

# TECHNICAL REFERENCE

## NetIQ Security Manager Log Archive Server Best Practices

January 9, 2012

This technical reference provides best practice information about the NetIQ® Security Manager™ log archive server component. It provides information about log archive server functionality, hardware requirements, troubleshooting suggestions, and instructions for baselining the log archive daily event volume.



## Legal Notice

NetIQ Security Manager is protected by United States Patent No: 05829001.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

© 2011 NetIQ Corporation. All rights reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This product claims FIPS compliance by use of one or more of the Microsoft cryptographic components listed below. These components were certified by Microsoft and obtained FIPS certificates via the CMVP.

- 893 Windows Vista Enhanced Cryptographic Provider (RSAENH)
- 894 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)
- 989 Windows XP Enhanced Cryptographic Provider (RSAENH)
- 990 Windows XP Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)
- 997 Microsoft Windows XP Kernel Mode Cryptographic Module (FIPS.SYS)
- 1000 Microsoft Windows Vista Kernel Mode Security Support Provider Interface (ksecdd.sys)
- 1001 Microsoft Windows Vista Cryptographic Primitives Library (bcrypt.dll)
- 1002 Windows Vista Enhanced Cryptographic Provider (RSAENH)
- 1003 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)
- 1006 Windows Server 2008 Code Integrity (ci.dll)
- 1007 Microsoft Windows Server 2008 Kernel Mode Security Support Provider Interface (ksecdd.sys)
- 1008 Microsoft Windows Server 2008
- 1009 Windows Server 2008 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)
- 1010 Windows Server 2008 Enhanced Cryptographic Provider
- 1012 Windows Server 2003 Enhanced Cryptographic Provider (RSAENH)

This product may also claim FIPS compliance by use of one or more of the Open SSL cryptographic components listed below. These components were certified by the Open Source Software Institute and obtained the FIPS certificates as indicated.

- 918 - OpenSSL FIPS Object Module v1.1.2 - 02/29/2008 140-2 L1
- 1051 - OpenSSL FIPS Object Module v 1.2 - 11/17/2008 140-2 L1
- 1111 - OpenSSL FIPS Runtime Module v 1.2 - 4/03/2009 140-2 L1

Note: Windows FIPS algorithms used in this product may have only been tested when the FIPS mode bit was set. While the modules have valid certificates at the time of this product release, it is the user's responsibility to validate the current module status.

EXCEPT AS MAY BE EXPLICITLY SET FORTH IN THE APPLICABLE END USER LICENSE AGREEMENT, NOTHING HEREIN SHALL CONSTITUTE A WARRANTY AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY NETIQ, ITS SUPPLIERS AND LICENSORS.

## Table of Contents

Introduction.....	1
Overview of Log Archival Process .....	1
Event Processing .....	1
Processing Partitions .....	2
Partitions.....	2
Indexes .....	3
Closing a Partition.....	4
Processing Forensic Analysis Queries .....	5
Uploading Data to the Reporting Server .....	6
Hardware Best Practices.....	6
Operating System Configuration .....	6
Planning Storage for Log Archives.....	6
Locating Temporary Index Directories .....	7
Processor and Memory Requirements.....	8
Limiting the Number of Indexing Jobs .....	8
Improving the Speed of Forensic Analysis Queries .....	9
Determining Performance Bottlenecks .....	9
Windows Recommended Performance Counters .....	9
NetIQ Security Manager Performance Counters.....	10
Troubleshooting a Backlog of Data .....	11
Baseline Log Archive Daily Event Volume with Microsoft Excel.....	12
About NetIQ .....	23

## Introduction

Security Manager provides log management, analysis, and query-based forensics to help you meet compliance and security mandates.

Of all Security Manager product components, the log archive server is the most resource-intensive component in a configuration group. Security Manager writes log archive data to disk and builds a full-text index for searching and reporting purposes.

To understand how to properly size the log archive server for your environment, it is helpful to understand how the log archival process works.

## Overview of Log Archival Process

Security Manager agents collect event data from logs across your enterprise and send it to the central computer, which then funnels the data to the **log archive server**.

The log archive server uses the NetIQ Security Manager Log Archive service to store collected log data in **log archives**.

A **log archive** is a folder that securely stores the log data in a binary, flat-file format. The log archive server stores data as separate **records**, with one record per event. The data is hashed, and you have the option of Security Manager digitally signing the data.

Log archives, also called **volumes**, contain folders called **partitions**. A **log archive partition** is a folder that stores log data collected each day.

Each log archive also contains a `VolumeInfo.xml` file, which Security Manager uses to track statistical information about the log archive as a whole. The `VolumeInfo.xml` file includes the following data:

- Total number of records currently in the log archive
- Total number of records groomed out of the log archive

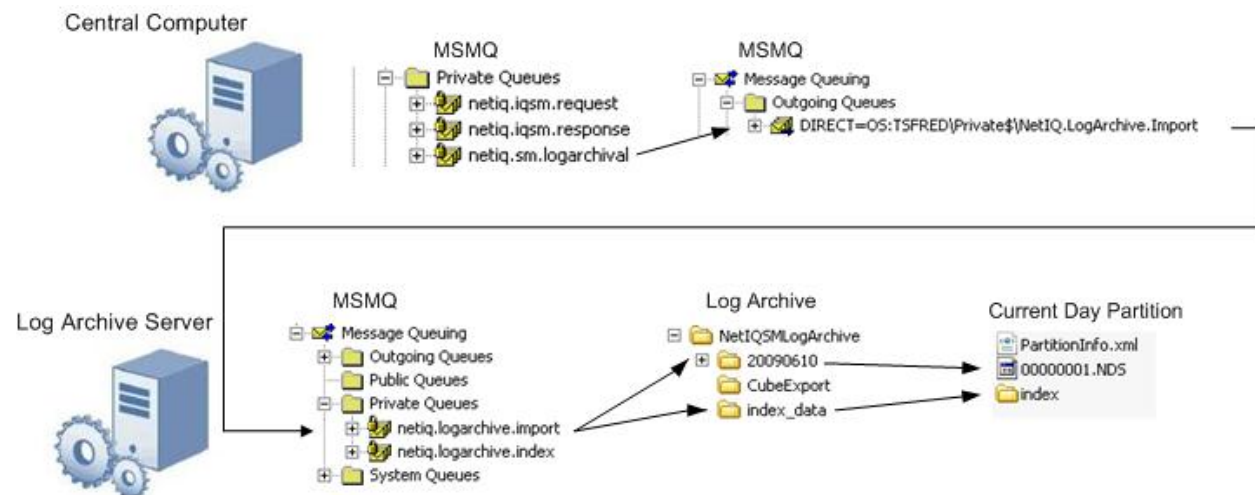
## Event Processing

Understanding the flow of log data during the log archival process will help you troubleshoot potential issues that might occur in your environment.

Each Security Manager agent builds event data into compressed record blocks, or packages, and sends them to the central computer, to the `netiq.sm.logarchive` Microsoft Message Queue (MSMQ). The central computer then places the data in an outgoing queue to be sent to the log archive server's import queue.

The log archive server receives the packages from the central computer and stores them in the `netiq.logarchive.import` queue.

The NetIQ Security Manager Log Archive service streams the data to the log archive (in this case, to the active volume, which is named `NetIQSMLogArchive` by default) and into the current day's partition. The data is stored in NetIQ data store ( `.NDS` ) files. The service places indexing data in the `index_data` folder, and then processes it into the designated partition's `index` folder.



## Processing Partitions

Security Manager names the **log archive partition**, the folder that stores log data collected each day, by using the date in local time on the log archive server (YYYYMMDD). For example, in the log archive above, the partition is named 20090610, for June 10, 2009.

### Partitions

When the central computer sends data to the log archive server, the log archive server appends the blocks of data to the most recent log archive file. Log archive files are collections of record blocks, each consisting of event data collected from logs. Each daily log archive partition contains one or more log archive files, depending on the amount of data collected that day. Security Manager names each log archive file sequentially, such as 00000001.NDS.

