CA Network Flow Analysis

Installation Guide

Release 9.3.0

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.

Related Documentation

CA provides a full set of technical documentation in the CA Network Flow Analysis Documentation Bookshelf. Access the bookshelf by clicking the Help link in the CA Network Flow Analysis user interface. You can open the guides in PDF and HTML format from the Documentation Bookshelf.

The documentation may have been updated since its release. To get the latest CA Network Flow Analysis documentation updates and localized documentation, download the Bookshelf from CA Support.

The documentation set for CA Network Flow Analysis 9.3.0 includes the following guides:

- *Online help*: Assistance for Administrators and operators, available through the Help link in the user interface.
- *Administrator Guide*: How to set up and maintain CA Network Flow Analysis.
- *Operator Guide*: How to use the NFA console to create, view, and manage reports.
- *Installation Guide*: How to install the software and perform one-time configuration tasks.
- *Upgrade Guide*: How to upgrade the software and perform initial configuration tasks.
- *Release Notes*: Summary of CA Network Flow Analysis enhancements, fixes, and open issues.
- *CA Anomaly Detector Guide:* How to install, upgrade, configure, and use CA Anomaly Detector.
- *CA Anomaly Detector Release Notes:* Overview of the product, system requirements/recommendations, and features.

The product PDFs are in the following directory:
<install_path>\Reporter\NetQoS.ReporterAnalyzer.WebSite\help\en_US\NFA_Bookshelf\Bookshelf_Files\PDF

To view the documentation PDF files, make sure that Adobe Reader is installed.

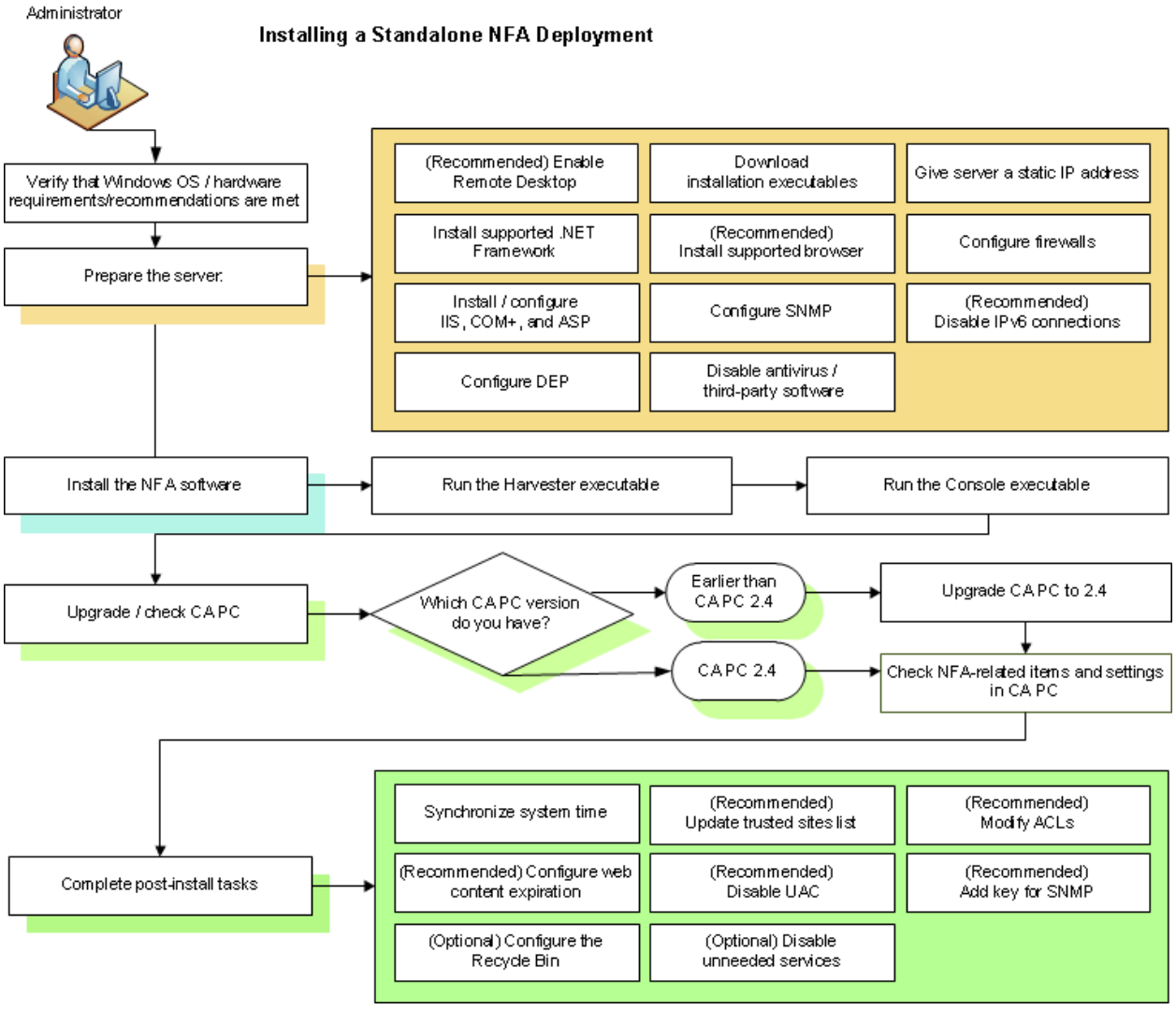
Contents

Chapter 1: Introduction

This guide describes how to install CA Network Flow Analysis 9.3.0, as illustrated in the following workflows.

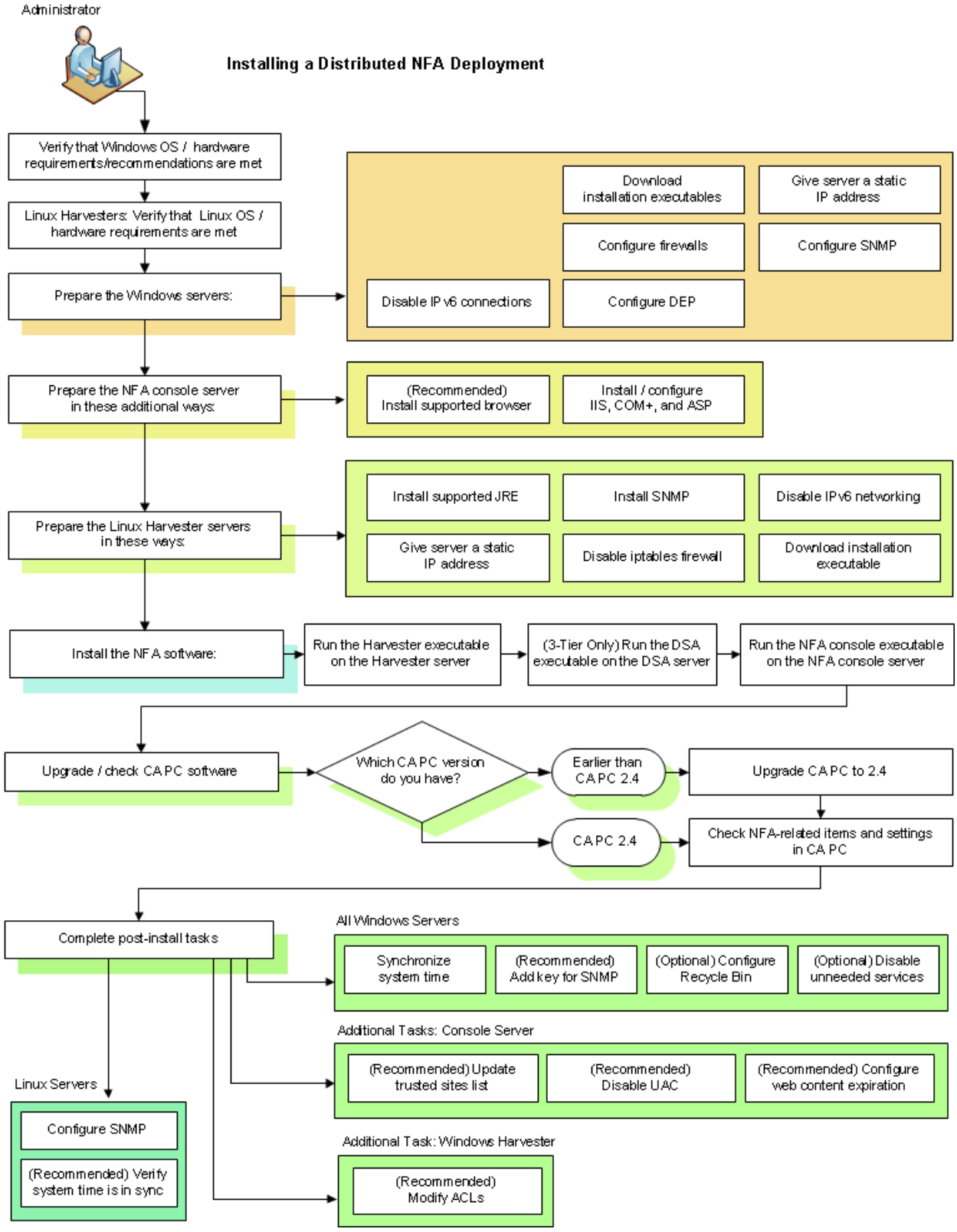
Workflow for Installing a Stand-Alone Deployment

Use the following diagram as a general checklist for installing a stand-alone deployment of CA Network Flow Analysis. See the related topics for complete information about the steps.



