CA Network Flow Analysis

Upgrade 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 upgrade to CA Network Flow Analysis 9.3.0.

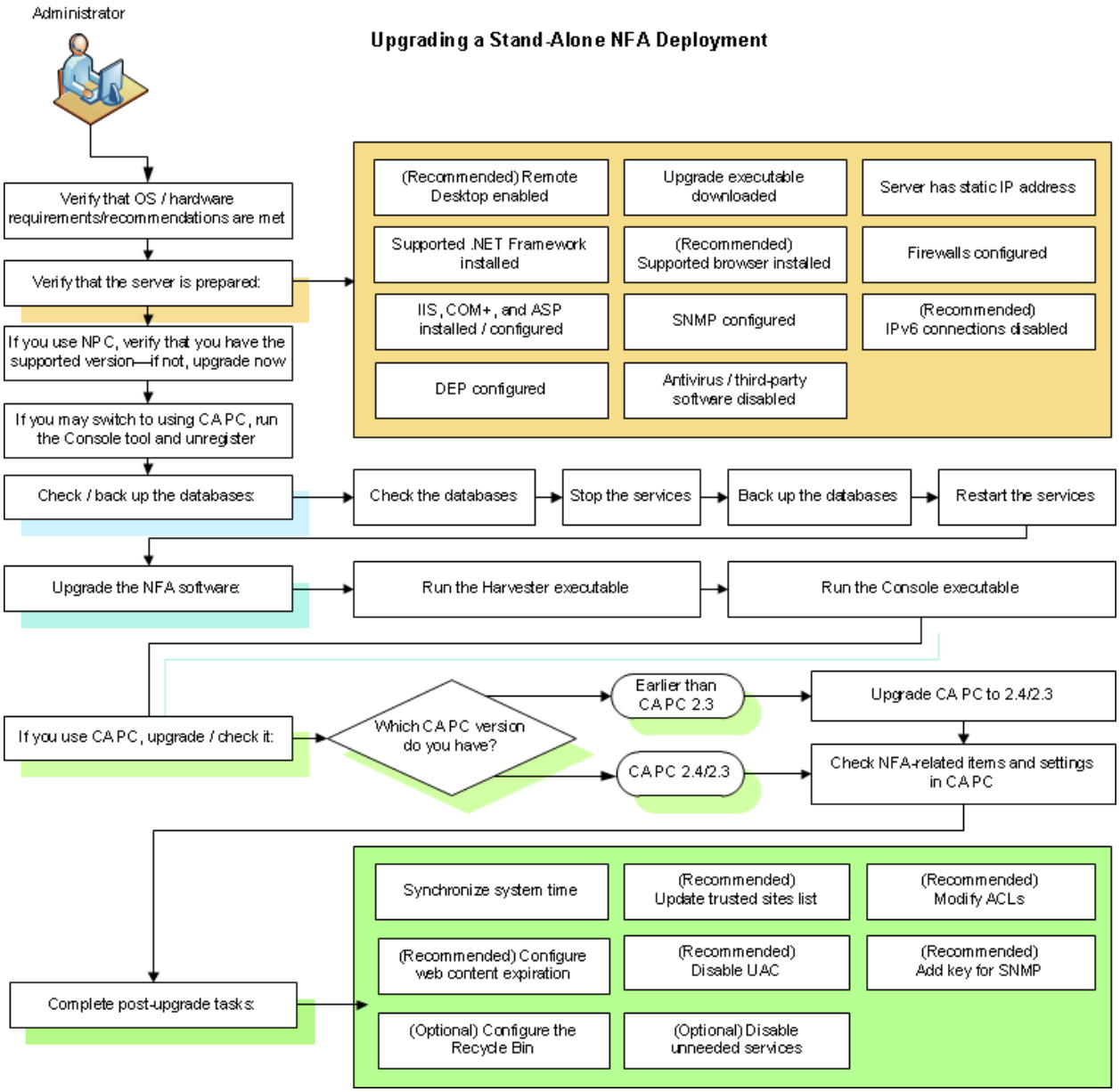
If you purchase hardware from CA Technologies, all components are delivered with the operating system and security settings already configured. Use the topics in this guide to verify the settings or update them to suit the needs of your organization.

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

The following diagrams show the steps for upgrading CA Network Flow Analysis.

