Installation Guide

CA Application Delivery Analysis

10.2

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.

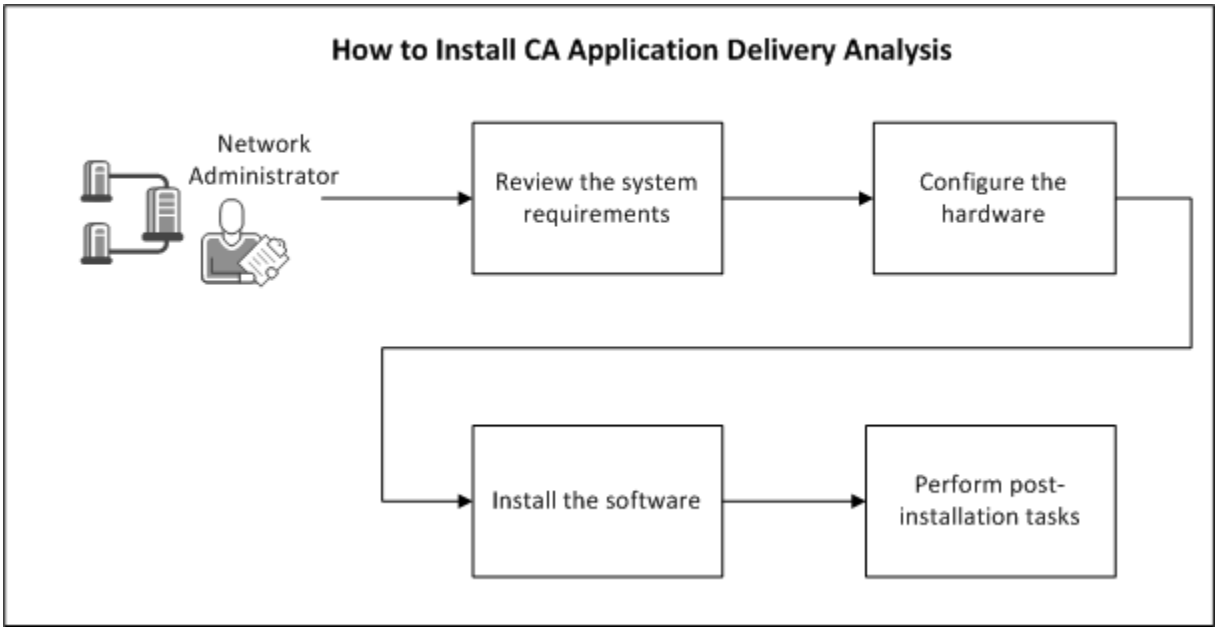
Contents

Appendix A: Deployment Best Practices 33

Chapter 1: Introduction

CA Application Delivery Analysis (CA ADA) provides end-to-end performance monitoring through report pages and views. CA ADA gathers troubleshooting information and helps you determine the source of an application, network, or server performance problem.

The following diagram describes the process of installing CA ADA.



More information:

System Requirements (see page 9)
Post-Installation Configuration (see page 29)
Installing the Software (see page 25)
Configuring the Hardware (see page 21)

Chapter 2: System Requirements

Configure and secure the operating system as described in this section.

A server administrator should install CA Application Delivery Analysis.

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:

Supported Operating Systems

CA Application Delivery Analysis components require Microsoft Windows 2008 R2, Standard Edition, with:

- The most recent service pack and important updates.
- Microsoft .NET Framework 3.5.1.
- Java Runtime Environment (JRE).

  Note: The CA ADA setup program installs the JRE. We do not recommend installing the JRE separately.
- English, Chinese (Simplified), or Japanese language.

  Note: The Regional Settings must use a period (.) to indicate a decimal value. For example, the Portuguese (Brazil) regional setting uses a comma symbol by default to indicate a decimal value. Customize the regional settings to change the decimal symbol to a period.
- Minimum display resolution of 1024x768 (XGA).
- ASP.NET 2.0, including COM+ network access, IIS, and ASP.
- Operating system configured as described in this document.
- Enable the SNMP and SMTP services.
- (Recommended) Enable Remote Desktop Connection to allow remote access by the administrator.
- An IPv4 host address. Installation is not supported at this time on servers with IPv6 addresses.

