Upgrade Guide

CA Application Delivery Analysis

Version 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

Chapter 1: Upgrading the Product

The upgrade process allows you to upgrade a:

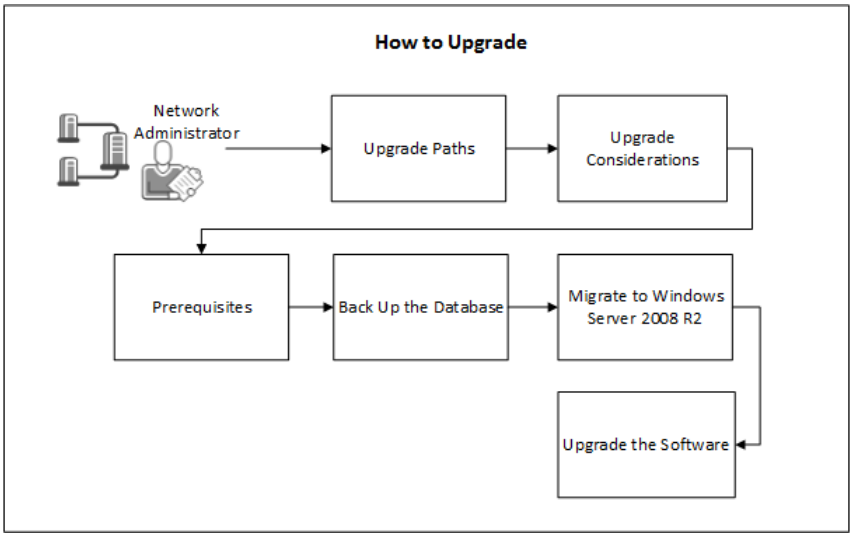
Standalone deployment

The management console and the CA Standard Monitor are installed on *the same* server.

Distributed deployment

The management console and the CA Standard Monitor are installed on *different* servers.

The following diagram describes the upgrade process.



The following topics describe the upgrade process:

1. Upgrade Paths (see page 8)
2. Upgrade Considerations (see page 9)
3. Prerequisites (see page 10)
4. Back up the Database
5. Migrate to Windows Server 2008 R2 (see page 13)
6. Upgrade the Software (see page 16)

Upgrade Paths

Upgrade CA Application Delivery Analysis from version 9.2 or above to version 10.2. If necessary, upgrade to version 9.2, and then upgrade to version 10.2.

Important! CA ADA version 10.2 is **not** compatible with CA Multi-Port Monitor version 9.2 or below. If you upgrade the CA ADA Manager to version 10.2, you must upgrade a version 9.2 Multi-Port Monitor to version 10.0 or later to resume data collection.

If you are running:

Windows Server 2008 R2 Standard

Upgrade CA Application Delivery Analysis to the current version.

Windows Server 2003

We recommend that you migrate CA ADA from Windows Server 2003 to Windows Server 2008 R2 Standard.

If CA Application Delivery Analysis is a registered data source with CA NetQoS Performance Center, and both products are installed on the same computer, **do not upgrade**. The CA Single Sign-On application that is provided with CA Application Delivery Analysis is not compatible with the CA Single Sign-On that is provided with the CA NetQoS Performance Center. Instead, migrate CA Application Delivery Analysis to Windows Server 2008.

This release of CA ADA includes an upgrade of the MySQL database from version 5.1 to 5.6. CA NetQoS Performance Center (CA NPC) requires MySQL version 5.1.

If you have CA NPC installed on the same server as CA ADA, you will receive a warning message during the upgrade of CA ADA, and you will not be allowed to continue.

To avoid this problem, ensure that CA NPC is installed on a separate server from CA ADA before you begin the upgrade of CA ADA. See the *Prerequisites* section later in this guide for information on uninstalling CA NPC.

