Abstract

This chapter describes the installation process of NetIQ AppManager and discusses customizations that were made specifically for the Microsoft® Systems Architecture (MSA) Internet Data Center (IDC) environment. The content in this chapter provides detailed steps about the installation, initial sizing, agent deployment, agent configuration, and rules customization.
<table>
<thead>
<tr>
<th>CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>INTRODUCTION</strong> ..........................1</td>
</tr>
<tr>
<td>System Prerequisites ..........................1</td>
</tr>
<tr>
<td><strong>INSTALLING COMPONENTS</strong> .................2</td>
</tr>
<tr>
<td>Installing the Repository and Management Server ..................2</td>
</tr>
<tr>
<td>Configuring Security on the Management Server ..................5</td>
</tr>
<tr>
<td><strong>AGENT DEPLOYMENT</strong> ........................6</td>
</tr>
<tr>
<td>Agent Install Preconfiguration ..................6</td>
</tr>
<tr>
<td>Creating Staging Directory ..................6</td>
</tr>
<tr>
<td>Operator Console ..................6</td>
</tr>
<tr>
<td>Modifying Default Install Job ..................6</td>
</tr>
<tr>
<td>Standard Server Installation ..................7</td>
</tr>
<tr>
<td>Adding Computers to the Console ..............8</td>
</tr>
<tr>
<td>Troubleshooting Installation Problems ..............9</td>
</tr>
<tr>
<td>Cluster Server ..................10</td>
</tr>
<tr>
<td>Manually Installed Agents ..................11</td>
</tr>
<tr>
<td><strong>APPMANAGER CONFIGURATION</strong> ..............13</td>
</tr>
<tr>
<td>Management Job Deployment ..................13</td>
</tr>
<tr>
<td>Active Directory ..................13</td>
</tr>
<tr>
<td>IIS Servers ..................14</td>
</tr>
<tr>
<td>SQL Servers ..................15</td>
</tr>
<tr>
<td>All Servers ..................17</td>
</tr>
<tr>
<td><strong>MANAGING APPMANAGER</strong> ..................18</td>
</tr>
<tr>
<td><strong>OPERATIONS MANAGER CONNECTOR</strong> ..............19</td>
</tr>
<tr>
<td><strong>SUMMARY</strong> ............................21</td>
</tr>
<tr>
<td>More Information ............................21</td>
</tr>
</tbody>
</table>
The NetIQ AppManager Suite is a comprehensive solution for managing and monitoring the performance and availability of distributed Microsoft® Windows® 2000 operating systems, applications, and hardware. AppManager allows system administrators to monitor computer resources and application configuration, check for potential system problems, initiate responsive actions, and gather performance data for real-time and historical reporting.

This document focuses on detailing the complete installation procedure for AppManager and how it is integrated into the base Internet Data Center architecture. The modifications to the default configuration are intended to be a template for real-world implementations of this architecture.

**System Prerequisites**

So that the monitoring and alerting solution can be implemented into the Internet Data Center environment, a fully configured, installed, and working base architecture must be in place. Additional prerequisites:

- All servers must be installed, configured, and networked.
- All designated management servers should have the base operating systems installed.
- The Dell OpenManage software must be installed on all servers.
- Microsoft SQL Server™ 2000 must be installed on the management database server (MSA04).

**Note**  SQL Server 2000 can be installed with all defaults, except the default security configuration. SQL Server must be configured for mixed-mode security, not native mode. Make this change during installation. If SQL Server is already installed, this option can be verified and/or changed by right-clicking the SQL Server in SQL Server Enterprise Manager, clicking Properties, and then clicking the Security tab.

After these prerequisites have been met, the implementation of the monitoring and alerting solution can proceed.
This section details the installation of the NetIQ AppManager components on the management servers within the Internet Data Center environment.

All components were installed on a single computer within the Internet Data Center environment. This step is best for lab environments where it is preferable to minimize the number of computers dedicated to monitoring tools. The NetIQ AppManager console can be installed on any computer. The agents can either be installed with the compact disc, or through the AMAdmin_AgentInstall Knowledge Script. For installations of more than 200 managed servers, you should install the management server and the repository on separate servers. Installations of more than 550 servers may need additional repositories. The following sections describe a procedure that installs AppManager in a manner that is applicable to the Internet Data Center environment.