Supported Web Browsers

Access to the management console is supported for the following browsers:

- Microsoft Internet Explorer 7 or 8

  When accessing the management console through Internet Explorer 8, the page formatting appears incorrect at the top of the page. To avoid this issue, press F12 in Internet Explorer and then set the Browser Mode to IE8 and the Document Mode to Quirks.
- Mozilla Firefox 11.x

Other browsers or versions may work with CA Application Delivery Analysis but have not been tested.

Hardware Requirements

Install the management console and standard monitor on separate servers. Configure the management console with one management NIC to receive response time metrics from a monitoring device, such as the CA Standard Monitor.

Management Console

CA has tested the management console on servers with the following specifications. The management console is supported on servers from any vendor, if the servers conform to these specifications, at a minimum.

- Two Intel® E5520 Xeon quad-core 2.66 GHz, 1333 MHz FSB processors
- 24 GB of RAM
- Six 146 GB SAS hard drives in RAID 5 configuration
- RAID controller with a battery-backed cache for up to eight SAS ports
- 10/100/1000 Mbps Ethernet RJ-45 port
- Intel 82576 Gigabit Ethernet Controller

Standard Monitor

CA has tested the CA Standard Monitor on servers with the following specifications. The Standard Monitor is supported on servers from any vendor, if the servers conform to these specifications, at a minimum.

- Intel® E5520 Xeon quad-core 2.66 GHz, 1333 MHz FSB processor
- 3 GB of RAM
- Three 146 GB SAS hard drives in RAID 5 configuration
- RAID controller with a battery-backed cache for up to eight SAS ports
- Two 10/100/1000 Mbps Ethernet RJ-45 ports

  (Optional) To monitor TCP traffic on 2 monitor NICs, provision an additional Ethernet RJ-45 port.
- Intel 82576 Gigabit Ethernet Controller

Virtual Machine Requirements

CA Application Delivery Analysis supports the management console and the CA Standard Monitor on VMware ESX® and VMware ESXi® 3.5, 4.0, or 5.0.

To achieve equal performance in an environment that stresses a physical server, more memory is required in VMware than on a physical server. Physical servers outperform virtual machines in the area of disk I/O. CA Application Delivery Analysis servers task the disk I/O heavily. Expect less-than-equal performance on a VMware machine.

A CA Standard Monitor that is deployed on VMware can receive data from a NI GigaStor Connector and WAN optimization devices such as Cisco WAE.

Important: Install VMware Tools on the virtual machines that host CA Application Delivery Analysis. Remove the CD/DVD drive from the virtual machine configuration.

Standard Monitor

CA has tested the Standard Monitor on a virtual machine with the following specifications. We recommend that your virtual machine conform to these specifications, at a minimum.

- One virtual processor
- 4 GB RAM
- 300 GB available disk space
- Two virtual network adapters (1 Gbit minimum). An uplink port (a physical port leaving the ESX Host) is required on one of the virtual network adapters.

  (Optional) To monitor TCP traffic on 2 monitor NICs, provision an additional Ethernet RJ-45 port.

Management Console

CA has tested the management console on a virtual machine with the following specifications. We recommend that your virtual machine conform to these specifications, at a minimum.

- One virtual processor
- 30 GB RAM
- 700 GB available disk space
- One virtual network adapter (1 Gbit minimum). An uplink port (physical port leaving the ESX Host) is required on the network adapter.

Firewall Requirements

The following list summarizes the firewall ports that must be open to allow communication among CA ADA components.

From management console

- To a CA Standard or Virtual Monitor on TCP 1000, 1001, 3308, and 8080
- To CA ADA Multi-Port Monitor on TCP 80 and 8080

From Standard or Virtual Monitor

- To a management console on TCP 3308

From CA ADA Multi-Port Monitor

- To a management console on TCP 80, TCP 3308, and TCP 8381.

