Micro Focus Security ArcSight Connectors

SmartConnector for IBM DB2 Multiple Instance UDB Audit File

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for IBM DB2 Multiple Instance UDB Audit File

June, 2018

Warranty

Restricted Rights Legend

Trademark Notices

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
02/15/2017	Updated description for Version parameter.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
08/30/2016	End of life for DB2 UDB versions 8.2 and 8.5 due to end of support by vendor.
06/30/2016	Added support for version 10.5.
11/17/2015	Added EventDetails mapping to System Administration mappings table.
08/14/2015	Updated version supported.
03/29/2013	First edition of this Configuration Guide.

SmartConnector for IBM DB2 Multiple Instance UDB Audit File

This guide provides information for installing the SmartConnector for IBM DB2 Multiple Instance UDB Audit File for use with multiple database audit files in batch mode and for configuring the device for log event collection. DB2 Multiple Instance UDB versions 9.7, 10.1, and 10.5 are supported.

Product Overview

The IBM DB2 Multiple Instance UDB Audit facility generates and lets you maintain an audit trail for a series of predefined database events from two databases. The records generated from this facility are kept in an audit log file. The SmartConnector for IBM DB2 Multiple Instance UDB Audit File accesses the log files you identify during SmartConnector installation and configuration, and processes these events.

> Custom log formats are not supported; only the default documented format is supported.

Configuration

Overview

The audit facility acts at an instance level, recording all instance-level and database-level activities. The audit log (db2audit.log) and the audit configuration file (db2audit.cfg) are located in the instance's security subdirectory. At the time you create an instance, read/write permissions are set on these files, where possible, by the operating system. By default, the permissions are read/write for the instance owner only.

> SYSADM authority is required to use the audit facility administrator tool **db2audit**.

The audit facility must be stopped and started explicitly. When starting, the audit facility uses existing audit configuration information. Because the audit facility is independent of the DB2 UDB server, it remains active even if the instance is stopped.

Authorized users of the audit facility can control the following actions within the audit facility:

- Start or stop recording auditable events within the DB2 UDB instance.
- Configure the behavior of the audit facility, including selecting the categories of auditable events to be recorded.
- Request a description of the current audit configuration.

- Flush any pending audit records from the instance and write them to the audit log.
- Extract audit records by formatting and copying them from the audit log to a flat file or ASCII delimited files. Extraction is done in preparation for analysis or pruning of log records.
- Prune audit records from the current audit log.

Ensure that the audit facility has been turned on by issuing the db2audit start command before using the audit utilities.

The categories of events available for auditing are:

- Audit (AUDIT). Generates records when audit settings are changed or when the audit log is accessed.
- Authorization Checking (CHECKING). Generates records during authorization checking of attempts to access or manipulate DB2 UDB objects or functions.
- Operation Context (CONTEXT). Generates records to show the operation context when a database operation is performed. This category allows for better interpretation of the audit log file.
- Execute (EXECUTE). Generates records when SQL statements are executed.
- Object Maintenance (OBJMAINT). Generates records when creating or dropping data objects.
- Security Maintenance (SECMAINT). Generates records when granting or revoking: object or database privileges, or DBADM authority.
- System Administration (SYSADMIN). Generates records when operations requiring SYSADM, SYSMAINT, or SYSCTRL authority are performed.
- User Validation (VALIDATE). Generates records when authenticating users or retrieving system security information.

The SQL statement providing the operation context might be very long and is completely shown within the CONTEXT record. This can make the CONTEXT record very large.

Be selective of the events to audit. Any operation on the database can generate several records. The actual number of records generated and moved to the audit log depends on the number of categories of events to be recorded as specified by the audit facility configuration.

Connector Operation

In previous releases of this connector, processed ascii files were renamed to `.processed`, `.processed_1`, and so on. This caused the number of files in the DB2 archive folder to multiply uncontrollably (since 8 `.del` log files are generated per minute). Therefore, the connector default behavior has been changed to delete the log files rather than rename and preserve them. To have these log files renamed rather than deleted, you can change the property `mode` from `DeleteFile` to `RenameFileInTheSameDirectory` in `agent.properties` (located at `$ARCSIGHT_HOME\current\user\agent` after connector installation.