Upgrade Considerations

CA Application Delivery Analysis 10.2 is a data source for:

- CA NetQoS Performance Center 6.2
- CA Performance Center 2.3

Before you upgrade, consider the following:

- Review the release notes for important information about what this release provides, including known issues with the upgrade.
- When upgrading a Standalone deployment, the upgrade process converts the management console to a Distributed management console. After the upgrade, the management console continues to provide SPAN monitoring support on its Monitor port. CA no longer provides a Standalone management console.
- When upgrading from CA ADA 9.2 or 9.3, the Standard Monitor and the ADA Manager must both be upgraded to 10.2 to work properly. While the ADA Manager and a Standard Monitor are at different versions, the data collected by the monitoring device is not available for reporting.
- As part of the upgrade process, in addition to upgrading CA Application Delivery Analysis, plan to upgrade the following products, if installed, to the supported versions listed below:
  - CA Multi-Port Monitor version 10.0 or higher.
  - NI GigaStor with NI Observer version 17, and the updated CA GigaStor Connector provided with CA Application Delivery Analysis version 10.2.

Prerequisites

Before you upgrade the CA Application Delivery Analysis software, perform the following tasks.

- When upgrading the CA ADA Manager:
  - Verify that you have sufficient disk space available. The amount of available disk space on the C: and D: drive partitions must be greater than the size of the directory *installpath*\mysql51\data\super.
- Verify that the Application Server role, which includes Microsoft .NET Framework 3.5.1, is installed. The upgrade program now requires Microsoft .NET Framework 3.5.1 to be installed.
- Disable the following types of third-party software on all servers and virtual machines:
  - Antivirus
  - Anti-spyware
  - Server monitoring and maintenance tools such as SMS, SUS, or MoM
- Back up any customized configuration files. For example, if you edited the InspectorAgent.exe.config file to disable packet capture investigations on a CA Application Delivery Analysis Standard Monitor, you will need to restore this change after the upgrade.
- Restart all servers to verify that available operating system patches are applied.

- Obtain the setup program, ADASetup<version>.xxx.exe, from CA Technical Support and copy the program to the servers or virtual machines on which 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.
- If CA NPC is installed on the same server as CA ADA, migrate CA NPC to a different server before beginning the upgrade of CA ADA.

  To uninstall CA NPC and migrate it to another server, follow these steps:

  1. Stop the NetQoS Mysql51 service from Windows Services. This stops all of the NetQoS services.
  2. Backup the following directories:

     (Required) Database directories

     - <install_directory>\Mysql51\data\netqosportal\
     - <install_directory>\Mysql51\data\em

     (Optional) Customized Event Manager Rules

     - <install_directory>\EventManager\EventManagerWS

     (Optional) Customized NPC logos or themes

     - <install_directory>\Portal\Website\CSS

     (Optional) If SSL is configured for NPC:

     - <install_directory>\SingleSignOn\Configuration\NetQoSPerformanceCenter.xml
  3. Disable CA NPC by deleting the following registry keys:
     - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetQoS Device Manager Service
     - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetQoS EventManager Service
  4. Reboot the server and verify that the following services are removed from Windows Services:
     - NetQoS Device Manager Service
     - NetQoS Event Manager Service
  5. Install CA NPC and Event Manager on a new server, following the instructions in the *CA NPC Installation Guide*. Note that CA ADA version 10.2 requires CA NPC version 6.2. Install to the same drive and path, if possible. If you install to a different drive and/or directory, follow step 15 below after restoring the databases.