By default, each log archive file contains up to 400 record blocks. Once Security Manager appends the maximum number of record blocks to a log archive file or when the NetIQ Security Manager Log Archive service restarts, Security Manager closes the current log archive file and creates a new file. When a log archive reaches the maximum size (configured either during installation or using the Log Archive Configuration utility), Security Manager stops storing data in the current log archive and starts storing data in the next available log archive on the log archive server computer.

If all log archives on the server are full, Security Manager stops collecting new event data and logs an Error event in the event log.

## Indexes

Security Manager indexes all data stored in the log archive. Security Manager automatically formats all collected records so the log archive server can index the data.

After the log archive server appends a record block to a log archive file, the server uncompresses the record block and stores part of the block in a `.indexing` file in the `index_data` folder. The log archive server then uses one or more special indexing processes to index the stored data.

By default, the number of indexing processes on a log archive server is equal to the number of processor cores on the log archive server computer.

When the log archive server indexes a partition, the log archive server creates an `index` folder within the partition, with one or more numbered subfolders, each of which contains a set of `.ix` files that the log archive server uses to store index information. Each log archive indexing process takes a `.indexing` file out of the `index_data` folder and adds the data from the file to the `.ix` index files for the current log archive partition. The process then deletes the `.indexing` file from the `index_data` folder.

Because of the nature of the information needed for indexing, files in the `index` folders can be very large. A log archive index file can be five to ten times the size of the data indexed.

At midnight each day, the NetIQ Security Manager Log Archive service creates a new partition for the new current day and redirects the data stream to the new current day's partition. Index processing continues on the previous day's partition until the log archive server processes all of that partition's index data from the `index_data` folder. When the log archive server finishes processing all index data, the partition is ready to be closed.

The `PartitionInfo.xml` file describes the contents of a given partition, and includes the following data:

- Total number of records currently in the log archive partition
- Total size of records currently in the log archive partition (including compressed size, uncompressed size, and total size on disk)
- Starting and ending dates for the records in the log archive partition
- Name of each `.NDS` file in the log archive partition
- Number of record blocks in each `.NDS` file in the partition
- Number of individual records in each `.NDS` file in the partition
- Total size of records currently in each `.NDS` file (including compressed size, uncompressed size, and total size on disk)
- Hash for each `.NDS` file in the partition

## Closing a Partition

Once an hour, the NetIQ Security Manager Log Archive service spawns the `CloseablePartitionLocatorJob`, which scans the `volumeinfo.xml` file and looks for open partitions. If the job finds an open partition, the job attempts to close the partition.

During the partition closing process:

1. The job verifies the index.
2. The job compresses the index using NTFS compression.
3. The job marks the partition as `Closed` in the `Partitioninfo.xml` and `Volumeinfo.xml` files.

The log archive server contains a `LogArchiveServer.txt` log file that records log archive activity. The following excerpt from the `LogArchiveServer.txt` file shows the `CloseablePartitionLocatorJob` closing the partition for April 10, 2010:

```
2010-04-11 00:02:25,171 [6] INFO
NetIQ.NERDS.DataStore.Storage.CloseablePartitionLocatorJob: Closing partition
20100410
2010-04-11 00:02:32,765 [6] INFO
NetIQ.NERDS.DataStore.Storage.PartitionClosedSubscriber: Partition
volume=Archive1;partition=20100410 closed.
```



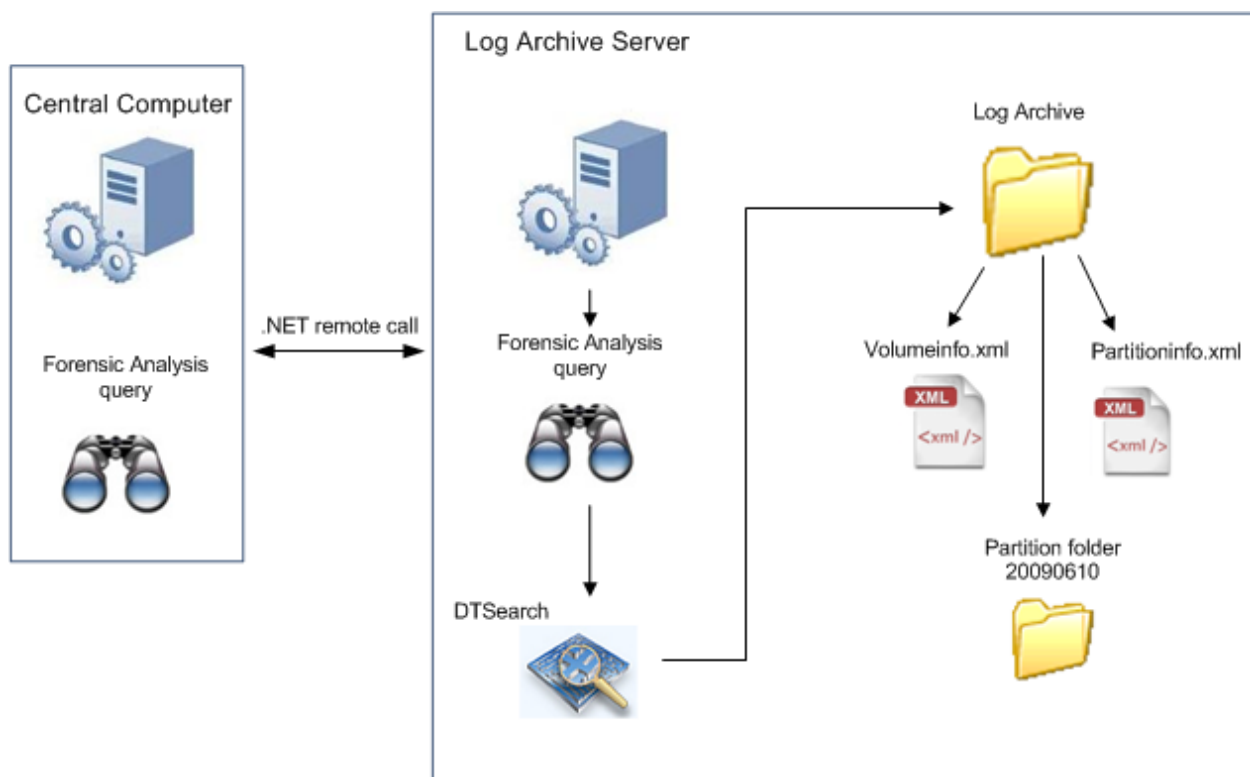
## Processing Forensic Analysis Queries

When the log archive server receives a Forensic Analysis query from the central computer, the server processes the query on each mounted log archive. The log archive service uses the DTSearch engine to locate the desired data within each archive.

The query contains computer GUIDs from the OnePoint database and the time is converted to Unix time (a number based on the seconds since January 1, 1970). The query examines the `Volumeinfo.xml` to determine which partitions to scan, taking groomed partitions and date ranges into account.

Once the query determines the partitions to search, the query searches each partition based on the other query parameters specified, such as `EventID` and `Event Source`.

The log archive server and central computer use .NET remote calls to send query data back and forth.



## Uploading Data to the Reporting Server

Security Manager provides the ability to run Trend Analysis reports on summarized log archive data. As data is indexed on the log archive server, the log archive server extracts a select number of fields and writes them to temporary files located in the CubeExport folder. On a scheduled interval, the log archive server will upload the exported data to the defined reporting server.

This upload process is off by default.

To configure and enable the export of summarized data to the reporting server, use the Log Archive Server Configuration Tool. For more information about enabling and configuring the export of log archive data, see the *Installation Guide for NetIQ Security Manager*.

If the log archive server cannot upload data to the reporting server, the server writes relevant error message to the Windows NT Event Log. You can troubleshoot potential problems using the error messages.

