User Guide

NetIQ® AppManager® Diagnostic Console

Version 2.1

August 2007

Solutions from Attachmate

Legal Notice

Contents

About This Guide

NetIQ® AppManager Diagnostic Console® (or Diagnostic Console) is the industry's leading solution for diagnosing and analyzing performance, availability, and server health for a broad spectrum of operating environments, applications, and server hardware.

Diagnostic Console provides system administrators with a central, easy-to-use console for viewing critical server and application resources across the enterprise. From Diagnostic Console, system administrators can manage computer and application resources, check for potential problems, and gather performance data for real-time and historical reporting and analysis.

Intended Audience

This *User Guide* is intended for administrators and users who are responsible for installing, configuring, and using Diagnostic Console to investigate and diagnose problems occurring on networked Windows platforms.

This guide assumes that you are already familiar with your operating system and the applications and processes that you intend to monitor.

Conventions

This guide uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	• Window and menu items • Technical terms, when introduced
Italics	• Book and installation kit titles • Variable names and values • Emphasized words
`Fixed Font`	• File and folder names • Commands and code examples • Text you must type • Text (output) displayed in the command-line interface

Getting Help

Diagnostic Console provides task-based, reference, and context-sensitive online help.

To access task-based online help or search for help topics, click **Help > NetIQ Diagnostic Console Help**. To view context-sensitive help within dialog boxes, click the **Help** button or press **F1**.

The Diagnostic Console documentation set is included with the setup program in the Web-downloadable package. Additional resources are available on the NetIQ Extended Support Web site.

In addition to Diagnostic Console documentation, you may want to consult your operating system application documentation for reference and conceptual information. This background information can help you get the most out of your Diagnostic Console installation.

About Attachmate

Attachmate, owned by an investment group led by Francisco Partners, Golden Gate Capital and Thoma Cressey Equity Partners, enables IT organizations to extend mission critical services and assure they are managed, secure and compliant. Attachmate's leading solutions include host connectivity, systems and security management, and PC lifecycle management. Our goal is to empower IT organizations to deliver trusted applications, manage service levels, and ensure compliance by leveraging knowledge, automation and secured connectivity. For more information, visit www.attachmate.com.

NetIQ Solutions from Attachmate

Attachmate provides a wide selection of systems and security management solutions to help you manage and secure all your essential platforms, including Windows, Unix, Linux, and iSeries. These Knowledge-Based Service Assurance products and solutions include embedded knowledge and tools to implement industry best practices and to better ensure operational integrity, manage service levels and risk, and ensure policy compliance. Our modular, best-of-breed solutions for Performance and Availability Management, Security Management, Configuration and Vulnerability Management, and Operational Change Control integrate through an open, service-oriented architecture allowing for common reporting, analytics and dashboards. Attachmate offers the following systems and security management solutions:

- **Performance and Availability Management** These products offer rapid time-to-value solutions that enable you to align your IT operations with business priorities and optimize the delivery of your IT-based business services. This solution automates the complete IT service management lifecycle: assessment of requirements, definition of Service Level Agreements, management of day-to-day operations, and review of operational metrics.

- **Security Management** These easy-to-install-and-deploy products provide effective protection from and response to security-related threats. This solution provides powerful features, such as real-time security event monitoring, mapping of threat indicators, policy violation alerts, and expedited incident forensics and resolution. These products reduce the time required to identify and resolve security threats.
- **Configuration and Vulnerability Management** These products allow you to quickly and easily assess vulnerabilities, manage security risks, and assure policy compliance. This powerful solution measures and enforces compliance to configuration baselines based on your corporate policies, regulations, and evolving security threats. You can use the latest security knowledge, which is updated in real time, to resolve compliance and configuration issues.
- **Operational Change Control** These products enable IT organizations to control, manage, and audit operational changes to servers, Active Directory, and Group Policy with unprecedented levels of accountability. NetIQ's Operational Change Control (OCC) solutions enable enterprise customers to meet IT compliance and operational integrity needs in the most cost-effective manner, by delegating access control, managing changes according to policy, and alerting and reporting on change activities and entitlements.

Contacting NetIQ Solutions Support

Contact us with your questions and comments. We look forward to hearing from you.

Sales Email:	info@netiq.com
Telephone:	713.418.5555 (United States) +353 (0) 91 782 677 (Europe, Middle East, and Africa) For other locations, see our Support Web site
Support Web Site:	www.netiq.com/support

Chapter 1

Getting Started

The information in this chapter helps you understand and use NetIQ AppManager Diagnostic Console. Diagnostic Console provides a user interface with a rich collection of features for remotely investigating and diagnosing problems occurring on networked Windows platforms.

Many features of Diagnostic Console are available in the native Windows tools for diagnosing the computer on which they reside. Diagnostic Console integrates these tools into a single application. Furthermore, Diagnostic Console can run the tools on *any* individual Windows server on the network, not just the local system.

Diagnostic Console is designed to be a standalone application, but it can also be integrated with NetIQ AppManager.

The following topics are discussed in this section:

- "Getting Help" on page 31

System Requirements

Note the following requirements for hardware and software:

Requirement	Notes
Hardware	
Intel Pentium processor	866 MHz or higher
256 MB of RAM	512 MB of RAM is recommended
150 MB of disk space during installation	If the .NET Framework is not installed, you need 220 MB of disk space during installation
60 MB of disk space after installation	• 20 MB in the AppManager Diagnostic Console install directory • 40 MB in the system's "Downloaded installations" directory If Microsoft .NET Framework is not installed, you need 110 MB of disk space after installation. .NET Framework is installed during setup for all supported operating systems *except* Windows Vista. For more information, see "Installing .NET Framework" on page 6.
Screen resolution of 1024x768 or higher	
16 bits of color depth or higher	
Software (on the console computer)	
A Microsoft Windows operating system	• Windows 2000, SP2 or later • Windows XP Professional, including SP1 and SP2 • Windows Server 2003, including SP1 and SP2 for Standard and Enterprise 32-bit versions • Windows Vista (Business and Ultimate) 32-bit versions. You need to manually install Microsoft .NET Framework 1.1 if you are running Windows Vista. For more information, see "Installing .NET Framework" on page 6.
Microsoft Terminal Service Client, or Remote Desktop Client	
Microsoft Internet Explorer 5.01 or later	
MDAC 2.6 or later	

Requirement	Notes
Software (on the target computers)	
A Windows operating system	• Windows 2000 (SP2 or later) with the Microsoft XML Parser installed. For more information, see "Installing Microsoft XML Parser" on page 8. • Windows XP Professional, including SP1 and SP2 • All Windows Server 2003 variants, including SP1 and SP2 for Standard and Enterprise 32-bit and 64-bit systems running Windows 2003 Server. Windows Server 2003 Service Pack 1 for Itanium-based systems is recommended. • Windows Vista (Business and Ultimate). **Important**: Windows Vista 32-bit version is supported as a target computer if you are using AppManager 7.0.1 as a data source; Vista 32-bit and 64-bit versions are supported if you are using WMI as a data source. • Windows NT 4.0, SP6a, except Terminal Server Edition. Windows NT is not supported as a target if you use AppManager as a data source. Windows NT is partially supported if you are using WMI as a data source; some necessary counters are not present in NT and so some graphs will not display the expected data
NetIQ AppManager (only if using AppManager as a data source)	• Version 6.0, 6.02, or 7.0 and later • Proper user permissions set in AppManager Security Manager. For more information, see "Setting General Security Manager Permissions" on page 16. • Microsoft Exchange 2000 or 2003, if diagnosing Exchange resources. For more information, see "Setting Security Manager Permissions for Exchange" on page 17. • If diagnosing Windows resources, you must have run the Discovery_NT Knowledge Script and discovered Windows resources on the target computer. • If diagnosing Exchange resources, you must have run the Discovery_Exchange Knowledge Script and discovered Exchange resources on the target computer. • If diagnosing Active Directory resources, you must have run the Discovery_AD Knowledge Script and discovered Active Directory resources on the target computer
NetIQ Performance Endpoints	For use with the Network Connectivity plug-in. For more information, see "Using the Network Connectivity Plug-in" on page 77.

Installing Diagnostic Console

Diagnostic Console ships with two installation programs:

- `setup.exe`, which installs the Diagnostic Console user interface
- `AM60_DiagnosticConsole_setup.exe`, which installs the Diagnostic Console agent and the Diag category of Knowledge Scripts

Which program you use depends on whether you will use AppManager with Diagnostic Console and which version of AppManager you will use.

- For AppManager 6.0 environments, you need to install the user interface on a designated computer, and then install the Diagnostic Console agent on the computers you want to diagnose and on the repository computer to install the Diag category of Knowledge Scripts.
- For AppManager 6.0.2 and 7.0 environments, you need to install only the user interface on a designated computer. The AppManager installation process for these versions automatically installs the Diagnostic Console agent during agent installation and the Diag category of Knowledge Scripts during repository installation.
- If you will *not* be using AppManager to help diagnose problems, you need to install only the user interface on a designated computer.

To install AppManager Diagnostic Console:

1. For all environments, run `setup.exe` on the designated computer.

   During the process, `setup.exe` performs a prerequisite check. If necessary, click the **Prerequisite** links in the dialog box to perform any corrective actions. If you need to update or install MDAC 2.6 or later, and you are asked to reboot, click **Yes**. After the reboot, re-run `setup.exe`.

   Also during the process, select the version of AppManager that you want to use with Diagnostic Console. If you will not be using AppManager, select any version.

Note Only in certain situations are you asked to select a version of AppManager. For more information, see "Upgrading From a Previous Version or Release" on page 5.

2. For AppManager 6.0 environments, run `AM60_DiagnosticConsole_setup.exe` on *each* computer that you want to diagnose, including the Exchange and Active Directory computers that you want to diagnose.

3. For AppManager 6.0 environments, run `AM60_DiagnosticConsole_setup.exe` on the AppManager repository computer to install the Diag category of Knowledge Scripts.

Upgrading From a Previous Version or Release

Upgrading from a *previous release* of version 2.1 or a *previous version* (such as version 2.0) **is not** supported. Before installing this release of version 2.1, you must first uninstall any previous release or version. If you install the August 2007 release of version 2.1 over any previous release or version, the installation does not perform properly, even though it may appear to do so. To ensure that you receive the updates to Diagnostic Console provided by the August 2007 release, uninstall any previous release of version 2.1 or any previous version.

In addition to uninstalling Diagnostic Console, you should remove associated files (not removed during uninstallation) if no other AppManager component is installed on the computer. Removing these associated files enables the Diagnostic Console installation to prompt you to choose an AppManager version.

To uninstall a previous release or version:

1. Uninstall Diagnostic Console using **Start > Settings > Control Panel** > **Add or Remove Programs**.
2. When prompted to uninstall Performance Endpoints, click **No** if you are upgrading from a previous release of version 2.1. Because previous releases of version 2.1 shipped with an earlier version of the Performance Endpoints, the upgrade to version 5.1, included in the August 2007 release of version 2.1, will work properly.
3. ***If no other AppManager components are installed on this computer***, navigate to the `\Program Files\NetIQ\AppManager\bin` directory and delete it.

Important In order for Diagnostic Console installation to prompt you to select the version of AppManager you will use, you must delete the `AppManager\bin` directory. The files in this directory contain information that causes Diagnostic Console to assume you will use the version of AppManager you used with the previous release of version 2.1. If you do not delete the `AppManager\bin` directory, you will be unable to tell Diagnostic Console that you want to work with any newer version of AppManager, such as version 7.0.

Installing .NET Framework

Microsoft.NET Framework version 1.1 is a pre-requisite for running Diagnostic Console and is installed during setup for all supported operating systems *except* Microsoft Windows Vista. For all operating systems except Vista, Diagnostic Console installs .NET Framework 1.1 if it is not already installed.

When Vista is installed, the Diagnostic Console process incorrectly detects the presence of version 1.1. Although Vista does not install .NET Framework 1.1 during its installation, it does create a .NET Framework folder, thereby causing Diagnostic Console to incorrectly assume that .NET Framework 1.1 is already installed.

In order for Diagnostic Console to operate properly on Vista, you must manually install .NET Framework 1.1. Download and install the following Microsoft packages:

- Microsoft .NET Framework Version 1.1 Redistributable Package: www.microsoft.com/downloads/details.aspx?familyid=262D25E3-F589-4842-8157-034D1E7CF3A3&displaylang=en
- Microsoft .NET Framework Version 1.1 Service Pack 1: www.microsoft.com/downloads/details.aspx?FamilyID=A8F5654F-088E-40B2-BBDB-A83353618B38&displaylang=en

Setting Administrative Privileges

Before you start the console, ensure that you have set the proper administrative privileges on the target computer.

- Administrative Privileges for WMI Data Sources
- Administrative Privileges for AppManager Data Sources

Administrative Privileges for WMI Data Sources

You must have administrative privileges on the target computer. If you attempt to diagnose a target computer for which you do not have administrative privileges, you will be denied access.

If you are denied access to a target computer, you can either log on to the console computer with a different account that has administrative privileges on the target computer or grant administrative privileges to your current console account on the target computer. For more information about this, see your Microsoft Windows documentation.

You must also be a member of the local administrators group on the Diagnostic Console computer.

Administrative Privileges for AppManager Data Sources

You must have administrative privileges on the target computer if you want to be able to use the Computer Management and Event Viewer Related Links. Both of these functions require administrator access.

For more information about assigning administrative privileges, see your Microsoft Windows documentation.

Installing Microsoft XML Parser

To diagnose a Windows 2000 computer and use AppManager as a data source, the Microsoft XML Parser must be installed on the Windows 2000 computer.

If the Microsoft XML Parser is not installed, the AppManager Operator Console and the Diagnostic Console raise events when you attempt to collect data using AppManager on the target computer.

You must manually install the Microsoft XML Parser on a Windows 2000 computer. This issue is not applicable to Windows Server 2003 and Windows XP computers. The Microsoft XML Parser is included with Windows Server 2003 and Windows XP.

The setup program for Microsoft XML Parser Version 3.0 SP1 is included in the AppManager installation kit in the `\appmanager\extras\utilities\msxml_setup` folder.

Starting the Console

You can start the console in one of several ways:

- Start Menu Using AppManager as Data Source
- Start Menu Using WMI as Data Source
- Command Line Using AppManager as Data Source
- Command Line Using WMI as Data Source
- AppManager Operator Console Extensions Menu

Start Menu Using AppManager as Data Source

Take the following steps to start Diagnostic Console when using AppManager as a data source. You can use AppManager as a data source when you want to use the Active Directory and/or Exchange plug-ins, in addition to the other plug-ins.

The AppManager agent must be installed on the target computer in order for you to use AppManager as a data source.

To start Diagnostic Console:

1. Click **Start > Programs > NetIQ > AppManager > Diagnostic Console > Diagnostic Console**. The NetIQ AppManager Diagnostic Console Logon dialog box is displayed.
2. In the Data Source panel, select **Use AppManager**.
3. In the AppManager Logon panel, select the name of the **Server** that is monitoring the target computer.
4. Type or select the name of the **Repository** for the server. The default is QDB.
5. Select to use **Windows** or **SQL Server** authentication. If you select **Use SQL Server authentication**, then enter the appropriate **Login Name** and **Password**.

6 Click **Logon** to populate the tabs in the Target Machine panel with the names of all the computers that are monitored by the computer you selected in the **Server** drop list.

7 In the Target Machine panel, click the tab that corresponds to the type of computer that you want to target.

8 Select the computer that you want to target. If the computer you want does not appear in the list, then you must add and discover it in the TreeView pane of the AppManager Operator Console of the computer you selected in the **Server** drop list. You can then attempt to target that computer with Diagnostic Console.

Notes

- For more information, see "How Diagnostic Console Interacts with AppManager" on page 12.
- To target an Exchange virtual server, click the **Exchange** tab and select the target computer that corresponds to the Exchange virtual server that you want to target.

9 Click **OK**. Diagnostic Console starts with the selected computer as the target.

Start Menu Using WMI as Data Source

Take the following steps to start Diagnostic Console when using WMI as a data source. You can use WMI as a data source when you want to use any plug-in other than Active Directory and Exchange.

To start Diagnostic Console:

1 Click **Start > Programs > NetIQ > AppManager > Diagnostic Console > Diagnostic Console**. The NetIQ AppManager Diagnostic Console Logon dialog box is displayed.

2 In the Data Source panel, select **Use Windows Management Interface**.

3 On the **NT** tab in the Target Machine panel, select the computer that you want to target.

   If the name or IP address that you want to target is not in the list, click **Add** and enter the name or IP address in the Add Target Machine dialog box. Click **OK** to return to the Logon dialog box.

4 Click **OK**. Diagnostic Console starts with the selected computer as the target.

Command Line Using AppManager as Data Source

From the command line, you can open Diagnostic Console on any target computer for which you have administrator privileges. Use the following command line syntax when using AppManager as your data source:

```
<install>\Bin\RTDC DATASOURCE=AM SERVER=<name of AppManager
server> DBNAME=<repository name> USER=<login name> PWD=<password>
COMPUTER=<name of target computer>
```

where `<install>` is the directory in which you installed Diagnostic Console. Use the `USER` and `PWD` arguments if you are logging on with SQL Server authentication. If you are logging on with Windows authentication, omit the `USER` and `PWD` arguments.

