CA Anomaly Detector

Guide

Release 9.3.0

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 33) -- Prerequisites, software versions supported, and instructions for installation and upgrade.
- Post-Installation Tasks (see page 33) -- Descriptions of CA Anomaly Detector-specific tasks to perform after the installation or upgrade.
- CA Anomaly Detector Views (see page 53) -- How to open and customize the views of anomaly activity, as well as descriptions of each view.
- Sensors and Troubleshooting (see page 69) -- 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, 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.

Contents

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.

Get Started with CA Anomaly Detector

To get started with CA Anomaly Detector 9.3.0, 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 18)
   - Operating System (see page 17)
   - (Recommended) Hardware Specifications (see page 18).
   - Installation and Upgrade Prerequisites (see page 20).
2. Verify that a supported version of Performance Center is installed in your environment: CA Performance Center version 2.4/2.3 or CA NetQoS Performance Center 6.1.205 SP2/6.1.194.

   For more information, see the *Installation Guide* for your Performance Center version.
3. Install or upgrade to version 9.3.0 of CA Anomaly Detector and CA Network Flow Analysis:
   - Install CA Anomaly Detector (see page 25).
   - Upgrade CA Anomaly Detector (see page 27).
4. Register CA Anomaly Detector as a data source for Performance Center: Register CA Anomaly Detector (see page 33).
5. (CA PC deployment) Enable CA Anomaly Detector configuration functions in the NFA console.
6. 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 36).
7. Enable the monitored products so their data is accessible to CA Anomaly Detector: Enable the Monitored Products (see page 38).
8. Configure the firewalls. (see page 40)
9. (Optional) Review the default sensor configurations and make any necessary changes: Configure the Sensors (see page 41).
10. (Optional) Configure targets for alerts, so that Syslog or SNMP trap messages are sent when alerts are triggered: Configure Alert Targets (see page 45).

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 your 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 network. The program 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. The program 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. The program 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.

The program 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 Performance Center Console, 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 so you get a full perspective of how key servers behave
- Identification of attacks before symptoms appear so you can prevent of downtime; isolate viruses quickly, and resolve problems

- 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 61).

Data Collection

Data is monitored in CA Network Flow Analysis databases by querying flow data directly from the Harvesters. If you add other products for monitoring, data is gathered for analysis from their databases. 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

The anomalies that are detected are shown on the Anomaly Detector page views, which are accessible in the Performance Center Console.

Note: For information about the supported versions of the monitored products and the number of instances supported, see Software Compatibility (see page 18).

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)

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
- 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 20)
  - Post-Installation Tasks (see page 33)

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 9.3.0 runs with CA Anomaly Detector 9.3.0, but not with previous versions of CA Anomaly Detector. 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:

Program	Supported Version	Required?
CA Anomaly Detector installation that you intend to upgrade *	9.2.1	Required for upgrades

Program	Supported Version	Required?
CA Performance Center	2.4/2.3	Required in a deployment that includes CA Performance Center
CA NetQoS Performance Center	6.1.205 SP2/6.1.194	Required in a deployment that includes CA NetQoS Performance Center
CA Network Flow Analysis (1 instance)	9.3.0	Required to enable AD 9.3.0 operation
CA NetVoyant (1-2 instances)	7.1 SP7	Optional data source for anomaly monitoring
CA Application Delivery Analysis (SuperAgent) (1-2 instances)	10.1	Optional data source for anomaly monitoring
CA Unified Communications Monitor (1-2 instances)	3.7	Optional data source for anomaly monitoring

* If your pre-upgrade CA Anomaly Detector version is earlier than 9.2.1, upgrade to version 9.2.1 before you begin.

Co-Installation

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

- Installation Order: Follow the order shown in the table.
- 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.
- With Other Related Software: You cannot install CA Anomaly Detector on a server that hosts any of the following software:
  - CA Performance Center
  - CA NetQoS Performance Center
  - CA Application Delivery Analysis (SuperAgent)
  - CA Unified Communications Monitor
  - CA NetVoyant

Components Installed on a Single Server	Supported?
CA Anomaly Detector (AD) with no other related software	Yes
NFA stand-alone (Harvester + NFA console software) + AD	Yes

Components Installed on a Single Server	Supported?
NFA console + AD	Yes
NPC + the current release of NFA or AD	No
CA PC + AD or any NFA component	No
ADA (SA), UCM, or NetVoyant + AD	No

Installation and Upgrade Prerequisites

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

- (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 Performance Center deployment, including the locations and IP addresses for all related components.
- Verify that you have access to the servers that host Performance Center and the products 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.

Additional Prerequisite Tasks

- Download the installation and upgrade files (see page 21).
- Installation Order (see page 22): If you co-install the product with CA Network Flow Analysis, install or upgrade CA Network Flow Analysis before CA Anomaly Detector.
- Check the nsas database (see page 22).
- Stop the services (see page 23).
- Back up the database and restart the services (see page 25).

