Started with CA Anomaly Detector ....................................................... 15

Chapter 2: Installation and Upgrade 17
Operating System Support ........................................................................... 17
Hardware Specifications ............................................................................... 18
Software Compatibility ............................................................................... 19
Co-Installation ............................................................................................. 20
Installation and Upgrade Prerequisites ......................................................... 21
Install CA Anomaly Detector ....................................................................... 22
Upgrade CA Anomaly Detector ................................................................... 24
Enable the Views ......................................................................................... 25
Uninstall CA Anomaly Detector .................................................................... 27

Chapter 3: Post-Installation Tasks 29
Register CA Anomaly Detector .................................................................... 29
Enable Configuration in the NFA Console ................................................... 31
Add Products to Monitor ............................................................................ 32
  Add Products for Monitor (CA Performance Center Deployment) ............... 32
  Add Products to Monitor (CA NetQoS Performance Center Deployment) ...... 33
Enable the Monitored Products' Collection Sources ..................................... 34
  Enable the Monitored Products (CA Performance Center Deployment) ......... 35
  Enable the Monitored Products (CA NetQoS Performance Center Deployment) 35
  Best Practices: Slow Harvester Rollout ..................................................... 36
Configure Firewalls ..................................................................................... 36
Sensor Configuration .................................................................................... 37
  Probability Thresholds .............................................................................. 37
  White List .................................................................................................. 38
  Absolute Thresholds ................................................................................. 38
  Configure Sensor Thresholds and Options ................................................. 39
Incoming Discard Rate ................................................................. 70
Incoming Error Rate ..................................................................... 70
Dropped Packets ........................................................................ 70
Buffer Misses ............................................................................ 70
CA Unified Communications Monitor Sensors .............................. 71
  Voice Call Fan Out ................................................................  71
  Voice Call DoS ........................................................................ 71
  Voice Server Distress .............................................................. 72
CA Application Delivery Analysis Sensors .................................... 72
  Retransmission Time .............................................................. 72
  Refused Sessions .................................................................... 73
  Packet Load ............................................................................ 73

Index .......................................................................................... 75
Chapter 1: Introduction to CA Anomaly Detector

CA Anomaly Detector gives you visibility into highly variable server and client traffic patterns. The program continually monitors baselines and rapidly analyzes the multiple flow patterns that may indicate misconfiguration, malicious attacks, or poor application delivery. CA Anomaly Detector can send alerts for as many as 27 types of potential anomalies.

This section introduces the CA Anomaly Detector product and its uses.

Overview of CA Anomaly Detector

Your network is one of your most critical resources—and one of your most vulnerable assets. Security threats affect network performance, and the reverse is also true. Whenever the network team makes even a small change, such as adding a new user, security and performance can be compromised.

CA Anomaly Detector is an important tool to help you take a proactive approach to network security and performance.

CA Anomaly Detector provides insight into customary network performance, traffic composition, and traffic volumes. The product alerts you when it detects certain types of data or patterns of anomalous behavior. Unlike other performance analysis products that are limited to one or two common traffic patterns, CA Anomaly Detector alerts you to anomalous behavior by using the powerful infrastructure that is already provided through the following allied products:

- NetFlow data distillation by CA Network Flow Analysis,
- SNMP collection by CA NetVoyant,
- TCP application performance from CA Application Delivery Analysis (SuperAgent), and
- Voice and video performance from CA Unified Communications Monitor.

By leveraging the data that your CA product suite collects, CA Anomaly Detector performs behavior analysis and security monitoring with minimal configuration and with no need for ongoing data entry.
Features and Benefits

CA Anomaly Detector goes beyond intrusion detection and other more static security tools to take a broader view of the network. The program can monitor the entire network from end to end. Instead of painstakingly applying a fixed set of rules to traffic, CA Anomaly Detector uses a set of dynamic algorithms to create and continually modify a unique profile of the monitored network. CA Anomaly Detector uses this profile in combination with efficient mathematical analysis to determine whether network traffic is anomalous.

In addition to detecting suspicious or damaged packets, CA Anomaly Detector identifies abnormally high flow and volume sources that can indicate a variety of issues. CA Anomaly Detector easily scales to create integrated monitoring and reporting across your enterprise. You receive alerts about potential problems, such as:

- Infected hosts
- Victims of infected hosts
- Unauthorized application servers
- Misconfigured servers

Operating in real time, the program identifies fan-out, SYN-only, and ICMP flood traffic that usually indicates a spreading virus, worm, or port-scanning activity. CA Anomaly Detector also alerts you to:

- Null routing and TTL-expired traffic—helping you identify poorly configured ACLs or routing loops
- Large ICMP or DNS packets that may indicate tunneling activities
- Sources of fragmented packets that double-load network devices and that can ultimately result in retransmission of TCP traffic. These symptoms can signal a frag attack. Knowledge about such sources enables you to make configuration changes that can improve network or application performance.

CA Anomaly Detector reports only the essential data you need to secure your system and stop intrusions, other security issues, and performance problems. Report views are shown in the Console for CA Performance Center or CA NetQoS Performance Center, where they contribute to an enterprise-wide perspective on network performance and health.

CA Anomaly Detector provides the following benefits:

- Trending, with per-host breakdown of anomaly sources for timely, precise troubleshooting
- Enterprise-wide correlation of anomalous behavior, broken out per host for full perspective of the behavior of key servers
- Identification of attacks before symptoms appear for prevention of downtime; quick virus isolation, and problem resolution
Features and Benefits

Chapter 1: Introduction to CA Anomaly Detector

- Accurate and complete data, collected by leveraging existing flow collection infrastructure for easy installation and configuration
- Lightweight reporting of essential data—giving you quick access to crucial information for identifying anomaly causes
- Integration with the following related products for enterprise-wide reporting on network health and application performance from a single console:
  - CA Performance Center or CA NetQoS Performance Center
  - CA Network Flow Analysis
  - CA Application Delivery Analysis (SuperAgent)
  - CA NetVoyant
  - CA Unified Communications Monitor

Probability Thresholds

CA Anomaly Detector uses a sophisticated mechanism to help avoid false positives, minimizing the number of alerts that do not correspond to true anomalies. The program uses probability threshold settings that you can customize to control the sensitivity of alert triggering. The thresholds are called probability thresholds because they are keyed to the probability that an actual anomaly has been detected.

In addition to a probability component, the threshold mechanism also relies on the following factors:

- A unique network profile that is based on statistics and the observation of typical operations
- Configurable alert levels, which are a function of the unique profile
- Statistical analysis to determine whether observed network behavior is anomalous or is within the normal range

To determine whether current data is anomalous, the detection process takes all previous data into account to create a statistics-based network profile. Using the profile as a reference, the anomaly detection process estimates and prioritizes any potentially anomalous network activity, based on percentiles and calculates the probability that the observed behavior is anomalous. The entire system is dynamic: It is updated each time it runs to ensure reliability and accuracy.
Correlated Anomalies

Correlated anomalies reduce alarm overload and help cull out false positives so you can focus on the events that are most likely to be issues. CA Anomaly Detector provides an Enterprise-Wide Correlated Anomalies view that highlights correlated anomalies. You can navigate from this view to more detailed information while you investigate. A correlated anomaly meets the following minimum requirements:

- Contains three or more anomaly instances
- Has an anomaly index of 2.0 or more
- Originates from a single device

An anomaly index of 2.0 or more indicates the presence of two or more primary anomalies or one primary anomaly and two or more secondary anomalies.

This cross-data source, temporal clustering provides actionable workflows that support a fast, proactive response to issues. For more information about the Enterprise-Wide Correlated Anomalies view, see Enterprise-Wide Correlated Anomalies (see page 53).

CA Anomaly Detector Data Collection

CA Anomaly Detector monitors the data in CA Network Flow Analysis databases, querying flow data directly from the Harvesters. If you add other products for monitoring, CA Anomaly Detector also contacts their databases to gather data for analysis. You can configure CA Anomaly Detector to monitor data from the following products:

- (Required) CA Network Flow Analysis
- (Optional) CA Application Delivery Analysis (SuperAgent)
- (Optional) CA NetVoyant
- (Optional) CA Unified Communications Monitor

CA Anomaly Detector displays information about the anomalies it finds through views in the Anomaly Detector report page, which is accessible in the Console for CA Performance Center or CA NetQoS Performance Center.
Scalability

CA Anomaly Detector is highly scalable. The program does not retain a lot of data. It collects and analyzes only the results of data analysis from the data sources that it is configured to analyze.

The MySQL database does not become overloaded easily. For example, after several weeks of running CA Anomaly Detector at a large enterprise, the database growth rate was equivalent to 4 GB per year. The typical growth rate in testing is 160,000 database rows per day.

Although you can run CA Anomaly Detector with most Harvesters, some limitations apply. In our testing, the following configurations were the maximum configurations that had acceptable performance:

- Linux-based Harvester that runs a maximum of 2 million flows per minute
- Windows-based Harvester that runs a maximum of 4 million flows per minute and does not run the Flow Cloner
- Windows-based Harvester that runs a maximum of 2 million flows per minute and runs the Flow Cloner

We support using a single instance of CA Anomaly Detector to monitor the following data sources:

- CA Network Flow Analysis: Single instance (Required)
- CA NetVoyant: Two instances (Optional)
- CA Application Delivery Analysis (SuperAgent): Two instances (Optional)
- CA Unified Communications Monitor: Two instances (Optional)

Get Started with CA Anomaly Detector

To get started with CA Anomaly Detector 9.2.0, complete the following tasks:

1. Verify that the installation server meets the following requirements and recommendations:
   - Upgrades: Verify that the existing software is supported for upgrade: Software Compatibility (see page 19)
   - Operating System (see page 17)
   - (Recommended) Hardware Specifications (see page 18).
   - Installation and Upgrade Prerequisites (see page 21).
2. Verify that CA Performance Center version 2.3.x or CA NetQoS Performance Center 6.1.205 SP2/6.1.194 is installed in your environment.

   For more information, see the CA Performance Center Installation Guide or the CA NetQoS Performance Center Installation Guide.

3. Install or upgrade to version 9.2.0 of CA Anomaly Detector and CA Network Flow Analysis:
   - Install CA Anomaly Detector (see page 22).
   - Upgrade CA Anomaly Detector (see page 24).

4. (CA PC deployment only) Enable the CA Anomaly Detector views for display in the Console: Enable the Views.

5. Register CA Anomaly Detector as a data source for CA Performance Center or CA NetQoS Performance Center: Register CA Anomaly Detector (see page 29).

6. (CA PC deployment only) Enable CA Anomaly Detector configuration in the NFA console.

7. Add CA Network Flow Analysis and any other products that you want CA Anomaly Detector to monitor: Add Products for CA Anomaly Detector to Monitor (see page 32).

8. Enable the monitored products so that their data is accessible to CA Anomaly Detector: Enable the Monitored Products (see page 34).

9. Configure the firewalls. (see page 36)

10. (Optional) Review the default sensor configurations and make any necessary changes: Configure the Sensors (see page 37).

11. (Optional) Configure targets for alerts, so that Syslog or SNMP trap messages are sent when alerts are triggered: Configure Alert Targets (see page 41).
Chapter 2: Installation and Upgrade

If you purchase hardware from CA Technologies, all components are delivered with the operating system and security settings already configured. If you purchase software only, use the topics in the CA Network Flow Analysis Installation Guide to complete basic system configuration tasks.

This section describes the configuration procedures that you perform specifically for CA Anomaly Detector.

Operating System Support

The CA Anomaly Detector installation server must be running Microsoft Windows Server 2008 R2, Standard edition on a 64-bit processor. In addition, the server must meet the following requirements:

- The most recent service pack and all important updates installed
- .NET Framework 3.5 SP1
- Java Runtime Engine (JRE) 1.6u41, which is included with the ISO files from CA Technical Support.
  We recommend that you install JRE 1.6u41, the version that is supported for CA Network Flow Analysis testing. Unsupported JRE versions may produce unexpected results.
- English language
- Minimum display resolution of 1024x768 (XGA)
- ASP.NET 2.0 installed, including COM+ network access, IIS, and ASP. ASP.NET 2.0 comes with the .NET Framework 3.5 SP1, as described in the CA Network Flow Analysis Installation Guide
- Operating system configured as described in the CA Network Flow Analysis Installation Guide, including enabling SNMP
- (Recommended) Remote Desktop Connection enabled to allow remote access by the administrator
- Server configured as described in:
  - Installation and Upgrade Prerequisites (see page 21)
  - Post-Installation Tasks (see page 29)
Notes:

- Before you begin the Windows-based tasks in this guide, log in as a user who is a member of the Administrators group.
- Install and register the Windows software.
- CA Anomaly Detector supports installation on servers with IPv4 addresses. Installation is not supported on servers with IPv6 addresses.
- We recommend that you configure a single NIC (network interface card) on the installation server.
- The requirements and recommendations that are described throughout this guide apply to both physical and virtual deployments.

