Clustering the NetIQ® Security Manager™ Log Archive

Technical Reference

August 31, 2007

Contents

Security Manager version 6.0 introduces the *log archive server* component for storing log data, which dramatically improves log storage space and performance. Previous versions of Security Manager stored log data in a Microsoft SQL Server database, which provided clustering capability. While the log archive server does not support clustering out-of-the-box, you can manually configure the log archive on an active/passive Windows Server 2003 cluster. A clustered log archive service provides high availability of your log archive data.

This *Technical Reference* provides information about clustering the log archive service using a Windows Server 2003 cluster.

Overview

Security Manager version 6.0 introduces the *log archive server* component for storing log data, which dramatically improves log storage space and performance. Previous versions of Security Manager stored log data in a Microsoft SQL Server database, which provided clustering capability. While the log archive server does not support clustering out-of-the-box, you can manually configure the log archive on an active/passive Windows Server 2003 cluster. A clustered log archive service provides high availability of your log archive data.

Supported Products

The Security Manager log archive server component supports Windows Server 2003 clusters.

Requirements

The following table lists additional requirements for a clustered log archive server. For more information about log archive server requirements, see the *Installation Guide for NetIQ Security Manager*.

Category	Requirements
Operating System	Microsoft Windows Server 2003.
Software	• Microsoft Windows Server 2003 Clustering Services • Microsoft Message Queuing (MSMQ) 3.0

Implementation Overview

The following table provides an overview of tasks to cluster the log archive service.

☑	Steps	See Section
☐	**1.** Configure a Windows Server 2003 cluster.	"Configuring a Windows 2003 Cluster with MSMQ"
☐	**2.** Install the log archive server component on both cluster nodes.	"Installing Log Archive Servers on the Cluster Nodes"
☐	**3.** Configure the cluster to fail over the log archive service.	"Configuring the Cluster to Support the Log Archive"
☐	**4.** Configure central computers to communicate with the log archive cluster.	"Configuring Central Computers to Use the Log Archive Cluster"
☐	**5.** Verifying a successful installation.	"Verifying a Successful Log Archive Cluster Installation"

Configuring a Windows 2003 Cluster with MSMQ

To support a clustered log archive, you first create a functioning two-node Windows Server 2003 cluster with MSMQ 3.0 installed. This document does not explain how to create a Windows Server 2003 cluster, but there are many Microsoft resources available.

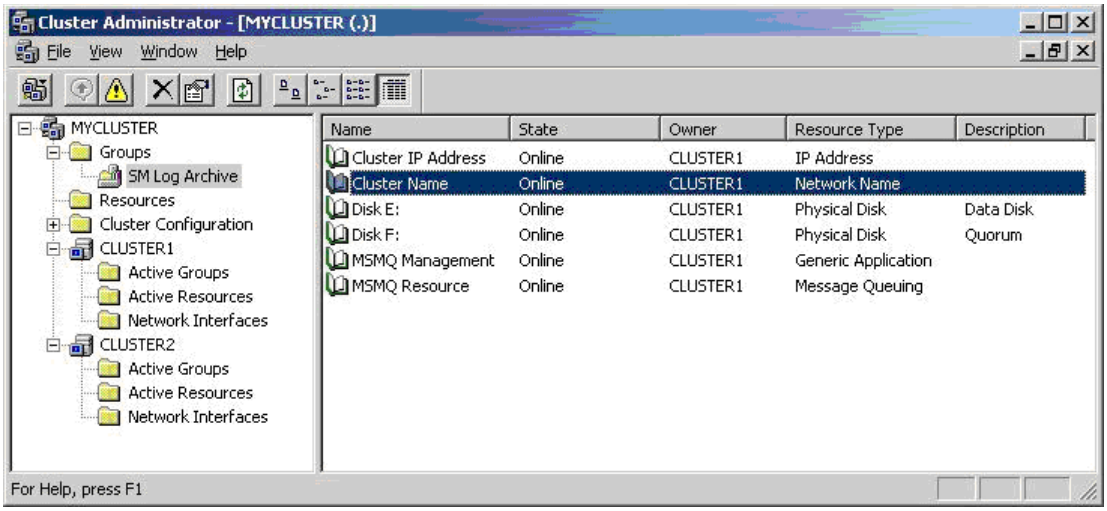
Creating a Windows Server 2003 Cluster

Create a basic two-node active/passive Windows Server 2003 cluster. For more information about creating the cluster, see the Microsoft article “Windows Server 2003 R2 Enterprise Edition – Cluster Server Resource Center” at www.microsoft.com/windowsserver2003/technologies/clustering/resources.mspx.

Configuring MSMQ on the Cluster

Install and configure MSMQ 3.0 on both cluster nodes. For more information about configuring MSMQ to run on the cluster, see the Microsoft article “Deploying Message Queuing (MSMQ) 3.0 in a Server Cluster” at download.microsoft.com/download/4/f/5/4f518f76-c1ce-431b-b79f-71caf9e27578/MSMQ3incluster.doc.

The following figure illustrates a cluster configuration *prior* to installing and configuring the log archive server. The virtual cluster server is **MYCLUSTER** and the two nodes are **CLUSTER1** and **CLUSTER2**.



The cluster group **SM Log Archive** will host the log archive. The MSMQ Management resource is described in the Microsoft document "Deploying Message Queuing (MSMQ) 3.0 in a Server Cluster" in the section "To manage an MSMQ virtual server from Computer Management."

Note
The log archive server does not require MSMQ triggers on the cluster.

The following sections describe how to configure the cluster group to host the log archive resource.

Installing Log Archive Servers on the Cluster Nodes

You need to install the log archive server component by itself on *each* cluster node. Perform the actual installation as if you are installing the log archive server to stand-alone computers. After successfully installing to both nodes, you can then configure the cluster to work with the log archive. For more information about installing Security Manager, see the *Installation Guide for NetIQ Security Manager*.

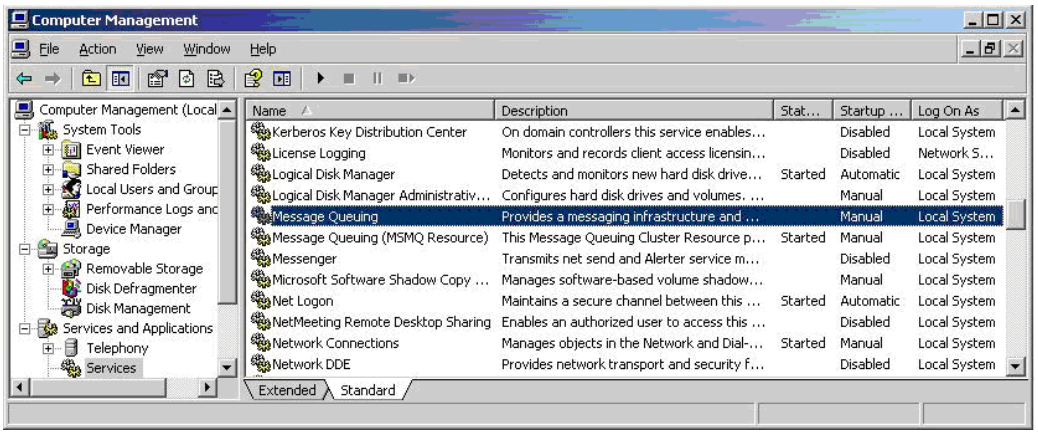
Note
Provide the *same* log archive data location on the *shared* drive and the same log archive name for both nodes of the cluster.

