CA Network Flow Analysis

Installation Guide

9.1.2

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

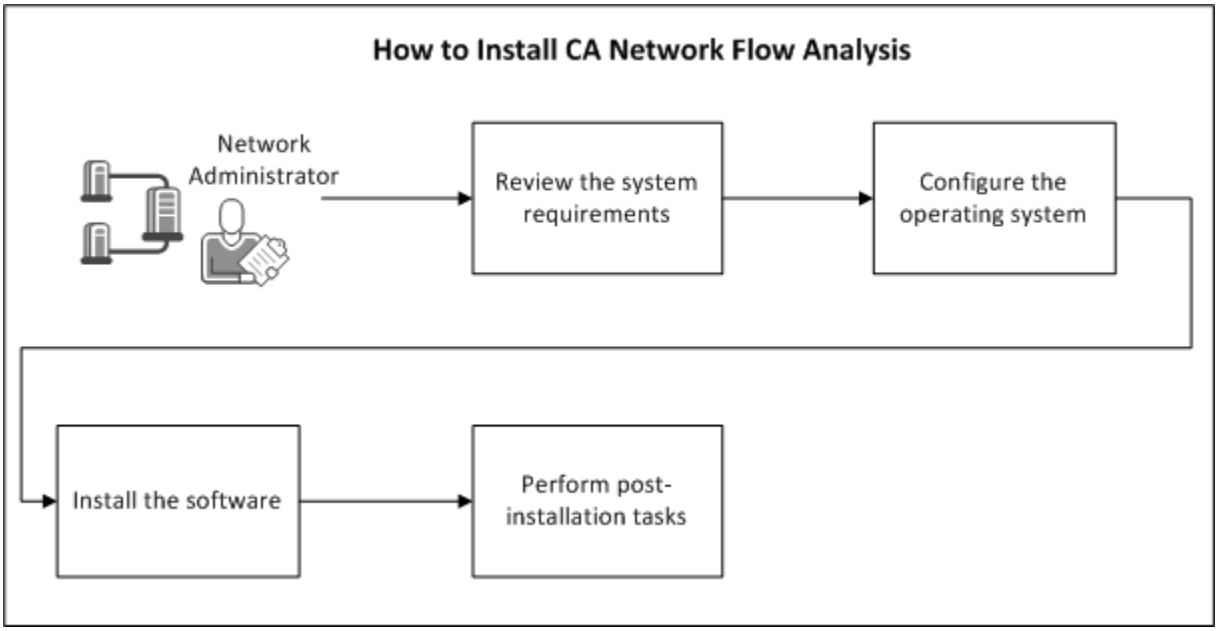
To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction

CA Network Flow Analysis helps you understand how application traffic affects your network performance.

The following diagram describes the process of installing CA Network Flow Analysis.



Chapter 2: System Requirements

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

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

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

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

This section contains the following topics:

Windows Operating System Requirements

Microsoft Windows servers that host CA Network Flow Analysis components have the following additional operating system requirements.

Microsoft Windows 2008 R2, Standard edition on a 64-bit processor, with:

- Latest service pack and all important updates installed
- CA Performance Center 2.2.00 installed
- .NET Framework 3.5 SP1

  If the .NET Framework software is missing or version 4.0 is installed, the a prerequisite check causes the installation or upgrade program to exit.
- Java Runtime Engine (JRE) 1.6u41 which is included with the ISO files from CA Technical Support.

  If the installation server does not have JRE version 1.6 installed, the installation or upgrade program fails to launch. We recommend that you install JRE 1.6u41, the version that was used in CA Network Flow Analysis 9.1.2 testing. Untested JRE versions may produce unexpected results.
- English, Chinese (Simplified), French (France), or Japanese language

- Service Control command (sc.exe file) in the Windows System32 directory

  This command is required for command-line operation. If the file is missing, a prerequisite check causes the installation or upgrade program to exit.
- Minimum display resolution of 1024x768 (XGA)
- NFA console and standalone servers: ASP.NET 2.0 installed, including COM+ network access, IIS, and ASP. ASP.NET 2.0 comes with the .NET Framework 3.5 SP1
- Operating system configured as described in this document, including SNMP enabled
- (Recommended) Remote Desktop Connection enabled to allow remote access by the administrator

Notes:

- CA Network Flow Analysis 9.1.2 supports installation on servers with IPv4 addresses. Installation is not supported at this time on servers with IPv6 addresses.
- We recommend that you configure a single NIC (network interface card) on each server.
- The requirements that are described throughout this section apply to both physical and virtual deployments.

Hardware Requirements for a Distributed Deployment (Windows)

In a *distributed* deployment, the NFA console and Harvester are installed on separate servers.

CA tested the CA Network Flow Analysis solution with the following recommended minimum hardware configuration. Your requirements may vary depending on the number of interfaces, applications, and users in your network.

Note: The recommended specifications described here apply to both physical and virtual deployments. The requirements represent the configuration of CA appliances that are currently shipping. You can run CA Network Flow Analysis successfully if your configuration does not meet these specifications, although your performance may vary. You can also run CA Network Flow Analysis on a configuration that exceeds these specifications.

NFA console server

The server that hosts the NFA console has the following recommended minimum specifications.

- 2.26-GHz quad-core processor
- 3 GB RAM
- Three 146-GB 10,000-RPM SAS hard drives in RAID 5 configuration
- 1-Gb LAN port
- Partition for the C: drive that contains 40 GB for the operating system
- Partition for a D: drive or other separate drive that contains 41 GB for the CA Network Flow Analysis installation files and at least 300 GB of available space for data

Harvester server

The server that hosts the Harvester has the following recommended minimum 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
- Partition for the C: drive that contains 40 GB for the operating system
- Partition for a D: drive or other separate drive that contains 41 GB for the CA Network Flow Analysis installation files and 1.5 TB of available space for data

Distributed Storage Appliance (DSA) server in a three-tier deployment

The server that hosts the Harvester has the following recommended minimum specifications.