Hardware Specifications

We tested the product with the following hardware configuration. Your requirements may vary depending on the characteristics and volume of interfaces, applications, and operators in your network.

Note: The recommended specifications represent the configuration of CA appliances that are currently shipping. You can run CA Anomaly Detector successfully if your configuration does not meet these specifications, although your performance may vary. You can also run CA Anomaly Detector on a configuration that exceeds these specifications.

System Specifications for CA Anomaly Detector installed stand-alone or co-installed with CA Network Flow Analysis:

- 2.26-GHz quad-core processor
- 3 GB RAM
- Three 146-GB 10,000-RPM SAS hard drives in RAID 5 configuration
- 1-Gb Ethernet port
- Partition for the C: drive that contains 12 GB for the operating system
- Partition for another drive that contains 41 GB for the product installation files and 200 GB of available space for data
Software Compatibility

CA Network Flow Analysis 9.2.0 runs with CA Anomaly Detector 9.2.0, but not with previous versions of CA Anomaly Detector. You must upgrade any previous version of CA Anomaly Detector that is currently installed.

CA Anomaly Detector requires that certain software is installed in your environment. The following table describes which software versions are supported:

<table>
<thead>
<tr>
<th>Program</th>
<th>Supported Version</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA Anomaly Detector installation that you intend to upgrade *</td>
<td>9.1.3</td>
<td>Required if upgrading</td>
</tr>
<tr>
<td>CA Performance Center</td>
<td>2.3.x</td>
<td>Required for viewing reports in a product suite that includes CA Performance Center</td>
</tr>
<tr>
<td>CA NetQoS Performance Center</td>
<td>6.1.205 SP2/6.1.194</td>
<td>Required in a product suite that includes CA NetQoS Performance Center</td>
</tr>
<tr>
<td>CA Network Flow Analysis (1 instance)</td>
<td>9.2.0</td>
<td>Required to enable AD 9.2.0 operation</td>
</tr>
<tr>
<td>CA NetVoyant (1-2 instances) **</td>
<td>7.1.108 SP6</td>
<td>Optional data source for anomaly monitoring</td>
</tr>
<tr>
<td>CA Application Delivery Analysis (SuperAgent) (1-2 instances) **</td>
<td>9.3.86</td>
<td>Optional data source for anomaly monitoring</td>
</tr>
<tr>
<td>CA Unified Communications Monitor (1-2 instances) **</td>
<td>3.6.213</td>
<td>Optional data source for anomaly monitoring</td>
</tr>
</tbody>
</table>

* If your pre-upgrade CA Anomaly Detector version is earlier than 9.1.3, upgrade to version 9.1.3 before you begin.

** These data source programs must be installed on a server that does not host CA Anomaly Detector or any CA Network Flow Analysis component.
Co-Installation

You can install CA Anomaly Detector on the same server that hosts CA Network Flow Analysis software or you can install the products on separate servers. The following table shows the supported configurations for co-installing CA Anomaly Detector with other related software.

- **Installation Order:** Follow the order shown in the table to co-install software.
- **Co-Installation with CA Network Flow Analysis:** You can install CA Anomaly Detector on a server that already hosts the CA Network Flow Analysis stand-alone deployment or the NFA console.
- **Co-Installation with CA Performance Center:** You cannot install CA Anomaly Detector on the Linux server that hosts CA Performance Center. If you already have an earlier version of CA Anomaly Detector co-installed with CA NetQoS Performance Center, you can continue to use this configuration.
- **Co-Installation with Other Data Sources:** If you have additional data source products, do not co-install them with CA Anomaly Detector or CA Network Flow Analysis.

<table>
<thead>
<tr>
<th>Components Installed on a Single Server</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA Anomaly Detector (AD) with no other related software component</td>
<td>Yes</td>
</tr>
<tr>
<td>NFA stand-alone (Harvester + NFA console software) + AD</td>
<td>Yes</td>
</tr>
<tr>
<td>NFA console + AD</td>
<td>Yes</td>
</tr>
<tr>
<td>NPC + NFA stand-alone (Harvester + NFA console) + AD</td>
<td>Yes</td>
</tr>
<tr>
<td>NPC + NFA console + AD</td>
<td>Yes</td>
</tr>
<tr>
<td>NPC + Event Manager * + NFA stand-alone (Harvester + NFA console) + AD</td>
<td>Yes</td>
</tr>
<tr>
<td>NPC + Event Manager * + NFA console + AD</td>
<td>Yes</td>
</tr>
<tr>
<td>CA PC + AD</td>
<td>No</td>
</tr>
<tr>
<td>ADA (SA), UCM, or NetVoyant + AD</td>
<td>No</td>
</tr>
</tbody>
</table>

* If the Event Manager is co-installed with CA Network Flow Analysis, the trap receiver in CA Network Flow Analysis is disabled automatically. In a CA Performance Center environment, the Event Manager is not a separate program and this behavior is not applicable.
Installation and Upgrade Prerequisites

Before you install or upgrade the software, perform the following tasks:

Download the Installation or Upgrade File

Download the installation and upgrade files from CA Technical Support:
1. Download the ISO file, which contains the ADSetup9.2.0.exe file—the installation or upgrade program for CA Anomaly Detector.
2. Burn the ISO file to a CD-ROM or DVD-ROM or extract the contents of the ISO file by using an ISO image software application.
3. Copy the ADSetup9.2.0.exe file to the CA Anomaly Detector installation server.
   Copy the file to the installation server whether you plan to install the software locally or remotely.

Co-Installation

If you are co-installing CA Anomaly Detector on a server with CA Network Flow Analysis, complete the CA Network Flow Analysis installation or upgrade before you install CA Anomaly Detector.

You can use the same server to install CA Anomaly Detector along with a stand-alone CA Network Flow Analysis deployment or with the NFA console component in a distributed deployment. Co-installation options are listed in Co-Installation (see page 20).

Upgrade: Back Up the Database

(Recommended) Back up the nsas database before you start an upgrade:
1. Stop the CA Anomaly Detector-related services:
   a. Click Start, Programs, Administrative Tools, Services.
   b. Stop the following services:
      ■ CA NFA Host Resolver Service
      ■ CA NFA Hunter Tracker Service
      ■ NetQoS Mysql51
2. Copy the following database to a remote location:
   <install_path>\MySql51\data\nsas
3. Restart the services that you stopped in step 1b.
General Prerequisites and Recommendations

- (Recommended) Review the topology of your network. For example, create a diagram of your network and its connections to ensure that you monitor the correct devices for the traffic that interests you.

- (Recommended) Collect information about the CA Performance Center or CA NetQoS Performance Center deployment that includes the locations and IP addresses for all related components.

- Verify that you have access to the servers that host CA Performance Center or CA NetQoS Performance Center and any products that you want to monitor. Make sure that all of the products are configured and functioning properly, including flow configuration on the routers.

- Prepare the server as described in the CA Network Flow Analysis Installation Guide or Upgrade Guide.

- Stop other programs from running during the installation or upgrade.

- Restart all servers to ensure that all operating system patches are applied.

- Ensure that no one else is logged in to the server during the installation or upgrade.

Install CA Anomaly Detector

Complete the steps in this topic to install CA Anomaly Detector on a Windows server or virtual machine.

If the CA Anomaly Detector and any related software components are co-installed, install the software in the order described in Co-Installation (see page 20). The installation steps are written with the expectation that you have already installed any related products that will be co-located with CA Anomaly Detector.

Follow these steps:

1. Log in to the CA Anomaly Detector server as a user who is a member of the Administrators group.

2. Verify that the ISO file is downloaded (see page 21). The ISO file contains the ADSetup9.2.0.exe file—the installation or upgrade program for CA Anomaly Detector.

   Copy the ADSetup9.2.0.exe file to the CA Anomaly Detector installation server, even if you plan to install the software remotely.

3. If the server will host any CA Network Flow Analysis software, install or upgrade the other software before you proceed (see page 20).


   The installation program opens.
5. Verify that English is selected, then click OK.
   The Welcome screen opens.

6. Click Next.
   The Pre-Installation Summary screen opens.

7. Review the information, then click Install.
   The Choose Install Folder screen opens.

8. (Optional) Specify a custom installation location:
   a. Click Choose in the Choose Install Folder screen to change the installation location.
      Use the same installation folder for CA Anomaly Detector and the NFA console or stand-alone installation. The default location is C:\CA\NFA. We recommend that you install CA Anomaly Detector on a non-system drive.
   b. Click Next when the installation path setting is correct.
      The Installing AD screen opens. When the installation is complete, the Install Complete screen opens and verifies that the installation was successful.

9. (Optional) If errors occurred during the installation, see the following log for details:
   <install_path>\AD_Install_<timestamp>

10. Click Done in the Install Complete screen.
    The installation program closes.

11. (Optional) Verify that the services are running:
    a. Click Start, Programs, Administrative Tools, Services.
    b. Verify that the AD-related services have the status Started:
       – CA NFA Host Resolver Service
       – CA NFA Hunter Tracker Service
       – NetQoS Mysql51

**Next:** Complete the post installation tasks (see page 29).
Upgrade CA Anomaly Detector

Complete the steps in this topic to upgrade CA Anomaly Detector on a Windows server or virtual machine.

If the CA Anomaly Detector and any related software components are co-installed, upgrade the software in the order described in Co-installation (see page 20). The upgrade steps are written with the expectation that you have already upgraded any related products that will be co-located with CA Anomaly Detector.

Follow these steps:

1. Log in as a user who is a member of the Administrators group.
2. Verify that the ISO file is downloaded (see page 21). The ISO file contains the ADSetup9.2.0.exe file—the Installation or upgrade program for CA Anomaly Detector.
   Copy the ADSetup9.2.0.exe file to the CA Anomaly Detector installation server, even if you plan to install the software remotely.
3. If the server will host any CA Network Flow Analysis software, install or upgrade the other software before you proceed (see page 20).
   The installation program opens.
5. Verify that English is selected, then click OK.
   The Prior Installation Detected message opens.
6. Review the information, then click OK.
   If the existing software version is not supported for upgrade, upgrade to the supported version.
   If the existing version is supported for upgrade, the Welcome screen opens.
7. Click Next.
   The Pre-Installation Summary screen opens.
8. Review the information, then click Install.
   The Installing AD screen opens. When the upgrade is complete, the Install Complete screen opens.
9. (Optional) If errors occurred during the upgrade, see the following logs for details:
   - General installation log: <install_path>\AD_Install_<timestamp>
   - Upgrade log: <install_path>\migrator\migrator.log
10. Click Done in the Install Complete screen.
   The program closes.
11. (Optional) Verify that the services are running:
   a. Click Start, Programs, Administrative Tools, Services.
   b. Verify that the AD-related services have the status Started:
      - CA NFA Host Resolver Service
      - CA NFA Hunter Tracker Service
      - NetQoS Mysql51

12. Verify that the software is upgraded to the correct version: To display the revision history and verify the current software version, complete the following substeps:
   a. Open a Command Prompt window
   b. Start MySQL by entering the following command:
      mysql
   c. Display the revision history by entering the following command:
      select * from revision_history

**Next:** Complete the post installation tasks (see page 29).

---

**Enable the Views**

If you plan to use CA Anomaly Detector with CA Performance Center, you must enable the views before you can display them for the first time. This topic describes how to enable the CA Anomaly Detector for display in the CA Performance Center Console.

**Note:** If you plan to use CA Anomaly Detector with CA NetQoS Performance Center, the views are already enabled. Skip this task and go to the post installation tasks (see page 29).

The views become available and useful when the following conditions are met:

- (Operating with CA Performance Center) The views are enabled as described in this topic.
- CA Anomaly Detector is registered with CA Performance Center (see page 29).

**Note:** The steps in this topic are written with the expectation that you have already installed or upgraded CA Network Flow Analysis and CA Performance Center.
Follow these steps:

1. Copy the required files from the CA Anomaly Detector server to the CA Performance Center server. For example, you can use SCP to copy the files into the target directory in a single operation.
   a. If you are performing the copy from the CA Performance Center server, log in as root or log in to an account that has sudo privileges.
   b. Copy the following two files from the NQAD/setup directory on the CA Anomaly Detector server:
      ■ anomalydetector_capc_addins.tar.gz: Definitions for the CA Anomaly Detector views
      ■ anomalydetector_capc_integration.sh: Script to unpack and load the view definitions
   c. Put the two .tar.gz and .sh files in the following directory on the CA Performance Center server: `<install_path>/PerformanceCenter/SQL/plugins`
      where
      `<install_path>` is the root installation directory for CA Performance Center. The default root path is `/opt/CA/`.