Download the Installation and Upgrade Files

Copy the files to the installation server whether you plan to install the software locally or remotely. This ensures that you have access to the files

1. Get the files for installing or upgrading the components:
   a. Log in to ca.support.com.
   b. Navigate to the Download Center at ca.support.com: For example, select Download Center from the Support menu in the left pane.
   c. Select the following navigation options:
      - Select a Product: Select 'CA Network Flow Analysis - MULTI-PLATFORM' to display the links for the NFA console, Harvester (Windows), Harvester (Linux), DSA, and CA Anomaly Detector installation and upgrade ISO files.
      - Select a Release: Select '9.3'
      - Select a Gen level: Select '0000'
   d. Download the ISO files from the Product Components list that is displayed.

      Note: An ISO file is an archive file that contains the contents of an optical disk. Each ISO file contains the files for installing or upgrading the component named in the file link.
2. Perform one of the following tasks:
   - Burn the ISO files to a CD-ROM or DVD.
   - Extract the contents of the ISO files by using an ISO image software application. Many ISO image applications are free.
3. Extract the appropriate files to the installation servers:
   - CA Anomaly Detector server
     - ADSetup9.3.0.exe
   - For co-installing on an NFA standalone server, also extract:
     - NFHarvesterSetup9.3.0.exe
     - RAConsoleSetup9.3.0.exe
   - For co-installing on an NFA console server (distributed deployment), also extract:
     - RAConsoleSetup9.3.0.exe

Installation Order

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 install CA Anomaly Detector on the server that hosts a stand-alone CA Network Flow Analysis deployment or the NFA console server in a distributed deployment.

Check the Database

We recommend that you check the nsas database before upgrading. You can use the mysqlcheck command to verify that the database tables are set up properly. The check can correct some types of problems and can help you avoid an upgrade failure.

This topic describes how to run the check. If the CA Anomaly Detector software is on an upgraded NFA console server or stand-alone server, you may have already checked the nsas database as part of the earlier upgrade.

Checking large database tables can be time-consuming. If you run the check on an entire database, each table in the database is locked in read-only state sequentially. The table that is being checked is unavailable for write operations.

You can run mysqlcheck without stopping the MySQL service.

Follow these steps:

1. Log in to the installation server as a user with administrator privileges.
2. Check the nsas database: Enter one of the following mysqlcheck commands at a command or shell prompt:
   - To check the tables in all of the applicable databases on the server (reporter, harvester, poller, data-retention, and nsas databases):

     ```
     mysqlcheck --all-databases
     ```

   - To check all of the tables in a single database:

     ```
     mysqlcheck --databases db_name
     ```

     Example:

     ```
     mysqlcheck --databases nsas
     ```

     where:

     db_name = Name of the database to check

     You do not need to specify the path to the database. The mysqlcheck command finds any or all databases that use the default port (port 3308).

The command checks each table, attempts to repair any problems, then analyzes and optimizes the table. The return text lists the database tables that were checked and reports the status for each one.

If the table passed the check, "OK" follows the table name. If a warning is returned and is followed by "OK," the problem was resolved. If unresolved errors occur, contact CA Support.

Next: Stop the services, then back up the databases, as described in the following topics.

Stop the Services

To prepare for backing up the database, stop the services on the installation server for CA Anomaly Detector.

Follow these steps:

1. Log in as a user who has administrator privileges for the product.
2. Open the Services window: Click Start, Control Panel, Administrative Tools, Services.
3. If CA Anomaly Detector is installed on the CA Network Flow Analysis stand-alone server, stop the CA NFA Harvester service and wait 15 minutes.

   Data file processing completes.
4. Stop the remaining services, as listed in the following table.

Service	Stand-Alone NFA with AD	NFA Console with AD	Anomaly Detector (not co-installed)
CA NFA Collection and Poller Webservices	Yes		
CA NFA Data Retention	Yes		
CA NFA DNS/SNMP Proxies	Yes		
CA NFA File Server	Yes	Yes (3-tier)	
CA NFA Harvester	Yes		
CA NFA Host Resolver Service	Yes (if AD is co-installed)	Yes (if AD is co-installed)	Yes
CA NFA Hunter Tracker Service	Yes (if AD is co-installed)	Yes (if AD is co-installed)	Yes

Service	Stand-Alone NFA with AD	NFA Console with AD	Anomaly Detector (not co-installed)
CA NFA Poller	Yes		
CA NFA Reaper	Yes		
CA NFA RibSource	Yes	Yes	Yes
NetQoS MySql	Yes	Yes	Yes
NetQoS NQMySql	Yes		
NetQoS Reporter Manager Service	Yes	Yes	
NetQoS Reporter/Analyzer General Services	Yes	Yes	
NetQoS Reporter/Analyzer Pump Service	Yes	Yes	
NetQoS Reporter/Analyzer Query Services	Yes	Yes	
NetQoS Reporter/Analyzer Watchdog	Yes	Yes	
NetQoS ReporterAnalyzer Report Service	Yes	Yes	

5. If CA Anomaly Detector is installed on the CA Network Flow Analysis stand-alone server or NFA console server, check the following directory:

   <install_path>\Netflow\datafiles\HarvesterWork

   When the HarvesterWork directory is empty, you can back up the database.

   The services are restarted automatically during the upgrade process.