Installing the Repository and Management Server

Generating the encryption key:

A NetIQ Encryption utility that enables you to work with your key files is available. The NetIQ Encryption utility application is a command-line application and is in either of the following locations on your AppManager compact disc:

- NetIQ\AM4.0\i386\rpckey.exe
- NetIQ\contrib\utilities\i386\rpckey.exe

To use the utility, from the command line, type:

`rpckey -generate path to file -pwd password`

For example:

`rpckey -generate c:\temp\key1.txt -pwd mykey`

Run this utility before proceeding with installation. It is important to remember the password and file location until after installation of the central components is complete. You may want to write this information down and then destroy it after installation.

To install the repository and management server:

1. Run Setup.exe from the AppManager installation directory (compact disc or `\file server\UNC\NetIQ\AppManager\`).
2. Click Begin Setup.
3. On the Welcome screen, click Next.
4. In the Select the option you want box, click Install Products, and then click Next.
5. Select an installation directory or accept the default directory, and then click **Next**.

6. In the **Products** box, click **AppManager**, and then click **Next**.

7. In the **Components** box, click all the listed options, and then click **Next**.

8. Read and accept the license agreement, and then click **Next**.

9. Select the appropriate license. If this is a trial or lab installation, make no changes to use the Trial license. If this is a production installation, you should have received a license key from NetIQ. Use the purchase license if you have one. You can add a purchase license later if you need to do so. Click **Next** when you are done.

10. Provide your name and organization information, and then click **Next**.

11. Accept the default for **SQL Server Name** and **Repository Name**, and then click **Next**.

12. Type the NetIQ SQL Server Systems Administrator (SA) password in the **SQL SA password** box. The default SQL NetIQ password is **netiq**. Change the NetIQ password, and then click **Next**.

   **Note** Accepting the default for this is not recommended as it is a security risk, just as a blank password is on the Windows Administrator account.

13. Accept the defaults for **Data file name** and **Log file name**.

14. Increase the **Data Device Size**. (Sizing information is available from NetIQ.)

15. Increase the **Log Device Size** to be 25 percent of the data device.

16. Move the data and log device paths onto physically separate drives or even separate controllers, if possible. See the SQL Server documentation for data and log device best practices. Click **Next**.

17. Accept the default account configuration (Local System) for **Management Server Configuration**, and then click **Next**.

18. At the **Management Server Security** screen, click **Maximum security to encrypt all communication**, and then click **Next**.

19. Enter the information for the RPC key file you created by using the rpckey.exe utility at the beginning of this section, type the password, and then click **Next**.

20. Accept the default ports, and then click **Next**.
21. In the Port Configuration for UNIX Servers dialog box ensure the following selections are set and then click **Next**:  
- Do **not** bind a port for Managing UNIX servers

22. Accept the default (all options selected) for **Applications to Monitor**, and then click **Next**.

23. Select the **Enable Report Agent** and **Perform Discovery** check boxes, and then click **Next**.

24. Accept the default **Local Repository Path**, and then click **Next**.

25. Enter the **MGMT_ACCT1** service account information, and then click **Next**.  
**Note** The option, **Agent service runs as LocalSystem account**, tells the installation process how to set up the service account of the Managed Client. The Managed Client on the central Management Server may be responsible for installing agents (Managed Clients) remotely onto other servers. Because the agent can be installed directly from the compact disc, some customers may decide never to use the remote-install option. In this case, this option can remain selected and the Managed Client on the Management Server will run as local system. In nearly all cases, some agents will be installed remotely from the Management Server by using the NetIQ AppManager console. It is, therefore, strongly recommended that the NetIQ_Managed Client (agent) service running on the central management server be provided with a service account powerful enough to install files and initiate services on target computers. This power requires at least local administrator authority on the target server. Domain administrator or enterprise administrator rights are not required for agent installation. The Internet Data Center lab installation used a domain administrator account for this service.

26. In the **Agent Configuration** dialog box, type the SA password for SQL Server on the management server (MSA04), and then click **Next**.

