HNAS File System Auditing Guide

FE-92HNAS072-03
February 2020

Copyrights and licenses

© 2019 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara Corporation (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara Corporation at https://support.hitachivantara.com/en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara Corporation.

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals to access relevant data; and

2. Verifying that data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, IBM, Lotus, MVS, OS/390, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft Corporate Logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Contents

Introduction

HNAS file system auditing can be used to record audit log events for certain operations performed by clients over the SMB and NFSv3 protocols.

By default, when file system auditing is enabled, access to the audited file system is only allowed for these two protocols. However, access by clients using other protocols like NFSv2, can optionally be allowed. When such access is allowed, access to file system objects through these protocols is not audited.

> When NFSv3 is audited, this only applies to exports directly associated with a filesystem. If the filesystem is accessed through a namespace, NFSv3 access is still allowed, but is not audited.

File system audit events are saved in the Windows Event Log File format (".evt"). Events can also be read using the EventLog Remoting Protocol [MS-EVEN].

Note: The links provided in this document to Microsoft information resources are provided for information and reference only and are not maintained or supported by Hitachi Vantara.

Configuration

File system configuration

File system audit logging is performed and controlled on a per file system basis.

To enable file system auditing on a file system, use the `filesystem-audit` console command or, in the NAS Manager, navigate to **File Services > File Systems Audit Policies**.

CLI Example

```
evs-select 1 filesystem-audit add -s 50MB auditfilesystem
```

> Client access for both SMB and NFSv3 is audit logged when enabled.

EVS configuration

If audit records are to be collected by a third party service or viewed with Windows Event Viewer, this must be enabled with the `audit-log-consolidated-cache` console command. For example:

```
evs-select 1 audit-log-consolidated-cache add -s 50MB auditfilesystem
```

When events are viewed with Windows Event Viewer, NAS file system auditing events are shown in the FS event log.

> **Note:** Events for any user who is a member of the Audit Service Accounts local group are excluded from the audit log. Adding the third party auditing software user to this group results in a small but measurable performance gain.

SMB auditing

Auditing of SMB is based on the open and close operations. The events logged by HNAS follow the formats described by Microsoft for object access auditing. For a concise list, see here. For further information, see here.

The following sections describe the supported events and variations from the equivalent Windows events.

560 Object Open

This event is logged when a client requests to open a file or directory. Reference documentation is here.

The HNAS event includes an Information field which will contain the string `Create` if the object was newly created by the open.

Format:

```
Object Open:
    Object Server:      %s
    Object Type: %s
    Object Name: %s
    Handle ID:   %s
    Process ID:  %s
    User Name:   %s
    Domain:      %s
    Logon ID:    %s
    Accesses:    %s
    Information: %s
```

562 Handle Closed

This event is logged when a handle is closed. This event will have been preceded by a `560 Object Open` or `563 Object Open for Delete` event. `Object Open` and `Handle Closed` events can be correlated using the combination of Process ID and Handle ID.

Reference documentation is here.

The HNAS event includes additional information fields:

- `Rename` displays the new pathname after an object has been renamed.
- `Operation` can include one or more of the following:
    - `Read`
    - `Write`
    - `Security`
    - `Audit`

  These show the operations that have occurred on the object between open and close. If multiple operations are displayed, the names will be space separated. `Security` denotes a modification to the object's security descriptor. `Audit` denotes a modification to the SACL part of the security descriptor (the SACL contains the audit configuration for the object).

- `Bytes Read` indicates how many bytes were read between open and close. If reads were hardware-accelerated, the string `Unknown` is displayed instead.

Format:

```
Handle Closed:
    Object Server:      %s
    Handle ID:    %s
    Process ID:   %s
    Rename:       %s
    Operations:   %s
    Bytes Read:   %s
```

563 Object Open for Delete

This event may be logged instead of `560 Object Open` when a client opens an object. This event is logged if any of the following are true:

- An object is opened with `delete on close` specified
- An object is unlinked using `SMB_COM_DELETE_DIRECTORY` or `SMB_COM_DELETE`
- An object is renamed using `SMB_COM_RENAME`

Reference documentation is here.