Command Line Using WMI as Data Source

From the command line, you can open Diagnostic Console on any target computer for which you have administrator privileges. Use the following command line syntax when using WMI as your data source.

```
<install>\Bin\RTDC DATASOURCE=WMI COMPUTER=<name of target
computer>
```

where `<install>` is the directory in which you installed Diagnostic Console.

AppManager Operator Console Extensions Menu

If you have AppManager Operator Console installed on your computer, you can start Diagnostic Console by clicking **Extensions > Diagnostic Console**. The Diagnostic Console Login dialog box is displayed with AppManager information already in place. You need to select the target computer before logging in. For more information, see "Start Menu Using AppManager as Data Source" on page 9 and follow the instructions beginning at Step 7.

How Diagnostic Console Interacts with AppManager

When you log on to Diagnostic Console, you can choose to use AppManager as your data source.

Two conditions must exist in order for Diagnostic Console to use AppManager as a data source:

- the computers on which you installed the Diagnostic Console agent must have been discovered in the TreeView pane of the AppManager Operator Console, *and*
- the AppManager agent must be installed on the target computer.

It is important to understand how Diagnostic Console interacts with AppManager before you choose it as a data source. You may have several tasks to perform in AppManager before Diagnostic Console is able to diagnose its data.

The following topics are discussed:

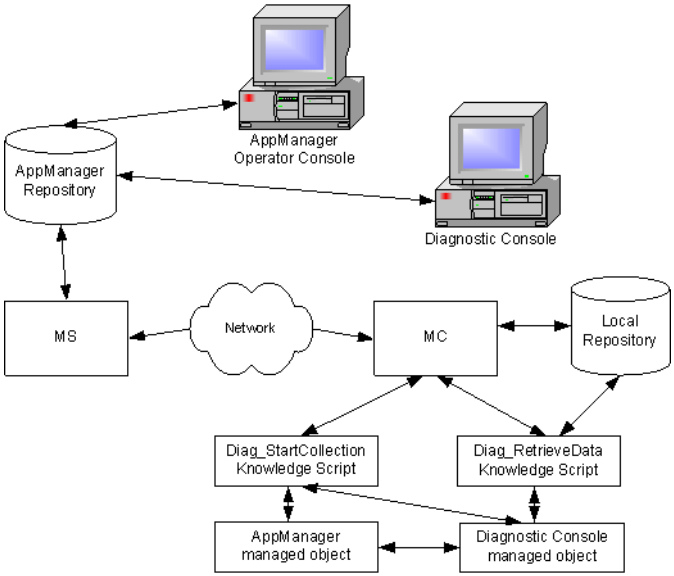
- Reviewing Diagnostic Console Architecture
- Setting AppManager to Collect Data Details
- Setting General Security Manager Permissions
- Setting Security Manager Permissions for Exchange
- Understanding Knowledge Script Jobs
- Using Action_Diagnose

Reviewing Diagnostic Console Architecture

Once you select AppManager as your data source and then log in to Diagnostic Console, AppManager invokes Knowledge Scripts that collect and retrieve data:

Knowledge Script	Description
Diag_StartCollectionAD	Tells the Diagnostic Console managed object to collect data relating to Active Directory. In addition, you can choose to enable or disable the collection of Active Directory object counts. AppManager invokes this script only if Active Directory is discovered on the target computer.
Diag_StartCollectionExchange	Tells the Diagnostic Console managed object to collect data relating to Microsoft Exchange. AppManager invokes this script only if Exchange is discovered on the target computer.
Diag_StartCollectionNT	Tells the Diagnostic Console managed object to collect data relating to Microsoft Windows.
Diag_RetrieveData	Tells the Diagnostic Console managed object to send all collected data back to the database. AppManager invokes two instances of this script: one for Windows data and one for Exchange data, and one for Active Directory data.

When the management server sees the Knowledge Script jobs in the AppManager database (QDB), it sends the jobs to the managed client. The managed client then runs the collection scripts, which collect data from the appropriate managed object. For example, Diag_StartCollectionNT collects CPU usage data from the Windows managed object. The collected data is passed to the Diagnostic Console managed object.



Meanwhile, the managed client runs Diag_RetrieveData, which retrieves the collected data from the Diagnostic Console managed object and passes it to the managed client. From there, the managed client sends the collected data back to the management server every 15 seconds. The management server inserts the data in the QDB. Diagnostic Console monitors the QDB for new data, which is displayed with every refresh of the charts and tables in the Console interface.

The collected Diagnostic data is stored in the AppManager repository in the same way that data from other Knowledge Script jobs is stored. Every night, a SQL job (`NetIQAMDCDailyQDB`) deletes all data that is more than 24 hours old or for which the job no longer exists, in order to prevent data buildup.

Setting AppManager to Collect Data Details

You need to configure AppManager to collect the data details that Diagnostic Console will diagnose. If you use AppManager as a data source and have not configured AppManager to collect data details, then Diagnostic Console will not start properly. The log-on process will time out while searching for AppManager data that does not exist.

Because of an issue in AppManager version 6.x, you may need to set the *global* data-collection option, causing all Knowledge Scripts that run to collect data details. By default, the global data-collection option is enabled. If you have disabled the option, you must enable it again before attempting to use AppManager as a data source.

The issue is corrected in AppManager version 7.x, and so you can collect data details on a per-script basis.

To collect data details for AppManager version 6.x:

1. From the AppManager Operator Console, click **File > Preferences**. The Preferences dialog box is displayed.
2. Click the **Repository** tab and then click the **Advanced Properties** button. The Advanced Options dialog box is displayed.
3. In the Data options panel, select **Collect data details with data point**.
4. Click **OK** twice to close the dialog boxes.

To collect data details for AppManager version 7.x:

1. From the Properties dialog box of the Knowledge Script you are running, click the **Advanced** tab.
2. In the Data options panel, select **Collect data details with data point**.
3. Click **OK**, or finish setting script parameters on the other tabs.

Setting General Security Manager Permissions

Every user of Diagnostic Console must have, at minimum, the following permissions set on the **Functional Rights** tab in AppManager Security Manager.

Jobs	Rights
For existing jobs	Permission to delete jobs, and either of the following: • Permission to start, stop, and close existing jobs, but not to modify job properties • Permission to start, stop, and close existing jobs, and to modify job properties
For new jobs	Permission to start new jobs and set their initial properties

Notes

- Any user using the default predefined role as a Read-Only user will be unable to use Diagnostic Console.
- You *must* have Administrator privileges set in Security Manager in order to stop and start services.
- Refer to the *Administrator Guide* for AppManager for more information about setting user permissions.

In addition to setting permissions on the **Functional Rights** tab, you also need to select the **Diag** check box on the **Knowledge Script** tab. This selection allows your user to view the Diag category of Knowledge Scripts in AppManager.

Setting Security Manager Permissions for Exchange

If you are using Diagnostic Console to diagnose target computers that are running Microsoft Exchange, then you need to set user permissions in AppManager Security Manager. Diagnostic Console is unable to collect Exchange data for Queue Status, Top Ten Users, and Top Ten Folders until you set user permissions.

To set Exchange permissions:

1. From the AppManager Operator Console, click **Extensions > Security Manager**. The Security Manager window is displayed.
2. Expand the Computers branch of the tree and select the Exchange computer that you want to target.
3. Click the **Exch2000/2003** tab and then click **Add**. The Add Exch 2K/2003 Mailbox dialog box is displayed.
4. In the **Server Name** field, type the name of the target computer.
5. In the **Profile** and **Mailbox Alias** fields, type the Exchange Profile and Mailbox Alias names you have set up using the Exchange administrator for the selected computer. The Exchange client profile is tied to the Windows user account you set up for the Exchange Managed Object service on the selected computer.
6. Click **OK**, then click **Apply**.

Note For more information about setting user permissions, see the *Administrator Guide* for AppManager.

Understanding Knowledge Script Jobs

The Knowledge Scripts for Diagnostic Console (on the **Diag** tab of the Operator Console) require no user interaction. Do *not* change the parameter settings for these scripts—you will severely impact the data that Diagnostic Console collects.

The Diag Knowledge Scripts run for 48 hours before stopping or until you log out of Diagnostic Console, whichever comes first. All normally terminated jobs are deleted from the AppManager Operator Console when you log out of Diagnostic Console. If a job is terminated abnormally for any reason—such as a power outage that turns off the Diagnostic Console computer—then it will not be deleted when Diagnostic Console is shut down. You should periodically check the Operator Console for abandoned Diag Knowledge Script jobs and delete them.

Using Action_Diagnose

Run this AppManager Knowledge Script to trigger Diagnostic Console to diagnose a problem on a target computer that has raised an event. For more information, see the following topics:

- How the Action Script Works
- Configuring the Script

How the Action Script Works

When you run a Monitoring Knowledge Script, you can choose to have Diagnostic Console diagnose the problem should the Monitoring script raise an event. AppManager uses an Action script, Action_Diagnose, to invoke Diagnostic Console.

Action_Diagnose uses an interface to Diagnostic Console to define the parameters of the diagnosis, run the diagnosis, and save the results. The parameters used to define the diagnosis are taken from the Monitoring script that generated the event.

Note If the AppManager report agent is installed on the same computer on which Action_Diagnose is run, then you can select to use the report agent settings, which allows the diagnosis results to be integrated with the AppManager Report Binder.

Upon completion of the diagnosis, AppManager raises an event that contains the results of the diagnosis. In the event message for a successful diagnosis, the **Message** tab contains the full path of the location of the output files. An event for an unsuccessful diagnosis contains an error message explaining why the diagnosis was unsuccessful.

The HTML report that is generated will contain hyperlinks to the Diagnostic Console plug-in report file. Click on these hyperlinks to open the report.

Configuring the Script

This section discusses the two ways in which you can configure Action_Diagnose.

Diagnostic Console and AppManager on one computer The most common configuration is one in which the AppManager server components (repository, management server, consoles, and agent, including the report agent) are installed on a single computer. Diagnostic Console is installed on this same computer. Installing both applications on the same computer allows Action_Diagnose to run on the management server computer, which is the default location.

To configure the script to run on the management server:

1. In the Properties dialog box of the Monitoring script, click the **Actions** tab.
2. Click **New**. A drop list is displayed in the **Action** field.
3. In the **Action** field, select **Action_Diagnose**.
4. Continue entering information on the other tabs, or click **OK** to start the monitoring job.

Diagnostic Console and AppManager on separate computers An alternative configuration is one in which Diagnostic Console and the AppManager agent (optionally, the report agent) are installed on a computer that is remote from the computer on which the AppManager repository and management server are installed. In this configuration, you must configure Action_Diagnose to run on the remote, or proxy, computer. Diagnostic Console does not support running the script on the managed client computer.

To configure the script to run on a proxy computer:

1. In the Properties dialog box of the Monitoring script, click the **Actions** tab.
2. Click **New**. A drop list is displayed in the **Action** field.
3. In the **Action** field, select **Action_Diagnose**.
4. In the **Location** field, select **Proxy**. The Computer Browser dialog box is displayed.
5. Select the computer on which Diagnostic Console and the AppManager agent are installed, and then click **OK**.
6. Continue entering information on the other tabs, or click **OK** to start the monitoring job.

Using the WMI Service

When you started Diagnostic Console, you may have elected to use the *Windows Management Information (WMI)* service (`WinMgmt.exe`) to gather information. See the following topics for more information about working with WMI.

- WMI and Windows 2000
- WMI and Windows NT 4.0

WMI and Windows 2000

Under certain circumstances in which target computers are running Windows 2000, WMI can consume large amounts of system resources, even to the point where you can no longer diagnose the target computer. If you notice this condition and it goes uncorrected by Windows, you can resolve it immediately by restarting the WMI service.

Microsoft has addressed this problem for Windows XP and Windows Server 2003.

WMI and Windows NT 4.0

For target computers running Windows NT 4.0, you must install the WMI package (`wmint4.exe`) available from Microsoft:

```
http://download.microsoft.com/download/platformsdk/wmint4/1.5/NT4/
EN-US/wmint4.EXE
```

In general, Windows NT target computers running the WMI package report less information than computers running Windows 2000, XP, or Server 2003. Some necessary counters are not present in NT and therefore some graphs will not display the expected data.

Reviewing the Diagnostic Console Interface

When you open Diagnostic Console on a target computer, the default view is the Summary plug-in, which is the root object in the TreeView, as shown below:

The Diagnostic Console interface is composed of several different panes, some of which change with the selected plug-in.

- The Navigation Pane
- The Performance Pane
- The Results Pane
- The Tasks Pane
- Refresh Rate

The Navigation Pane

The *Navigation Pane*, on the left of the interface, is composed of four distinct areas. You can show or hide the Navigation Pane by selecting **View > Navigation Pane**. The Navigation Pane is visible by default.

Navigation Pane Area	Description
Data Source	Indicates whether the data source is WMI or AppManager. If the data source is AppManager, then the source computer is also identified.
Computer field	Displays the target computer. The drop list contains a history list of the most recently targeted computers. As you target other computers (using WMI as a data source), the history list will continue to grow to unlimited size. You can edit it in the registry at any time by altering **RecentComputers**, located at: `HKEY_CURRENT_USER\Software\NetIQ\AppManager\Diagnostic Console` You can target only one computer at a time. If you want to look at several computers simultaneously, you will need to start additional instances of Diagnostic Console, each targeting a different computer.
TreeView	Standard tree view of the available Diagnostic Console plug-ins, with Summary as the root object.
Information box	A brief description of the selected plug-in. This is the only area of the Navigation Pane that changes when a different plug-in is selected. **Note** Many of the definitions of terminology discussed in the Information box are provided by the following: • msdn.microsoft.com • www.microsoft.com/technet

The Performance Pane

Across the top of the interface, and to the right of the Navigation Pane, is the *Performance Pane*. The Performance Pane contains graphical representations of CPU usage, virtual memory usage, and disk usage for the target computer. The data is updated in real-time.

In addition, for the Active Directory and Exchange plug-ins, the Performance Pane contains a Services chart that indicates which Active Directory or Exchange service is up, down, or not applicable to the target computer.

If you are targeting a computer running Windows 2000 Server Service Pack 2, the Disk Usage chart will not contain any data.

The Results Pane

The *Results Pane* is the main pane of the interface and shows the data that is specific to the plug-in that is currently selected and changes as the plug-in selection changes.

The Tasks Pane

The Tasks Pane, on the right side of the interface, consists of two sections: Tasks and Related Links. You can show or hide the Tasks Pane by selecting **View > Tasks Pane**.

Tasks

The Tasks section is specific to the selected plug-in and changes as the plug-in selection changes. For any given plug-in, the Tasks section will contain all or some of the following tasks.

Task	Description
Browse Network Drive	Allows you to revisit the contents of a mapped network drive. For more information, see "Network Drives" on page 58.
Create Process	Allows you to create, or launch, a process. For more information, see "Creating a Process" on page 97.

Task	Description
Create Service	Allows you to create a service. For more information, see “Creating Services” on page 116.
Delete Service	Allows you to delete a service. For more information, see “Deleting Services” on page 116.
End Process	Allows you to stop a process. For details, see “Stopping a Process” on page 98.
Export Data	Creates and displays an HTML page that summarizes the Results Pane. This page is simultaneously stored in the `\Export` directory of your Diagnostic Console installation path. If you used the default installation directory, the complete path will be: `C:\Program Files\NetIQ\AppManager\Diagnostic Console\Export\<computer>\<name of plug-in>` where `<computer>` is the name of the target computer. Images are stored in the same directory as the HTML page. Whenever you export the Results Pane, the new page replaces the previously exported HTML page. If your browser is set up for international symbols, it should be set to the proper encoding on the browser’s **View** menu.
IMAP4	Displays charts that highlight various information related to the IMAP4 protocol. For more information, see “IMAP4 Charts” on page 101.
Map Network Drive	Maps the selected drive on the target computer to a local drive on the console computer. For more information, see “Network Drives” on page 58.
MAPI	Displays charts that highlight various information related to the MAPI protocol. For more information, see “MAPI Charts” on page 101.
MTA	Displays charts that highlight various information related to the MTA protocol. For more information, see “MTA Charts” on page 102.
Overview	Displays the default view of the Protocols plug-in. For more information, see “Overview Panels” on page 100.
OWA	Displays charts that highlight various information related to the OWA protocol. For more information, see “OWA Charts” on page 102.
Pause/Resume Service	Allows you to pause and/or resume a service. For more information, see “Pausing/Resuming Services” on page 116.
POP3	Displays charts that highlight various information related to the POP3 protocol. For more information, see “POP3 Charts” on page 103.