Configure Auditing and Events

To manually configure auditing of events, run a cron job as shown in the following samples.

```
# commit audit records
db2audit flush

# generates binary audit files
db2audit archive to <archivepath>

# for database level auditing
# (This command is not executed as part of automatic
auditing)
db2audit archive database <databasename> to <archivepath>

# extract ascii (.del) files from the binary audit files
db2audit extract delasc to <archivepath> from path
<archivepath> files <binary audit filenames>

# the binary audit files need to be manually removed, the
extracted .del
# files will be automatically removed by the connector
rm <binary audit filenames>
```

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

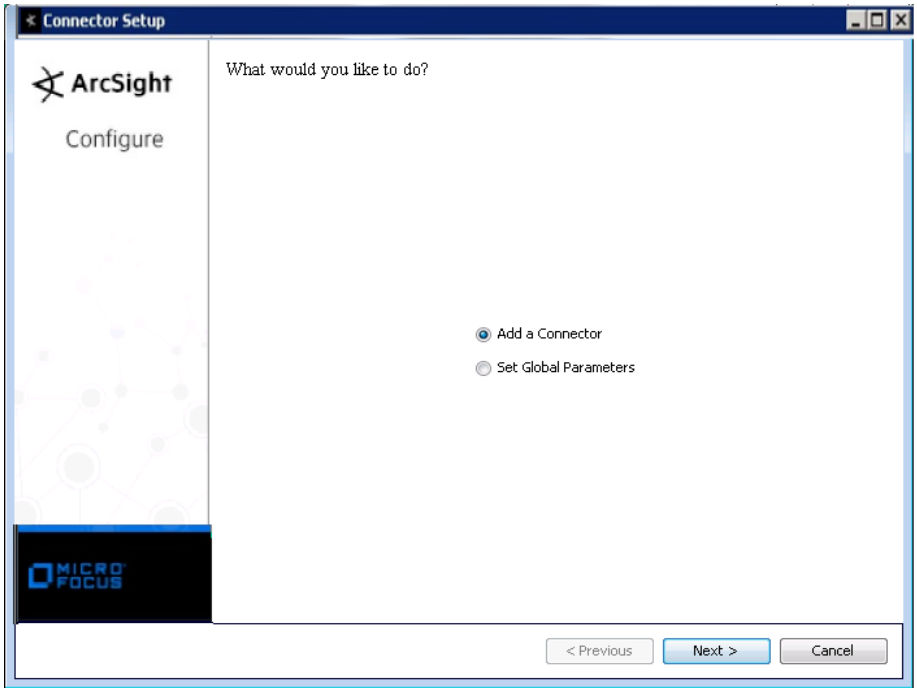
Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the Micro Focus SSO site.
2. Start the SmartConnector installation and configuration wizard by running the executable.

   Follow the wizard through the following folder selection tasks and installation of the core connector software:

   Introduction
   Choose Install Folder
   Choose Shortcut Folder
   Pre-Installation Summary
   Installing...
3. When the installation of SmartConnector core component software is finished, the following window is displayed:



Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

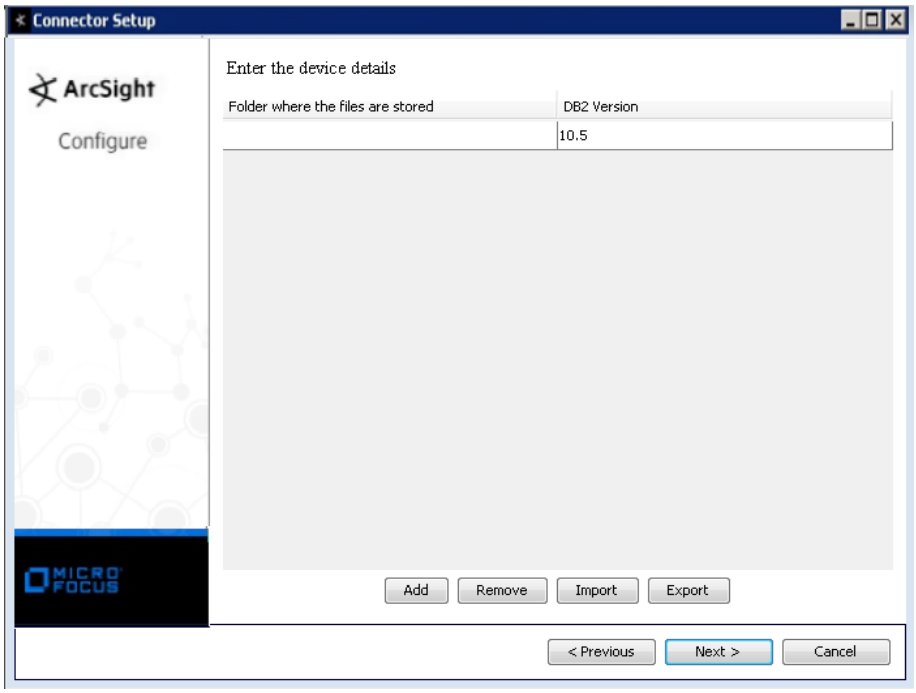
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the Micro Focus SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.