  CA Single Sign-on settings on CA Application Delivery Analysis use a different port, TCP 8381, to authenticate the user. When you sign in to the CA Multi-Port Monitor, it will redirect to the CA Single Sign-on application running on TCP 8381 of the CA ADA Manager. Verify that your firewall configuration allows this.

  After you install, if necessary, you can update the CA Single Sign-on settings on CA ADA to use a different TCP port. For more information, contact CA Technical Support.

From Metric Engine on a Cisco NAM

- To a management console on TCP 9996

From FlowAgent on a Cisco WAE

- To a CA Standard or Multi-Port Monitor on TCP 7878
- To a management console on TCP 7878

From NI GigaStor Connector

- To a CA Standard or Multi-Port Monitor on UDP 9995
- To a management console on TCP 1001

Adobe Applications

Adobe Acrobat Reader and Flash Player are required to view reports, charts, and the product documentation.

- Install the latest version of Acrobat Reader from http://get.adobe.com/reader/.
- Install the latest version of Flash Player from http://get.adobe.com/flashplayer/.

Install Server Roles and Role Services

Install the required Windows server roles and role services.

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. Select Roles in the Console tree on the left.
4. Click Add Roles.

   The Add Role Wizard opens.
5. Click Next.
6. Select Application Server from the Select Server Roles list.

   The Application Server role includes .NET Framework 3.5.1.
7. Click Next.
8. Click Next.

   The Select Role Services page for Application Server is displayed.
9. Add the Web Server (IIS) Support role service:
   a. Select the Web Server (IIS) Support check box.

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

      The Web Server (IIS) Support option is highlighted on the Select Role Services page.
10. Add the COM+ role service:
    a. Select the COM+ Network Access check box.
    b. Click Next.
11. Enable IIS 6 Management Compatibility:
    a. Click Next again.

       The Select Role Services page for Web Server (IIS) is displayed.
    b. Select the IIS 6 Management Compatibility check box in the Management Tools section of the list, and click Next.

       The Confirm Installation Selections page summarizes the configuration of the Application Server role, the Web Server (IIS) roles, and .NET Framework 3.5.1 features.

12. Install the IIS and COM+ role services and options you selected:
    a. Click Install.

       The Progress page is shown. When the installation is complete, the Results page opens.

    b. (Optional) Click Print, e-mail, or save the installation report, review the information, and 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 Add Role Wizard closes.

13. 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, and 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.

14. Exit from the Server Manager window.

Install the SNMP Service and the SMTP Server

Install the SNMP service and the SMTP server.

The Simple Network Management Protocol (SNMP) is required by the CA ADA 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 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, and take up more space.

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 CA ADA. Removing unneeded services helps secure your servers, but is not required. If the following services are needed for another reason, do not disable them.

Follow these steps:

1. Log in as a user who has administrator privileges for the server.
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 when 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

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.

Follow these steps:

1. Log in as a user who has administrator privileges for the server.
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 empty TrapConfiguration registry key is created in the following location: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters.

Chapter 3: Configuring the Hardware

When configuring CA ADA on a physical server, you need the following types of cables:

Power cables

Connect the server to two power supplies, preferably two separate UPS devices. The second cable is required for a backup power source.

Management NIC cable

Copper 1-Gb cable

When plugged into a switch, the management NIC provides network access to the CA ADA server.

The management NIC also receives performance data from Cisco WAE and NAM devices, and from NI GigaStor.

Monitor NIC cable

Copper 1-Gb cable

Collects network traffic from a mirrored port on a switch.

This section contains the following topics:

Configure the Management Console Server

Use this procedure to configure a physical server that hosts the management console.

