IBM Tivoli Identity Manager (TIM)

FlexConnector

(ArcSight Flex Connector DB - TimeBase)

Author Information

Dave Munger
dave.munger@gmail.com

DOCUMENT REVISION

Version #	Publication date	Modification description	Modified by
1.01	2011-12-06	Typo correction	Dave Munger
1.00	2011-11-30	First publication of the document	Dave Munger

Information

Hi everyone,

I have developped this FlexConnector for IBM TIM software. This flexConnector retrieve all audit event generated by TIM software. Don't hesitate to reuse all information present in this document. Also, if you have some information that you would like to add to this document or any comment or question, please contact me.

Enjoy!!!

Dave

A special note for Jay Heidecker...who help me for the timestamp conversion... Thanks Jay!!!

Section 1. Initial information about Tivoli Identity Manager (TIM)

For this case, we suppose that we have one server.

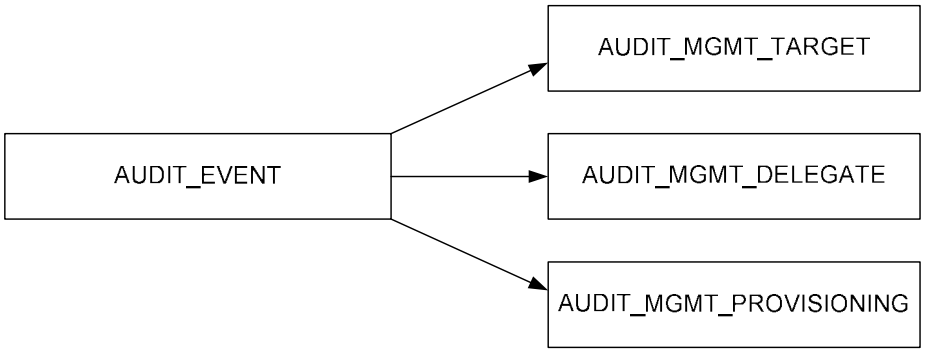
TIM Database Server Name : SRVTIM
TIM Database Server IP Address : 192.168.1.10
TIM Version: 5.1

TIM Database type : DB2
TIM Database Name: ITIMDB
TIM Database port (for the listener) : tcp / 50002

Section 2. Audits Events Stored in TIM that we want to add in the SIEM solution.

First, it's important to understand that all audit event are stored in one table. And, in some case, this table has a reference with two others tables.

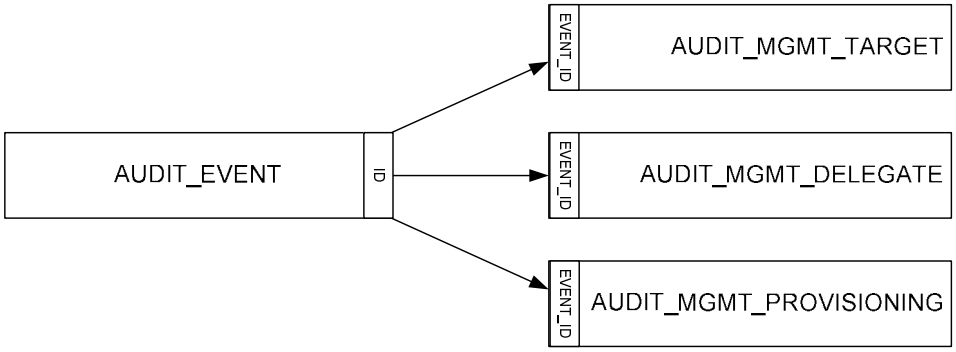
Figure 1 - Link between TIM table



All information are stored in AUDIT_EVENT. Also, all entry in the table AUDIT_EVENT has one unique ID. This unique ID is located in the column ID (for the AUDIT_EVENT table). This unique ID is also used to find information stored in AUDIT_MGMT_TARGET, AUDIT_MGMT_DELEGATE and the table AUDIT_MGMT_PROVISIONING.

The unique ID is under the column ID for the AUDIT_EVENT table. For the AUDIT_MGMT_TARGET, AUDIT_MGMT_DELEGATE and the table AUDIT_MGMT_PROVISIONING table, the unique ID is located under the column EVENT_ID.

Figure 2 - Link between TIM table with "master" column



All event have a unique ID. So, it's impossible to use the "ArcSight FlexConnector ID-based Database" because the unique ID of each entry are not continuous. For example, the first event can have the unique ID 100 and the second event can have the number 1. Then we have decided to use the "ArcSight FlexConnector Time-based database". The timestamp of all events are under the column "TIMESTAMP". Also, the "TIMESTAMP" column is define has "VARCHAR" type in the database.

AUDIT_EVENT and link with other tables

Contain fields common to all audit events. Other separate tables are created for particular event type only when it contain more attributes.

Event Category	**Link with other table**
Person Management	audit_mgmt_target --> only if action is "Person transfer"
OrgRole Management	audit_mgmt_target --> only if action is "Add member"
ITIM Group Management	audit_mgmt_target --> only if action is "Add member" or "Remove Member"
Service Management	audit_mgmt_target --> only if action is "Add" or "Modify" or "Remove Adoption Rule".
Account Management	audit_mgmt_provisioning --> all time

Section 3. TIM tables columns description

This section contain a description of all columns for tables used by the flexconnector.