27. Clear the **Distributed Event Console** and **Developer Console Utilities** check boxes, and then click **Next**.

28. If prompted, click **Yes** to stop Microsoft Internet Information Service (IIS).

29. A warning that AppManager requires disk performance counters to be started is displayed. Click **OK**.

30. When setup is complete, click **OK**.

31. Click **No** to register this installation later.

32. Click **OK** to confirm.
This completes the installation of the AppManager central components.

**Configuring Security on the Management Server**
Before continuing with installation and configuration, the NetIQ account must be granted access to the repository.

**To give the NetIQ account access to the repository:**

1. Click **Start**, point to **Programs**, click **NetIQ**, click **AppManager**, click **Tools & Utilities**, and then click **Security Manager**.
2. Log on to the repository by using SA credentials.
3. On the **Security** menu, click **User setup**.
4. In the left pane, click **dbo**, and then click **Add**.
5. Click **Close** to complete the operation.
6. Exit **Security Manager**.
This section details how to configure the AppManager console, set up a staging directory, and install AppManager agents.

**Agent Install Preconfiguration**
This section discusses the preconfiguration requirements for AppManager agents.

**Creating Staging Directory**
The AppManager agent installation requires a share location for the installation components. In this case, we will put the files on MSA04.

To create the AppManager agent installation share:
1. Create a folder on the server MSA04 called **NQInstall**.
2. Share this folder out so it can be accessed through the network.
3. Copy the files from the i386 folder on the compact disc or from file share into the **NQInstall** folder.
4. Copy the encryption key file created earlier into the **NQInstall** folder. All servers must be able to access this file at agent-installation time.

**Operator Console**
Refer to the AppManager Users Guide for an introduction to the console. This document assumes some basic knowledge of the console.

**Modifying Default Install Job**
The standard agent installation Knowledge Script should be modified for convenience of installation and maintenance. In this section, we will modify the defaults so the parameters, such as user name and password, do not have to be repeated every time the Knowledge Script is run.

To modify the defaults:
1. On the database server (MSA04), click **Start**, point to **Programs**, click **NetIQ**, click **AppManager**, and then click **Operator Console**.
2. Log on to the Operator console by using the NetIQ account credentials created earlier, and then click **Logon**.
3. In the **Knowledge Script Pane**, click the **AMAdmin** tab.
4. Double-click **AgentInstall40**.

**Note** Knowledge Scripts are named in the form **Tab_ScriptName**. The AgentInstall Knowledge Script on the **AMAdmin** tab is **AMAdmin_AgentInstall40**. **NT_LogicalDiskSpace** is the **LogicalDiskSpace** object found on the **NT** tab.
5. Click the **Values** tab and then make the changes defined in the following table.

<table>
<thead>
<tr>
<th>Field name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User for temporary service on target</td>
<td>MGMT service account, such as MGMT_ACCT1</td>
</tr>
<tr>
<td>Password for temporary service on target</td>
<td>Password for MGMT_ACCT1 account</td>
</tr>
<tr>
<td>Domain of temporary service on target</td>
<td><em>domain name</em></td>
</tr>
<tr>
<td>UNC Path to Installation File</td>
<td><code>\\MSA04\NQInstall</code> (created earlier)</td>
</tr>
<tr>
<td>Management Server Name</td>
<td>MSA04</td>
</tr>
<tr>
<td>Select Security Level</td>
<td>Maximum Security</td>
</tr>
<tr>
<td>Maximum Security Password</td>
<td>Enter the password used with the <code>rpckey.exe</code> utility</td>
</tr>
<tr>
<td>Maximum Security Key File</td>
<td><code>\\MSA04\NQInstall\key file name</code></td>
</tr>
<tr>
<td>List of Authorized Management Servers</td>
<td>MSA04</td>
</tr>
<tr>
<td>Install SQL managed object</td>
<td>Y</td>
</tr>
<tr>
<td>Install Dell OpenManage managed object</td>
<td>Y</td>
</tr>
<tr>
<td>Install IIS managed object</td>
<td>Y</td>
</tr>
<tr>
<td>Install Cluster server managed object</td>
<td>Y</td>
</tr>
<tr>
<td>Install Transaction Server managed object</td>
<td>Y</td>
</tr>
<tr>
<td>Install WMI managed object</td>
<td>Y</td>
</tr>
<tr>
<td>Install WTS Server managed object</td>
<td>Y</td>
</tr>
<tr>
<td>Install Site server managed object</td>
<td>Y</td>
</tr>
<tr>
<td>Install MS Active Directory managed object</td>
<td>Y</td>
</tr>
<tr>
<td>Install Web Services managed object</td>
<td>Y</td>
</tr>
</tbody>
</table>