Follow these steps:

1. Connect one end of the power cables to the power outlets on the server.
2. Connect the other end of the power cables to two separate power supplies.
3. Connect one end of the management cable to a NIC on the server.
4. Connect the other end of the management cable to a switch that enables network access to the management console.
5. Turn on the server.
6. Configure network connections (see page 22) for the NICs.
7. Assign IP addresses (see page 23) to the NICs.

Configure the Standard Monitor Server

Use this procedure to configure a physical server that hosts the standard monitor.

Follow these steps:

1. Connect one end of the power cables to the power outlets on the server.
2. Connect the other end of the power cables to two separate power supplies.
3. Connect one end of the monitor and management cables to NICs on the server.
4. Connect the other end of the monitor cable to a mirrored switch port.
5. Connect the other end of the management cable to the management console server.
6. Turn on the server.
7. Configure network connections (see page 22) for the NICs.
8. Assign IP addresses (see page 23) to the NICs.

Configure Network Connections for NICs

Configure the network interface cards (NICs) on each server where you plan to install the management console or CA Standard Monitor.

- For a CA Standard Monitor, set up network connections for the management and monitor NICs. Note that up to 2 monitor NICs can be configured to receive traffic.
- For a management console, set the priority of the management NIC.

Follow these steps:

1. From the Control Panel, click Network Connections.

   The Network Connections window opens.

2. Review the names of the LAN or High-Speed Internet Connections. If necessary, change the default names to correspond to the interfaces, as shown in the following list:

   Copper Ethernet adapter

   Default name: Local Area Connection 2

   New name to assign: Management

   Copper Ethernet adapter

   Default name: Local Area Connection 3

   New name to assign: Monitor

Gigabit Fiber port

Default name: Local Area Connection

New name to assign: Fiber Monitor

Tip: You can identify devices by disconnecting the cable from the back of the device and noting which interface status changes to "disconnected" in the Network Connections dialog.

3. Disable unused monitor NICs on the management console or CA Standard Monitor.
   a. Right-click the NIC.
   b. Select Disable.
4. Click Advanced, Advanced Settings, Adapters and Bindings.
5. Use the up arrow to move the management NIC to the first position in the Connections pane. This action sets the priority and lets CA ADA operate correctly.
6. Clear the following Internet Protocol (TCP/IP) check boxes for all NICs:
   - File and Printer Sharing for Microsoft Networks
   - Client for Microsoft Networks
7. Click OK.

Assign an IP Address to the Management NIC

Assign a static IP address, subnet mask, and default gateway to the management NIC on a management console or a CA Standard Monitor.

Note: The Management NIC is the only NIC that transmits data to the network. The IP addresses assigned to other NICs, such as a Monitor NIC, do not need to be valid for the network to which they are connected, nor do they require a default gateway assignment.

Follow these steps:

1. Open the Control Panel and select Network Connections.
2. Right-click the management network connection and select Properties.
3. Click Properties on the General tab.
4. Clear the check boxes for all network components *except* Internet Protocol Version 4 (TCP/IPv4).
5. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties.
6. Select Use the following IP address, and enter an IP address, subnet mask, and default gateway.

7. Click OK.
8. Repeat steps 5 through 7 for the monitor NICs, using the following suggested values:

   Monitor NIC

   IP address: 1.1.0.2

   Subnet mask: 255.0.0.0

   Fiber Monitor NIC

   IP address: 1.1.0.1

   Subnet mask: 255.0.0.0

Chapter 4: Installing the Software

This section contains the following topics:

Prerequisites

Perform the following tasks before installing the CA ADA software:

- Download the latest CA ADA setup file, ADASetup10.2.xxx.exe, from CA Support.
- Verify the currently installed software version. If necessary, upgrade to the latest version. To verify the software version, log in to the CA ADA console and click the About link. For information about upgrading CA ADA, see the *Upgrade Guide*.
- Do not install CA ADA on the same computer as NetQoS Performance Center 6.1 or above. The CA Single Sign-on application that is provided with CA ADA is not compatible with the CA Single Sign-on that is provided with the CA NetQoS Performance Center. If necessary, install CA ADA on a different computer.
- Extract or copy the setup file to the servers or virtual machines where you want to install the software.
- Verify that the setup file has permission to run:
  a. Right-click the setup file, and select Properties.
  b. Click Unblock.
  c. Click OK.