The CubeExport folder should never contain more temporary files than two times the number of index jobs. For example, if there are four index jobs, there should be no more than eight temporary files in the folder. If there are more files than you anticipate in the CubeExport folder, there is an issue with the upload process.

## Hardware Best Practices

Log archive server performance is more dependent on the underlying disk input/output (I/O) capacity available than any other resource, because of the intense nature of writing indexes and searching those indexes for data. For more information about specific hardware requirements, see the *Installation Guide for NetIQ Security Manager*.

## Operating System Configuration

For optimal performance, use a 64-bit architecture-based operating system for the log archive server. Additionally, do not place the operating system page file on any storage device that is being used as part of the actual log archive.

This guideline is important for environments that include blade servers, which use some form of shared storage for data. Ensure that the page file is located on its own dedicated disk.

## Planning Storage for Log Archives

Security Manager stores the actual log data in the log archives. Security Manager creates a new partition daily in which all log data is stored. Security Manager also writes the indexes for each partition into these folders. The amount of space required for a log archive is largely dependent on the amount of data being fed into the log archive server and the online data retention period.

Each event takes approximately 300 bytes of space, once the index is written. A simple formula for calculating the space required per day in gigabytes is:

$$(x * 300) / 1,000,000,000$$

Where  $x$  is the number of events received per day.

Consider the following guidelines when building the storage array to host your log archives. Treat the log archive server as a high-speed relational database management system (RDBMS). Almost all of the rules that apply to a busy RDBMS database apply to the log archive server.

- The storage array should be dedicated and not shared with any other applications. This guideline also applies to the physical disks in the array and not just to a logical disk presented by a storage area network (SAN). If disk I/O is consumed by something other than the log archive server, performance may be affected.
- Configure the storage array in an optimal Redundant Array of Independent Disks (RAID) setup. RAID 10 is the best solution, as it provides the benefit of striping as well as the fault tolerance of mirroring. RAID 5 is acceptable in some environments but trades some of the I/O in exchange for fewer disks. Avoid a RAID 6 configuration, as it adds the overhead of a second parity bit and further reduces I/O capacity.
- Disks in the storage array should be fast. 15K RPM disks are optimal. In some cases, 10K RPM disks are acceptable, but 10K RPM should be the absolute minimum speed. Do not use any disk speed slower than 10K RPM to store data for an active log archive on the log archive server.
- Connect the storage array to the log archive server in the most optimal configuration possible, preferably using a fiber channel. Several successful implementations exist that use iSCSI. If you use iSCSI, use it on a dedicated network with speeds greater than or equal to 10GB per second.
- Do not write to multiple log archives simultaneously. Some customers present multiple log archives to the log archive server to allow for smaller archives. Significant performance problems have been identified when users rotate log archives in and out of Read-only status. If the indexing process does not complete, and a partition remains open, query speeds drop dramatically.

## Locating Temporary Index File Directories

In high-event-load environments, move the temporary index file locations off of the main log archive, which is `NetIQSMLogArchive` by default. Think of the temporary index files as a transaction log for an RDBMS database. The indexing process uses lots of temporary information, with significant amounts of data going in and out at high speeds.

You can move the temporary index files by following the instructions in NetIQ Knowledge Base article [NETIQKB72195](#). If you move your temporary index file locations, follow these guidelines:

- Disks should be dedicated and should not be part of the array presented as the main log archive (this means separate physical disks).
- Disk speed should be no less than 15K RPM.
- Configure disks in a RAID 0 array. Log archive indexing does not require fault tolerance.
- Use one disk per indexing job and locate disks dedicated to indexing in an internal array to eliminate any potential issues with network interconnects.
- Allocate 32GB of disk space for each indexing job.

## Processor and Memory Requirements

While the disk subsystem is the most important hardware component to consider when building a log archive server, there is also significant overhead required for building and writing indexes. Consider the following guidelines for processors and memory.

NetIQ Corporation recommends 1GB per core, with a minimum of 4GB in the log archive server. The log archive server takes advantage of multi-core processors, and creates an additional indexing process for each core available, which allows for an increase in indexing power.

A general guideline in sizing the log archive server is to allocate one core for each two high-speed disks per 1000 sustained events per second. The more processors in a system, the better.

## Limiting the Number of Indexing Jobs

Because they constantly start and shut down, indexing jobs can cause latency overhead and greater disk usage. Consider limiting the number of indexing jobs in the following situations:

- When disk I/O can no longer keep up with the indexing speed of the log archive server
- If the log archive server is not receiving large volumes of events, and your environment has several available cores

### To limit the number of indexing jobs:

1. Contact NetIQ Technical Support to determine the optimal number of indexing jobs for your specific environment.
2. Log onto your log archive server.
3. Open Windows Explorer.
4. Browse to the `C:\Documents and Settings\All Users\Application Data\NetIQ\Security Manager` folder.
5. Use a text editor such as Notepad to open the `LogArchiveConfiguration.config` file.
6. Find the following section:

```
<IndexingSettings>
  <PropertyList>
    <Property name="IndexJobCount" value="default" />
```

7. Change the default value based on the event-per-second load. For example, changing `default` to `8` will limit the number of indexing jobs to 8. Changing `default` to `2` will limit the number of indexing jobs to 2.
8. Save your changes to the `LogArchiveConfiguration.config` file.
9. Restart the NetIQ Security Manager Log Archive service.

## Improving the Speed of Forensic Analysis Queries

The log archive server builds a full-text index to allow fast searching. While the index inherently increases Forensic Analysis query performance, you can also build optimal queries to reduce query time. Use the following guidelines to build optimal queries:

- Limit the query to as few endpoints as possible. In the Forensic Analysis Wizard, select a computer group that contains a targeted set of computers, such as `windows 2008 Domain Controllers`, instead of `All windows Servers`.
- Further reduce the number of targeted endpoints by defining specific criteria in the wizard's **Filters** tab.
- Search the minimum number of days required to meet the need of the query. Searching a targeted seven days for activity is better than searching all data for the last 60 days. Queries that target a large number of days take time even on the most optimal hardware.
- Avoid starting the `contains` clause with a wild card, such as `Message contains *username`. The wild card at the beginning starts a non-indexed search. However, you can use a trailing wild card, which is a wild card at the end of the `contains` clause. For example, `Message contains username*`.

## Determining Performance Bottlenecks

If the data load is too great or the hardware provided is insufficient, the log archive server will not meet performance expectations. You can troubleshoot potential performance problems. The best way to begin determining problems is to use Windows standard performance counters. A number of performance counters for the log archive server processes are available, as well.

### Windows Recommended Performance Counters

You can review the following Windows standard performance counters to troubleshoot performance problems.

Performance Counter	Description
MSMQ Queue\Messages in Queue (For the <code>netiq.sm.logarchive1</code> queue on the central computer)	Displays the number of blocks of events sent from the agents to the central computer. If this number is greater than 40 in a low data-volume environment, or greater than 150 in high data-volume environment, then this number might indicate log data is backing up on the central computer.
MSMQ Queue\Messages in Queue (For the <code>netiq.logarchive.import</code> queue on the log archive server)	Displays the number of aggregated blocks of events sent from the central computer to the log archive server. If this number is greater than 5, it indicates that the log archive is either not running or unable to keep up with log volume.

