INTEGRATION WITH THIRD PARTY SIEM SYSTEMS

TECHNICAL ARTICLE

November 2012

Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from NetWrix Corporation of any features or functions discussed. NetWrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice.

NetWrix is a registered trademark of NetWrix Corporation. The NetWrix logo and all other NetWrix product or service names and slogans are registered trademarks or trademarks of NetWrix Corporation. Active Directory is a trademark of Microsoft Corporation. All other trademarks and registered trademarks are property of their respective owners.

Disclaimers

This document may contain information regarding the use and installation of non-NetWrix products. Please note that this information is provided as a courtesy to assist you. While NetWrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-NetWrix product and contact the supplier for confirmation. NetWrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-NetWrix products.

Table of Contents

1. INTRODUCTION

1.1 Overview

If your organization is already using a third-party Security Information and Event Management (SIEM) solution, NetWrix products composing the NetWrix Active Directory Change Reporter pack can help protect these investments by integrating with major SIEM systems and letting you manage audit data in your usual way, but with improved performance and increased reliability of the collected audit data.

NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter, and NetWrix Exchange Change Reporter can integrate with all major SIEM solutions, including Microsoft System Center Operations Manager (SCOM), RSA enVision®, Arc-Sight® Logger™, Novell® Sentinel™, NetIQ® Security Manager™, IBM Tivoli® Security Information and Event Manager™, and many others.

When integration with SIEM products is enabled, a custom Windows event log is created called NetWrix Change Reporter. This event log will generate events for each detected change. You can configure custom processing rules, alerts and reports in your SIEM solution to track these events.

This article contains the NetWrix Change Reporter events specification and explains how to enable the integration.

1.2 How This Guide is Organized

This section explains how this guide is organized and provides a brief overview of each chapter.

- Chapter 1 Introduction the current chapter. The chapter explains the purpose of this document, defines its audience and explains its structure.
- Chapter 2 Enabling Integration explains how to enable integration with third-party SIEM solutions.
- Chapter 3 Event Types provides a description of event types and their properties.
- Chapter 4 Sample Events Descriptions provides descriptions of sample events.
- Appendix: Related Documentation provides a list of documents available to support integration with Third Party SIEM solutions.

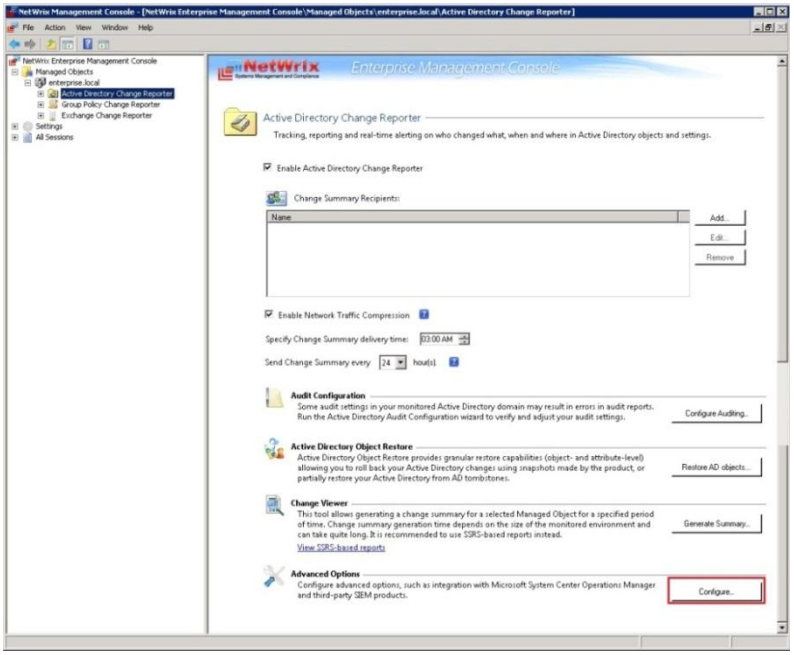
2. ENABLING INTEGRATION

The procedure below provides instructions on how to enable integration with third-party SIEM solutions by the example of NetWrix Active Directory Change Reporter.