- 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 for a D: drive or other separate drive that contains 41 GB for the CA Network Flow Analysis installation files and 1.5 TB of available space for data

Hardware Requirements for a Standalone System (Windows)

A *standalone* configuration is a single server on which the NFA console and Harvester are installed.

CA tested the CA Network Flow Analysis solution with the following recommended hardware configuration. Your requirements may vary depending on the number of interfaces, applications, and users in your network.

Note: The recommended specifications described here apply to both physical and virtual deployments. The requirements 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.

The server has the following minimum requirements:

- 2.26-GHz quad-core processor
- 3 GB RAM
- Three 146-GB 10,000-RPM SAS hard drives in RAID 5 configuration
- 1-Gb LAN port
- Partition for the C: drive that contains 40 GB for the operating system
- Partition for a D: drive or other separate drive that contains 41 GB for the CA Network Flow Analysis installation files and at least 300 GB of available space for data

Linux Operating System Requirements

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

- Red Hat Enterprise Linux 5.5 or 5.6 on a 64-bit processor
- Java Runtime Engine (JRE) 1.6u41, which is included with the ISO files from CA Technical Support.

  If the installation server does not have JRE version 1.6 installed, the installation or upgrade program fails to launch. We recommend that you install JRE 1.6u41, the version that was used in CA Network Flow Analysis 9.1.2 testing. Untested JRE versions may produce unexpected results.
- English, Chinese (Simplified), French (France), or Japanese language
- 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 files
  - 1.5 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 9.1.2 supports installation on servers with IPv4 addresses. Installation is not supported at this time on servers with IPv6 addresses.
- The requirements described in this section apply to both physical and virtual deployments.

Important: CA Network Flow Analysis requires DNS resolution. If DNS is not configured, add system entries to the /etc/hosts file on your server manually.

Chapter 3: Preparing Windows Servers for the Upgrade

This section contains the following topics:

Prepare the Windows Servers

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

- System Requirements: Verify that the installation servers meet the requirements that are described in Windows Operating System Requirements (see page 9).
- Localized deployments: Verify that the appropriate language packs are installed.

Verify that each of the Windows servers has the following software installations and configurations in place:

Standalone Server	Distributed NFA Console Server	Distributed Harvester Server	Distributed 3-Tier DSA Server
■ Java Runtime Engine (JRE) 1.6u41 *			
■ SC.exe in the Windows System32 directory *			
■ .NET Framework 3.5 SP1 *			
■ General prerequisites (see page 37)			
■ Firewall on Windows servers (see page 17)			
■ SNMP and SMTP on Windows servers (see page 23) **			
■ Flash Player and Reader (see page 21) **			
■ IIS, COM+, and ASP (see page 21) **			
■ Web content expiration (see page 24)			
■ Supported browser (see page 17) **			
■ Community name "public" (see page 24)			
■ Disabling IPv6 addresses on Windows (see page 25)			
■ SMTP relay restrictions (see page 26)			
■ DEP setting (see page 27) **			
■ Recycle Bin (see page 28)			
■ Disabling unneeded services (see page 29)			
■ Preventing SNMP from logging false positives (see page 30)			

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

Note: 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 during installation.

Supported Web Browsers

A browser is required on the NFA console or standalone server. Microsoft Internet Explorer version 8 is recommended. Other browsers or browser versions may work with CA Network Flow Analysis, but have not been tested.

Note: To set up CA Network Flow Analysis and work with data in the CA Performance Center Console, use Internet Explorer 8 with compatibility mode turned off. To work in CA Network Flow Analysis directly, you can use Internet Explorer 7 or 8 with compatibility mode turned on or off.

If Internet Explorer 8 Developer Tools are installed, you can turn off compatibility mode for the current browser session:

1. Press F12 on your keyboard.
2. Click the Browser Mode item on the main menu.
3. Select Internet Explorer 8.

Firewall Requirements

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:

- Standalone system (see page 17)
- Two-tier distributed deployment (see page 18)
- Three-tier distributed deployment (see page 19)

Ports to Open for a Standalone System

Open the following ports on a standalone 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]
	Trap destination	■ UDP 162 [traps]
Router	Harvester	■ UDP 9995 [flow]
Administrators and users	NFA console	■ TCP/HTTP 80 [UI access and SNMP web services] ■ TCP/HTTP 8381 [Single Sign-On] ■ TCP 8681 [Report Information Base (RIB) reporting]
CA Performance Center Console	NFA console	■ TCP/HTTP 80 [device and interface synchronization with CA Performance Center] ■ TCP 8681 [data import for CA Network Flow Analysis views in CA Performance Center]
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]

From	To	Port [Function]
	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]
	Trap destination	■ UDP 162 [traps]
Router	Harvester	■ UDP 9995 [flow]
Administrators and users	NFA console	■ TCP/HTTP 80 [UI access and SNMP web services] ■ TCP/HTTP 8381 [Single Sign-On] ■ TCP 8681 [Report Information Base (RIB) reporting]
CA Performance Center Console	NFA console	■ TCP/HTTP 80 [device and interface synchronization with CA Performance Center] ■ TCP 8681 [data import for CA Network Flow Analysis views in CA Performance Center]
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]

From	To	Port [Function]
	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]
	DSA	■ TCP 3307 [CA MySQL] ■ TCP 3308 [MySQL] ■ UDP 161 [Watchdog service]
Harvester	Routers (SNMP interface, read-only)	■ UDP 161 [SNMP polling]
	Trap destination	■ UDP 162 [traps]
DSA	NFA console	■ TCP 3308 [MySQL] ■ TCP 8080 [File Web Service, which retrieves files from the NFA console without using a file share]
Router	Harvester	■ UDP 9995 [flow]
Administrators and users	NFA console	■ TCP/HTTP 80 [UI access and SNMP web services] ■ TCP/HTTP 8381 [Single Sign-On] ■ TCP 8681 [Report Information Base (RIB) reporting]
CA Performance Center Console	NFA console	■ TCP/HTTP 80 [device and interface synchronization with CA Performance Center] ■ TCP 8681 [data import for CA Network Flow Analysis views in CA Performance Center]
Administrators	Each server	■ TCP 3389 [Remote Desktop, if Remote Desktop is used] ■ TCP 5800, 5801, 5900, 5901 [VNC, if VNC is used]

Install the Reader and Flash Player Applications

Adobe Flash Player is required to view reports and status. Install the latest version of Flash Player from http://get.adobe.com/flashplayer/.