Performance Counter	Description
PhysicalDisk\Avg. Disk Queue Length	Used to determine disk performance issues for the database server, log archive server, and even agents and central computers.  If this number is twice the number of spindles on the drive that hosts the OnePoint database, the log archive, or the agent and central computer queues, there is likely a problem.
Physical Disk\Disk Reads/sec Physical Disk\Disk Writes/sec	Used to determine potential disk I/O issues. Keep these numbers below 20ms. As that number grows, so will the performance degradation and will typically reach an unacceptable range when this number reaches 50ms.
<p><b>NOTE:</b></p> <p>If you use a SAN for your log archive server, most Windows disk-related performance counters for the disk I/O will not be as accurate as performance counters that are typically available in SAN management software.</p>	

## NetIQ Security Manager Performance Counters

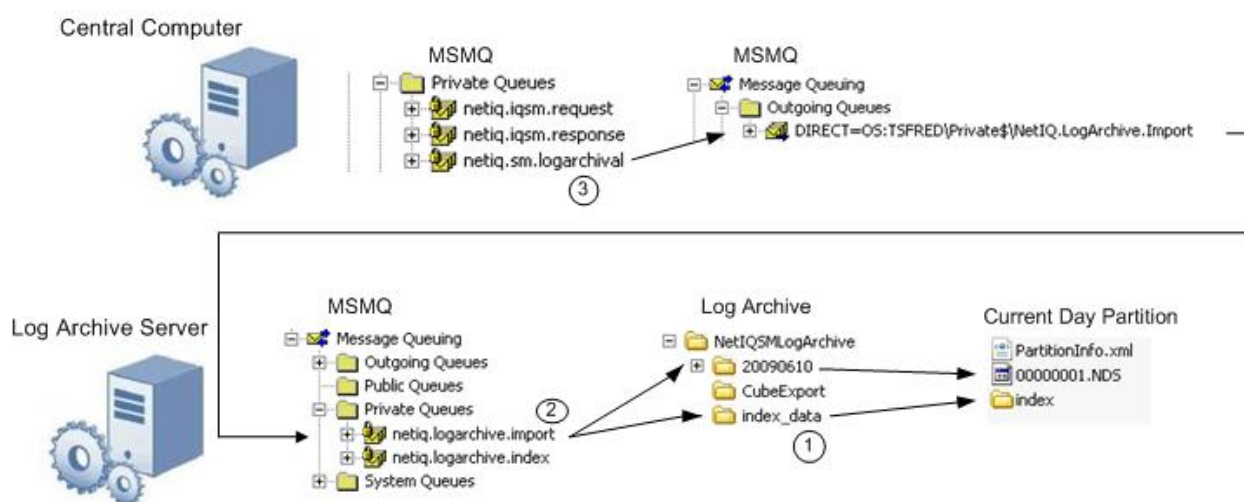
You can review the following NetIQ Security Manager performance counters to troubleshoot performance problems.

Performance Counter	Description
NetIQ Log Archive\Messages Invalid Bytes	Displays the total number of bytes of messages that were malformed.
NetIQ Log Archive\Messages Invalid Count	Displays the total number of messages that were malformed. If this value is greater than 1, the log archive has received a corrupt message from the MSMQ queue.
NetIQ Log Archive\Messages Read Bytes	Displays the total number of bytes of messages that were accepted by the log archive.
NetIQ Log Archive\Messages Read Count	Displays the total number of messages that were accepted by the log archive.
NetIQ Log Archive\Messages Rejected Bytes	Displays the total number of bytes of all messages submitted to the log archive that were rejected.
NetIQ Log Archive\Messages Rejected Count	Displays the total number of messages submitted to the log archive that were rejected. If this value does not equal 0, the log archive has received a message contained a corrupt block of records and could not be process the corrupt data.
NetIQ Log Archive\Messages Sent Bytes	Displays the total number of bytes of all messages submitted to the log archive that were accepted.
NetIQ Log Archive\Messages Sent Count	Displays the total number of messages submitted to the log archive that were accepted.
NetIQ Log Archive\Messages Sent Uncompressed Bytes	Displays the total number of bytes of uncompressed data in messages submitted to the log archive that were accepted.

Performance Counter	Description
NetIQ Log Archive\Pending Reporting Tables	Displays the number of fact tables that are waiting to be processed on the reporting server. If this number does not reset to 0 roughly every hour, the reporting server may not be accessible, or there may be some other problem uploading the cube data to the reporting server.
NetIQ Log Archive\Records Sent Count	Displays the total number of records accepted by the log archive.
NetIQ Log Archive\Records Sent Uncompressed Bytes	Displays the total number of uncompressed bytes of all records successfully sent to the log archive for long-term storage since the server started.

## Troubleshooting a Backlog of Data

If your log archive server experiences issues while receiving or processing log data, those issues can create a backlog of data through the system. You can trace the backlog backwards using the following illustration.



To trace the backlog, start with (1) the `index_data` folder located in the log archive, by default `NetIQSMLogArchive`. If the number of files in this folder grows to 25,000, data is no longer imported to the log archive. The log archive service will begin importing data again when the file count gets below 25,000.

If the `index_data` folder is not the backlog, (2) check the `netiq.logarchive.import` queue of the log archive server. A large number of messages in the queue is an indication that the data cannot be written into the log archive. This issue is typically caused by lack of space on the disk.

The next step is to (3) check the `netiq.sm.logarchival` queue on the central computer. A large number of messages in this queue can be an indication of communication problems between the central computer and the log archive server.

For more assistance troubleshooting issues on your log archive server, contact NetIQ Technical Support.



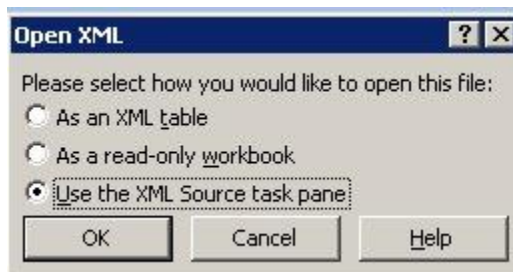
## Baseline Log Archive Daily Event Volume with Microsoft Excel

You can create baselines for the daily event volume of a log archive server by using a combination of Microsoft Excel and the `volumeinfo.xml` file, located in the root level of the log archive.

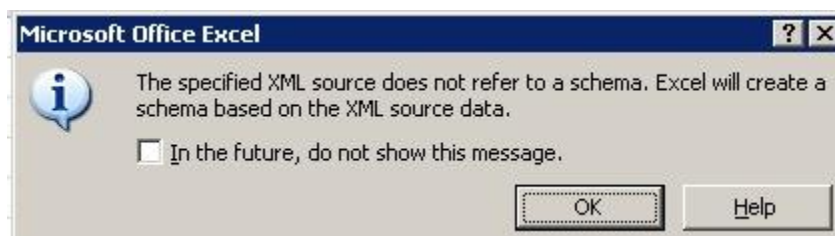
A baseline determines normal log activity. Changes to the normal level of activity can indicate a potential security issue in your environment.

### To create a log archive activity baseline:

1. Open Windows Explorer.
2. Browse to the root level of the main log archive.
3. Copy the `volumeinfo.xml` file to your desktop.
4. Right-click `volumeinfo.xml` and open it using Excel 2007 or later.
5. Select **Use the XML Source task pane** and click **OK**.