Procedure 1. To enable integration with third-party SIEM solutions

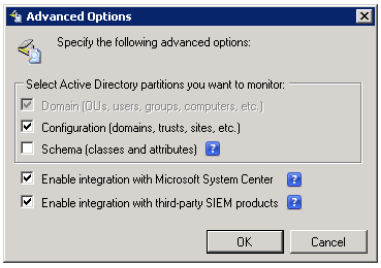
1. In NetWrix Enterprise Management Console, navigate to **Managed Objects** → **<Managed_Object_name>** → <**NetWrix module**>.
2. In the right pane, click the **Configure** button next to **Advanced Options**:

Figure 1: The Product Settings Page



3. In the Advanced Options dialog, select the **Enable integration with Microsoft System Center** option to integrate the product with Microsoft SCOM, or the **Enable integration with third-party SIEM products** option to integrate the product with a different SIEM solution, and click **OK** to save the changes:

Figure 2: Advanced Options Dialog



Note: To integrate the product with Microsoft SCOM, you need to install NetWrix SCOM Management Pack for Change Reporter Suite. This solution allows SCOM to capture events written by NetWrix products into a dedicated event log and generate corresponding reports and alerts. For a detailed description of the alerts triggered by SCOM alerting rules, refer to the following specifications: NetWrix Active Directory Change Reporter SCOM Alerts Specifications and NetWrix Exchange Change Reporter SCOM Alerts Specifications.

3. EVENT TYPES

There are two categories of the NetWrix Change Reporter events:

- *Audit Events:* contain the information on data collection.
- *General Events*: contain the information on errors that occurred during data collection, messages on successful data collection, and other general data.

Table 1: Event Properties

Property	Audit Event	General Event
Source	Product name: • NetWrix Active Directory Change Reporter • NetWrix Group Policy Change Reporter • NetWrix Exchange Change Reporter	
Category	Audit (id=1)	General (id=2)
Level	Success Audit / Failure Audit	Information / Warning / Error
ID	1001 – 1008	2001 - 2013

3.1 Audit Events

The table below provides a description of the audit events sorted by their ID.

Table 2: Events Description

ID	Name	Description	Change type string in description	Change detail string in description	Source	
					Active Directory Change Reporter Exchange Change Reporter	Group Policy Change Reporter
1001	Add	Object added	Added	-	+	+
1002	Remove	Object removed	Removed	-	+	+
1003	Modify	Single-valued string was modified. Empty values reported as empty quoted strings in description templates	Modified	< attribute > changed from "<old value>" to "<new value>"	+	+
1004	Modify by Events	Information extracted from Windows Event Log. (e.g. user account enabled/disabled, account locked/unlocked	Modified	< attribute >	+	

1005	Value Added	Value was added to the multi-valued attribute (e. g. a new member was added to a group)	Modified	<attribute>: Added: "<new value>"	+	
1006	Value Removed	Value was removed from the multi-valued attribute, (e. g. a member was removed from a group)	Modified	< attribute >: Removed: "<old value>"	+	
1007	Modified and Reverted Back	Attribute was modified and then rolled back to its previous value. Intermediate values are unknown.	Modified	< attribute >: Modified and Reverted back	+	
1008	Access	Access to file system objects (e.g. successful or failure file reads; failure attempts to access a folder or share)	Read	-		

The insertion strings, described in Table 3: below, are displayed in the **Details** tab of the **Event Properties** dialog box:

Figure 3: Event Properties

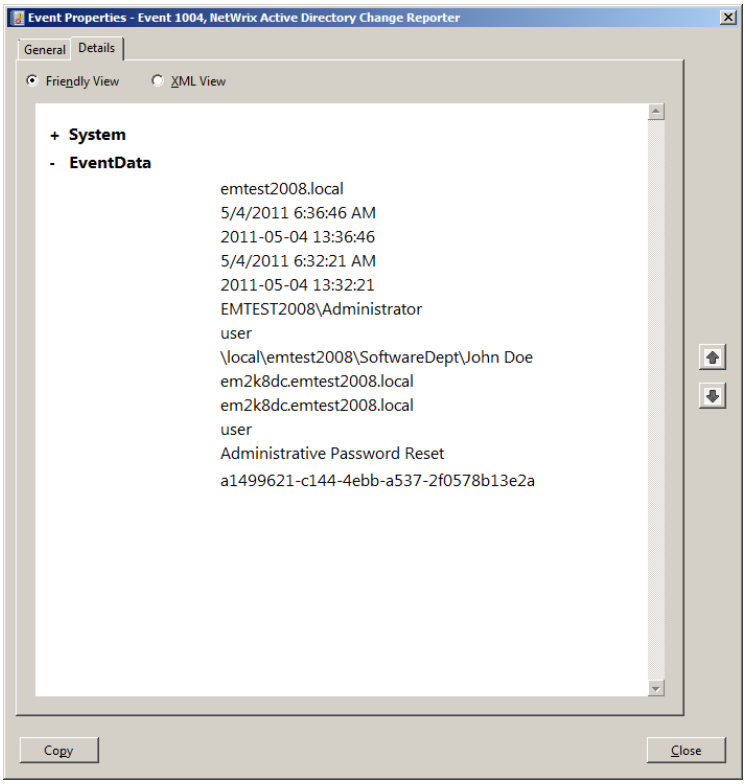


Table 3: Insertion Strings Details

String number	Generic Content	Event Source Specific		
		ADCR	ECR	GPCR
Event Source Name	Product name	NetWrix Active Directory Change Reporter	NetWrix Exchange Change Reporter	NetWrix Group Policy Change Reporter
1	Managed Object	Domain	Domain	Domain
2	When detected (local)[1]	-//-	-//-	-//-
3	When detected (UTC)[2]	-//-	-//-	-//-
4	When changed (local)	-//-	-//-	-//-
5	When changed (UTC)	-//-	-//-	-//-
6	The name of the user who made the change (DOMAIN\user)	-//-	-//-	-//-
7	Object type	AD object type (computer/user/ group, etc.)	AD object type (computer/user/ group, etc.)	“Policy”
8	Object path	AD path: \local\amdom\ Users\testUser1	AD path: \local\amdom\ Users\testUser1	\zone\domain\ GPO Display Name\Path
9	The name of the server where NetWrix software that detected the change is installed	-//-	-//-	-//-
10	The server where the change was made (DC, file server, etc.)	-//-	-//-	-//-
11	Custom field	Depends on type (see below)	Schema-based name, e.g. msExchExchange Server, msExchRpcHttpVi rtualDirectory	GPO Display Name
12	Internal name of the attribute that was changed	-//-	-//-	GPO setting attribute name (currently is equivalent to [13], but should be changed to a real internal name when Group Policy Change Reporter provides this information)
13	Display name of the attribute that was changed	-//-	-//-	Friendly attribute name (GPO setting attribute

				name)
14	The previous value of the attribute (or removed values if a multi-valued attribute). Can be empty.	-//-	-//-	-//-
15	The current value of the attribute (or added values if a multi-valued attribute). Can be empty.	-//-	-//-	-//-
16	Object GUID	AD object GUID	AD object GUID	Group Policy object GUID
17	Custom field	n/a	n/a	Group Policy Change Type: 1 - policy added 2 - policy removed 3- policy modified

[1] Local time written using the default locale format (for example 03/16/2011 6:37:43 PM)
[2] UTC value written using the SQL date format (MM-DD-YYYY hh:mm:ss)

3.1 1. Reporter Specific Information

This section provides detailed information on the Audit Events specific to each NetWrix change reporter.

The following Audit Events information is product-specific:

- **Active Directory Change Reporter**
  Custom field (insertion string #11) values:

Object Type	Value
group	The complete group type name, such as: - Distribution Domain Local Group - Distribution Global Group - Distribution Universal Group - Security Domain Local Group - Security Global Group - Universal Security Group

- **Group Policy Change Reporter**
  The Add/Remove events (Event ID 1001 or 1002) are generated only when a Group Policy object is added or removed. Changes to policy settings are always displayed as the Modified event (ID 1003).

3.2 General Events

The following table provides a description of the general events sorted by their ID.

Table 4: Events Description

ID	Name	Description
2001	Error	Error while processing Managed Object.
2002	Warning	Warning while processing Managed Object.
2010	Information	Audit data collection started.
2011	Information	Audit data collection completed successfully.
2012	Warning	Audit data collection completed with warnings.
2013	Error	Audit data collection completed with errors.