Adobe Acrobat Reader is required on any system that is used to view the product documentation in PDF format. Install the latest version of Acrobat Reader from http://get.adobe.com/reader/.

Enable IIS, COM+, and ASP

Enable IIS, IIS 6 Management Compatibility mode, COM+ Network Access, and ASP on a standalone installation server or an NFA console installation server.

Follow these steps:

1. Log in to the server as an administrator.
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.

      A confirmation message appears.
   d. Click Add Required Role Services in the confirmation message.

      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.

      A confirmation message appears.
   b. Click Add Required Role Services in the confirmation message, 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 appears in the wizard.

   b. Select the IIS 6 Management Compatibility check box in the Management Tools section of the list, then 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 Progress page is shown until the installation is complete, when the Results page opens.

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

      The Installation Report page displays a summary of your changes, information about the changes, and the location of the full installation log.

   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 on the left.

      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 Progress page is shown until the installation is complete, when the Results page opens.

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

      The Installation Report page displays a summary of your changes, information about the changes, and the location of the full installation log.

   f. Click Close.

      The Installation Results page closes.

9. Exit from the Server Manager window.

Configure SNMP on a Windows Server

Install the SNMP service and the SMTP server on a standalone installation server or an NFA console installation server.

The Simple Network Management Protocol (SNMP) is required by the Watchdog services. The Simple Mail Transfer Protocol (SMTP) service is an IIS component that is used for delivering outgoing email messages.

Follow these steps:

1. Log in to the server as an administrator.
2. Navigate to Administrative Tools, Server Manager.

   The Server Manager window opens.
3. Click Features in the Console tree on the left.

   The Server Manager window displays a list of features that are installed on the server.
4. Click Add Features under Features Summary.

   The Select Features page displays a list of installed and available features in the Add Features wizard.
5. Select SNMP Service in the Features list.

   A confirmation message appears.
6. Click Add Required Features.

   The Confirm Installation Services page identifies the features to be installed. The page also displays important messages about the installation.
7. Click Install.

   The Installation Progress page shows the progress of the installation. When installation is complete the Installation Results page identifies the new features and indicates whether you need to restart the server.
8. Click Close.

   A message asks whether you want to restart the server now.
9. Click No.
10. Repeat steps 5 through 8 for the SMTP Server.

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

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

Configure Web Content Expiration

Configure IIS to ensure that the displayed data is fresh. With the Expire Web Content Immediately setting enabled, the browser displays an updated page from the server rather than a cache.

Note: Complete this task for a standalone installation server or an NFA console installation server.

Follow these steps:

1. Log in to the server as an administrator.
2. Navigate to Administrative Tools and double-click Internet Information Services (IIS) Manager.

   The Internet Information Services Manager window opens.
3. Click your server name in the Connections pane.

   The server features appear in the right pane.
4. Double-click the HTTP Response Headers icon in the HTTP Features group.

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

   The Set Common Headers dialog opens.
6. Select the following options:
   - "Expire Web content" check box
   - Immediately
7. Click OK.

   The Set Common Headers dialog closes.
8. Close the Internet Information Services Manager window.

Configure "public" as a Community Name

The community name "public" must be an accepted to prevent polling errors, and to help CA Network Flow Analysis components work properly.

Follow these steps:

1. Log in to the server as an administrator.
2. Select Start, Administrative Tools, Server Manager.

   The Server Manager window opens.

3. Expand the Configuration list in the Console tree on the left.
4. Click Services under Configuration.

   The Services list opens.
5. Right-click the SNMP Service row and select Properties.

   The SNMP Service Properties dialog opens.
6. Click the Security tab.
7. Click Add.

   The SNMP Service Configuration dialog opens.
8. Set the following options:
   - Community rights: Select Read Only.
   - Community Name: Enter **public**.
9. Click Add.

   The SNMP Service Properties dialog displays "public" in the list of accepted community names.
10. Click OK.

Configure the IP Address Format on Windows Servers

Make sure that the connections for your Windows installation servers are not set up to bind to IPv6 addresses.

Note: These 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 to the server as an administrator.
2. Open the Network Connections window:
   a. Open the Control Panel and click Network and Internet.

      The Network and Internet window opens.

   b. Click Network and Sharing Center.

      The Network and Sharing Center window opens.

   c. Click Change adapter settings on the left side of the window.

      The Network Connections window opens.
3. Right-click the connection and select Properties from the menu.

   The Properties dialog box opens.

4. Clear the check box labeled 'Internet Protocol Version 6 (TCP/IPv6),' if it is selected.
5. Click OK.

   Any changes that you have made are saved. The Properties dialog box closes.
6. Close the Network Connections window.

Configure SMTP Relay Restrictions

You can control mail relays to the IIS Simple Mail Transport Protocol (SMTP) virtual server for tighter security. When the SMTP virtual server is openly accessible, a user can distribute unwanted email through it.

Configure SMTP virtual server relay restrictions to allow access only to 127.0.0.1 and to disallow all other computers. The restrictions allow only selected computers to relay messages through the SMTP virtual server. Other computers cannot relay messages to the SMTP virtual server even when they meet the requirements set in the Authentication dialog.

Follow these steps:

1. Log in to the server as an administrator.
2. Install the SMTP Server feature (see page 23).
3. Navigate to Administrative Tools and double-click Internet Information Services (IIS) 6.0 Manager.