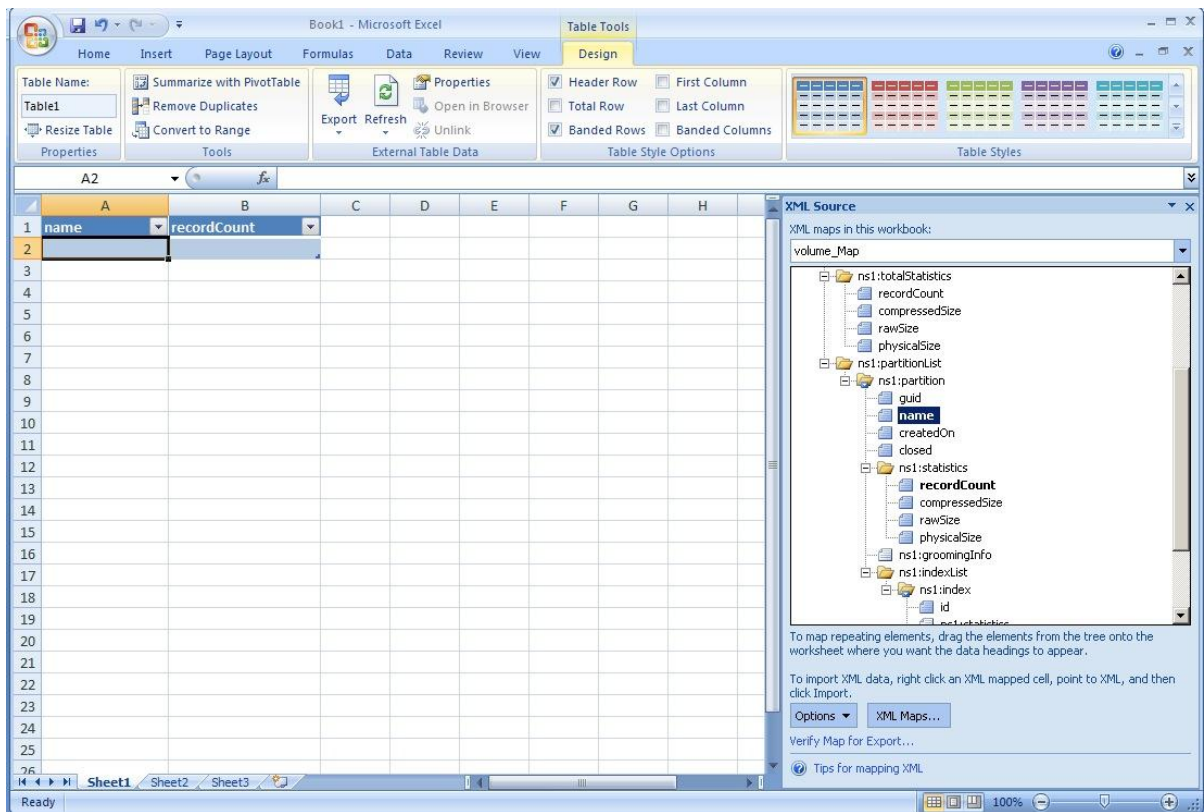


6. Click **OK**.

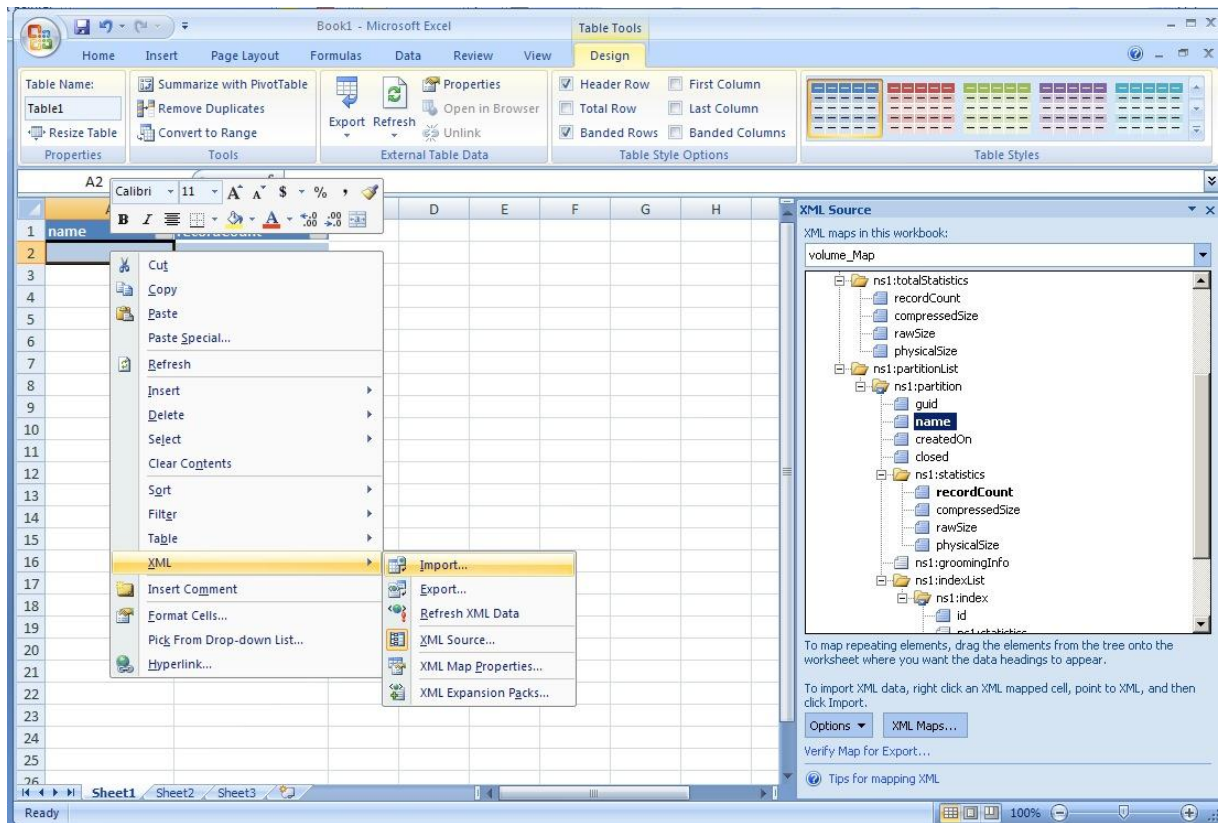




- Under **ns1:partition**, select name and drag the element to Column A. Under **ns1:statistics**, select recordCount and drag the element to Column B.



- Right-click the A2 cell and select **XML > Import**.

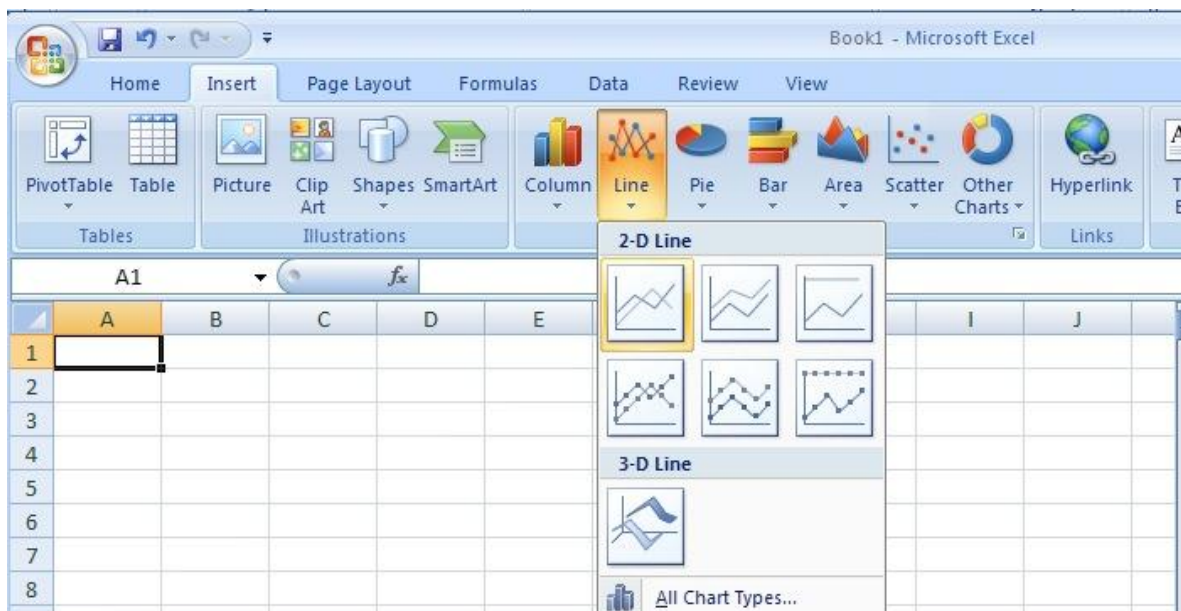


- In the Import XML dialog box, browse to and select the volumeInfo.xml file, then click **Import**.