Let start :

AUDIT_EVENT table

The AUDIT_EVENT table is common for all audit events. However, the value for some columns is different depending on the event. Refer to the next

Column Name	Column Description
ID*	ID by which this event is identified. Primary key.
ITIM_EVENT_CATEGORY	Tivoli Identity Manager type of the event
ENTITY_NAME	Name of the Tivoli Identity Manager entities altered by this event. The size of this column is 100 characters assuming that the name of the entity getting audited is 100 or less character long.
ENTITY_DN	DN of the entity involved in this event.
ENTITY_TYPE	Type of the Tivoli Identity Manager entity.
ACTION*	The value of this column depends on the event type. Each event type has a set of actions.
WORKFLOW_PROCESS_ID	Process ID of the workflow initiated. This column is applicable to workflow operations.
INITIATOR_NAME	Requester of this operation.
INITIATOR_DN	Distinguished name of the requester in the LDAP directory.
CONTAINER_NAME	Name of the container that holds the entity.
CONTAINER_DN	Distinguished name of the container that holds the entity.
RESULT_SUMMARY	The results of an event: Success Failure If the operation is submitted to workflow,

	this column will indicate whether the operation was successfully submitted to workflow.
TIMESTAMP*	The time when the audit event occurs. It is also a start time of the operation.
COMMENTS	Description for this event.

* The column is required and not null.

AUDIT_MGMT_TARGET table

See the description of all table in AUDIT_MGMT_TARGET.

Column Name	Column Description
ID*	ID by which this event is identified. Primary key.
ITIM_EVENT_CATEGORY	Tivoli Identity Manager type of the event
ENTITY_NAME	Name of the Tivoli Identity Manager entities altered by this event. The size of this column is 100 characters assuming that the name of the entity getting audited is 100 or less character long.
ENTITY_DN	DN of the entity involved in this event.
ENTITY_TYPE	Type of the Tivoli Identity Manager entity.

Section 4. ArcSight event field mappings

This section contain event field mapping information.

Just before starting, we have decided to use a couple of arcsight events fields to specify a couples of things.

- event.deviceVendor = "IBM"
- event.deviceProduct = "TIM"
- event.deviceFacility = *Contain the identification of the conditional map used to parse event. It's only for troubleshooting purpose.*
    - ex: event.deviceFacility = "0-0"

Figure 3 - How to troubleshoot the parser

```
#
conditionalmap[0].mappings[0].values=Authentication
conditionalmap[0].mappings[0].event.message=ENTITY_NAME
conditionalmap[0].mappings[0].event.deviceFacility=__stringConstant(0-0)
conditionalmap[0].mappings[0].event.deviceAction=RESULT_SUMMARY
conditionalmap[0].mappings[0].event.attackerUserName=ENTITY_NAME
conditionalmap[0].mappings[0].event.targetProcessName=ENTITY_TYPE
conditionalmap[0].mappings[0].event.targetServiceName=ACTION
conditionalmap[0].mappings[0].event.deviceCustomString6=COMMENTS
conditionalmap[0].mappings[0].event.deviceCustomString6Label=__stringConstant(COMMENTS)
#
```

Event field mapping for "Authentication" event

AUDIT_EVENT table and ArcSight event field mapping		
Column Name and Value	**AUDIT_EVENT Column**	**ArcSight event field Mapping**
ITEM_EVENT_CATEGORY If value = Authentication	ENTITY_NAME	event.message
	RESULT_SUMMARY	event.deviceAction
	ENTITY_NAME	event.attackerUserName
	ENTITY_TYPE	event.targetProcessName
	ACTION	event.targetServiceName
	COMMENTS	event.deviceCustomString6

Manual event field Mapping	
Event field	**Value**
event.endTime	Use the value in column "TIMESTAMP"
event.deviceVendor	"IBM"
event.deviceProduct	"TIM"
event.deviceFacility	"0-0"
event.deviceCustomNumber1	Use the value in column "ID"
event.deviceCustomNumber1Label	"TIMEventID"
event.name	Use the value in column "ITEM_EVENT_CATEGORY"
event.targetServiceName	User the value in column "ACTION"
event.deviceCustomString6Label	"COMMENTS"

Event field mapping for "Reconciliation" event

AUDIT_EVENT table and ArcSight event field mapping		
Column Name and Value	**AUDIT_EVENT Column**	**ArcSight event field Mapping**
ITEM_EVENT_CATEGORY If value = Reconciliation	ENTITY_NAME	event.message
	RESULT_SUMMARY	event.deviceAction
	INITIATOR_NAME	event.attackerUserName
	ACTION	event.targetServiceName
	ENTITY_DN	event.deviceCustomString1
	ENTITY_TYPE	event.deviceCustomString2
	CONTAINER_NAME	event.deviceCustomString3
	CONTAINER_DN	event.deviceCustomString4
	COMMENTS	event.deviceCustomString6