   The Internet Information Services (IIS) 6.0 Manager window opens.
4. Expand your server name in the Console tree on the left.

   The server details are expanded. The SMTP Virtual Server appears under your server.

   Note: If the SMTP Virtual Server is not visible, add the SMTP server feature (see page 23).
5. Right-click Default SMTP Virtual Server and click Properties.

   The Default SMTP Virtual Server Properties dialog opens.
6. Click the Access tab, then click Relay.

   The Relay Restrictions dialog opens.
7. Click Add.

   The Computer dialog opens.
8. Specify the following settings:
   - Select Single computer.
   - IP address: Enter **127.0.0.1**.

9. Click OK.

   The Relay Restrictions dialog shows 127.0.0.1 in the Computers list. The computer with the IP address 127.0.0.1 has the status of "Granted" in the Access column.

10. Specify the following relay restrictions options:

    - "Only the list below:" Selected. This option allows only the computers in the Computers list to relay messages through the SMTP virtual server.
    - "Allow all computers which successfully authenticate to relay, regardless of the list above" check box: Cleared.

11. Click OK.

    The SMTP Virtual Server Properties dialog opens. With the options you chose, only the listed computers can relay messages through the SMTP virtual server. Unlisted computers cannot relay messages to the SMTP virtual server even if they meet the requirements set in the Authentication dialog.

12. Click OK.

    The SMTP Virtual Server Properties dialog closes.

13. Select File, Exit in the Internet Information Services (IIS) 6.0 Manager window.

Configure DEP

Data Execution Prevention (DEP) helps to prevent code executing from data pages. We recommend that you configure the DEP policy as described in this topic.

Follow these steps:

1. Log in to the server as an administrator.
2. Open the Advanced tab of the System Properties dialog. For example:
   a. Select Start and right-click Computer.
   b. Select Properties from the menu.

      The System window opens.

   c. Click "Advanced system settings" on the left.

      The System Properties dialog opens with the Advanced tab displayed.
3. Click Settings in the Performance section.

   The Performance Options dialog opens.
4. Click the Data Execution Prevention tab.
5. Select "Turn on DEP for essential Windows programs and services only."

6. Save your settings and exit:
   a. Click OK in the Performance Options dialog.

      Your settings are saved and the dialog closes.

   b. Click OK in the System Properties dialog.
7. A message opens and informs you that you must restart your system to make the new settings take effect.
8. (Optional) Restart your system before you install or upgrade the software.

   If you proceed with software installation or upgrade without restarting the system, the prerequisite test displays a warning about your DEP configuration

Configure the Recycle Bin

Optionally, configure the way the Recycle Bin deletes files.

Follow these steps:

1. Right-click the Recycle Bin and select Properties.

   The Recycle Bin Properties dialog opens.
2. Select Local Disk (C:).
3. Select "Don't move files to the Recycle Bin. Remove files immediately when deleted."
4. Click Apply.
5. Repeat steps 2 through 4 for each additional drive that you want to configure.
6. Click OK.

Disable Unneeded Services

Use the Services window to disable unnecessary services.

Follow these steps:

1. Navigate to the Administrative Tools window.
2. Double-click Services.

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

   Do not select Stop or the services will start again when the server is rebooted.

- 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

Prevent False Positive Events

We recommend that you create an empty TrapConfiguration key in the Windows Registry to prevent the SNMP service from logging false positive events.

Follow these steps:

1. Log in as a user who is a member of the Administrators group.
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.

Chapter 4: Preparing Linux Servers for the Upgrade

This section contains the following topics:

Prepare the Linux Servers

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

- System Requirements: Verify that the installation servers meet the requirements described in Linux Operating System Requirements (see page 12).
- Verify that each of the Harvester Linux servers is ready for the installation by:
  - Installing the supported version of the JRE: Java Runtime Engine (JRE) 1.6u41.
  - 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 32)

    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 34)
  - Disabling IPv6 networking (see page 33)

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 during installation.
- The appropriate language packs are required for localized deployments.

Configure SNMP on Linux Servers

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

- Install Net-SNMP if it is not already installed.
- Set up the Net-SNMP configuration file.
- Configure SNMP to start automatically on boot.
- Start the snmpd service.

Follow these steps:

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

   b. Get and install Net-SNMP if it is not installed. For example, you can get Net-SNMP from the Linux Package Manager.
2. Log in as root and open a shell prompt.
3. Highly Recommended: Copy the configured Net-SNMP configuration file to the Netflow directory, overwriting the unconfigured snmpd.conf file. To enable Watchdog SNMP polling for the Harvester, you must complete this step.

   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.

   a. Back up the configuration file in /etc, for example by entering the following command (Recommended):
      `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 directory you used for installing the Harvester: /opt/CA/NFA/ or a custom location
   c. Copy the snmpd.conf file to the /etc/snmp directory, overwriting the existing file:
      `cp -i snmpd.conf /etc/snmp`
   d. Confirm the overwrite 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`

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

5. 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 appropriate community string setting.

Disable IPv6 Networking on Linux Servers

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

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

To disable IPv6 networking, modify the following files:

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

Follow these steps:

1. Make sure that you are logged in with root privileges.
2. Edit the modprobe.conf file:

   a. Open the /etc/modprobe.config file in a text editor.

   b. Append the following line:
   `install ipv6 /bin/true`

   c. Save and close the file.

   The modprobe.conf file is now configured so that when the system attempts to load the IPv6 kernel module, it executes the command 'true' instead of loading the module. The 'true' command performs no action.