6. Stop the *NetQoS Mysql51* service on the new CA NPC server. Copy the directories and files from step 2 above back to their original locations, to restore the databases and configuration settings.
7. Start all NetQoS services on the CA NPC server and verify that they start correctly.
8. Launch the CA NPC web page and go to *Admin, Data Sources.* Find the Event Manager Data Source, select it, and click Edit.
9. Change the Host Name (IP address) to reflect the IP address of the new Data Source.
10. Launch the Single Sign-On Configuration tool from the desktop, and select the Performance Center tab.
11. Edit the Web Service Host and the Web Site Host to be the IP address of the new CA NPC server.
12. Note: If using CA NPC 6.1SP2 / SSO 6.1.4, the Web Service Host and Web Site Host parameters do not get exposed in the Single Sign-On Configuration Tool. On the CA NPC server run the following, replacing the x.x.x.x with the IP address of the new CA NPC server:
    - mysql -P3308 -D netqosportal -t -e "update performance_center_properties set propValue='x.x.x.x' where propName='NpcWebServiceHost' or propname='NpcWebSiteHost';"
13. You can verify that these values are changed to the new CA NPC IP address by running the following query.
    - mysql -P3308 -D netqosportal -t -e "select * from performance_center_properties where propname='NpcWebServiceHost' or propname='NpcWebSiteHost';"
14. From the CA NPC web UI, go to *Admin, Data Sources* and click *Resync All* on each of the Data Sources. This pushes the updated SSO settings down to all data sources.
15. If you have installed CA NPC to a different drive or path than where it was originally installed, run the following command, replacing *C:/NetQos/portal/tzinfo* with your installation path:
    - mysql -P3308 -D netqosportal –t –e “Update general set value=”C:/NetQos/portal/tzinfo” where attribute=’TimeZoneDirectory’;”
16. Recycle the *NetQoS Device Manager* Service and verify that all data sources are syncing properly on the CA NPC *Admin, Data Sources* page.

You can now safely upgrade the CA ADA console to version 10.2..

Migrate to Windows Server 2008 R2

We recommend that you migrate CA ADA components from Windows Server 2003 to Windows Server 2008 R2 Standard, including:

- CA Standard Monitor
- CA Virtual Systems Monitor
- CA ADA Manager

Migrate CA ADA monitoring devices before you migrate the CA ADA Manager. For information about installing CA ADA on Windows Server 2008 R2 Standard, see the *Installation Guide*.

Migrate CA ADA Monitoring Devices

Migrate a CA ADA monitoring device from Windows Server 2003 to Windows Server 2008 R2, including:

- CA Standard Monitor
- CA Virtual Systems Monitor

Do not perform an in-place upgrade of the Windows operating system. Instead, provision a new server with:

- Windows Server 2008 R2 Standard

  Important! Plan to migrate the existing IP addresses of the CA ADA monitoring device to the new server. The same management and monitor IP addresses are required.

- CA ADA 10.2

  Note: It is not required to preserve the CA ADA installation path.

For complete information about installing CA ADA, see the *Installation Guide*.

Follow these steps:

1. On the Windows 2003 server that hosts the CA ADA monitoring device:
   a. Make a note of the management and monitor IP addresses.
   b. Remove the CA ADA monitoring device from the network.
2. On the Windows 2008 server where you plan to host the CA ADA 10.2 monitoring device:
   a. Change the management and monitor IP addresses to match the Windows 2003 server.
   b. Install the CA ADA monitoring device.
   c. Reboot the server.
   d. Connect the mirrored switch port to the monitor NIC.
   e. In Services Manager, verify that the CA ADA Monitor service is running.
3. Log in to the CA ADA management console as an administrator and perform the following tasks:
   a. Click the Administration page.
   b. Click the gear icon, then click Synchronize Monitor Devices.
   c. Wait up to 10 minutes to verify that the management console receives data from its monitoring devices.

Migrate CA ADA Manager

Migrate the CA ADA Manager from Windows Server 2003 to Windows Server 2008 R2 Standard.

Do not perform an in-place upgrade of the Windows operating system. Instead, provision a new server with:

- Windows Server 2008 R2 Standard

  Important! Plan to migrate the existing IP address of the CA ADA Manager to the new server. The same management IP address is required.

- CA ADA 10.2

  Important! Plan to install CA ADA 10.2 to the same disk and folder location. The same CA ADA installation path is required. For example, if the CA ADA Manager is installed to C:\NetQoS on Windows Server 2003, it must be installed to C:\NetQoS on Windows Server 2008. Note that by default, CA ADA 10.2 is installed to C:\CA.