Manual event field Mapping	
Event field	**Value**
event.endTime	Use the value in column "TIMESTAMP"
event.deviceVendor	"IBM"
event.deviceProduct	"TIM"
event.deviceFacility	"0-1"
event.deviceCustomNumber1	Use the value in column "ID"
event.deviceCustomNumber1Label	"TIMEventID"
event.name	Use the value in column "ITEM_EVENT_CATEGORY"
event.deviceCustomString1Label	"ServiceName"
event.deviceCustomString2Label	"RessourceType"
event.deviceCustomString3Label	"targetContainerName"
event.deviceCustomString4Label	"targetContainerID"
event.deviceCustomString6Label	"COMMENTS"

Event field mapping for "SelfPasswordChange" event

AUDIT_EVENT table and ArcSight event field mapping		
Column Name and Value	**AUDIT_EVENT Column**	**ArcSight event field Mapping**
ITEM_EVENT_CATEGORY If value = Reconciliation	ITIM_EVENT_CATEGORY	Event.name
	ID	event.deviceCustomNumber1
	TIMESTAMP	Event.endTime
	ENTITY_NAME	event.message
	RESULT_SUMMARY	event.deviceAction
	ENTITY_NAME	event.attackerUserName
	ENTITY_DN	event.attackerUserId
	ACTION	event.targetServicename
	WORKFLOW_PROCESS_ID	event.deviceCustomNumber2
	INITIATOR_NAME	event.targetUserName
	INITIATOR_DN	event.targetUserId
	CONTAINER_NAME	event.deviceCustomString4
	CONTAINER_DN	event.deviceCustomString5
	COMMENTS	event.deviceCustomString6

Manual event field Mapping	
Event field	**Value**
event.deviceVendor	"IBM"
event.deviceProduct	"TIM"
event.deviceFacility	"0-2"
event.deviceCustomNumber1Label	"TIMEventID"
event.deviceCustomNumber2Label	"WorkFlowProcessID"
event.deviceCustomString4Label	"targetContainerName"
event.deviceCustomString5Label	"targetContainerID"
event.deviceCustomString6Label	"COMMENTS"

Event field mapping for "RuntimeEvent" event

AUDIT_EVENT table and ArcSight event field mapping		
Column Name and Value	**AUDIT_EVENT Column**	**ArcSight event field Mapping**
ITEM_EVENT_CATEGORY If value = RuntimeEvent	ITIM_EVENT_CATEGORY	Event.name
	ID	event.deviceCustomNumber1
	TIMESTAMP	Event.endTime
	ENTITY_TYPE	event.message
	RESULT_SUMMARY	event.deviceAction
	ENTITY_NAME	event.attackerUserName
	ENTITY_DN	event.attackerUserId
	ACTION	event.targetServicename
	WORKFLOW_PROCESS_ID	event.deviceCustomNumber2
	INITIATOR_NAME	event.targetUserName
	INITIATOR_DN	event.targetUserId
	CONTAINER_NAME	event.deviceCustomString4
	CONTAINER_DN	event.deviceCustomString5
	COMMENTS	event.deviceCustomString6

Manual event field Mapping	
Event field	**Value**
event.deviceVendor	"IBM"
event.deviceProduct	"TIM"
event.deviceFacility	"0-3"
event.deviceCustomNumber1Label	"TIMEventID"
event.deviceCustomNumber2Label	"WorkFlowProcessID"
event.deviceCustomString4Label	"targetContainerName"
event.deviceCustomString5Label	"targetContainerID"
event.deviceCustomString6Label	"COMMENTS"

Event field mapping for "PolicyManagement" event

AUDIT_EVENT table and ArcSight event field mapping		
Column Name and Value	**AUDIT_EVENT Column**	**ArcSight event field Mapping**
ITEM_EVENT_CATEGORY If value = PolicyManagement	ITIM_EVENT_CATEGORY	Event.name
	ID	event.deviceCustomNumber1
	TIMESTAMP	Event.endTime
	ENTITY_TYPE	event.message
	RESULT_SUMMARY	event.deviceAction
	INITIATOR_NAME	event.attackerUserName
	INITIATOR_DN	event.attackerUserId
	CONTAINER_DN	event.attackerUserPrivileges
	WORKFLOW_PROCESS_ID	event.deviceCustomNumber2
	ACTION	event.deviceCustomString1
	CONTAINER_NAME	event.deviceCustomString2
	ENTITY_NAME	event.deviceCustomString3
	ENTITY_DN	event.deviceCustomString4
	COMMENTS	event.deviceCustomString6

Manual event field Mapping	
Event field	**Value**
event.deviceVendor	"IBM"
event.deviceProduct	"TIM"
event.deviceFacility	"0-4"
event.deviceCustomNumber1Label	"TIMEventID"
event.deviceCustomNumber2Label	"WorkFlowProcessID"
event.deviceCustomString1Label	"ACTION"
event.deviceCustomString2Label	"attackerContainerName"
event.deviceCustomString3Label	"ENTITY_NAME"
event.deviceCustomString4Label	"policyDN"
event.deviceCustomString6Label	"COMMENTS"