3. Edit the network file:
   a. Open the /etc/sysconfig/network file in a text editor.
   b. Update or add the following lines to match the text strings shown:
      ```
      NETWORKING_IPV6=no
      IPV6INIT=no
      ```
   c. Save and close the file.
4. Reboot the server:
   ```
   reboot
   ```
5. Verify that IPv6 is disabled:
   a. Enter the following command at a terminal:
      ```
      lsmod | grep ipv6
      ```
      If the command returns no output, the IPv6 kernel module is not running: It has been removed successfully.
   b. Enter the /sbin/ifconfig command:
      ```
      /sbin/ifconfig
      ```
      Check the output to verify that it contains only IPv4 addresses and no IPv6 addresses.

Disable the iptables Firewall for Linux Servers

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 Requirements list (see page 17). In addition make sure that you have full localhost to localhost access. This step is required because CA Network Flow Analysis uses RMI (Remote Method Invocation) access.

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

Follow these steps:

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

   ```
   service iptables stop

   chkconfig iptables off

   chkconfig –-list |grep iptables
   ```

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

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

Chapter 5: Installing the Software

This section contains the following topics:

Prerequisites

Before you install or upgrade the CA Network Flow Analysis software, perform the following tasks:

- Obtain the CA Network Flow Analysis installation files from CA Technical Support. Then perform one of the following tasks:
  - Burn the ISO files to a CD-ROM or DVD.
  - Extract the contents of the ISO files by using an ISO image software application. Many ISO image applications are free.

  Extract the appropriate files to the installation servers:
  - Standalone servers:
    - NFHarvesterSetup9.1.2.exe
    - RAConsoleSetup9.1.2.exe
    - consoletool-exe.jar
  - Windows Harvester servers in distributed architecture deployments:
    - NFHarvesterSetup9.1.2.exe
  - Linux Harvester servers in distributed architecture deployments:
    - NFHarvesterSetup9.1.2.bin
  - DSA servers in three-tier distributed architecture deployments:
    - NFDSASetup9.1.2.exe

  You can install the software locally or remotely.
- Install CA Performance Center 2.2.00 in your environment. CA Network Flow Analysis 9.1.2 is not compatible with previous versions of CA Performance Center.

  Administrators use CA Performance Center for several administrative functions, including creating and managing groups, domains, user accounts, and user settings.
- Assign a static IP address to the server. Set the Harvester server IP address to match the flow export destination that is assigned to each router.

- Prepare the servers as described in the following sections:
  - Preparing Windows Servers for the Upgrade
  - Preparing Linux Servers for the Upgrade

  In particular, verify that the servers meet the following requirements :
  - (All Servers) The supported JRE version is installed: Java Runtime Engine (JRE) 1.6u41.
  - (Windows Servers) The Service Control command (sc.exe file) is in the Windows System32 directory. This command is required for command-line operation. If the file is missing, the prerequisite check for it fails and the upgrade program exits.
  - (Windows Servers) The .NET Framework version 3.5 SP1 is installed.
- Disable the following third-party software on all installation servers:
  - Server monitoring and maintenance software
  - Antivirus

  Note: When you enable antivirus scans later, exclude the CA Network Flow Analysis installation path and its subdirectories.
- Exclude the following directories from real-time scans:C:\Windows\Temp and *<NFA_install_path>* and all its subdirectories. Real-time scans of these directories can corrupt the database.
- Do not implement drive space compression on the installation server. Drive space compression can cause database losses and degraded system performance.
- Stop other programs from running during the installation or upgrade.
- Restart all servers to ensure that all the installed operating system patches are applied.
- Ensure that no one else is logged in to the server during the installation or upgrade.

Note: If you exit from the upgrade program before the upgrade is completed, then restart the upgrade, the program resumes from your last saved change. The program does not start over from the beginning.

Install the Components on a Standalone Server

A *standalone configuration* consists of one server that hosts the NFA console and the Harvester. Complete the steps in this topic to install all of the CA Network Flow Analysis components on a single Windows server or virtual machine.

Before You Begin: Verify that the installation server meets the following requirements:

- Server is upgrade-ready as described in Prepare the Windows Servers (see page 16).
- Java Runtime Engine (JRE) 1.6u41 is installed.

Follow these steps to complete the Harvester phase of the installation:

1. Log in to the server as an administrator.
2. Start the Harvester phase of the installation: Double-click the NFHarvesterSetup9.1.2.exe file.

   A check verifies that the installation server has a supported version of the Java Runtime Engine (JRE) installed. If the check fails, an error message opens (see page 63). You cannot launch the upgrade program until this problem is corrected.

   If the server passes the Java prerequisite check, the program starts and the language selection screen opens.
3. Verify that the appropriate language is selected, then click OK.

   The Welcome screen opens.

   Click Next in the Welcome screen.

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

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

6. Verify or specify the installation directories:

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

      The default location is C:\CA\NFA. We recommend that you install CA Network Flow Analysis components on a nonsystem drive that you have set up for CA Network Flow Analysis. The NFA console will be installed to the same directory that you choose for the Harvester.

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

      The Select a Location for the MySQL Data Directory screen opens after a moment. This screen shows the default installation path for the MySQL data directory.

   c. (Optional) Click Choose to change the MySQL installation location.

      We recommend that you use a drive that has at least 40 GB of available space for the database.

   d. Click Next when the MySQL database path setting is correct.

      The Select a Location for the MySQL Temp Directory screen opens, which shows the default installation path for the MySQL tmp directory.

   e. (Optional) Click Choose to change the tmp directory location.

   f. Click Next when the MySQL tmp directory path setting is correct.

      MySQL51 is configured, then the Pre-Installation Summary screen opens.

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

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

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

   <NFA_install_path>/Harvester_Install_MM_DD_YY_hh_mm_ss.log (where MM_DD_YY_hh_mm_ss reflects the timestamp)

9. Click Done in the Install Complete screen.

   The Harvester installation program closes.

Follow these steps to complete the NFA console phase of the installation:

1. Start the NFA console installation software: Double-click the RAConsoleSetup9.1.2.exe file in Windows Explorer.

   A check verifies whether a supported version of the Java Runtime Engine (JRE) is installed. If the check fails, an error message opens (see page 63). You cannot launch the upgrade program until this problem is corrected.