Follow these steps:

1. On the Windows 2003 server that hosts the CA ADA Manager:
   a. Make a note of the host IP address and the CA ADA installation path, including disk and folder.
   b. In Services Manager, stop the NetQoS MySql51 service.
   c. Copy the *drive*:\netqos\mysql51\data\super folder and its contents to a shared folder.
   d. Remove the CA ADA Manager from the network.
2. On the Windows 2008 server where you plan to host the CA ADA Manager 10.2:
   a. Change the host IP address to match the Windows 2003 server.
   b. Install the CA ADA Manager to the same disk and folder location where it was installed on the Windows 2003 server.
   c. Reboot the server.
   d. In Services Manager, stop the NetQoS MySQL51 service.
   e. In Windows Explorer, browse to the CA ADA installation directory and delete the \mysql51\data\super folder and its contents.
   f. Copy the \super folder and its contents from the shared folder to the \mysql51\data\ folder.
   g. When the copy completes, reboot the server.
   h. In Services Manager, verify that the CA ADA Monitor service is running. If necessary, set the service startup type to Automatic and start the service to resume data collection.

3. Log in to the CA ADA management console as an administrator and perform the following tasks:
   a. Click the Administration page.
   b. Click the gear icon, then click Synchronize Monitor Devices.
   c. Wait up to 10 minutes to verify that the management console receives data from its monitoring devices.

Upgrade the Software

Upgrade the software in a Standalone or Distributed deployment. In a:

Distributed deployment

Upgrade the CA Standard monitoring devices before you upgrade the management console.

Standalone deployment

The management console and standard monitor are automatically upgraded.

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

After the upgrade, restore any customized configuration files. For example, if you edited the InspectorAgent.exe.config file to disable packet capture investigations on a CA Standard Monitor, restore this change after the upgrade.

Follow these steps:

1. Log in to the server or virtual machine as an administrator.
2. In Services, stop the CA ADA Inspector service.
3. Double-click the ADASetup<version>.xxx.exe file.

   The Welcome dialog opens.
4. Click Next.

   The License Agreement window opens.
5. Read and accept the license agreement, then click Next.

   The Existing Product Version Detected window opens.
6. Click Next.

   The Upgrade Summary window opens and identifies the installation folder. You cannot change the installation folder.

7. Click Install.

   The upgrade process begins. Messages indicate the progress of the upgrade.

8. When upgrading the CA ADA Manager, the Database Health Check window opens. Click Yes to perform the check.

   When upgrade is complete, the Install Complete window opens.

9. Select "Yes, restart my system," then click Done.

   Upgrade is successful when new data appears in reports in the management console within 30 minutes.

10. (*Optional, but recommended*) Perform a Disk Defragmentation on the installation drive.

    a. Stop all CA- and NetQoS-related services.

    b. Run the Disk Defragmenter tool from the System Tools window.

More information:

Database Health Check Failed (see page 18)

Troubleshooting

See the following sections for more information.

CA Single Sign-On Port Change

If you upgraded from CA Application Delivery Analysis version 9.1, CA Single Sign-On settings on CA Application Delivery Analysis now 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 Application Delivery Analysis Manager. Verify that your firewall configuration allows this.

After you upgrade, if necessary you can update the CA Single Sign-On settings on CA Application Delivery Analysis to use a different TCP port. For more information, contact CA Technical Support.

Failed to Remove Portions of the Previous Installation

If the upgrade executable does not complete and the “Failed to remove portions of the previous installation” message appears, follow these instructions:

1. Cancel out of the upgrade script using the Cancel button.
2. After all instances of the upgrade script end, reboot the server that you were upgrading.
3. Launch the upgrade script again.

Database Health Check Failed

If the upgrade program does not complete and the “Database Health Check Failed” message appears, follow these instructions:

1. To help us quickly correct the problem, take a screen shot of the error and note the table causing the issue.
2. Log into CA Support Online and search for “MySQL database corruption.” Follow the instructions in the resulting solution article to repair the table noted in the screen shot.
3. Run the upgrade program again.