To install and configure the log archive server on both cluster nodes:

1. Choose a node to install first, and ensure it is the *active* node so that you have access to the shared drive.
2. Log on to the computer on which you want to install the log archive server component using an account that is a member of the local Administrators group. Also ensure your logon account is a member of the Microsoft SQL Server sysadmin role on the database server and reporting server.
3. Ensure the *local node's* Message Queuing service is running prior to installing the log archive server. With a clustered MSMQ, the local node's Messaging Queuing service is off by default. Enable the local MSMQ from Window's service control manager.

Note
A second Message Queuing service for the *cluster* is also running on the currently active node. The cluster's Message Queuing service name includes the cluster resource name (**MSMQ Resource** in our example). Ensure the *other* Message Queuing service, which is for the local node, is started.

The following figure illustrates the two entries for Message Queuing on the currently active node.



4. Install the log archive server on the currently *active* node.
   a. Close all open applications.
   b. Run the setup program from the Security Manager installation kit.

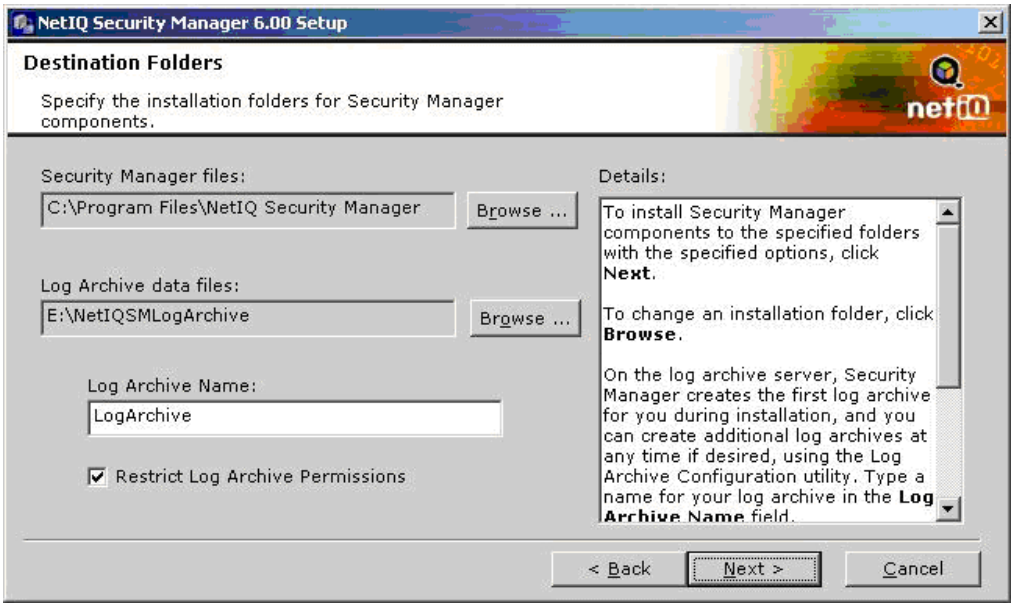
c. Click the Production Setup tab and click **Begin Production Setup**.

d. On the **Installation Type** window, select **Log Archive Server**.

e. During installation, specify a log archive data location on the *shared* clustered drive.

Note
Provide the *same* log archive data location on the *shared* drive and the *same* log archive name for both nodes of the cluster.

The following figure illustrates a log archive folder on the E: drive, a shared resource.

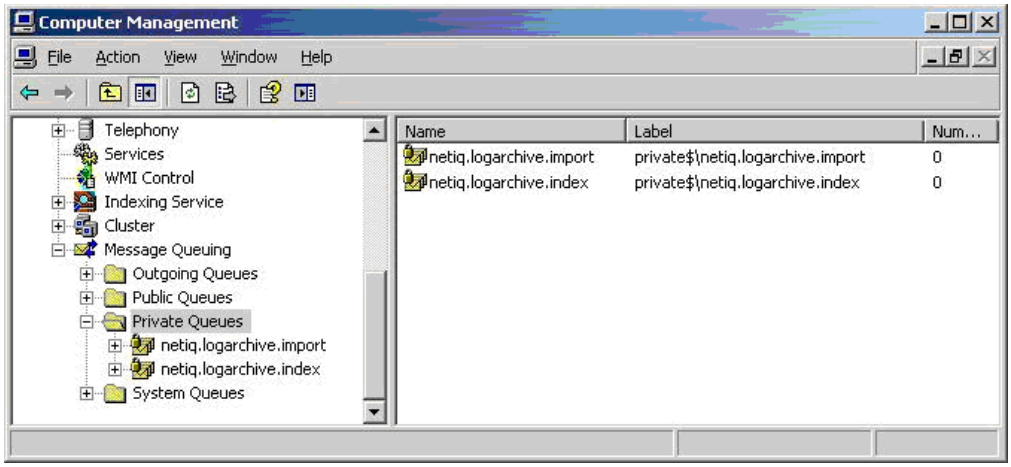


f. During installation, specify a service account for the service to use on the clustered node. The clustered log archive server will function correctly if you specify different service accounts on the two nodes, but use the same service account to avoid confusion.

g. Follow the instructions in the setup program until you reach the Finished window.

5. When the installation is complete, stop the NetIQ Security Manager Log Archive service from the service control manager.

6. Remove the MSMQ queues from the local node. In the left pane of the Computer Management window, expand **Message Queuing**, right-click **Private Queues** and select **Delete** from the menu. These queues are not used by the clustered log archive.