   If the server passes the Java prerequisite check, 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 in the Welcome screen.

   The NFA Console License Agreement screen opens.

4. Review and accept the license agreements:

   a. Read the NFA console license agreement and scroll down.

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

5. Click Next.

   Prerequisite tests are run on the installation server. If an error message opens that requires attention, see Troubleshooting.

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

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

   b. Click OK to close the message.

      A test verifies that the installed version of CA Network Flow Analysis is supported for upgrade. The Singlebox Confirmation message opens when the verification is complete. This message asks you to confirm that you want a standalone deployment of CA Network Flow Analysis.

7. Review the Singlebox Confirmation information and click OK.

   The Pre-Installation Summary screen opens after a moment.

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

   The Installing NFA screen opens. Progress is shown in the status bar and messages. When the NFA console installation is complete, the Install Complete screen opens.

   a. Select "Yes, restart my system."

   b. Click Done.

      The NFA console is installed and your system is ready for post-installation configuration (see page 53).

Next: Complete the post-upgrade tasks.

Install a Distributed Deployment

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

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

- Upgrade the Harvester on a Windows Server, or
- Upgrade the Harvester on a Linux Server
- Upgrade the Console

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

- Upgrade the Harvester on a Windows Server
- Upgrade the DSA Server
- Upgrade the Console

Note: The steps in these topics assume that you follow the recommended upgrade order: Harvester upgrades, DSA upgrades (if any), then NFA console upgrade.

Install the Harvester on a Windows Server

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

In a distributed deployment, each Harvester is 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.

Before You Begin: Verify that the installation server meets the following requirements:

- Server is upgrade-ready as described in Prepare the Windows Servers (see page 16).
- Java Runtime Engine (JRE) 1.6u41 is installed.

Follow these steps:

1. Log in to the server as a user with administrative privileges.
2. Start the upgrade: Double-click the NFHarvesterSetup9.1.2.exe file in Windows Explorer on the Harvester server.

   A check verifies that the installation server has a supported version of the Java Runtime Engine (JRE) installed. If the check fails, an error message opens (see page 63). You cannot launch the upgrade program until this problem is corrected.

   If the server passes the Java prerequisite check, the program starts and the language selection screen opens.
3. Verify that the appropriate language is selected, then click OK.

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

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

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

      Once the server passes the required checks and you close any noncritical messages that appear, the Choose Install Folder screen opens and displays the default root installation path.
7. Verify or specify the installation directories:
   a. (Optional) Click Choose in the Choose Install Folder screen to change the installation location.

      The default location is C:\CA\NFA. We recommend that you install CA Network Flow Analysis components on a nonsystem drive that you have set up for CA Network Flow Analysis. The NFA console will be installed to the same directory that you choose for the Harvester.

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

   The Select a Location for the MySQL Data Directory screen opens after a moment. This screen shows the default installation path for the MySQL data directory.

c. (Optional) Click Choose to change the MySQL installation location.

   We recommend that you use a drive that has at least 40 GB of available space for the database.

d. Click Next when the MySQL database path setting is correct.

   The Select a Location for the MySQL Temp Directory screen opens, which shows the default installation path for the MySQL tmp directory.

e. (Optional) Click Choose to change the tmp directory location.

f. Click Next when the MySQL tmp directory path setting is correct.

   MySQL51 is configured, then the Pre-Installation Summary screen opens.

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

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

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

   <NFA_install_path>/Harvester_Install_MM_DD_YY_hh_mm_ss.log (where MM_DD_YY_hh_mm_ss reflects the timestamp)

10. Click Done in the Install Complete screen.

    The Harvester installation program closes.

Next: Repeat these steps to install a Harvester on another server or install the console (see page 49).

Install the Harvester on a Linux Server

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

Before You Begin: Verify that the following requirements are met:

- Server is upgrade-ready as described in Prepare the Linux Servers (see page 31).
- Java Runtime Engine (JRE) 1.6u41 is installed.
- SNMP is configured as described in Configure SNMP on a Linux Server (see page 32).

Follow these steps:

1. Log in to the target computer 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.

2. Open a command prompt window.

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

   Example:
   `ulimit -n 65536`

4. Prepare the installation or upgrade file for execution:

   a. 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. 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 NFHarvesterSetup9.1.2.bin`

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

      The file permission settings are displayed.

5. Run the installation or upgrade software:

6. ./NFHarvesterSetup9.1.2.bin

   A check verifies that the installation server has a supported version of the Java Runtime Engine (JRE) installed. If the check fails, an error message opens (see page 63). You cannot launch the upgrade program until this problem is corrected.

   If the server passes the Java prerequisite check, the program starts and the language selection screen opens.

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

   The Welcome screen opens.

8. Click Next in the Welcome screen.

   The License Agreement screen opens.

9. Review and accept the license agreement:

   a. Read the license agreement and scroll down.

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

c. Click Next.

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

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

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

b. Click OK to close the message.

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

11. Verify or specify the installation directories:

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

The default location is /opt/CA/NFA. We recommend that you install CA Network Flow Analysis components on a nonsystem drive that you have set up for CA Network Flow Analysis. The NFA console will be installed to the same directory that you choose for the Harvester.

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

The Select a Location for the MySQL Data Directory screen opens after a moment. This screen shows the default installation path for the MySQL data directory.

c. (Optional) Click Choose to change the MySQL installation location.

We recommend that you use a drive that has at least 40 GB of available space for the database.

d. Click Next when the MySQL database path setting is correct.

The Select a Location for the MySQL Temp Directory screen opens, which shows the default installation path for the MySQL tmp directory.

e. (Optional) Click Choose to change the tmp directory location.

f. Click Next when the MySQL tmp directory path setting is correct.

MySQL51 is configured, then the Pre-Installation Summary screen opens.