6. Click **OK**.

**Standard Server Installation**

All servers, including the special servers described in the following sections (cluster servers and Microsoft Active Directory® directory service servers), should be processed through the standard server installation steps. Special server consideration is *in addition to* standard server deployment operations.
Adding Computers to the Console
The first step in adding computers is establishing logical groups. Groups can be added, removed, or renamed later; their members modified; and new overlapping logical groupings established. For now, create only the basic groups and populate their members.

To create groups:

1. If it is not already open, launch the AppManager Operator console (click the Start button, point to Programs, click NetIQ, click AppManager, and then click Operator Console).
2. Right-click Master, and then click Create Server Group.
3. In the Group Name box, type AD Servers, and then click OK.
4. In the tree view, expand Master, right-click AD Servers, and then click Add Computer.
5. Type the server names MSADC1 and MSADC2, separated by commas in the dialog box. Ensure that the Discover Windows NT objects automatically check box is selected. Click OK.
6. Repeat the previous steps to create the following groups with the following members:
   - DNS Servers: MSADNS1 & MSADNS2
   - IIS Servers: MSAWEB1 - MSAWEB33
   - Management Servers: MSA01 & MSA04
   - SQL Servers: MSADNODE1 & MSADNODE2
   - Staging Servers: MSAAPP
7. Right-click the Management Servers group, and then click Properties.
8. In the left pane, select the MSA04 server checkbox, click Add, and then click OK.
9. Drag the AMAdmin_AgentInstall40 Knowledge Script from the Knowledge Script Pane (right center) into Master in the tree view (top-left pane). All servers should go green as long as you hold down the left mouse button.
10. When you let go of the mouse button, you will be presented with a configuration dialog for the job. Move to the Objects tab. Expand Management Servers, and then clear the MSA04 object.
11. All the other default values for the Knowledge Scripts are correct. The values were configured earlier. Click OK. The job will appear in the list pane at the bottom.
Note Numerous errors are likely to pop up in the Events tab of the list pane. An event indicating that a job was aborted requires investigation (check to see if the server can be reached, if there is free disk space, if the administrative shares, such as c$, are still available, and so on). Any error messages of the type "Agent Install partially complete," community-string errors, or errors indicating that IIS was not detected on a server (errno=-2) can be closed and deleted. Success events can also be closed and deleted.

12. To close an alert, select the check box on the Events tab of the list pane.

13. After an alert is closed, it can be deleted to keep the list pane from becoming cluttered. Select closed events by clicking and dragging, or using SHIFT+click to select items. Right-click the selected items and then click Delete Event or press the DELETE key.

14. Click the Jobs tab of the list pane. Any jobs with a Stopped status can be deleted.

Troubleshooting Installation Problems
If the previous steps are followed carefully and the Internet Data Center network and security settings have not yet been applied, reinstalling the agent can fix most problems. If an agent installation has already been attempted on a particular server, it is common that locked files can prevent agent reinstallation.

If an agent reinstallation results in one of the following:

- Agent computer is displayed as grayed-out in the console.
- Agent computer is shown in the console with no details (that is, the computer node in the tree view cannot be expanded to show items such as Disks, Services, or other resources).
- The NetIQMC and NetIQCCM services are missing from the agent computer, but the HKLM\Software\NetIQ registry key is present and/or c:\program files\NetIQ files are present.
- There is an event for that agent for AgentInstall40 in the AppManager console indicating that the installation failed.

The following steps should be used to resolve the problem:

1. On the agent computer, in the folder C:\Program Files\NetIQ\AppManager\Bin\ rename the file NetIQNTLog.exe to NetIQNTLog_Old.exe.