Workflow for Installing a Distributed Deployment

Use the following diagram as a general checklist for installing a distributed deployment of CA Network Flow Analysis. See the related topics for complete information.


Administrator
Installing a Distributed NFA Deployment
Verify that Windows OS / hardware requirements/recommendations are met
Linux Harvesters: Verify that Linux OS / hardware requirements are met
Prepare the Windows servers:
Download installation executables
Give server a static IP address
Configure firewalls
Configure SNMP
Disable IP v6 connections
Configure DEP
Prepare the NFA console server in these additional ways:
(Recommended) Install supported browser
Install / configure IIS, COM+, and ASP
Prepare the Linux Harvester servers in these ways:
Install supported JRE
Install SNMP
Disable IPv6 networking
Give server a static IP address
Disable iptables firewall
Download installation executable
Install the NFA software:
Run the Harvester executable on the Harvester server
(3-Tier Only) Run the DSA executable on the DSA server
Run the NFA console executable on the NFA console server
Upgrade / check CA PC software
Which CA PC version do you have?
Earlier than CA PC 2.4
Upgrade CA PC to 2.4
CA PC 2.4
Check NFA-related items and settings in CA PC
Complete post-install tasks
All Windows Servers
Synchronize system time
(Recommended) Add key for SNMP
(Optional) Configure Recycle Bin
(Optional) Disable unneeded services
Additional Tasks: Console Server
(Recommended) Update trusted sites list
(Recommended) Disable UAC
(Recommended) Configure web content expiration
Linux Servers
Configure SNMP
(Recommended) Verify system time is in sync
Additional Task: Windows Harvester
(Recommended) Modify ACLs

Chapter 2: Download the Installation Files

Copy the installation/upgrade files to the installation server so you are certain to 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: 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 one of the available ISO files 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 free ISO image applications are available.
3. Extract the appropriate files to the installation servers:
   - Stand-alone servers:
     - NFHarvesterSetup9.3.0.exe
     - RAConsoleSetup9.3.0.exe
   - Windows Harvester servers in distributed deployments:
     - NFHarvesterSetup9.3.0.exe
   - Linux Harvester servers in distributed deployments:
     - NFHarvesterSetup9.3.0.bin
   - NFA console servers in distributed deployments:
     - RAConsoleSetup9.3.0.exe

- DSA servers in three-tier distributed deployments:
  - DSASetup9.3.0.exe

You can install or upgrade the software locally or remotely.

Chapter 3: System Recommendations and Requirements

This section describes the hardware and operating system recommendations and requirements for the CA Network Flow Analysis component servers.

If you purchase hardware from CA Technologies, all components are delivered with the operating system and security settings already configured. Use the topics in this guide to verify the settings or update them to suit the needs of your organization.

If you purchase software only, configure and secure the operating system as described in this guide.

Before you begin, copy any files that you need to the installation server. After you secure the operating system, you may not be able to access the share folders that contain the files.

This section contains the following topics:

Windows Operating System Requirements

Microsoft Windows servers that host CA Network Flow Analysis components must be running Microsoft Windows Server 2008 R2, Standard edition on a 64-bit processor. In addition, the servers must meet the following requirements:

- The most recent service pack and all important updates installed
- English, Chinese (Simplified), French (France), or Japanese language

  Appropriate language packs installed on all servers for localized deployments
- Minimum display resolution of 1024x768 (XGA)
- Server configured as described in:
  - Prepare the Windows Servers (see page 19)
  - Post-Installation Tasks (see page 47)

Notes:

- Before you begin the tasks in this guide, log in to a Windows server as a user who is a member of the Administrators group or in to a Linux server with root privileges.
- CA Network Flow Analysis 9.3.0 supports installation on servers with IPv4 addresses. Installation is not supported at this time on servers with IPv6 addresses.
- Install and register the Windows software.
- CA Network Flow Analysis 9.3.0 supports installation and upgrade on servers with IPv4 addresses, but not IPv6 addresses.
- We recommend that you configure a single NIC (network interface card) on each server.
- The requirements and recommendations in this section apply to both physical and virtual deployments.

Windows Server Hardware

In a *distributed* deployment, the CA Network Flow Analysis components are installed on separate servers.

A *stand-alone server* is a single server that is used for installing all of the CA Network Flow Analysis components.

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.

Notes:

- The recommended specifications described here apply to both physical and virtual deployments. The specifications represent an optimal configuration, such as the configuration of CA appliances that are currently shipping. You can run CA Network Flow Analysis successfully on configurations that do not meet these specifications, although your performance may vary.
- Performance is improved by running the software and the operating system on separate drives. It is possible to install and run the software and operating system on the same drive, however.

The following recommended specifications apply to dedicated servers that are used to install one or more CA Network Flow Analysis components:

Stand-alone or NFA console server

- 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 40 GB for the operating system
- Partition on any drive that contains 41 GB for the installation/upgrade files and at least 200 GB of available space for data

Harvester server

- Two 2.26-GHz quad-core processors
- 12 GB RAM
- Six 300-GB, 10,000-RPM SAS hard drives in RAID 5 configuration
- 1-Gb Ethernet port
- Partition for the C: drive that contains 40 GB for the operating system
- Partition on any drive that contains 41 GB for the installation/upgrade files and 1 TB of available space for data

Data Storage Appliance (DSA) server (3-tier architecture only)

- 2.26-GHz quad-core processor
- 12 GB RAM
- Six 300-GB, 10,000-RPM SAS hard drives in RAID 5 configuration
- 1-Gb Ethernet port
- Partition for the C: drive that contains 40 GB for the operating system
- Partition on any drive that contains 41 GB for the installation/upgrade files and 1 TB of available space for data

Linux Server Hardware and Operating System

For a distributed deployment, CA Network Flow Analysis supports running the Harvester on dedicated Linux servers that meet the following system requirements:

- Red Hat Enterprise Linux 5.5 or 5.6 on a 64-bit processor
- English, Chinese (Simplified), French (France), or Japanese language

  Appropriate language packs installed on all servers for localized deployments

We recommend that Linux Harvester servers meet the following specifications:

- Two 2.26-GHz quad-core processors
- 12 GB RAM

- Six 300-GB, 10,000-RPM SAS hard drives in RAID 5 configuration
- 1-Gb Ethernet port
- Root partition that contains 40 GB of available space
- Partition for CA Network Flow Analysis that contains the following amounts of available space:
  - 41 GB for the installation/upgrade files
  - 1 TB for data

If you do not have enough available space in the /tmp directory and you cannot configure it, relocate the directory. Export the IATEMPDIR environment variable (for the Install Anywhere temporary directory) to set a new location, and select a directory with sufficient space.

Notes:

- CA Network Flow Analysis 9.3.0 supports installation on servers with IPv4 addresses. Installation is not supported at this time on servers with IPv6 addresses.
- The specifications described in this section apply to both physical and virtual deployments.

Chapter 4: Preparing Windows Servers

This section contains the following topics:

Prepare the Windows Servers

Before you begin the installation, verify that the following conditions are met. Failure to meet these requirements and recommendations can result in data loss, increased down time, software conflicts, or installation failure.

Notes:

- If you use CA NetQoS Performance Center, verify that a supported version is installed in your deployment (see page 48). Install a supported version of Performance Center on a separate server after you install CA Network Flow Analysis
- Stop other programs from running during the installation or upgrade.
- When you apply Windows updates, restart all servers to ensure that the updates are applied.
- Ensure that no one else is logged in to the server during the installation or upgrade.

Complete the following tasks on each Windows server:

Stand-Alone Server	Distributed NFA Console Server	Distributed Harvester Server	Distributed 3-Tier DSA Server
■ If possible, meet Windows hardware recommendations (see page 16)			
■ Meet Windows operating system requirements (see page 15)			
■ Download the installation files (see page 13)			
■ Assign a static IP address to each server. Set the Harvester server IP address to match the flow export destination that is assigned to each router.			

Stand-Alone Server	Distributed NFA Console Server	Distributed Harvester Server	Distributed 3-Tier DSA Server
■ Install the supported version of .NET Framework (see page 22) *			
■ (Recommended) Enable Remote Desktop Connection to allow remote access			
■ (Recommended) Install a supported browser (see page 21) **			
■ Configure the firewall (see page 22)			
■ Install IIS, COM+, and ASP (see page 25) **			
■ Configure SNMP (see page 27) **			
■ (Recommended) Disable IPv6 connections (see page 29)			
■ Configure DEP (see page 30)			
■ Disable the following third-party software: Antivirus, server monitoring, and maintenance software until the installation is complete. If you enable antivirus scans later, exclude the CA Network Flow Analysis installation path and its subdirectories.			

* If this requirement is not met, the installation program either does not open or does not complete successfully.
** If the server fails to pass the check for this requirement, a warning message opens.

General Notes:

- Stop other programs from running during the installation or upgrade.
- When you apply Windows updates, restart all servers to ensure that the updates are applied.
- Ensure that no one else is logged in to the server during the installation or upgrade.