Event field mapping for "ContainerManagement" event

AUDIT_EVENT table and ArcSight event field mapping		
Column Name and Value	**AUDIT_EVENT Column**	**ArcSight event field Mapping**
ITEM_EVENT_CATEGORY If value = ContainerManagement	ITIM_EVENT_CATEGORY	event.name
	ID	event.deviceCustomNumber1
	TIMESTAMP	event.endTime
	ENTITY_TYPE	event.message
	RESULT_SUMMARY	event.deviceAction
	INITIATOR_NAME	event.attackerUserName
	INITIATOR_DN	event.attackerUserId
	CONTAINER_DN	event.attackerUserPrivileges
	WORKFLOW_PROCESS_ID	event.deviceCustomNumber2
	ENTITY_NAME	event.targetUserName
	ENTITY_DN	event.targetUserId
	ACTION	event.deviceCustomString1
	CONTAINER_NAME	event.deviceCustomString2
	COMMENTS	event.deviceCustomString6

Manual event field Mapping	
Event field	**Value**
event.deviceVendor	"IBM"
event.deviceProduct	"TIM"
event.deviceFacility	"0-5"
event.deviceCustomNumber1Label	"TIMEventID"
event.deviceCustomNumber2Label	"WorkFlowProcessID"
event.deviceCustomString1Label	"ACTION"
event.deviceCustomString2Label	"attackerContainerName"
event.deviceCustomString6Label	"COMMENTS"

Event field mapping for "ITIMConfiguration" event

AUDIT_EVENT table and ArcSight event field mapping		
Column Name and Value	**AUDIT_EVENT Column**	**ArcSight event field Mapping**
ITEM_EVENT_CATEGORY If value = ITIMConfiguration	ITIM_EVENT_CATEGORY	event.name
	ID	event.deviceCustomNumber1
	TIMESTAMP	event.endTime
	ENTITY_TYPE	event.message
	RESULT_SUMMARY	event.deviceAction
	INITIATOR_NAME	event.attackerUserName
	INITIATOR_DN	event.attackerUserId
	CONTAINER_DN	event.attackerUserPrivileges
	WORKFLOW_PROCESS_ID	event.deviceCustomNumber2
	ACTION	event.deviceCustomString1
	CONTAINER_NAME	event.deviceCustomString2
	ENTITY_DN	event.deviceCustomString3
	ENTITY_NAME	event.deviceCustomString4
	COMMENTS	event.deviceCustomString6

Manual event field Mapping	
Event field	**Value**
event.deviceVendor	"IBM"
event.deviceProduct	"TIM"
event.deviceFacility	"0-6"
event.deviceCustomNumber1Label	"TIMEventID"
event.deviceCustomNumber2Label	"WorkFlowProcessID"
event.deviceCustomString1Label	"ACTION"
event.deviceCustomString2Label	"attackerContainerName"
event.deviceCustomString3Label	"ENTITY_DN"
event.deviceCustomString4Label	"ENTITY_NAME"
event.deviceCustomString6Label	"COMMENTS"

Event field mapping for "Migration" event

AUDIT_EVENT table and ArcSight event field mapping		
Column Name and Value	**AUDIT_EVENT Column**	**ArcSight event field Mapping**
ITEM_EVENT_CATEGORY If value = Migration	ITIM_EVENT_CATEGORY	event.name
	ID	event.deviceCustomNumber1
	TIMESTAMP	event.endTime
	ENTITY_TYPE	event.message
	RESULT_SUMMARY	event.deviceAction
	INITIATOR_NAME	event.attackerUserName
	INITIATOR_DN	event.attackerUserId
	ACTION	event.deviceCustomString2
	COMMENTS	event.deviceCustomString6

Manual event field Mapping	
Event field	**Value**
event.deviceVendor	"IBM"
event.deviceProduct	"TIM"
event.deviceFacility	"0-7"
event.deviceCustomNumber1Label	"TIMEventID"
event.deviceCustomString2Label	"ACTION"
event.deviceCustomString6Label	"COMMENTS"

Event field mapping for "PersonManagement" event

AUDIT_EVENT table and ArcSight event field mapping		
Column Name and Value	**AUDIT_EVENT Column**	**ArcSight event field Mapping**
ITEM_EVENT_CATEGORY If value = PersonManagement	ITIM_EVENT_CATEGORY	event.name
	ID	event.deviceCustomNumber1
	TIMESTAMP	event.endTime
	ENTITY_TYPE	event.message
	RESULT_SUMMARY	event.deviceAction
	INITIATOR_NAME	event.attackerUserName
	INITIATOR_DN	event.attackerUserId
	CONTAINER_DN	event.attackerUserPrivileges
	ENTITY_NAME	event.targetUserName
	ENTITY_DN	event.targetUserId
	WORKFLOW_PROCESS_ID	event.deviceCustomNumber2
	ACTION	event.deviceCustomString1
	CONTAINER_NAME	event.deviceCustomString2
	COMMENTS	event.deviceCustomString6

AUDIT_MGMT_TARGET table and ArcSight event field mapping	
AUDIT_EVENT Column	**ArcSight event field Mapping**
TARGET_ENTITY_NAME	event.deviceCustomString3
TARGET_ENTITY_TYPE	event.deviceCustomString4
TARGET_ENTITY_DN	event.deviceCustomString5

Manual event field Mapping	
Event field	**Value**
event.deviceVendor	"IBM"
event.deviceProduct	"TIM"
event.deviceFacility	"0-8"
event.deviceCustomNumber1Label	"TIMEventID"
event.deviceCustomNumber2Label	"WorkFlowProcessID"
event.deviceCustomString1Label	"ACTION"
event.deviceCustomString2Label	"original"
event.deviceCustomString3Label	"target"
event.deviceCustomString4Label	"target_Container_Type"
event.deviceCustomString5Label	"target_Container_ID"
event.deviceCustomString6Label	"COMMENTS"