2. Verify that the .tar.gz and .sh files are in the correct location:
   a. Navigate to the plugins directory:
      ```
      cd `<install_path>/PerformanceCenter/SQL/plugins`
      ```
      where
      `<install_path>` is the root installation directory for CA Performance Center. The default root path is `/opt/CA/`.
   b. List the contents of the plugin directory:
      ```
      ls -l
      ```
      The return text should include the two files:
      anomalydetector_capc_addins.tar.gz
      anomalydetector_capc_integration.sh

3. Prepare the script file:
   a. Make the script user-executable:
      ```
      chmod u+x anomalydetector_capc_integration.sh
      ```
   b. (Optional) Display the permissions to verify that the file is executable:
      ```
      ls -al
      ```

4. Run the script:
   ```
   ./anomalydetector_capc_integration.sh
   ```
   The script unpacks the .tar.gz file, loads the view definitions into CA Performance Center, then restarts two services to initiate the change. The following phrase in the return text reports that the view definitions have been uploaded:
   Completed loading package; com.ca.im.plugin.anomalydetector
The last section of the return text reports the Performance Center and Performance Center Console services being stopped and restarted.

The views now are enabled. As soon as CA Anomaly Detector is registered and begins monitoring data, the views are available in the CA Performance Center Console.

Next: Complete the post installation tasks (see page 29).

Uninstall CA Anomaly Detector

CA Anomaly Detector 9.2.0 includes an option to uninstall the product, which you can use after an installation or upgrade.

You should be able to install and uninstall the software once or twice without any problem. If you have ongoing problems, contact CA Support rather than continue to install and uninstall the software.

As an alternative to using the Uninstaller, you can uninstall the software from the Control Panel. The program is listed as AD in the Windows Add or Remove Programs or Programs and Features window.

Follow these steps:
1. Log in as a user who is a member of the Administrators group.
2. Perform the following preliminary steps:
   ■ Open the Services window and verify that the NetQoS Mysql51 service is running. If the service is not running, start it.
   ■ If the installation server is also used to host CA Performance Center or CA Network Flow Analysis, back up your data and configuration files, as described in the CA Network Flow Analysis Administrator Guide and CA Performance Center Installation Guide.
   ■ Exit from all applications--with no exceptions.
3. If you plan to uninstall both CA Anomaly Detector and CA Network Flow Analysis from the same server, uninstall the CA Network Flow Analysis software first, as described in the CA Network Flow Analysis Installation Guide.
4. Start the Uninstaller for CA Anomaly Detector: Double-click the AD_Uninstaller.exe file in the following location: <install_path>\Uninstall\NQAD.
   The Uninstall window opens.
5. Click Next if you are ready to proceed.
   As soon as you click Next, the Cancel button is disabled. The Uninstaller has no Undo option: Once you begin uninstalling the software, you cannot restore the deleted files automatically.
The uninstall program removes the program and data files, including the following CA Network Flow Analysis and MySQL elements:

- Registry entries
- Shortcuts, links, and aliases
- Most files
- Some directories

As the uninstaller runs, the screen displays progress messages. When the process is complete, the screen displays a list of the directories and files that were not deleted.

**Note:** Leave the file system undisturbed while uninstallation is in progress. Do not attempt to view the progress in Windows Explorer, for example.

Once the program finishes, the Uninstall Complete screen opens.

6. Click Done to close the program.

   Wait a few minutes to allow the helper process to finish the final cleanup.

   Some files are not deleted until this phase is finished. Once the final cleanup is finished, the Uninstaller itself is deleted.

**Notes:**

- The uninstallation log is at: `<install_path>\AD_Uninstall_<timestamp>.txt`.
- You may want to manually delete any remaining CA Anomaly Detector directories, files, and services. If other related software is installed on the server, do not delete the MySQL service.
- If you make an unsuccessful attempt to reinstall the software, contact CA Support.
Chapter 3: Post-Installation Tasks

If you purchase hardware from CA Technologies, all components are delivered with the operating system and security settings already configured. If you purchase software only, use the topics in the CA Network Flow Analysis Installation Guide to complete basic system configuration tasks.

This section describes the configuration procedures that you perform specifically for CA Anomaly Detector. The tasks described here assume that you have completed the steps for pre-installation and installation or upgrade.

Be prepared to configure the firewalls to allow communication between CA Anomaly Detector and other components. For information about configuring firewalls, see Configure Firewalls (see page 36).

This section contains the following topics:
- Register CA Anomaly Detector (see page 29)
- Enable Configuration in the NFA Console (see page 31)
- Add Products to Monitor (see page 32)
- Enable the Monitored Products' Collection Sources (see page 34)
- Configure Firewalls (see page 36)
- Sensor Configuration (see page 37)
- Configure Alert Targets (see page 41)

Register CA Anomaly Detector

To display CA Anomaly Detector data in reports, you must add CA Anomaly Detector as a data source to CA Performance Center or CA NetQoS Performance Center.

Follow these steps:

1. Log in to the CA Performance Center Console or CA NetQoS Performance Center Console as a user with administrator privileges.
2. Select Admin, Data Sources.
   The page for managing data sources opens:
   - Manage Data Sources page (CA PC)
   - Data Source List page (NPC)
3. Click Add (CA PC) or New (NPC).
   The dialog for adding a data source opens.
4. Specify values for the following options:
   - **Source Type**: Select Anomaly Detector from the list. If it is not listed, verify that you have performed the steps in *Enable the Views* (see page 25).
     All related products and selected third-party integrations are listed in the Source Type list regardless of whether they are installed in your environment. If a data source type is not listed, check to see if you have already registered the maximum number of data sources for that type.
   - **Status**: Select Enabled.
   - **Host Name**: Enter the IP address or name of the server that hosts the CA Anomaly Detector software.
   - **Protocol**: Select the protocol to use for contacting CA Anomaly Detector.
     Select https if your network uses SSL for communications. If you select the https option, verify that you have configured the system correctly for https access. For more information, see the *Single Sign-on User Guide*.
   - **Port**: Enter the Port for CA Anomaly Detector.
     The port you specify depends on the protocol you select. The recommended port for the http protocol is 80. The recommended port for the https protocol is 443. If you plan to use SSL for communication with CA Performance Center or CA NetQoS Performance Center, see the *Single Sign-on User Guide*.
   - **Web Console**: Confirm whether the Web Console address is the same as the Host Name. If it is different, click the "Same as above" check box to provide the Web Console information.
     The default setting is for the Web Console address to be the same as the Host Name.
   - **Web Console**: Same as Data Source: Confirm whether the same IP address, port, and protocol are used for the Web Console as for the host server. If any of the values are different, clear the "Same as above" check box to provide the Web Console information.
   - **Display Name**: (Optional) Enter a user-friendly name for the data source. This name is shown on the Admin menu under Product Settings.
     If you do not specify a name, a default name is generated automatically. The default name consists of the data source type combined with the host name. For example, you can specify AnomalyDetector_London as the Display Name in place of a default name like AnomalyDetector@xxx.x.x.xx.
   - **Enabled**: Select the Enabled check box.

5. **Click Test** to verify that the connection to CA Anomaly Detector works.
   If the connection fails, verify that the server name or IP address is accurate for the source type. If the connection fails again, contact *CA Support*. 
6. Click Save when the settings are complete and the connection test has succeeded. You return to the main page, which shows CA Anomaly Detector in the list of data sources.

**Enable Configuration in the NFA Console**

If your deployment includes CA Performance Center, you use the NFA console to perform administration for CA Anomaly Detector. Skip this task if your deployment includes CA NetQoS Performance Center.

*Follow these steps:*

1. Log in to the NFA console as a user with administrator privileges, if you are not already logged in.
2. Click Administration.
   The Administration page opens.
3. Click Anomaly Detector in the menu pane.
   The Anomaly Detector page opens with the View Monitored Products page displayed.
4. Click Add/Edit Anomaly Detector.
   The Add/Edit Anomaly Detector dialog opens.
5. Select values for the following options:
   - **Protocol:** Select the protocol to use for contacting CA Anomaly Detector. Select https if your network uses SSL for communications. If you select the https option, verify that you have configured the system correctly for https access. For more information, see the *Single Sign-on User Guide*.
   - **IP Address:** Enter the IP address of the server that hosts the CA Anomaly Detector software that you want to administer.
6. Click Save.
   You return to the Anomaly Detector page. The configuration options are now enabled, so you can add products for CA Anomaly Detector to monitor (see page 32).
Add Products to Monitor

The next step is to add CA Network Flow Analysis as a monitored product for CA Anomaly Detector. You also have the option to add more products that CA Anomaly Detector can monitor for anomalies. This task is described in the following topics:

- Add Products to Monitor (CA Performance Center Deployment) (see page 32)
- Add Products to Monitor (CA NetQoS Performance Center Deployment) (see page 33)

Add Products for Monitor (CA Performance Center Deployment)

You must add an instance of CA Network Flow Analysis for CA Anomaly Detector to monitor. You also have the option to add any other products that you want to monitor for anomalies. This topic describes how to complete this task in a CA Performance Center deployment.

Follow these steps:

1. Log in to the CA Performance Center Console as a user with administrator privileges, if you are not already logged in.

2. Click Admin, Data Source Settings: Name of the CA Anomaly Detector instance that you want to configure.

   The Anomaly Detector page opens in the NFA console.

3. Click Add on right bottom corner of the Anomaly Detector page (View Monitored Products tab).

   The Add Monitored Product dialog opens.

4. Add a CA Network Flow Analysis instance as a monitored product: Specify values for the following options:

   - Type: Select the product name from the list: CA Network Flow Analysis.
     
     If CA Network Flow Analysis is not listed, verify that you have not already registered a CA Network Flow Analysis instance as a monitored product. You can register only one instance of CA Network Flow Analysis to a single instance of CA Anomaly Detector.

   - IP Address: Enter the IP address of the CA Network Flow Analysis server.

5. Click Save.

You return to the Anomaly Detector page, which shows the instance of CA Network Flow Analysis that you added. All of the currently configured Harvesters are added as potential data collectors on the Collection Sources tab, but the Harvesters are not enabled at this point.
6. (Optional) Add another monitored product: Repeat the previous two steps until you have added all of the monitored products that you need.

- If you add CA NetVoyant Enterprise, enter the IP address of the individual pollers instead of the NetVoyant Master Console.

- You can monitor multiple instances of some products, as listed in Software Compatibility (see page 19).

The list of monitored products page reflects your changes. CA Anomaly Detector contacts the product to add the collection sources to the View Collection Sources tab.

Add Products to Monitor (CA NetQoS Performance Center Deployment)

You must add an instance of CA Network Flow Analysis for CA Anomaly Detector to monitor. You also have the option to add any other products that you want to monitor for anomalies. This topic describes how to complete this task in a CA NetQoS Performance Center deployment.

Follow these steps:

1. Log in to the CA NetQoS Performance Center Console as a user with administrator privileges, if you are not already logged in.

2. Click Admin, Product Settings: Name of the CA Anomaly Detector instance.

   The Monitored Products page opens in the CA NetQoS Performance Center Console with the View Monitored Products tab displayed.

3. Click New on the Monitored Products page.

   The New Monitored Product page opens.

4. Add CA Network Flow Analysis as a monitored product: Specify values for the following options:

   - Type: Select the product name from the list: ReporterAnalyzer.
     
     If ReporterAnalyzer is not listed, verify that you have not already registered a CA Network Flow Analysis instance as a monitored product. You can register only one instance of CA Network Flow Analysis to a single instance of CA Anomaly Detector.

   - IP Address: Enter the IP address of the CA Network Flow Analysis server.

5. Click Save.

   You return to the Monitored Products page, which shows the instance of CA Network Flow Analysis that you added. All of the currently configured Harvesters are added as potential data collectors on the Collection Sources tab, but the Harvesters are not enabled at this point.
Enable the Monitored Products' Collection Sources

6. (Optional) Add another monitored product: Repeat the previous two steps until you have added all of the monitored products that you need.
   - If you add CA NetVoyant Enterprise, enter the IP address of the individual pollers instead of the NetVoyant Master Console.
   - You can monitor multiple instances of some products, as listed in Software Compatibility (see page 19).

   The list of monitored products page reflects your changes. CA Anomaly Detector contacts the product to add the collection sources to the View Collection Sources tab.

Enable the Monitored Products' Collection Sources

After you add products for CA Anomaly Detector to monitor, enable the products so that monitoring can begin.

This task is described in the following topics:

- Enable the Monitored Products (CA Performance Center Deployment) (see page 35)
- Enable the Monitored Products (CA NetQoS Performance Center Deployment) (see page 35)

When you add CA Network Flow Analysis as a monitored product, the Harvesters that are configured with the CA Network Flow Analysis instance are added automatically as possible data collection sources. You can enable as many or as few Harvesters as you need. Special considerations apply when you enable Harvesters, as described in Best Practices: Slow Harvester Rollout (see page 36).

   The product databases are the collection sources for the CA Application Delivery Analysis (SuperAgent), CA NetVoyant, and CA Unified Communications Monitor products.
Enable the Monitored Products (CA Performance Center Deployment)

This topic describes how to enable the monitored products for CA Anomaly Detector in a deployment that includes CA Performance Center. As soon as the products are enabled, CA Anomaly Detector can begin monitoring their data for anomalies.