Task	Description
Remove Network Drive	Allows you to unmap a drive. For more information, see "Network Drives" on page 58.
Restart Computer	Restarts the target computer. For more information, see "Restarting and Shutting Down a Computer" on page 119.
Route Table	Displays the Routing Table for Windows XP or Server 2003 target computers. For more information, see "Routing Table" on page 94.
Run DC Diag	Launches the Microsoft support tool `dcdiag.exe`. This tool analyzes the state of Domain Controllers in a forest or enterprise, and reports any problems to assist in troubleshooting. DC Diag helps you identify abnormal behavior in your system. For help using DC Diag, see Microsoft Support Tools Help, or specify `/h` in the **Arguments** field of the Task Results dialog box. Once you click **Run DC Diag**, the Tasks Results window appears to display the results of the analysis. To save the results of the analysis as a text file, click **File > Save** or **File > Save As**. To rerun the analysis, click **File > Rerun Command**, or click the **Rerun** button. **Note** This task works only if Microsoft Support Tools are installed on the Diagnostic Console computer. Microsoft Support Tools are available on the platform CD or from the Microsoft Web site.
Run FRS Ultrasound	Launches Microsoft Ultrasound, a support tool for monitoring FRS (File Replication Service) and for diagnosing related issues. FRS replicates files and folders in the `SYSVOL` file share on Domain Controllers and files in Distributed File System (DFS) targets. Ultrasound consists of a controller, a database, a console, and WMI providers for Domain Controllers. You should install the Microsoft Ultrasound controller on a computer that is a member of a domain. The installation will fail if you install the controller on a computer that is a member of a work group. **Note** This task works only if Microsoft Ultrasound is installed on the Diagnostic Console computer in the default location suggested by the Ultrasound setup program. Microsoft Ultrasound is available as a download from the Microsoft Web site.
Run Replication Monitor	Launches the Microsoft support tool `replmon.exe`. This tool allows you to view the status of replication agents and troubleshoot potential problems at the Distributor. You can also use this tool to determine which servers hold the operations master roles in a forest, and to identify the Domain Controllers and Global Catalog servers for the forest. **Note** This task works only if Microsoft Support Tools are installed on the Diagnostic Console computer. Microsoft Support Tools are available on the platform CD or from the Microsoft Web site.

Task	Description
Service Properties	Opens the Services Properties dialog box. For more information, see "Service Properties" on page 115.
Shutdown Computer	Shuts down the target computer. For more information, see "Restarting and Shutting Down a Computer" on page 119.
SMTP	Displays charts that highlight information related to the SMTP protocol. For more information, see "SMTP Charts" on page 104.
Start/Restart Service	Allows you to start or restart a service. For more information, see "Starting/Restarting Services" on page 115.
Stop Service	Allows you to stop a service. For more information, see "Stopping Services" on page 116.
View Categorizer	Displays five charts relating to the Message Categorizer queue. For more information, see "Message Categorizer Queue Charts" on page 42.
View Log File List	Displays information about the transaction log for storage groups. For details, see "Log File List" on page 72.
View Overview	Displays the default view of the Information Store plug-in. For more information, see "Overview Charts" on page 68.
View Queues (Advanced Queues plug-in)	Displays the default view of the Advanced Queues plug-in. For details, see "WMI Query Table" on page 40.
View Queues (Information Store plug-in)	Displays charts that highlight various information related to Information Store queues. For details, see "Queue Charts" on page 69.
View SP/Hotfixes	Displays the **Hotfixes** tab of the Windows plug-in. The **Hotfixes** tab provides details about Windows service packs, hotfixes, and quick fix engineering (QFE) information. For more information, see "Hotfixes Tab" on page 133.
View Top Ten Folders	Displays information about the 10 largest folders for mailbox and public stores. For details, see "Top Ten Folders" on page 70.
View Top Ten Users	Displays information about the 10 most frequent users for mailbox and public stores. For details, see "Top Ten Users" on page 71.

Related Links

The Related Links section provides access to NetIQ and to sources of information about the target computer.

Link	Function
Computer Management	Opens the Computer Management dialog box for the target computer. This is the same dialog box that you can access from the **Start > Programs > Administrative Tools** menu on the target computer.
Event Viewer	Launches the MMC administrative tool, `eventvwr.mmc`. You can also find this tool on the Computer Management dialog box. See the previous row for navigation instructions.
Performance Endpoints	Opens the NetIQ Performance Endpoint Web page, where you can obtain information and download the software. To test network connectivity, you need NetIQ Performance Endpoint software installed on each computer you intend to test. As part of the installation process, the endpoint for Windows is automatically installed on the computer where you installed Diagnostic Console. For more information, see "Installing Performance Endpoints" on page 78.
Remote Desktop	Accesses the target computer in a separate window. Diagnostic Console will launch either the Remote Desktop program or Terminal Services client, whichever you have installed on your computer. You can access any Windows Server or Windows XP computer that supports Terminal Services or Remote Desktop. You must be a member of the Administrator group on the remote computer to use Remote Desktop.
Submit Comments to NetIQ	Allows you to contact NetIQ if you have problems with Diagnostic Console, comments about its performance, or suggestions for improving it.

Refresh Rate

When you use WMI as a data source, the Diagnostic Console interface refreshes itself every five seconds, pulling in any data that has been collected since the last refresh. The data collection rate varies by plug-in, but is based on a multiple of the refresh rate.

When you use AppManager as a data source, the Diagnostic Console interface refreshes itself every 10 seconds, pulling in any data that has been collected since the last refresh. The data collection rate varies by plug-in, but is based on a multiple of the refresh rate.

Reviewing Plug-ins

Diagnostic Console provides a variety of plug-in modules for displaying diagnostic information for specific components, services, or applications. To open a plug-in, simply click the plug-in name in the Navigation Pane. The contents of the Results Pane change according to the plug-in that you select.

Plug-in	What It Does
Active Directory	Provides an overall view of the health of Active Directory on the target computer. Also displays information seen in four other Active Directory plug-ins: • Database • LSASS • Replication • SYSVOL For more information, see "Understanding the Active Directory Plug-in" on page 34.
Advanced Queues	Provides details about each queue for each virtual server related to the target computer. Each tab contains graphs and a table that detail the number of messages for the Local Queue, the Pre-Submission queue, the Pre-Categorizer queue, the Pre-Dynamic queue, and any local queues. For more information, see "Using the Advanced Queues Plug-in" on page 39.
CPU	Provides basic information about the target computer, such as processor type and manufacturer, as well as graphical representations of processor time, performance rates, context switches per second, and processor queue length. For more information, see "Using the CPU Plug-in" on page 43.
Database	Provides information (DIT volume usage and object counts) about the Active Directory database on the target computer. For more information, see "Using the Database Plug-in" on page 47.
Directory Services	Identifies the Domain Controller and Global Catalog of the target computer, as well as the response time of each to the server. In addition, you can use the Directory Services plug-in to monitor the number of LDAP searches per second, the total number of LDAP searches, the number of cache hits per second, and the total number of cache hits. For more information, see "Using the Directory Services Plug-in" on page 49.

Plug-in	What It Does
Disks	Provides a description of every drive on the target computer, as well as graphical representations of disk usage, disk KB per second, disk I/O per second, percent disk time, and disk queue length. For more information, see "Using the Disks Plug-in" on page 53.
Exchange	Provides an overall view of the health of Exchange on the target computer, displaying information gathered from four other plug-ins: • Advanced Queues • Directory Services • Information Store • Protocols For more information, see "Understanding the Exchange Plug-in" on page 60.
Information Store	Provides information about the server's Storage Groups. Each tab contains a section for each mailbox and public folder that identifies the location of the .edb and .stm files, indicates the size of the Send and Receive queues, and displays the amount (in MB) of used and free space. For more information, see "Using the Information Store Plug-in" on page 67.
LSASS	Provides information (connection information, NTDS performance, and response time), pertinent to the target computer, about Active Directory server functions provided by the LSASS service. For more information, see "Using the LSASS Plug-in" on page 63.
Memory	Provides a description of the target computer's virtual memory usage, page file, and configuration. In addition, this plug-in provides a graphical representation of memory pages per second, physical memory usage, and page file usage. For more information, see "Using the Memory Plug-in" on page 73.
Network Interface	Provides a list of the target computer's network interfaces, as well as a detailed description of the configurations and protocols for each interface. For more information, see "Using the Network Interface Plug-in" on page 91.
Network Connectivity	Provides the means for running ping and endpoint tests, and displays the test results. For more information, see "Using the Network Connectivity Plug-in" on page 77.
Network Performance	Provides a graphical representation of details about network traffic: utilization, Kbytes per second, packets per second, and average packet size in bytes. For more information, see "Using the Network Performance Plug-in" on page 89.

Plug-in	What It Does
Processes	Provides information about every process that is running on the target computer, such as average CPU, memory usage, virtual memory size, and process ID. For more information, see "Using the Processes Plug-in" on page 95.
Protocols	Provides information about the six protocols that Exchange uses: SMTP, MTA, MAPI, OWA, POP3, and IMAP4. For each protocol, you can determine whether it is up or down, and view charts that display metrics such as queue length and number of messages sent. For more information, see "Using the Protocols Plug-in" on page 99.
Replication	Provides information, pertinent to the target computer, about the Active Directory server functions related to partition replication. For more information, see "Using the Replication Plug-in" on page 105.
Security Subsystem	Provides information about the target computer related to kerberos and NTLM authentication. For more information, see "Using the Security Subsystem Plug-in" on page 111.
Services	Provides information about every service that is running on the target computer, such as a description, the status, and the startup type. For more information, see "Using the Services Plug-in" on page 113.
Shutdown	Provides information related to the shutdown conditions of the target computer, such as shutdown and startup time, the elapsed amount of downtime, and the percentage of time the target computer was available. For more information, see "Using the Shutdown Plug-in" on page 117.
System	Provides details regarding the target computer: computer system, operating system, main board, and BIOS. For more information, see "Using the System Plug-in" on page 125.
SYSVOL	Provides information related to the SYSVOL share for the target computer, such as response time and status. For more information, see "Using the SYSVOL Plug-in" on page 129.
Windows	Provides detailed information about the Windows operating system and environment on the target computer. Detailed information includes build number, operating system name, users, and service pack version. For more information, see "Using the Windows Plug-in" on page 131.

Getting Help

To get help for the console itself or for a plug-in, click **Help > Diagnostic Console Help**.

Chapter 2

Using the Active Directory Plug-in

The Active Directory plug-in provides an overall view of the health of Active Directory on the target computer. This plug-in also displays information seen in four other Active Directory plug-ins:

- Database
- LSASS
- Replication
- SYSVOL

See the following topics for more information about the function of the Active Directory plug-in and the data in the Results Pane.

Understanding the Active Directory Plug-in

In order to diagnose Active Directory data, you must have selected AppManager as a data source when you logged in to Diagnostic Console. Once you select AppManager as your data source and then log in, AppManager invokes two Knowledge Scripts that collect and retrieve data related to Active Directory:

- **Diag_StartCollectionAD** tells the Diagnostic Console managed object to collect data relating to Active Directory. In addition, you can choose to enable or disable the collection of Active Directory object counts.
- **Diag_RetrieveData** tells the Diagnostic Console managed object to send all collected data back to the database.

The Knowledge Scripts for Diagnostic Console require no user interaction. Do *not* change the parameter settings for these scripts—you will severely impact the data that Diagnostic Console collects.

Note The Diag Knowledge Scripts runs for 48 hours before stopping or until you exit Diagnostic Console, whichever comes first.

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source, pulling in any data that has been collected since the last refresh. The data collection rate for the Active Directory plug-in is every 15 seconds, with the exception of the /3GB Option portion of the DC Information chart. Memory data for /3GB is collected every 100 seconds.

Active Directory Services Chart

In each of the Active Directory plug-ins, the Performance Pane contains a chart that is specific to Active Directory: the Active Directory Services chart. In the Active Directory Services chart, a green, upward-pointing arrow indicates that the service is up and running. A red, downward-pointing arrow indicates that the service is down. N/A indicates that the service is not applicable for the targeted computer.

DC Information Chart

The DC Information chart displays data about the Domain Controller that is being diagnosed.

Item	Description
FQDN	Fully qualified DNS name of the Domain Controller.
Site	Name of the site in which the Domain Controller resides.
DC IP Address	Primary IP address of the Domain Controller.
GC	Fully qualified DNS name of the Global Catalog server being used by the Domain Controller.
GC Site	Name of the site in which the listed Global Catalog resides.
DNS Servers	IP addresses of the DNS servers for the Domain Controller.
/3GB Option	Indicates whether the /3GB option has been set. /3GB specifies that three GB of RAM be reserved for applications and that one GB of RAM be reserved for system. This option is supported on Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows Server 2003 Enterprise Edition, and Windows Server 2003 Datacenter Edition for systems with more than one GB of RAM. This option is not supported on 64-bit systems, and will display “n/a” if you are targeting a 64-bit computer.

Roles Chart

The Roles chart identifies the FSMO (Flexible Single Master Operation) roles and server functions that the Domain Controller is performing:

Role	Description
PDC	Primary Domain Controller (PDC) master role, which is responsible for logon authentication within the domain. The PDC emulator acts like a Windows NT PDC for Windows 2000 domains that have Windows NT backup Domain Controllers still in operation or have downlevel clients that expect a PDC to be present.
Schema	Schema Master FSMO role, which controls changes to the schema, a blueprint of all Active Directory objects and their attributes.
Domain Naming	Controls the addition and removal of domains in the forest.
Infrastructure	Updates changes to group members.
RID	Relative ID master role, which manages the distribution of RID numbers to other Domain Controllers.
GC	Global Catalog Server role, which provides universal group membership information to a Domain Controller when a logon occurs.
Pref. Bridgehead	Bridgehead servers replicate data for Active Directory sites. You can set a preferred bridgehead, which then is the only bridgehead server that the Knowledge Consistency Checker will use.
ISTG	Short for Inter-Site Topology Generator. Manages the inbound replication connection objects for all bridgehead servers in the site in which it is located

DIT Volume Usage Chart

The DIT Volume Usage chart displays key information about the volume containing the Active Directory database, `ntds.dit`. For more information, see "DIT Volume Usage Chart" on page 48. Click in this chart to display the Database plug-in.

Client Sessions Chart

The Client Sessions chart indicates the number of active Address Book, LDAP, and XDS client sessions. For more information, see "Client Sessions Chart" on page 64. Click in this chart to display the LSASS plug-in.

NETLOGON Chart

The NETLOGON chart displays the following information:

Item	Description
DNS Records Registered	Indicates, with a green or red light, whether all records are registered in DNS. Click on this item to display the LSASS plug-in.
SYSVOL Ready	Indicates, with a green or red light, whether the SYSVOL folder is shared and a local connection could be made. For more information, see "Using the SYSVOL Plug-in" on page 129. Click on this item to display the SYSVOL plug-in.

Replication Partitions Table

The Replication Partitions table displays key information about each replication partition in the database. For more information see "Replication Partitions chart" on page 108. Click in this chart to display the Replication plug-in.

Performance Charts

Three charts in the Results Pane present metrics related to NTDS performance. For more information, see "NTDS Performance Charts" on page 64. Click on any of these charts to display the LSASS plug-in.

Chart	Description
LSASS CPU Usage	Displays the amount of CPU used by the LSASS process.
LSASS Memory Usage	Displays the amount of memory used by the LSASS process.
LDAP Searches/Sec	Displays the number of Lightweight Directory Access Protocol searches performed per second.

Response Time Charts

Two charts in the Results Pane present metrics related to response time. For more information, see "Response Times Charts" on page 65. Click on either of these charts to display the LSASS plug-in.

Chart	Description
DC Bind Time	Displays the amount of time it takes to perform a Lightweight Directory Access Protocol bind to the local Domain Controller.
GC Bind Time	Displays the amount of time it takes to perform a Global Catalog bind to the local Domain Controller.

Chapter 3

Using the Advanced Queues Plug-in

The Advanced Queues plug-in provides details about each queue for each virtual server related to the target computer. Each virtual server has a tab that displays a table and graphs that detail the number of messages for the Local Queue, the Pre-Submission Queue, the Pre-Categorizer Queue, and the Pre-Routing Queue.

To access the Advanced Queues plug-in, expand the Exchange plug-in in the Navigation Pane.

See the following topics for more information about the function of the Advanced Queues plug-in and the data in the Results Pane:

- "Data Collection Rate" on page 39
- "WMI Query Table" on page 40
- "Local Queue Length Chart" on page 40
- "Pre-Submission Queue Length Chart" on page 41
- "Pre-Categorizer Queue Length Chart" on page 41
- "Pre-Routing Queue Length Chart" on page 41
- "Message Categorizer Queue Charts" on page 42

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source, pulling in any data that has been collected since the last refresh. The collection rate for the data that appears in the View Queues task view and the View Categorizer task view is three times the refresh rate, or every 30 seconds.

WMI Query Table

The WMI Query table, which appears above the charts in the Results Pane, displays the results of a WMI query by the AppManager Exchange2000_QueueStatus Knowledge Script.

Column	Description
Queue	Name of the WMI queue
Number of Messages	Number of messages in the queue
Total Size of Messages	Size in KB of the messages in the queue
Elapsed Time in Queue	Amount of time, in milliseconds, that messages reside in a message queue

Local Queue Length Chart

The Local Queue Length chart presents the number of messages in the local queue (this queue contains messages that are queued for local delivery on the server running Exchange to an Exchange mailbox). Under normal operating conditions, this number is rarely greater than zero.

A reading of greater than zero indicates that the server is receiving more messages than it can process. If this number increases steadily over time, there is probably a problem with the Exchange Store to which you are trying to deliver messages.

The data in the Local Queue Length chart is the same data that is referenced by *LocalAsyncQueue* in the table above the chart and by *Local delivery* in Exchange System Manager.

Pre-Submission Queue Length Chart

The Pre-Submission Queue Length chart presents the number of messages that have been acknowledged and accepted, but not yet processed by the SMTP service.

The data in the Pre-Submission Queue Length chart is the same data that is referenced by *PreSubmissionQueue* in the table above the chart and by *PreSubmissionQueue* in Exchange System Manager.

Note This chart is supported only for Exchange 2000 SP2 or later.