Event field mapping for "OrgRoleManagement" event

AUDIT_EVENT table and ArcSight event field mapping		
Column Name and Value	**AUDIT_EVENT Column**	**ArcSight event field Mapping**
ITEM_EVENT_CATEGORY If value = OrgRoleManagement	ITIM_EVENT_CATEGORY	event.name
	ID	event.deviceCustomNumber1
	TIMESTAMP	event.endTime
	ENTITY_TYPE	event.message
	RESULT_SUMMARY	event.deviceAction
	INITIATOR_NAME	event.attackerUserName
	INITIATOR_DN	event.attackerUserId
	CONTAINER_DN	event.attackerUserPrivileges
	WORKFLOW_PROCESS_ID	event.deviceCustomNumber2
	ACTION	event.deviceCustomString1
	CONTAINER_NAME	event.deviceCustomString2
	CONTAINER_DN	event.deviceCustomString3
	ENTITY_NAME	event.deviceCustomString4
	ENTITY_DN	event.deviceCustomString5
	COMMENTS	event.deviceCustomString6

AUDIT_MGMT_TARGET table and ArcSight event field mapping	
AUDIT_EVENT Column	**ArcSight event field Mapping**
TARGET_ENTITY_NAME	event.targetUserName
TARGET_ENTITY_TYPE	event.targetUserId
TARGET_ENTITY_DN	Event.targetUserPrivileges

Manual event field Mapping	
Event field	**Value**
event.deviceVendor	"IBM"
event.deviceProduct	"TIM"
event.deviceFacility	"0-9"
event.deviceCustomNumber1Label	"TIMEventID"
event.deviceCustomNumber2Label	"WorkFlowProcessID"
event.deviceCustomString1Label	"ACTION"
event.deviceCustomString2Label	"original"
event.deviceCustomString3Label	"original_Container_DN"
event.deviceCustomString4Label	"role_Name"
event.deviceCustomString5Label	"role_DN"
event.deviceCustomString6Label	"COMMENTS"

Event field mapping for "ITIMGroupManagement" event

AUDIT_EVENT table and ArcSight event field mapping		
Column Name and Value	**AUDIT_EVENT Column**	**ArcSight event field Mapping**
ITEM_EVENT_CATEGORY If value = ITIMGroupManagement	ITIM_EVENT_CATEGORY	event.name
	ID	event.deviceCustomNumber1
	TIMESTAMP	event.endTime
	ENTITY_TYPE	event.message
	RESULT_SUMMARY	event.deviceAction
	INITIATOR_NAME	event.attackerUserName
	INITIATOR_DN	event.attackerUserId
	CONTAINER_DN	event.attackerUserPrivileges
	WORKFLOW_PROCESS_ID	event.deviceCustomNumber2
	ACTION	event.deviceCustomString1
	CONTAINER_NAME	event.deviceCustomString2
	CONTAINER_DN	event.deviceCustomString3
	ENTITY_NAME	event.deviceCustomString4
	ENTITY_DN	event.deviceCustomString5
	COMMENTS	event.deviceCustomString6

AUDIT_MGMT_TARGET table and ArcSight event field mapping	
AUDIT_EVENT Column	**ArcSight event field Mapping**
TARGET_ENTITY_NAME	event.targetUserName
TARGET_ENTITY_TYPE	event.targetUserId
TARGET_ENTITY_DN	Event.targetUserPrivileges

Manual event field Mapping	
Event field	**Value**
event.deviceVendor	"IBM"
event.deviceProduct	"TIM"
event.deviceFacility	"0-10"
event.deviceCustomNumber1Label	"TIMEventID"
event.deviceCustomNumber2Label	"WorkFlowProcessID"
event.deviceCustomString1Label	"ACTION"
event.deviceCustomString2Label	"original"
event.deviceCustomString3Label	"original_Container_DN"
event.deviceCustomString4Label	"Group_Name"
event.deviceCustomString5Label	"Group_DN"
event.deviceCustomString6Label	"COMMENTS"

Event field mapping for "ServiceManagement" event

AUDIT_EVENT table and ArcSight event field mapping		
Column Name and Value	**AUDIT_EVENT Column**	**ArcSight event field Mapping**
ITEM_EVENT_CATEGORY If value = ServiceManagement	ITIM_EVENT_CATEGORY	event.name
	ID	event.deviceCustomNumber1
	TIMESTAMP	event.endTime
	ENTITY_TYPE	event.message
	RESULT_SUMMARY	event.deviceAction
	INITIATOR_NAME	event.attackerUserName
	INITIATOR_DN	event.attackerUserId
	CONTAINER_DN	event.attackerUserPrivileges
	WORKFLOW_PROCESS_ID	event.deviceCustomNumber2
	ACTION	event.deviceCustomString1
	CONTAINER_NAME	event.deviceCustomString2
	CONTAINER_DN	event.deviceCustomString3
	ENTITY_NAME	event.deviceCustomString4
	ENTITY_DN	event.deviceCustomString5
	COMMENTS	event.deviceCustomString6