Follow these steps:

1. Log in to the NFA console as a user with administrator privileges, if you are not already logged in.
2. Display the list of collection sources for CA Anomaly Detector:
   a. Select Administration.
      The Administration page opens.
   b. Click Anomaly Detector in the menu pane.
      The Anomaly Detector page opens.
   c. Click the View Collection Sources tab.
      The collection sources are displayed in a table.
3. Select the name of each collection source that you want to enable.
   Note: Special considerations apply when you enable Harvesters, as described in Best Practices: Slow Harvester Rollout (see page 36).
4. Click Enable.
   CA Anomaly Detector begins to monitor the selected collection sources. The source shows as Enabled in the State column.

Enable the Monitored Products (CA NetQoS Performance Center Deployment)

This topic describes how to enable the monitored products for CA Anomaly Detector in a deployment that includes CA NetQoS Performance Center. As soon as the products are enabled, CA Anomaly Detector can begin monitoring their data for anomalies.

Follow these steps:

1. Log in to the CA NetQoS Performance Center Console as a user with administrator privileges, if you are not already logged in.
2. Select Admin, Product Sources: Name of the Anomaly Detector instance.
   The Monitored Products page opens with the View Monitored Products page displayed.
3. Click the View Collection Sources tab.
   The collection sources are displayed in a table.
4. Select a collection source that you want to enable.

   **Note:** Special considerations apply when you enable Harvesters, as described in the **Best Practices: Slow Harvester Rollout** (see page 36).

5. Click Edit.

   The Edit Collection Source dialog opens.

6. Select the State check box to enable the collection source.

7. Click Save.

   You return to the list of collection sources. The State value is updated to reflect your change. CA Anomaly Detector begins to monitor the collection source.

**Best Practices: Slow Harvester Rollout**

When you enable a Harvester for monitoring, performance demands for the Harvester increase. CA Anomaly Detector queries the Harvesters for flow data every 15 minutes. The Harvesters in turn search the flow archive—a cache of raw flow data—for the requested data. Searches can include millions of flows.

We strongly recommend that you enable Harvesters gradually. For example, enable two or three Harvesters, wait 15 minutes, then check the query time for the Harvesters on the Collection Sources page. Query times should be less than 15 minutes.

To check Harvester errors in the NFA console, open the NFA console, click Administration, and click the Harvester icon.

The program may take as long as 15 minutes to query newly added Harvesters. The current reporting interval must be completed before the program can query the newly added Harvesters.

You can add a maximum of 10 Harvesters to a single instance of CA Anomaly Detector.

**Configure Firewalls**

Modify your firewall as needed to enable CA Anomaly Detector and the Harvesters to communicate. In addition, review your Access Control Lists (ACLs) and make any changes that are needed.

The following ports are used by default for communication:

- **CA Anomaly Detector server to the Harvester ports:**
  - TCP 3307 (MySQL server)
  - UDP 161 (Watchdog services)
Sensor Configuration

Most sensors are enabled by default, even sensors that do not have a collection source. The inactive sensors have no effect on data analysis until the appropriate data source is added. If you disable inactive sensors, remember to manually enable them again when you add the corresponding collection source.

Probability Thresholds

The probability threshold is a sensitivity setting that increases or decreases the likelihood that the sensor will send out alerts when it detects a monitored behavior. For more information about probability thresholds, see Probability Thresholds (see page 13).

The default threshold for all sensors is 90% probability. As you raise the probability threshold, fewer alerts are likely to be sent and it is more likely that real issues triggered the alerts.

<table>
<thead>
<tr>
<th>Probability Threshold</th>
<th>Number of Anomalies Reported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower</td>
<td>More</td>
</tr>
<tr>
<td>Higher</td>
<td>Less</td>
</tr>
</tbody>
</table>

If you monitor a device that has a known issue, you may want to raise the probability threshold to prevent false alerts. A lower probability setting may be better for a critical item that is fairly stable, so that you are notified about issues early.
White List

Use the White List to exclude servers from monitoring and from reports when you edit a sensor configuration (see page 39). The White List typically consists of hosts that are known to be safe.

Do not add a host to the White List if the host is important and the host may be vulnerable to attack. For example, do not add DNS servers to the White List even though these servers may generate spurious anomalies. As CA Anomaly Detector continues to gather data about typical behavior, it should create fewer spurious anomalies for hosts like DNS servers.

Absolute Thresholds

You have the option to set an absolute threshold so that alerts are generated when the threshold is violated, provided that alerts are enabled. Absolute thresholds are applied before probability thresholds.

The following table lists the sensors and units of measure for absolute thresholds.

<table>
<thead>
<tr>
<th>Sensor</th>
<th>Looks For:</th>
<th>Unit of Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Misses</td>
<td>Pattern in buffer misses</td>
<td>buffer misses</td>
</tr>
<tr>
<td>Congestion Sources</td>
<td>Sources of overloading based on ICMP Source Quench</td>
<td>flows</td>
</tr>
<tr>
<td>Destination Unreachable Sources</td>
<td>High-volume sources of network, host, or port unreachable messages</td>
<td>host or port unreachable messages</td>
</tr>
<tr>
<td>Dropped Packets</td>
<td>Pattern in queue drops</td>
<td>dropped packets</td>
</tr>
<tr>
<td>Fragmented Packet Sources</td>
<td>Large sources of fragmented packets</td>
<td>fragmented packets</td>
</tr>
<tr>
<td>Frags And Loss Sources</td>
<td>Sources of fragmentation and packet loss</td>
<td>flows</td>
</tr>
<tr>
<td>High and Variable Vol-In</td>
<td>Highest-volume and variability destinations</td>
<td>bytes in</td>
</tr>
<tr>
<td>High and Variable Vol-Out</td>
<td>Highest-volume and variability sources</td>
<td>bytes out</td>
</tr>
<tr>
<td>High Flow Sources</td>
<td>Top sources of data flows</td>
<td>flows</td>
</tr>
<tr>
<td>High Packet Fan Out</td>
<td>Sources of the largest fan-out traffic patterns</td>
<td>destination hosts</td>
</tr>
<tr>
<td>Incoming Discard Rate</td>
<td>Pattern in incoming discards</td>
<td>discard rate</td>
</tr>
<tr>
<td>Incoming Error Rate</td>
<td>Pattern in incoming errors</td>
<td>error rate</td>
</tr>
<tr>
<td>Large DNS Packet Sources</td>
<td>Large sources of DNS packets that are larger than normal</td>
<td>flows</td>
</tr>
</tbody>
</table>
### Sensor Configuration

<table>
<thead>
<tr>
<th>Sensor</th>
<th>Looks For:</th>
<th>Unit of Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large ICMP Packet Sources</td>
<td>Large sources of ICMP packets that are larger than normal</td>
<td>flows</td>
</tr>
<tr>
<td>Non-local Sources</td>
<td>Top sources of non-local traffic</td>
<td>non-local traffic</td>
</tr>
<tr>
<td>Packet Load</td>
<td>Pattern in bytes per packet to server</td>
<td>bytes per packet</td>
</tr>
<tr>
<td>Previously Null Routed Srcs</td>
<td>Hosts with high volumes of traffic that is no longer null-routed</td>
<td>flows</td>
</tr>
<tr>
<td>Refused Sessions</td>
<td>Pattern in refused sessions</td>
<td>percent</td>
</tr>
<tr>
<td>Retransmission Time</td>
<td>Pattern in retransmissions</td>
<td>seconds</td>
</tr>
<tr>
<td>RST-Only Sources</td>
<td>Highest-volume sources of RST-only flows</td>
<td>flows</td>
</tr>
<tr>
<td>SYN/RST-Only Packet Srcs</td>
<td>Highest-volume sources of SYN/RST-only flows</td>
<td>flows</td>
</tr>
<tr>
<td>SYN-Only Packet Sources</td>
<td>Highest-volume sources of SYN-only flows</td>
<td>flows</td>
</tr>
<tr>
<td>TTL Expired Sources</td>
<td>High-volume sources of TTL expired packets</td>
<td>flows</td>
</tr>
<tr>
<td>Voice Call DoS</td>
<td>DoS in voice calls</td>
<td>calls per minute</td>
</tr>
<tr>
<td>Voice Call Fan Out</td>
<td>Pattern in fan-out of voice calls</td>
<td>call ratio</td>
</tr>
<tr>
<td>Voice Server Distress</td>
<td>Call Server Distress</td>
<td>Volume Weighted Error Ratio</td>
</tr>
</tbody>
</table>

### Configure Sensor Thresholds and Options

You can configure sensors to have different probability thresholds and to include the following optional features: absolute thresholds, alerts, and host exclusions.

**Follow these steps:**

1. Display the Data Source List page, if it is not open already:
   
a. Log in to the CA Performance Center Console or CA NetQoS Performance Center Console as a user with administrator privileges, if you are not already logged in.

   b. Select Admin, Data Sources.

      The page for managing data sources opens:

      - Manage Data Sources page (CA Performance Center)
      - Data Source List page (CA NetQoS Performance Center)

2. Click the name of the CA Anomaly Detector instance that you want to configure.

   The Monitored Products page opens.
3. Click View Sensors.

The Sensors page opens and displays the first group of sensors. Click the page numbers at the bottom to page through the sensor list.

4. Double-click the row for the sensor that you want to edit.

The Edit Sensor page opens.

5. Edit any of the following options that you want to change:

   ■ Probability Threshold: (Optional) Change the numeric value to change the probability threshold.
   
   The probability threshold determines the likelihood that the sensor will send out alerts when it detects the behavior it monitors. For more information about probability thresholds, see Probability Thresholds (see page 13).

   ■ Absolute Threshold: (Optional) Enter a numeric value to create an absolute threshold.
   
   Enter the absolute threshold value based on the unit of measure for the sensor. An absolute threshold signals an anomaly if the threshold is exceeded. The anomaly triggers an alert if you select the Alert option. For information about the units of measure for absolute thresholds, see Absolute Thresholds (see page 38).

   Absolute thresholds are applied before probability thresholds. The program continues to calculate the percentiles for the host/sensor combination even if you set an absolute threshold. These calculations are used if the absolute threshold is removed later or if the probability threshold is exceeded first. An anomaly is created if either threshold is exceeded.

   ■ Alert: (Optional) Select the Alert check box to send alerts when the probability or absolute threshold is exceeded.
   
   This option is enabled for most sensors by default. The exceptions are sensors that are most useful when you monitor correlated anomalies (that is, when alerts are triggered for multiple types of sensors).

   For information about setting up Syslog or SNMP trap alert targets, see Configure Alert Targets (see page 41).

   ■ State: Select the State box to enable the sensor or clear the check box to disable the sensor.

   ■ IP address: (Optional) Enter a host IP address and click Add to add the host to the White List, so the host is excluded from anomaly reporting:
   
   The IP address appears in the White List field.

   ■ White List: (Optional) Highlight a host in the White List field and click Remove to delete the host from the White List.

6. Close the Edit Sensor page: Click Save or Cancel.

You return to the Sensors page, which reflects any changes that you saved.
Configure Alert Targets

Alerts are enabled for most sensors by default. The anomalies that result are displayed on the Anomaly Detector reports page in the Performance Center Console. You can also configure the alerts to trigger Syslog messages, SNMP trap messages, or both.

- **Syslog Alerts** (see page 41)
- **SNMP Trap Alerts** (see page 46)

Syslog Alerts

Alerts are enabled for most sensors by default, but messages for the alerts are not sent to a Syslog server unless you configure the target for Syslog messages (see page 41).

About Syslog Alerting

The alerting feature lets you specify parameters for alerts to be sent to a CEF-compliant Syslog server. Syslog is a standard protocol for handling log messages in a heterogeneous environment. A Syslog server that is running a syslog daemon collects log messages, and sometimes filters and processes the messages. The log messages pass to the Syslog server from devices on the network such as routers and switches.

Each syslog message corresponds to a single alert for an anomaly cluster or for a basic anomaly. An anomaly cluster alert contains details about the basic anomalies in the cluster. The details can give the appearance of multiple entries in the message.

The alert format complies with the Common Event Format (CEF) standard. The message type formats are described in the following topics:

- **Example of a Basic Anomaly Message** (see page 43)
- **Example of an Anomaly Cluster Message** (see page 44)

Configure the Target for Syslog Messages

Configure Syslog alerting to identify a target Syslog server that will receive messages when sensors report a threshold violation. If Syslog alerting is not configured, the alerts that sensors generate may appear on the Anomaly Detector report page, but no messages are sent to report the alerts.