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

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

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

<NFA_install_path>/Harvester_Install_MM_DD_YY_hh_mm_ss.log (where MM_DD_YY_hh_mm_ss reflects the timestamp)

14. Click Done in the Install Complete screen.

    The Harvester installation program closes.

Next: Repeat these steps to install a Harvester on another server or install the console (see page 49).

Install the DSA in a Three-Tier Distributed Deployment

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

Before You Begin: Verify that the installation server meets the following requirements:

- Server is upgrade-ready as described in Prepare the Windows Servers (see page 16).
- Java Runtime Engine (JRE) 1.6u41 is installed.
- CA Network Flow Analysis software is installed on the Harvester servers.

Follow these steps:

1. Start the installation: Double-click the NFDSASetup9.1.2.exe file in Windows Explorer.

   A check verifies that the installation server has a supported version of the Java Runtime Engine (JRE) installed. If the check fails, an error message opens (see page 63). You cannot launch the upgrade program until this problem is corrected.

   If the server passes the Java prerequisite check, the program starts and the language selection screen opens.

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

   The License Agreement screen opens.

3. Review and accept the license agreement:

   a. Read the license agreement and scroll down.

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

   c. Click Next.

      Prerequisite tests are run to identify problems on the server. If a a problem is found, an error message opens. A critical problem causes the program to exit. A Pre-requisite Check Warning message or other warning message opens for non-critical problems, which gives you the option to make corrections now or after the installation or upgrade is complete.

4. Review the test results in the Pre-requisite Check Warning message, if it opens:
   a. Correct problems now or wait until the program finishes. For more information about the warnings, see the Troubleshooting section.
   b. Click OK to close the message.

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

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

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

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

      MySQL51 is configured, then the Pre-Installation Summary screen opens.
6. Review the pre-installation information, then click Install.

   The Installing DSA screen opens, which shows the progress. When the installation is complete, the Install Complete screen opens and reports any errors that occurred.
7. Click Done in the Install Complete screen.

   The installation program closes.

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

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

Next:

- To install an additional DSA on another server, repeat these steps.
- To upgrade the console server, go to the next topic.

Install the NFA Console

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

Before You Begin: Verify that the installation server meets the following requirements:

- Server is upgrade-ready as described in Prepare the Windows Servers (see page 16).
- Java Runtime Engine (JRE) 1.6u41 is installed.
- The CA Network Flow Analysis software is installed on the Harvester servers.
- If you have a three-tier architecture deployment, the CA Network Flow Analysis software is installed on the DSA servers.

Follow these steps:

1. Log in to the NFA console server as a user who has administrator privileges for the system and for CA Network Flow Analysis.
2. Start the installation: Double-click the RAConsoleSetup9.1.2.exe file in Windows Explorer on the NFA console server.

   A check verifies that the installation server has a supported version of the Java Runtime Engine (JRE) installed. If the check fails, an error message opens (see page 63). You cannot launch the upgrade program until this problem is corrected.

   If the server passes the Java prerequisite check, the program starts and the language selection screen opens.
3. Verify that the appropriate language is selected, then click OK.

   The Welcome screen opens.

4. Click Next in the Welcome screen.

   The License Agreement screen opens.

5. Review and accept the license agreements:

   a. Read the NFA console license agreement and scroll down.

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

6. Click Next.

   Prerequisite tests are run on the installation server, as described in Troubleshooting. If the server fails any noncritical tests, the Pre-requisite Check Warning message opens. If the server fails the test to verify the presence of the Service Control command, a separate error message opens.

7. If the '"sc.exe" is not installed' error message opens, the upgrade program closes when you close the error message. Restore the missing sc.exe file and start the upgrade again. For more information see the Troubleshooting topic (see page 64).

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

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

9. Click OK to close the message.

   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 Pre-Installation Summary screen opens after a moment.

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

    The Installing NFA screen opens. Progress is shown in the status bar and messages. When the NFA console upgrade is complete, the Install Complete screen opens and reports any errors.

12. (Optional) If errors occurred during the upgrade, see the installation log: <NFA_install_path>/NFA_Install_<timestamp>.log.
13. Exit from the installation program:
    a. Select one of the restart options:
       - Yes, restart my system: Restart the system as soon as you click Done.
       - No, I will restart my system myself: Defer the restart to be performed manually.
    b. Click Done.

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

Next: Complete the post-upgrade tasks (see page 53).

Chapter 6: Post-Installation Tasks

This section contains the following topics:

Install CA Performance Center

Install CA Performance Center 2.2.00 on a separate server, as described in the *CA Performance Center Installation Guide.*

Modify the Firewall

Verify that the required ports are open, as described in the following topics about preparing the servers for the upgrade.

Windows servers:

- Ports to Open for a Standalone System (see page 17)
- Ports to Open for a Two-Tier Distributed Deployment (see page 18)
- Ports to Open for a Three-Tier Distributed Deployment (see page 19)

Linux Harvester servers:

- Disable the iptables Firewall for Linux Servers (see page 34)

Synchronize System Time (Windows)

Synchronize the system time among all servers that have CA Network Flow Analysis components installed. Perform the following steps on each server, unless the system time is synchronized automatically.

Follow these steps:

1. Right-click the date or time on the right edge of the taskbar and select 'Adjust date/time.'

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

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

   The system time is synchronized with the selected server.
7. Click OK in the Internet Time Settings dialog.
8. 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 (Windows)

Add the console server to the list of trusted internet sites. The process varies by browser. The following instructions are for Microsoft Internet Explorer.

Follow these steps:

1. Launch Internet Explorer on the console computer.
2. Click Tools, Options.
3. Click the Trusted Sites icon on the Security tab.
4. Click Sites.
5. Enter **http://localhost** in the "Add this Web site to the zone" field.
6. Click Add.

Modify the Router Access Control Lists (Windows)

If the NFA console and Harvesters are installed on separate servers, the router access control lists (ACLs) must be configured to permit the Harvesters to perform SNMP polling.