7. When the deletion is complete, stop the local node's MSMQ service from the service control manager.

8. Make the second node the active node, and repeat Steps **2** through **7** on the second node.

Creating the Cluster Queues

The log archive server requires two queues to operate:

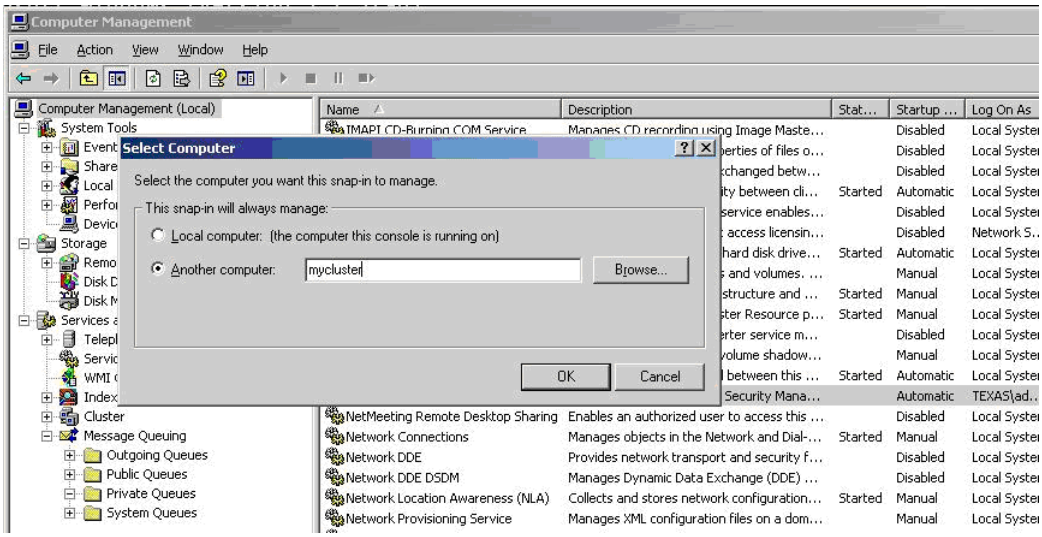
- netiq.logarchive.import
- netiq.logarchive.index

In a non-clustered installation, the Security Manager setup program creates these queues automatically. In a cluster, you must create the queues manually using MSMQ administration. Create the queues on one node, and set the security for the queues on both nodes, as described in the following procedure.

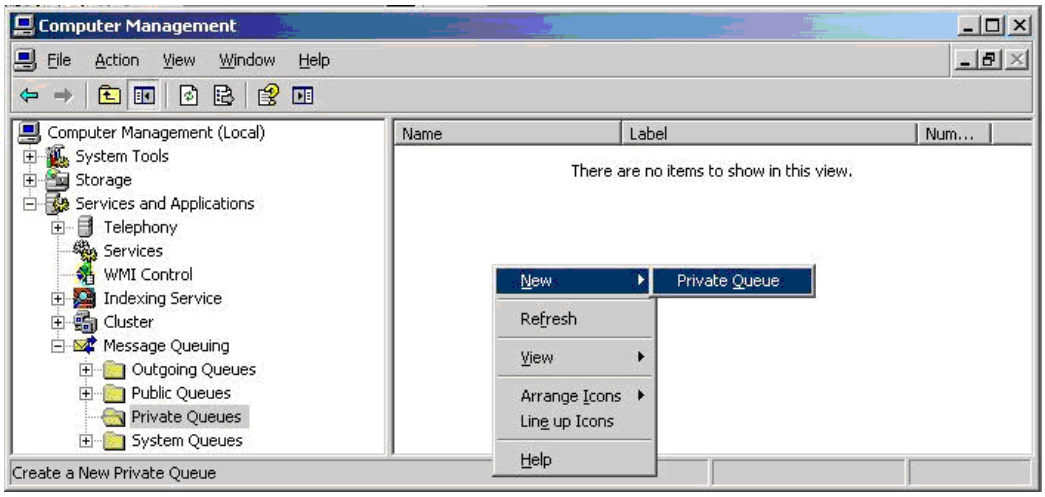
Note
When you create or configure the queues on a node, that node must be the active node.

To create the MSMQ queues for use on both cluster nodes:

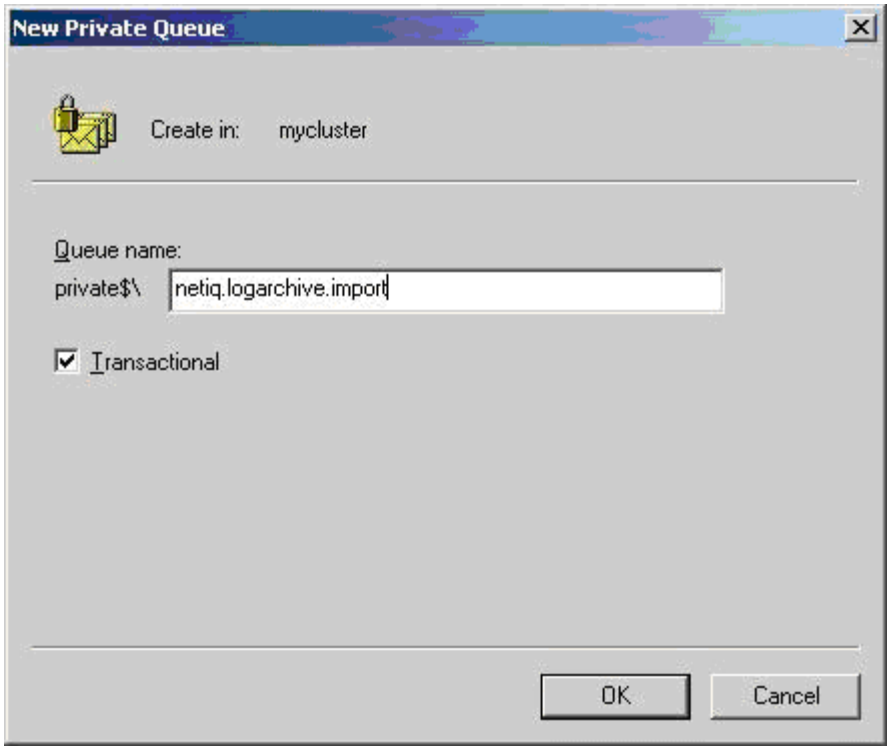
1. On the active node, right-click **My Computer** and select **Manage**.
2. In the Computer Management window, right-click the root node **Computer Management (Local)**, and select **Connect to another computer** from the menu. In the Select Computer dialog, enter the name of the cluster (**mycluster** in this example) in the **Another computer** field. Although Computer Management still indicates (Local), you are now modifying the cluster resources, including the clustered MSMQ.