Prerequisites for Syslog Alerting:

- Set up a Syslog server.
- Configure a service on the Syslog server to read syslog messages from CA Anomaly Detector.
Configure Alert Targets

Follow these steps:

1. Display the Data Source List page:
   a. Log in to the CA Performance Center Console or CA NetQoS Performance Center Console as a user with administrator privileges, if you are not already logged in.
   b. Select Admin, Data Sources.
      The page for managing data sources opens:
      – Manage Data Sources page (CA Performance Center)
      – Data Source List page (CA NetQoS Performance Center)

2. Click the name of the CA Anomaly Detector instance that you want to configure.
   The Monitored Products page opens.

3. Click View Alert Targets.
   The Alert Targets page opens.

4. Double-click the syslogging row.
   The Edit Alert Target page opens.

5. Specify the Target: Enter the IP address or DNS hostname of the system that will receive the Syslog information.

6. Select one or both of the following options to enable the alert:
   ■ Basic State: Send alerts whenever any single sensor detects an anomaly that crosses a threshold.
   ■ Cluster State: Send alerts only when the requirements for a correlated anomaly are met.
      This is the recommended setting for first-time use of CA Anomaly Detector. If you have already disabled alerts for the sensors that are irrelevant to you, the recommended setting is Basic State. For more information about these recommendations, see the Best Practice note that follows.

   For information about what constitutes a correlated anomaly, see Correlated Anomalies on page 7 (see page 14).

7. Click Save.
   You return to the Alert Targets page, which reflects any changes you saved.
Best Practices:

Alerts are enabled for most sensors by default so that when you start using CA Anomaly Detector, you can review a wide range of anomalous behaviors with a minimum of configuration. If you use Syslog alerting and you select the Basic State option at this stage, you may see so many anomalies that you cannot determine which ones are significant.

If you begin by selecting the Cluster State option for alert targets, the anomalies you see are much more likely to be significant. You can quickly determine which sensors are useful to you. At this point you can disable alerts for the other sensors, then start using the Basic State option. This produces an expanded set of results for the anomaly types that interest you. The anomalies from the other sensors are eliminated.

To explore all of the potential anomaly cluster types, you may want to enable any disabled sensors. In this case, use the Cluster State option.

Example of a Basic Anomaly Message

A Syslog Basic Anomaly message reports an alert for a single anomaly instance. The following example shows the message fields for a Basic Anomaly message:

```
02-12-2009 17:51:42 Local0.Alert 10.0.23.138 Feb 12 17:51:42 sk23-138 CEF:0|NetQoS|AnomalyDetector|2.0.12.1|23|Frags and Loss Sources|5|src=XXX.XX.XXX start=2/12/2009 5:36:00 PM msg=metric 2 anomaly probability 1%. A router close to the issue (for further analysis or ACL) is XX.XXX.XX.XXX and IN interface is 2130925934
```

The sixth CEF field, the msg=metric field, identifies the sensor type that detected the violation. The sensor type in the example is Frags and Loss Sources. The main body of the CA Anomaly Detector information follows msg=.

```
msg=metric METRICVALUE anomaly probability PROBVALUE%. OptionalROUTERINFOVALUE
```

where:

**METRICVALUE**

Actual value, expressed in the units of measure for the sensor. This value is an integer with a value over 0 in the example. The data type is double, and double.maxvalue is positive 1.79769313486232e308. The significance of the integer depends on the sensor type. For example, the integer for a FanOut sensor represents the number of hosts with which the source IP communicated. For information about the units of measure that each sensor type measures, see [Configure Sensor Thresholds and Options](#) (see page 39).
**PROBVALUE%**

The percentage of anomaly probability, expressed as a value between 1 and 100. In the example, the value is 1. This value is the statistical probability that a sensor has detected anomalous traffic. You can use thresholds to suppress Syslog messages when the probability is low. You can specify the threshold for each sensor independently.

**ROUTERINFOVALUE**

(Optional) The optional ROUTERINFOVALUE field is provided for anomalies that are based on NetFlow. The close router and interface information is derived from the router that sent the flow data.

A router close to the issue (for further analysis or ACL) is ROUTERIPADDRESSVALUE and IN interface is INIFINDEX

where:

**ROUTERIPADDRESSVALUE**

IP address of the router, as reported by NetFlow.

**INIFINDEX**

Interface (IF) index on the incoming interface of the router, as reported by NetFlow.

**Note:** If you want to write a parser to handle Syslog Basic Anomaly or Anomaly Cluster messages, specify a value for the msg= field. The other fields are in the CEF standard format, and you do not need to specify their values.

**Example of an Anomaly Cluster Message**

A Syslog Anomaly Cluster message reports an alert for a group of anomalies. The following example shows the message fields for an Anomaly Cluster message:

```
02-12-2009 17:51:42 Local0.Alert 10.0.23.138 Feb 12 17:51:42
sk23-138
CEF:0|NetQoS|AnomalyDetector|9.2.0.1|2161393963:1234482300|AnomalyCluster|10|src=xxx.212.65.43 start=2/12/2009 5:45:00 PM
msg=AnomalyCluster: anomalies included Frags, FragsAndLoss
anomalyScore 10 max anomaly probability 90%. Routers/interfaces
close to the issue (for further analysis or ACL) are 10.00.00.100
: 12, 10.00.30.100 : 0, 172.10.00.9 : 2, 10.20.00.10 : 169418917
```

The sixth CEF field identifies the sensor types that detect the violation. The message contains multiple sensor types, so the sixth CEF field always has the value AnomalyCluster. The list of sensor types is contained in the message body. The msg field format is as follows:

```
msg=AnomalyCluster: anomalies included LISTOFANOMALIESVALUE
anomalyScore CLUSTERSCOREVALUE max anomaly probability
PROBVALUE%. Optional ROUTERINFOVALUE
```
where:

**LISTOFANOMALIESVALUE**

List of the anomalies in the cluster, which is comma-delimited in the following manner: fanOut, SYNOnly, and topNullRoutes.

**CLUSTERSCOREVALUE**

Weighted severity value. The cluster score is the weighted count of anomalies. Secondary role anomalies, such as flows, volume in, and volume out, count as 0.5. All other anomalies count as 1.

**PROBVALUE**

Maximum anomaly probability of the anomalies in the cluster. The PROBVALUE field is similar to the field in the basic anomaly message, except that it identifies the maximum probability across all the anomalies in the cluster.

**ROUTERINFOVALUE**

(Optional) The optional ROUTERINFOVALUE field is provided for anomalies that are based on NetFlow. The close router and interface information is derived from the router that sent the flow data. The format for ROUTERINFOVALUE is as follows:

**Routers/interfaces close to the issue (for further analysis or ACL) are ROUTERandINTERFACElistVALUE**

where:

**ROUTERandINTERFACElistVALUE**

List of the router IP addresses and the associated incoming IF index. For example, enter 199.30.15.30 : 1, 199.30.15.30 : 1, 199.30.15.30 : 1. The router : interface pairs follow the same order as the anomaly types that are reported in the LISTOFANOMALIESVALUE field.
SNMP Trap Alerts

You can enable SNMP traps to be sent to a third-party network monitoring program. If you enable SNMP trap alerts, an SNMP trap is sent each time a threshold violation triggers an alert. You also can set the alert to be triggered only by a correlated anomaly.

Multiple targets for SNMP traps are not supported.

Follow these steps:

1. Configure the trap receiver to listen for traps from the CA Anomaly Detector server.
   Use the MIB file to import the CA Anomaly Detector Object IDs (OIDs) into your trap receiver. The MIB file is located in the following directory on the CA Anomaly Detector server:
   <install_path>\NQAD\MIB\NetQoS-AnomalyDetector-mib
   The steps for importing the OIDs and configuring the trap receiver are specific to the trap receiver.

2. Display the Data Source List page:
   a. Log in to the CA Performance Center Console or CA NetQoS Performance Center Console as a user with administrator privileges, if you are not already logged in.
   b. Select Admin, Data Sources.
      The page for managing data sources opens:
      – Manage Data Sources page (CA Performance Center)
      – Data Source List page (CA NetQoS Performance Center)

3. Click the name of the CA Anomaly Detector instance that you want to configure.
   The Monitored Products page opens.

4. Click View Alert Targets.
   The Alert Targets page opens.

5. Double-click the snmp_traps row.
   The Edit Alert Target page opens.

6. Specify the Target: Enter the IP address or DNS hostname of the system that will receive the SNMP traps.

7. Select one or both of the following options to enable the alert:
   - Basic State: Send alerts whenever any single sensor detects an anomaly that crosses a threshold.
Cluster State: Send alerts only when the requirements for a correlated anomaly are met.

This is the recommended setting for first-time use of CA Anomaly Detector. If you have already disabled alerts for the sensors that are irrelevant to you, the recommended setting is Basic State. For more information about these recommendations, see the Best Practices note at the end of the topic about configuring Syslog alerts (see page 41).

For information about what constitutes a correlated anomaly, see Correlated Anomalies on page 7 (see page 14).

8. Click Save.

You return to the Alert Targets page, which reflects any changes you saved.
Chapter 4: CA Anomaly Detector Reports

CA Anomaly Detector provides data to compile and display in predefined reports.

This section describes the predefined CA Anomaly Detector reports in the CA Performance Center Console or the CA NetQoS Performance Center Console. For more information about using CA Performance Center, see the Administrator Guide and the Operator Guide for the Performance Center version that you use.

Display Predefined Reports

The predefined CA Anomaly Detector reports are displayed in the Console for CA Performance Center or CA NetQoS Performance Center. To view the reports, open the Anomaly Detector report page in one of the following ways:

- (CA PC) Open the CA Performance Center Console and select Dashboards, Operations Displays: Anomaly Detector.
- (NPC) Open the CA NetQoS Performance Center Console and select Reports, Operations: Anomaly Detector.

To view the reports, your user account must be assigned a role that gives you access to the report menu. User account settings are managed in the Console for CA Performance Center or CA NetQoS Performance Center. For more information about user account permissions, see the Administrator Guide for the Performance Center version that you use.

Customize Predefined Reports

To change the reporting time frame for the views on the Anomaly Detector report page, use the controls at the top of the page in one of the following ways:

- Choose a reporting time frame from the drop-down list.
- Click the scroll button on the left or right side of the date to move the reporting day forward or backward.
- Click the start date or end date and select a new start or end date from the calendar that opens.
- Click the starting hour, starting minute, ending hour, or ending minute and select a new value from the drop-down list.
You can also customize the report page to change which views are included, the view order, the page layout, the page title, and the label of the menu option that opens the page. To access these editing options, select More in the upper right corner, then select Edit Dashboard (CA PC) or Edit Report (NPC).

For more information about customizing report pages, see the Administrator Guide for the Performance Center version that you use.

### Predefined Reports

The following types of predefined reports are available:

- **Anomaly Activity** (see page 50)
- **Anomaly Detector Overall Status** (see page 51)
- **Top Enterprise-Wide Network Anomalies** (see page 51)
- **Top Anomalies by Host** (see page 52)
- **Top Anomalies by Interface** (see page 52)
- **Enterprise-Wide Correlated Anomalies** (see page 53)
- **Enterprise-Wide Anomalies** (see page 54)
- **Anomaly Activity** (see page 52)

### Anomaly Activity

The Anomaly Activity view displays anomalous activity as a bar chart. This view gives you a visual overview of how many anomalies and anomaly clusters occurred compared to all of the records. The number of records that were processed is shown in the hundreds of thousands.

Changing the time frame can show when the issue began and help find patterns.
Anomaly Detector Overall Status

The Anomaly Detector Overall Status table lists the number of records that were processed during the selected time frame, the number of anomalies, and the number of anomaly clusters.

![Anomaly Detector Overall Status Table]

Top Enterprise-Wide Network Anomalies

The Top Enterprise-Wide Network Anomalies pie chart shows the top 10 anomaly types for the reporting time frame.

This view shows the type of network traffic that had the highest proportion of anomalous traffic. This data may give you the first insight into poor network performance.

![Top Enterprise-wide Network Anomalies]

The legend identifies the number of instances and the colors for each anomaly type. Anomaly types are named for the corresponding sensors. For a description of each sensor, see Sensors Overview (see page 59).

The Top Enterprise-Wide Network Anomalies view is most useful for tracking sudden changes in network behavior. For example, suppose that the Enterprise-Wide Network Anomalies view shows that the Large DNS Packet Sources category accounts for 25% of all potentially anomalous network behavior for the past week. If the summary indicates that Large ICMP Packets account for 50% of such traffic today, you would follow up with an investigation.
Predefined Reports

**Top Anomalies by Host**

The Top Anomalies by Host pie chart shows the top 10 anomalous hosts, ranked by the number of anomalies for the reporting time frame. The number of instances is shown next to each pie slice.

![Image of Top Anomalies by Host chart]

**Top Anomalies by Interface**

The Top Anomalies by Interface pie chart shows the anomalies for the top 10 interfaces, ranked by number of anomalies. The number of instances is shown next to each pie slice.

![Image of Top Anomalies by Interface chart]
Enterprise-Wide Correlated Anomalies

The Enterprise-Wide Correlated Anomalies table summarizes the anomalous behaviors that are most likely to be malicious or damaging to the network.