For more information about the services and databases, see the following topics:

- *CA Network Flow Analysis Upgrade Guide* - The "Back Up the Databases and Restart the Services" topic describes the databases.
- *CA Network Flow Analysis Administrator Guide* - The "Service Management" topic describes the services for CA Network Flow Analysis and CA Anomaly Detector.

Back Up the Databases and Restart the Services

Before you upgrade, back up the databases and files that are listed in the following table.

Important:

- Run backups concurrently. If you restore data from backups that have different timestamps, problems can result. Ensure that your backed-up data files are timestamped with the same hour.
- Store backups to a remote location to guard against the possibility of a hardware or operating system failure on the main server. For example, back up the databases to an administrative share or mapped network drive.

Follow these steps:

1. Log in as a user who has administrator privileges for the product.
2. Connect to the server:
   a. Open a Remote Desktop session.
   b. Initiate a Terminal Services or VNC session to the installation server.
3. Copy each target directory and file to a remote location.
4. Restart the services.

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 19). 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 20). The ISO file contains the ADSetup9.3.0.exe file--the Installation or upgrade program for CA Anomaly Detector.

   Copy the ADSetup9.3.0.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 19).
4. Double-click the ADSetup9.3.0.exe file in Windows Explorer.

   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 nonsystem 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 Mysql

Next: Complete the post installation tasks (see page 33).

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 19). 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 has administrator privileges for CA Network Flow Analysis.
2. Verify that the ISO file is downloaded (see page 20). The ISO file contains the ADSetup9.3.0.exe file--the Installation or upgrade program for CA Anomaly Detector.

   Copy the ADSetup9.3.0.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 19).
4. Double-click the ADSetup9.3.0.exe file in Windows Explorer.

   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 Mysql
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 33).

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 33).

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 33).

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 33).

Uninstall CA Anomaly Detector

CA Anomaly Detector 9.3.0 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 has administrator privileges for CA Network Flow Analysis.
2. Perform the following preliminary steps:
   - Open the Services window and verify that the NetQoS Mysql service is running. If the service is not running, start it.
   - If the installation server is also used to host Performance Center, back up your data and configuration files, as described in the *CA Network Flow Analysis Administrator Guide* and the *Installation Guide* for your version of Performance Center.
   - 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 40).

This section contains the following topics:

Register CA Anomaly Detector

To display CA Anomaly Detector data in views, you must add CA Anomaly Detector as a data source for Performance Center.

Follow these steps:

1. Display the Data Source List page:
   a. Log in to the 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 (CA PC) or Data Source List (NPC).
2. Click Add (CA PC) or New (NPC).

   The dialog for adding a data source opens.

3. 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 28).

     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 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.

4. 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.

5. 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 tasks 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 36).

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) (see page 36)
- Add Products to Monitor (CA NetQoS Performance Center) (see page 37)

Add Products to Monitor (CA Performance Center)

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 at the bottom 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.

   The Anomaly Detector page shows the NFA console 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 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 18).

   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)

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 with the View Monitored Products tab displayed.
3. Click New.

   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.

   The Monitored Products page now 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 all of the monitored products 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 18).

   The list of monitored products page is updated to show 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) (see page 39)
- Enable the Monitored Products (CA NetQoS Performance Center) (see page 39)

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 40).

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)

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 40).
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)

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 Best Practices: Slow Harvester Rollout (see page 40).

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)

- CA Anomaly Detector server to other servers that host data sources (NFA console, CA Application Delivery Analysis (SuperAgent), CA NetVoyant, and CA Unified Communications Monitor):
  - TCP 3308 (MySQL server)
- CA Anomaly Detector server ports (outbound):
  - UDP 514 (Syslog alerting)
  - UDP 162 (SNMP alerting)
- Performance Center server to the CA Anomaly Detector server:
  - TCP/HTTP 80, if http is used for communication
  - TCP/HTTPS 443, if https is used for communication
- CA Performance Center to the CA Anomaly Detector server:
  - TCP 8681, which CA PC uses to request data for the views

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 14).

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.

Probability Threshold	Number of Anomalies Reported
Lower	More
Higher	Less

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 views when you edit a sensor configuration (see page 43). 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.

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

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

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:
   a. Log in to the 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 (CA PC) or Data Source List (NPC).
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 14).

   - 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 42).

     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 settling up Syslog or SNMP trap alert targets, see Configure Alert Targets (see page 45).

   - 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 in the Anomaly Detector page views. You can also receive anomaly information by configuring the alerts to trigger Syslog messages, SNMP trap messages, or both.

- Syslog Alerts (see page 45)
- SNMP Trap Alerts (see page 50)

Set Up 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 45).

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 47)
- Example of an Anomaly Cluster Message (see page 48)

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 in the Anomaly Detector page views, 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.

Follow these steps:

1. Display the Data Source List page:
   a. Log in to the 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 (CA PC) or Data Source List (NPC).
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 15).
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.X.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 43).