Pre-Categorizer Queue Length Chart

The Pre-Categorizer Queue Length chart presents the number of messages waiting for advanced address resolution. From this queue, the messages either go to the local queue or are sent to the routing engine to be delivered elsewhere. A high figure here compared to your baseline can indicate message flow problems.

The data in the Pre-Categorizer Queue Length chart is the same data that is referenced by *PreCatQueue* in the table above the chart and by *Messages awaiting directory lookup* in Exchange System Manager.

Pre-Routing Queue Length Chart

The Pre-Routing Queue Length chart presents the number of messages waiting to be routed to a destination server. Messages move from here to a link queue.

The data in the Pre-Routing Queue Length chart is the same data that is referenced by *PreRoutingQueue* in the table above the chart and by *Messages waiting to be routed* in Exchange System Manager.

Message Categorizer Queue Charts

Click the **View Categorizer** task link to review five charts relating to the Message Categorizer queue.

Chart	Description
Address Lookups	Number of address lookups dispatched per second to the directory service
Categorizations Failed (DS Connection Failure)	Number of categorizations that failed because of a directory service connection failure
Recipients NDRd By Categorizer	Number of recipients for which Message Categorizer is set to generate an NDR (non-delivery report)
Categorizations In Progress	Number of messages in the Message Categorizer queue. This figure indicates how well SMTP is processing LDAP (Lightweight Directory Access Protocol) lookups against Global Catalog servers. This figure should be at or around zero unless you are expanding distribution lists. Use this figure to assess the health of your Global Catalogs. If access to your Global Catalogs is slow, this figure can increase.
LDAP Connections Currently Open	Number of open LDAP connections

Chapter 4

Using the CPU Plug-in

The CPU plug-in provides basic information about the target computer, such as processor type and manufacturer, as well as graphical representations of processor time, performance rates, context switches per second, and processor queue length.

See the following topics for even more information about the function of the CPU plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 43
- "CPU Table" on page 44
- "Processor Time Graph" on page 45
- "Context Switches/sec Graph" on page 45
- "Performance Rates Graph" on page 46
- "Processor Queue Length Graph" on page 46

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source and every five seconds when you use WMI as a data source. A refresh pulls in any data that has been collected since the last refresh. The data collection rate for the CPU plug-in is the same as the refresh rate.

CPU Table

The CPU table in the Results Pane displays the following information:

Item	Description
Processor	A string uniquely identifying each processor.
Manufacturer	The name of the processor's manufacturer.
Name	The processor’s label.
Caption	A short description of the processor.
Current Clock Speed	The current speed (in MHz) of the processor.
Maximum Clock Speed	The maximum speed (in MHz) of the processor.
External Clock	The external clock frequency. If the frequency is unknown, this field is empty.
Data Width	Processor data width in bits.
L2 Cache Size	The size of the processor's Level 2 cache (external memory area that has a faster access time than RAM).
L2 Cache Speed	The clock speed of the processor's Level 2 cache (external memory area that has a faster access time than RAM).
Voltage	The voltage of the processor, if the SMBIOS specifies a voltage value. Otherwise, null.
Processor ID	The Processor ID property contains processor-specific information that describes the processor's features. Refer to Microsoft’s WMI documentation for the format.
Socket	The type of chip socket used for the processor.
Stepping	The revision level of the processor within the processor family.

Processor Time Graph

This graph plots the following quantities:

Plotted Quantity	Description
User	The percentage of processor busy time in “User” mode—this mode is used for applications, environment subsystems, and integral subsystems.
Privileged	The percentage of processor busy time in ”Privileged” mode—this mode is used for operating system components and hardware-manipulating drivers.
Total	The total percentage of all processor busy time.

Context Switches/sec Graph

Context Switches per second is the combined rate at which all processors on the computer are switched from one thread to another. Context switches occur when a running thread voluntarily relinquishes the processor, is preempted by a higher priority ready thread, or switches between user-mode and privileged (kernel) mode to use an Executive or subsystem service. The value reported is the sum of Context Switches per second for all threads running on all processors in the computer and is measured in numbers of switches. There are context switch counters on the System and Thread objects. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.

Performance Rates Graph

This graph plots the following quantities:

Plotted Quantity	Description
Interrupts/sec	The average number of hardware interrupts per second, not including Deferred Procedure Calls (DPC), which are counted separately. This value is an indirect indicator of the activity of devices that generate interrupts, such as the system clock, the mouse, disk drivers, data communication lines, network interface cards and other peripheral devices.
DPC Queued/sec	The overall rate at which DPCs are added to the processor's DPC queue. DPCs are interrupts that run at a lower priority than standard interrupts. Each processor has its own DPC queue.
DPC Rate	The rate at which DPCs are added to the processor's DPC queue between the timer ticks of the processor clock. DPCs are interrupts that run at a lower priority than standard interrupts. Each processor has its own DPC queue.

Processor Queue Length Graph

Processor Queue Length is the number of threads in the processor queue. Unlike the disk counters, this counter shows ready threads only, not threads that are running. There is a single queue for processor time even on computers with multiple processors. Therefore, if a computer has multiple processors, you need to divide this value by the number of processors servicing the workload. A sustained processor queue of less than 10 threads per processor is normally acceptable, depending on the workload.

Chapter 5

Using the Database Plug-in

The Database plug-in provides information about the Active Directory database of the target computer, such as DIT volume usage and object counts. See the following topics for even more information about the Database plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 47
- "DIT Volume Usage Chart" on page 48
- "Object Counts Table" on page 47

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source, pulling in any data that has been collected since the last refresh. The collection rate for the Database plug-in is also every 10 seconds, with the exception of the data in the Object Counts table. That collection rate is six times the refresh rate, or every one minute.

Object Counts Table

The Object Counts table displays the total number of objects found in the directory, and then breaks down the total by object type for the common naming contexts in Active Directory. The amount of time needed to collect object counts depends on the number of objects in your Active Directory. The Status field in the Object Counts table will indicate the state of the collection.

In AppManager, the Diag_StartCollectionAD Knowledge Script controls the collection of Active Directory object counts. The collection of this data causes a small increase in the overall CPU usage of the LSASS process. The increased usage is necessary for calculating the various object counts.

To avoid the increased LSASS CPU load, you can disable the collection of object counts by setting the *Collect database object count* parameter of the script to "No."

Note If you disable this parameter, the Object Counts table remains blank.

DIT Volume Usage Chart

DIT is the Active Directory database, `ntds.dit`. The DIT Volume Usage pie chart in the Results Pane displays the following information:

Item	Description
Size	Total capacity of the volume
Free	Free space available on the volume
DIT	Size of the ntds.dit
SYSVOL	Total size of the files under the SYSVOL share, if they are present on the volume
Logs	Total size of the database transaction logs, if they are present on the volume
Other	Total capacity of the volume, less the amounts for free space, DIT, AD Logs, and SYSVOL
DIT:	Path and filename of the DIT file
Logs:	Path of the Active Directory log files

Chapter 6

Using the Directory Services Plug-in

The Directory Services plug-in monitors various metrics for the Directory Service Access process, the Directory Service Access cache, and the SA NSPI Proxy.

To access the Directory Services plug-in, expand the Exchange plug-in in the Navigation Pane.

See the following topics for even more information about the Directory Services plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 49
- "DS Access Process Chart" on page 50
- "DS Access Cache Chart" on page 50
- "SA NSPI Proxy Chart" on page 51

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source, pulling in any data that has been collected since the last refresh. The data collection rate for the Directory Services plug-in is twice the refresh rate, or every 20 seconds.

DS Access Process Chart

The Directory Service Access process has memory cache to help reduce the number of LDAP requests. The following table describes the charts in the DS Access Process section of the Results Pane.

Chart	Description
LDAP Search Time	Amount of time (in ms) it takes to send an LDAP search request and receive a response.
LDAP Read Time	Amount of time it takes to send an LDAP read request and receive a response.
No. User Sync GC	Number of LDAP connections opened against Global Catalogs for use by Synchronous User Context operations. **Note** This chart displays data only if you are targeting an Exchange 2000 computer. The performance counter that provides the data for this chart does not exist in Exchange 2003.

DS Access Cache Chart

The Access Cache contains the results of recent Global Catalog queries. The Global Catalog contains all of the Active Directory information for a host domain. The following table describes the charts in the DS Access Cache section of the Results Pane.

Chart	Description
Cache Hits/Sec	Number of "object found in cache" events per second.
Cache Misses/Sec	Number of "object not found in cache" events per second.

SA NSPI Proxy Chart

In Exchange 2000, Microsoft changed how directory services were handled -- now everything is done through Active Directory. But older e-mail clients do not know how to talk to Active Directory, so Microsoft has a proxy (NSPI - Name Service Provider Interface) that takes old requests and forwards them to Active Directory.

The following table describes the charts in the SA NSPI Proxy section of the Results Pane.

Chart	Description
Client Connection Count	Number of clients that are connected to the NSPI Proxy.
Total Failed Client Connections	Number of failed connect operations from clients. This figure is an accumulation of all failures since the NSPI Proxy was started.
Total Failed Server Connections	Number of failed connect operations to the Domain Controller. This figure is an accumulation of all failures since the NSPI Proxy was started.

Chapter 7

Using the Disks Plug-in

The Disks plug-in provides a description of every drive on the target computer, as well as graphical representations of disk usage, disk KB per second, disk I/O per second, percent disk time, and disk queue length.

See the following topics for even more information about the Disks plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 53
- "Diagnosing Windows Computers" on page 54
- "Disks Tables" on page 54
- "Disk KB Per Second Graph" on page 56
- "Percent Disk Time Graph" on page 56
- "Disk I/O Per Second Graph" on page 57
- "Disk Queue Length Graph" on page 57
- "Usage Pie Chart" on page 57
- "Network Drives" on page 58

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source and every five seconds when you use WMI as a data source. The refresh pulls in any data that has been collected since the last refresh. The data collection rate for the Disks plug-in is five times the refresh rate.

Diagnosing Windows Computers

If you select a target computer that is running Windows NT or 2000, you will not see values in the Disks charts or tables unless you have run `diskperf -y` on the target computer. `Diskperf -y` controls the collection of performance counter data. If you are targeting a Windows 2000 computer, you can do this by physically going to the computer or you can use Remote Desktop, provided that Terminal Services has been installed on the target computer. If you are targeting a Windows NT computer, you must physically go to the target computer; Remote Desktop is not supported for target computers that are running Windows NT.

Note You can also use AppManager Operator Console to run the NTAdmin_RunDOS Knowledge Script on the remote computer.

`Diskperf -y` is automatically enabled in Windows XP or 2003. However, if you have disabled it for any reason, be sure to enable it again before attempting to collect disk usage data.

Disks Tables

Disks supported by this plug-in include both magnetic media (floppy disk, hard disk, removable cartridge) and optical media (CD-ROM, WORM, Erasable Optical).

- Logical Disks Table
- Physical Disks Table

Logical Disks Table

A logical disk is a storage device created by sub-dividing a physical storage disk into one or more parts (logical devices). Click the **Logical Disks** tab to reveal the Logical Disks table, which is described below:

Field	Description
Drive	Drive name, such as C:
Description	Type of drive, such as CD-ROM.
Volume Name	Volume name, if any.
File System	File system, such as FAT32, if applicable.
Used Space	Disk space taken up by data in Gigabytes.
Free Space	Disk space free of data in Gigabytes.
Capacity	Total disk space in Gigabytes.
Serial Number	Serial number of drive, if any.

If your target computer is a Windows 2000, XP, or 2003 server system, then the Logical Disks table will display network drives that have been mapped to that system.

Physical Disks Table

A physical disk is a single storage device. Click the **Physical Disks** tab to reveal the Physical Disks table, which is described below:

Field	Description
Drive	Name of physical (not logical) drive.
Manufacturer	Name of manufacturer.
Model	Manufacturer's model number.
Interface	Interface type of the drive, such as SCSI.
Size	Size of the disk drive = (total number of cylinders) x (tracks/cylinder) x (sectors/track) x (bytes/sector).
Media Type	Type of media used by the device, such as removable media.

Field	Description
Media Loaded	“Yes” if media for the drive is loaded. Will always be “Yes” for fixed drives.
Partitions	Number of partitions seen by the operating system.

Disk KB Per Second Graph

This graph plots the following quantities:

Plotted Quantity	Description
Read	Disk reads in Kb/sec
Write	Disk writes in Kb/sec
Total	Total disk reads and writes in Kb/sec

The Disk KB Per Second graph does not reflect data for mapped drives because the Windows program `diskperf` does not track performance metrics for mapped drives.

Percent Disk Time Graph

This graph plots the following quantities:

Plotted Quantity	Description
Read	Percent of time disk is busy reading
Write	Percent of time disk is busy writing
Total	Percent of time disk is busy reading or writing

The Percent Disk Time graph does not reflect data for mapped drives because the Windows program `diskperf` does not track performance metrics for mapped drives.

Disk I/O Per Second Graph

This graph plots the following quantities:

Plotted Quantity	Description
Transfers	Total number of read/write transfers in Kb/sec.
Splits	Split IO/sec reports the rate at which I/Os to the disk split into multiple I/Os. A split I/O may result from: • requesting data that is too large to fit into a single I/O • a fragmented disk
Reads	Disk reads in Kb/sec
Writes	Disk writes in Kb/sec

The Disk I/O Per Second graph does not reflect data for mapped drives because the Windows program `diskperf` does not track performance metrics for mapped drives.

Disk Queue Length Graph

This graph plots the following quantities:

Plotted Quantity	Description
Current	Current length of disk I/O queue length
Average	The average number of both read and write requests that were queued for the selected disk during the sample interval

The Disk Queue Length graph does not reflect data for mapped drives because the Windows program `diskperf` does not track performance metrics for mapped drives.

Usage Pie Chart

The Usage pie chart, which displays only in the **Logical Disks** tab, indicates the percentage of Used and Free space on the drive that you select in the Logical Disks table.

Network Drives

Click the **Map Network Drive** task link to map the selected drive on the target computer to a local drive on the console computer. It may take as long as two minutes for the drive to appear in the Logical Drives list. You cannot map a network drive that is not shared. If you attempt to do so, you will get an error message stating that the drive cannot be mapped—the message will not tell you why, however.

This task does not appear in the Tasks Pane unless you have targeted a remote computer.

To unmap a drive, click the **Remove Network Drive** task link. This task appears only if you have mapped a network drive.

Once a drive is mapped and as long as it has not been unmapped, you can use the **Browse Network Drive** task to revisit the contents of the mapped network drive.

These three tasks are unavailable if you use AppManager as a data source.

Chapter 8

Using the Exchange Plug-in

The Exchange plug-in provides an overall view of the health of Exchange 2000 or 2003 on the target computer, displaying information gathered from three other plug-ins:

- Advanced Queues
- Information Store
- Protocols

See the following topics for even more information about the Exchange plug-in and the data in the Results Pane.

- "Understanding the Exchange Plug-in" on page 60
- "Data Collection Rate" on page 60
- "Exchange Services Chart" on page 61
- "Exchange Information Chart" on page 61
- "Protocols - Overall Load Chart" on page 61
- "Advanced Queues - Messages Chart" on page 61
- "Information Store Chart" on page 61

Understanding the Exchange Plug-in

In order to diagnose Exchange data, you must select AppManager as a data source when you log in to Diagnostic Console. Once you select AppManager as your data source and then log in, AppManager invokes two Knowledge Scripts that collect and retrieve data related to Exchange:

- **Diag_StartCollectionExchange** tells the Diagnostic Console managed object to collect data relating to Active Directory.
- **Diag_RetrieveData** tells the Diagnostic Console managed object to send all collected data back to the database.

The Diag Knowledge Scripts require no user interaction. Do *not* change the parameter settings for these scripts—you will severely impact the data that Diagnostic Console collects.

The Diag Knowledge Scripts run for 48 hours before stopping or until you log out of Diagnostic Console, whichever comes first.

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source, pulling in any data that has been collected since the last refresh. The data collection rate for the Exchange plug-in varies according to the data being collected:

Data	Data Collection Rate
Exchange Information chart	Once
Protocols - Overall Load	Three times the refresh rate, or every 30 seconds
Advanced Queues - Messages	Three times the refresh rate, or every 30 seconds
Information Store	Six times the refresh rate, or every 60 seconds

Exchange Services Chart

In the Exchange plug-ins, the Performance Pane contains a chart that is specific to Exchange: the Exchange Services chart. In the Exchange Services chart, a green, upward-pointing arrow indicates that the service is up and running. A red, downward-pointing arrow indicates that the service is down. N/A indicates that the service is not applicable for the targeted computer.

Exchange Information Chart

The Exchange Information chart identifies the version of Exchange that is running on the target computer.

Protocols - Overall Load Chart

The Overall Load chart displays the current number of receive messages, operations, and commands in the queue, by protocol.

Advanced Queues - Messages Chart

The Messages chart displays the total number of messages in the Local, Pre-Categorizer, and Pre-Routing queues. The data in this chart, which corresponds to data in the charts in the Advanced Queues plug-in, is an aggregate of all data across all virtual servers.

Information Store Chart

The Information Store chart displays the total number, in MB, of free space and used space in the mail store and public folders.

Chapter 9

Using the LSASS Plug-in

The LSASS plug-in provides information about core Active Directory server functions provided by the LSASS service on the target computer. Monitored functions include connection information, NTDS performance, and response time.