Parameter	Setting
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The Micro Focus SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
2. Select **IBM DB2 Multiple Instance UDB Audit File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Folder where the files are stored	Enter the absolute path to the folder containing the log files. The db2audit command lets you specify the output folder and the logs will be generated in the specified location (and subsequently deleted after processing).
DB2 Version	Enter the appropriate database version number. Possible values are 9.7, 10.1, or 10.5.

You can click the Export button to export the host name data you have entered into the able into a CSV file; you can click the Import button to select a CSV file to import into the table rather than add the data manually. See the "SmartConnector User's Guide" for more information.

Select a Destination

1. The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2. Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3. Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.

4. If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1. Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2. The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3. If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4. Click **Next** on the summary window.

5. To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

DB2 UDB Audit Log Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High, Medium, Low
Destination Host Name	HostName
Destination Process Name	ApplicationName
Destination User Name	UserID
Device Custom Number 1	EventCorrelator
Device Custom Number 2	EventStatus
Device Custom Number 3	OriginNodeNumber
Device Custom String 1	AuthorizationID
Device Custom String 2	PackageSchema
Device Custom String 3	PackageName
Device Custom String 4	PackageVersion
Device Custom String 6	PolicyName
Device Event Category	Category
Device Event Class Id	Category plus AuditEvent
Device Product	'DB2'

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	Timestamp
Device Severity	EventStatus
Device Vendor	'IBM'
Device Version	'10.5'
Event Outcome	EventStatus (Success or Failure)
External Id	GlobalTransactionID
File ID	InstName
File Name	DatabaseName
File Path	DataPath
Name	AuditEvent
Reason	EventStatus
Source Host Name	ClientWorkstationName
Source Process Name	ClientApplicationName
Source User ID	OriginalUserID
Source User Name	ClientUserID

DB2 Checking Log Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High, Medium, Low
Destination Host Name	HostName
Destination Process Name	ApplicationName
Destination User Name	UserID
Device Custom Number 1	EventCorrelator
Device Custom Number 2	EventStatus
Device Custom Number 3	OriginNodeNumber
Device Custom String 1	AuthorizationID
Device Custom String 2	PackageSchema
Device Custom String 3	PackageName
Device Custom String 4	PackageVersion
Device Custom String 5	ObjectName
Device Event Category	Category
Device Event Class Id	Category plus AuditEvent
Device Product	'DB2'
Device Receipt Time	Timestamp
Device Severity	EventStatus
Device Vendor	'IBM'
Device Version	'10.5'
Event Outcome	EventStatus (Success or Failure)
External Id	GlobalTransactionID
File ID	InstName
File Name	DatabaseName
Name	AuditEvent

ArcSight ESM Field	Device-Specific Field
Reason	EventStatus
Source Host Name	ClientWorkstationName
Source Process Name	ClientApplicationName
Source User ID	OriginalUserID
Source User Name	ClientUserID

DB2 Context Log Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High, Medium, Low
Destination Host Name	HostName
Destination Process Name	ApplicationName
Destination User Name	UserID
Device Custom Number1	EventCorrelator
Device Custom Number3	OriginNodeNumber
Device Custom String1	AuthorizationID
Device Custom String2	PackageSchema
Device Custom String3	PackageName
Device Custom String4	PackageVersion
Device Event Category	Category
Device Event Class Id	Category plus AuditEvent
Device Product	'DB2'
Device Receipt Time	Timestamp
Device Severity	EventStatus
Device Vendor	'IBM'
Device Version	'10.5'
External Id	GlobalTransactionID
File ID	InstName
File Name	DatabaseName
Message	StatementText
Name	AuditEvent
Source Host Name	ClientWorkstationName
Source Process Name	ClientApplicationName
Source User ID	OriginalUserID
Source User Name	ClientUserID

DB2 Execute Log Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High, Medium, Low
Destination Host Name	HostName
Destination Process Name	ApplicationName
Destination User Name	UserID

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	EventCorrelator
Device Custom Number 2	EventStatus
Device Custom Number 3	OriginNodeNumber
Device Custom String 1	AuthorizationID
Device Custom String 2	PackageSchema
Device Custom String 3	PackageName
Device Custom String 4	PackageVersion
Device Custom String 6	PolicyName
Device Event Category	Category
Device Event Class Id	Category plus AuditEvent
Device Product	'DB2'
Device ReceiptTime	Timestamp
Device Severity	EventStatus
Device Vendor	'IBM'
Device Version	'10.5'
Event Outcome	EventStatus (Success or Failure)
External Id	GlobalTransactionID
File ID	InstName
File Name	DatabaseName
Message	StatementText
Name	AuditEvent
Reason	EventStatus
Source Host Name	ClientWorkstationName
Source Process Name	ClientApplicationName
Source User Name	ClientUserID