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|Anom
alyCluster|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%. OptionalROUTERINFOVALUE
```

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.

Set Up 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: Select Admin, Data Sources.

   The page for managing data sources opens: Manage Data Sources (CA PC) or Data Source List (NPC).

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 45).

     For information about what constitutes a correlated anomaly, see Correlated Anomalies on page 7 (see page 15).

8. Click Save.

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

Chapter 4: CA Anomaly Detector Views

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

This section describes the predefined CA Anomaly Detector views in the Performance Center Console. For more information about using Performance Center, see the help for your version of Performance Center.

Display Predefined Views

The predefined CA Anomaly Detector views are displayed in the Performance Center Console. To see the views, open the Anomaly Detector page:

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

To see the views, your user account must have a role that gives you access to the view menu. User account settings are managed in the Performance Center Console, as described in the *Administrator Guide* for your version of Performance Center.

Customize Predefined Views

To change the reporting time frame for the views on the Anomaly Detector 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 period forward or backward by a day.
- Click the start date or end date and select a new 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 view 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 view pages, see the *Administrator Guide* for your version of Performance Center.

Set a Custom Time Frame

You can select a different time frame for the data shown in the current dashboard or view page. You can select the day, the start time, and the end time using the time period selectors.

Follow these steps:

1. Navigate to a dashboard or view page.
2. Click the date links in the upper-left corner of the dashboard page to open the calendar panes.
3. Select the beginning day and ending day of the new time period on the calendar panes.
4. Click the hours or minutes links to specify the beginning and ending times of the new time period.
5. Click Set.

   The custom time frame is applied to all of the views on the dashboard or page.

Change the View Settings

You can change several settings for a view. This topic describes how to open the dialog for editing view settings. The options that are available vary.

Follow these steps:

1. Open the page that contains the view you want to modify.
2. (Optional) Change the time frame (see page 54).

3. Open the dialog for editing the view settings:
   - (CA PC) Click the Edit icon  in the view title bar and select Edit from the menu.
   - (NPC) Click the View icon  next to the view name and select Edit from the menu.

     The settings dialog opens.
4. (Optional) Change any of the following options:
   - Title: Change the name that is shown in the view title bar.
   - Context Settings: Make a selection in the All Groups tree.

     The context determines which data can be reflected in the view.

     The Context Settings option is not applicable to the Anomaly Trend view or the Anomaly Drill-In table.
   - Apply Changes:
     - My Current Session: Apply the changes to the view during the current Performance Center session, but revert to the usual settings at the next log-in.
     - My User Account: Apply the changes to the view whenever you log in with the current user account.
     - (CA PC) For All Tenant Users: Apply the changes to the view for all user accounts in the current tenant.
5. Click Save (CA PC) or OK (NPC) to save your changes.

   The settings dialog closes. The view reflects your changes.