This view shows anomaly clusters that occurred during the reporting time frame. Anomaly clusters are better indicators for problems than single anomalies. Many types of intrusions or attacks involve multiple instances of anomalous network behavior. Instances are often clustered around a group of a few hosts at first, then the behavior spreads. This view identifies network locations to begin investigating if you suspect malicious activity.

An anomaly is *correlated* when the following requirements are met:

- Three or more anomaly instances exist.
- Two different anomaly types are present or have an Anomaly Index above 2.0.
- One device is the source of the anomalies.

Correlation is useful because many attacks on networks and components display a fan-out behavior, which affects seemingly unrelated devices and produces unexpected traffic from multiple sources. Correlation is performed according to an algorithm that considers the typical patterns for each type of monitored network traffic.

The Enterprise-Wide Correlated Anomalies view provides the following information about anomalous network behavior:

**Host**

The IP address of the host that displays the anomalous behavior. The host may be a client computer, a server, a router, or a router interface. The program attempts to resolve the hostname of any IP address and displays that name in the Host field.

**Anomaly Index**

The count of the anomalies in the cluster, weighted by their role as either primary or secondary. The higher the index number, the more severe the issue is.
Predefined Reports

**Types**

The number of different types of anomalous network behavior during the reporting period.

**Date**

The date and time of the first correlated anomaly on the host. Click the Date link to jump to the Anomaly Drill-in page.

Click a Date link to jump to the Anomaly Drill-In page (see page 56), which contains a table that describes the corresponding anomalies. Click the links in the Anomaly Drill-In page table to view additional reports:

- Host link: Display the configuration page for a Flow Forensics report in CA Network Flow Analysis, which has filters pre-configured to match the selected anomaly type and host. Run the report to see more detail.

- Date link: Display a trend plot for the anomaly.

The time may vary by up to 15 minutes from the time when the flows actually took place. Data is pulled from the Harvesters for analysis at 15-minute polling intervals.

**Enterprise-Wide Anomalies**

The Enterprise-Wide Anomalies view is a comprehensive summary of the anomalous behavior during the reporting time frame, with details about the anomaly type, location, and size.

This view is useful for beginning an investigation of problematic network behavior or for initiating troubleshooting procedures to stem an attack. The Enterprise-Wide Anomalies view provides more detailed information about the anomalies you see in other views. This view also identifies the network locations to begin investigating.
The Enterprise-Wide Anomalies view provides the following information about anomalous network behavior:

**Anomaly Type**

The type of anomalous behavior detected. For a description of each anomaly type that you can enable for monitoring, see Sensors Overview (see page 59).

**Host**

The name or IP address of the host on which the anomalous behavior is detected. The host may be a client system, a server, a router, or a router interface. The program attempts to resolve the hostname of any IP address and displays that name in this field.

**Probability**

The calculated likelihood that flagged packet flows are truly anomalous.

Probability is expressed as a percent. For example, if the probability for an anomaly type is 91%, the packet flows that triggered the anomalous behavior report are calculated to have a 91% probability of being anomalous. In this case, the packet flows have a low probability of occurring normally on this network.

For more information about how the probability algorithm operates, see Probability Thresholds (see page 13).

**Value**

The value that triggered the anomalous behavior report, expressed in the units of measure shown in the Unit column. For example, the value could be the number of gigabytes of data in the anomalous flow.

**Metric/Unit**

The unit of measurement that is used to express the Value, such as packets, flows, or destination hosts (dest hosts).

**Discovered by**

The router, interface, or data source that detected the anomalous data.

**Date**

The date and time that the anomalous behavior is detected. The time may vary by up to 15 minutes from the time when the flows actually took place. Data is pulled from the Harvesters for analysis at 15-minute polling intervals.
The Enterprise-Wide Anomalies view provides several links that you can use to begin investigations into anomalous behavior:

- **Date**: Click a Date link to go to the Detail page, which shows a trend chart of the anomaly value and probability over time. For more information, see Detail Pages (see page 56).
- **Discovered By**: Click a "Discovered By" link to view details. The destination is determined by the type of link you click. For example, a link that is the IP address for a CA Network Flow Analysis sensor opens the corresponding interface pages in CA Performance Center or CA NetQoS Performance Center.
- **Host**: Click a Host link to open a report with more details. The sensor determines which type of report is defined. Many sensor types open the page for defining a Flow Forensics report in CA Network Flow Analysis, which has pre-populated report filters.

**Detail Pages**

To access detailed information about correlated anomalies, click the Date column links in the Enterprise-wide Correlated Anomalies view or the Enterprise-wide Anomalies view. To access the Anomaly Trend view, click the Host name in either the Enterprise-Wide Anomalies or the Anomaly Drill-In views.

**Anomaly Drill-In**

If you drill into an anomaly cluster (shown in the Enterprise-wide Correlated Anomalies table), the Anomaly Drill-In table opens. The table lists each anomaly with its probability, value, the originating router and interface, and the time that the anomaly occurred. Use the time link to drill into a trend chart that shows the value and probability over time.

The Anomaly Drill-In view provides the following information about each anomaly:

**Anomaly Type**

The type of anomalous network behavior detected. Anomaly types correspond to the sensors, which are described in Sensors Overview (see page 59).

**Host**

The name or IP address of the host on which the anomalous behavior is detected. The host may be a client system, a server, a router, or a router interface. The program attempts to resolve the hostname of any IP address and display that name in this field.
Predefined Reports

Chapter 4: CA Anomaly Detector Reports

Prob(%)  
The calculated likelihood that flagged packet flows are truly anomalous. Probability thresholds are discussed in more detail in Probability Thresholds (see page 13). Probability is expressed as a percent. For example, if the probability for an anomaly type is 91%, the packet flows that triggered the anomalous behavior report are calculated to have a 91% probability of being anomalous. In this example, the packet flows had a low probability of occurring normally on this network. For more information about how the probability algorithm operates, see Probability Thresholds (see page 13).

Value  
The value that is used to determine the severity of the deviation from the baseline profile of network behavior. Shows what was measured in the network traffic.

Metric/Unit  
The unit of measurement that is used to express the Value, such as packets, flows, or destination hosts (dest hosts).

Discovered By  
The router, interface, or other data source that detected the anomalous data.

Date  
The date and time that the anomalous behavior was detected. The time may vary by up to 15 minutes from the time when the flows actually took place. Data is pulled from the Harvesters for analysis at 15-minute polling intervals.

Anomaly Trend  
The Anomaly Trend view shows the value and probability of the anomaly over time in a trend chart. To display the Anomaly Trend view, click a link in the Date column in either the Anomaly Drill-in view or the Enterprise-Wide Anomalies view.
The Anomaly Trend view shows the pattern of deviation from normal network behavior. You can see when the behavior began and how severe the behavior was. A longer term view can help to determine daily, weekly, or monthly patterns.

The recorded values are shown as a blue trend line on the X-Axis. The probability that the behavior is a true anomaly is shown as a pink trend line on the Y-axis.
Chapter 5: Sensors and Troubleshooting

CA Anomaly Detector features 27 sensors that evaluate the data that the data source products generate.

This section describes the sensors, the types of issues they can detect, and steps to try when you troubleshoot issues.

Sensors Overview

CA Anomaly Detector provides a diverse set of sensors that search for potential network anomalies in the collected data.

Most sensors are enabled by default. The sensors become active as soon as you add the supporting data source to CA Anomaly Detector. You can disable sensors or apply filtering to exclude selected devices for individual sensors.

Sensor configuration also includes a probability factor. This factor controls sensor sensitivity and frequency of alerts. For more information, see Probability Thresholds (see page 37).

Built-in Workflows

Workflows are built into the views to let you research and troubleshoot anomalies quickly. To use the workflows, click the view links and jump to preconfigured reports or to a general page.

Discovered By Link

Click the "Discovered by" link to go to one of the following locations:

- A router interface report in CA Performance Center or CA NetQoS Performance Center (CA Network Flow Analysis anomalies)
- The main page for the supporting product (CA Application Delivery Analysis (SuperAgent), CA NetVoyant, or CA Unified Communications Monitor anomalies)
Anomaly Index

The anomaly correlation algorithm compares each particular behavior to the typical patterns for the network traffic type. The Anomaly Index in the Correlated Anomalies view is a count of the number of anomalies in an anomaly cluster, weighted by their role as either primary or secondary.

Host Link Destinations

The Host links in the Enterprise-Wide Anomalies view and the Anomaly Drill-in views take you to more granular information about the device that has the anomaly. Many links open the page for a Flow Forensics report in CA Network Flow Analysis, which has pre-populated report filters. Clicking a Host link may be the first step in troubleshooting the anomaly.

CA Network Flow Analysis Sensors

CA Network Flow Analysis provides information to help you understand how application traffic affects your network’s performance. CA Network Flow Analysis enables you to see which applications are using bandwidth, who is using the bandwidth, and when. By knowing which applications and users are consuming bandwidth, you can make timely and cost-effective decisions to optimize network performance.

When you add CA Network Flow Analysis as a data source for CA Performance Center or CA NetQoS Performance Center, the Harvesters are added as possible data sources for CA Anomaly Detector automatically. Special considerations apply when you enable Harvesters as data sources, as described in Best Practices: Slow Harvester Rollout (see page 36).

RST-Only Sources

The RST-Only Sources sensor looks for the following types of connections:

- Hosts that send out RST TCP packets with no ACK packets to acknowledge an open connection to a server
- Servers that receive only RST packets from certain hosts with no ACK or SYN packets.
Troubleshooting an RST-Only Sources Alert

An alert from the RST-Only Sources sensor may indicate one of the following issues:

- A server that is running out of resources for an active application.
  Investigate whether a server upgrade is needed.
- A server that has a previously active application, which has become inactive.
  Try restarting associated application services.
- Users who are connecting to the wrong server.
  Check for DNS issues and correct any issues that you find.
- A host that is the victim of port-scanning activity.
  Identify and use the firewall or ACL to block the offending host from sending data on the network while you investigate.

Fragmented Packet Sources

The Fragmented Packet Sources sensor looks for sources of packet fragmentation. Packet fragmentation may indicate poor application delivery or "frag attacks" that can circumvent Access Control Lists (ACLs) and stateless firewalls.

Troubleshooting a Fragmented Packet Sources Alert

An alert from the Fragmented Packet Sources sensor may indicate one of the following issues:

- A Layer 3 network maximum transmission unit (MTU) mismatch.
  Check the MTU settings on the affected interfaces. Interfaces on the same router can have different MTU settings. Any IP packets that exceed the configured maximum number of bytes are broken into fragments. Stateless firewalls in particular often drop packet fragments.
- A "frag attack" that is designed to exhaust network resources.
  Packets can be fragmented normally by routers if the packets exceed the MTU size on a router interface. In this case, a flag is set in the IP header to indicate that the segment is a fragment. The packets continue until the end of fragment (EOF) flag is set. In a frag attack, fragmented packets are sent in a steady stream, but a packet with the EOF flag set is never sent. The packets eventually fill the receive buffer on the target host and disable it.
  If you suspect a frag attack, identify and block the offending host from sending data on the network by using a firewall or ACL.
- Attempted reconnaissance or fingerprinting.
  Fragmented packets may indicate that an attacker is probing the host for system credentials, such as operating system level and known vulnerabilities.
  Identify and block the offending host from sending data on the network by using a firewall or ACL.

Even though a host who communicates with another host across a VPN tunnel is a legitimate source for fragmented packets, the host is still a source of increased packet load. Adjusting the MTU on the host with the VPN client can help.

CA Anomaly Detector currently cannot actually identify the sources of packet fragmentation. The software can identify only the original source of the IP packet. Any Layer 3 device along the path may be the source of the actual act of fragmenting the packet.

**Large DNS Packet Sources**

The Large DNS Packet Sources sensor looks for DNS requests that are larger than typical requests. Such packets may indicate tunneling attempts or data exfiltration.

**Troubleshooting a Large DNS Packet Sources Alert**

An alert from the Large DNS Packet Sources sensor may indicate data exfiltration activity. Data exfiltration is a network security violation in which a user discreetly attempts to send data from an internal network to an external location.

If you suspect data exfiltration, click the link for the offending host to investigate the suspected user by using a Flow Forensics report in CA Network Flow Analysis. For more information, see Built-in Workflows (see page 59). You can also use other packet-inspection tools (such as CA GigaStor) to identify the data that was sent.
Large ICMP Packet Sources

The Large ICMP Packet Sources sensor looks for ICMP packets that are unusually large. Large packets may indicate tunneling attempts or data exfiltration.

Troubleshooting a Large ICMP Packet Sources Alert

An alert from the Large ICMP Packet Sources sensor may indicate data exfiltration activity. Data exfiltration is a network security violation in which a user discreetly attempts to off-load data from an internal network to an external location.