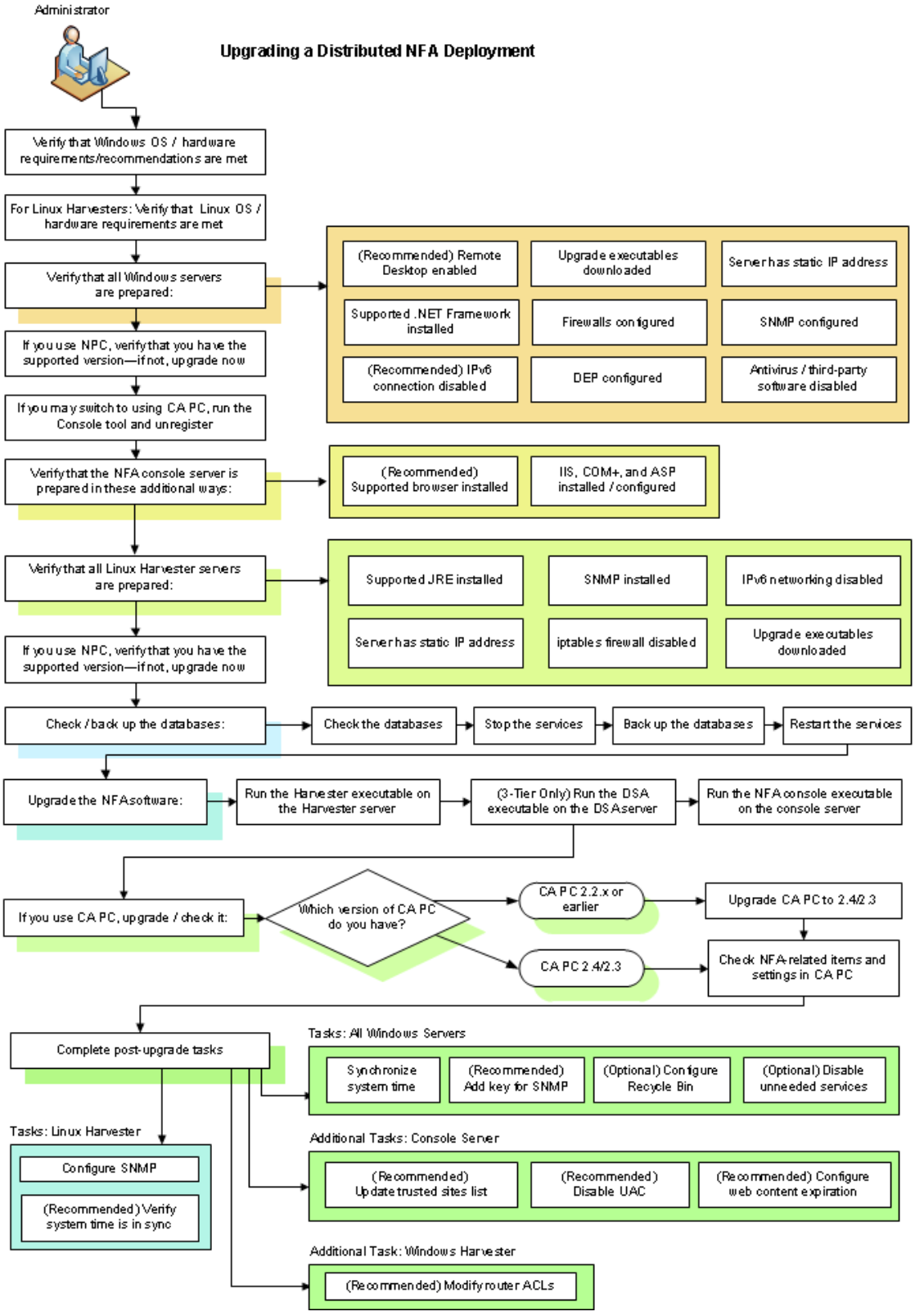
Workflow for Upgrading a Stand-Alone Deployment

Use the following diagram as a general checklist for upgrading a stand-alone deployment. See the related topics for complete information about the steps.



Workflow for Upgrading a Distributed Deployment

Use the following diagram as a general checklist for upgrading a distributed deployment. See the related topics for complete information about the steps.


Administrator
Upgrading a Distributed NFA Deployment
Verify that Windows OS / hardware requirements/recommendations are met
For Linux Harvesters: Verify that Linux OS / hardware requirements are met
Verify that all Windows servers are prepared:
(Recommended) Remote Desktop enabled
Upgrade executables downloaded
Server has static IP address
Supported .NET Framework installed
Firewalls configured
SNMP configured
(Recommended) IPv6 connection disabled
DEP configured
Antivirus / third-party software disabled
If you use NPC, verify that you have the supported version—if not, upgrade now
If you may switch to using CA PC, run the Console tool and unregister
Verify that the NFA console server is prepared in these additional ways:
(Recommended) Supported browser installed
IIS, COM+, and ASP installed / configured
Verify that all Linux Harvester servers are prepared:
Supported JRE installed
SNMP installed
IPv6 networking disabled
Server has static IP address
iptables firewall disabled
Upgrade executables downloaded
If you use NPC, verify that you have the supported version—if not, upgrade now
Check / back up the databases:
Check the databases
Stop the services
Back up the databases
Restart the services
Upgrade 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 console server
If you use CA PC, upgrade / check it:
Which version of CA PC do you have?
CA PC 2.2.x or earlier
Upgrade CA PC to 2.4/2.3
CA PC 2.4/2.3
Check NFA-related items and settings in CA PC
Complete post-upgrade tasks
Tasks: All Windows Servers
Synchronize system time
(Recommended) Add key for SNMP
(Optional) Configure Recycle Bin
(Optional) Disable unneeded services
Tasks: Linux Harvester
Configure SNMP
(Recommended) Verify system time is in sync
Additional Tasks: Console Server
(Recommended) Update trusted sites list
(Recommended) Disable UAC
(Recommended) Configure web content expiration
Additional Task: Windows Harvester
(Recommended) Modify router ACLs

Software Versions that Are Supported for Upgrade

CA Network Flow Analysis 9.3.0 supports upgrades from the following versions to the current configuration:

- CA Network Flow Analysis 9.2.1
- CA Performance Center 2.4/2.3 or CA NetQoS Performance Center 6.1.205 SP2/6.1.194
- (Optional) CA Anomaly Detector 9.2.1

From	Upgrade To
NFA 9.2.1 operating with CA PC 2.3.x	NFA 9.3.0 operating with CA PC 2.4/2.3
NFA 9.2.1 operating with NPC 6.1.205 SP2/6.1.194	NFA 9.3.0 operating with NPC 6.1.205 SP2/6.1.194

When you upgrade the software, you continue to use the same architecture you used for release 9.2.1, as shown in the following list:

- Stand-alone to stand-alone
- Distributed 2-tier to distributed 2-tier
- Distributed 3-tier to distributed 3-tier

CA Network Flow Analysis 9.2.1 is the only software version that you can upgrade directly to release 9.3.0. If you have an earlier version, upgrade to version 9.2.1 before you proceed. For more information, see the *CA Network Flow Analysis 9.2.1 Upgrade Guide*.