2. Reinstall the agent by using the AMADMIN_AgentInstall40 Knowledge Script as described in the previous section.
**AppManager Hotfix**

Once agent is installed on all servers you will need to apply hotfix NETIQKB3013 on servers that have Dell OpenManage software. After this you can run Discovery_Dell KS.

**Cluster Server**

The following information is based on the Knowledge Base article numbered NKB0506 available on the NetIQ Web site. The clustered Microsoft SQL Server computers require some additional setup. The discovery job run on MSADNODE 1 and MSADNODE 2 during agent install may not discover SQL Server on the inactive node. First check to see if SQL Server is detected on both nodes. Do this by checking to see that the SQL Server object appears in the details of both nodes. In the tree view (top left), expand both SQL Server computer nodes and then check for SQL Server.

If SQL Server is missing from the inactive node, take the following steps:

1. Fail the cluster over, making the inactive node active (see Microsoft Cluster Administrator online help for details).
2. Drag **Discover_SQL** into the now-active node. Accept all the defaults and click **OK**.
3. Verify that the SQL Server object exists in the now-active node after the job is complete.

After SQL Server has been discovered on both nodes, it is important to set resource dependencies for SQL Server monitoring jobs. The following steps provide an example of setting up resource-dependent, disk free-space monitoring.

**To set resource dependencies from SQL Server monitoring jobs:**

1. In the AppManager Operator console, locate the NT_LogicalDiskSpace knowledge script in the Knowledge Script Pane. Right-click the Knowledge Script, and then click **Copy Knowledge Script**.
2. Name the copy **SQL_LogicalDiskSpace** and then click **OK**.
3. You should now see SQL_LogicalDiskSpace in the SQL tab of the Knowledge Script pane.
4. Drag and drop the AMADMIN_SetResDependency knowledge script into the **SQL Servers** group. Do not click **OK** yet.
5. On the **Values** tab, define the **Knowledge Script Category** to SQL. Set the **Required available resources** to a shared resource such as Z:, then click **OK** to run the job one time.
5. Test the resource dependency by dropping a SQL Knowledge Script (that is SQL_LogicalDiskSpace) into the SQL Server group (accept the default values, but change the schedule to run every five minutes). If SQL Server is active on MSADNODE 2, the job on MSADNODE 2 should display a status of running-active in the console. The job on MSADNODE 1 should have a status of running-inactive. Test other non-SQL Server Knowledge Scripts (such as NT_MemUtil). These scripts should appear as active on both nodes.

6. Finally, you can test failover by moving the SQL Server group to the other node. When the next scheduled iteration of the SQL Server job occurs, the status of each node should be reversed.

**Manually Installed Agents**
Servers not in a domain, servers with limited connectivity to MSA04, or servers without connectivity to the installation software share point must be installed manually.

1. Log in to the server to be monitored using the local administrator account.

2. Copy the encryption key file (created when the AppManager Management Server was installed) to a directory on the local machine.

3. Run setup.exe in the AppManager installation source directory or CD.

4. Click **Begin Setup**.

5. At the Welcome screen, click **Next**.

6. At the **Install AppManager** screen accept the default (Install Products) and click **Next**.

7. At the **Choose Destination Location** screen, click **Next**.

8. At the **NetIQ Product** screen, accept the default (AppManager) and click **Next**.

9. At the **NetIQ AppManager Components** screen, accept the default (AppManager Management Agent), and click **Next**.

10. At the first **NetIQ AppManager Agent Configuration** screen, select all components and click **Next**.

11. At the next **NetIQ AppManager Agent Configuration** screen, accept the defaults and click **Next**.

12. At the next **NetIQ AppManager Agent Configuration** screen, accept the default repository path and click **Next**.
13. At the next NetIQ AppManager Agent Configuration screen, select Use local system account. Click Next.

14. At the Managed Client Security screen, select Maximum security to encrypt all communication and click Next.

15. Fill in details for maximum security configuration, including the path for the encryption key file copied in step 1. Click Next.

16. At the next NetIQ AppManager Agent Configuration screen, enter the name of the NetIQ Management Server (e.g. MSA04). If the Management Server cannot be pinged from the monitored server, enter the IP Address of the Management Server. Click Next.