Zoom In to Narrow the Time Frame

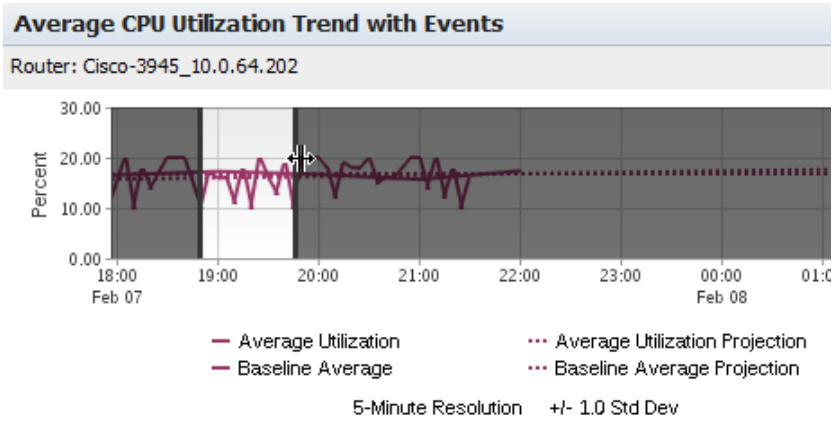
This topic describes how to zoom in to narrow the time frame for a trend chart in the CA Performance Center Console. This option is not applicable to trend charts in the CA NetQoS Performance Center Console.

You can look more closely at the data points from a small range by using the zoom feature. The ability to "zoom in" on a time frame is available for views that contain trend (line) charts. The feature is not available for bar charts, tables, or gauges.

Follow these steps:

1. Navigate to a dashboard page.
2. (Optional) Change the time frame, if necessary.
3. Select a view that contains a line chart.

   Note: You cannot zoom in on a bar chart, table, or gauge.
4. Click and drag, using the mouse to select an area of the chart.



   Select an area that spans at least 30 minutes. Black lines appear to indicate a valid selection.

   When you release the mouse button, the custom time period you selected is applied to the current view.
5. (Optional) Click Undo, just below the view, to return to the previous time frame.

   The view is refreshed. The previous time period is now applied to the view.
6. (Optional) Click Apply to Dashboard.

   The dashboard page is refreshed. The new time period is now applied to all views on the current dashboard page.

Predefined Views

The following types of predefined views are available:

Built-in CA Anomaly Detector Views on the Anomaly Detector Page:

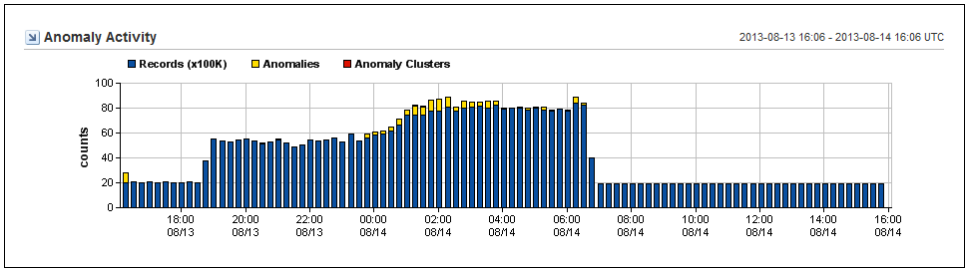
- Anomaly Activity (see page 57)
- Anomaly Detector Overall Status (see page 58)
- Enterprise-Wide Correlated Anomalies (see page 61)
- Top Anomalies by Host (see page 59)
- Top Anomalies by Interface (see page 60)
- Top Enterprise-Wide Network Anomalies (see page 58)

Additional View that You Can Add to a Custom Page:

- Enterprise-Wide Anomalies (see page 63)

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 in comparison to all of the records that were processed.



The example graphic shows the number of records in the hundreds of thousands (Y-Axis) over a 24-hour period. Activity is shown along the X-Axis each time the program runs (usually at 15-minute intervals).

You can edit the following view settings:

- Time frame for all views on the page, as described in Set a Custom Time Frame (see page 54).

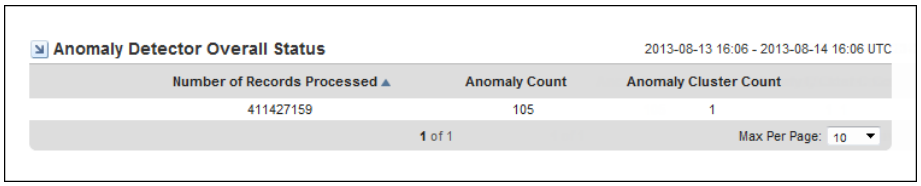
  By changing the time frame for the page, you can discover when the issue began and look for patterns.

- View title and context.

This view is included by default on the Anomaly Detector page in the Performance Center Console. The example graphic shows the view as it appears in the CA NetQoS Performance Center Console.

Anomaly Detector Overall Status

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



You can edit the following view settings:

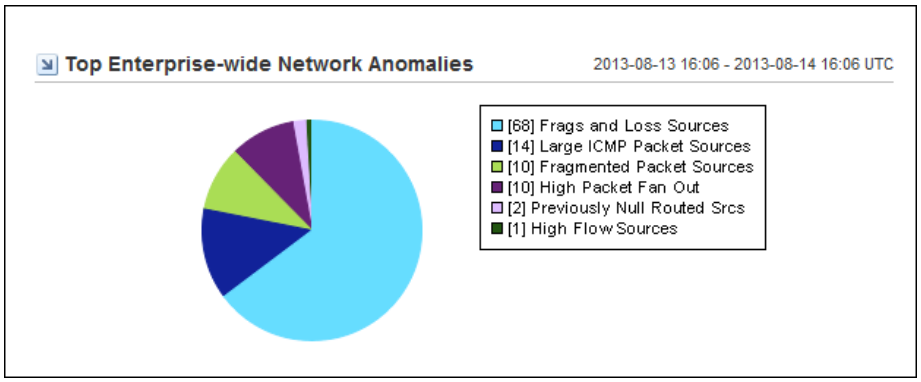
- Time frame for all views on the page, as described in Set a Custom Time Frame (see page 54)
- View title and context

This view is included by default on the Anomaly Detector page in the Performance Center Console. The example graphic shows the view as it appears in the CA NetQoS Performance Center Console.

Top Enterprise-Wide Network Anomalies

The Top Enterprise-Wide Network Anomalies pie chart shows the top 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.



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 69).

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 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.

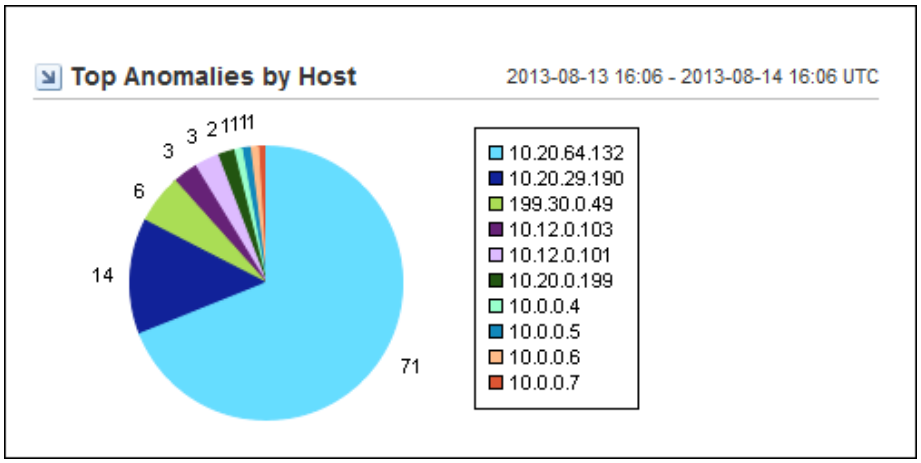
You can edit the following view settings:

- Time frame for all views on the page, as described in Set a Custom Time Frame (see page 54)
- View title and context

This view is included by default on the Anomaly Detector page in the Performance Center Console. The example graphic shows the view as it appears in the CA NetQoS Performance Center Console.

Top Anomalies by Host