Notes:

- Upgrade CA Network Flow Analysis before any upgrade you make to Performance Center.
- Do not install or upgrade any CA Network Flow Analysis component on a server that has Performance Center installed. You can co-locate the NFA console or stand-alone deployment with CA Anomaly Detector, but not with any other related software.
- If you plan to switch between CA NetQoS Performance Center (NPC) and CA Performance Center (CA PC), unregister before you upgrade CA Network Flow Analysis. Unregister before a switch from NPC to CA PC or a switch from CA PC to NPC.
- Windows NT LAN Manager (NTLM) is not supported by the Single Sign-On tool.

Download the Upgrade 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 2: System Recommendations and Requirements

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

This section contains the following topics:

Windows Operating System Requirements

You can install and upgrade CA Network Flow Analysis 9.3.0 on servers with the following operating systems:

- Windows Server 2008 R2 Standard edition (all components)

  For help with upgrading your Windows operating system in preparation for the software upgrade, contact CA Technical Support.

- Red Hat Enterprise Linux 5.5 or 5.6 (Harvester)

If you add new component servers to your deployment, use servers that have one of the following operating systems:

- Harvester: Windows Server 2008 R2 Standard edition or Red Hat Enterprise Linux 5.5 or 5.6
- DSA: Windows Server 2008 R2 Standard edition

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)

- Upgrades to CA Network Flow Analysis 9.3.0 require additional space for database backup and migration. To determine the space needed:
  1. Locate the CA/NFA/MySql51/data directory.
  2. Determine the size of the directory.
  3. Add the size of the directory to the size of the 9.3.0 product install (~1.5 GB) to get the required free disk space.
- Server configuration as described in:
  - Verify That the Windows Servers Are Prepared (see page 21)
  - Post-Upgrade Tasks (see page 65)

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 log in to a Linux server with root privileges.
- 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.

If you have either of the following special situations, ask for help from your CA Support Availability Manager:

- DSA on Linux: Migrating Linux DSAs to Windows servers
- Changing the Installation Drive: Moving the installation location for any component to a new drive

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 3: Preparing Windows Servers

This section contains the following topics:

Verify that the Windows Servers Are Prepared

Before you begin the upgrade, 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 upgrade.

Verify that the following conditions are met:

- Installation servers have fully operational installations of CA Network Flow Analysis software that is supported for upgrade (see page 11).
- Your deployment includes a supported version of Performance Center (see page 66).
- The Windows servers meet the requirements in the following table.

Stand-Alone Server	Distributed NFA Console Server	Distributed Harvester Server	Distributed 3-Tier DSA Server
■ Windows operating system requirements are met (see page 15)			
■ (Recommended) Windows hardware recommendations are met (see page 17)			
■ (Recommended) Remote Desktop connection is enabled to allow remote access			
■ Upgrade executables are downloaded to the servers (see page 12)			
■ Static IP address is assigned to each server. Set the Harvester server IP address to match the flow export destination that is assigned to each router.			
■ Supported version of .NET Framework is installed (see page 24) *			
■ (Recommended) Supported browser is installed (see page 23) **			
■ Firewalls are configured (see page 24)			
■ IIS, COM+, and ASP are installed (see page 27) **			
■ SNMP is configured (see page 29) **			
■ IPv6 addresses are disabled (see page 31)			
■ DEP is configured (see page 32)			
■ The following third-party software is disabled until the upgrade is complete: Antivirus, server monitoring, and maintenance software. If you enable antivirus scans later, exclude the CA Network Flow Analysis installation path and its subdirectories.			
■ Databases are checked (see page 41)			
■ Services are stopped (see page 43), databases are backed up, and services are restarted			

* The upgrade program does not open or does not complete successfully unless this requirement is met.
** If the server fails to pass this check, 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 24)
- Two-tier distributed deployment (see page 25)
- Three-tier distributed deployment (see page 26)

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]

From	To	Port [Function]
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]
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]

From	To	Port [Function]
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]
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]

From	To	Port [Function]
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]
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.

Prepare to Change the Performance Center Version

The NFA console or stand-alone server must be registered as a data source for a supported version of CA Performance Center (CA PC) or CA NetQoS Performance Center (NPC). If you plan to to switch between NPC and CA PC, prepare for the switch as described in this topic:

1. Prepare for unregistering from your current Performance Center version as described below.
2. Unregister from Performance Center
3. Perform the CA Network Flow Analysis upgrade.

Important! We generally do not recommend unregistering. Many customizations are lost when you unregister and register again. Read this topic carefully to prepare for these events.

General Guidelines

- If you need to upgrade CA Performance Center to version 2.4, upgrade CA Network Flow Analysis first.
- If you plan to switch between types of Performance Center, unregister before you upgrade CA Network Flow Analysis. For example, unregister before you switch from CA NetQoS Performance Center to CA Performance Center or you switch from CA Performance Center to CA NetQoS Performance Center.

Results of Unregistering from CA NetQoS Performance Center

If you unregister CA Network Flow Analysis from CA NetQoS Performance Center and register again with CA Performance Center, the following rules apply.

- Domains:
  - The default domain is retained. Groups, users, devices (routers), interfaces, protocol names, and ToS labels that are assigned to the default domain retain their assignments.
  - Custom domains are deleted.
  - Groups, users, devices (routers), and interfaces in custom domains are reassigned to the default domain.
  - Protocol names, ToS labels, AS names, and IP addresses in custom domains become inaccessible.
- User accounts:
  - User accounts are retained if the users have valid product privilege settings (User, Power User, or Administrator) for CA Network Flow Analysis. User accounts with no product privilege for CA Network Flow Analysis are deleted.

- User accounts that are associated with custom domains will be associated with the default domain instead.
- If the user account nqadmin exists and has a product privilege that is lower than Administrator, this user account acquires the Administrator product privilege.

You cannot add new users or edit user account settings after you unregister.

- Roles:
  - Custom and default roles are retained and continue to be associated with user accounts.
- Groups: Retained if the following conditions are met:
  - The group is a default group in CA NetQoS Performance Center or is a group that was pushed up to CA NetQoS Performance Center. 'Dynamic groups,' for example, cross-product groups, are deleted.
  - The group has contents--that is, the group is not empty.