17. If prompted to enable disk performance counters, follow the instructions and click OK.

18. Repeat steps 1-17 for each machine that requires that an agent be manually installed.

Once installation is complete, the new agent will show up as a machine in the Treeview pane in the AppManager console. It will be in the root of the tree, but should be moved into an appropriate group.
Now you can configure AppManager to be a valuable monitoring tool for the Internet Data Center environment. At this point in the process, console and back-end components are installed and configured, the agents are deployed, and the repository is loaded with Knowledge Scripts that provide value. However, as yet, none are running on servers (except for the resource-dependent monitoring on the clustered SQL Server computers).

**Management Job Deployment**

The setup procedures have already shown detailed information on the mechanics of dropping and configuring jobs. This section will reduce the how-to detail and instead describe the jobs and configurations to be deployed.

**Note** When naming a Knowledge Script, the part before the underscore denotes the tab name, and the part after the underscore denotes the job name. For instance, CLIENT_URLConnectivity would be the URLConnectivity job found in the CLIENT tab.

**Active Directory**

The following steps detail the creation of Active Directory jobs configured for the Microsoft System Architecture Internet Data Center environment.

**To configure the Active Directory jobs:**

1. Drop **AD_Authentications** into the **Active Directory** group. Change the schedule to run every 15 minutes. Change the **Collect Data** value to **y**.
2. Drop **AD_CacheHitRate** into the **Active Directory** group. Change the schedule to run every 15 minutes. Change the **Collect Data** value to **y**.
3. Drop **AD_ConnectivityObject** into computer **MSA04**. Change the **Collect Data** value to **y**.
4. Drop **AD_GlobalCatalogHealth** into the **Active Directory** group. Accept all defaults.
5. Drop **AD_ResponseTime** into the **Active Directory** group. Change the schedule to run every 15 minutes. Change value **LDAP path** to LDAP://YourWebSite.com/rootDSE. Change the **Collect Data** value to **y**.

**Note** The following steps verify that the correct IP address is returned by the Domain Name System (DNS) service for critical servers. The IP addresses, server names, and cluster virtual names stated below assume that your deployment of the Internet Data Center exactly mirrors the deployment described in this guide. If you have made changes to the names and IP addresses for your installation, please update the values below.
6. Drop \texttt{NETSERVICES\_DNSHealthCheck} into the \textit{Active Directory} group. Change the schedule to run every 15 minutes. Change the hostname for name resolution value to MSADC1.MSAIDC.EMC.com. Change the hostip that should be returned value to 192.168.13.20.

7. Again drop \texttt{NETSERVICES\_DNSHealthCheck} into the \textit{Active Directory} group. Change the schedule to run every 15 minutes. Change the hostname for name resolution value to MSADC2.MSAIDC.EMC.com. Change the hostip that should be returned value to 192.168.13.21. Change the Auto-Start Service value to \texttt{n}.

8. For a third time, drop \texttt{NETSERVICES\_DNSHealthCheck} into the \textit{Active Directory} group. Change schedule to run every 15 minutes. Change hostname for name resolution value to MSADSQL1.MSAIDC.EMC.com. Change the hostip that should be returned value to 192.168.12.214. Change the Auto-Start Service value to \texttt{n}.

\textbf{IIS Servers}

This section shows the jobs that were configured for the IIS servers.

\textbf{To configure jobs for the IIS computers:}

1. Drop \texttt{IIS\_ASPQueueBusy} into the \textit{IIS Servers} group. Accept all the defaults for schedule and values.

2. Drop \texttt{IIS\_ASPRestRequestError} into the \textit{IIS Servers} group. Accept all the defaults for schedule and values.

3. Drop \texttt{IIS\_ASPThroughput} into the \textit{IIS Servers} group. Change the schedule to run every 10 minutes.

4. Drop \texttt{IIS\_HealthCheck} into the \textit{IIS Servers} group. Change the schedule to run every 10 minutes.

5. Drop \texttt{IIS\_HTTPBytes} into the \textit{IIS Servers} group. Change the \textit{Collect Data} value to \texttt{y}.

6. Drop \texttt{IIS\_HTTPNotFound} into the \textit{IIS Servers} group. Accept all the defaults for schedule and values.

7. Drop \texttt{CLIENT\_URLConnectivity} into computer \texttt{MSA01}. Change the \textit{URLs to Monitor} value to the internal URL of your Web site for initial testing.