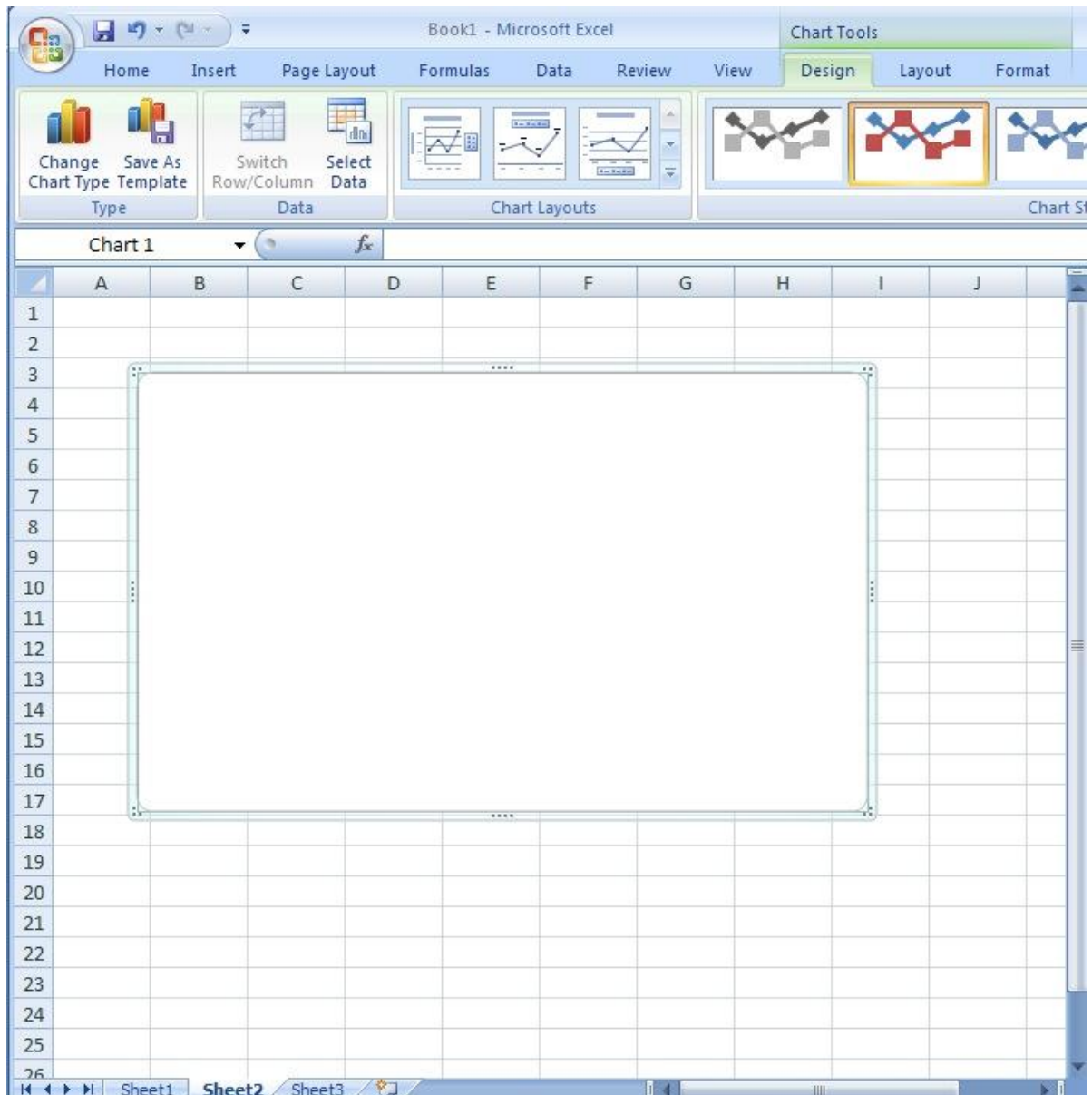
- Microsoft Excel displays your log archive data in the two columns. Delete the last row, which has a record count of 0. This row represents the latest date partition created, and the log archive server has not updated the record count for that day.

	name	recordCount	C	D	E	F	G	H	I	J
34	20091114	6393289								
35	20091115	3521544								
36	20091116	7123383								
37	20091117	7612231								
38	20091118	9902271								
39	20091119	7501510								
40	20091120	7327631								
41	20091121	6230005								
42	20091122	3627713								
43	20091123	10041947								
44	20091124	8479611								
45	20091125	8845578								
46	20091126	11973420								
47	20091127	9250854								
48	20091128	9037782								
49	20091129	10211818								
50	20091130	0								
51										

- Navigate to Sheet2.
- On the **Insert** tab, in the **Charts** group, click **Line**.
- Under **2-D Line**, click **Line**. Use the Excel screen tips to ensure you select the **Line** option and not any of the **Stacked Line** or **Line with Markers** options. Screen tips display the chart names if you rest the mouse pointer over any of the chart choices.



14. Microsoft Excel displays the following empty chart.



15. Right-click the chart and click **Select Data**.
16. Delete all text in the **Chart data range** field except =.
17. To graph the data in Sheet1, navigate to Sheet1 while leaving the Select Data Source dialog box open and select all data in Column B, from B2 down.

18. Click **OK**.

The screenshot shows the 'Select Data Source' dialog box in Microsoft Excel. The dialog box is positioned over a spreadsheet with the following data:

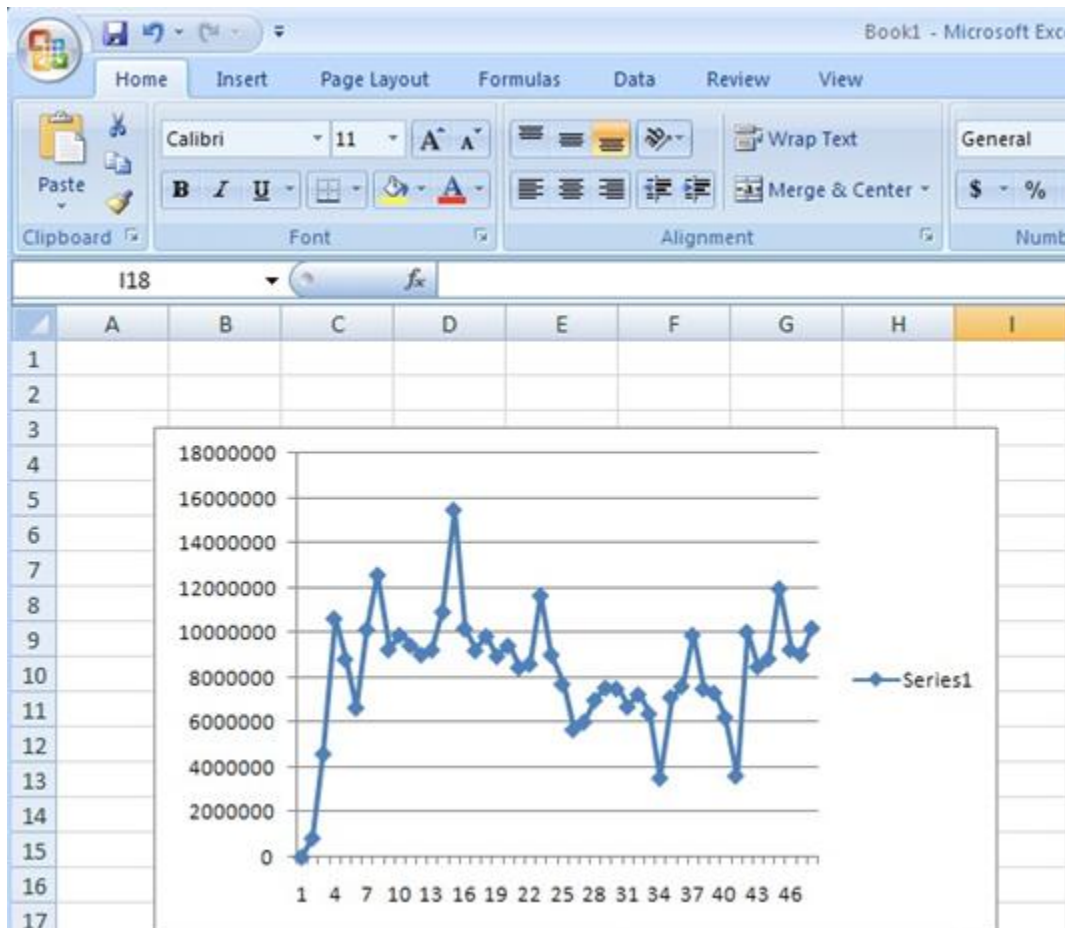
name	recordCount
20091013	660
20091014	844620
20091015	4600788
20091016	10639001
20091017	8822296
20091018	6659418
20091019	10146839
20091020	12582288
20091021	9257120
20091022	9901361
20091023	9437431
20091024	9020320
20091025	9236535
20091026	10936116
20091027	15487866
20091028	10188345
20091029	9212538
20091030	9850911
20091031	8956178
20091101	9426167
20091102	8453547
20091103	8610515
20091104	11665909
20091105	9022844
20091106	7718041