  Custom and default groups require cleanup on the Manage Groups page in CA Performance Center after you unregister and register with the newer software. The following changes may occur:
  - Some group names change slightly. For example, the group 'All Interfaces' is renamed 'Interfaces.'
  - Structures may flatten so that a group that was nested under another group is not nested.
  - Groups may be relocated:

    A custom group that originally was shown on the Manage Groups page under All Groups/System Groups/Data Sources/ReporterAnalyzer is under Network Flow Analysis in the new group tree. The new location is All Groups/Inventory/Data Sources/Network Flow Analysis.

    If the custom group originally was not under ReporterAnalyzer, it is moved to sit under Network Flow Analysis.
  - Duplicate groups may be created.
  - Empty custom groups are deleted.
- SNMP profiles: SNMP profiles from CA NetQoS Performance Center 6.1.205 SP2/6.1.194 are retained with no changes in their status.
- Single Sign-On (SSO) customizations: LDAP and other SSO customizations are retained.

  If you change to a new SSO version, update the SSO configuration settings as described in the *Single Sign-On User Guide*.

Follow these steps:

1. Log in to the Console for CA NetQoS Performance Center as a user who is a member of the Administrators group.
2. Review your records of the customizations in CA NetQoS Performance Center, such as:
   - User accounts and their roles, product permissions, groups, and domain access
   - Custom roles and standard roles that have been customized, including any assignments for top-level menus, dashboards, and dashboard menus
   - Group structure and naming conventions
   - Custom domains and their contents, such as groups, devices, interfaces, SNMP profiles, report folders, AS names, protocol names, ToS labels, and IP addresses

   Remember that these elements may require checking, restructuring, or restoration.
3. (Optional) Prepare for the effects of unregistering:

   Consider giving a unique name to each group so it is easy to restore the group hierarchy. For example, name each group in a way that indicates its relationship to other groups.

   To ensure that no groups are deleted, flatten the group hierarchy before you unregister.
4. Open the Data Source List page: Click Admin, NetQoS Settings: Data Sources.
5. Select the Reporter Analyzer or CA Network Flow Analysis data source.
6. Click Delete.

Chapter 4: Preparing Linux Servers

This section contains the following topics:

Verify that the Linux Servers Are Prepared

Before you begin the upgrade, 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 upgrade.

- System Requirements: Verify that the upgrade servers meet the Linux requirements and recommendations (see page 18).
- Software Requirements: Verify that the upgrade servers have fully operational CA Network Flow Analysis software that is supported for upgrade (see page 11).
- Verify that each of the Harvester Linux servers is ready for the upgrade by:
  - Assigning 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.
  - Configuring SNMP (see page 38)

    If SNMP is not running, the upgrade program displays a warning. You can bypass the warning and configure SNMP after the upgrade, however.
  - Disabling the iptables firewall (see page 39)
  - Disabling IPv6 networking (see page 39)
  - Stopping services (see page 44)
  - Backing up the databases (see page 45)