See the following topics for even more information about the function of the LSASS plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 63
- "Summary Tab" on page 64
- "DNS Registrations Tab" on page 65

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source, pulling in any data that has been collected since the last refresh. The collection rate for the LSASS plug-in is also every 10 seconds, with the exception of the data collected for DNS registrations. That collection rate is twice the refresh rate, or every 20 seconds.

Summary Tab

The following topics discuss the types of information displayed in the charts and graphs on the **Summary** tab.

- Client Sessions Chart
- NTDS Performance Charts
- Response Times Charts

Client Sessions Chart

The Client Sessions chart displays the following information:

Item	Description
Address Book	Number of active Address Book client sessions.
LDAP	Number of active LDAP client sessions.
XDS	Number of active Extended Directory Service client sessions. This value indicates the number of connections from other Windows 2000 services and the Exchange Administrator program. **Note** This metric is available only when targeting Windows 2000 server. If you are targeting any other system, then the XDS metric is n/a.

NTDS Performance Charts

Seven charts in the **Summary** tab present metrics related to NTDS performance.

Chart	Description
LSASS CPU Usage	Displays the amount of processor time used by the LSASS process.
LSASS Memory Usage	Displays the amount of memory used by the LSASS process.
Sub-level Searches/sec	Displays the number of sub-level searches performed per second.
LDAP Searches/sec	Displays the number of Lightweight Directory Access Protocol searches performed per second.
LDAP Binds/sec	Displays the number of binds performed per second.

Chart	Description
AB Searches/sec	Displays the number of Address Book searches performed per second.
AB ANR/sec	Displays the number of Ambiguous Name Resolution (ANR) queries performed per second.

Response Times Charts

Four charts in the **Summary** tab present metrics related to response time.

Chart	Description
DC Bind Time	Displays the amount of time it takes for the Domain Controller to perform an LDAP (Lightweight Directory Access Protocol) bind.
GC Bind Time	Displays the Amount of time it takes for the Global Catalog server to perform an LDAP bind.
Sub-search Query Time	Displays the amount of time it takes to perform a sub-search query.
ANR Query Time	Displays the amount of time it takes to perform an Ambiguous Name Resolution (ANR) query.

DNS Registrations Tab

The following table identifies the types of information displayed in the columns on the **DNS Registrations** tab. Each row in the table represents a DNS resource record in the database.

Column	Description
Registered	Indicates whether the DNS resource is registered to the Domain Controller. A registered resource is one that responds to a DNS lookup request. For more information about the registration, position your mouse pointer over the icon in the Registered column. Pop-up text indicates a return code and explains why the DNS record is registered or not.
Owner name	Full name of the DNS resource.
TTL (ms)	Amount of time (in milliseconds) that DNS clients can store information about this DNS resource record.

Column	Description
Class	Identifies a protocol family, such as INT for Internet.
Type	Specific classification of the DNS resource record. • An **A** record is a host address record, which maps a DNS domain name to a single 32-bit IP version 4 address. • A **CNAME** record is an alias record, which indicates an alternate or alias DNS domain name for a name already specified in other resource record types. • An **SRV** record is a service record, which allows administrators to use several servers for a single DNS domain. DNS clients that use SRV-type query ask for a specific TCP/IP service and protocol mapped to a specific DNS domain and receive the names of any available servers.
Data	Type-specific additional information. • For an A-type record, the data is the IP address of the host. • For a CNAME-type record, the data is fully qualified name for the target host. • For a SRV-type record, the data is the host name, priority, weight, and port number.

Chapter 10

Using the Information Store Plug-in

The Information Store plug-in provides information about the server's Storage Groups. Each tab contains a chart for each mailbox and public folder that identifies the location of the `.edb` and `.stm` files, indicates the size of the Send and Receive queues, and displays the amount (in MB) of used and free space.

Two charts at the bottom of the Results Pane indicate the amount of CPU and memory in use for `store.exe`.

To access the Information Store plug-in, expand the Exchange plug-in in the Tree View. See the following topics for even more information about the function of the Information Store plug-in and the data in the Results Pane.

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source, pulling in any data that has been collected since the last refresh. The data collection rate varies depending on the data being collected, as shown in the following table:

Data	Collection Rate
View Overview	Six times the refresh rate, or every 60 seconds
View Queues	Twice the base refresh, or every 20 seconds
Top 10 Users	Thirty times the refresh rate, or every 300 seconds
Top 10 Folders	Thirty times the refresh rate, or every 300 seconds
Log File List	Thirty times the refresh rate, or every 300 seconds

Overview Charts

Click the **View Overview** task link to display the default view of the Information Store plug-in. The Overview provides information about the server's Storage Groups. Each tab contains a section for each mailbox and public folder that identifies the location of the `.edb` and `.stm` files, indicates the size of the Send and Receive queues, and displays the amount (in MB) of used and free space.

The following table defines the items that you find in the charts in the Results Pane.

Items	Definition
Mailbox Store	Also known as a private information store in Exchange 5.5 and earlier. Mailbox stores contain individual user mailboxes, which in turn contain items to which only individual users have access.
Public Folder Store	Contains public folders, which in turn contain items to which all users have access.
Send Queue Size	Number of messages in the store's send queue. This figure should remain generally at zero during normal operations.
Receive Queue Size	Number of messages in the store's receive queue. This figure should remain generally at zero during normal operations.

Items	Definition
Other space	Equals the Total Disk Space less the amount of Free space, less the size of the `.stm`, less the size of the `.edb`.
% CPU for store.exe	Percentage of processing capacity used by the Exchange 2000 or 2003 `store.exe` process.
Memory for store.exe	Working set, or amount of memory used, for the `store.exe` process.

Queue Charts

Click the **View Queues** task link to display charts that highlight various information related to queues.

Chart	Description
Messages Sent/Min	Rate at which messages are sent to other storage providers.
Message Opens/Sec	Rate at which requests to open messages are submitted to the Exchange store. The value of this counter is specific to your organization.
Folder Opens/Sec	Rate at which requests to open folders are submitted to the information store.
Local Delivery Rate	Rate at which messages are being delivered locally. The value of this counter is specific to your organization.
Send Queue Size	Number of messages in the store's send queue. This figure should remain generally at zero during normal operations.
Receive Queue Size	Number of messages in the store's receive queue. This figure should remain generally at zero during normal operations.

Top Ten Folders

Click the **View Top Ten Folders** task link to display information about the 10 largest folders for mailbox and public stores.

Column Name	Description
Folder	Name of the folder
Path	File path of the folder
Size (KB)	Size of the folder, in kilobytes
Total Items	Number of messages in the folder
Created	Date the folder was created
Last Access	Date and time of the most recent access

In order for the Diag_StartCollectionExchange script to gather the data that the **View Top Ten Folders** task displays, the AppManager agent services must run as a Windows user account with an associated Exchange profile and mailbox. For help setting up Exchange mailboxes and profiles, see your Exchange documentation, the *Installation Guide* for AppManager, and the *AppManager for Exchange Management Guide*.

For more information about the Diag_StartCollectionExchange script, see "How Diagnostic Console Interacts with AppManager" on page 12.

Top Ten Users

Click the **View Top Ten Users** task link to display information about the 10 most frequent users for mailbox and public stores.

Column Name	Description
Mailbox	Name of the mailbox
Size (KB)	Size of the mailbox, in kilobytes
Total Items	Number of messages in the mailbox
Last Logged on By	Login ID of the user who last logged on to the mailbox
Email	E-mail address of the user who last logged on
Last Logon Time	Date and time of the most recent logon incident
Last Logoff Time	Date and time of the most recent logoff incident

In order for the Diag_StartCollectionExchange script to gather the data that the **View Top Ten Users** task displays, the AppManager agent services must run as a Windows user account with an associated Exchange profile and mailbox. For help setting up Exchange mailboxes and profiles, see your Exchange documentation, the *Installation Guide* for AppManager, and the *AppManager for Exchange Management Guide*.

Note For more information about the Diag_StartCollectionExchange script, see "How Diagnostic Console Interacts with AppManager" on page 12.

Log File List

Click the **View Log File List** task link to display information about the transaction log for each storage group.

Column Name	Description
Transaction Log	Name of the transaction log
Location	Location of the transaction log
Size	Size of the transaction log
Date	Date and time of the creation of the transaction log

Chapter 11

Using the Memory Plug-in

The Memory plug-in provides a description of the target computer's virtual memory usage, page file, and configuration. In addition, this plug-in provides a graphical representation of memory pages per second, and physical and virtual memory usage.

The Memory plug-in is *not* supported for target computers that are running Windows NT 4.0.

See the following topics for even more information about the function of the Memory plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 73
- "Memory Pages (per second) Graph" on page 74
- "Physical Memory Usage Chart" on page 75
- "Virtual Memory Usage Chart" on page 75
- "Memory Usage Table" on page 75
- "Page Files Table" on page 76
- "Configuration Table" on page 76

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source and every five seconds when you use WMI as a data source. The refresh pulls in any data that has been collected since the last refresh. The data collection rate for the Memory plug-in is twice the refresh rate.

Memory Pages (per second) Graph

This graph plots the following quantities:

Plotted Quantity	Description
Total Faults	Average number of pages faulted per second. This value is measured in number of pages faulted per second because only one page is faulted in each fault operation, therefore this figure is also equal to the total number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (those for which the faulted page is found elsewhere in physical memory). Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.
Transition Faults	Measured per second, the number of page faults that are resolved by recovering pages that were being used by another process sharing the page, or were on the modified page list or the standby list, or were being written to disk at the time of the page fault. The pages were recovered without additional disk activity. Transition faults are counted in numbers of faults; because only one page is faulted in each operation, it is also equal to the number of pages faulted.
Disk Read	Measured per second, the number of pages that are read from disk to resolve hard page faults. Hard page faults occur when a process refers to a page in virtual memory that is not in its working set or elsewhere in physical memory, and must be retrieved from disk. When a page is faulted, the system tries to read multiple contiguous pages into memory to maximize the benefit of the read operation.
Disk Write	Measured per second, the number of pages that are written to disk to free up space in physical memory. Pages are written back to disk only if they are changed in physical memory, so they are likely to hold data, not code. A high rate of pages output might indicate a memory shortage. Windows writes more pages back to disk to free up space when physical memory is in short supply. This counter shows the number of pages, and can be compared to other counts of pages, without conversion.
Disk Total	Rate at which pages are read from or written to disk to resolve hard page faults. This is a primary indicator of the kinds of faults that cause system-wide delays. It is the sum of Pages Read/sec and Pages Written/sec. It is counted in numbers of pages, so it can be compared to other counts of pages, such as Page Faults/sec, without conversion. It includes pages retrieved to satisfy faults in the file system cache (usually requested by applications) and non-cached mapped memory files.

Physical Memory Usage Chart

The Physical Memory Usage pie chart indicates the percentage of Available and Used physical memory on the target computer.

Physical memory is the amount of RAM (random access memory) installed. RAM is semiconductor-based memory that can be read and written by the microprocessor or other hardware devices.

Virtual Memory Usage Chart

The Virtual Memory Usage pie chart indicates the percentage of Available and Used virtual memory on the target computer.

Virtual memory is a combination of physical memory and paging files into one virtually addressable storage space.

Memory Usage Table

The following table describes the fields in the Memory Usage table:

Field	Description
Physical/Total	Total physical memory
Physical/Available	Physical memory unused and available in megabytes
Virtual/ Total	Total virtual memory
Virtual/Available	Virtual memory unused and available in megabytes

Page Files Table

The following table describes the fields in the Page Files table:

Field	Description
Path	Path to the page file
Size	Amount of disk space allocated for use by the page file
Current Usage	Amount of disk space currently used by the page file
Peak Usage	Highest page file usage

Configuration Table

The configuration is a list of the physical memory chips that are installed. The following table describes the fields in the Configuration table:

Field	Description
Description	Text description of the memory.
Device Locator	Label of the socket or circuit board containing the memory, such as SIMM 3.
Capacity	Total capacity of the memory in megabytes.
Data Width	Data width of the memory in bits.
Speed	Speed of the memory.
Type	Type of physical memory.
Form Factor	Form factor for the chip, such as SIMM (3) or TSOP (9).
Bank Label	Label of the bank where the memory is located.

Chapter 12

Using the Network Connectivity Plug-in

The Network Connectivity plug-in provides the means for running ping and endpoint tests, and displays the test results.

To access the Network Connectivity plug-in, expand the Network Interface plug-in in the Navigation Pane.

You must have NetIQ Performance Endpoint software installed on all computers for which you want to test connectivity. For more information, see "Installing Performance Endpoints" on page 78.

See the following topics for even more information about the function of the Network Connectivity plug-in and the data in the Results Pane.

Installing Performance Endpoints

Before you can test network connectivity, you need to install NetIQ Performance Endpoint software on each computer you intend to test. See the following topics for more information:

- Installing Endpoint Software on a Diagnostic Console Computer
- Installing Endpoint Software on Target Computers

Endpoints include a README text file that is available in the default program folder (`C:\Program Files\NetIQ\Endpoint`). The README file contains information about installation, compatibility, and the operating systems supported by Performance Endpoints.

The NetIQ Web site also offers a free *Performance Endpoints* guide that you can consult online at www.netiq.com/support/pe/documentation.asp.

Installing Endpoint Software on a Diagnostic Console Computer

As part of the installation process, the endpoint for Windows is automatically installed on the computer on which you installed Diagnostic Console.

However, if you rebooted during the Diagnostic Console installation, it is possible that the endpoint software was not installed properly.

Therefore, if you rebooted during installation, you should:

1. Choose **Start > Settings > Control Panel > Add/Remove Programs.**
2. Choose **NetIQ AppManager Diagnostic Console**, and click **Change/Remove**.
3. When the Installation wizard opens, select **Repair**, click **Next**, and then click **Finish** to reinstall the endpoint software.

Note If the endpoint software is properly installed, you should find a NetIQ Endpoint service running. Open the Services plug-in and verify

that the service is running, both on your own computer and on target computers.

Installing Endpoint Software on Target Computers

NetIQ provides Performance Endpoint software free of charge. Users on your network can install endpoints on their computers by visiting the NetIQ Web site at **www.netiq.com/download/endpoints** and downloading the endpoint appropriate for the operating system they are using. The whole procedure should take users less than five minutes. You should also read the endpoint documentation available at **www.netiq.com/support/pe/documentation.asp**. The *Performance Endpoints* guide and the individual endpoint manuals found on this site explain how to install and deploy endpoints for all supported operating systems.

Endpoints for Windows support the TCP, UDP, SPX, and IPX protocols. In these environments, the endpoint runs as a service after you enable it during installation. With other operating systems, the endpoint starts automatically. It functions only during tests and should not interfere with other application traffic on your computer.

To stop the endpoint:

1. Open a command prompt window and navigate to the directory where the endpoint is installed.
2. To stop a Windows Me endpoints, type `endpoint -k`.
3. To stop a Windows 2000, Windows XP, or Windows Server 2003 endpoint, type `net stop netiqendpoint`.
4. Alternatively, access the Services dialog box from the Control panel, select **NetIQ Endpoint**, and click **Stop**. For information on stopping endpoints for other operating systems, see the *Performance Endpoints* guide.

Selecting Endpoints for Connectivity Testing

Enter the names or network addresses for the endpoint computers you want to test in the fields labeled **From Endpoint 1** and **To Endpoint 2**. Endpoint 1 designates the computer that initiates a connectivity test, while Endpoint 2 indicates the partner computer.

Use numerical IP addresses for the TCP/IP protocol to eliminate DNS latency from your response time results.

Note Even if you can reach a computer by using `ping`, you must have endpoint software installed on that computer if you want to use the connectivity testing functions other than Traceroute. Traceroute tests do not require endpoint software to be installed on Endpoint 2.

Running Tests and Viewing results

When you have chosen your protocol and measurement type, click **Run** to run the test. The details automatically appear in the NetIQ Endpoint Test Results panel.

If two or more instances of Diagnostic Console attempt to monitor target computers with the Network connectivity plug-in, only the first instance will run. The first instance takes over the network port, which is then not available to the other.

Protocols

Diagnostic Console supports the following protocols for network connectivity testing: *TCP*, *UDP*, *SPX*, and *IPX*. Only the connectionless protocols, UDP and IPX, support Streaming tests. Only UDP and TCP support Traceroute tests.

Be careful to select a protocol that is enabled on both of the computers you are testing, as well as on the computer that is running Diagnostic Console. If you select a protocol that is not used by both computers,

you will get an error message. You should also make sure the network addresses you entered correspond to the protocol you selected.

Protocol	Description
TCP	Transmission Control Protocol—a connection-oriented protocol that is defined at the Transport layer of the OSI reference model. Provides reliable delivery of data.
UDP	User Datagram Protocol—a connectionless Transport layer protocol in the TCP/IP protocol stack that simply allows datagrams to be exchanged without acknowledgements or delivery guarantees, requiring other protocols to handle error processing and retransmission.
SPX	Sequenced Packet Exchange—a protocol used in Novell Netware networks that augments the datagram service; it was derived from the Switch-to Switch Protocol of the XNS protocol suite.
IPX	Internetwork Packet Exchange—a protocol used in Novell Netware networks for transferring information from servers to workstations. Similar to IP and XNS.