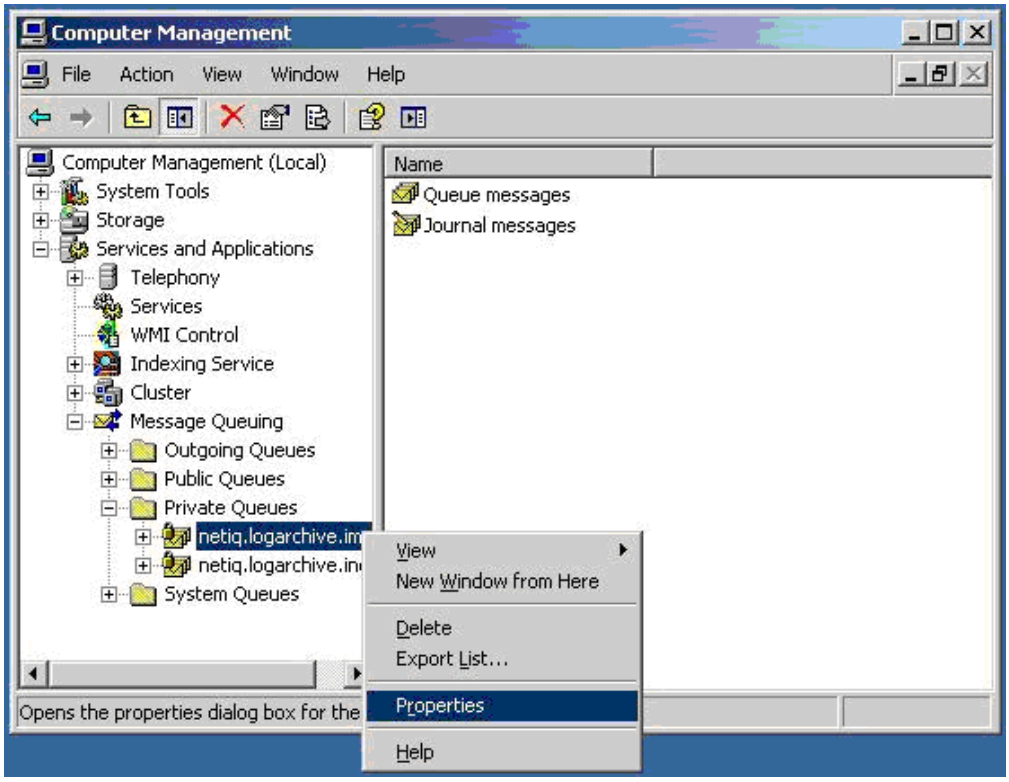
3. In the left pane, expand **Message Queuing** and click **Private Queues**.
4. In the right pane, right-click and select **New > Private Queue** from the menu to create an MSMQ queue.



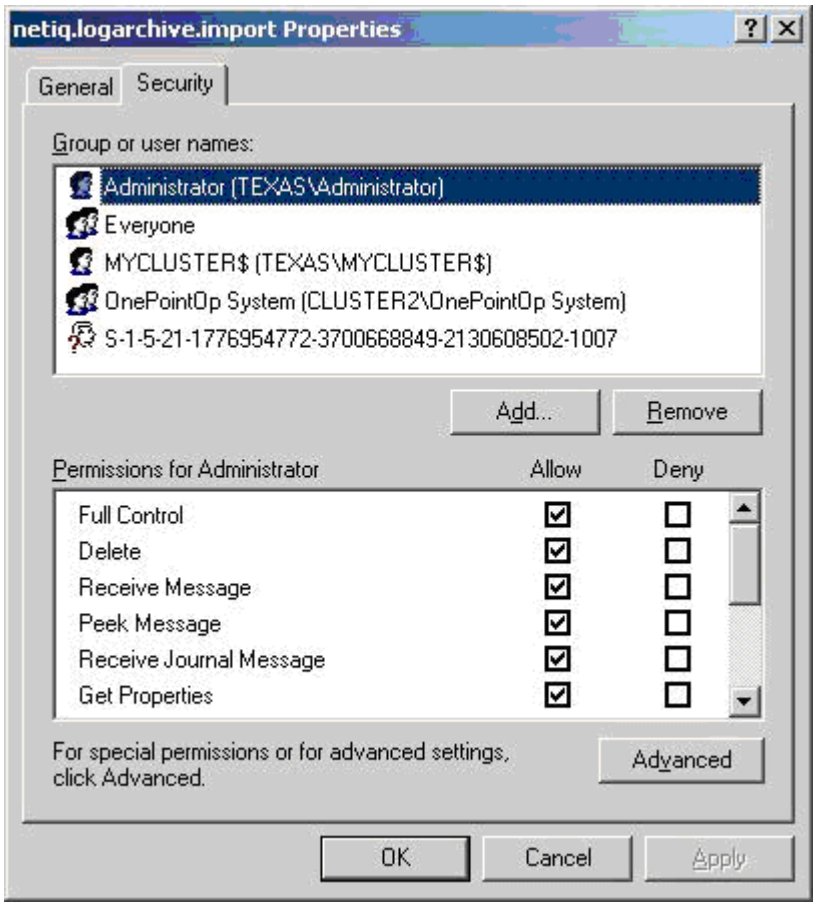
5. In the **Queue name** field, type `netiq.logarchive.import`, select the **Transactional** check box, and click **OK**. Note the "Create in: mycluster" indicates that you are adding to the cluster MSMQ.



6. Right-click the queue name and select **Properties** to assign rights to the new queue.

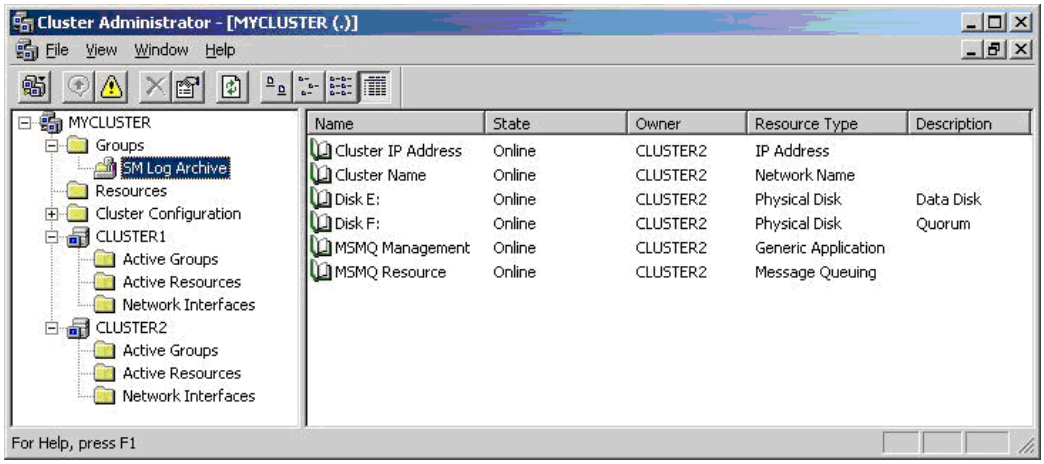


7. Grant full rights to the OnePointOp System group for the queue.



8. Repeat Steps **4** through **7** for the second queue, using `netiq.logarchive.index` for the queue name.

9. Move the active node to the second node. In the left pane of Cluster Administrator, expand **Groups**, right-click the group name (SM Log Archive in this example), and select **Move Group** from the menu.