- 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 66)
  - 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 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 24). 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
   ```

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.

Chapter 5: Check and Back Up the Databases

This section contains the following topics:

Check the MySQL Databases

We recommend that you check the database tables before upgrading. Checking the database tables corrects some problems and helps to avoid failures and recovery assistance with CA Support. This topic describes how to run the mysqlcheck command before the upgrade to verify that the database tables are set up properly.

You can run the mysqlcheck command to check the following databases:

- reporter: Located on each stand-alone or NFA console server (which typically contains some large tables)
- harvester: Located on each stand-alone or Harvester server
- poller: Located on each stand-alone or Harvester server
- data_retention: Located on the following servers: Stand-alone, Harvesters, and DSAs
- nsas: Located on the CA Anomaly Detector server, which can be the stand-alone, NFA console, or separate server

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 MySQL: The MySQL deamon process (mysqld) can continue to run on Linux servers and the MySQL service can continue to run on Windows servers.

Follow these steps:

1. Log in to one of the CA Network Flow Analysis servers as a user with administrator privileges. On a Linux Harvester server, log in as root.
2. Check the following databases:
   - Stand-alone server: harvester, reporter, poller, and data_retention databases
   - Harvester server (distributed deployment): harvester, poller, and data_retention databases
   - NFA console server (distributed deployment): reporter database
   - DSA server (distributed deployment): nqrptr database
   - CA Anomaly Detector server: nsas database (if CA Anomaly Detector is installed on the stand-alone server or the NFA console server
3. 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:

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

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

     ```
     mysqlcheck --databases db_name
     ```

     Example:

     ```
     mysqlcheck --databases reporter
     ```

   where:

   db_name = Name of the database that you want to check

   You do not need to specify the path to the database. The mysqlcheck command will find any or all databases that use the default port (port 3308). The custom storage engine does not support the use of the mysqlcheck command for its archive and archive15 databases. The command fails to run even if you specify the correct port (port 3307) for the connection to these databases.

   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 table.

   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

Before you back up the databases and upgrade the CA Network Flow Analysis software, prevent new data from being sent to the NFA console until the upgrade is complete. Failure to stop the services does not cause the upgrade to fail, but some collected data is not processed.

Stop Services on Windows Servers

To prepare for backing up the databases, stop the services on all of the Windows servers in your CA Network Flow Analysis deployment.

Follow these steps:

1. Log in as a user who has administrator privileges for CA Network Flow Analysis.
2. Open the Services window: Click Start, Control Panel, Administrative Tools, Services.
3. Stop the CA NFA Harvester service on each Harvester server.
4. Wait 15 minutes for data file processing to complete.
5. Stop the remaining CA Network Flow Analysis services on each Windows server:

Service	Stand-Alone	Harvester	Console	DSA	Anomaly Detector
CA NFA Collection and Poller Webservices	Yes	Yes			
CA NFA Data Retention	Yes	Yes		Yes	
CA NFA DNS/SNMP Proxies	Yes	Yes			
CA NFA DSALoader				Yes	
CA NFA File Server	Yes	Yes			
CA NFA Harvester	Yes	Yes			
CA NFA Host Resolver Service *					Yes *
CA NFA Hunter Tracker Service *					Yes *
CA NFA Poller	Yes	Yes			
CA NFA Pump				Yes	
CA NFA Reaper	Yes	Yes			
CA NFA RibSource	Yes		Yes		
NetQoS MySql	Yes	Yes	Yes	Yes	

Service	Stand-Alone	Harvester	Console	DSA	Anomaly Detector
NetQoS NQMySql	Yes	Yes		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		

* If CA Anomaly Detector is installed on the stand-alone CA Network Flow Analysis server or NFA console server, stop these CA Anomaly Detector services.

The services and data collection stop. The data files are processed within 15 minutes.

6. Check the following directory on the NFA console server:

   <install_path>\Netflow\datafiles\HarvesterWork

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

   The services are restarted automatically during the upgrade process.

Stop Services on Linux Servers

To prepare for the database backups, stop the services on any Linux Harvester servers that are in your product deployment.

Follow these steps:

1. Log in as root or with a sudo user account.
2. Stop the nfa_harvester (CA NFA Harvester) service on each Linux Harvester server.
3. Wait 15 minutes for data file processing to complete.
4. Stop the following services on each Linux Harvester server:
   - mysql (NetQoS MySQL)
   - nfa_collpollws (CA NFA Collection and Poller Webservices)
   - nfa_dataretention (CA NFA Data Retention)
   - nfa_filewebservice (CA NFA File Server)
   - nfa_mysqlCSE (NetQoS NQMySql Custom Storage Engine)

- nfa_poller (CA NFA Poller)
- nfa_proxies (CA NFA DNS/SNMP Proxies)
- nfa_reaper (CA NFA Reaper)

After you stop the services, the Time BIN (.tbn) files are collected and processed within 15 minutes.

5. Check the following directory on the NFA console server:
<install_path>\Netflow\datafiles\HarvesterWork

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

The services are restarted automatically during the upgrade process.

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.

Database	Stand-Alone	Harvester (Distributed)	NFA Console (Distributed)	DSA Server (Distributed)	Anomaly Detector
reporter: Enterprise Overview data; NFA console configuration data	Important		Important		
harvester: Harvester configuration data	Important	Important			
nqrptr: Configuration for collecting historical (15-minute) data				Important	
nsas: Anomaly Detector configuration data					Important
poller: Poller configuration data	Important	Important			

Database	Stand-Alone	Harvester (Distributed)	NFA Console (Distributed)	DSA Server (Distributed)	Anomaly Detector
ReaperArchive15: Historical (15-minute) data	Recommended	Recommended		Recommended	
Customized Files: Configuration or other files that have been customized	Important	Important	Important	Important	
Customized data_retention: Settings to regulate data retention	Important if customized	Important if customized		Important if customized	
ReaperArchive: Realtime (1-minute) data	Optional, rarely backed up	Optional, rarely backed up			

The following list describes the databases and their locations:

- reporter: Back up the previous 24 hours of Enterprise Overview data, NFA console configuration settings, and synchronization information.

  Path: <install_path>\MySql\data\reporter directory

- harvester: Back up the Harvester configuration data.

  Path: <install_path>\MySql\data\harvester directory

- nqrptr: Back up the configuration data for collecting historical (15-minute data) on the DSA servers in a three-tier deployment.

  Path: <install_path>\MySql\data\nqrptr directory

- nsas: If CA Anomaly Detector is installed on the same server as the NFA console or the stand-alone server, back up the configuration data for running CA Anomaly Detector. If CA Anomaly Detector is located on its own server, you can perform this backup when you upgrade CA Anomaly Detector.

  Path: <install_path>\MySql\data\nsas

- poller: Back up the Poller configuration data. The poller and harvester configuration data are essential to perform the relational mapping that provides access to 15-minute data. The poller configuration data provides information about devices and interfaces to enable polling, such as persistent IDs for interfaces.

  Path: <install_path>\MySql\data\poller directory

- ReaperArchive15: Optionally, back up the historical (15-minute) data that is stored for the reporting routers and interfaces. This backup is optional, but many administrators do back up the 15-minute data.