Measurements

The Network Connectivity plug-in takes the following measurements:

- Response Time
- Throughput
- Streaming
- Traceroute

Response Time

The Response Time test uses two parameter options: *Iterations* and *Data Size*:

- **Iterations**—the number of times Diagnostic Console measures Response Time during a test. Enter a value from 1 to 10 in this field. The default is 3. Choosing several iterations provides you with data that is more valid statistically.
- **Data Size**—the size in bytes of the data block to send between the selected endpoints. Enter a value from 1 byte to 32,000 bytes. The default is 100 bytes.

Response Time tests return three different time readings in milliseconds: minimum, average, and maximum. The times are broken out so that you can check for variations. Values of less than one millisecond are rounded up to one millisecond.

In theory, one-way response time can be calculated by halving the Response Time results. However, this calculation is sometimes inaccurate because the routes to and from the endpoints may differ. You can discover whether the routes are identical by running a Traceroute test.

Throughput

Throughput has one parameter option, *Data Size*, which accepts values from 1 kByte to 1,000 kBytes. The default value is 100 kBytes.

The Throughput test helps you gain information about your network's performance by comparing the operating speed of your network hardware with the actual throughput you achieve at a given moment. When you run Throughput tests using different values in the **Data Size** field, you can compare your network's handling of various data loads.

The Throughput test measures the time, in kbps or Mbps, it takes to send a certain quantity of data from Endpoint 1 to Endpoint 2 and receive a return acknowledgment.

Note Throughput units are expressed with abbreviations: an uppercase "K" represents 1,024; a lowercase "k" represents 1,000. Similarly, an uppercase "B" represents bytes; a lowercase "b" represents bits.

If you test Throughput on a network with plenty of bandwidth, you may wonder why the results can be low compared to the total available bandwidth. Throughput is intentionally designed to generate small, brief data flows so as not to swamp your network; it is limited to a single connection and sends no more than one MB of data.

Endpoint computer operating systems and protocol stacks can limit throughput; with today's computers it is difficult to get throughput greater than 100 Mbps with a single connection.

Streaming

Streaming tests emulate the behavior of applications that use streaming, such as voice over IP or video broadcasts. They send data without acknowledgments, using the connectionless protocols IPX or UDP. Packets are sent in one direction only, from Endpoint 1 to Endpoint 2.

The Streaming test uses two parameters options: *Data Rate* and *Duration*.

- **Data Rate** controls the rate at which streams of data are sent from Endpoint 1 to Endpoint 2. It indicates how much bandwidth your multimedia traffic might need and makes it easy for you to compare the speed of your network hardware with the actual data rate your network is achieving.

  You can choose the units, kbps or Mbps, that are appropriate for a selected application. Legitimate values range from 0.001 Mbps (1 kbps) to 1Mbps (1,000 kbps). The default settings are 50 kbps or 0.050 Mbps.

- **Duration** determines the total amount of time spent sending data from Endpoint 1 to Endpoint 2. Values can range from five seconds to 30 seconds. The default is 10 seconds.

The Streaming test sends 101-byte datagrams for a UDP test. Each datagram consists of a 64-byte payload, a 20-byte IP header, an 8-byte standard UDP header, and a 9-byte NetIQ endpoint header. For an IPX streaming test, the packets are 111 bytes because the IPX header size is 30 bytes.

When you run a Streaming test, the endpoints keep track of lost data (data not received by Endpoint 2). Lost data is shown as a percentage of data sent and as a value expressed in bytes. Lost data of less than 0.10% is not displayed.

In Streaming tests, lost data is often considerable. Data loss has three typical causes.

- The data rate may be higher than the maximum throughput potential, causing lost packets during transmission—check to make sure that you selected the correct units.
- The network may be congested.
- The network may be configured to give non-streaming traffic priority over streaming traffic, discarding datagram packets when the two compete for bandwidth.

Try running a Throughput test in the corresponding connection-oriented protocol for comparison. If your throughput is unexpectedly low, network congestion is the likely cause.

Traceroute

A Traceroute test describes the path or route that a packet takes between two endpoints in a network, detailing the sequence and duration of each hop. A “hop” is a jump from one router to another, or from an endpoint computer to a router. The test shows a maximum of 30 hops.

Endpoint 2 in a Traceroute test does not need to have NetIQ Endpoint software installed.

When you see asterisks (* *) in the data, traceroute data was unavailable for that hop. Data may be unavailable because a firewall is blocking the ICMP message, because the message timed out, or because connectivity was lost.

Standard Ping Test Panel

The Standard Ping Test panel displays either a chart or log that reports the results of a ping test. The ping test automatically sends and receives packets between the Console computer and the target computer. You cannot stop it.

The ping test sends a 60-byte packet every time the screen refreshes—that is, every time the Next Update bar restarts. This refresh interval is five times the Update Speed set in the **View** menu. You can see the exact interval between pings by reading the log.

The log shows the round trip time rounded to the nearest millisecond, except that round trip times of less than one msec are shown as "<1 msec."

A return packet that is not received within the refresh interval will not be recognized.

The chart scale is large, so you may not always see recognizable activity. However, when the test is successful, you will see a plot segment. Whenever the ping test fails, the graph will be missing a segment.

Firewalls

Firewalls are designed to prevent unauthorized access to or from a private network. See the following topics for more information about firewalls and the Network Connectivity plug-in.

- Endpoints and Firewalls
- Traceroute Tests and Firewalls
- Network Address Translation and Firewalls

Endpoints and Firewalls

If a firewall filters traffic on your network, you may have to take certain steps to run tests between endpoints. Firewalls located in either of the following two locations can prevent connectivity tests from completing:

- Between the Diagnostic Console host and Endpoint 1
- Between Endpoint 1 and Endpoint 2

Many types of firewalls will not allow connectivity tests to run without additional configuration. If the test fails, the connectivity program returns an error message after two minutes from the start of the test. Different types of tests use different ports. Thus, unless you have configured your firewall to open all defined ports, you may find that some tests between a given endpoint pair complete, while others do not.

However, because the connectivity tests use fixed port numbers to communicate with the endpoints, it is easy to configure your firewall to allow the test data flows. Keep a record of the test setup you had entered when a connectivity test failed to complete. The Network Connectivity plug-in uses different ports for tests that use different protocols. In addition, different ports are used for data that instructs Endpoint 1 which type of test to perform and how to perform it, for data that actually flows between the endpoint computers to test their connection, and for data informing the console what results the test returned.

When deciding which ports to open, keep in mind that test setup, streaming test results, and collecting CPU utilization always require a connection-oriented protocol.

The table below describes the data flows that may be affected and the corresponding port numbers used by the connectivity program that you may need to configure at your firewall:

Data Flow	Port Number Used
Console to Endpoint 1, test setup (TCP)	10115
Console to Endpoint 1, test setup (SPX)	10117
Endpoint 1 to Endpoint 2, test data (all protocols)	10113
Endpoint 2 to Endpoint 1, streaming test results (TCP), CPU utilization	10115
Endpoint 2 to Endpoint 1, streaming test results (SPX), CPU utilization	10117
Endpoint 1 to Console, test results (TCP, SPX)	10114

When a firewall is not configured to allow the connectivity test data to pass, you will typically see one of the following error messages, depending on where in the test the connection failed:

- **CHR0200**: The connection attempt timed out.
- **CHR0201**: The address is in a network that is unreachable.
- **CHR0204**: There is no remote program waiting to accept our sockets connection.
- **CHR0342**: The test failed to complete within two minutes and has been stopped.

Traceroute Tests and Firewalls

Traceroute depends on ICMP echo requests and replies. In order to run Traceroute tests across a firewall, ICMP echo requests and replies must be opened at the firewall. If your firewall is configured not to let ICMP echo requests into your network and Endpoint 1 is outside the firewall, Traceroute tests will fail. Endpoint 1 cannot send an ICMP echo request through the firewall.

However, you can configure your firewall to allow ICMP echo replies (rather than requests) into your network and let you run Traceroute tests by choosing as Endpoint 1 a computer inside the firewall. Do the following:

- Enable ICMP echo requests to pass from inside the firewall to outside the firewall.
- Enable ICMP echo replies to pass from outside the firewall to inside the firewall.

Opening ICMP echo requests from outside the firewall to the network inside the firewall jeopardizes network security, because it lets any application using the ICMP protocol enter your network behind the firewall.

Network Address Translation and Firewalls

Tests run for Throughput or Response Time with TCP or UDP through firewalls that perform network address translation (NAT) will fail if:

- the console is on the secure side of a firewall, *and*
- the test runs between Endpoint 1 on the unsecure side and Endpoint 2 on the secure side.

The test will time out two minutes after it starts. With the same configuration, however, and NAT disabled, tests will complete normally. You may see this behavior when attempting to run tests for Throughput or Response Time with TCP or UDP.

Chapter 13

Using the Network Performance Plug-in

The Network Performance plug-in provides a graphical representation of details about network traffic: utilization, Kbytes per second, packets per second, and average packet size in bytes.

To access the Network Performance plug-in, expand the Network Interface plug-in in the Navigation Pane.

The Network Performance plug-in is not supported for target computers that are running Windows NT 4.0.

See the following topics for even more information about the function of the Network Performance plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 89
- "Graphs" on page 90

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source and every five seconds when you use WMI as a data source. The refresh pulls in any data that has been collected since the last refresh. The data collection rate for the Network Performance plug-in is five times the refresh rate.

Graphs

The four graphs in the Network Performance plug-in represent the different network entities:

Graph	Description
Utilization	Displays the network traffic (bytes) as a percentage of the capability of the network connection.
Kbytes per Second	Displays the number of KBs transmitted, received, and total per second, depending on the tab you choose.
Packets per Second	Displays the number of packets transmitted, received, and total per second, depending on the tab you choose.
Average Packet Size (Bytes)	Displays the average packet size for packets received, packets sent, and total packets, depending on the tab you choose.

Chapter 14

Using the Network Interface Plug-in

The Network Interface plug-in provides a list of the target computer's network interfaces, as well as a detailed description of the configuration and protocols for each interface.

See the following topics for even more information about the function of the Network Interface plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 91
- "Listed Interfaces Table" on page 92
- "Information Table" on page 93
- "Routing Table" on page 94

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source and every five seconds when you use WMI as a data source. The refresh pulls in any data that has been collected since the last refresh. The data collection rate for the Network Interface plug-in is five times the refresh rate.

Listed Interfaces Table

The following table describes the fields of the Listed Interfaces table:

Field	Description
Description	Description of each network device associated with the target computer.
Service Name	Additional description.

Information Table

The following table describes the fields of the Information table. The contents of the table change as you select different interfaces in the Listed Interfaces table.

Field	Description
Item	List of TCP/IP, DHCP, DNS, WINS, and MAC parameters for the selection in the Listed Interface table. • **TCP/IP**—Transmission Control Protocol/Internet Protocol—a set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic. • **DHCP**—Dynamic Host Configuration Protocol—a TCP/IP service protocol that offers dynamic leased configuration of host IP addresses and distributes other configuration parameters to eligible network clients. DHCP provides safe, reliable, and simple TCP/IP network configuration, prevents address conflicts, and helps conserve the use of client IP addresses on the network. DHCP uses a client/server model in which the DHCP server maintains centralized management of IP addresses that are used on the network. DHCP-supporting clients can then request and obtain the lease of an IP address from a DHCP server as part of their network boot process. • **DNS**—Domain Name System—a hierarchical, distributed database that contains mappings of DNS domain names to various types of data, such as IP addresses. DNS allows you to locate computers and services by user-friendly names, and it also allows you to discover other information stored in the database • **MAC**—Media Access Control—the physical address of the network adapter. A MAC address is assigned by the manufacturer to uniquely identify the network adapter. • **WINS**—Windows Internet Name System—a software service that dynamically maps TCP/IP addresses to computer names (NetBIOS names). WINS allows users to access resources by name instead of requiring them to use IP addresses that are difficult to recognize and remember
Value	Value of each parameter.

Routing Table

The Routing Table lists the possible routes to certain network destinations and the metrics associated with those devices. To display the Routing Table for Windows XP or Server 2003 target computers, click the **Route Table** task link. This task is disabled for other operating systems.

Chapter 15

Using the Processes Plug-in

The Processes plug-in provides information about every process that is running on the target computer, such as average CPU, memory usage, virtual memory size, and process ID.

To access the Processes plug-in, expand the Windows plug-in in the Navigation Pane.

The Processes plug-in is *not* supported for target computers that are running Windows NT 4.0.

See the following topics for even more information about the function of the Processes plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 95
- "Processes Table" on page 96
- "Graphs" on page 97
- "Creating a Process" on page 97
- "Stopping a Process" on page 98

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source and every five seconds when you use WMI as a data source. The refresh pulls in any data that has been collected since the last refresh. The data collection rate for the Processes plug-in is twice the refresh rate.

Processes Table

The Processes table lists all of the running processes (instances of an application or service) for all users on the target computer.

Process	Description
Image Name	Name of the process.
PID	Unique identifier assigned to a process while it is running.
Avg CPU	Average percentage of CPU usage that the process has consumed. The average is calculated from the most recent 200 samples.
Last CPU	Most recently sampled value of percentage of CPU usage that the process has consumed.
MEM Usage	Number of pages currently resident in memory for the process, in MBytes.
VM Size	Amount of virtual memory, or address space, committed to the process.
Handles	Number of object handles in the process's object table.
Threads	Number of threads running in the process.
Uptime	Elapsed time since the process was last started.
Page Faults/sec	Number of times per second that data has to be retrieved from disk for the process because it was not found in memory.
IO Read Bytes/sec	Rate at which the process is reading bytes from I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os.
IO Write Bytes/sec	Rate at which the process is writing bytes to I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os.
IO Other Bytes/sec	Rate at which the process is issuing bytes to I/O operations that do not involve data such as control operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os.

Graphs

The Results Pane contains three graphs, which are described below. Each graph pertains to the process selected in the Processes table. The graphs change each time you highlight a new process. If you select **_Total** from the table, you will see the totals for all processes.

Process Total	Description
Processor Usage	Shows the CPU usage for the highlighted process, as listed in the Processes table under **Last CPU**.
Memory	Shows the memory usage for the highlighted process, as listed in the Processes table under **MEM Usage**. Note that both physical and virtual memory are plotted.
Count	Shows the thread and handle counts for the highlighted process, as listed in the Processes table under **Threads** and **Handles**.

Creating a Process

You use the **Create Process** task link to create, or launch, a process. This task is not available if you use AppManager as a data source.

To create a process:

1. Click **Create Process** to open the Create Process dialog box.
2. In the **Command line** field, enter the fully qualified path to the process, such as `C:\winnt\system32\notepad.exe`. If you do not enter a fully qualified path, and your path environment variable is extremely long, the Create Process task may not work.
3. In the **Working directory** field, enter the location in which to store any working files for the process, such as `C:\Documents and Settings\your name here\My Documents`.
4. Click **OK** to start the new process.

Any task that you create on a remote computer running Windows 2000 SP3, Windows XP, or Windows Server 2003 will not be created interactively. In other words, the task will be created without a user interface. If you walk over to that computer and look at the screen, your task will not show up on the screen, but it will appear in the process list of Task Manager. This behavior is different from Windows 2000 SP2 and earlier, which can create a process interactively (with a user interface).

Stopping a Process

To stop a process, highlight it in the Processes table and click the **End Process** task link. You will be prompted to confirm that you want to stop the process. This task is not available if you use AppManager as a data source.

Chapter 16

Using the Protocols Plug-in

The Protocols plug-in provides information about the protocols that Exchange uses: SMTP, MTA, MAPI, OWA, POP3, and IMAP4. For each protocol, you can determine whether it is up or down, and view charts that display metrics such as queue length and number of messages sent.

To access the Protocols plug-in, expand the Exchange plug-in in the Navigation Pane.

See the following topics for even more information about the function of the Protocols plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 99
- "Overview Panels" on page 100
- "IMAP4 Charts" on page 101
- "MAPI Charts" on page 101
- "MTA Charts" on page 102
- "OWA Charts" on page 102
- "POP3 Charts" on page 103
- "SMTP Charts" on page 104

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source, pulling in any data that has been collected since the last refresh. The data collection rate for the Protocols plug-in is three times the refresh rate, or every 30 seconds.

Overview Panels

The Overview is the default view of the Protocols plug-in. It displays separate panels that provide summary information about each protocol.

Panel	Description
SMTP	Displays the number of requests in the Local and Remote queues, and presents the number of messages sent and received, per second. This figure is an aggregate of data across all virtual servers.
MTA	Displays the number of requests in the Queue and the Work Queue, the number of MTA messages per second, and the number of messages sent and received, per second.
MAPI	Displays the number of RPC requests and the number of RPC operations per second.
OWA	Displays the number of requests in the Client Out and Store Out queues, and presents the number of message opens and sends, per second.
POP3	Displays the number of requests in the Client Out and Store Out queues, and presents the number of commands per second. This figure is an aggregate of data across all virtual servers.
IMAP4	Displays the number of requests in the Client Out and Store Out queues, and presents the number of commands per second. This figure is an aggregate of data across all virtual servers.

IMAP4 Charts

Internet Message Access Protocol (IMAP) is a protocol for retrieving e-mail messages. The latest version, IMAP4, is similar to POP3 but supports some additional features. Click the **IMAP4** task link to display charts that highlight information related to the IMAP4 protocol:

Chart Name	Description
Client Out Queue Length	Length of queue from client to store
Store Out Queue Length	Length of queue from store to client
Commands	Number of commands per second, which includes commands such as APPEND, EXAMINE, LIST, LSUB, SELECT SUBSCRIBE, and UNSUBSCRIBE

If IMAP4 has been disabled on the target Exchange server, then no data will display in the IMAP4 charts of the Protocols plug-in. If you restart the services, you need to restart Diagnostic Console before you will see any IMAP4 data in the charts.