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



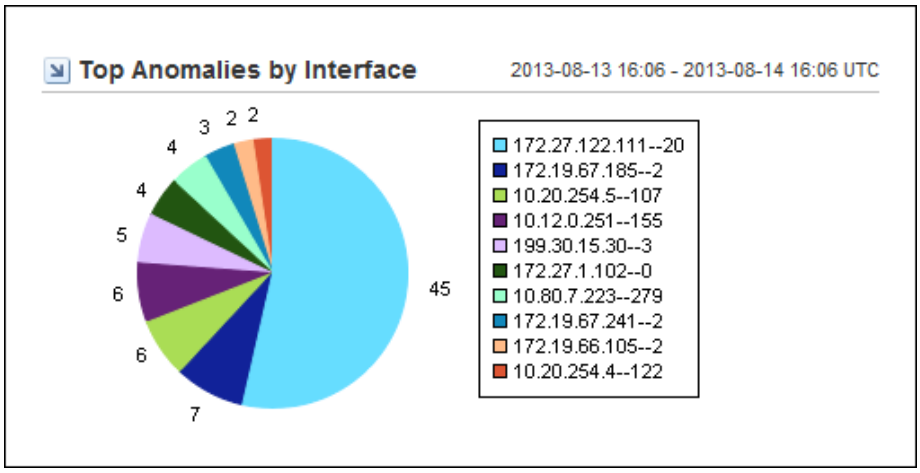
You can edit the following view settings:

- Time frame for all views on the page, as described in Set a Custom Time Frame (see page 54)
- View title and context

This view is included by default on the Anomaly Detector page in the Performance Center Console. The example graphic shows the view as it appears in the CA NetQoS Performance Center Console.

Top Anomalies by Interface

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



You can edit the following view settings:

- Time frame for all views on the page, as described in Set a Custom Time Frame (see page 54)
- View title and context

This view is included by default on the Anomaly Detector page in the Performance Center Console. The example graphic shows the view as it appears in the CA NetQoS Performance Center Console.

Enterprise-Wide Correlated Anomalies

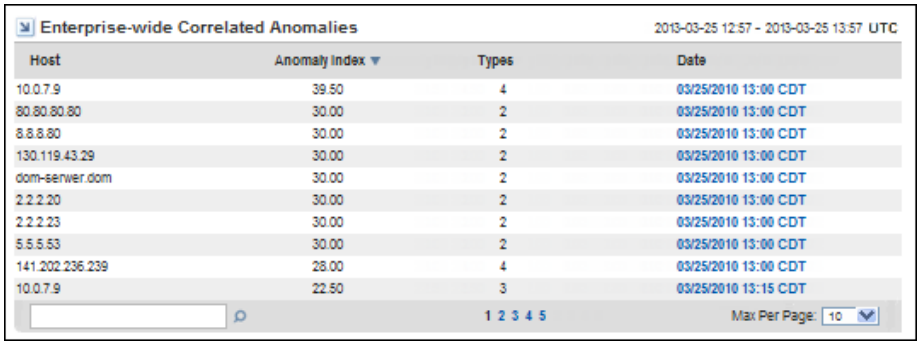
The Enterprise-Wide Correlated Anomalies table summarizes the anomalous behaviors that are most likely to be damaging to the network. This view identifies network locations that you can begin investigating if you suspect malicious activity.

Anomaly clusters are better indicators for problems than single anomalies. Many types of 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 in a fan-out behavior. In a fan-out behavior, seemingly unrelated devices are affected and unexpected traffic is produced from multiple sources.

Correlation is performed by using an algorithm that considers the typical patterns for each type of monitored network traffic.

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.



You can change the time frame for this view and all views on the page, as described in Set a Custom Time Frame (see page 54).

You can edit the following view settings:

- Time frame for all views on the page, as described in Set a Custom Time Frame (see page 54)
- View title and context

This view is included by default on the Anomaly Detector page in the Performance Center Console. The example graphic shows the view as it appears in the CA NetQoS Performance Center Console.

The 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 an interface. The program attempts to resolve the hostname of the 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 anomaly correlation algorithm compares each particular behavior to the typical patterns for the network traffic type. The higher the index number, the more severe the issue is.

Types

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

Date

The date and time of the first correlated anomaly on the host.

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 intervals.

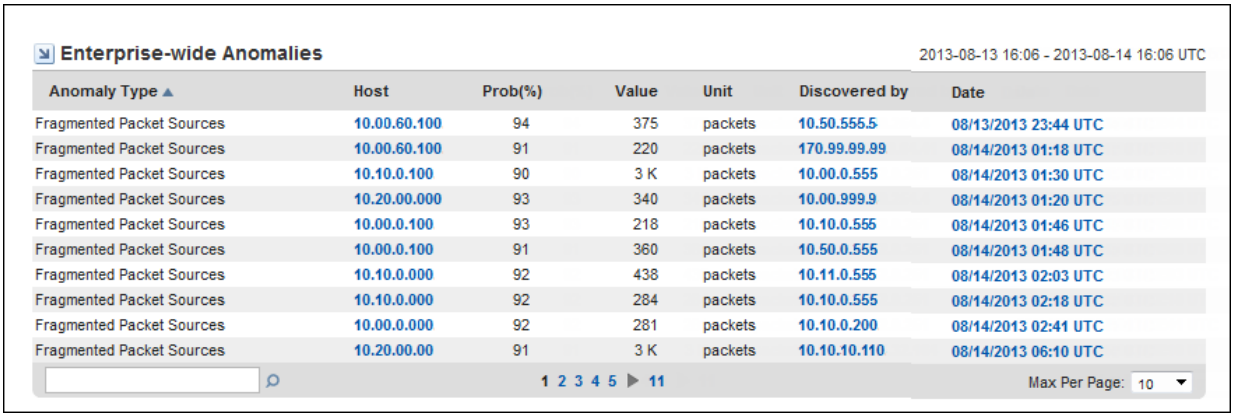
Date Link

Click the *Date* link In the Enterprise-Wide Correlated Anomalies view to go to the Anomaly Detector Drill-In table (see page 64).

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 problem behavior or for initiating troubleshooting procedures to stem an attack. The view provides more detailed information about the anomalies you see in other views. This view also identifies network locations to begin investigating.



Enterprise-wide Anomalies 2013-08-13 16:06 - 2013-08-14 16:06 UTC

Anomaly Type ▲	Host	Prob(%)	Value	Unit	Discovered by	Date
Fragmented Packet Sources	10.00.60.100	94	375	packets	10.50.555.5	08/13/2013 23:44 UTC
Fragmented Packet Sources	10.00.60.100	91	220	packets	170.99.99.99	08/14/2013 01:18 UTC
Fragmented Packet Sources	10.10.0.100	90	3 K	packets	10.00.0.555	08/14/2013 01:30 UTC
Fragmented Packet Sources	10.20.00.000	93	340	packets	10.00.999.9	08/14/2013 01:20 UTC
Fragmented Packet Sources	10.00.0.100	93	218	packets	10.10.0.555	08/14/2013 01:46 UTC
Fragmented Packet Sources	10.00.0.100	91	360	packets	10.50.0.555	08/14/2013 01:48 UTC
Fragmented Packet Sources	10.10.0.000	92	438	packets	10.11.0.555	08/14/2013 02:03 UTC