Localization Notes:

- To support non-Latin characters such as Japanese and Simplified Chinese, any command line clients that you use for installation must be configured for UTF-8 encoding. If UTF-8 encoding is not enabled, these characters may not display properly.
- The appropriate language packs are required for localized deployments.
- Regional Settings must use a period (.) to indicate a decimal value. If your deployment is localized to French, change the decimal symbol to a period in the Region and Language: Customize Format dialog.

Web Browser Support

For client systems that are used to log into the NFA console: We recommend Microsoft Internet Explorer version 8. Other browsers or browser versions may work with the NFA console, but have not been tested.

For installation systems: If you install a browser, install Microsoft Internet Explorer version 8.

Required/Optional	Browser Support	Servers to Configure
Browser Required	Internet Explorer 8 recommended	Systems that are used to log into the NFA console
Browser Optional	Internet Explorer 8 required if a browser is installed	Installation servers

To set up CA Network Flow Analysis and work with data in the CA Performance Center Console, use Internet Explorer with Compatibility View turned off. You can use Internet Explorer in the NFA console with Compatibility View turned on or off.

If Internet Explorer Developer Tools are installed, you can use F12 to access Compatibility View options for the current browser session:

1. Press F12.

   A new pane opens in the lower half of the window.

2. Click the Browser Mode item on the main menu.
3. Select the Internet Explorer option that does not contain the phrase "Compatibility View."

Notes:

- For more information about browser versions, see the *Readme*.
- For information about setting up the browser on the CA NetQoS Performance Center Console server, see the topic "Set Up Internet Explorer" in the CA NetQoS Performance Center Installation Guide.

Install .NET Framework

Install .NET Framework 3.5.1 on all of the Windows servers, logged on as a user who is a member of the Administrators group.

If the .NET Framework software is missing, a prerequisite check causes the installation or upgrade program to exit.

Required/Optional	Servers to Configure
Required	All servers

Firewall Configuration

For CA Network Flow Analysis to work properly in a firewall-protected environment, certain ports must be open. The following topics summarize the ports that must be open to allow communication among the CA Network Flow Analysis components. To perform these tasks, log in as a user who is a member of the Administrators group.

- Stand-alone system (see page 22)
- Two-tier distributed deployment (see page 23)
- Three-tier distributed deployment (see page 24)

Ports to Open for a Stand-Alone System

Open the following ports for a stand-alone system to allow CA Network Flow Analysis communications to function properly.

From	To	Port [Function]
NFA console	Outbound	■ TCP 25 [SMTP email reports] ■ UDP 53 [DNS]
Harvester	Routers (SNMP interface, read-only)	■ UDP 161 [SNMP polling]
Harvester	Trap destination	■ UDP 162 [traps]
Router	Harvester	■ UDP 9995 [flow]
Administrators and operators	NFA console	■ TCP/HTTP 80 [UI access and SNMP web services] ■ TCP/HTTP 8381 [Single Sign-On]

From	To	Port [Function]
CA PC / NPC Console	NFA console	■ TCP/HTTP 80 [device and interface synchronization with CA PC / NPC] ■ TCP 8681 [data import for NFA views in CA PC / NPC]
Administrators	Each server	■ TCP 3389 [Remote Desktop, if Remote Desktop is used] ■ TCP 5800, 5801, 5900, 5901 [VNC, if VNC is used]

Ports to Open for a Two-Tier Distributed Deployment

Two-Tier Distributed Deployment

NFA console and Harvesters on separate servers, but no DSA

Open the following ports in a two-tier distributed deployment to allow communication among the NFA console, Harvesters, and other elements.

From	To	Port [Function]
NFA console	Outbound	■ TCP 25 [SMTP email reports] ■ UDP 53 [DNS]
NFA console	Harvester	■ TCP 3307 [CA MySQL] ■ TCP 3308 [MySQL] ■ TCP 8066 [SOAP web service calls] ■ TCP 8080 [File web server port for collecting Harvester files] ■ UDP 161 [Watchdog service]
Harvester	Routers (SNMP interface, read-only)	■ UDP 161 [SNMP polling]
Harvester	Trap destination	■ UDP 162 [traps]
Router	Harvester	■ UDP 9995 [flow]
Administrators and operators	NFA console	■ TCP/HTTP 80 [UI access and SNMP web services] ■ TCP/HTTP 8381 [Single Sign-On]
CA PC / NPC Console	NFA console	■ TCP/HTTP 80 [device and interface synchronization with CA PC / NPC] ■ TCP 8681 [data import for NFA views in CA PC / NPC]

From	To	Port [Function]
Administrators	Each server	■ TCP 3389 [Remote Desktop, if Remote Desktop is used] ■ TCP 5800, 5801, 5900, 5901 [VNC, if VNC is used]

Ports to Open for a Three-Tier Distributed Deployment

Three-Tier Distributed Deployment

NFA console, Harvester, and DSA components on separate servers

Open the following ports in a three-tier distributed deployment to allow communication among the NFA console, Harvesters, DSAs, and other elements.

From	To	Port [Function]
NFA console	Outbound	■ TCP 25 [SMTP email reports] ■ UDP 53 [DNS]
NFA console	Harvester	■ TCP 3307 [CA MySQL] ■ TCP 3308 [MySQL] ■ TCP 8066 [SOAP web service calls] ■ TCP 8080 [File web server port for collecting Harvester files] ■ UDP 161 [Watchdog service]
NFA console	DSA	■ TCP 3307 [CA MySQL] ■ TCP 3308 [MySQL] ■ UDP 161 [Watchdog service]
Harvester	Routers (SNMP interface, read-only)	■ UDP 161 [SNMP polling]
Harvester	Trap destination	■ UDP 162 [traps]
DSA	NFA console	■ TCP 3308 [MySQL] ■ TCP 8080 [File Web Service, which retrieves files from the NFA console without using a file share]
Router	Harvester	■ UDP 9995 [flow]
Administrators and operators	NFA console	■ TCP/HTTP 80 [UI access and SNMP web services] ■ TCP/HTTP 8381 [Single Sign-On]

From	To	Port [Function]
CA PC / NPC Console	NFA console	■ TCP/HTTP 80 [device and interface synchronization with CA PC / NPC] ■ TCP 8681 [data import for NFA views in CA PC / NPC]
Administrators	Each server	■ TCP 3389 [Remote Desktop, if Remote Desktop is used] ■ TCP 5800, 5801, 5900, 5901 [VNC, if VNC is used]

Install IIS, ASP, and COM+

Use the steps in this topic to install the following required components on a stand-alone server or NFA console server:

- IIS
- ASP
- IIS 6 Management Compatibility
- COM+ Network Access

Required/Optional	Servers to Configure
Required	Stand-alone, Console

Follow these steps:

1. Log in as a user who has administrator privileges for CA Network Flow Analysis.
2. Select Start, Administrative Tools, Server Manager.

   The Server Manager window opens.
3. Expand the Roles list in the Console tree on the left.
4. Add the IIS role service:
   a. Click the Application Server link under Roles in the Console tree on the left.

      The Application Server view opens in the right pane.
   b. Click the Add Role Services link in the Role Services section.

      The Add Role Services wizard opens to the Select Role Services page.
   c. Select the Web Server (IIS) Support check box.
   d. Click Add Required Role Services in the confirmation message that opens.

      The Web Server (IIS) Support option is highlighted on the Select Role Services page.

5. Add the COM+ role service:
   a. Select the COM+ Network Access check box.
   b. Click Add Required Role Services in the confirmation message that opens, then click Next.

      The Web Server (IIS) page of the Add Role Services wizard opens.
6. Enable IIS 6 Management Compatibility:
   a. Click Next again.

      A list of role services opens.
   b. Select the IIS 6 Management Compatibility check box in the Management Tools section.
   c. Click Next.

      The Confirm Installation Selections page summarizes your actions and displays related messages.
7. Install the IIS and COM+ role services and options you selected:
   a. Click Install.

      The Results page opens when the installation or upgrade is complete.
   b. (Optional) Click 'Print, e-mail, or save the installation/upgrade report, review the information,' then close the page.
   c. Click Close.

      The Results page closes.
8. Add and install the ASP role service:
   a. Click the Web Server (IIS) link under Roles in the Console tree.

      The Web Server (IIS) view opens in the right pane.
   b. Click the Add Role Services link in the Role Services section.

      The Add Role Services wizard opens to the Select Role Services page.
   c. Select the ASP check box under Application Development in the list and click Next.

      The Confirm Installation Selections page summarizes your actions and related messages.
   d. Click Install.

      The Results page opens when the installation or upgrade is complete.

e. (Optional) Click 'Print, e-mail, or save the installation/upgrade report, review the information,' then close the page.

f. Click Close.

The Installation Results page closes.

9. Exit from the Server Manager window.

Configure SNMP on Windows Servers

The Simple Network Management Protocol (SNMP) service is required by the Watchdog services. Use the steps in this topic to configure the SNMP service on the Windows servers in your deployment.

Required/Optional	Servers to Configure
Required	All servers

Follow these steps:

1. Log in as a user who has administrator privileges for CA Network Flow Analysis.
2. Open the Server Manager window: Select Start, Administrative Tools, Server Manager.
3. Install the SNMP services:
   a. Click Features in the left pane.

   The Server Manager window displays a list of the installed features.

   b. Click Add Features in the right pane.

   The Add Features wizard opens and shows the selected and available features.

   c. Select the SNMP Services check box.

   A confirmation message appears.

   d. Click Add Required Features.

   The Confirm Installation Services page identifies the features to be installed and displays messages.

   e. Click Install.