10. Repeat Steps **6** through **7** on the `netiq.logarchive.import` queue to set its security on the second node.

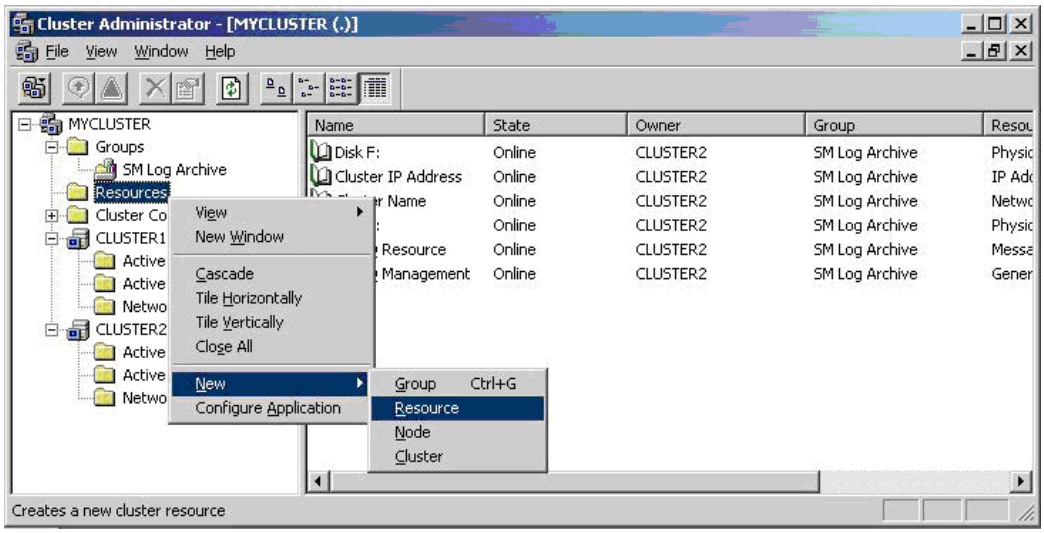
11. Repeat Steps **6** through **7** on the `netiq.logarchive.index` queue to set its security on the second node.

Configuring the Cluster to Support the Log Archive

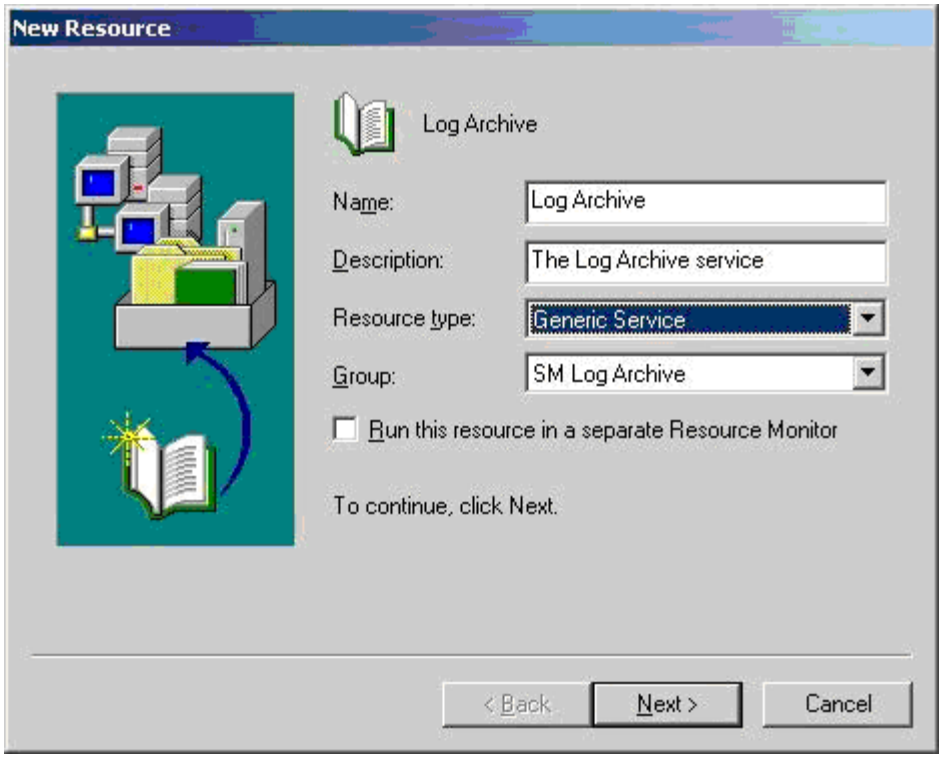
Now that the queues are created and the security properly set, you can configure the cluster to recognize the log archive.

To configure the cluster for the log archive:

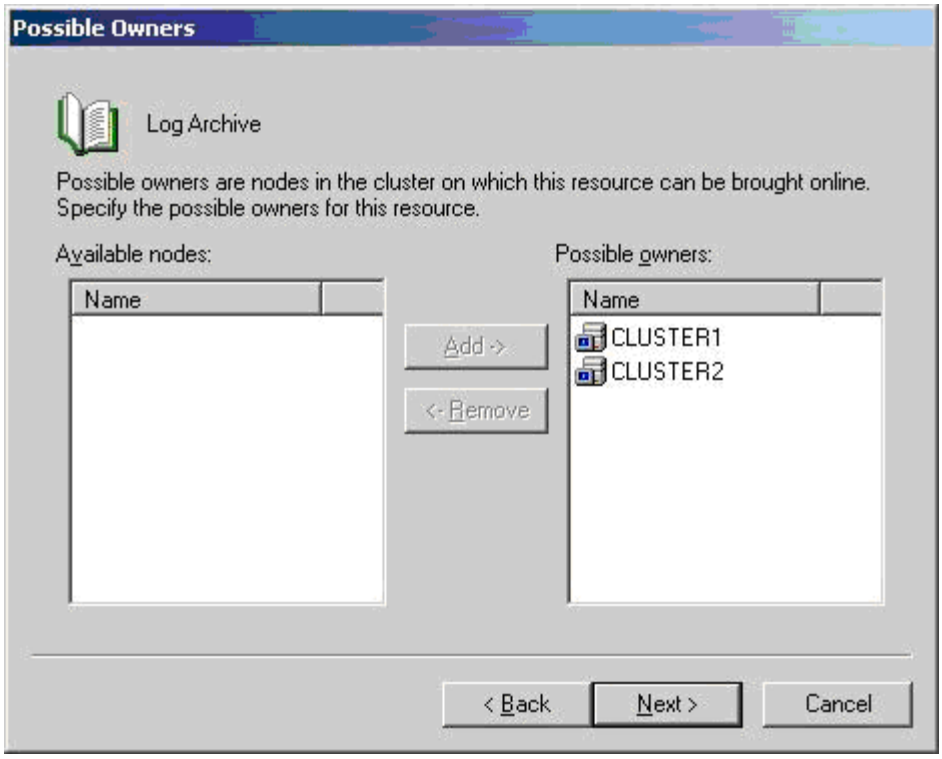
1. Add a new resource for the log archive service. In the left pane of Cluster Administrator, right-click **Resources** and select **New > Resource** from the menu.