AUDIT_MGMT_TARGET table and ArcSight event field mapping	
AUDIT_EVENT Column	**ArcSight event field Mapping**
TARGET_ENTITY_NAME	event.targetUserName
TARGET_ENTITY_TYPE	event.targetUserId
TARGET_ENTITY_DN	Event.targetUserPrivileges

Manual event field Mapping	
Event field	**Value**
event.deviceVendor	"IBM"
event.deviceProduct	"TIM"
event.deviceFacility	"0-11"
event.deviceCustomNumber1Label	"TIMEventID"
event.deviceCustomNumber2Label	"WorkFlowProcessID"
event.deviceCustomString1Label	"ACTION"
event.deviceCustomString2Label	"original"
event.deviceCustomString3Label	"original_Container_DN"
event.deviceCustomString4Label	"Service_Name"
event.deviceCustomString5Label	"Service_DN"
event.deviceCustomString6Label	"COMMENTS"

Event field mapping for "AccountManagement" event

AUDIT_EVENT table and ArcSight event field mapping		
Column Name and Value	**AUDIT_EVENT Column**	**ArcSight event field Mapping**
ITEM_EVENT_CATEGORY If value = AccountManagement	ITIM_EVENT_CATEGORY	event.name
	ID	event.deviceCustomNumber1
	TIMESTAMP	event.endTime
	ENTITY_TYPE	event.message
	RESULT_SUMMARY	event.deviceAction
	INITIATOR_NAME	event.attackerUserName
	INITIATOR_DN	event.attackerUserId
	CONTAINER_DN	event.attackerUserPrivileges
	ENTITY_NAME	event.targetUserName
	ENTITY_DN	event.targetUserId
	ENTITY_TYPE	event.targetUserPrivileges
	WORKFLOW_PROCESS_ID	event.deviceCustomNumber2
	ACTION	event.deviceCustomString1
	COMMENTS	event.deviceCustomString6

AUDIT_MGMT_PROVISIONING table and ArcSight event field mapping	
AUDIT_EVENT Column	**ArcSight event field Mapping**
OWNER_NAME	event.deviceCustomString2
OWNER_DN	event.deviceCustomString3
SERVICE_NAME	event.deviceCustomString4
ACCESS_NAME	event.deviceCustomString5

Manual event field Mapping	
Event field	**Value**
event.deviceVendor	"IBM"
event.deviceProduct	"TIM"
event.deviceFacility	"0-12"
event.deviceCustomNumber1Label	"TIMEventID"
event.deviceCustomNumber2Label	"WorkFlowProcessID"
event.deviceCustomString1Label	"ACTION"
event.deviceCustomString2Label	"targetFullName"
event.deviceCustomString3Label	"targetDN"
event.deviceCustomString4Label	" targetUserServiceBelong"
event.deviceCustomString5Label	" targetAccesAcquired"
event.deviceCustomString6Label	"COMMENTS"

Event field mapping for "DelegateAuthority" event

AUDIT_EVENT table and ArcSight event field mapping		
Column Name and Value	**AUDIT_EVENT Column**	**ArcSight event field Mapping**
ITEM_EVENT_CATEGORY If value = AccountManagement	ITIM_EVENT_CATEGORY	event.name
	ID	event.deviceCustomNumber1
	TIMESTAMP	event.endTime
	ENTITY_TYPE	event.message
	RESULT_SUMMARY	event.deviceAction
	INITIATOR_NAME	event.attackerUserName
	INITIATOR_DN	event.attackerUserId
	CONTAINER_DN	event.attackerUserPrivileges
	ENTITY_NAME	event.targetUserName
	ENTITY_DN	event.targetUserId
	ENTITY_TYPE	event.targetUserPrivileges
	WORKFLOW_PROCESS_ID	event.deviceCustomNumber2
	ACTION	event.deviceCustomString1
	CONTAINER_NAME	event.deviceCustomString2
	CONTAINER_DN	event.deviceCustomString3
	COMMENTS	event.deviceCustomString6

AUDIT_MGMT_DELEGATE table and ArcSight event field mapping	
AUDIT_EVENT Column	**ArcSight event field Mapping**
DELEGATE_NAME	event.deviceCustomString2
DELEGATE_DN	event.deviceCustomString3
DELEGATE_START_TIME	event.deviceCustomDate1Label
DELEGATE_END_TIME	event.deviceCustomDate2Label

Manual event field Mapping	
Event field	**Value**
event.deviceVendor	"IBM"
event.deviceProduct	"TIM"
event.deviceFacility	"0-13"
event.deviceCustomNumber1Label	"TIMEventID"
event.deviceCustomNumber2Label	"WorkFlowProcessID"
event.deviceCustomString1Label	"ACTION"
event.deviceCustomString2Label	"original"
event.deviceCustomString3Label	"original_Container_DN"
event.deviceCustomString4Label	"accountOfAccoutAuthoDelegated"
event.deviceCustomString5Label	"accountDNofDelegation"
event.deviceCustomString6Label	"COMMENTS"
event.deviceCustomDate1Label	"delegationStartTime"
event.deviceCustomDate2Label	"delegationEndTime"

Event field mapping for all other events (default map)