   The Installation Results page opens when the installation or upgrade is complete.

4. Close the Server Manager window:
   a. Click Close.

      A message asks whether you want to restart the server now.

   b. Click Yes.

      After the server restarts, the Features view in the Server Manager window shows the newly installed feature.

5. Display the list of community names for the SNMP service:
   a. Select Start, Administrative Tools, Services.

      The Services window opens.

   b. Right-click the SNMP Service and select Properties.

      The SNMP Service Properties dialog opens.

   c. Select the Security tab.

6. Verify that the appropriate community name is in the "Accepted community names" list. The default community name is "public."
7. If the appropriate community name is not listed, add it:
   a. Click Add.

      The SNMP Service Configuration dialog opens.

   b. Set the following options:
      - Community rights: Select Read Only.
      - Community Name: Enter **public** or a custom community name. Use the same community name throughout the CA Network Flow Analysis deployment:

        snmpd.conf file on each Linux server

        SNMP service on each Windows server

        Watchdog Settings page of the NFA console

   c. Click Add.

      The SNMP Service Configuration dialog closes. The SNMP Service Properties dialog displays the new name in the "Accepted community names" list.

8. Save your changes and exit:
   a. Click OK in the SNMP Service Properties dialog.

      Your changes are saved and the dialog closes.

   b. Select File, Exit in the Services window.

      The Services window closes.

Disable IPv6 Connections on Windows Servers

This release does not support connections to IPv6-formatted addresses. This topic describes how to set up Windows Server 2008 systems so that they do not connect to IPv6 addresses. If connection to IPv6-formatted addresses is enabled, data collection fails.

Required/Optional	Servers to Configure
Recommended	All servers

The instructions are based on the assumption that each server has a single network interface card, which is the recommended configuration.

Follow these steps:

1. Log in as a user who has administrator privileges for CA Network Flow Analysis.
2. Open the Network Connections window:
   a. Select Start, Control Panel.
   b. Click Network and Internet in the Control Panel.
   c. Click Network and Sharing Center in the Network and Internet window that opens.
   d. Click "Change adapter settings" on the left side of the Network and Sharing Center window that opens.

      The Network Connections window opens and shows the currently configured connections.
3. Right-click the connection.
4. Select Properties from the menu.

   The Properties dialog opens.
5. Clear the 'Internet Protocol Version 6 (TCP/IPv6)' check box, if it is selected.
6. Click OK.

   The dialog closes and your changes are saved.
7. Select Organize, Close in the Network Connections window.

   The window closes.

Configure Data Execution Prevention (DEP)

Data Execution Prevention (DEP) helps to prevent code executing from data pages. This topic describes how to configure the appropriate DEP policy level.

Required/Optional	Servers to Configure
Required	All servers

Follow these steps:

1. Log in as a user who has administrator privileges for CA Network Flow Analysis.
2. Open the Control Panel and click the System link.
3. Click the Advanced tab in the System Properties dialog that opens.
4. Click Settings.
5. Click the Data Execution Prevention tab in the Performance Options dialog that opens.
6. Select "Turn on DEP for essential Windows programs and services only."
7. Save your settings and exit:
   a. Click OK in the Performance Options dialog.
   b. Click OK in the System Properties dialog.

      A message opens and informs you that you must restart your system to implement the new settings.
8. (Optional) Restart your system before you install or upgrade the software.

   If you proceed without restarting the system, the prerequisite test displays a warning about the DEP configuration.

Chapter 5: Preparing Linux Servers

This section contains the following topics:

Prepare the Linux Servers

Before you begin the installation, verify that the following conditions are met. Failure to comply with these requirements can result in data loss, increased down time, software conflicts, or a failed installation.

- System Requirements: Verify that the installation servers meet the requirements and recommendations (see page 17).
- Verify that each of the Harvester Linux servers is ready for the installation by:
  - Assigning a static IP address to each server. Set the Harvester server IP address to match the flow export destination for each router.
  - Disabling the following third-party software: Antivirus, server monitoring, and maintenance software. If you enable antivirus scans later, exclude the CA Network Flow Analysis installation path and its subdirectories
  - Installing SNMP (see page 32)

    If SNMP is not running, the installation program displays a warning. You can bypass the warning and install SNMP later.
  - Disabling the iptables firewall (see page 34)
  - Disabling IPv6 networking (see page 33)

General Notes:

- Stop other programs from running during the installation.
- Ensure that no one else is logged in to the server during the installation.

Localization Notes:

- To support non-Latin characters such as Japanese and Simplified Chinese, any command line clients that you use for installation must be configured for UTF-8 encoding. If UTF-8 encoding is not enabled, these characters may not display properly.
- The appropriate language packs are required for localized deployments.
- Regional Settings must use a period (.) to indicate a decimal value. If your deployment is localized to French, change the decimal symbol to a period in the Region and Language: Customize Format dialog.
- Polling fails if DNS resolution is not configured. For more information, see the Readme.

Install SNMP on Linux Servers

To configure a Linux server for a Harvester, complete the following main tasks:

- If Net-SNMP if it is not already present on the installation or upgrade server, install it as described in this topic.
- Finish SNMP configuration after the installation or upgrade is complete: (see page 49)
  - Set up the Net-SNMP configuration file.
  - Configure SNMP to start automatically on boot.
  - Start the snmpd service.

Verify that Net-SNMP is present on the server and install it if necessary. Net-SNMP is required to support Watchdog functionality.

Follow these steps:

1. Open the Linux Package Manager and look for listings that contain "net-snmp."

   If you do not find any "net-snmp" listings, Net-SNMP is not installed.
2. Get and install Net-SNMP if it is not installed. For example, you can get Net-SNMP from the Linux Package Manager.

Disable IPv6 Networking on Linux Servers

Disable IPv6 networking on each Linux server that has a Harvester installed.

Note: Complete this task before you add the Harvester in the NFA console. If IPv6 is enabled when you add a Harvester in the NFA console, the Harvester automatically binds with an IPv6-format address, which prevents CA Network Flow Analysis from receiving its data.

To disable IPv6 networking, modify the following files:

- Kernel driver configuration file, modprobe.conf, which is located by default in the /etc directory
- RHEL networking configuration file, network, which is located by default in the /etc/sysconfig directory

Follow these steps:

1. Make sure that you are logged in with root privileges.
2. Edit the modprobe.conf file:
   a. Open the /etc/modprobe.config file in a text editor.
   b. Append the following line:
      `install ipv6 /bin/true`
   c. Save and close the file.

      The modprobe.conf file is now configured so that when the system attempts to load the IPv6 kernel module, it executes the command 'true' instead of loading the module. The 'true' command performs no action.
3. Edit the network file:
   a. Open the /etc/sysconfig/network file in a text editor.
   b. Update or add the following lines to match the text strings shown:
      `NETWORKING_IPV6=no`
      `IPV6INIT=no`
   c. Save and close the file.
4. Reboot the server:
   `reboot`

5. Verify that IPv6 is disabled:

   a. Enter the following command at a terminal:
   `lsmod | grep ipv6`

   If the command returns no output, the IPv6 kernel module is not running: It has been removed successfully.

   b. Enter the /sbin/ifconfig command:
   `/sbin/ifconfig`

   Check the output to verify that it contains only IPv4 addresses and no IPv6 addresses.

Disable the iptables Firewall

We recommend that you disable the iptables firewall and stop the iptables service on each Linux server that has a Harvester installed. Disabling iptables ensures that all the required ports are open and that the iptables firewall does not impact performance adversely.

Note: If your enterprise requires the use of iptables, make sure that you open all of the applicable firewall ports in the firewall configuration list (see page 22). In addition make sure that you have full localhost-to-localhost access. This step is required because CA Network Flow Analysis uses RMI (Remote Method Invocation) access.

Complete the following steps to disable all levels of iptables and allow communication among CA Network Flow Analysis components.

Follow these steps:

1. Log in as root or with a sudo user account.
2. Run the following commands in a command prompt window:

   ```
   service iptables stop

   chkconfig iptables off

   chkconfig –-list |grep iptables
   ```

3. Review the output of the last command to make sure that all of the iptables levels are off, as shown in the following example:

   ```
   iptables 0:off 1:off 2:off 3:off 4:off 5:off 6:off
   ```

Chapter 6: Install the Software

This section contains the following topics:

Install the Components on a Stand-Alone Server

A *stand-alone* server is a single server that hosts the NFA console and the Harvester. Complete the steps in this topic to install all of the components on a single Windows server or virtual machine.

Follow these steps to complete the Harvester phase:

1. Verify that the installation server is prepared as described in Prepare the Windows Servers (see page 19).
2. Log in as a user who has administrator privileges for CA Network Flow Analysis.
3. Start the Harvester phase of the installation: Double-click the NFHarvesterSetup9.3.0.exe file.
4. Verify that the appropriate language is selected, then click OK.

   The Welcome screen opens.
5. Click Next.

   The CA NFA Harvester License Agreement screen opens.
6. Review and accept the license agreement:
   a. Read the license agreement and scroll down.
   b. If you want to continue under the terms of the license agreement, click the option to accept it. This option is activated when you scroll to the bottom.
   c. Click Next.