\textbf{Note}  The \texttt{CLIENT\_URLConnectivity} KS makes an HTTP connection to the Web addresses listed in \textit{URLs to Monitor}. MSA01 will not be able to see the external Web site addresses because of the network topology and security. Enter the physical name of a Web server (for example, http://iis01/default.html) to monitor the default.html page. Optionally, enter multiple URLs, separated by commas (for example, http://iis01/default.html,http://iis02/default.html) to monitor multiple servers. This way, a notification of failure from AppManager will indicate that a server is not serving pages, and will indicate which server is having
problems. Additional monitoring is possible if the KS is dropped onto a server that can see the external network, such as a DNS advertising server, and is configured to monitor the external web site URL (for example, http://www.northwindtraders.com). Because the routing will send the http request outside the IDC environment, it is a test of both the Web servers and the Web load balancing. Failure of this KS would indicate that customers cannot reach the Web page in question.

**SQL Servers**

Because many SQL Server application monitoring Knowledge Scripts require SA or some SQL Server user privilege, SQL Server security must be configured before starting SQL Server monitoring. This is only required for SQL Server running in Mixed Security Mode. If SQL Server is running in Native (Windows) Authentication mode, the AppManager agent services (netiqmc and netiqccm) on the SQL Server computers must be modified to run as a service account with access to the database.

**To configure SQL Server security for Knowledge Scripts:**

1. Determine which account should be used for AppManager access to SQL Server. If an account other than SA is used, security and accessibility should be verified with SQL Server Query Analyzer prior to configuring AppManager security.

2. On MSA04, start the **NetIQ Security Manager**. (Click **Start**, point to **Programs**, click **NetIQ**, click **AppManager**, click **Tools & Utilities**, and then click **Security Manager**.)

3. Log on by using the SA credentials.

4. Expand **Computers** in the tree view and then click **MSADNODE1**.

5. Switch to the **SQL** tab in the right pane.

6. Select the **clustered virtual server name** from the drop-down list. **Note** If there is more than one virtual server name, repeat these steps for each virtual server.

7. Type the **SA password** and then click **Logon**.

8. The log ons configured on the SQL Servers are available in the details pane. Select the check boxes next to the log ons that apply to the account you want to use. If you just want to use the SA password, make no changes.

9. Right-click each log on that will be used by the monitoring scripts and select **Password**.

10. Enter the password for the selected account and click **OK**.
11. Click **Apply**. AppManager now has the password in an encrypted store for use by the SQL Server application Knowledge Scripts.

12. Repeat steps 4-11 for **MSADNODE2**.

13. Close **Security Manager**.

The next step is to start running application jobs for monitoring the SQL Server databases.

**To run application jobs for monitoring SQL Server databases:**

1. Drop **SQL_Accessibility** into the **SQL Servers** group. Change the **Collect Data** value to **y**. Change the **SQL Login** value to the log on you want to use (SA is fine for this). Change the **Database Name** value to any databases you want to monitor. Leaving this field blank will cause the Knowledge Script to attempt to connect to every database on the server. It is recommended that this field be left blank, because it is assumed that all non-essential databases (such as Northwind) will be removed from the SQL Server cluster.

2. Drop **SQL_CacheHitRatio** into the **SQL Servers** group. Change the **Collect Data** value to **y**.

3. Drop **SQL_DBSpace** into the **SQL Servers** group. Change the **Collect Data** value to **y**. Change the **Available Space** value to **5**.

4. Drop **SQL_NearMaxConnect** into the **SQL Servers** group. Accept the defaults for schedule and values.

5. Drop **SQL_ProcessingTime** into the SQL Servers group. Accept the default schedule and values. Change **SQL Login** to **SA**.
   
   **Note** You can run any SQL script, time the SQL Server response, and graph the data by using the SQL_ProcessingTime Knowledge Script.

6. Drop **MSCS_GroupDown** into the **SQL Servers** group. Accept the default schedule and values.
   
   **Note** Both SQL Servers should show a green right arrow when you hold down the mouse button and drag the MSCS Knowledge Scripts into the SQL Servers group. If only one server has this green right arrow, drag DISCOVERY_MSCS into the server that is not illuminated.