  Path: <install_path>\Netflow\datafiles\ReaperArchive15 directory

- Customized configuration files: Back up any customized configuration files--files that you customized or that were customized by CA Support. In addition, back up any customizations that you made to the website or reports.

  The CA Network Flow Analysis configuration files typically have a .config, conf., or .ini extension and are located in the product installation path. Other customizations may include .css files and report logos.

- ReaperArchive: (Recommended) Back up the historical (15-minute) data.

  Path: <install_path>\Netflow\datafiles\ReaperArchive directory

- Customized data_retention: If you customized any data retention settings, back up the data retention configuration data. It is unusual to customize data retention settings except with the assistance of CA Support. Changes to data retention settings can cause problems from rising demands on drive space.

  Path: <install_path>\MySql\data\data_retention directory

Follow these steps:

1. Log in as a user who has administrator privileges for CA Network Flow Analysis.
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 (see page 43).

Chapter 6: Install the Software

This section contains the following topics:

Upgrade a Stand-Alone Server

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

Note: The program checks for server problems at various points during the installation or upgrade. If a problem is found, an error message opens (see page 79). A critical problem causes the program to exit. A warning message opens for non-critical problems, which you can correct at any time. The pre-requisite checks look for general indicators that problems exist: They do not warn you about all problems. You are responsible for preparing the server properly and for completing all required post-installation steps.

Follow these steps to complete the Harvester phase:

1. Verify that the server is upgrade-ready as described in Verify That the Windows Servers Are Prepared (see page 21).
2. Log in to the server as a user who is a member of the Administrators group.
3. Stop the pump service on the NFA console server:
   a. Click Start, Programs, Administrative Tools, Services.
   b. Right-click the NetQoS Reporter/Analyzer Pump service.
   c. Select Stop in the right-click menu.

      The service stops.
4. Log in to the Harvester server as a user who is a member of the Administrators group.
5. Start the Harvester phase of the upgrade: Double-click the NFHarvesterSetup9.3.0.exe file. If you do not have this file, download it to the server (see page 12).

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

   The Welcome screen opens.

7. Click Next.

   The CA NFA Harvester License Agreement screen opens.

8. Review and accept the license agreement:

   a. Read the 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.

      Prerequisite tests look for problems and may cause an error message to open.

9. If the Pre-requisite Check Warning message opens, review it, correct or note any non-critical problems, then click OK.

   The Upgrading Existing Installation message opens and the Choose Install Folder screen opens. This screen displays the original root installation path as the default setting.

10. Verify that the specified installation directory is correct, then click Next.

    Important: If you do not use the original installation path, the upgraded software will not run properly.

    If the program does not find certain expected directories in the installation path, an error message opens and the upgrade stops. This problem does not occur when the previous software installation is fully functional.

    The Pre-Installation Summary screen opens.

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

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

12. (Optional) If errors occurred during the upgrade, see the following logs for details:

    - General installation log: <install_path>\Harvester_Install_<timestamp>.log (where <timestamp> is the time that the log was created)
    - Upgrade migration log: <install_path>\migrator.log

13. Click Done in the Install Complete screen.

    The Harvester upgrade program closes.

Follow these steps to complete the NFA console phase:

1. Start the NFA console upgrade software: Double-click the RAConsoleSetup9.3.0.exe file in Windows Explorer. If you do not have this file, download it to the server (see page 12).

   The program starts and the language selection screen opens.

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

   The Welcome screen opens.

3. Click Next.

   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.

   f. Click Next.

5. If the Pre-requisite Check Warning message opens, review it, correct or note any non-critical problems, then click OK.

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

6. Review the information and click OK.

   The Pre-Installation Summary screen opens.

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

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

8. Exit from the upgrade 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 upgrade program closes. If you selected the option to restart now, the system restarts and the upgrade is finalized.

9. (Optional) Check the revision history to verify that the software is upgraded to the correct version:
   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-upgrade tasks (see page 65).

Note: If you interrupt and restart the upgrade, the upgrade resumes from your most recently saved change.

Upgrade 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 upgrade each component server.

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

- Upgrade the Harvester on a Windows Server (see page 53), or
- Upgrade the Harvester on a Linux Server (see page 56)
- Upgrade the Console (see page 61)

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

- Upgrade the Harvester on a Windows Server (see page 53)
- Upgrade the DSA Server (see page 58)
- Upgrade the Console (see page 61)

The steps in these topics are written for the recommended upgrade order: Harvester upgrades, DSA upgrades (if any), then NFA console upgrade.

If you interrupt and restart the upgrade, the upgrade resumes from your most recently saved change.

Note: The program checks for server problems at various points during the installation or upgrade. If a problem is found, an error message opens (see page 79). A critical problem causes the program to exit. A warning message opens for non-critical problems, which you can correct at any time. The pre-requisite checks look for general indicators that problems exist: They do not warn you about all problems. You are responsible for preparing the server properly and for completing all required post-installation steps.

Upgrade the Harvester on a Windows Server

In a distributed deployment, each Harvester is installed on a separate server. To upgrade 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 upgrade-ready as described in Verify That the Windows Servers Are Prepared (see page 21).
2. Log in to the NFA console server as a user who is a member of the Administrators group.

3. Stop the pump service on the NFA console server:
   a. Click Start, Programs, Administrative Tools, Services.
   b. Right-click the NetQoS Reporter/Analyzer Pump service.
   c. Select Stop in the right-click menu.

      The service stops.
4. Log in to the Harvester server as a user who is a member of the Administrators group.
5. Start the upgrade: Double-click the NFHarvesterSetup9.3.0.exe file in Windows Explorer on the Harvester server. If you do not have this file, download it. (see page 12)

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

   The Prior Installation Detected message opens.
7. Review the message and click OK.

   The Welcome screen opens.
8. Click Next.

   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, click the option to accept the license agreement. This option is activated when you scroll to the bottom.
   c. Click Next.

      Prerequisite tests look for problems and may cause an error message to open.
10. If the Pre-requisite Check Warning message opens, review it, correct or note any non-critical problems, then click OK.