Format:

```
Object Open For Delete:
    Object Server:      %s
    Object Type:  %s
    Object Name:  %s
    Handle ID:    %s
    Process ID:   %s
    User Name:    %s
    Domain:       %s
    Logon ID:     %s
    Accesses:     %s
```

564 Object Deleted

This event is logged when a file or directory is deleted. Reference documentation is here.

Format:

```
Object Deleted:
    Object Server:      %s
    Handle ID:    %s
    Process ID:   %s
```

SMB examples

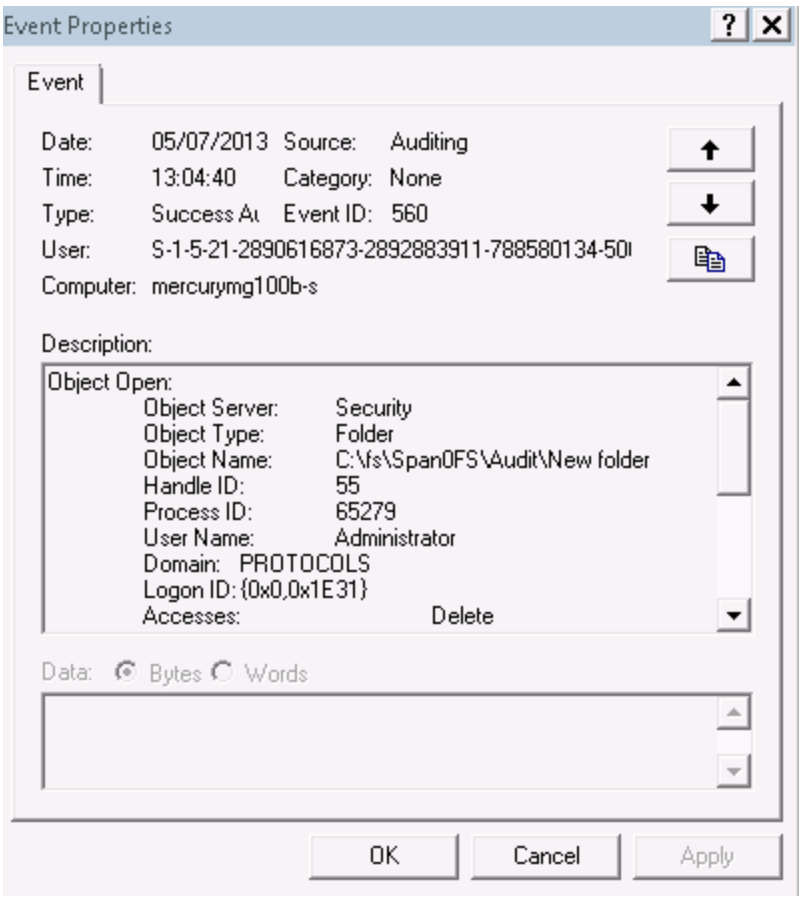
Create or open a directory

When a directory is opened or created, a `560 Object Open` event is logged. If the directory was created, the Information field includes `Create`.