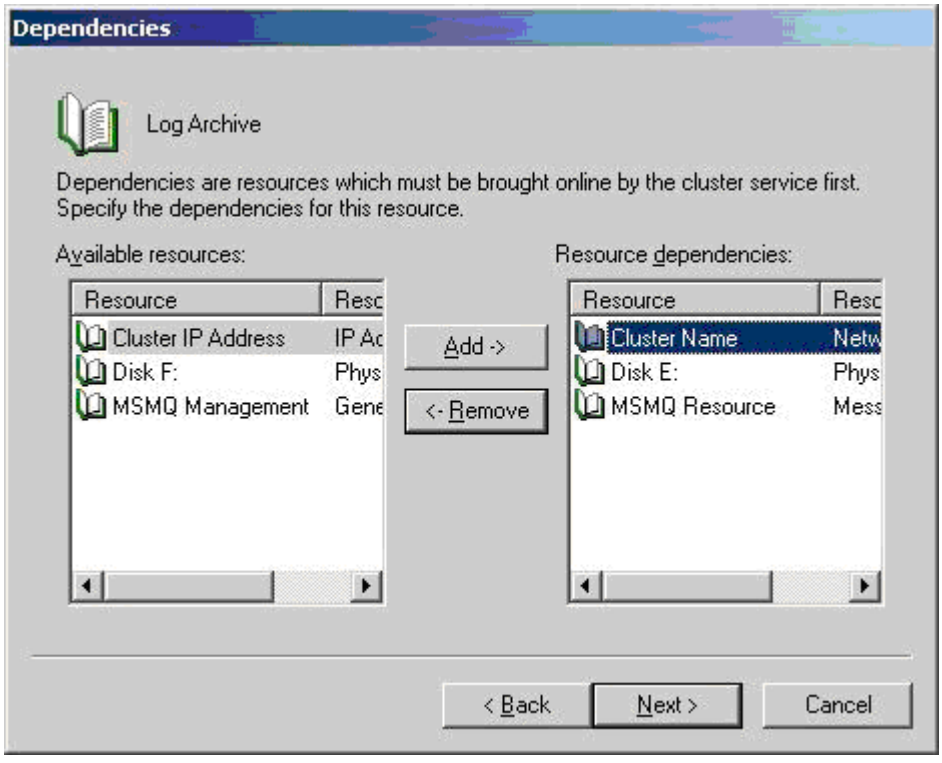
2. In the New Resource window, type a **Name** and **Description** for your log archive service resource, select Generic Service from the **Resource type** list, and select your log archive cluster group name from the **Group** list. Click **Next**.



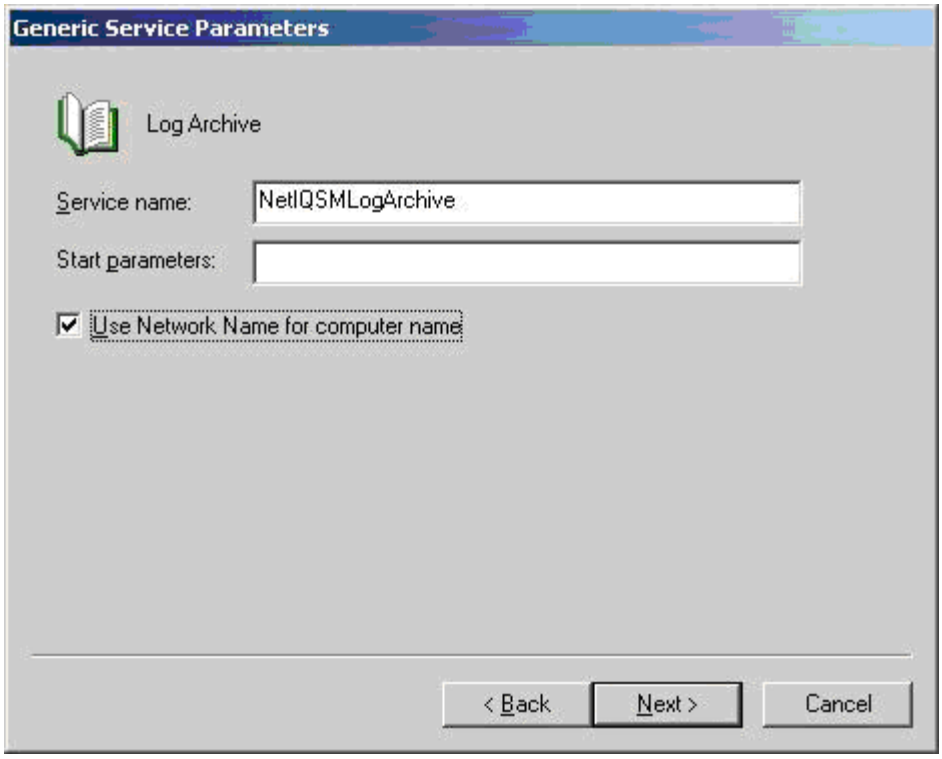
3. Select each node and click **Add** to move both nodes to the **Possible owners** list. Click **Next**.