The following table describes the insertion strings displayed on the Details tab of the Event Properties dialog:

Table 5: Insertion Strings Details

String number	Description	Event ID
1	Managed Object name (e.g. domain, computer collection, etc.)	All
2	The name of the server where NetWrix software is installed	All
3	User account used for data collection	All
4	The error location (e.g. DC, server name, domain)	2001/2002
5	The error or warning message text	2001/2002

General events are recorded to the NetWrix Change Reporter event log to reflect the progress of a Managed Object processing. The following table explains the event recording sequence:

Table 6: Event Recording Sequence

Step Name	Generated Events
Data collection start	Event 2010, one for each Managed Object.
Data processing	Events 2001 and 2002, if some errors or warnings occurred during data processing.
Data collection completed	One of the following events: 2011/2012/2013, representing the status of the data collection operation – e.g. *successful*, *with warnings* or *with errors*.

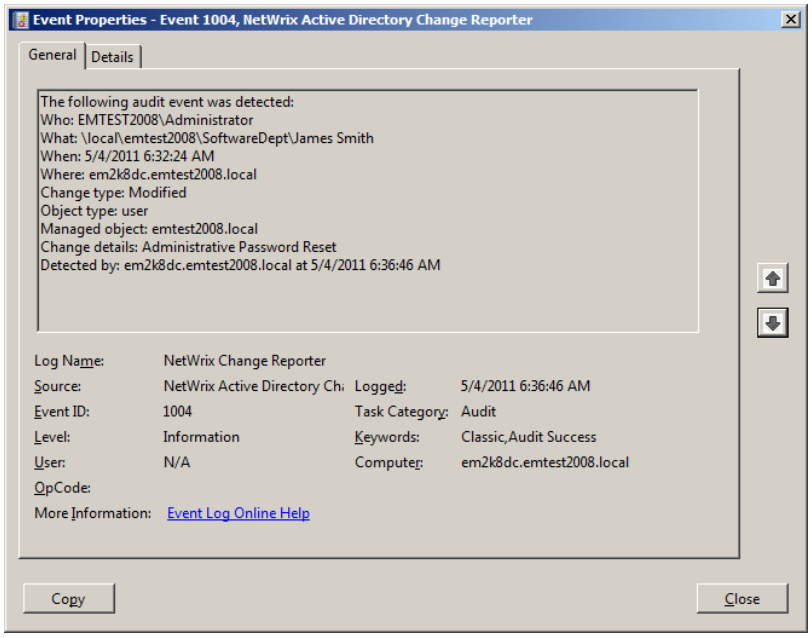
4. SAMPLE EVENTS DESCRIPTIONS

4.1 Audit Events

General Tab

The Event Properties General tab shows the event description in the upper grid and the general properties information below the grid:

Figure 4: General Tab



The sample descriptions for the NetWrix Active Directory Change Reporter events are as follows:

Event ID: 1001

```
Who: system
What: \local\amdom\Configuration\Sites\Default-First-Site-
Name\Servers\MINV2\NTDS Settings\a8f9388b-89ff-41f7-83e8-cb1fdbd856bc
When: 03/17/2011 7:17:26 PM
Where: unknown
Change type: Added
Object type: nTDSConnection
Managed object: amdom.local
Detected by: amik.amdom.local at 03/17/2011 10:56:26 PM
```

Event ID: 1002

```
Who: system
What: \local\amdom\Users\state.local$
When: 03/17/2011 2:16:16 PM
Where: Agrig.amdom.local
Change type: Removed
Object type: user
Managed object: amdom.local
Detected by: amik.amdom.local at 03/17/2011 10:56:26 PM
```

Event ID: 1003

```
Who: EXCH2003B\Administrator
What: \LOCAL\EXC\EXCH2003\Users\Administrator
```

```
When: 03/17/2011 7:40:06 PM
Where: EXCH2003.EXCH2003.BYTSENKO.LOCAL
Change type: Modified
Object type: user
Change details: 'Storage Limits/Prohibit send at (Bytes)' changed from
'empty' to '124'
Managed object: exch2003.bytsenko.local
Detected by: amik.amdom.local at 03/17/2011 10:56:26 PM
```

Event ID: 1004

```
Who: AMDOM\Administrator
What: \local\amdom\amiks\TestUser4
When: 03/17/2011 7:17:06 PM
Where: Agrig.amdom.local
Change type: Modified
Object type: user
Managed object: amdom.local
Change details: User Account Disabled
Detected by: amik.amdom.local at 03/17/2011 10:56:26 PM
```