AUDIT_EVENT table and ArcSight event field mapping	
ID	event.deviceCustomNumber1
TIMESTAMP	event.endTime
ENTITY_TYPE	event.message
RESULT_SUMMARY	event.deviceAction
INITIATOR_NAME	event.attackerUserName
INITIATOR_DN	event.attackerUserId
CONTAINER_DN	event.attackerUserPrivileges
WORKFLOW_PROCESS_ID	event.deviceCustomNumber2
ENTITY_TYPE	event.deviceCustomString1
ACTION	event.deviceCustomString2
CONTAINER_NAME	event.deviceCustomString3
ENTITY_DN	event.deviceCustomString4
ENTITY_NAME	event.deviceCustomString5
COMMENTS	event.deviceCustomString6
Manual event field Mapping	
Event field	**Value**
event.deviceVendor	"IBM"
event.deviceProduct	"TIM"
event.deviceFacility	"default parser"
event.deviceCustomNumber1Label	"TIMEventID"
event.deviceCustomNumber2Label	"WorkFlowProcessID"
event.deviceCustomString1Label	"policyActionType"
event.deviceCustomString2Label	"ACTIONl"
event.deviceCustomString3Label	"attackerContainerName"
event.deviceCustomString4Label	"ENTITY_DN"
event.deviceCustomString5Label	"ENTITY_NAME"
event.deviceCustomString6Label	"COMMENTS"

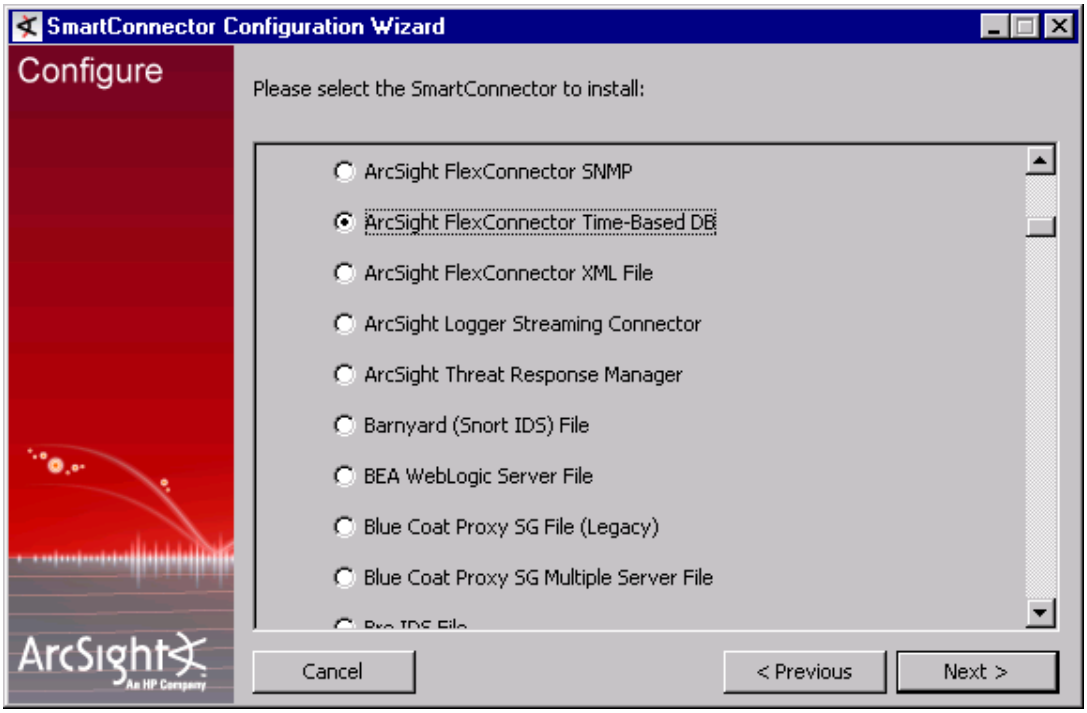
Section 5. Installation the flexConnector

Step 1. Install the SmartConnector (latest release) and select all the default option except for the screen that appear on the next step.

Step 2. Select "ArcSight FlexConnector Time-Based DB".

Step 3. Select "ArcSight FlexConnector Time-Based DB".