If you suspect data exfiltration, click the link for the offending host and investigate the suspected user in a Flow Forensic report in CA Network Flow Analysis. For more information about this step, see Built-in Workflows (see page 59). You also can use any packet-inspection tools that you have, such as CA GigaStor, to identify the data that was off-loaded.

TTL Expired Sources

The TTL Expired Sources sensor looks for possible router misconfiguration, such as routing loops, by monitoring for time to live (TTL) expiration messages.

Troubleshooting a TTL Expired Sources Alert

An alert from the TTL Expired Sources sensor may indicate one of the following issues:

- A network configuration issue such as a routing loop or equipment problem. A routing loop occurs when packets are routed incorrectly so that they travel in a continuous circle. The loop typically occurs when a router or line fails before routine notifications about the link failure have had time to reach the other network routers. Routing loops often appear when network changes are made. Try to identify and correct any network outage that becomes apparent. Try to find any "black hole" network ranges and check the associated routers.

- Heavy traceroute activity. Investigate any unusual traceroute activity to determine whether the activity is legitimate. For example, investigate whether the traceroute activity is performed for testing or troubleshooting.
**Congestion Sources**

The Congestion Sources sensor monitors ICMP Source Quench messages by looking for devices that are overwhelmed by incoming traffic.

If the packet receiver experiences congestion, it sends a source quench message to the packet sender, which causes the sender to initiate a TCP slow start. This has a significant negative impact on performance. CA Anomaly Detector reports the host that is the source of the overwhelming traffic and indicates which congested router reported the issue.

**Troubleshooting a Congestion Sources Alert**

Look at the load on the device that issues the source quench message. Legitimate traffic may be overloading the device.

If the host is under attack, correlated anomalies are likely to appear in the Enterprise-Wide Correlated Anomalies view.

**Previously Null Routed Sources**

The Previously Null Routed Sources sensor aggregates data about traffic from null-routed sources. The sensor reports on the hosts with the highest volume of normally-routed traffic that previously had null-routed traffic.

**Troubleshooting a Previously Null Routed Sources Alert**

An alert from the Previously Null-Routed Sources sensor may indicate that Access Control Lists (ACLs) are applied inconsistently across the enterprise. ACL problems may result from a security violation.

Audit all ACLs to ensure that they are properly configured and conform to established network access and usage policies. Try to determine whether the ACLs have unauthorized modifications.

It is also possible that the host is sending malicious traffic in various ways and the ACLs are catching some of that traffic. It may be worthwhile to investigate the type of traffic that the ACLs do not block. To do this, use the Host link on the Anomaly Drill-in to run a CA Network Flow Analysis Flow Forensic report.
SYN/RST-Only Packet Sources

The SYN/RST-Only Packet Sources sensor looks for hosts that send out unusually large amounts of SYN-RST packets. This behavior may indicate a SYN or RST flood.

Troubleshooting an SYN/RST-Only Packet Sources Alert

An alert from the SYN/RST-Only Packet Sources sensor may indicate that someone is attempting to hack into the network. Specifically, SYN-RST packets are associated with attempts to bypass a firewall perimeter.

SYN/RST-only packet flows signal a connection establishment request that is immediately followed by a reset request, which is not characteristic of normal TCP behavior. This behavior typically indicates scanning activity, which may include OS fingerprinting.

SYN-Only Packet Sources

The SYN-Only Packet Sources sensor looks for:

- Hosts that send out only SYN TCP packets with no corresponding ACK packets to acknowledge an open connection to a server
- Servers that receive only SYN packets from certain hosts with no corresponding ACK or RST packets.

Requests for a server connection without establishing a valid socket are typical of a denial-of-service attack by using SYN packet reflection.

Troubleshooting a SYN-Only Packet Sources Alert

An alert from the SYN-Only Packet Sources sensor may indicate a worm infection or a SYN flood, which is a type of denial of service attack.

A SYN flood involves a series of SYN TCP packets that contain invalid source IP addresses. The target server is unable to establish a valid connection in response to the SYN request, but it still allocates the necessary resources and waits until a timeout expires for the ACK packet from the requesting host. The server is quickly brought to a standstill by trying to process invalid connection requests.

If you suspect a denial of service attack, use CA Anomaly Detector to identify each offending host, then use firewalls or ACLs to try to block the host from sending data on the network. You also can take the affected server offline.
High Packet Fan Out

The High Packet Fan Out sensor looks for packets that fan out from a single host to many hosts. Packet fanning is typical of a spreading virus or worm. A High Packet Fan Out anomaly is a primary type of anomaly, which typically occurs in conjunction with another type of anomaly.

Troubleshooting a High Packet Fan Out Alert

An alert from the High Packet Fan Out Sources sensor may indicate a spreading virus or worm infection. Some viruses or worms operate by creating "zombie" hosts that spread the infection in a fan-out pattern.

If you suspect a virus infection, use CA Anomaly Detector to identify each offending host, then use a firewall or ACL to try to block the host from sending data on the network. You also can take the affected server offline.

High and Variable Volume-Out

The High and Variable Volume-Out sensor tracks host volume and detects sudden changes in server output. These changes may indicate server misconfiguration, virus infection, or unauthorized activity, such as BitTorrent server activity. These conditions produce a secondary type of alert, which typically occurs with another type of anomaly.

Troubleshooting a High and Variable Volume-Out Alert

An alert from the High and Variable Volume-Out sensor may indicate one of the following issues:

- Server misconfiguration.
  
  Find the source of the anomalous traffic and investigate the activity.

- A new authorized or unauthorized application that is deployed on the network.
  
  Find the source and investigate. Such behavior may indicate the presence of a BitTorrent or other peer-to-peer file-sharing server.

  Peer-to-peer file-sharing or other unauthorized activity often consumes excessive network resources. This type of activity potentially can expose your enterprise to copyright-infringement legal action.
High and Variable Volume-In

The High and Variable Volume-In sensor tracks host volume and detects sudden changes in incoming volume. These changes may indicate server misconfiguration, virus infection, or unauthorized activity, such as BitTorrent server activity. The activity produces a secondary type of alert, and it typically occurs together with another type of anomaly.

Troubleshooting a High and Variable Volume-In Alert

An alert from the High and Variable Volume-In sensor may indicate one of the following issues:

- Server misconfiguration.
  
  Find the source of the anomalous traffic and investigate the activity.

- A new authorized or unauthorized application that is deployed on the network.
  
  Find the source and investigate. The behavior may indicate the presence of a BitTorrent or other peer-to-peer file sharing server.

  Peer-to-peer file-sharing or other unauthorized activity often consumes excessive network resources. This type of activity potentially can expose your enterprise to copyright-infringement legal action.

High Flow Sources

The High Flow Sources sensor tracks host flows and detects sudden changes in output that may indicate server misconfiguration, virus infection, or unauthorized activity, such as BitTorrent server activity.

Troubleshooting a High Flow Sources Alert

An alert from the High Flow Sources sensor may indicate an increase in connections. The increase is often caused by the introduction of a new authorized or unauthorized application on the network.

Find the source and investigate. The behavior may indicate the presence of a BitTorrent or other peer-to-peer file sharing server.

Peer-to-peer file-sharing or other unauthorized activity often consumes excessive network resources. This type of activity potentially can expose your enterprise to copyright-infringement legal action.
Ffrags and Loss Sources

The Frags and Loss Sources sensor looks for sources that cause packet loss by monitoring "Fragment reassembly time exceeded" messages. Packet fragmentation can be used to circumvent blocking rules on some firewalls.

Troubleshooting a Frags and Loss Sources Alert

Fragmentation and packet loss occurs when you deploy high bit-rate Windows Media content.

Fragmentation can cause retransmissions when some fragments fail to arrive in time so that the packet is lost. Reliable protocols such as TCP retransmit all of the fragments in order to recover from the loss of a single fragment.

Dest Unreachable Sources

The Dest (Destination) Unreachable Sources sensor looks for unusually high levels of network traffic that fails to reach the destination designated by the packet. The sensor operates by monitoring ICMP return codes, whether for a network, host, or port. This type of traffic flood consumes bandwidth on the affected link, which causes reduced performance for the link’s legitimate users.

Troubleshooting a Dest Unreachable Sources Alert

An ICMP flood (also known as Ping flood or Smurf attack) is one source of a Destination Unreachable Sources alert. This type of Denial of Service attack sends large amounts of ICMP packets or over-sized ICMP packets to a system. The goal of the attack is to crash the system’s TCP/IP stack so that the system stops responding to TCP/IP requests.

An ICMP attack can come in many forms. An ICMP flood is typically accomplished by broadcasting a lot of ICMP pings or UDP packets. The attack sends so much data to the system that it slows down enough to disconnect from normal business applications due to timeouts.

If you suspect a Denial of Service attack, use CA Anomaly Detector to identify each offending host, then use a firewall or ACL to try to block the host from sending data on the network. You also can set up an ACL that blocks external traffic to the affected host or you can take the affected server offline.
Non-Local Sources

The Non-Local sensor is turned off by default. Consult with your technical representative to determine whether this sensor is beneficial for your network.

The Non-Local sensor looks for traffic that does not have either a private source or destination IP address. The sensor assumes that the enterprise uses private IP addresses internally—that the majority of traffic has a private source or destination IP address.

For example, suppose a system in the network has a fake external IP address and the system sends messages to another fake external IP address. The resulting traffic can stop legitimate network traffic by tying up the routers and interfaces closest to that system.

Depending on your enterprise network configuration, legitimate traffic may flow between non-private IP addresses. If this is the case, your technical representative may be able to help you configure the sensor to exclude IP address ranges and avoid false alerts.

Troubleshooting a Non-Local Alert

Determine whether the non-private IP addresses are used for legitimate traffic. If the traffic is not legitimate, use the router and interface information that CA Anomaly Detector provides to apply ACLs to mitigate the traffic while you locate the offending source device.

CA NetVoyant Sensors

CA NetVoyant is a performance analysis and reporting software package that automates the collection, analysis, and reporting of critical device data. Using Simple Network Management Protocol (SNMP), CA NetVoyant automatically polls and correlates data from devices on your network. Data from routers, switches, servers, RMON2 probes, frame relay circuits, logical segments, and wide area links are collected and organized to give you information about your network.

CA Anomaly Detector contacts the CA NetVoyant database to gather data for analysis. The following sensors are used to detect anomalies in the data that CA NetVoyant collects that could indicate an issue with your network.
**Incoming Discard Rate**

The Incoming Discard Rate sensors look for patterns of incoming packets that are dropped even though they contain no errors.

**Troubleshooting an Incoming Discard Rate Alert**

An Incoming Discard Rate alert may indicate one of the following issues:

- Overutilization
- Denial of service
- VLAN misconfiguration

This alert may also result from inbound policing on the interface. QoS policies affect discards-in and discards-out counters, depending on whether the QoS policy is inbound or outbound.

**Incoming Error Rate**

The Incoming Error Rate sensor looks for patterns in incoming errors.

**Troubleshooting an Incoming Error Rate Alert**

Incoming Errors typically relate to CRC or other physical layer conditions and are not due to QoS, routing, or configuration issues.

**Dropped Packets**

The Dropped Packets sensor looks for patterns in queue drops.

**Troubleshooting a Dropped Packets Alert**

Dropped packets, or queue drops, may indicate buffer depletion. Input queue drops typically occur when a packet is process-switched. A process switch means that the router cannot use a preferable route-cache method, such as fast switching or Cisco Express Forwarding (CEF), to handle the forwarding decision. If input drops are still present, it implies that there is simply too much traffic. Output drops are caused by a congested interface.
Buffer Misses

The Buffer Misses sensor looks for patterns in buffer misses. Buffer failures are one of the most common reasons for packet drops.

Troubleshooting a Buffer Miss Alert

Look at the buffers on your router to determine whether they are configured properly.

CA Unified Communications Monitor Sensors

CA Unified Communications Monitor (UCM) ensures the availability and performance of Cisco Voice over IP (VoIP) systems. The program passively monitors the VoIP call setup traffic and the call quality for IP phones, call servers, and voice gateways and keeps a continuous record of VoIP call setup performance and call quality from one end of the network to the other.

CA Anomaly Detector contacts the UCM database to gather data for analysis. The following sensors are used to detect anomalies in the UCM data, which may indicate an issue with your VoIP network.

Voice Call Fan Out

The Voice Call Fan Out sensor looks for patterns in voice call fan outs. In a fan out, a single IP phone calls a large number of unique phone numbers in a short time.

Troubleshooting a Voice Call Fan Out Alert

The IP Address of the phone that originates the call fan-out is identified in the anomaly event. Check the phone at this address to determine why it originates fan-out calls. Use the UCM dashboard to determine which calls were made in the fan-out time frame.

Voice Call DoS

The Voice Call DoS sensor looks for a single phone that calls repeatedly over a short time. This type of attack differs from other Denial of Service (DoS) attacks because of its low volume. It only takes about 10 calls per minute to keep a phone ringing all the time. A traditional intrusion detection system may not catch the attack.