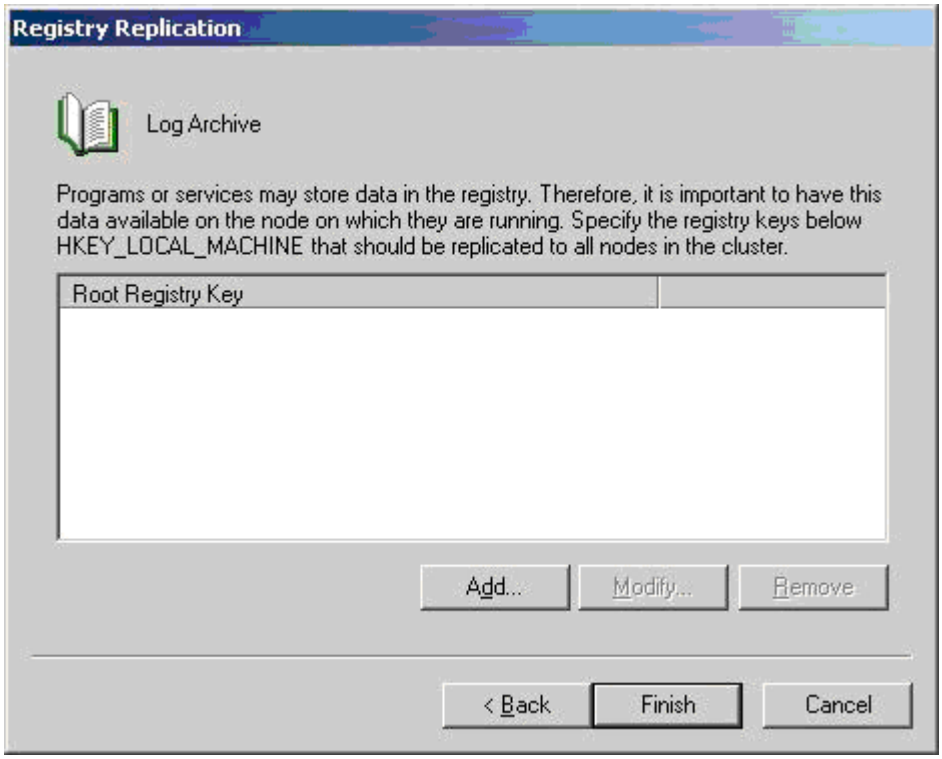
4. Set the dependencies to include the Cluster Name, the MSMQ Resource, and the disk that will host the data.Click **Next**



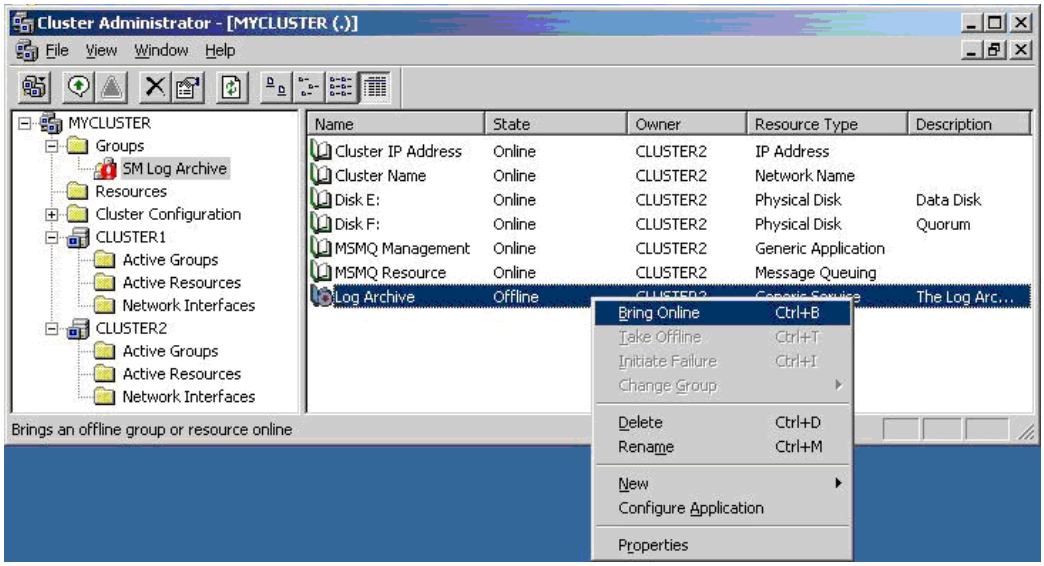
5. Type `NetIQSMLogArchive` in the Log Archive **Service name** field, select the **Use Network Name for computer name** check box, and click **Next**.



6. Click **Finish**. You do not need to specify any replicated registry keys.



7. In the left pane of Cluster Administrator, expand **Groups** and select the group (SM Log Archive in this example) to display its resources. In the right pane, right-click the new log archive service resource and select **Bring Online**.



8. When the resource is online, right-click the log archive group (**SM Log Archive** in this example) and select **Move Group** to test the group failover. Verify the group fails over to the other node.

Configuring Central Computers to Use the Log Archive Cluster

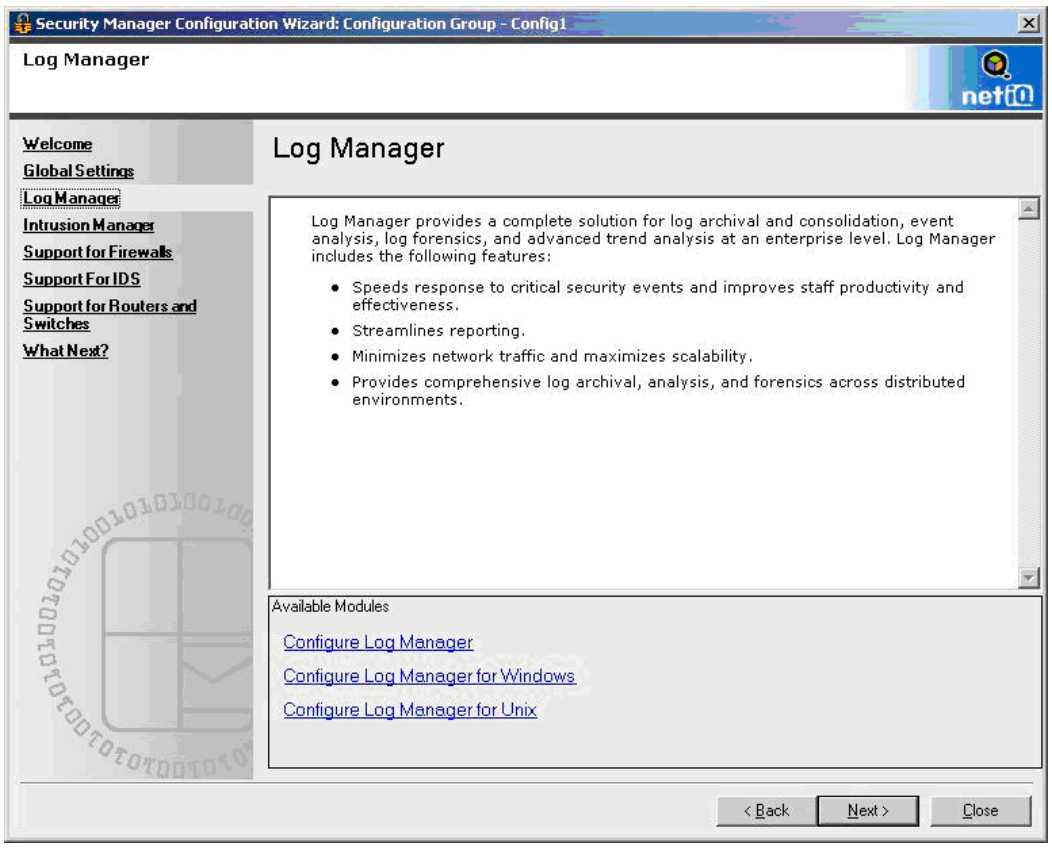
Your cluster is now configured to support the log archive service. If you have *not* yet installed your central computers, install them now and specify the cluster name (MYCLUSTER in this example) for the log archive name during installation.