Event ID: 1005

```
Who: AMDOM\Admin
What: \local\amdom\OUAdmin
When: 03/17/2011 7:17:06 PM
Where: Agrig.amdom.local
Change type: Modified
Object type: organizationalUnit
Managed object: amdom.local
Change details: Object Security: Added: 'Permissions: Print Operators
(Allow: Read permissions, Read all properties, List contents)'
Detected by: amik.amdom.local at 03/17/2011 10:56:26 PM
```

Event ID: 1006

```
Who: AMDOM\Administrator
What: \local\amdom\Users\test
When: 03/18/2011 7:17:06 PM
Where: Agrig.amdom.local
Change type: Modified
Object type: group
Managed object: amdom.local
Change details: Security Global Group Member: Removed:
'amdom.local/Users/newuser'
Detected by: amik.amdom.local at 03/18/2011 10:56:26 PM
```

Event ID: 1007

```
Who: system
What: \local\amdom\Configuration\Sites\Default-First-Site-Name\NTDS Site
Settings
When: 03/17/2011 7:17:06 PM
Where: unknown
Change type: Modified
Object type: nTDSSiteSettings
Managed object: amdom.local
Change details: interSiteTopologyGenerator: modified and reverted back
Detected by: amik.amdom.local at 03/18/2011 6:56:26 AM
```

The sample descriptions for the NetWrix Group Policy Change Reporter events are as follows:

Event ID: 1001

```
The following audit event was detected:
Who: RABBIT\Administrator
```

```
What: \local\rabbit\New Group Policy Object
When: 06.04.2011 18:56:03
Where: DR-DC.rabbit.local
Change type: Added
Object type: Policy
Managed object: rabbit.local
Detected by: wks165.rabbit.local at 06.04.2011 18:57:52
```

Event ID: 1002

```
The following audit event was detected:
Who: RABBIT\Administrator
What: \local\rabbit\New Group Policy Object
When: 06.04.2011 19:00:49
Where: DR-DC.rabbit.local
Change type: Removed
Object type: Policy
Managed object: rabbit.local
Detected by: wks165.rabbit.local at 06.04.2011 19:02:24
```

Event ID: 1003

```
The following audit event was detected:
Who: RABBIT\Administrator
What: \local\rabbit\New Group Policy Object\General\Details
When: 06.04.2011 18:56:03
Where: DR-DC.rabbit.local
Change type: Modified
Object type: Policy
Change details: 'GPO Status' changed from '' to 'Enabled'
Managed object: rabbit.local
Detected by: wks165.rabbit.local at 06.04.2011 18:57:52
```

The table below contains sample values of the general properties:

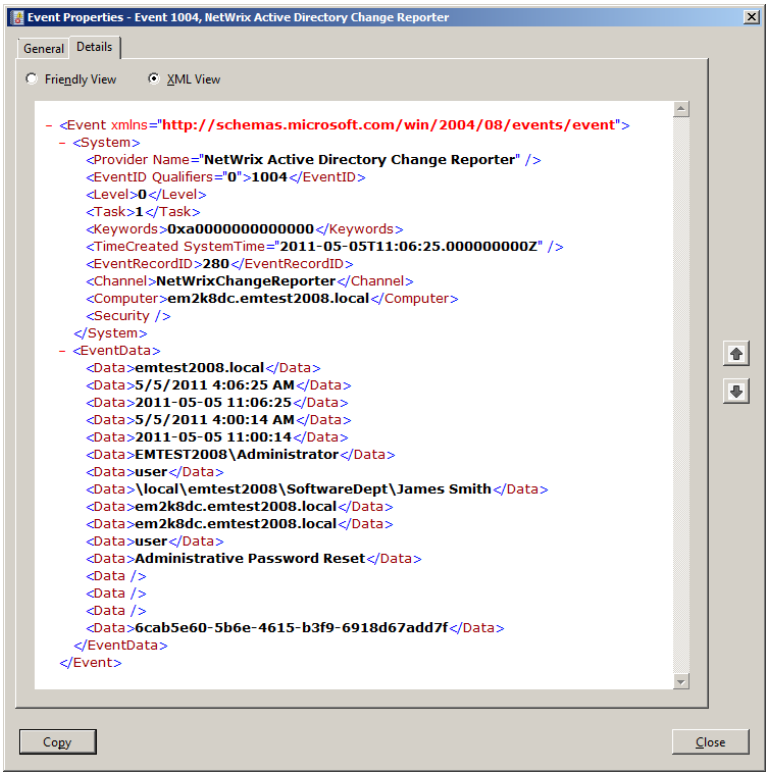
Table 7: General Properties

Field Name	Sample Value
Log Name	NetWrix Change Reporter
Source	NetWrix Active Directory Change Reporter
Event ID	1004
Level	Information
User	N/A (this field is used by .NET Framework. Its value for the NetWrix Change Reporter events is always N/A)
Logged	5/4/2011 6:36:46 AM (date and time)
Task Category	Audit
Keywords	Classic, Audit Success
Computer	em2k8dc.emtest2008.local
OpCode	<not used>

Details Tab

The Details tab supports data display in both Friendly and XML View modes. To set a mode, select the corresponding radio button:

Figure 5: Details Tab



In the XML View mode, you can see the following insertion strings between the <EventaData> and </EventData> tags (for details, refer to Table 3: Insertion Strings):

[1] "emtest2008.local"

[2] "5/4/2011 6:36:46 AM"

[3] "2011-05-04 13:36:46"

[4] "5/4/2011 6:32:21 AM"

[5] "2011-05-04 13:32:21"

[6] "EMTEST2008\Administrator"

[7] "user"

[8] "\local\emtest2008\SoftwareDept\John Doe"

[9] "em2k8dc.emtest2008.local"

[10] " em2k8dc.emtest2008.local "

[11] "user"

[12] "Administrative Password Reset"

[13] <empty>

[14] <empty>

[15] <empty>

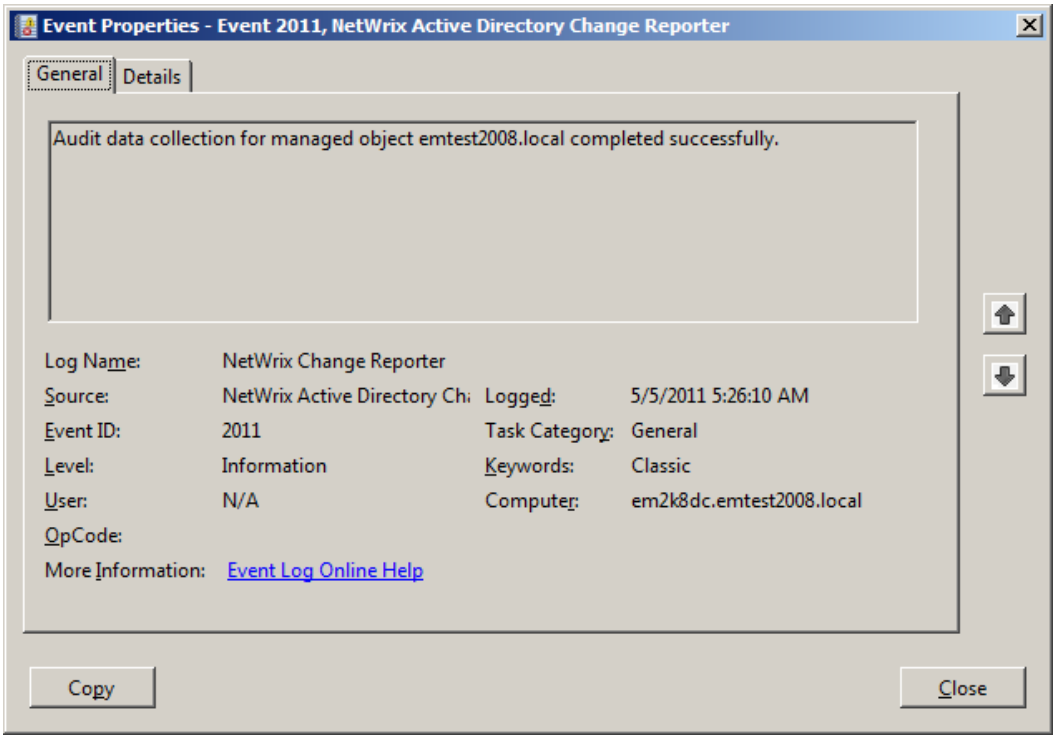
[16] "a1499621-c144-4ebb-a537-2f0578b13e2a"

4.2 General Events

General Tab

The Event Properties General tab shows the event description in the upper grid and the general properties information below the grid:

Figure 6: General Tab



The sample descriptions for the NetWrix Change Reporter events are as follows:

Event ID: 2001

The following warning has occurred on %Computer name% while processing %Object%: <warning text>

Event ID: 2002

The following error has occurred on %Computer name% while processing %Object%: <error text>

Event ID: 2010

Audit data collection for managed object %Object% started under user %User name%.