MAPI Charts

Messaging Application Programming Interface (MAPI) is a system built into Microsoft Windows that enables different e-mail applications to work together to distribute mail. As long as both applications are MAPI-enabled, they can share mail messages with each other.

Click the **MAPI** task link to display charts that highlight information related to the MAPI protocol:

Chart Name	Description
RPC Requests	Number of client requests that are being processed by the Information Store
RPC Operations/sec	Rate at which RPC operations occur

MTA Charts

The Message Transfer Agent (MTA) is the program responsible for receiving incoming e-mails and delivering the messages to individual users. The MTA transfers messages between computers. Hidden from the average user, it is responsible for routing messages to their proper destinations. MTAs receive messages from both MUAs (mail user agents) and other MTAs, although single-user computers more often retrieve mail messages using POP3.

Click the **MTA** task link to display charts that highlight information related to the MTA protocol:

Chart Name	Description
Queue Length	Number of outstanding messages queued for transfer to the entity
Work Queue Length	Number of outstanding messages in the Work Queue, which indicates the number of messages not yet processed to completion by the MTA
Receive Messages	Rate at which messages are received from the connected entity
Send Messages	Rate at which messages are sent to the connected entity
Messages	Rate at which messages are processed

OWA Charts

Outlook Web Access (OWA) provides access to messages, calendars, contacts, tasks, and public folders from any computer with an Internet connection and a Web browser.

Click the **OWA** task link to display charts that highlight information related to the OWA protocol:

Chart Name	Description
Client Out Queue Length	Length of queue from client to store
Store Out Queue Length	Length of queue from store to client
Message Opens	Rate per second at which messages are opened
Message Sends	Rate per second at which messages are sent

POP3 Charts

Post Office Protocol (POP) is a protocol used to retrieve e-mail from a mail server. Most e-mail applications (sometimes called an e-mail client) use the POP protocol, although some can use the newer IMAP4 (Internet Message Access Protocol).

There are two versions of POP. The first, called *POP2*, became a standard in the mid-1980s and requires SMTP to send messages. The newer version, *POP3*, can be used with or without SMTP. Click the **POP3** task link to display charts that highlight information related to the POP3 protocol:

Chart Name	Description
Client Out Queue Length	Length of queue from client to store
Store Out Queue Length	Length of queue from store to client
Commands	Number of commands per second, which includes commands such as DEL, LAST, LIST, NOOP, RSET, and STAT

If POP3 has been disabled on the target Exchange server, then no data will display in the POP3 charts of the Protocols plug-in. If you restart the services, you need to restart Diagnostic Console before you will see any POP3 data in the charts.

SMTP Charts

Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP3 or IMAP4. In addition, SMTP is generally used to send messages from a mail client to a mail server.

Click the **SMTP** task link to display charts that highlight information related to the SMTP protocol:

Chart Name	Description
Local Queue Length	Number of requests in the Local queue
Remote Queue Length	Number of requests in the Remote queue
Messages Received	Rate at which inbound messages are being received
Messages Sent	Rate at which outbound messages are being sent.

Chapter 17

Using the Replication Plug-in

The Replication plug-in provides information about the Active Directory server functions related to partition replication on the target computer. Monitored functions include partitions, replication information, connection information, and NTDS performance. See the following topics for even more information about the function of the Replication plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 105
- "Replication Partitions Tab" on page 106
- "Connection Objects Tab" on page 109

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source, pulling in any data that has been collected since the last refresh. The collection rate for the Replication plug-in is every 15 seconds, with the exception of the data for the Insufficient Topology section of the Replication Partitions chart. That collection rate is every 30 seconds.

Replication Partitions Tab

The following topics explain the contents of the charts on the **Replications Partitions** tab.

- Replication Information Chart
- NTDS Performance Charts
- Replication Partitions chart

Replication Information Chart

The Replication Information chart displays the following information:

Item	Description
Ignore GC Failures	Windows 2000 Domain Controllers must be able to contact a Global Catalog server in order to evaluate universal group memberships during client logon. When enabled, this setting disables the requirement for contacting the Global Catalog server, but has significant security implications. For more information, see Microsoft KB article Q241789.
KCC Disabled (Intersite)	Indicates whether intersite topology generation, which is managed by the Knowledge Consistency Checker, has been disabled.
KCC Disabled (Intrasite)	Indicates whether intrasite topology generation, which is managed by the Knowledge Consistency Checker, has been disabled.
No GC Logon Enabled	Indicates whether logon is allowed without using a Global Catalog server.
Tombstone Lifetime	An object that is deleted is flagged and moved to the hidden Deleted Objects container in the partition in which the object was deleted. The deleted object remains in the Deleted Objects container for the tombstone lifetime.

NTDS Performance Charts

Four charts in the **Replication Partitions** tab display metrics relating to NTDS performance:

Item	Description
Replication Queue	Number of replication operations on the directory that are queued for this server but not yet performed.
Scheme Mismatches	Number of sync requests made to neighbors that failed because their schema were out of sync.
Inbound Replication Bytes	Three data streams: • Intersite, the compressed size in bytes of inbound compressed replication data. • Intrasite, the number of bytes replicated in that were not compressed at the source. • Total, the total number of bytes replicated in (sum of the number of bytes never compressed and the number of compressed bytes).
Outbound Replication Bytes	Three data streams: • Intersite, the compressed size in bytes of outbound compressed replication data. • Intrasite, the number of bytes replicated out that were not compressed at the source. • Total, the total number of bytes replicated in (sum of the number of bytes never compressed and the number of compressed bytes).

Replication Partitions chart

The Replication Partition chart displays the following information about replication partitions:

Item	Description
Health	Indicates the health of replication for a partition between the Domain Controller being diagnosed and the partner Domain Controller: • Green indicates good health • Yellow indicates that the number of consecutive failures is greater than two • Red indicates that one or more of the following is true: - Last successful replication was at least two weeks ago - Insufficient topology - No partner - Replication failed due to lingering objects
Partner	Name of a partner Domain Controller that replicates changes to the Domain Controller that you are diagnosing.
Partner Site	Name of the site in which the partner resides.
Last Success	Date and time of the last successful replication cycle. Formatted in the time zone of the Diagnostic Console computer that you are using, which is not necessarily the time zone of the target computer.
Consecutive Failures	Number of consecutive failed replication attempts that have occurred since the last successful replication attempt.
Insufficient Topology	Indicates whether the KCC (Knowledge Consistency Checker) has insufficient topology information to generate the necessary connection objects for replication.
Lingering Objects	Indicates whether lingering objects exist. Lingering objects (also known as zombies) can occur if a Domain Controller, unable to replicate changes for an entire tombstone lifetime, connects for replication after object deletions have occurred.

Connection Objects Tab

The table on the **Connection Objects** tab displays all connection objects between the monitored Domain Controller and other Domain Controllers with which it has established connections.

Column Name	Explanation
Enabled	Indicates whether the connection object is enabled.
Name	An auto-generated title, unless the connection is manually created, in which case the connection object name is displayed.
Server	Name of the server that has a connection object with the monitored computer.
Site	Associated site of the server referenced in the connection object.
Direction	Direction of the connection object between the monitored computer and the specified server.
Transport	Network protocol used by the connection object.
Changed	Date on which the connection object was last modified.
Created	Date on which the connection object was created.

Chapter 18

Using the Security Subsystem Plug-in

The Security Subsystem plug-in provides information about authentications for kerberos, NTLM, and the Key Distribution Center. See the following topics for even more information about the function of the Security Subsystem plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 111
- "Kerberos Authentications/sec Chart" on page 111
- "NTLM Authentications/sec Chart" on page 112
- "Key Distribution Center Charts" on page 112

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source, pulling in any data that has been collected since the last refresh. The data collection rate for the Security Subsystem plug-in is also every 10 seconds.

Kerberos Authentications/sec Chart

Kerberos is an Internet standard authentication protocol, the default protocol among Windows computers (2000, 2003, XP, etc.) within an Active Directory forest. The Kerberos Authentications/sec chart displays the number of Kerberos authentications serviced per second by the Domain Controller.

NTLM Authentications/sec Chart

Windows NT LAN Manager (NTLM) is the Secure Sockets Layer protocol for Windows NT. The NTLM Authentications/sec chart displays the number of NTLM authentications serviced per second by the Domain Controller.

Key Distribution Center Charts

The Key Distribution Center (KDC) is a network service that supplies ticket-granting tickets (TGT) and service tickets to users on the network. KDC provides two services: the *Authentication Service* and the *Ticket Granting Service*.

The Authentication Service provides the initial authentication of the user on the network and provides the users with a TGT. Users who request access to a network service supply a TGT to the Ticket Granting Service. The Ticket Granting Service then provides users with a service ticket that allows authentication with the target network service. In a Windows 2000 environment, the KDC service is run at all Domain Controllers.

The KDC AS Requests/sec chart displays the number of Authentication Service requests serviced per second by the KDC.

The KDC TGS Requests/sec chart displays the number of Ticket Granting Service requests serviced per second by the KDC.

Chapter 19

Using the Services Plug-in

The Services plug-in provides information about every service that is running on the target computer, such as a description, the status, and the startup type.

To access the Services plug-in, expand the Windows plug-in in the Navigation Pane.

The Services plug-in is *not* supported for target computers that are running Windows NT 4.0.

See the following topics for even more information about the function of the Services plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 114
- "Services Table" on page 114
- "Service Properties" on page 115
- "Starting/Restarting Services" on page 115
- "Stopping Services" on page 116
- "Pausing/Resuming Services" on page 116
- "Creating Services" on page 116
- "Deleting Services" on page 116

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source and every five seconds when you use WMI as a data source. The refresh pulls in any data that has been collected since the last refresh. The data collection rate for the Services plug-in is 100 times the base rate, or every 1,000 or 500 seconds, depending on your data source.

Services Table

The Services table lists all of the services that are running on the target computer. The data in the table is the same as the data found in the Services window, which you can view by clicking **Start > Settings > Control Panel > Administrative Tools > Services**.

If you double-click a service in the table, you will open a Properties dialog box for the service. Most of the information in this dialog box is read-only. However, if the service is stopped, you can change its Startup Type or enter startup parameters.

The following table describes the fields in the Services table:

Item	Description
Name	Display name of the service.
Description	Can be a considerably more detailed description, depending on the version of Windows the computer is running. When diagnosing Windows 2000, the Description is a repeat of the Name. Microsoft is aware of this problem and has fixed it in Windows XP and 2003 Servers, where you see the full description.
Status	Status of the service, such as Running, Stopped, Paused, etc.
Startup Type	Automatic, Manual, or Disabled. If the Startup Type is Disabled, you will not be able to start the service until you have changed it to Automatic or Manual.
Logon As	Logon account required to start or stop this service, or alter its properties. You cannot change this from the Services plug-in. However, you can change it by opening the Services window at **Start > Settings > Control Panel > Administrative Tools > Services**.

You can stop, start, create, delete, pause, or resume the services that appear in the list. Not all tasks are applicable to every service; those that are appear in the Tasks Pane when you click on a service in the Services table.

If you make a change to a service, such as running one of the tasks in the Tasks Pane, changing a service by means of **Start > Settings > Control Panel > Administrative Tools > Services**, or changing a service by means of the command line, you might expect to see an immediate change of the service's status in the Services table. However, changes to the Services table are dependent upon the refresh rate for the Services plug-in, as well as the amount of time it takes for the agent to return data to the AppManager repository and then to Diagnostic Console.

Service Properties

Select a service and then click **Service Properties** to open the Services Properties dialog box. From this dialog box, you can view a subset of the information that you get from **Start > Programs > Administrative Tools > Services** on the target computer. The Service Properties dialog box indicates the status of the selected service, the startup type, the executable path, and any dependencies.

Starting/Restarting Services

If a service is not running/running, the **Start Service/Restart Service** link is displayed in the Tasks pane.

- To *restart* a service that is currently running, highlight it in the Services table and click **Restart Service**.
- To start a service that is not running, highlight it in the Services table and click **Start Service**.

If you highlight a service that is not running, the **Restart Service** task does not display in the Tasks Pane.

Stopping Services

To stop a service, highlight it in the Services table and click **Stop Service**. You will *not* be prompted to verify that you want to stop the service. If you highlight a service that is not running, **Stop Service** does not appear in the Tasks Pane.

Pausing/Resuming Services

Some services allow you to pause them as an alternative to stopping and restarting them. If you highlight such a service when it is running, a **Pause Service** task is displayed. When you click this task, the service is paused and the **Pause Service** task is replaced by a **Resume Service** task. Clicking the **Resume Service** task resumes the service and toggles back to the **Pause Service** task. This task is not available if you use AppManager as a data source.

Creating Services

Use the **Create Service** task link to create a service using the Create Service dialog box. Make the appropriate entries and then click **OK**. This task is not available if you use AppManager as a data source.

Deleting Services

To delete a service, highlight it in the Services table and click the **Delete Service** task link. You will be prompted to confirm that you want to delete the service. This task is not available if you use AppManager as a data source.

Chapter 20

Using the Shutdown Plug-in

The Shutdown plug-in provides information related to the shutdown conditions of the target computer, such as shutdown and startup time, the elapsed amount of downtime, the percentage of time the target computer was available, and whether the shutdown was planned.

See the following topics for even more information about the function of the Shutdown plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 117
- "Shutdown Table" on page 118
- "Summary Panel" on page 118
- "Availability Pie Chart" on page 118
- "Restarting and Shutting Down a Computer" on page 119

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source and every five seconds when you use WMI as a data source. The refresh pulls in any data that has been collected since the last refresh. The data collection rate for the Shutdown plug-in is 2,000 times the refresh rate, or every 20,000 or 10,000 seconds, depending on your data source.

Shutdown Table

The Shutdown table lists all the shutdowns and restarts of the target computer. This information comes from the Windows Event Log, so every shutdown included in the log is shown. Clearing the event log will empty this table.

Item	Description
Shutdown Time	Time of shutdown
Downtime	Elapsed time until next boot
Startup Time	Time of boot
Planned	Was shutdown planned?

The Shutdown plug-in displays only planned shutdown and startup cycles for workstations. However, the plug-in displays both expected and unexpected shutdowns for servers.

Summary Panel

The Summary panel shows the date and time of last reboot, the overall elapsed time, the overall uptime, and the overall downtime since the event log was last cleared.

Availability Pie Chart

The Availability pie chart displays the percentage of up and down time for the target computer.

Restarting and Shutting Down a Computer

Click the **Restart Computer** task link to restart a target computer.

Click the **Shutdown Computer** task link to shut down a target computer.

Neither task is available if you use AppManager as a data source.

Chapter 21

Using the Summary Plug-in

The Summary plug-in provides an overall view of the health of the target computer, displaying information gathered from all of the other plug-ins. See the following topics for even more information about the function of the Summary plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 121
- "Windows Table" on page 122
- "Processes Graph" on page 122
- "Memory Graph" on page 122
- "CPU Graph" on page 123

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source and every five seconds when you use WMI as a data source. The refresh pulls in any data that has been collected since the last refresh. The data collection rate for the Summary plug-in is twice the refresh rate.

Windows Table

The Windows plug-in is the source for all of the data in the Windows table:

Item	Description
Operating System Name	Name of the Windows operating system that is in use.
Version	Version number of the operating system.
Service Pack Version	Version number of the latest service pack in use.
Up Time	Amount of time that has elapsed time since the operating system was last started.
System Directory	Complete path of the Windows system directory.

Processes Graph

The Processes plug-in provides all of the data in the Processes graph, which plots the percentage of CPU usage for each of the top three processes for the target computer.

Memory Graph

The Memory plug-in provides all of the data in the Memory graph, which plots the following information:

Plotted Quantity	Description
Total Faults	Average number of pages faulted per second. This value is measured in number of pages faulted per second because only one page is faulted in each fault operation, therefore this figure is also equal to the total number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (those for which the faulted page is found elsewhere in physical memory). Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Plotted Quantity	Description
Transitions	Measured per second, the number of page faults that are resolved by recovering pages that were being used by another process sharing the page, or were on the modified page list or the standby list, or were being written to disk at the time of the page fault. The pages were recovered without additional disk activity. Transition faults are counted in numbers of faults; because only one page is faulted in each operation, it is also equal to the number of pages faulted.
Disk Reads	Measured per second, the number of pages that are read from disk to resolve hard page faults. Hard page faults occur when a process refers to a page in virtual memory that is not in its working set or elsewhere in physical memory, and must be retrieved from disk. When a page is faulted, the system tries to read multiple contiguous pages into memory to maximize the benefit of the read operation.
Disk Writes	Measured per second, the number of pages that are written to disk to free up space in physical memory. Pages are written back to disk only if they are changed in physical memory, so they are likely to hold data, not code. A high rate of pages output might indicate a memory shortage. Windows writes more pages back to disk to free up space when physical memory is in short supply. This counter shows the number of pages, and can be compared to other counts of pages, without conversion.