    The Choose Install Folder screen opens and displays the original root installation path as the default setting.
11. Verify that the specified installation directory is correct, then click Next.

    Important: If you do not use the original installation path, the upgraded software will not run properly.

    If the program does not find certain expected directories in the installation path, an error message opens and the upgrade stops. This problem does not occur when the previous software installation is fully functional.

    The Pre-Installation Summary screen opens.

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

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

13. (Optional) If errors occurred, see the following logs for details:
    - General installation log: <install_path>\Harvester_Install_<timestamp>.log.
    - Upgrade migration log: <install_path>\migrator.log

14. Exit from the upgrade 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 upgrade program closes. If you selected the option to restart now, the system restarts and the upgrade is finalized.

15. (Optional) Verify that the following conditions are met:
    - Harvester services are running.
    - Harvester is receiving data.
    - The revision history shows that the component is upgraded to the correct version. To display the revision history, complete the following substeps:
      a. Start MySQL by entering the following command in a Command Prompt window: mysql
      b. Display the revision history by entering the following command: select * from revision_history

Next:

- To upgrade another Harvester, repeat these steps on the additional Harvester server.
- To continue upgrading a two-tier deployment, Upgrade the Console server (see page 61).
- To continue upgrading a three-tier deployment, Upgrade the DSA server (see page 58).

Upgrade the Harvester on a Linux Server

A two-tier distributed deployment may include one or more Linux Harvester servers. To upgrade 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 upgrade-ready as described in Verify That the Linux Servers Are Prepared (see page 37).
2. Log in to the NFA console server as a user who is a member of the Administrators group.
3. Stop the pump service on the NFA console server:
   a. Click Start, Programs, Administrative Tools, Services.
   b. Right-click the NetQoS Reporter/Analyzer Pump service.
   c. Select Stop in the right-click menu.

      The service stops.
4. 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.
5. Open a command prompt window.
6. Run the following command to change the ulimit for the open files limit:
   `ulimit -n ulimit_number`

   Example:
   `ulimit -n 65536`
7. 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.

8. Run the installation or upgrade software:
   `./NFHarvesterSetup9.3.0.bin`

   The language selection screen opens.

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

   The Prior Installation Detected message opens.

10. Review the message and click OK.

    The Welcome screen opens.

11. Click Next.

    The License Agreement screen opens.

12. Review and accept the license agreement:

    a. Read the 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.

       Prerequisite tests look for problems and may cause an error message to open.

13. If the Pre-requisite Check Warning message opens, review it, correct or note any non-critical problems, then click OK.

    The Choose Install Folder screen opens. This screen displays the original root installation path as the default setting.

14. Verify that the specified installation directory is correct, then click Next.

    Important: If you do not use the original installation path, the upgraded software will not run properly.

    If the program does not find certain expected directories in the installation path, an error message opens and the upgrade stops. This problem does not occur when the previous software installation is fully functional.

    The Pre-Installation Summary screen opens.

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

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

16. (Optional) Review the errors by checking the installation log (Harvester_Install_<timestamp>.log in the <install_path> directory).

17. Click Done.

    The upgrade program closes. The Harvester is upgraded and the CA Network Flow Analysis services are started automatically.

18. (Optional) Verify that the following conditions are met:
    - (Two-tier architecture deployment) Harvester services are running.
    - Harvester is receiving data.
    - The revision history shows that the component is upgraded to the correct version. To display the revision history, complete the following substeps:
        a. Start MySQL by entering the following command in a Command Prompt window: mysql
        b. Display the revision history by entering the following command: select * from revision_history

Next:

- To upgrade another Harvester, repeat these steps on the additional Harvester server.
- To continue upgrading a two-tier deployment, Upgrade the Console Server (see page 61).
- To continue upgrading a three-tier deployment, Upgrade the DSA Server (see page 58).

Upgrade the DSA in a Three-Tier Distributed Deployment

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

Note: If you have a Linux DSA, contact your CA Support Availability Manager or Sales Account team to inquire about obtaining a Windows-based DSA.

Follow these steps:

1. Verify that the installation server meets the following requirements:
    - The server is upgrade-ready as described in Verify That the Windows Servers Are Prepared (see page 21).
    - The Harvester servers have been upgraded (see page 53).
2. Verify that processing is complete for the collected DSA data:
    a. Log in to the NFA console server with an account that has administrator privileges for CA Network Flow Analysis.
    b. Locate the following directory on the NFA console server: <install_path>\Reporter\datashare\data\<DSA_server_IP_address>

c. Verify that the directory does not contain any .csv files. If .csv files are present, keep checking until the files are gone. The files are processed and gone within 15 minutes.

3. Log in to the DSA server as a user who is a member of the Administrators group.
4. Start the upgrade: Double-click the DSASetup9.3.0.exe file in Windows Explorer.

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

   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, click the option to accept the license agreement. This option is activated when you scroll to the bottom.
   c. Click Next.

      Prerequisite tests look for problems and may cause an error message to open.
7. If the Pre-requisite Check Warning message opens, review it, correct or note any non-critical problems, then click OK.

   The Choose Install Folder screen opens and displays the original root installation path as the default setting.
8. Proceed through the options to verify the installation directories:
   a. Click Next.

      Important: You must use the original installation path or the upgraded software will not run properly.

      If the program does not find certain directories in the installation path, an error message opens and the upgrade stops. This problem does not occur when the previous software installation is fully functional.

      The Select a Location for the MySQL Data Directory screen opens, which shows the original installation path for the MySQL data directory.

      The Folder Selected Is Not Empty message also opens, which asks you to verify that you have backed up the directory contents.
   b. Click Next in the Select a Location for the MySQL Data Directory screen.

      Important: You must use the original installation path for the MySQL data directory.

      The Select a Location for the MySQL Temp Directory screen opens, which shows the original installation path for the MySQL tmp directory.
   c. Click OK.

d. Click Next.

Important: You must use the original installation path for the MySQL temp directory.

MySQL is configured, then the Pre-Installation Summary screen opens.

e. Click Next.

Important: You must use the original installation path for the MySQL temp directory.

MySQL is configured, then the Pre-Installation Summary screen opens.

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