7. Drop **MSCS_NetInterfaceDown** into the **SQL Servers** group. Accept the default schedule and values.

8. Drop **MSCS_NodeDown** into the **SQL Servers** group. Accept the default schedule and values.

9. Drop **MSCS_ResourceDown** into the **SQL Servers** group. Accept the default schedule and values.
All Servers
This section shows how the jobs were applied to all servers.

To apply jobs to all servers:

1. Drop **NT_DNSConnectivity** into **Master**. Change the **Remote DNS host name** to **msadc1**. Change the **DNS domain name** to **msaidc.emc.com**. On the **Objects** tab, clear the **Active Directory** group.

2. Drop **NT_ServiceDown** into **Master**. Change the schedule to run every 15 minutes. Change the **Services, separated by comma w/ no space** to value * (asterisk).

3. Drop **NT_TopCpuProcs** into **Master**. Change the **Collect Data** value to **y**. Change the **Total CPU usage** value to **190**.

4. Drop **NT_TopMemoryProcs** into **Master**. Change the **Collect Data** value to **y**. Change the **Event** value to **n**. Total CPU usage value should be between 0 and 100.
MANAGING APPMANAGER

The use of views, the graph control, and management of AppManager alerts are beyond the scope of this document. For information on using the console, adding and modifying Knowledge Scripts, graphing data, and managing alerts and events, see the AppManager Users Guide.
This section looks at the steps required to install the Microsoft Operations Manager connector.

**To install the Operations Manager Connector:**

1. Download the XMP Connector for NetIQ AppManager from the NetIQ AppManager Web site or from the NetIQ AppManager compact disc.

2. Ensure that you have installed an AppManager agent on the Operations Manager and that you have also installed an Operations Manager agent on the AppManager management server.


4. Run Setup.exe in the XMP Connector for NetIQ AppManager directory.

5. On the Welcome Screen, click Next.

6. Accept the default Program Manager Group, and then click Next.

7. Click Next to allow the installer to copy files.

8. Click Next to set up the connector.

9. Type the name of the DCAM server (MSA01) in the Consolidator Host box. Clear the Enable Incoming MOM Events check box, and then click Next to proceed.

10. Accept the default (all options checked) and then click Next.

11. Accept the severity level defaults and then click Finish.

12. Click Yes to restart the AppManager Management Service.

13. Click OK twice.

   **Note** If you get an error that the Management Server could not be started, start the NetIQMS service manually from the Services control in Computer Management.

14. Go to the Operations Manager or Security Manager Consolidator (MSA01).

15. Run Setup.exe in the XMP Connector for NetIQ AppManager directory.


17. At the Update XMP screen, select Yes to import the Connector XMP. Click Next.

18. In the Start Installation dialog box, click Next.
19. Click **Finish**.

20. When the installer is finished, open the Operations Manager management console.

21. Move to Microsoft Operations Manager (Default), click **Rules**, and then click **Processing Rule Groups**. Expand **NetIQ XMP – Extended Management Pack Solutions** and verify that there is an XMP Connector for NetIQ AppManager group.

22. Click **Configuration**, right-click **Agent Managers**, and then click **Scan All Managed Computers**.

23. Click **OK**.

Watch for alerts from running AppManager jobs. Events in the **Events** tab will also show up in the Operations Manager **All Open Alerts** view. It may take 5 to 20 minutes for alerts to start showing up from AppManager, and only new alerts will be forwarded.
The dependence of Web sites on networks and uninterrupted services puts considerable pressure on operations staff to ensure ongoing service availability, health, and performance. A well-designed management system is critical to the successful management and operation of large business sites. The deployment tools allow smooth and rapid growth of Web sites. Powerful monitoring and troubleshooting tools allow operations staff to quickly deal with problems of components and services before business is affected. The management system itself must be highly available to ensure continuous operations. By installing and configuring NetIQ AppManager into the base Internet Data Center architecture, you are able to take the necessary steps to ensure your environment is up and running.

More Information

For general information about the NetIQ AppManager product, refer to the NetIQ Web site at:
http://www.netiq.com