Example: *Audit data collection for managed object emtest2008.local started under user EMTEST2008\Administrator.*

Event ID: 2011

Audit data collection for managed object %Object% completed successfully.

Event ID: 2012

Audit data collection for managed object %Object% completed with warnings. For details, see previous events.

Event ID: 2013

Audit data collection for managed object %Object% completed with errors. For details, see previous events.

The table below contains sample values of the general properties:

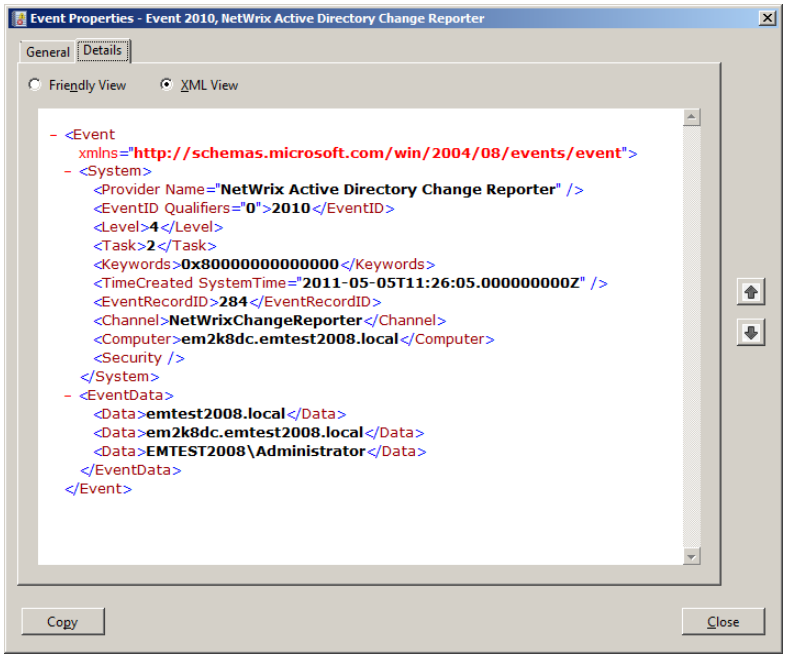
Table 8: General Properties

Field Name	Sample Value
Log Name	NetWrix Change Reporter
Source	NetWrix Active Directory Change Reporter
Event ID	2011
Level	Information
User	N/A (this field is used by .NET Framework. Its value for the NetWrix Change Reporter events is always N/A)
Logged	5/5/2011 5:26:10 AM (date and time)
Task Category	General
Keywords	Classic
Computer	em2k8dc.emtest2008.local
OpCode	<not used>

Details tab

The Details tab supports data display in both Friendly and XML View modes. To set a mode, select the corresponding radio button:

Figure 7: Details Tab



In the XML View mode, you can see the following insertion strings between the <EventaData> and </EventData> tags (for details, refer to Table 5: Insertion Strings Details):

[1] "emtest2008.local"

[2] "em2k8dc.emtest2008.local"

[3] "EMTEST2008\Administrator"

A APPENDIX: RELATED DOCUMENTATION

The table below lists all documents available to support integration with Third Party SIEM solutions:

Table 9: Related Documentation

Document Name	Overview
Integration with Third Party SIEM Systems	The current document contains the NetWrix Change Reporter events specification and explains how to enable integration with Third Party SIEM Systems.
NetWrix Active Directory Change Reporter SCOM Alerts Specification	The technical article contains specification of alerts generated by SCOM Management Pack for NetWrix Active Directory Change Reporter.
NetWrix Exchange Change Reporter SCOM Alerts Specification	The technical article contains specification of alerts generated by SCOM Management Pack for NetWrix Exchange Change Reporter.