      Prerequisite tests run to look for problems on the server. If a problem is found, an error message opens. A critical problem causes the program to exit. A Pre-requisite Check Warning message or other warning message opens for non-critical problems, which gives you the option to make corrections now or after the installation or upgrade is complete.
7. Review the test results in the Pre-requisite Check Warning message, if it opens:
   a. Correct problems now or wait until the program finishes. For more information about the warnings, see the Troubleshooting (see page 61) section.
   b. Click OK to close the message.

8. Verify or specify the installation directory:
   a. (Optional) Click Choose in the Choose Install Folder screen to change the installation location.

      The default location is C:\CA\NFA. We recommend that you install CA Network Flow Analysis components on a drive that is dedicated to CA Network Flow Analysis--not the operating system drive. The NFA console will be installed to the same directory that you choose for the Harvester.

   b. Click Next when the installation path setting is correct.

      The Pre-Installation Summary screen opens.
9. Review the pre-installation information, then click Install.

   The Installing Harvester screen opens. When the installation is complete, the Install Complete screen opens and reports any errors that occurred.
10. (Optional) If errors occurred during the installation, see the following log for details:

    <install_path>\Harvester_Install_<timestamp>.log (where <timestamp> is the time the log was created)
11. Click Done in the Install Complete screen.

    The Harvester installation program closes.

Follow these steps to complete the NFA console phase:

1. Start the NFA console installation software: Double-click the RAConsoleSetup9.3.0.exe file in Windows Explorer.

   The language selection screen opens.
2. Verify that the appropriate language is selected, then click OK.

   The Welcome screen opens.
3. Click Next in the Welcome screen.

   The NFA Console License Agreement screen opens.
4. Review and accept the license agreements:
   a. Read the NFA console license agreement and scroll down.
   b. If you want to continue, click the option to accept the license agreement This option is activated when you scroll to the bottom.
   c. Click Next.

      The Third-Party License Agreement screen opens.
   d. Read the third-party license agreement and scroll down.
   e. If you want to continue, click the option to accept the third-party license agreement. This option is activated when you scroll to the bottom.

5. Click Next.

   Prerequisite tests run. If an error message opens that requires attention, see Troubleshooting (see page 61).

6. Review the test results in the Pre-requisite Check Warning message, if it opens:

   a. Fix any noncritical problems now or wait until the program finishes.

   b. Click OK to close the message.

      The Singlebox Confirmation message opens and asks you to confirm that you want a stand-alone deployment.

7. Review the information and click OK.

   The Pre-Installation Summary screen opens.

8. Review the pre-installation information, then click Install.

   The Installing NFA screen opens. When the NFA console installation is complete, the Install Complete screen opens.

   a. Select "Yes, restart my system."

   b. Click Done.

      Installation is complete.

Next: Complete the post-installation tasks. (see page 47)

Install a Distributed Deployment

In a distributed deployment, CA Network Flow Analysis components are distributed among multiple servers. The topics in this section describe how to install the software on each component server.

To install a two-tier distributed deployment, complete the following procedures:

- Install the Harvester on a Windows Server (see page 38) or
- Install the Harvester on a Linux Server (see page 39)
- Install the NFA Console (see page 43)

To install a three-tier distributed deployment, complete the following procedures:

- Install the Harvester on a Windows Server (see page 38)
- Install the DSA Server (see page 41)
- Install the NFA Console (see page 43)

Note: The steps in these topics assume that you follow the recommended installation order: Harvesters first, DSAs second (if any), then the NFA console last.

Install the Harvester on a Windows Server

Distributed deployments have separate servers for the NFA console and the Harvester. Complete the steps in this topic to install the Harvester on a dedicated Windows server or virtual machine.

In a distributed deployment, each Harvester is on a separate server. To install a Harvester on a dedicated Windows server or virtual machine, complete the steps in this topic. These steps apply to a two-tier or three-tier distributed deployment.

Follow these steps:

1. Verify that the server is prepared as described in Prepare the Windows Servers (see page 19).
2. Log in as a user who has administrator privileges for CA Network Flow Analysis.
3. Start the installation: Double-click the NFHarvesterSetup9.3.0.exe file in Windows Explorer on the Harvester server.

   The language selection screen opens.
4. Verify that the appropriate language is selected, then click OK.

   The Welcome screen opens.
5. Click Next in the Welcome screen.

   The License Agreement screen opens.
6. Review and accept the license agreement:
   a. Read the license agreement and scroll down.
   b. If you want to continue under the terms of the license agreement, click the option to accept it. This option is activated when you scroll to the bottom.
   c. Click Next.

      Prerequisite tests are run to identify problems on the server. If a problem is found, an error message opens, as described in Troubleshooting (see page 61).
7. If the Pre-requisite Check Warning message opens, review the test results:
   a. Correct problems now or wait until the program finishes. For more information about the warnings, see the Troubleshooting (see page 61) section.
   b. Click OK to close the message.

      Once the server passes the required checks and you close any noncritical messages, the Choose Install Folder screen opens and displays the default root installation path.

8. Verify or specify the installation directory:

   a. (Optional) Click Choose in the Choose Install Folder screen to change the installation location.

      The default location is C:\CA\NFA. We recommend that you install CA Network Flow Analysis components on a drive that is dedicated to CA Network Flow Analysis--not the operating system drive. The NFA console will be installed to the same directory that you choose for the Harvester.

   b. Click Next when the installation path setting is correct.

      The Pre-Installation Summary screen opens.

9. Review the pre-installation information, then click Install.

   The Installing Harvester screen opens. When the installation is complete, the Install Complete screen opens and reports any errors that occurred.

10. (Optional) If errors occurred during the installation, see the following log for details:

    <install_path>\Harvester_Install_<timestamp>.log (where <timestamp> is the time the log was created)

11. Click Done in the Install Complete screen.

    The Harvester installation program closes.

Next: Repeat these steps to install a Harvester on another server or install the NFA console (see page 43).

Install the Harvester on a Linux Server

A two-tier distributed deployment of CA Network Flow Analysis may include one or more Linux Harvester servers. To install the Harvester software on a dedicated Linux server or virtual machine, complete the steps in this topic.

Follow these steps:

1. Verify that the server is prepared as described in Prepare the Linux Servers (see page 31).
2. Log in to the Harvester server as root.

   You can install the software locally or remotely--for example, by using ssh when you are logged in with root privileges.

   Note: If you do not have root access, use an account with sudo privileges.

3. Open a command prompt window.

4. Run the following command to change the ulimit for the open files limit:
   `ulimit -n ulimit_number`

   Example:
   `ulimit -n 65536`

5. Prepare the installation/upgrade file for execution:

   a. Log in to the Harvester server as root.

      You can install or upgrade the software locally or remotely--for example, by using ssh when you are logged in with root privileges. If you do not have root access, use an account with sudo privileges.

   b. Execute the chmod command on the file in a terminal window:
      `chmod u+x NFHarvesterSetup9.3.0.bin`

   c. (Optional) Execute the list command to verify that the file is executable:
      `ls -al`

      The file permission settings are displayed.

6. Run the installation or upgrade software:

   ./NFHarvesterSetup9.3.0.bin

   The language selection screen opens.

7. Verify that the appropriate language is selected, then click OK.

   The Welcome screen opens.

8. Click Next in the Welcome screen.

   The License Agreement screen opens.

9. Review and accept the license agreement:

   a. Read the license agreement and scroll down.

   b. If you want to continue under the terms of the license agreement, click the option to accept it. This option is activated when you scroll to the bottom.

   c. Click Next.

      Prerequisite tests are run to identify problems on the server. If a problem is found, an error message opens, as described in Troubleshooting (see page 61).

10. If the Pre-requisite Check Warning message opens, review the test results:

    a. Correct problems now or wait until the program finishes. For more information about the warnings, see the Troubleshooting (see page 61) section.

    b. Click OK to close the message.

       Once the server passes the required checks and you close any noncritical messages, the Choose Install Folder screen opens and displays the default root installation path.

11. Verify or specify the installation directory:

    a. (Optional) Click Choose in the Choose Install Folder screen to change the installation location.

       We recommend that you install CA Network Flow Analysis components on a partition that is dedicated to CA Network Flow Analysis. The NFA console will be installed to the same directory that you choose for the Harvester.

    b. Click Next when the installation path setting is correct.

       The Pre-Installation Summary screen opens.

12. Review the pre-installation information, then click Install.

    The Installing Harvester screen opens, which shows the progress. When the installation is complete, the Install Complete screen opens and reports any errors that occurred.

13. (Optional) If errors occurred during the installation, see the following log for details:

    <install_path>/Harvester_Install_<timestamp>.log (where <timestamp is the time the log was created)

14. Click Done in the Install Complete screen.

    The Harvester installation program closes.

Next: Repeat these steps to install a Harvester on another server or install the console (see page 43).

Install the DSA in a Three-Tier Distributed Deployment

In a three-tier distributed deployment, each DSA is installed on a separate server. To install a DSA on a dedicated Windows server or virtual machine, complete the steps in this topic.

Follow these steps:

1. Verify that the following conditions are met:
   - The server is prepared as described in Prepare the Windows Servers (see page 19).
   - The CA Network Flow Analysis software is installed on the Harvester servers.
2. Log in as a user who has administrator privileges for CA Network Flow Analysis.
3. Start the installation: Double-click the DSASetup9.3.0.exe file in Windows Explorer.

   The language selection screen opens.

4. Verify that the appropriate language is selected, then click OK.

   The License Agreement screen opens.