DB2 Object Maintenance Log Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High, Medium, Low
Destination Host Name	HostName
Destination Process Name	ApplicationName
Destination User Name	UserID
Device Custom Number 1	EventCorrelator
Device Custom Number 2	EventStatus
Device Custom Number 3	OriginNodeNumber
Device Custom String 1	AuthorizationID
Device Custom String 2	PackageSchema
Device Custom String 3	PackageName
Device Custom String 4	PackageVersion
Device Custom String 5	ObjectName
Device Custom String 6	SecurityPolicyName
Device Event Category	Category

ArcSight ESM Field	Device-Specific Field
Device Event Class Id	Category plus AuditEvent
Device Product	'DB2'
Device Receipt Time	Timestamp
Device Severity	EventStatus
Device Vendor	'IBM'
Device Version	'10.5'
Event Outcome	EventStatus (Success or Failure)
External Id	GlobalTransactionID
File ID	InstName
File Name	DatabaseName
Name	AuditEvent
Reason	EventStatus
Source Host Name	ClientWorkstationName
Source Process Name	ClientApplicationName
Source User ID	OriginalUserID
Source User Name	ClientUserID

DB2 Security Maintenance Log Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High, Medium, Low
Destination Host Name	HostName
Destination Process Name	ApplicationName
Destination User Name	UserID
Device Custom Number 1	EventCorrelator
Device Custom Number 2	EventStatus
Device Custom Number 3	OriginNodeNumber
Device Custom String 1	AuthorizationID
Device Custom String 2	PackageSchema
Device Custom String 3	PackageName
Device Custom String 4	PackageVersion
Device Custom String 5	ObjectName
Device Event Category	Category
Device Event Class Id	Category plus AuditEvent
Device Product	'DB2'
Device Receipt Time	Timestamp
Device Severity	EventStatus
Device Vendor	'IBM'
Device Version	'10.5'
Event Outcome	EventStatus (Success or Failure)
External Id	GlobalTransactionID
File ID	InstName
File Name	DatabaseName

ArcSight ESM Field	Device-Specific Field
File Permission	AccessType
Name	AuditEvent
Reason	EventStatus
Source Host Name	ClientWorkstationName
Source ProcessName	ClientApplicationName
Source User ID	OriginalUserID
Source User Name	ClientUserID

DB2 System Administration Log Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High, Medium, Low
Destination Host Name	HostName
Destination Process Name	ApplicationName
Destination User Name	UserID
Device Custom Number 1	EventCorrelator
Device Custom Number 2	EventStatus
Device Custom Number 3	OriginNodeNumber
Device Custom String 1	AuthorizationID
Device Custom String 2	PackageSchema
Device Custom String 3	PackageName
Device Custom String 4	PackageVersion
Device Custom String 5	EventDetails
Device Event Category	Category
Device Event Class Id	Category plus AuditEvent
Device Product	'DB2'
Device Receipt Time	Timestamp
Device Severity	EventStatus
Device Vendor	'IBM'
Device Version	'10.5'
Event Outcome	EventStatus (Success or Failure)
External Id	GlobalTransactionID
File ID	InstName
File Name	DatabaseName
Name	AuditEvent
Reason	EventStatus
Source Host Name	ClientWorkstationName
Source Process Name	ClientApplicationName
Source User ID	OriginalUserID
Source User Name	ClientUserID

DB2 Validate Log Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High, Medium, Low
Destination Host Name	HostName
Destination Process Name	ApplicationName
Destination User Name	UserID
Device Custom Number 1	EventCorrelator
Device Custom Number 2	EventStatus
Device Custom Number 3	OriginNodeNumber
Device Custom String 1	AuthorizationID
Device Custom String 2	PackageSchema
Device Custom String 3	PackageName
Device Custom String 4	PackageVersion
Device Event Category	Category
Device Event Class Id	Category plus AuditEvent
Device Product	'DB2'
Device Receipt Time	Timestamp
Device Severity	EventStatus
Device Vendor	'IBM'
Device Version	'10.5'
Event Outcome	EventStatus (Success or Failure)
External Id	GlobalTransactionID
File ID	InstName
File Name	DatabaseName
Name	AuditEvent
Reason	EventStatus
Source Host Name	ClientWorkstationName
Source Process Name	ClientApplicationName
Source User ID	OriginalUserID
Source User Name	ClientUserID