Troubleshooting a VoIP DoS Attack Alert

The anomaly event identifies the IP address of the phone that is called. Check to see who is calling the phone. Use the UCM dashboard to determine which calls were made during the attack time frame.
Voice Server Distress

The Voice Server Distress sensor looks for calls that are not completed, which are going through a specific call server. The calls are either abandoned or they fail setup. The abandonments and failures are weighted with the call volume to determine whether to flag a server. Even if the condition does not result from a security attack on the server, it is still a performance anomaly that warrants investigation.

Troubleshooting a Voice Server Distress Alert

The anomaly event identifies the IP address of a call server that has a large percentage of errored or abandoned calls. Use the UCM dashboard to look at the details of calls that are attempted, completed, and in error for the call server during the anomaly time frame.

CA Application Delivery Analysis Sensors

CA Application Delivery Analysis (SuperAgent) provides end-to-end performance monitoring through reports and views that show historically normal performance for users and metrics that cross acceptable performance thresholds. CA Application Delivery Analysis (SuperAgent) gathers troubleshooting information and helps you determine the origin of an application, network, or server performance problem.

CA Anomaly Detector contacts the CA Application Delivery Analysis (SuperAgent) database to gather data for analysis. The following sensors are used to detect anomalies in the data collected by CA Application Delivery Analysis (SuperAgent) that may indicate an issue with your network.

Retransmission Time

The Retransmission Time sensor looks for patterns in retransmissions.

TCP retransmission behavior has a significantly negative effect on application performance and network use. Communication across the affected connection can slow to a halt until a missing segment is retransmitted successfully. Only a limited number of missing segments can remain outstanding at any time.

Troubleshooting a Retransmission Time Alert

An anomaly in retransmission delay typically is caused by several critical components:

- Congested Path: Retransmission delay can increase when interfaces between the clients and servers are congested.
- QoS: A misapplied QoS policy for a particular application may cause increased buffer or queue drops.
Backup/Routing Issue: A change in the per hop route may cause the issue. Additional retransmission delay may result from routing changes that add congestion to a pipe that is already congested or a pipe that is smaller, such as a backup link.

Identify sources of packet loss along the traffic paths. Keep in mind that the paths going to the server may be different from the paths coming from the server. If that is the case, analyze all paths.

Refused Sessions

The Refused Sessions sensor looks for a pattern in refused sessions. Refused session counts may indicate a SYN attack or a server that cannot respond to all requests.

Troubleshooting a Refused Sessions Alert

A server tends to stop fulfilling and refusing sessions when it reaches its capacity to handle more data. Sessions also may be refused because a load balancer is sending heartbeat messages to the servers.

Refused Sessions counts also may result when legitimate traffic overloads a server that has inadequate resources for additional TCP session requests.

An alert may indicate a SYN or RST flood. If this is the case, the anomaly should be visible in the Enterprise-Wide Correlated Anomalies view.

Packet Load

The Packet Load sensor looks for changes in the number of bytes per packet that goes to a particular server. Applications that run on servers typically have a fairly constant ratio between the number of packets they receive in requests for their service and the packet volume. This sensor looks for anomalous changes in that ratio.

Troubleshooting a Packet Load Alert

In WAN applications, you want to have as much data in each packet as the maximum transmission unit (MTU) allows. Applications that have less data in the packets have to wait longer to get data across the network. Analyze whether the application is loading the packets fully to send to remote users.

An alert may indicate varying implementation of the clients or it may indicate that unexpected clients are trying to subvert the server.
Index

A

absolute thresholds
  described • 38
Access Control Lists (ACLs)
  need for configuring • 36
Add New Data Source page
  displaying/using in CA PC • 29
alerts
  enabling for sensors • 39
  enabling for SNMP traps • 46
  notes about targets • 41
Syslog alerts • 41
  Syslog anomaly cluster messages • 44
  Syslog basic anomaly messages • 43
Anomaly Activity
  view described • 50
anomaly clusters
  Syslog alert message format • 44
Anomaly Detector Overall Status
  view described • 51
Anomaly Drill-In
  accessing view • 56
  Host link destinations • 60
  view described • 56
Anomaly Index
  described • 60
Anomaly Trend
  accessing drill-in view • 56
  drill-in view described • 57

B

basic anomaly messages
  format for Syslog alerts • 43
BitTorrent servers
  High & Variable Volume-In alert • 67
  High & Variable Volume-Out alert • 66
Buffer Misses sensor (NetVoyant)
  troubleshooting alerts • 71

C

CA Application Delivery Analysis (SuperAgent)
  adding as a monitored product • 32
  co-installation not supported • 20
  enabling as collection source • 34
  Packet Load sensor • 73
  Refused Sessions sensor • 73
  Retransmission Time sensor • 72
  version supported • 19
CA NetVoyant
  adding as a monitored product • 32
  Buffer Misses sensor • 71
  co-installation not supported • 20
  Dropped Packets sensor • 70
  enabling as collection source • 34
  Incoming Discord Rate sensor • 70
  Incoming Error Rate sensor • 70
  version supported • 19
CA Network Flow Analysis
  adding as a monitored product • 32
  co-installation options • 20
  Congestion Sources sensor • 64
  Dest Unreachable Sources sensor • 68
  enabling as collection source • 34
  enabling Harvesters • 36
  Fragmented Packet Sources sensor • 61
  Frags and Loss Sources sensor • 68
  High and Variable Volume-In sensor • 67
  High and Variable Volume-Out sensor • 66
  High Flow Sources sensor • 67
  High Packet Fan Out sensor • 66
  Large DNS Packet Sources sensor • 62
  Large ICMP Packet Sources sensor • 63
  Non-Local sensor • 69
  Previously Null Routed Sources sensor • 64
  requirement to monitor • 14
  restriction on number of instances • 15
  RST-Only Sources sensor • 60
  SYN/RST-Only Packet Sources sensor • 65
  SYN-Only Packet Sources sensor • 65
  TTL Expired Sources sensor • 63
  version required • 19
CA PC / NPC
  co-installation options • 20
  customizing predefined AD reports • 49
  displaying predefined AD reports • 49
  registering data sources • 29
  version support • 19
CA Unified Communications Monitor
  adding as a monitored product • 32
enabling as collection source • 34
version supported • 19
Voice Call DoS sensor • 71
Voice Call Fan Out sensor • 71
Voice Server Distress sensor • 72
collection sources
adding for AD • 32
enabling • 34
Congestion Sources
troubleshooting alerts • 64
correlated anomalies
Anomaly Index field described • 60
characteristics described • 14
drilling in to details • 56
view of • 53
data ex-filtration
Large DNS Packet Sources alert • 62
Large ICMP Packet Sources alert • 63
data sources
registering with CA PC • 29
data volume changes
High & Variable Volume-In alert • 67
High & Variable Volume-Out alert • 66
database
mySQL database growth rate • 15
Destination Unreachable Sources
troubleshooting alerts • 68
Discovered by links
destinations for • 59
DNS issues
RST-Only Sources alert • 60
Dropped Packets sensor (NetVoyant)
troubleshooting alerts • 70
Enterprise-Wide Anomalies
Host link destinations • 60
view described • 54
Enterprise-Wide Correlated Anomalies
view described • 53
Event Manager
co-installation options • 20
features
of CA Anomaly Detector • 12
file sharing
High Flow Sources alert • 67
firewalls
ports to configure • 36
frag attacks
Fragmented Packet Sources alert • 61
Fragmented Packet Sources
troubleshooting alerts • 61
Frag and Loss Sources
troubleshooting alerts • 68
getting started
overview of tasks • 15
hardware recommendations
for installation server • 18
Harvesters
best practice for enabling • 36
High and Variable Volume-In
troubleshooting alerts • 67
High and Variable Volume-Out
troubleshooting alerts • 66
High Flow Sources
troubleshooting alerts • 67
High Packet Fan Out
troubleshooting alerts • 66
Host links
destinations for • 60
ICMP floods
Destination Unreachable Sources alert • 68
Incoming Discard Rate sensor (NetVoyant)
troubleshooting alerts • 70
Incoming Error Rate sensor (NetVoyant)
troubleshooting alerts • 70
installation
collection sources
co-installation options • 20
hardware recommendations • 18
operating system support • 17
overview of tasks • 15
prerequisites • 21
software compatibility • 19
steps • 22

L
Large DNS Packet Sources
  troubleshooting alerts • 62
Large ICMP Packet Sources alert
troubleshooting • 63
Layer 3 MTU mismatch
  Fragmented Packet Sources alert • 61

M
messages
  for Syslog anomaly clusters • 44
  for Syslog basic anomalies • 43
MIB file
  location of • 46
monitored products
  adding for AD • 32
  enabling as collection sources • 34
  list of products to monitor • 14

N
Non-Local sensor
  troubleshooting alerts • 69

O
overview
  of CA Anomaly Detector • 11

P
Packet Load sensor (ADA)
  troubleshooting alerts • 73
port scanning
  RST-Only Sources alert • 60
ports
  configuring for firewall • 36
predefined reports
  customizing in CA PC • 49
  displaying in CA PC • 49
prerequisites
  for installation/upgrade • 21
  hardware recommendations • 18
  software compatibility • 19
  supported operating systems • 17
Previously Null Routed Sources
  troubleshooting alerts • 64
probability thresholds
  configuring for sensors • 39
  described • 37
  factors for calculating • 13
  probability defined • 54

R
Refused Sessions sensor (ADA)
  troubleshooting alerts • 73
registering
  with CA PC • 29
reporting
  enabling by registering • 29
reports
  Anomaly Activity • 50
  Anomaly Detector Overall Status • 51
  Anomaly Drill-In • 56
  Anomaly Trend (drill-in) • 57
  customizing in CA PC • 49
  displaying predefined reports • 49
  drill-in views in CA PC • 57
  drilling in to correlated anomaly details • 56
  Enterprise-Wide Anomalies • 54
  Enterprise-Wide Correlated Anomalies • 53
  pre-defined report types • 50
  Top Anomalies by Host • 52
  Top Anomalies by Interface • 52
  Top Enterprise-Wide Network Anomalies • 51
Retransmission Time sensor (ADA)
  troubleshooting alerts • 72
routing loops
  TTL Expired Sources alert • 63
RST-Only Sources
  troubleshooting alerts • 60

S
scalability
  discussed • 15
sensitivity settings
  for probability thresholds • 37
sensors
  Buffer Misses (NetVoyant) • 71
  configuring • 39
  Congestion Sources • 64
  Destination Unreachable Sources • 68
  Dropped Packets (NetVoyant) • 70
  Fragmented Packet Sources • 61
  Frags and Loss Sources • 68
High and Variable Volume-In • 67
High and Variable Volume-Out • 66
High Flow Sources • 67
High Packet Fan Out • 66
Host link destinations • 60
Incoming Discard Rate (NetVoyant) • 70
Incoming Error Rate (NetVoyant) • 70
Large DNS Packet Sources • 62
Large ICMP Packet Sources • 63
Non-Local • 69
overview of • 38
Packet Load (ADA) • 73
Previously Null Routed Sources • 64
Refused Sessions (ADA) • 73
Retransmission Time (ADA) • 72
RST-Only Sources • 60
SYN/RST-Only Packet Sources • 65
SYN-Only Packet Sources • 65
TTL Expired Sources • 63
Voice Call DoS (UCM) • 71
Voice Call Fan Out (UCM) • 71
Voice Server Distress (UCM) • 72
servers
excluding from monitoring • 39
SNMP traps
enabling alerts for • 46
OIDs for • 46
SYN floods
SYN-Only Packet Sources • 65
SYN/RST-Only Packet Sources
troubleshooting alerts • 65
SYN-Only Packet Sources
troubleshooting alerts • 65
Syslog alerts
anomaly cluster messages • 44
basic anomaly messages • 43
described • 41
Syslog server
configuring • 41

T

targets
configuring Syslog alerts • 41
for alerts (introduction) • 41
thresholds
absolute thresholds described • 38
configuring for sensors • 39
probability thresholds described • 37
Top Anomalies by Host
view described • 52
Top Anomalies by Interface
view described • 52
Top Enterprise-Wide Network Anomalies
view described • 51
tunneling
TTL Expired Sources alert • 63
traps
enabling SNMP trap alerts • 46
TTL Expired Sources
troubleshooting alerts • 63
hardware recommendations • 18
operating system support • 17
overview of tasks • 15
prerequisites • 21
software compatibility • 19
steps • 24

V

viruses
High and Variable Volume-In alert • 67
High and Variable Volume-Out alert • 66
Voice Call DoS sensor (UCM)
troubleshooting alerts • 71
Voice Call Fan Out sensor (UCM)
troubleshooting alerts • 71
Voice Server Distress sensor (UCM)
troubleshooting alerts • 72

W

White List
configuring for sensors • 39
described • 38
Windows
supported versions • 17
workflows
for quick troubleshooting • 59
worm infections
  SYN-Only Packet Sources • 65