Fragmented Packet Sources	10.10.0.000	92	284	packets	10.10.0.555	08/14/2013 02:18 UTC
Fragmented Packet Sources	10.00.0.000	92	281	packets	10.10.0.200	08/14/2013 02:41 UTC
Fragmented Packet Sources	10.20.00.00	91	3 K	packets	10.10.10.110	08/14/2013 06:10 UTC

1 2 3 4 5 ▶ 11 Max Per Page: 10

You can edit the following view settings:

- Time frame for all views on the page, as described in Set a Custom Time Frame (see page 54)
- View title and context

This view is not included by default on the Anomaly Detector page in the Performance Center Console. To see this view, add it to a page or to a new custom page. The graphic shows an example view in the CA NetQoS Performance Center Console.

The view provides the following information about anomalous network behavior:

Anomaly Type

The type of anomalous behavior. For a description of each anomaly type that you can enable for monitoring, see Sensors Overview (see page 69).

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

For more information about the probability algorithm, see Probability Thresholds (see page 14).

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.

Links and Detail Pages

Links are included in some views to help kick-start anomaly troubleshooting. Links take you to preconfigured reports or to a general page of additional detail. The following views include links:

- Enterprise-Wide Correlated Anomalies
- Enterprise-wide Anomalies
- Anomaly Detector Drill-In

Date Link

Click the *Date* link to go to the Anomaly Trend view (see page 66). This view shows the value and probability of the anomaly over time.

Discovered by Link

Click a *Discovered By* link to view details. The link destination is determined by the type of anomaly:

- CA Network Flow Analysis Anomalies: Router or interface page in the Performance Center Console
- Anomalies from other data sources: Main page for the originating product

Host Link

Click a *Host* link to go to more granular information about the device that has the anomaly. Clicking a Host link may be the first step in troubleshooting the anomaly.

Host link destinations are based on the sensor type. For many CA Network Flow Analysis sensors, the Host link opens the page for defining a Flow Forensics report in the NFA console, which has pre-populated report filters.

Anomaly Drill-In

If you drill into an anomaly cluster from the Enterprise-wide Correlated Anomalies view (see page 63), the Anomaly Drill-In table opens. For each anomaly, the table lists the probability, value, originating router and interface, and the time that the anomaly occurred. You can use the Date 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 behavior. For a description of each anomaly type that you can enable for monitoring, see Sensors Overview (see page 69).

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 an interface. The program attempts to resolve the hostname of any IP address and displays that name in this field.

Host Link

Click a *Host* link to go to more granular information about the device that has the anomaly. Clicking a Host link may be the first step in troubleshooting the anomaly.

Host link destinations are based on the sensor type. For many CA Network Flow Analysis sensors, the Host link opens the page for defining a Flow Forensics report in the NFA console, which has pre-populated report filters.

Prob(%)

The calculated likelihood that flagged packet flows are truly anomalous.

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

For more information about the probability algorithm, see Probability Thresholds (see page 14).

Value

The value that triggered the report of anomalous behavior, 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.

Discovered by Link

Click a *Discovered By* link to view details. The link destination is determined by the type of anomaly:

- CA Network Flow Analysis Anomalies: Router or interface page in the Performance Center Console
- Anomalies from other data sources: Main page for the originating product