CPU Graph

The CPU plug-in provides all of the data in the CPU graph, which plots the following information:

Plotted Quantity	Description
User	Percentage of processor busy time in “User” mode—this mode is used for applications, environment subsystems, and integral subsystems.
Privileged	Percentage of processor busy time in ”Privileged” mode—this mode is used for operating system components and hardware-manipulating drivers.
Total	Total percentage of all processor busy time.

Chapter 22

Using the System Plug-in

The System plug-in provides information regarding the target computer: computer system, operating system, main board, and BIOS. See the following topics for even more information about the function of the System plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 125
- "System Table" on page 126

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source and every five seconds when you use WMI as a data source. The refresh pulls in any data that has been collected since the last refresh. The collection rate for the System plug-in is 10 times the refresh rate.

System Table

The Results Pane contains one table that is divided into four sections:

- Computer System Section
- Operating System Section
- Main Board Section
- BIOS Section

For some target computers, data you expect to see in the tables may be incomplete, or even missing entirely, because the Windows Management Information (WMI) service on that computer did not return the data for those topics.

For example, the System plug-in might not show any information under "Main Board" for some computer systems.

Computer System Section

The following table describes the fields in the Computer System section:

Item	Description
Computer Name	Name of the target computer.
Domain	Name of the domain to which the computer belongs.
DNS Name	Name of the computer used by the Domain Name Service.
Description	String describing the system.
Type	Basic architecture.
Manufacturer	Name of the computer manufacturer.
Model	Target computer's product name assigned by the manufacturer.
Primary Owner	Primary user of the target computer.

Operating System Section

The following table describes the fields in the Operating System section:

Item	Description
Caption	Short description of the operating system.
Version	Version number of the operating system.
Windows Directory	Directory where the operating system is installed.
Local Time Zone (console)	Time zone of the console computer.
Local Time (console)	Time as reported by the console computer.
Remote Time Zone	Time zone of the target computer.
Remote Time	Time as reported by the target computer.
Remote Time Delta	Time difference between the target computer and the local computer.
Remote Time to Local Time	Time value as reported by the target computer, converted to the time value of the local computer.

Main Board Section

The following table describes the fields in the Main Board section:

Item	Description
Description	Description of the object.
Manufacturer	Manufacturer of the base board.
Product	Base board part number defined by the manufacturer.
Serial Number	Product serial number.
Version	Version of the physical element.

BIOS Section

The following table describes the fields in the BIOS section:

Item	Description
Name	Name used to identify this software element.
Version	Version of the BIOS. This string is created by the BIOS manufacturer.
Manufacturer	Manufacturer of this software element.
Serial Number	Assigned serial number of this software element.
SMBIOSBIOS Version	BIOS version as reported by SMBIOS.
Status	Current status of the object. Various operational and non-operational statuses can be defined. Operational statuses are "OK", "Degraded" and "Pred Fail.”

Chapter 23

Using the SYSVOL Plug-in

The System Volume (SYSVOL) is a shared directory that stores the server copy of the domain's public files that must be shared for common access and replication throughout a domain. The SYSVOL plug-in displays SYSVOL response time and statistics.

See the following topics for even more information about the function of the SYSVOL plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 129
- "SYSVOL Status Chart" on page 130
- "FRS CPU Usage Chart" on page 130
- "SYSVOL Response Time Chart" on page 130

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source, pulling in any data that has been collected since the last refresh. The collection rate for the SYSVOL plug-in is every 15 seconds.

SYSVOL Status Chart

The Status chart in the Results Pane displays the following information:

Item	Description
Status	Status, up or down, that indicates whether the SYSVOL share exists and can be connected to locally using `\\localhost\SYSVOL`.
Location	Filespec of the SYSVOL folder.
Size	Total space, in MB, used by the files in the SYSVOL directory.
# of Files	Number of files in the SYSVOL directory.

FRS CPU Usage Chart

The FRS CPU Usage chart indicates the amount of processor time used by the File Replication Service.

SYSVOL Response Time Chart

The SYSVOL Response Time chart displays in milliseconds the amount of time it takes to perform a local connection to `\\localhost\SYSVOL` on the Domain Controller that you are diagnosing.

Chapter 24

Using the Windows Plug-in

The Windows plug-in provides detailed information about the Windows operating system and environment on the target computer. Detailed information includes build number, operating system name, users, and service pack version.

See the following topics for even more information about the function of the Windows plug-in and the data in the Results Pane.

- "Data Collection Rate" on page 131
- "Operating System Tab" on page 132
- "Hotfixes Tab" on page 133
- "Environment Tab" on page 134

Data Collection Rate

The Diagnostic Console interface refreshes itself every 10 seconds when you use AppManager as a data source and every five seconds when you use WMI as a data source. The refresh pulls in any data that has been collected since the last refresh. The data collection rate for the Windows plug-in is 10 times the refresh rate.

Operating System Tab

If you are diagnosing an NT 4.0 computer, the Windows plug-in displays only a sub-set of the information that is displayed when you are diagnosing a computer that is running Windows 2000 or later.

Click the **Operating System** tab to display the table. The fields in this table vary with the system. The following is an example:

Item	Description
Build Number	Build number of the operating system.
Build Type	Type of build used for the operating system. Examples are retail build and checked build.
Local Time (console)	Operating system's local date and time of day.
Local Time Zone (console)	Time zone of the local computer.
Locale	Locale of the target computer.
Manufacturer	Name of the operating system's manufacturer.
Number of Users	Number of user sessions for which the operating system is currently storing state information.
Operating System Name	Name of the operating system. Serves as key of the operating system instance.
Organization	Registered user's company name.
Registered User	Name of the registered user of the operating system.
Remote Time	Time as reported by the target computer.
Remote Time Delta	Time difference between the target computer and the local computer.
Remote Time to Local Time	Time value as reported by the target computer, converted to the time zone of the local computer.
Remote Time Zone	Time zone of the target computer.
Serial Number	Operating system product serial identification number.
Service Pack Version	Latest service pack installed.
Status	Current status of the object. Various operational and non-operational statuses can be defined. Operational statuses are "OK", "Degraded" and "Pred Fail" (for Predicted Failure).

Item	Description
System Device	Physical disk partition where the operating system is installed.
System Directory	Directory where the operating system is loaded.
System Startup Time	Time when the operating system was last booted. Not available for Windows 2000.
Up Time	Elapsed time since last boot.
Version	Version number of the operating system.

Hotfixes Tab

The **Hotfixes** tab identifies the current operating system and which, if any, service pack is installed. In addition, the tab includes a table that discusses the following information, which is taken from entries in the Windows registry:

Item	Description
Product	Name of the product targeted by the hotfix, such as Windows 2000, DataAccess, or Windows Media Player. **Note** Product information is not available if you chose WMI as your data source.
Hotfix ID	Identification number of a hotfix.
Description	Description of the hotfix.
Installed By	User ID of the person who installed the hotfix.
Installed Date	Date the hotfix was installed. **Note** The installation date is not available if you chose WMI as your data source.

Environment Tab

Click the **Environment** tab to reveal the table. The fields in this table vary with the system being monitored. The following is an example:

User	Item	Description
<Local User1>	TEMP	Alias for path to TEMP directory for user number 1.
<Local User1>	TMP	Alias for path to TMP directory for user number 1 (Same as TEMP directory in this case).
<Local User2>	TEMP	Alias for path to TEMP directory for user number 2.
<Local User2>	TMP	Alias for path to TMP directory for user number 2 (Same as TEMP directory in this case).
.....repeat last two entries as needed up to “Number of Users.”		
SYSTEM	ComSpec	Alias for opening a command window.
SYSTEM	NUMBER_OF_ PROCESSORS	Number of processors.
SYSTEM	OS	Operating system.
SYSTEM	OS2LibPath	Path to system32\os2\dll.
SYSTEM	Path	Path variable.
SYSTEM	PATHEXT	Extensions that can be run from the command line.
SYSTEM	PROCESSOR_ ARCHITECTURE	Basic processor architecture (family).
SYSTEM	PROCESSOR_ IDENTIFIER	More detail about the processor architecture.
SYSTEM	PROCESSOR_ LEVEL	More detail about the processor architecture.
SYSTEM	PROCESSOR_ REVISION	More detail about the processor architecture.
SYSTEM	TEMP	Alias for path to TEMP directory.
SYSTEM	TMP	Alias for path to TMP directory.
SYSTEM	windir	Alias for path to Windows directory.

Appendix A

Troubleshooting

The topics in this section present a few of the steps you can take to troubleshoot some data collection-related problems.

Charts Show More Sample Points Than Expected

Symptom: When you use AppManager as a data source, charts show more sample points at startup than you expect.

Possible cause: You have more than one instance of Diagnostic Console simultaneously targeting the same computer. The AppManager agent that runs on the target computer stores a number of recent samples for reporting to the database. A second diagnosis on the same computer

could receive these samples when it queries for its first sampling interval.

Resolution: None, except to realize that the extra data points are current samples, not erroneous data.

Data Does Not Display for a Long Time

Symptom: It takes a long time for Diagnostic Console to display any data after you start it.

Possible causes: The target computer's System event log is very large, and it takes a long time for WMI queries to search through the log for "shutdown" events. Or, the target computer has high CPU utilization while the WMI search is underway.

Resolution: Frequently clean up your event log in order to reduce the size. The smaller the event log, the quicker WMI can search through it.

Network delays between the target, the QDB, and the Console computer also may contribute to data delays.

Data Does Not Display in POP3 or IMAP4 Charts

Symptom: Data does not display in the POP3 or IMAP 4 charts of the Protocols plug-in.

Possible cause: Most likely, the services have been disabled on the target Exchange server.

Resolution: Restart the services. You need to restart Diagnostic Console before you will see any POP3 or IMAP4 data in the charts.

Data is Not Reported by Target Computer or Connectivity Tests

Symptom: Data is not displayed for a given plug-in or network connectivity tests do not provide results.

Possible cause: The appropriate counters on the target computer may be missing or corrupted.

Resolution: For an explanation and resolution, refer to: **http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q275659**.

Diagnostic Console Will Not Shut Down

Symptom: Diagnostic Console remains open or generates an error message after you have attempted to shut it down using standard methods.

Cause: The connection between the Console computer and the WMI target computer has been severed.

Resolution: Maintain the connection between the Console computer and the WMI target computer. If the connection is lost, the threads that query for data using WMI get stuck in the WMI libraries.

Expired Network Interface Configuration Appears

Symptom: A defunct/expired network interface configuration appears in the Network Interfaces plug-in.

Possible cause: You may be running Diagnostic Console against VMWare targets. The VMWare hardware emulation may be returning false information through the WMI.

Resolution: None.

Memory Capacity Values are Inconsistent

Symptom: Physical memory capacity values differ within charts in the Memory plug-in.

Possible cause: You may be running Diagnostic Console against VMWare targets. The VMWare hardware emulation may be returning false information through the WMI.

Resolution: None.

Memory Usage Increases

Symptom: Occasional increases in memory usage that appear to be memory leaks.

Possible cause: Diagnostic Console is built using the Microsoft.NET Framework, which supplies advanced memory management capabilities. From time to time, you might notice what appear to be memory leaks. However, these performance characteristics are actually the normal result of the .NET Framework's garbage collection features and do not represent incorrect behavior.

Resolution: None. For more information, see **http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q318263**.

Note If you are running Diagnostic Console against VMWare targets, you may find that the figure indicated in this field does not match the amount of physical memory indicated in the Virtual Memory Usage table. The VMWare hardware emulation may be returning false information through WMI.

Percent Measurements Exceed 100

Symptom: You run `perfmon.exe` on a target computer and notice percentage measurements of disk usage for which the values exceed 100 percent.

Cause: Microsoft discusses the reason for this inaccuracy in Microsoft Knowledge Base Article Q310067, which you can find at: **http://support.microsoft.com/default.aspx?scid=KB;EN-US;310067**.

Resolution: Diagnostic Console normalizes these values, in the manner recommended by Microsoft, so that the Console values to not exceed 100 percent.

Results Seem Inconsistent

Symptom: You notice small differences between data collected by WMI and data collected from Performance Counters.

Possible causes: There may be small differences between data obtained by different means, owing to:

- different measurement technique, or
- different instant of sampling, or
- different sampling intervals.

Resolution: None. For example, if you obtain data from `perfmon.exe` and compare it with Diagnostic Console data, you may see slight differences. It is virtually impossible for you to sample at the same instant that Diagnostic Console refreshes.

Stop/Start/Reset Services Task is Unsuccessful

Symptom: You are unable to perform the Stop/Start/Reset Service task from the Services plug-in. Diagnostic Console may freeze for up to 90 seconds, then refresh, but the service that you selected has not been stopped, started, or reset.

Cause: A bug exists in the AppManager 6.0 version of the NTAdmin_RestartService Knowledge Script. Diagnostic Console invokes this script when you run the Stop/Start/Reset Services task.

Resolution: Contact NetIQ Solutions Support for a patch for the Knowledge Script: **www.netiq.com/support**.

Appendix B

Using License Manager

The topics in this section describe how to view and update Diagnostic Console license information.

- About Diagnostic Console License Keys
- What If You Do Not Know Your License Key Number?
- Viewing License Information
- Updating an Expired License
- Adding a License Key
- Requesting Licensing Information
- Importing License Keys From a File

About Diagnostic Console License Keys

Diagnostic Console comes with an evaluation license key that allows unlimited use for a specific number of days from the date you install the Diagnostic Console. When you purchase Diagnostic Console, you are given a permanent 15-digit license key with no expiration date.

During the Diagnostic Console installation, you are prompted to enter your license key. However, you can use the default evaluation key, which is automatically entered, and update the license information after you complete the installation process. See "Adding a License Key" on page 143 for more information.

What If You Do Not Know Your License Key Number?

The person installing Diagnostic Console might not be the person who purchased it for your organization and, therefore, might not know the license key number.

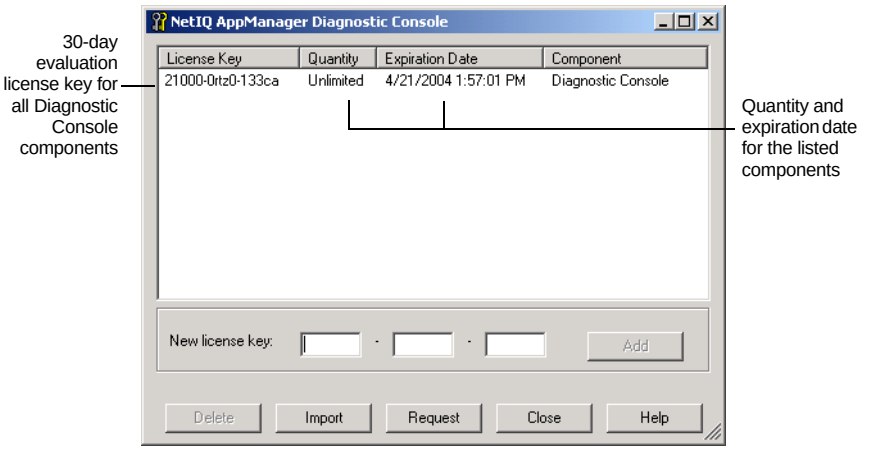
To obtain a license key number for Diagnostic Console, send an e-mail to **licensekey@netiq.com**. Include:

- Your first and last name
- The e-mail address to which you want the license sent
- A telephone number where you can be reached in case there is a problem fulfilling your request
- The host name or IP address for your Diagnostic Console server

To purchase Diagnostic Console, contact your authorized NetIQ representative.

Viewing License Information

From Diagnostic Console, click **Help > License Manager** to view license information.



Updating an Expired License

If you have installed an evaluation copy of the Diagnostic Console, you should note the expiration date. The expiration date is displayed in the License Manager and in the About the Diagnostic Console dialog box.

If the Diagnostic Console evaluation period has expired, click **Update license** when prompted, and then enter a new license key. For more information, see the next section.

Adding a License Key

As you convert from an evaluation copy, you need to update the Diagnostic Console license information.

You do not need to re-install Diagnostic Console to add a new license key. If you purchase Diagnostic Console after the evaluation period, you only need to add the new permanent license key.

To add a license key:

1. From Diagnostic Console, click **Help > License Manager**.
2. In the **New license key** fields, enter the 15-digit license key you were given. Use the format `nnnnn-nnnnn-nnnnn`.
3. Click **Add**. The component and expiration date appear in the list.
4. Click **Close**.

Requesting Licensing Information

You can request licenses by calling our toll-free number or by sending an e-mail request.

To request licenses by e-mail:

1. From Diagnostic Console, click **Help > License Manager**.
2. Click **Request**.

3 Check **Send NetIQ licensing information from your repository** to include information about your current licenses with your request.

For	Type
Your name	Your first and last name.
Your email address	The e-mail address to which you want licenses sent.
Your phone number	A telephone number where you can be reached in case there is a problem fulfilling your request.
SMTP computer name	The name of your SMTP server. You can enter the host name or the IP address for the server.

4 Click **Request Licenses**. The License Manager sends your request to NetIQ support. You will receive an e-mail response to your request.

Importing License Keys From a File

If you have more than one or two license keys or need to update multiple license keys, you may want to import the information from a file rather than entering the keys manually. When you purchase Diagnostic Console or request new licenses, you also receive a text file that contains all of the license keys.

To import the license keys from a text file:

1 From Diagnostic Console, click **Help > License Manager**.

2 Click **Import**.

3 Locate the `license.txt` file you received from NetIQ.

4 Click **Open**. The license key information is imported and displayed in the License Manager.