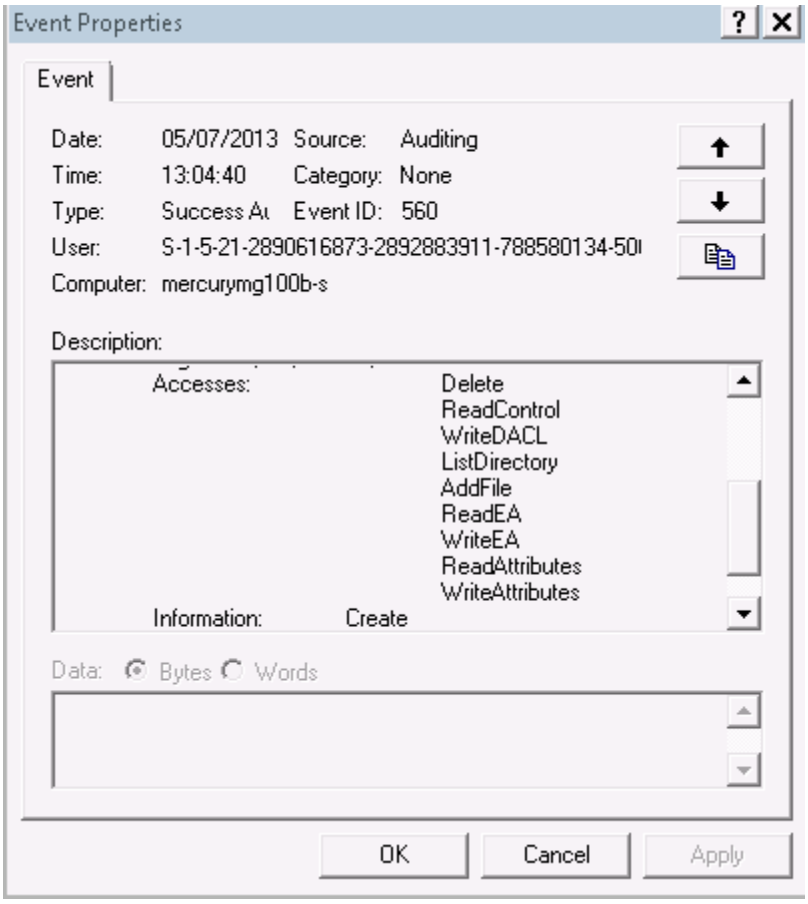
Example viewed from `audit-log-show`:

```
560 AuditSuccess 2013-07-05 13:04:53 Auditing (SID S-1-5-21-2890616873-2892883911-
788580134-500): Object Open:, Object Server:Security, Object Type:Folder, Object
Name:C:\fs\Span0FS\Audit\New folder, Handle ID:68, Process ID:65279, User
Name:Administrator, Domain:PROTOCOLS, Logon ID:{0x0,0x1E31},
Accesses:Delete|ReadAttributes, Information:
```

Example viewed from Windows Event Viewer (part 1):



Example viewed from Windows Event Viewer (part 2):



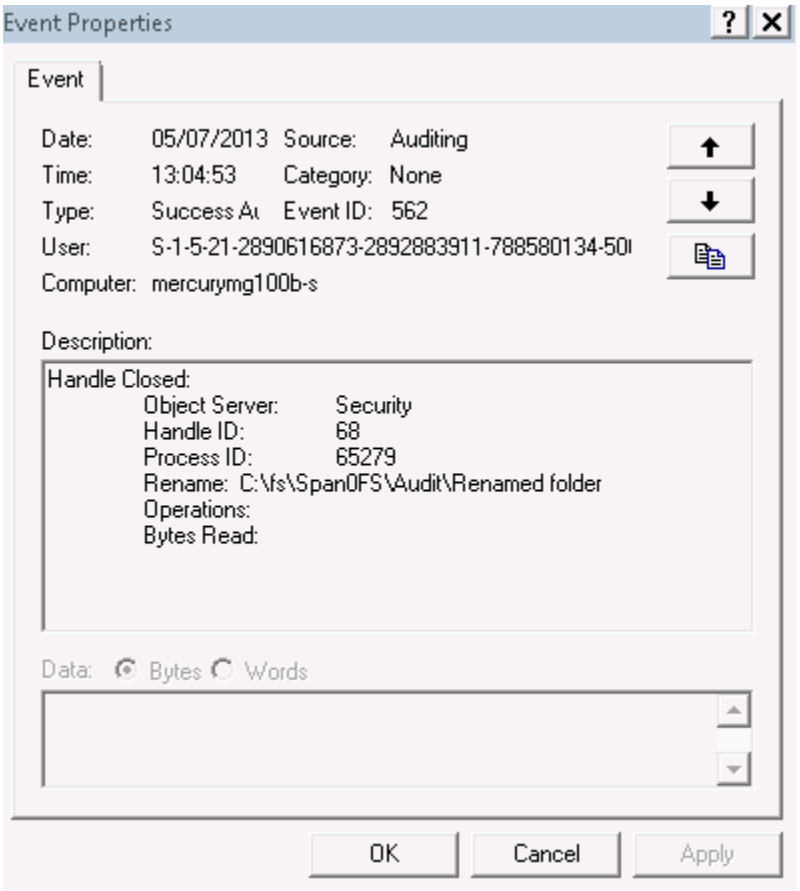
Rename a directory

When a directory which was previously opened is renamed, a `562 Handle Closed` event is logged and the new path will be shown in the Rename additional information field.