5. Review and accept the license agreement:
   a. Read the license agreement and scroll down.
   b. If you want to continue under the terms of the license agreement, click the option to accept it. This option is activated when you scroll to the bottom.
   c. Click Next.

      Prerequisite tests run to look for problems on the server. If a problem is found, an error message opens. A critical problem causes the program to exit. A Pre-requisite Check Warning message or other warning message opens for non-critical problems, which gives you the option to make corrections now or after the installation or upgrade is complete.
6. Review the test results in the Pre-requisite Check Warning message, if it opens:
   a. Correct problems now or wait until the program finishes. For more information about the warnings, see the Troubleshooting (see page 61) section.
   b. Click OK to close the message.

      Once the server passes the required checks and you close any warning messages that appear, the Choose Install Folder screen opens. This screen displays the original root installation path as the default setting.
7. Verify or specify the installation directories:
   a. (Optional) Click Choose in the Choose Install Folder screen to change the installation location.
   b. Click Next when the installation path setting is correct.

      The Select a Location for the MySQL Data Directory screen opens. This screen shows the default installation path for the MySQL data directory.
   c. (Optional) Click Choose to change the MySQL installation location, which shows the default installation path for the MySQL database directory

      We recommend that you use a drive that has at least 40 GB of available space for the database.
   d. Click Next when the MySQL database path setting is correct.

      The Select a Location for the MySQL Temp Directory screen opens, which shows the default installation path for the MySQL tmp directory.
   e. (Optional) Click Choose to change the tmp directory location.
   f. Click Next when the MySQL tmp directory path setting is correct.

      MySQL is configured, then the Pre-Installation Summary screen opens.
8. Review the pre-installation information, then click Install.

   The Installing DSA screen opens. When the installation is complete, the Install Complete screen opens and reports any errors that occurred.

9. Click Done in the Install Complete screen.

   The installation program closes.

10. (Optional) Verify the following:

    - Services are running.
    - The DSA is receiving data.
    - The revision history shows that the DSA is the correct version. To display the revision history:
      - Start MySQL by entering the following command in a Command Prompt window:

        mysql

      - Display the revision history by entering the following command:

        select * from revision_info

11. (Optional) Check the DSA_Install_<timestamp> log periodically. This log is located at the install path root level--for example, in the \CA\NFA directory. Use the log to monitor the migration of the DSA database tables to the new format.

    The database table migration begins as soon as the CA NFA DSA Loader service restarts. The log lists the tables as they are migrated. Nine tables are migrated for each agent or interface. If you have many agents and an extensive amount of stored data, migration may continue for some time. Reports will have limited access to your historical (15-minute) data until the migration is complete.

Next:

- To install an additional DSA on another server, repeat these steps.
- To install the NFA console, go to the next topic (see page 43).

Install the NFA Console

Distributed deployments use separate servers for the NFA console, Harvesters, and any DSAs in the deployment. Complete the steps in this topic to install the NFA console on a dedicated Windows server or virtual machine.

Follow these steps:

1. Verify that the installation server meets the following requirements:
   - The server is prepared as described in Prepare the Windows Servers (see page 19).
   - The software is installed on the Harvester servers.
   - If you have a three-tier architecture deployment, the software is installed on the DSA servers.

2. Log in to the NFA console server as a user who has administrator privileges for the system and for CA Network Flow Analysis.
3. Start the installation: Double-click the RAConsoleSetup9.3.0.exe file in Windows Explorer on the NFA console server.

   The language selection screen opens.
4. Verify that the appropriate language is selected, then click OK.

   The Welcome screen opens.
5. Click Next.

   The License Agreement screen opens.
6. Review and accept the license agreements:
   a. Read the NFA console license agreement and scroll down.
   b. If you want to continue, click the option to accept the license agreement This option is activated when you scroll to the bottom.
   c. Click Next.

      The Third-Party License Agreement screen opens.
   d. Read the third-party license agreement and scroll down.
   e. If you want to continue, click the option to accept the third-party license agreement. This option is activated when you scroll to the bottom.
7. Click Next.

   Prerequisite tests run, as described in Troubleshooting (see page 61). If the server fails any noncritical tests, the Pre-requisite Check Warning message opens.
8. If the Pre-requisite Check Warning message opens, review the test results:
   a. Correct problems now or wait until the program finishes. For more information about the warnings, see the Troubleshooting (see page 61) section.
   b. Click OK to close the message.
9. Click Next.

   The Choose Install Folder screen opens.
10. (Optional) Click Choose to change the program installation location when prompted or enter a new path manually.

    The Select Architecture screen opens.

11. Select the architecture mode for your distributed deployment:
    - 2-tier: Choose the 2-tier mode if you do not have any DSA servers in your deployment.
    - 3-tier: Choose the 3-tier mode if you have one or more DSA servers in your deployment.

    The option determines whether the program will recognize DSA servers as part of the deployment.

    Note: Choose the architecture mode carefully. After you install the software, you cannot switch to the other architecture in a subsequent upgrade.

    The Pre-Installation Summary screen opens.
12. Review the pre-installation information, then click Next.

    The Installing NFA screen opens and installation starts. Once installation starts you cannot cancel it.

    When the program finishes, the Install Complete screen opens and reports any errors.
13. (Optional) If errors occurred, see the installation log: <install_path>\NFA_Install_<timestamp>.log.
14. Exit from the installation program:
    a. Select one of the restart options:
       - Yes, restart my system: Restart the system as soon as you click Done.
       - No, I will restart my system myself: Defer the restart to be performed manually.

    b. Click Done.

       The installation program closes. If you selected the option to restart now, the system restarts and the installation is finalized.

Next: Complete the post-installation tasks (see page 47).

Chapter 7: Post-Installation Tasks

Complete the following post-installation tasks on each of the Windows servers:

- Install Performance Center in your deployment (see page 48)
- Configure SNMP on Linux Harvester servers (see page 49)
- Exclude the following directories from real-time scans: C:\Windows\Temp and <install_path> and all its subdirectories. Real-time scans of these directories can corrupt the database.
- Do not implement drive space compression. Drive space compression can cause database losses and can degrade system performance.
- We recommend that you install Adobe Flash Player on systems with desktops that access the NFA console and install Adobe Reader on systems with desktops that access the PDF documentation.

Stand-Alone Server	Distributed NFA Console Server	Distributed Harvester Server	Distributed 3-Tier DSA Server
Synchronize system time (see page 50)			
(Recommended) Update the list of trusted internet sites (see page 51) *			
(Recommended) Modify router ACLs (see page 52) **		(Recommended) Modify router ACLs (see page 52) **	
(Recommended) Disable UAC (see page 52)			
(Recommended) Configure Web content expiration (see page 53)			
(Recommended) Create a TrapConfiguration key (see page 54)			
(Optional) Configure the Recycle Bin (see page 54)			
(Optional) Disable unneeded Windows services (see page 55)			

* Complete this task for the systems that will access the NFA console as well as the stand-alone server or NFA console server.

** In a distributed deployment, verify that the router access control lists (ACLs) are configured to enable the Harvesters to perform SNMP polling.

This section contains the following topics:

Install Performance Center

Your deployment must include either CA Performance Center or CA NetQoS Performance Center. After you install CA Network Flow Analysis, register it as a data source in the Performance Center Console. You use the Performance Center Console to perform certain administrative tasks. You also use it to view CA Network Flow Analysis data alongside data from other data sources. Until you register the product as a data source, some of the function links on the Administration page are disabled.

Verify that you have one of the following programs installed:

- CA Performance Center 2.4/2.3, installed on a Linux server that does not have a Harvester installed or
- CA NetQoS Performance Center 6.1.205 SP2/6.1.194, installed on a server that is running Windows Server 2008 R2 Standard edition

  You cannot co-locate CA Performance Center or CA NetQoS Performance Center with the current release of any CA Network Flow Analysis component or CA Anomaly Detector.

  If you uninstall CA Network Flow Analysis from a server that has any related software installed, the related software is disabled.

Required/Optional	Servers to Configure
Required	Linux CA PC server or Windows NPC server

Documentation for installing Performance Center is available from CA Support: Refer to the Bookshelf for your software version:

- *CA Performance Center Installation Guide* in the *CA Performance Center 2.4 Bookshelf*
- *CA NetQoS Performance Center Installation Guide* from the CA NetQoS Performance Center documentation

Configure SNMP on Linux Servers

To configure a Linux server for a Harvester, complete the following tasks:

- Set up the Net-SNMP configuration file.
- Configure SNMP to start automatically on boot.
- Start the snmpd service.

Required/Optional	Servers to Configure
Required	Linux Harvesters

Follow these steps:

1. Log in as root and open a shell prompt.
2. (Highly Recommended) Use the following steps to set up the Net-SNMP configuration file. This configuration file is needed for Watchdog SNMP polling.

   Note: If you have a custom (non-default) snmp configuration file at /etc/snmp/snmp.conf, you may want to skip this step and update your existing configuration file instead. In this case, consult with an administrator to update the required settings to match the settings in the example configuration file. For example, make sure the rocommunity value is set as shown in the example configuration file.