Install the Management Console

Use this procedure to install the management console on a physical server or virtual machine. A CA Standard Monitor is also installed, but is not automatically added as a monitoring device. After installation, manually add the monitoring device (see page 29) as a source of response time data.

The setup program logs its status in *drive*:\CA\ADA_Uninstaller\Logs.

Follow these steps:

1. Log in to the server as an administrator.
2. Double-click the ADASetup10.1.xxx.exe file.

   The Welcome dialog opens.
3. Click Next.

   The License Agreement dialog opens.
4. Read and accept the license agreement, and click Next.

   The Choose Install Set dialog opens.
5. Select Distributed Manager, and click Next.

   The Information dialog reminds you to register CA ADA as a data source for CA SOLVE:Access or CA Performance Center.
6. Click Continue.

   The Choose Install Folder dialog opens.
7. (*Optional*) Click Choose to select a different location. The default location is C:\CA.
8. Click Next.

   The Pre-Installation Summary dialog summarizes the installation parameters.
9. Click Install.

   The installation process begins. Messages indicate the progress of the installation. When installation is complete, the Install Complete dialog opens.
10. Select Yes, restart my system.
11. Click Done.

    After the server restarts, you can add a monitoring device, such as a CA Standard Monitor, to the management console.

More information:

Post-Installation Configuration (see page 29)

Install the Standard Monitor

Use this procedure to install the monitoring device.

The setup program logs its status in *drive*:\CA\ADA_Uninstaller\Logs.

Follow these steps:

1. Log in to the server as an administrator.
2. Double-click the ADASetup10.1.xxx.exe file.

   The Welcome dialog opens.
3. Click Next.

   The License Agreement dialog opens.
4. Read and accept the license agreement, and click Next.

   The Choose Install Set dialog opens.
5. Select Single-Port Monitor, and click Next.

   The Information dialog reminds you to register CA ADA as a data source for CA SOLVE:Access or CA Performance Center.
6. Click Continue.

   The Choose Install Folder dialog opens.
7. (*Optional*) Click Choose to select a different location. The default location is C:\CA.
8. Click Next.

   The Pre-Installation Summary dialog summarizes the installation parameters.
9. Click Install.

   The installation process begins. Messages indicate the progress of the installation. When installation is complete, the Install Complete dialog opens.
10. Select Yes, restart my system.
11. Click Done.

    After the server restarts, your system is ready for post-installation configuration (see page 29).

Install a Virtual Monitor

Use this procedure to install the CA Virtual Monitor.

The setup program logs its status in *drive*:\CA\ADA_Uninstaller\Logs.

Follow these steps:

1. Log in to the virtual machine as an administrator.
2. Double-click the ADASetup10.1.xxx.exe file.

   The Welcome dialog opens.
3. Click Next.

   The License Agreement dialog opens.
4. Read and accept the license agreement, and click Next.

   The Choose Install Set dialog opens.
5. Select Virtual Monitor, and click Next.

   The Information dialog reminds you to register CA ADA as a data source for CA SOLVE:Access or CA Performance Center.
6. Click Continue.

   The Choose Install Folder dialog opens.
7. (*Optional*) Click Choose to select a different location. The default location is D:\CA.
8. Click Next.

   The Pre-Installation Summary dialog summarizes the installation parameters.
9. Click Install.

   The installation process begins. Messages indicate the progress of the installation. When installation is complete, the Install Complete dialog opens.
10. Select Yes, restart my system.
11. Click Done.

    After the virtual machine restarts, your system is ready for post-installation configuration (see page 29).

Chapter 5: Post-Installation Configuration

This section contains the following topics:

Install CA Application Delivery Analysis Updates

Install any updates that are available from CA Support.