Example viewed from `audit-log-show`:

```
562 AuditSuccess 2013-07-05 13:04:53 Auditing (SID S-1-5-21-2890616873-2892883911-
788580134-500): Handle Closed:, Object Server:Security, Handle ID:68, Process
ID:65279, Rename:C:\fs\Span0FS\Audit\Renamed folder, Operations:, Bytes Read:
```

Example viewed from Windows Event Viewer:



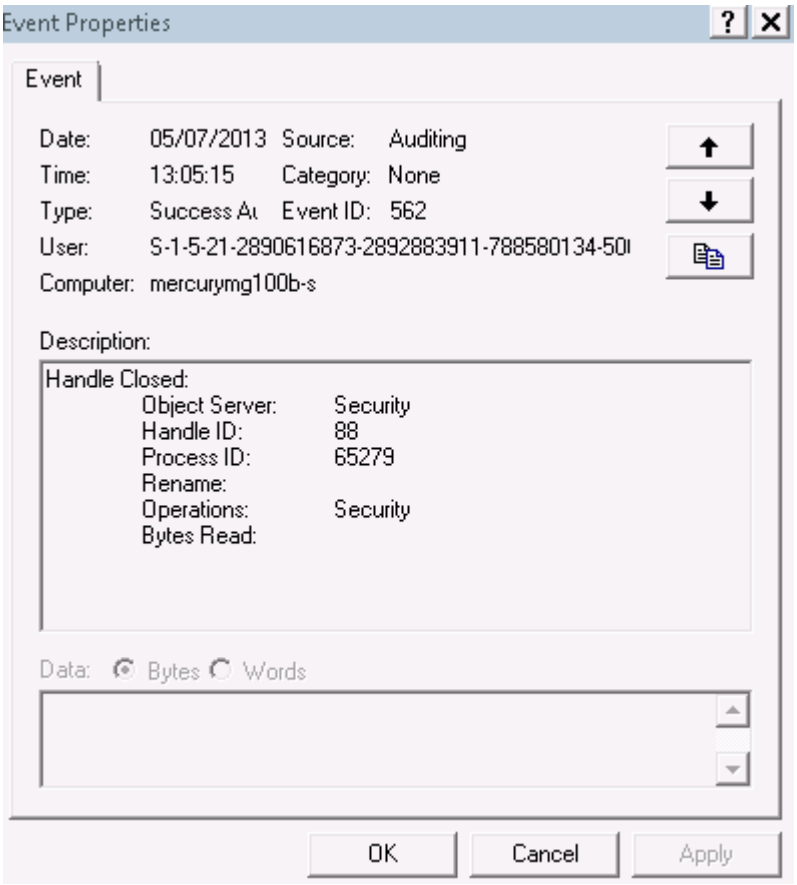
Change security on a directory

When the security is modified on a directory, the `562 Handle Closed` event includes `Security` in the Operations additional information field.

Example viewed from `audit-log-show`:

```
562 AuditSuccess 2013-07-05 13:05:15 Auditing (SID S-1-5-21-2890616873-2892883911-
788580134-500): Handle Closed:, Object Server:Security, Handle ID:88, Process
ID:65279, Rename:, Operations:Security, Bytes Read:
```

Example viewed from Windows Event Viewer:



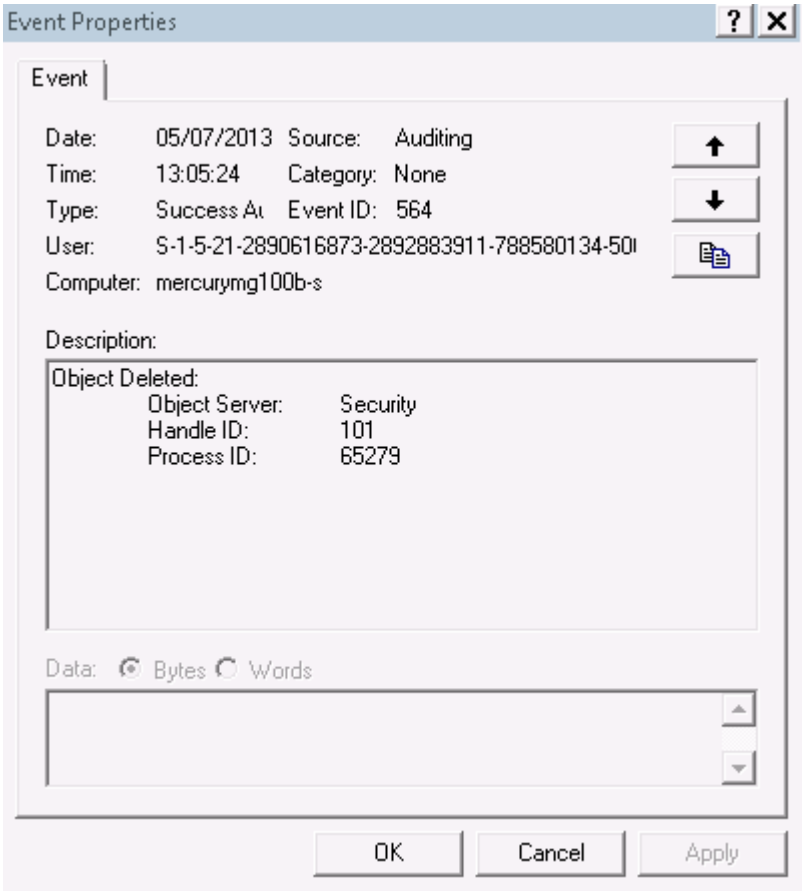
Delete a directory

When a directory is deleted, a `564 Object Deleted` event is logged.

Example viewed from `audit-log-show`:

```
564 AuditSuccess 2013-07-05 13:05:24 Auditing (SID S-1-5-21-2890616873-2892883911-
788580134-500): Object Deleted:, Object Server:Security, Handle ID:101, Process
ID:65279
```

Example viewed from Windows Event Viewer:



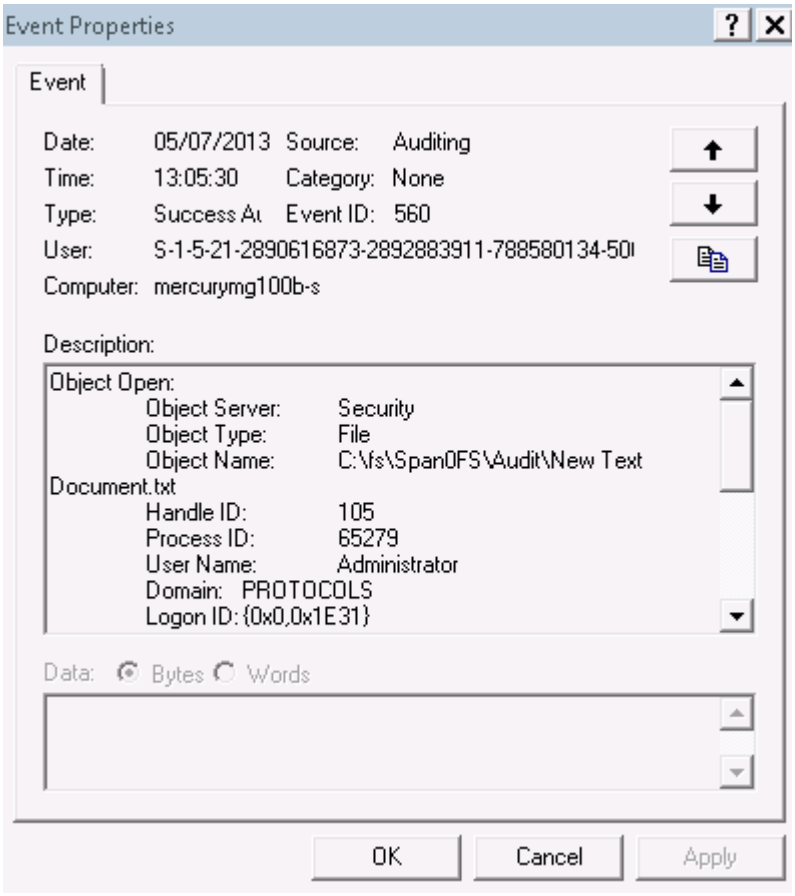
Create or open a file

When a file is opened or created, a `560 Object Open` event is logged. If the file was created, the Information field will include `Create`.