   If you use a custom community name as the rocommunity value, use the same community name throughout the CA Network Flow Analysis deployment:

   - The snmpd.conf file on each Linux Harvester server
   - SNMP service on each Windows server
   - Watchdog Settings page of the NFA console

   a. (Recommended) Back up the configuration file in /etc, for example by entering the following command:
   `cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bak`

b. Change to the Netflow directory:
```
cd <install_dir>/Netflow
```
where <install_dir> is the target directory for installing the Harvester: /opt/CA/NFA/ or a custom location

c. Copy the snmpd.conf file in the Netflow directory to the /etc/snmp directory, overwriting the existing file:
```
cp -i snmpd.conf /etc/snmp
```

d. Confirm the overwrite operation when prompted.

e. Verify that the configuration file is in place:
```
ls -l /etc/snmp/snmpd.conf
```

f. Verify that the configuration file has the correct permissions:
```
chmod 600 snmpd.conf
```

3. Configure SNMP to start automatically on every boot by entering the following command:
```
chkconfig snmpd on
```

4. Start the SNMP service in either of the following ways:

- Enter the command:
```
service snmpd start
```
- Navigate to Services in the user interface, select snmpd, Start, then click Save.

  The SNMP service starts with the community name that is defined in the snmpd file.

Synchronize System Time

Synchronize the system time among all servers that have CA Network Flow Analysis components installed, unless the system time is synchronized automatically. We also recommend that you synchronize the system time for any Linux servers in your deployment, including the server that hosts CA Performance Center.

Required/Optional	Servers to Configure
Required	All servers

This topic describes an approach for synchronizing system time on Windows Server 2008 servers.

Follow these steps:

1. Log in as a user who has administrator privileges for CA Network Flow Analysis.
2. Right-click the date or time on the right edge of the taskbar and select 'Adjust date/time.'

   The Date and Time dialog opens.
3. Click the Internet Time tab.
4. Click 'Change settings.'

   The Internet Time Settings dialog opens.
5. Select the 'Synchronize with an Internet time server' check box.
6. Select the server with which you want to synchronize. The default selection is time.windows.com.
7. Click 'Update Now.'

   The system time is synchronized with the selected server.
8. Click OK in the Internet Time Settings dialog.
9. Click OK in the Date and Time dialog.

Note: If you have collection devices in different time zones, set each device to its local time zone. Times are converted to Greenwich Mean Time (GMT).

Update the List of Trusted Internet Sites

Add the NFA console server to the list of trusted internet sites, unless your browser security settings allow unrestricted access to internet sites.

Note: The steps in this task are written for Internet Explorer 8, the recommended browser version.

Required/Optional	Servers to Configure
Recommended	Stand-alone, NFA console

Follow these steps:

1. Log in as a user who has administrator privileges for CA Network Flow Analysis.
2. Launch Internet Explorer on the NFA console server.
3. Click Tools, Internet Options.

   The Internet Options window opens.

4. Select the Security tab.
5. Click the Trusted Sites icon.
6. Click Sites.

   The Trusted Sites dialog opens.
7. Enter **https://localhost** in the "Add this Web site to the zone" field.
8. Click Add.

   Your change is saved and the site is added to the Websites list.
9. Exit:
   a. Click Close.
   b. Click OK in the Internet Options window.

      The Internet Options window closes.

Modify the Access Control Lists

We recommend that you configure the router access control lists (ACLs) to ensure that Harvesters can perform SNMP polling.

Required/Optional	Servers to Configure
Recommended	Stand-alone, Windows Harvesters

Note: If you configure flow to be exported from loopback interfaces, verify that CA Network Flow Analysis can access the IP addresses of those interfaces.

Disable User Account Control (UAC)

We recommend that you disable User Account Control (UAC) on any Windows stand-alone server or NFA console server. UAC is not fully supported for the current version of CA Network Flow Analysis. Enabling UAC on the stand-alone server or NFA console server can result in unexpected behavior.

Required/Optional	Servers to Configure
Recommended	Stand-alone, NFA console

Follow these steps:

1. Log in as a user who has administrator privileges for CA Network Flow Analysis.
2. Click Start, Control Panel, User Accounts.

   The User Accounts window opens.
3. Click "Change User Account Control settings."

   The User Account Control Settings dialog opens.
4. Move the slider bar to the bottom "Never notify" level, if it is not already at this level.

   UAC is set to be disabled for all local accounts on the server.
5. Click OK.

   You return to the User Accounts tasks page.
6. Close the window.

Configure Web Content Expiration

We recommend that you configure IIS to ensure that fresh web content is displayed. With the Expire Web Content Immediately setting enabled, the browser displays an updated page from the server rather than cached content.

Required/Optional	Servers to Configure
Recommended	Stand-alone, NFA console

Follow these steps:

1. Log in as a user who has administrator privileges for CA Network Flow Analysis.
2. Select Start, Administrative Tools, Internet Information Services (IIS) Manager.

   The Internet Information Services Manager window opens.
3. Display the options for expiring web content:
   a. Click the server name in the Connections pane.

      The server features are displayed.
   b. Double-click the HTTP Response Headers icon in the HTTP Features group.

      The window displays the current HTTP Response Headers.
   c. Click Set Common Headers in the Actions pane.

      The Set Common Headers dialog opens.

4. Select the following options:
   - "Expire Web content" check box
   - Immediately
5. Exit:
   a. Click OK to save your changes and close the dialog.
   b. Close the Internet Information Services Manager window.

Create a TrapConfiguration Key

We recommend that you create an empty TrapConfiguration key in the Windows Registry to prevent the SNMP service from logging false positive events. This topic describes how to perform this step.

Required/Optional	Servers to Configure
Recommended	All servers

Follow these steps:

1. Log in as a user who has administrator privileges for CA Network Flow Analysis.
2. Open a command prompt window.
3. Run the following command:

   ```
   reg add
   HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\TrapConf
   iguration
   ```

   If the command executes successfully, the return value is: "The operation completed successfully."

   The TrapConfiguration registry key is created in the following location: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters.

Configure the Recycle Bin

Optionally, you can configure the Recycle Bin to remove deleted files from the server immediately. The default behavior is for the system to save copies of deleted files in the Recycle Bin.

Required/Optional	Servers to Configure
Recommended	All servers

Follow these steps:

1. Log in as a user who has administrator privileges for CA Network Flow Analysis.
2. Right-click the Recycle Bin icon on the desktop.
3. Select Properties from the menu.

   The Recycle Bin Properties dialog opens.
4. Select Local Disk (C:) on the General tab.
5. Select the option that is labeled "Don't move files to the Recycle Bin. Remove files immediately when deleted."
6. Click Apply.
7. Repeat these steps for each additional drive that you want to configure.
8. Click OK.

Disable Unneeded Windows Services

You have the option to disable services that are not needed by the product. This step is designed to help secure your servers. This step is not required. If the following services are needed for another reason, do not disable them.

If you want to disable unneeded services on the Windows servers in your deployment, use the steps in this topic.

Required/Optional	Servers to Configure
Optional	Any servers (Windows)

Follow these steps:

1. Log in as a user who has administrator privileges for CA Network Flow Analysis.
2. Open the Services window: Select Start, Administrative Tools, Services.

   The Services window opens.
3. Right-click the following services and select Manual or Disabled.

   Do not select Stop or the services will restart whenever the server is rebooted.

Windows Server Services That You Can Disable

- Application Layer Gateway Service
- Application Management
- Certificate Propagation
- Distributed Link Tracking Client
- Distributed Transaction Coordinator
- DNS Client
- Function Discovery Resource Publication
- Human Interface Device Access
- IP Helper
- Link-Layer Topology Discovery Manager
- Microsoft Iscsi Initiator Service
- Multimedia Class Scheduler
- Netlogon
- Network List Service
- Network Location Awareness
- Portable Device Enumerator Service
- Print Spooler
- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Remote Registry
- Resultant Set of Policy Provider
- Secondary Logon
- Smart Card
- Smart Card Removal Policy
- Special Administration Console Helper
- SSDP Discovery
- Tablet PC Input Service
- Telephony
- Volume Shadow Copy
- Windows Audio
- Windows Audio Endpoint Builder
- Windows CardSpace
- Windows Color System
- WinHTTP Web Proxy Auto-Discovery Service
- WMI Performance Adapter

Chapter 8: Uninstalling the Software

The CA Network Flow Analysis 9.3.0 includes an option to uninstall the product, which you can use to remove CA Network Flow Analysis after an installation or upgrade.

Notes:

- The Uninstaller has no Undo option: Once you uninstall the software, you cannot restore the deleted files automatically.
- You should be able to install and uninstall the CA Network Flow Analysis software once or twice without incident. If you have ongoing problems, contact CA Support instead of installing and uninstalling the software repeatedly.

Important! Do not use the Uninstall option if you have upgraded from CA NetQoS ReporterAnalyzer 9.0.1.

This section contains the following topics:

Uninstallation Prerequisites

Before you begin uninstalling the CA Network Flow Analysis software from a server, verify that the component is working properly.

Verify that the appropriate databases are present, as listed in the following table.