If you have already installed your central computers, you can configure them to use the new clustered log archive.

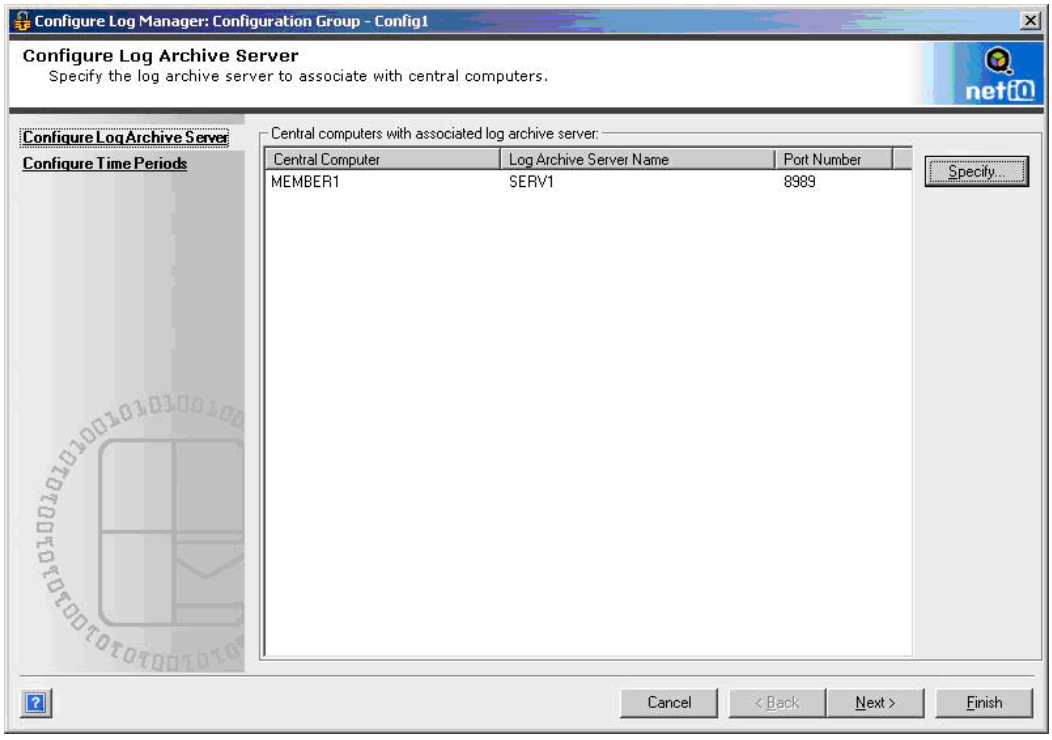
To configure previously-installed central computers to use the clustered log archive:

1. Start the Security Manager Control Center in the NetIQ Security Manager program group.
2. In the Navigation pane, click **Configuration Groups**.
3. Select the desired configuration group in the central pane, and on the Tasks menu, click **Launch the Configuration Wizard**.

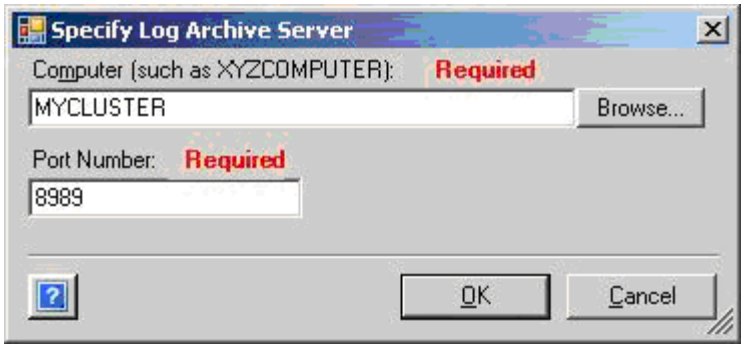
4. In the Configuration Wizard Welcome page, click **Log Manager**.



5. Select **Configure Log Manager** to display the list of central computers.



6. Select a central computer you want to send data to the clustered log archive, and click **Specify**.



7. Type the log archive cluster name (MYCLUSTER in this example) in the **Computer** field, and click **OK** to set the log archive server for the specified central computer.

8. Repeat Steps **6** through **7** for all central computers you want to use the clustered log archive.

Verifying a Successful Log Archive Cluster Installation

After successfully completing the procedures in this document, you have a highly available log archive server. The log archive server is running on one node in a two-node cluster, receiving data from its central computer, and storing data in the log archive folder.

Verify the log archive cluster is successfully installed by performing the following tasks:

- Manually fail over the cluster group to the other node. For more information about failing over the cluster group, see *Step **8*** on page *13*.
- Observe that the log archive server created log archive files (`.nds`) in today's partition of the log archive directory. For more information about log archive server partitions and files, see the *User Guide for NetIQ Security Manager*.
- View statistics about existing log archive files using the Log Archive Configuration utility. For more information about viewing log archive statistics, see the *User Guide for NetIQ Security Manager*.
- Run Forensic Analysis queries and verify that the reports contain the expected stored log data. For more information about Forensic Analysis, see the *User Guide for NetIQ Security Manager*.

Troubleshooting a Log Archive Cluster Installation

If you cannot verify a successful log archive cluster installation, you may want to take one of the following actions.

- Troubleshoot and reconfigure the log archive server using the Log Archive Configuration utility. For more information about using the Log Archive Configuration utility, see the *User Guide for NetIQ Security Manager*.
- Uninstall and reinstall the log archive server on both cluster nodes. If you uninstall the log archive server, before reinstalling it, manually delete the existing log archive configuration file and log archive data.

  To delete the log archive configuration file and data:

1. Navigate to *`SystemDrive`*`\Documents and Settings\All Users\Application Data\NetIQ\Security Manager`, where *`SystemDrive`* is the drive where Windows is installed on the computer.
2. Delete the file `LogArchiveConfiguration.config`.
3. Delete *`LogArchive`* including all subfolders, where `LogArchive` is the log archive path and folder name, `C:\NetIQSMLogArchive` by default.