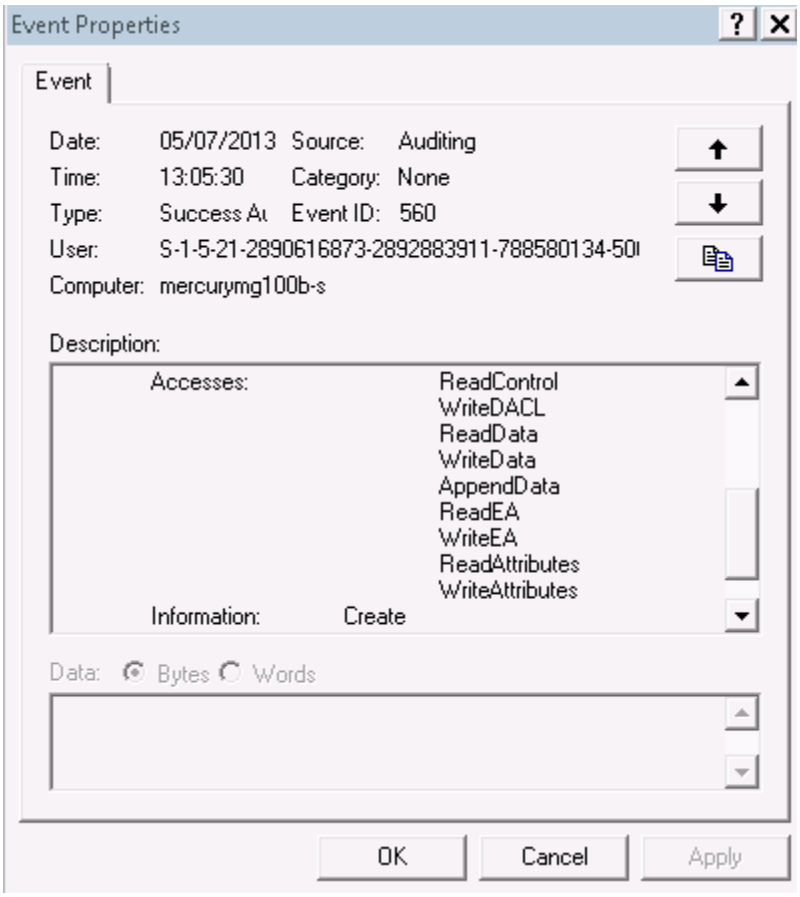
Example viewed from audit-log-show:

```
560 AuditSuccess 2013-07-05 13:05:30 Auditing (SID S-1-5-21-2890616873-2892883911-
788580134-500): Object Open:, Object Server:Security, Object Type:File, Object
Name:C:\fs\Span0FS\Audit\New Text Document.txt, Handle ID:105, Process ID:65279,
User Name:Administrator, Domain:PROTOCOLS, Logon ID:{0x0,0x1E31},
Accesses:ReadControl|WriteDACL|ReadData|WriteData|AppendData|ReadEA|WriteEA|ReadAtt
ributes|WriteAttributes, Information:Create
```

Example viewed from Windows Event Viewer (part 1):



Example viewed from Windows Event Viewer (part 2):