Database	Location
reporter	<install_path>\MySql\data\ reporter on the stand-alone or NFA console server
harvester	<install_path>\MySql\data\ harvester on the stand-alone or Harvester servers
nqrptr	<install_path>\MySql\data\nqrptr directory on the DSA servers in a three-tier deployment
poller	<install_path>\MySql\data\ poller on the stand-alone or Harvester servers
ReaperArchive15	<install_path>\Netflow\datafiles\ ReaperArchive15 on the stand-alone or Harvester servers
data_retention	<install_path>\MySql\data\ data_retention on the stand-alone or Harvester servers
ReaperArchive	<install_path>\Netflow\datafiles\ ReaperArchive on the stand-alone or Harvester servers

Verify that the CA Network Flow Analysis services and MySQL are running, as listed in the following table:

Service	Stand-Alone	Harvester	Console	DSA (3-Tier)
CA NFA Collection and Poller Webservices (nfa_collpollws on Linux)	Yes	Yes		
CA NFA Data Retention (nfa_dataretention on Linux)	Yes	Yes		
CA NFA DNS/SNMP Proxies (nfa_proxies on Linux)	Yes	Yes	Yes	Yes
CA NFA DSALoader				Yes
CA NFA File Server (nfa_filewebservice on Linux)	Yes	Yes	Yes (3-tier)	
CA NFA Harvester (nfa_harvester on Linux)	Yes	Yes		
CA NFA Poller (nfa_poller on Linux)	Yes	Yes		
CA NFA Pump				Yes
CA NFA Reaper (nfa_reaper on Linux)		Yes		
CA NFA RibSource	Yes		Yes	
NetQoS MySql	Yes	Yes	Yes	Yes
NetQoS NQMySql (nfa_mysqlCSE on Linux)	Yes	Yes	Yes	Yes
NetQoS Reporter Manager	Yes		Yes	
NetQoS Reporter/Analyzer General Services	Yes		Yes	
NetQoS Reporter/Analyzer Pump	Yes		Yes	
NetQoS Reporter/Analyzer Query Services	Yes		Yes	
NetQoS Reporter/Analyzer Report	Yes		Yes	
NetQoS Reporter/Analyzer Watchdog	Yes		Yes	

Uninstall the Software

This topic describes how to uninstall the CA Network Flow Analysis software by using the Uninstaller. You also can uninstall the software from the Windows Add or Remove Programs window, where it is listed under the publisher CA Technologies, Inc.

Note: The steps in this topic assume that you are uninstalling the CA Network Flow Analysis software from a standalone or distributed deployment server that has no other related software installed.

Follow these steps:

1. Log in as a user who has administrator privileges for CA Network Flow Analysis.
2. Back up your data and configuration files. For information about this step, see the *CA Network Flow Analysis Administrator Guide.*
3. Exit from all applications--with no exceptions.
4. Start the Uninstaller: Double-click the Uninstaller shortcut in <install_path>\Uninstall:

   - Stand-alone system: Double-click Uninstall Reporter shortcut to uninstall the NFA console first, then double-click the Uninstall Harvester shortcut to uninstall the Harvester.

     If you attempt to uninstall the Harvester software first, an error message opens.

   - Distributed deployment: Double-click Uninstall Reporter (NFA console server), Uninstall Harvester (Harvester server), or Uninstall DSA (DSA server).

   The Uninstall window opens.
5. Click **Uninstall**.

   The Uninstaller removes all of the program and data files, including the following CA Network Flow Analysis and MySQL elements:

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

   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 Uninstall Complete screen.
7. 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.
8. Check the following to verify the uninstall:
   a. Verify that the Registry keys in the following location are deleted:

      HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NetQoS

   b. Verify that the CA Network Flow Analysis services are removed.
   c. Verify that the CA Network Flow Analysis programs (such as NFA or Harvester and MySQL) are no longer visible from the Control Panel. If they are, select each program individually and click **Uninstall**.

Notes:

- The uninstallation log is at the root level of the original installation path. For example, the Harvester uninstallation log is at: <install_path>\Harvester_Uninstall_<timestamp>.txt.
- You may want to manually delete any CA Network Flow Analysis directories and files that are still present.
- If you make an unsuccessful attempt to reinstall the software, contact CA Support.

Chapter 9: Troubleshooting

This section provides some troubleshooting tips for problems that are revealed by prerequisite tests. Prerequisite tests can generate warnings or failure notices. If you receive a warning, you can correct the problem immediately or after the installation or upgrade software runs. Failures must be corrected before you can continue. Most of the troubleshooting topics are for prerequisite failures.

Note: Many prerequisite tests rely on general indicators to identify problem areas. Passing a prerequisite test is not a guarantee that everything is configured properly. It is important to meet all of the server requirements, verify that supported versions of the required software are installed and complete all of the configuration tasks.

The following prerequisite tests are run:

Test	Description	Warning or Failure	Server
Browser	Checks the Registry for a browser. Verify that a supported browser version is installed (see page 21).	Warning	Stand-alone Distributed: NFA console
DEP	Verifies that the winmgt service is running. Configure DEP as described in this guide (see page 30).	Warning	Stand-alone Distributed: NFA console, Harvester (Windows)
FIPS Algorithm Policy	Verifies that the FIPS Algorithm policy is not enabled (see page 62).	Verify automatic fix or Failure	Stand-alone Distributed: NFA console
IIS Installed	Verifies that the wcsvc service is running. Install and configure IIS as described in this guide. (see page 25)	Warning	Stand-alone Distributed: NFA console
IIS Version	Checks the Registry for IIS version 7.0.	Warning	Stand-alone Distributed: NFA console
.NET 3.5 Version	Checks for .NET version 3.5 SP1. If .NET version 3.5 is found, turns on SP1.	Failure	Stand-alone Distributed: NFA console
NPC Installation Detected	Checks if NPC is installed on the server (see page 63).	Failure	Stand-alone Distributed: NFA console
SNMP	Verifies that the snmp service is running and the process ID is present. Configure SNMP on Windows servers (see page 27) and Linux servers (see page 32).	Warning	Stand-alone Distributed: NFA console, all Harvesters

Test	Description	Warning or Failure	Server
Windows 2003 Detected	Verifies that the server is running Windows Server 2008, not Windows Server 2003 (see page 64).	Failure	Windows servers

This section contains the following topics:

FIPS Algorithm Policy Is Enabled

Valid on Console only

When I click Next in the License Agreement screen in the installation or upgrade program for the NFA console, a Pre-requisite Check Warning message opens, which includes the following text:

> "The FipsAlgorithmPolicy registry key for this system is set to enabled. If the following key is enabled, Windows will not allow certain algorithms to run..."

The error message opens because a system check found the FipsAlgorithmPolicy key in the Windows Registry, which indicates that the Federal Information Processing Standard (FIPS) 140 cryptographic standard is enabled. While this policy is enabled, the server can run only the cryptographic algorithms that have been submitted to and approved by the National Institute of Standards and Technology (NIST).

This restriction can cause problems connecting to databases through Open Database Connectivity (ODBC). Problems with CA Network Flow Analysis connectivity may result.

To disable the FipsAlgorithmPolicy Registry key, click OK in the Pre-requisite Check Warning message. The FIPS algorithm policy is disabled and does not restrict database connections.

NPC Installation Detected

Valid on Console

If you attempt to launch the installation or upgrade program on a server that has NetQoS Performance Center installed, an error message opens, and the installation is canceled.

CA Network Flow Analysis cannot be installed on the same server as CA NetQoS Performance Center. NPC must be completely removed before you proceed with the CA Network Flow Analysis installation or upgrade.

SC.exe Is Not Installed

Valid on Console, Harvester, or DSA

When I click Next in the License Agreement screen of the installation or upgrade program, an error message opens, which begins with the following text:

> "sc.exe is not installed. The installer was unable to find "sc.exe" in the System32 folder."

A system check did not find the Service Control command (the sc.exe file) in the Windows/System32 directory. The Service Control command is used for communicating with the Service Controller during command line operations. If the file is missing, the installation or upgrade program exits.

The sc.exe file is included with the Windows Server software by default. To correct the problem, restore the missing sc.exe from your Windows Server installation software, Windows Resource Kit, or other resource.

SNMP Is Not Enabled

When I click Next in the License Agreement screen of the installation or upgrade program, an SNMP warning message opens. The message reads:

> "Pre-requisite Check Warning The following issues were found: SNMP is not enabled. While not required before installation, some functionality may not work correctly if these are not addressed."

The SNMP warning message opens because the prerequisite check does not find that the snmpd daemon is running. You can correct the problem when the warning appears or you can proceed with the installation or upgrade. In any case, CA Network Flow Analysis will not run properly until you configure SNMP (see page 32) and make sure that the snmpd and snmptrapd daemons are running.

Use the following procedures to check the SNMP status on a Linux server.

Follow these steps:

1. (Optional) Enter the status command in a terminal window:
   `/etc/init.d/snmpd status`

   The command returns the process ID of the snmpd daemon. If the return text does not list a process ID for the snmpd daemon is not running.

2. (Optional) Check the status in the Service Configuration window:

   a. Open the Service Configuration window: Select System, Administration, Server Settings, Services.

      The Service Configuration window opens with the Background Services tab selected.

   b. Locate snmpd and snmptrapd in the service list.

   c. Check the status of these services:

      - Select snmpd and review the status message that is displayed.
      - Select snmptrapd and review the status message that is displayed.

   d. Close the Service Configuration window.

Windows Server 2003 Found

If you attempt to launch the installation or upgrade program on a server that is running Windows Server 2003, an error message opens. Installation and upgrade for Windows servers is supported only for servers that are running Windows Server 2008 R2, Standard edition.

Upgrade to Windows Server 2008 R2, Standard edition before you proceed with the installation or upgrade.

Index

L

N

O

P

R

S

T

U

W