Note: If loopback interfaces source the flow packets, verify that CA Network Flow Analysis can access the IP addresses of those interfaces.

Chapter 7: Uninstalling CA Network Flow Analysis

The CA Network Flow Analysis 9.1.2 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, we recommend that you contact CA Support rather than continue to install and uninstall the software.

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.

Complete the following checks:

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

Database	Location	Standalone	Harvesters	NFA Console
reporter	<NFA_Install_Path>\MySql51\data\ reporter	Yes		Yes
harvester	<NFA_Install_Path>\MySql51\data\ harvester	Yes	Yes	
poller	<NFA_Install_Path>\MySql51\data\ poller	Yes	Yes	
ReaperArchive15	<NFA_Install_Path>\Netflow\datafiles\ ReaperArchive15	Yes	Yes	
data_retention	<NFA_Install_Path>\MySql51\data\ data_retention	Yes	Yes	
ReaperArchive	<NFA_Install_Path>\Netflow\datafiles\ ReaperArchive	Yes	Yes	

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

Service	Standalone	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 MySql51	Yes	Yes	Yes	Yes
NetQoS NQMySql51 (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 CA Network Flow Analysis

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.

Follow these steps:

1. Log in to the server as an administrator.
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 <NFA_install_path>\Uninstall:
   - Standalone 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 uninstall 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

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

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

   Once the program finishes, the Uninstall Complete screen opens.
6. Click Done to close the 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.

Notes:

- The uninstallation log is at the root level of the original installation path. For example, the Harvester uninstallation log is at: <NFA_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 8: Troubleshooting

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

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

The following prerequisite tests are run:

Test	Description	Warning or Upgrade/Install Failure	Server
Browser	Checks the Registry for a browser. Verify that a supported browser version is installed (see page 17).	Warning	Standalone Distributed: NFA console
DEP	Verifies that the winmgt service is running. Configure DEP as described in this guide (see page 27).	Warning	Standalone Distributed: NFA console, Harvester (Windows)
FIPS Algorithm Policy	Verifies that the FIPS Algorithm policy is not enabled (see page 62).	Verify automatic fix or Failure	Standalone Distributed: NFA console
Flash Player	Checks the Registry for any version of Flash Player (see page 21).	Warning	Standalone Distributed: NFA console
IIS Installed	Verifies that the wcsvc service is running. Install and configure IIS as described in this guide (see page 21).	Warning	Standalone Distributed: NFA console
IIS Version	Checks the Registry for IIS version 7.0.	Warning	Standalone Distributed: NFA console
Java Version	Verifies that the supported version of the Java Runtime Engine (see page 63) is installed.	Failure	All servers
.NET 3.5 Version	Checks for .NET version 3.5 SP1. If .NET version 3.5 is found, turns on SP1.	Failure	Standalone Distributed: NFA console
.NET 4.0 Version	Verifies that .NET version 4.0 is not installed.	Failure	Standalone Distributed: NFA console

Test	Description	Warning or Upgrade/Install Failure	Server
Service Control comnd	Verifies that the the Windows System32 directory contains the sc.exe file (see page 64).	Failure	Standalone Distributed: NFA console, Harvester (Windows)
SNMP	Verifies that the snmp service is running and the process ID is present. Configure SNMP on Windows servers (see page 23) and Linux servers (see page 32).	Warning	Standalone Distributed: NFA console, all Harvesters
Windows 2003 Detected	Verifies that the server is running Windows Server 2008, not Windows Server 2003.	Failure	Standalone Distributed: NFA console, Harvester (Windows), DSA

This section contains the following topics:

FIPS Algorithm Policy Is Enabled

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 algortihm policy is disabled and does not restrict database connections.

Java Is Not Installed

If you attempt to launch the installation or upgrade program on a server that does not have a supported version of the Java Runtime Engine (JRE), an error message opens. You must install a supported version of the JRE, before you can proceed.

The error message reads:

> "No Java virtual machine could be found from your PATH environment variable. You must install a VM prior to running this program."

Follow these steps:

1. (Optional) Determine which JRE version the server is running:
   a. Enter the following command at a command prompt or in a terminal window:
   `java -version`
   The command returns the JRE version that is installed.
2. Download the appropriate JRE installation file to the installation server.
3. (Windows) Run the JRE .exe installation file:
   a. Open the Run window: Select Start, Run.
   b. Specify the path and file name for the installation program in either of the following ways:
      - Click Browse and use the Browse window to locate and select the file.
      - Enter the path and the file name in the Open field.
      - Click OK.
   c. Follow the prompts to complete installation.
4. (Linux) Run the JRE .bin installation file:
   a. Navigate to the JRE .bin file location in a terminal window.
   b. Enter the following command:
   `./jre`
   The JRE installation program starts.
   c. Follow the prompts to complete installation.
5. (Optional) Repeat Step 1 to verify that the JRE version is updated correctly.

SC.exe Is Not Installed

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 upgrade. In any case, CA Network Flow Analysis will not run properly until you configure SNMP (see page 32) and make sure that the snmpd and snmptrapd daemons are running.

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

Follow these steps:

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

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

2. (Optional) Check the status in the Service Configuration window:
   a. Open the Service Configuration window: Select System, Administration, Server Settings, Services.

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

   b. Locate snmpd and snmptrapd in the service list.
   c. Check the status of these services:
      - Select snmpd and review the status message that is displayed.
      - Select snmptrapd and review the status message that is displayed.
   d. Close the Service Configuration window.

Windows 2003 System Detected

When I click Next in the License Agreement screen in the installation or upgrade program, an error message opens, which has the title:

"Windows 2003 system detected"

The error message opens because a system check discovered that the installation server is running Windows Server 2003. For the 9.1.2 release, installations and upgrades are supported only for servers that run Windows Server 2008 R2 operating system. The installation or upgrade program exits when you click OK to close the error message. Before you upgrade the CA Network Flow Analysis software, upgrade your operating system.

Index