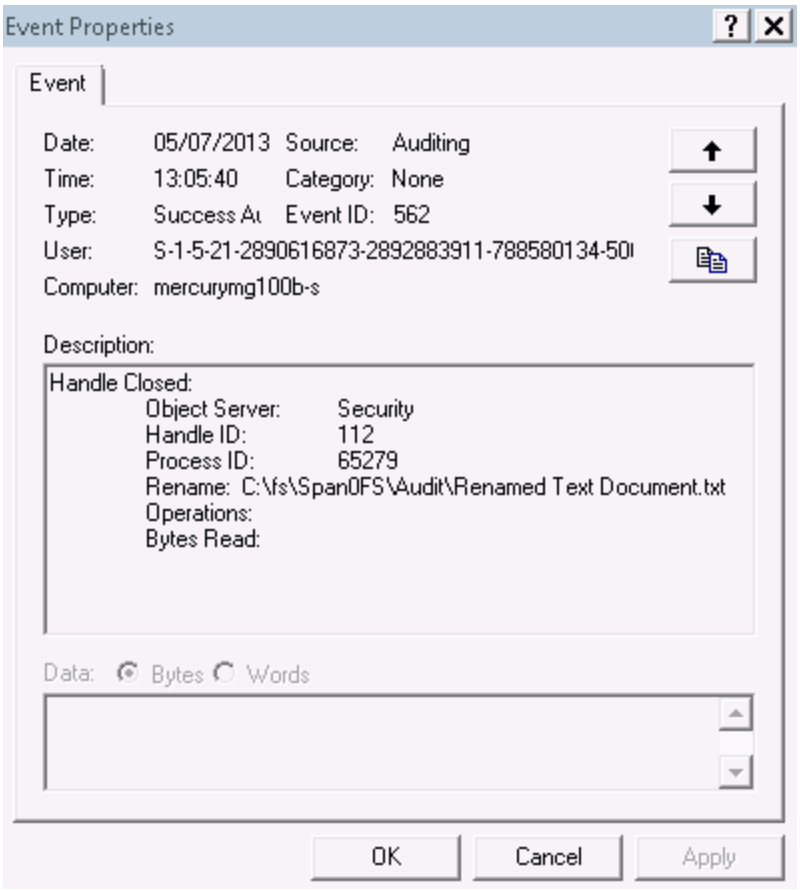
Rename a file

When a file which was previously opened is renamed, a `562 Handle Closed` event is logged, and the new path will be shown in the Rename additional information field.

Example viewed from `audit-log-show`:

```
562 AuditSuccess 2013-07-05 13:05:40 Auditing (SID S-1-5-21-2890616873-2892883911-
788580134-500): Handle Closed:, Object Server:Security, Handle ID:112, Process
ID:65279, Rename:C:\fs\Span0FS\Audit\Renamed Text Document.txt, Operations:, Bytes
Read:
```

Example viewed from Windows Event Viewer:



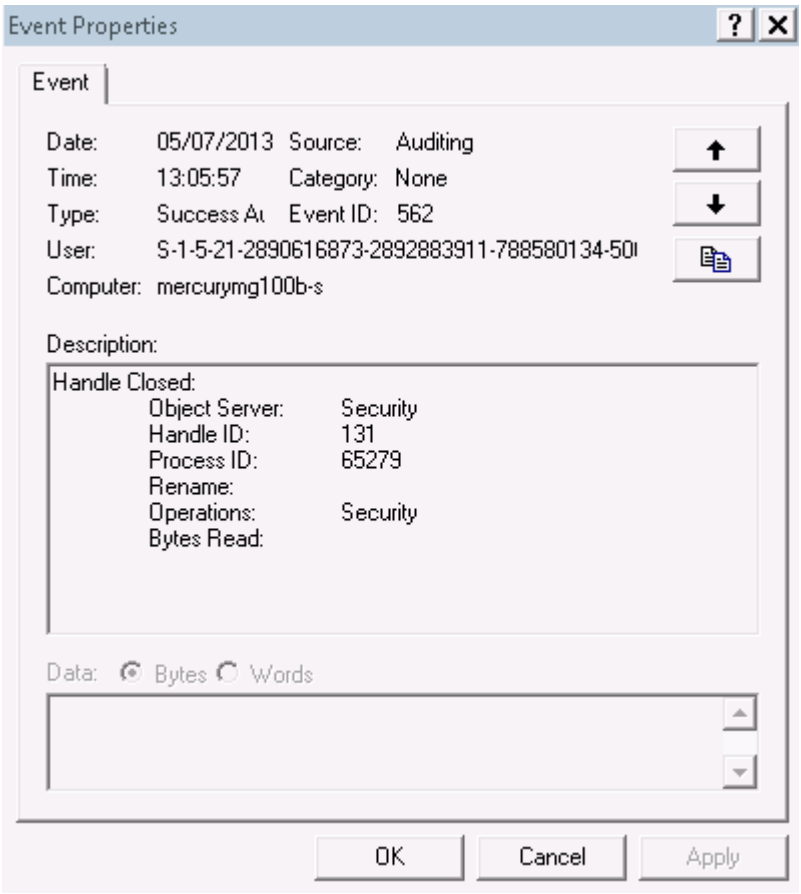
Change security on a file

When the security is modified on a file the 562 Handle Closed event will include Security in the Operations additional information field.

Example viewed from audit-log-show:

```
562 AuditSuccess 2013-07-05 13:05:57 Auditing (SID S-1-5-21-2890616873-
2892883911-788580134-500): Handle Closed:, Object Server:Security,
Handle ID:131, Process ID:65279, Rename:, Operations:Security, Bytes
Read:
```

Example viewed from Windows Event Viewer:



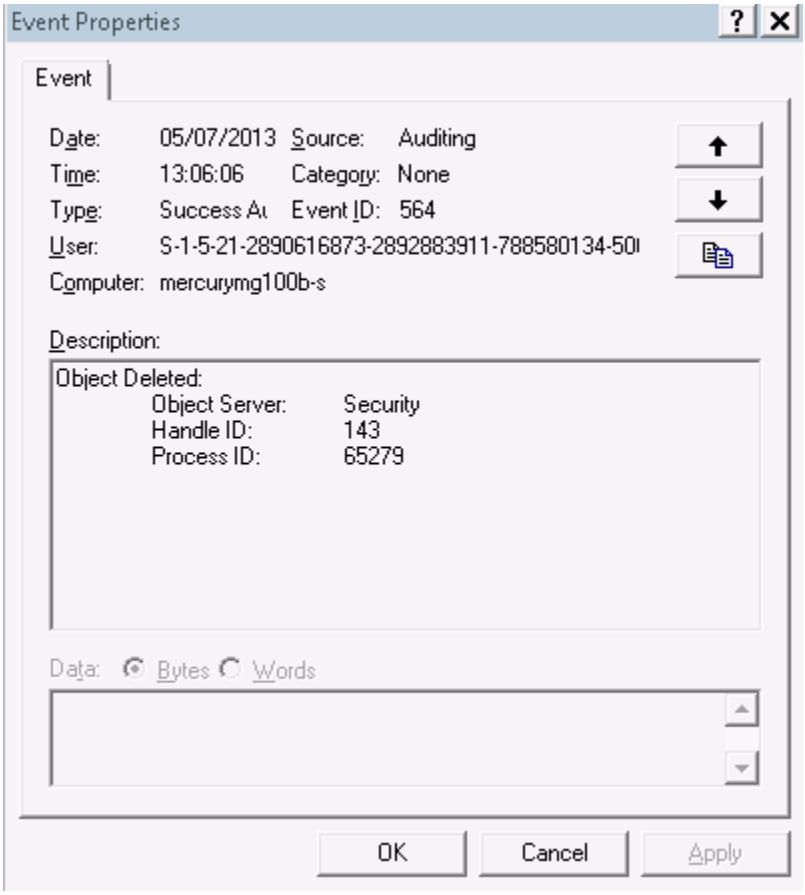
Delete a file

When a file is deleted, a `564 Object Deleted` event is logged.

Example viewed from `audit-log-show`:

```
564 AuditSuccess 2013-07-05 13:06:06 Auditing (SID S-1-5-21-2890616873-2892883911-
788580134-500): Object Deleted:, Object Server:Security, Handle ID:143, Process
ID:65279
```

Example viewed from Windows Event Viewer:



NFSv3 auditing

As NFSv3 is a stateless protocol and does not have event operations, auditing checks must be performed on each I/O operation. This can be costly in terms of system performance.

To disable NFSv3 auditing, use the `-p` option with the `filesystem-audit` command and omit the NFSv3 parameter.