Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for IBM DB2 Multiple Instance UDB Audit File SmartConnector

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Document Revision History

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to ArcSight Product Documentation Community on the Micro Focus Security Community.

Document Changes

Date	Product Version	Description
MM/DD/YYYY	X.X.X.X	Description of change

Contents

Configuration Guide for 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.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provides information about configuring SmartConnectors to collect events from different sources.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

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. When 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.

Configuring 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>
```

Installing the SmartConnector

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

Preparing to Install the SmartConnector

(missing or bad snippet)(missing or bad snippet)

Installing and Configuring the SmartConnector

(missing or bad snippet)

1. Select **IBM DB2 Multiple Instance UDB Audit File** from the **Type** drop-down, then click **Next**.
2. 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.

3. Click **Export** to export the host name data you have entered into the able into a CSV file or click **Import** to select a CSV file to import into the table rather than add the data manually.

(missing or bad snippet)

Connecting to an IBM DB2 Database

For IBM DB2 connectors, DB2 drivers are no longer provided in the connector installation due to licensing requirements. Later versions of DB2 drivers can be found here, but users require IBM login credentials. IBM requires a license jar to be added to the connector in order to connect to the database.

To connect to an IBM DB2 database:

1. Copy the following files from IBM DB installation location, for example, `C:\Program Files\IBM\SQLLIB\java`:

   `db2jcc4.jar`

   `db2jcc_license_cu.jar`
2. Add them to the `current\user\agent\lib` directory in the installation folder of each connector that needs to connect to a DB2 instance.

Connector Operation

In the 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 as 8 `.del` log files are generated per minute.

To overcome this challenge, the connector default behavior is set to delete the log files rather than to rename and preserve them. However, to rename the log files rather than delete:

1. Open the `agent.properties` file located in `$ARCSIGHT_HOME\current\user\agent.`
2. Change the property `mode` from `DeleteFile` to `RenameFileInTheSameDirectory`

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'
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

ArcSight ESM Field	Device-Specific Field
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'

ArcSight ESM Field	Device-Specific Field
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 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

ArcSight ESM Field	Device-Specific Field
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
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 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

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	ObjectName
Device Custom String 6	SecurityPolicyName
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 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

ArcSight ESM Field	Device-Specific Field
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
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

ArcSight ESM Field	Device-Specific Field
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

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

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for IBM DB2 Multiple Instance UDB Audit File SmartConnector (SmartConnectors 8.3.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!