Exclude Directories from Anti-virus Scans

If you must install antivirus software, exclude the following directories from virus scans:

- C:\Windows\Temp
- The installation directory for CA ADA and its subdirectories. By default, CA ADA is installed to C:\CA.

Synchronize the System Time and Time Zone

Follow these steps:

1. Log in as a user with administrator privileges to the server.
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 NTP time server to synchronize with. 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 a CA Standard Monitor in a different time zone, set each monitoring device to its local time zone. Use an NTP server to help ensure that times are accurate. Times are converted to Greenwich Mean Time (GMT).

Perform Configuration Tasks from the Management Console

Use the management console to:

- Add a CA Standard Monitor as a monitoring device.
- Define the server subnets and client networks you want to monitor.

Note: For more information, see the CA Application Delivery Analysis online help or the *CA Application Delivery Analysis Administrator Guide*.

Follow these steps:

1. Click the Administration page.
2. Add the monitoring device:
   a. Click Data Monitoring, Monitoring Devices in the Show Me menu.
   b. Click Add ADA Monitor under the Show Me menu.

      Standard Monitor Properties opens.
   c. Complete the fields in Standard Monitor Properties and click OK.

      Provide the IP addresses for the management and monitor NICs you configured in Configure Network Interface Cards (see page 22). For more information, click Help.
3. Define the server subnets you want:
   a. Click Data Monitoring, Servers in the Show Me menu.
   b. Scroll to the Server Subnet List and click Add Server Subnet.
   c. Add Server Subnets opens.
   d. Complete the fields in Server Subnets and click OK.

      For information about setting server subnet properties, click Help.
4. Define the client networks you want:
   a. Click Data Monitoring, Networks in the Show Me menu.
   b. Click Add Network under the Show Me menu.
   c. Network Properties opens.
   d. Complete the fields in the Network Properties and click OK.
   e. For information about network properties, click Help.
5. Click the link to synchronize the monitoring device and begin collecting data based on the current server subnet and client network definitions.

Appendix A: Deployment Best Practices

The topics in this section provide advice about server configuration and placement to help you monitor all relevant traffic.

How to Determine Server Placement

The CA ADA server requires connectivity to a SPAN or mirror port on each network switch that handles the traffic you want to monitor. Connectivity typically occurs at the access layer. Install a CA ADA management console in close proximity to the monitoring devices it connects to.

The server must be able to see as much of the relevant network traffic as possible. Consider the following questions:

- Which applications do you want to monitor?
- Which servers host these applications?
- Which switches are these servers connected to?
- Which subnets do users access the monitored applications from?

How to Monitor Unidirectional Streams

Unidirectional streams can be seen with an inline fiber tap. Some taps are designed with one inlet and two outlet network cards, one for transmit and one for receive. In this case, a multi-NIC monitor, such as CA ADA Multi-Port Monitor, is required for CA ADA to accurately account for the traffic.

In an asymmetric routing environment, one core switch routes data into the data center. A different core switch routes traffic that exits the data center. Two port mirrors to the same monitor are required to capture the transmit and receive traffic for the server farm.

The CA Standard Monitor cannot monitor unidirectional or asymmetric traffic.

How to Mirror Switch Ports

On a network switch, the *port mirroring* function sends copies of network packets from one port to another switch or port for analysis.

Port mirroring is a safe, effective way to mirror traffic to CA ADA monitoring devices.

Some switches do not provide the diverse range of TCP packet mirroring capabilities that these scenarios require.

Where traffic cannot be mirrored optimally, use alternatives such as fiber taps.

Note: The port mirroring function on Cisco switches is named Switched Port Analyzer (SPAN).

Mirror the switch ports, where traffic travels to and from the monitored servers, to the monitor NIC on the CA ADA server or to the ports where CA ADA monitoring devices are connected. When mirror ports are configured correctly, CA ADA monitors the flow of application traffic between clients and servers without the use of desktop or server agents.

For more information, see the *Data Acquisition Best Practices Guide*.