The 'Select Data Source' dialog box has the following fields and controls:

- Chart data range:** `=Table1[recordCount]`
- Switch Row/Column:** A button with arrows indicating the ability to switch between row and column data.
- Legend Entries (Series):** A list box with buttons for 'Add', 'Edit', 'Remove', and arrows for moving items up and down.
- Horizontal (Category) Axis Labels:** A list box with an 'Edit' button.
- Hidden and Empty Cells:** A checkbox at the bottom left.
- OK** and **Cancel** buttons at the bottom right.

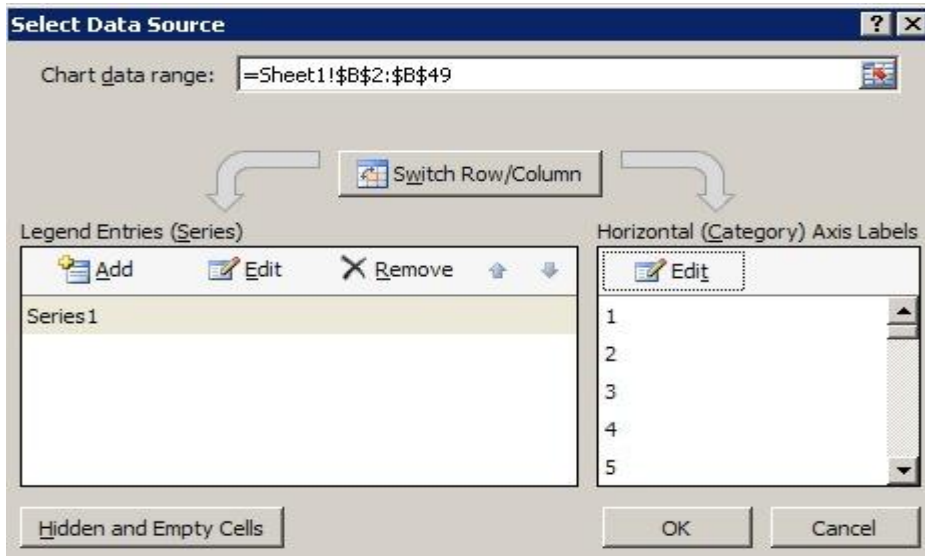


- To modify the chart so that the horizontal axis displays the dates, right-click **Series 1** and select **Delete**.

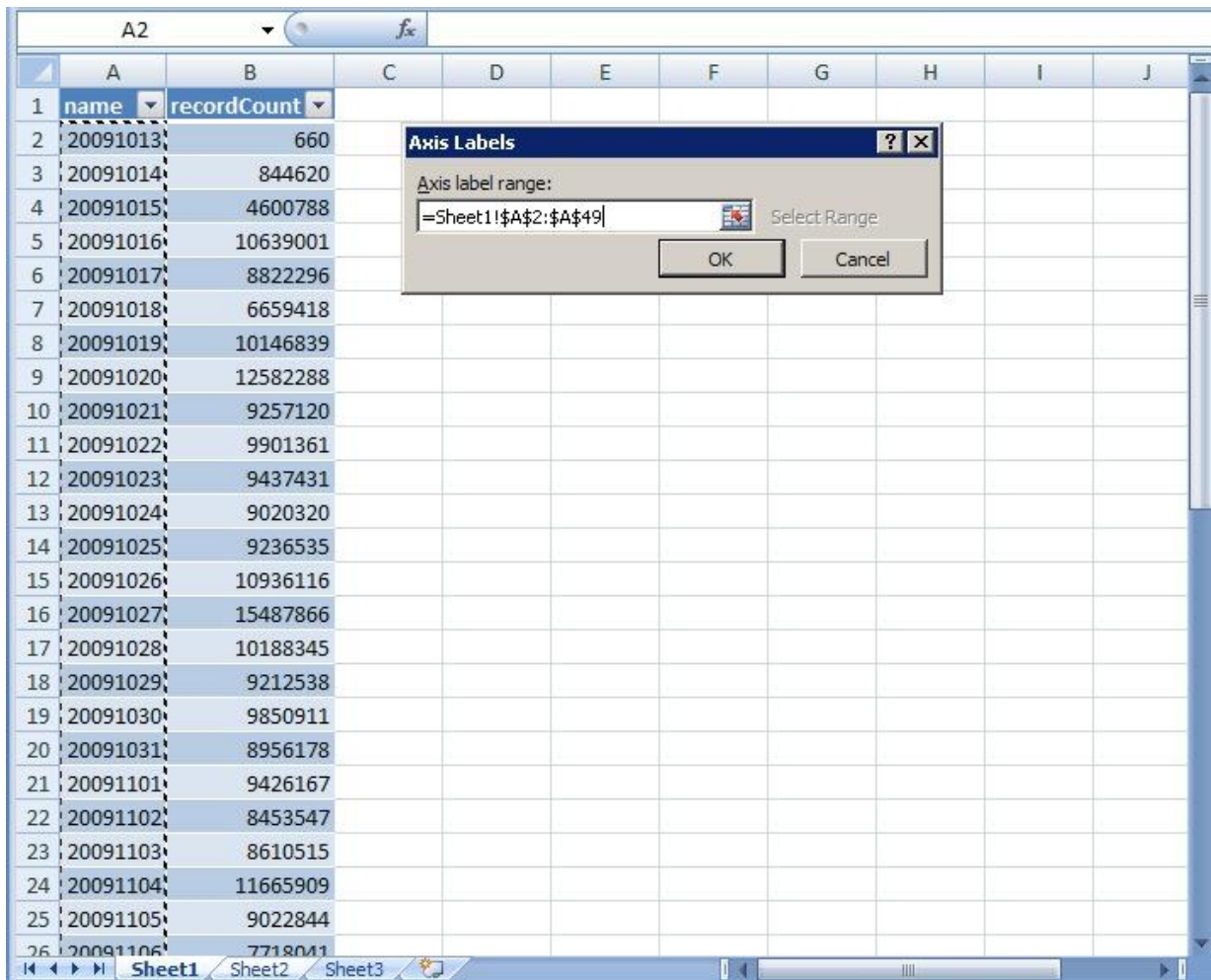


- Right-click the chart and click **Select Data**.