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

10. Click Done.

    The upgrade program closes. The DSA is upgraded and the DSA services are restarted.

11. (Optional) Verify that the following conditions are met:

    - DSA services are running.
    - The DSA is receiving data.
    - The revision history shows that the component is upgraded to the correct version. To display the revision history, complete the following substeps:

      a. Start MySQL by entering the following command in a Command Prompt window: mysql

      b. Display the revision history by entering the following command: select * from revision_history

12. (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 migration of DSA database table data begins as soon as the CA NFA DSALoader service restarts. The DSA_Install 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.

Next:

- To upgrade an additional DSA on another server, repeat these steps.
- To upgrade the console server (see page 61), go to the next topic.

Upgrade 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 upgrade the NFA console on a dedicated Windows server or virtual machine.

Follow these steps:

1. Verify that the server meets the following requirements:
   - The server is upgrade-ready as described in Verify That the Windows Servers Are Prepared (see page 21).
   - The Harvester servers have been upgraded (see page 53).
   - If you have a three-tier architecture deployment, the DSA servers have been upgraded (see page 58).
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. (Three-tier architecture only) Verify that the DSAs have retrieved all of the 15-minute data from the NFA console server:
   a. Locate the following directory on the NFA console server:
   <install_path>\reporter\datashare\data\<DSA_server_IP_address>
   b. Verify that the directory does not contain .csv files. If .csv files are present, wait until the files are gone. Once you stop the pump service, the .csv files should be gone within 15 minutes.
4. Start the upgrade: Double-click the RAConsoleSetup9.3.0.exe file in Windows Explorer on the NFA console server.

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

   The Welcome screen opens.
6. Click Next.

   The License Agreement screen opens.
7. 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.

f. Click Next.

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

   a. Correct the problems now or wait until the upgrade program finishes. For more information about the warnings, see Troubleshooting (see page 79).

   b. Click OK.

      The Upgrading Existing Installation message opens.

9. Review the information:

   a. Verify that the existing and post-upgrade version information is correct, then click OK.

      The message reopens and reports the root installation path. The upgrade program always uses the original path, which is C:\CA\NFA by default.

   b. Review the path information, then click OK.

      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 default location is C:\CA\NFA. Use the same installation path for the Harvester and for NFA console servers. We recommend that you install CA Network Flow Analysis components on a nonsystem drive.

    The Pre-Installation Summary screen opens.

11. Review the information, then click Install.

    The Installing NFA screen opens. When the upgrade is complete, the Install Complete screen opens and reports any errors.

12. (Optional) If errors occurred, see the installation log: <install_path>\NFA_Install_<timestamp>.log.

13. Exit from the upgrade 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 upgrade program closes. If you selected the option to restart now, the system restarts and the upgrade is finalized.

14. (Optional) Check the revision history to verify that the software is upgraded to the correct version:
    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-upgrade tasks (see page 65).

Chapter 7: Post-Upgrade Tasks

Complete the following post-installation tasks:

- Configure SNMP on any Linux Harvesters in your deployment. (see page 66)
- 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 degraded system performance.
- We recommend that you install Flash is on systems with desktops that access the NFA console and install Reader on systems with desktops that access PDF documentation.

<table>
<tr><th>Stand-Alone Server</th><th>Distributed NFA Console Server</th><th>Distributed Harvester Server (Windows)</th><th>Distributed 3-Tier DSA Server</th></tr>
<tr><td colspan="4">■ Synchronize system time (see page 68).</td></tr>
<tr><td colspan="2">■ (Recommended) Update the list of trusted internet sites. (see page 69) *</td><td colspan="2"></td></tr>
<tr><td>■ (Recommended) Modify router ACLs (see page 70)</td><td></td><td>■ (Recommended) Modify router ACLs. (see page 70) **</td><td></td></tr>
<tr><td colspan="2">■ (Recommended) Disable UAC. (see page 70)</td><td colspan="2"></td></tr>
<tr><td colspan="2">■ (Recommended) Configure Web content expiration (see page 71).</td><td colspan="2"></td></tr>
<tr><td colspan="4">■ (Recommended) Add a key to prevent SNMP false positives. (see page 72)</td></tr>
<tr><td colspan="4">■ (Optional) Configure the Recycle Bin. (see page 72)</td></tr>
<tr><td colspan="4">■ (Optional) Disable unneeded services (see page 73).</td></tr>
</table>

* Verify that this task also has been completed for the systems that access the NFA console.

** 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:

Upgrade and Check Performance Center

Make sure the NFA console server or stand-alone server is registered as a data source for one of the following:

- CA Performance Center version 2.4/2.3 or
- CA NetQoS Performance Center 6.1.205 SP2/6.1.194

If you need to upgrade CA Performance Center, upgrade it now. For instructions, see the *CA Performance Center Installation Guide*.

If CA Network Flow Analysis is not registered as a data source, some of the function links on the Administration page are disabled. For instructions about registering, see the *CA Network Flow Analysis Administrator Guide* topic "Register CA Network Flow Analysis." After you register, review the results in the Performance Center Console and the NFA console. Make any adjustments that are needed.

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 prerequisite tests detect. Prerequisite tests can generate warnings or failure notices. If you receive a warning, you can correct the problem immediately or wait until the installation or upgrade software runs. You must correct a failure before you can continue. Most of the troubleshooting topics describe prerequisite failures.

Note: Prerequisite tests often rely on general indicators to identify problems. Passing a prerequisite test is not a guarantee that everything is configured properly. It is important to meet all of the requirements and complete the configuration tasks that are described in this guide.

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 23).	Warning	Stand-alone or NFA console
DEP	Verifies that the winmgt service is running. Configure DEP as described in this guide. (see page 32)	Warning	Windows servers
FIPS Algorithm Policy	Verifies that the FIPS Algorithm policy is not enabled (see page 80).	Verify automatic fix or Failure	Stand-alone or NFA console
IIS Installed	Verifies that the wcsvc service is running. Install and configure IIS as described in this guide (see page 27).	Warning	Stand-alone or NFA console
IIS Version	Checks the Registry for IIS version 7.0.	Warning	Stand-alone or NFA console
.NET 3.5 Version	Checks for .NET version 3.5 SP1. If version 3.5 is found, turns on SP1.	Failure	Stand-alone or NFA console
NPC Installation Detected	Checks if NPC is installed on the server (see page 81).	Failure	Stand-alone or NFA console
Service Control command	Verifies that the Windows System32 directory contains the sc.exe file (see page 81).	Failure	Windows servers
SNMP	Verifies that the snmp service is running and the process ID is present. Configure SNMP on Windows servers (see page 29) and Linux servers (see page 38).	Warning	All servers

Test	Description	Warning or Failure	Server
Windows 2003 Detected	Verifies that the server is running Windows Server 2008, not Windows Server 2003 (see page 82).	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 38) 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

I

L

M

N

O

P

R

S

T

U

W