Figure 4 - FlexConnector Installation selection

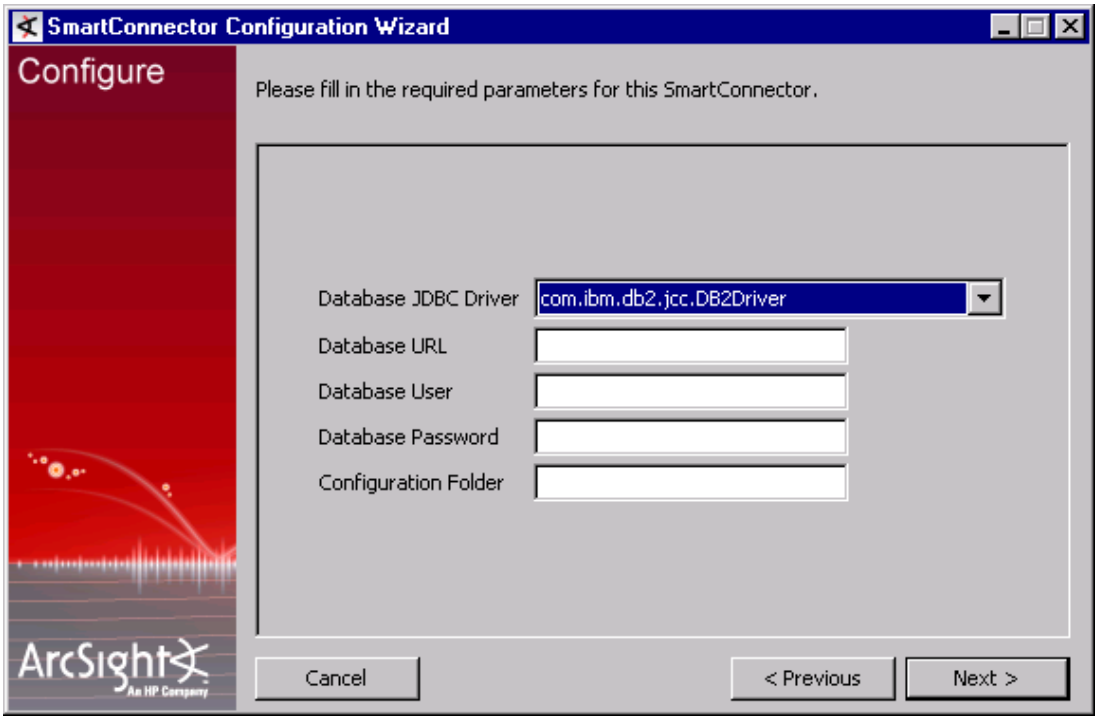


Step 4. Create a directory named "TIM" under $ARCSIGHT_HOME\current\user\agent\flexagent

Step 5. Copy the file "tim.sdktbdatabase.properties" in the folder (see section 4 for the file): $ARCSIGHT_HOME\current\user\agent\flexagent\TIM

Step 6. Select "com.ibm.db2.jcc.DB2Driver".

Figure 5 - Database JDBC driver selection



Step 7. Now, enter the good parameter in the field.

Database URL : jdbc:db2://*ip_address_of_the_db_server*:*tcp_port_listener*/*tim_database_name*

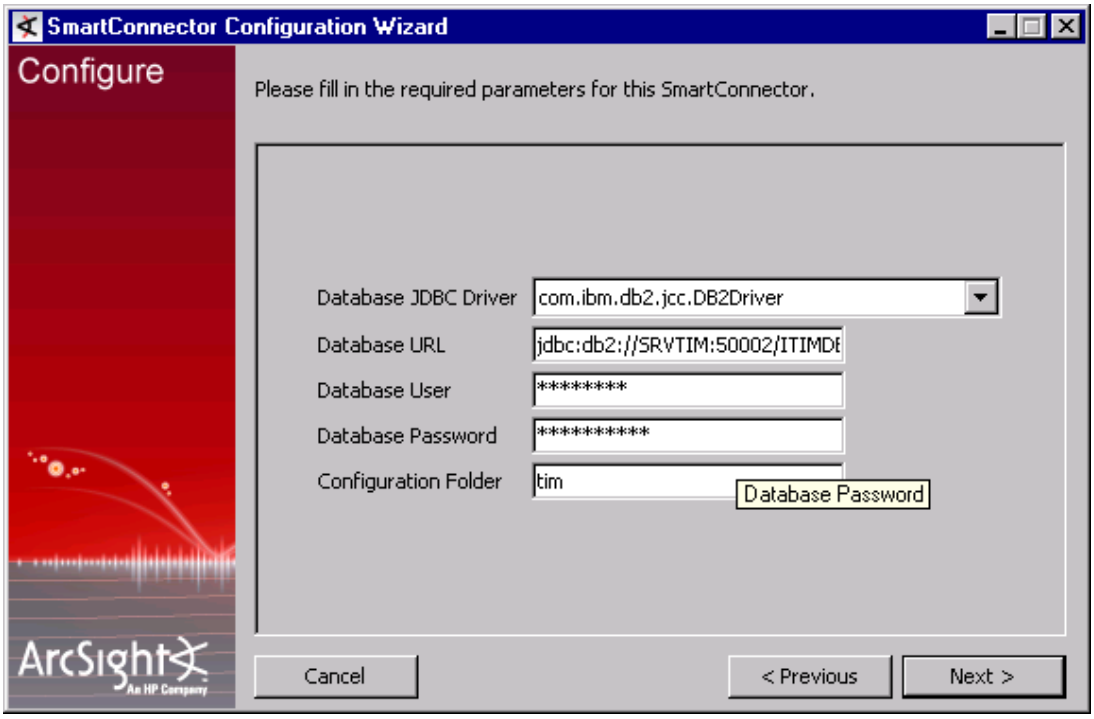
For this case : jdbc:db2://SRVTIM:50002/ITIMDB

Database User : *Enter the username of your ITIM user*

Database Password : *Enter the password of the username that you have entered in the previous field.*

Configuration Folder : TIM

Figure 6 - Database connection details



Section 6. Understanding "tim.sdktbdatabase.properties"

The file contain all information needed to understand everything. Read the section 5 of this document to understand how to install and use it.

tim.sdktbdatabase.properties

Section 7. Categorization file

Copy this file under the directory
$ARCSIGHT_HOME\current\user\agent\acp\categorizer\current\IBM

Create the directory IBM

TIM.csv