21. Under **Horizontal (Category) Axis Labels**, click **Edit**.



22. Leaving the Axis Labels dialog box open, navigate to Sheet1 and select all dates in Column A.

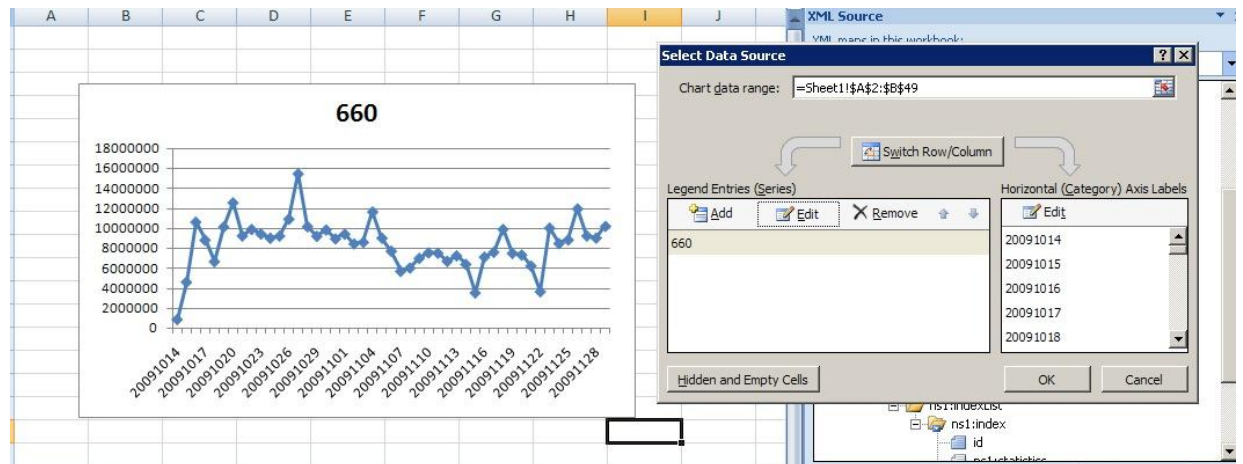


1	name	recordCount
2	20091013	660
3	20091014	844620
4	20091015	4600788
5	20091016	10639001
6	20091017	8822296
7	20091018	6659418
8	20091019	10146839
9	20091020	12582288
10	20091021	9257120
11	20091022	9901361
12	20091023	9437431
13	20091024	9020320
14	20091025	9236535
15	20091026	10936116
16	20091027	15487866
17	20091028	10188345
18	20091029	9212538
19	20091030	9850911
20	20091031	8956178
21	20091101	9426167
22	20091102	8453547
23	20091103	8610515
24	20091104	11665909
25	20091105	9022844
26	20091106	7718041

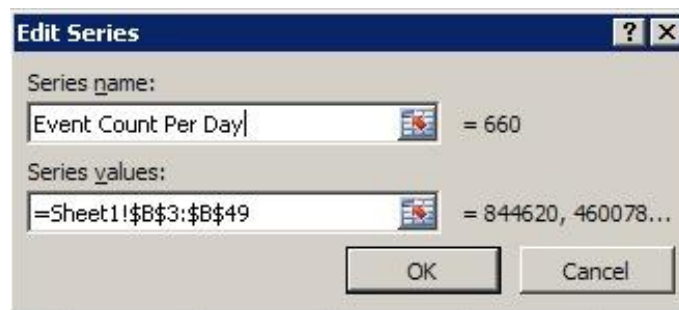


23. Click OK. Microsoft Excel displays the dates as the horizontal axis of the chart.

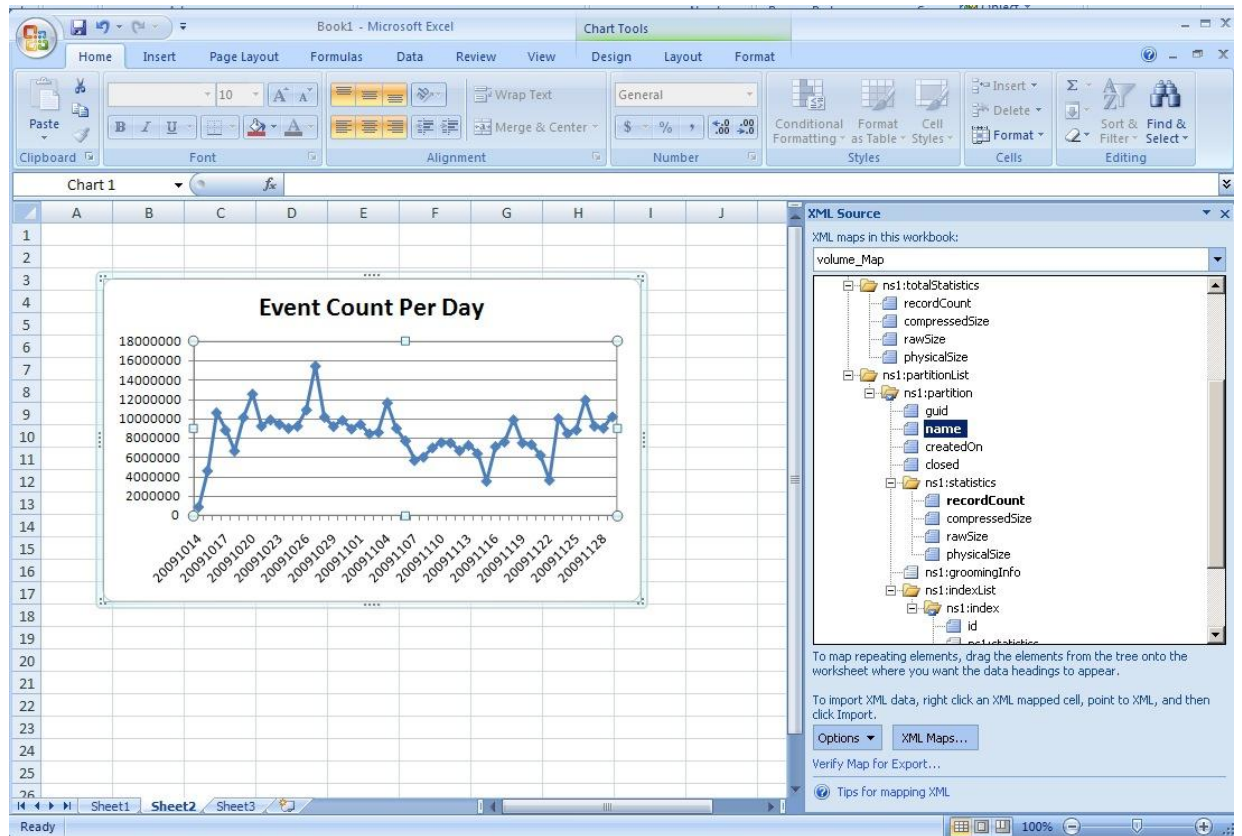
24. Change the Series name. In this example, the name is 660. Select 660 and click Edit.



25. Change the **Series name** to Event Count Per Day. Ensure the **Series values** field includes all cells in Column B of Sheet1, including the first data cell. Click **OK**, and then click **OK** again.



26. The chart shows the event count on the Y axis and dates on the X axis. You can also change the format or resize the chart.



27. Save the Microsoft Excel file.

## About NetIQ

NetIQ is an enterprise software company with relentless focus on customer success. Customers and partners choose NetIQ to cost-effectively tackle information protection challenges and IT operations complexities. Our portfolio of scalable, automated management solutions for Security & Compliance, Identity & Access, and Performance & Availability and our practical, focused approach to solving IT challenges help customers realize greater strategic value, demonstrable business improvement and cost savings over alternative approaches.

For more information, visit [NetIQ.com](http://NetIQ.com).

### Worldwide Headquarters

1233 West Loop South, Suite 810  
Houston, Texas 77027 USA  
Worldwide: 713.548.1700  
N. America Toll Free: 1.888.323.6768  
info@netiq.com  
NetIQ.com

### For a complete list of our offices

in North America, Europe, the  
Middle East, Africa, Asia-Pacific  
and Latin America, please visit  
[www.netiq.com/contacts](http://www.netiq.com/contacts).