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.

Date Link

Click the *Date* link to go to the Anomaly Trend view (see page 66). This view shows the value and probability of the anomaly over time.

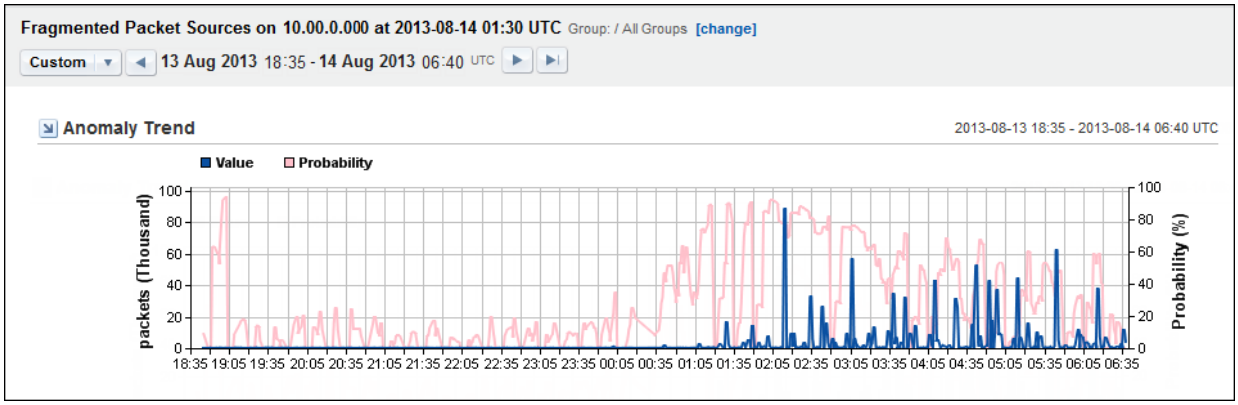
You can edit the following view settings:

- Time frame, as described in Set a Custom Time Frame (see page 54).
- View title.

Note: If your deployment includes CA Performance Center, you can use the Zoom feature to interactively limit the time frame (see page 56).

Anomaly Trend

The Anomaly Trend view shows the value and probability of the anomaly over time. To display this trend chart, click a link in the Date column in either the Anomaly Drill-in view (see page 65) or the Enterprise-Wide Anomalies view (see page 63). The following example shows an Anomaly Trend view in the CA NetQoS Performance Center Console.



The 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 patterns over days, weeks, or months.

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.

You can edit the following view settings:

- Time frame, as described in Set a Custom Time Frame (see page 54)
- View title

Note: If your deployment includes CA Performance Center, you can use the Zoom feature to interactively limit the time frame (see page 56).

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 41).

CA Network Flow Analysis Sensors

CA Network Flow Analysis provides information to help you understand how application traffic affects your network performance. CA Network Flow Analysis enables you to see which applications are using bandwidth, who is using the bandwidth, and when. This knowledge helps you can timely and cost-effective decisions to optimize network performance.

When you add CA Network Flow Analysis as a data source for Performance Center, the Harvesters are added automatically as possible data sources for CA Anomaly Detector. Special considerations apply when you enable Harvesters as data sources, as described in Best Practices: Slow Harvester Rollout (see page 40).

Sensors:

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 usual. Such packets may indicate tunneling attempts or data exfiltration. Data ex-filtration is a network security violation in which a user discreetly attempts to send data from an internal network to an external location.

Troubleshooting a Large DNS Packet Sources Alert

If you suspect data ex-filtration, click the link for the offending host to investigate the suspected user by using a Flow Forensics report in the NFA console. You can also use other packet-inspection tools 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 ex-filtration. Data ex-filtration is a network security violation in which a user discreetly attempts to off-load data from an internal network to an external location.

Troubleshooting a Large ICMP Packet Sources Alert

If you suspect data ex-filtration, click the link for the offending host and investigate the suspected user in a Flow Forensics report in the NFA console. You also can use a packet-inspection tool 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 Flow Forensic report in the NFA console.

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.

Frags 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.

Sensors:

Incoming Discard Rate (see page 79)
Incoming Error Rate (see page 80)
Dropped Packets (see page 80)
Buffer Misses (see page 80)

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.

Sensors:

Voice Call Fan Out (see page 81)
Voice Call DoS (see page 81)
Voice Server Distress (see page 81)

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 abandons 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.

Sensors:

Retransmission Time (see page 82)
Refused Sessions (see page 83)
Packet Load (see page 83)

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 heart beat 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

D

E

F

G

H

I

T

U

V

W