Exploration of HP ArcSight Database Connectors and best practices

Neela Jorapur, Farid Merchant
Technical Solution Consultants
Agenda

- Database Connectors overview
- Types of database connectors
- Common issues and troubleshooting tips
- Best practices
- Resources
Exploration of HP ArcSight Database Connectors and best practices

Database Connectors overview
Database Connector overview

- Uses JDBC/OBDC to connect to the Device Database
- Connector uses SQL query stored in the parser to pull events from the database
- Specific target database and product version identified using Version Query
- MaxID query or LastDate query run to identify where to start pulling events from the table

Note: By Default, connector will start retrieving data from the time it is installed, it will not retrieve historical data
Database Connector overview

Connection methods

**ODBC (Open DataBase Connectivity)**
- Windows based

**JDBC (Java DataBase Connectivity)**
- OS independent
- Uses drivers supplied by DB Vendors
- Drivers for SQL Server needs to be downloaded and copied to the connector directory by users; Other drivers are built-in the connector (Sybase, Oracle)
Exploration of HP ArcSight Database Connectors and best practices

Types of Database Connectors
Types of Database Connectors: ID based

- ID used to retrieve events from the device database
- Sample database events

<table>
<thead>
<tr>
<th>EventId</th>
<th>Incident Time</th>
<th>Signature</th>
<th>SourceIP</th>
<th>Destination IP</th>
<th>Priority</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>123456</td>
<td>09/01/05 12:56:00</td>
<td>Port Scan</td>
<td>9.10.11.12</td>
<td>13.14.15.16</td>
<td>1</td>
<td>TCP</td>
</tr>
<tr>
<td>123457</td>
<td>09/01/05 12:54:00</td>
<td>ICMP Failure</td>
<td>1.2.3.4</td>
<td>5.6.7.8</td>
<td>3</td>
<td>ICMP</td>
</tr>
</tbody>
</table>

- Examples for ID Based Connectors are:
  - SiteProtector DB
  - MS Forefront DB
  - Symantec Endpoint Protection DB
  - Flex Connector ID Based (<product_name>.sdkbdatabase.properties)
Types of Database Connectors: ID based

Parser example: Site Protector DB Connector

version.order=4
- when multiple parsers are in place, tells the connector which one to try first

version.id=2.1SP9.0/3.0
- If the version.query succeeds, the deviceVersion field is set to the value of version.id

version.query=SELECT 1 FROM Version WHERE AttributeName='ServiceRelease' AND (AttributeValue like '2.9%' OR AttributeValue like '3.0%')
- Version query specifies a unique entity in the database schema that differentiates it from other database versions
- Version query used only at startup time
Types of Database Connectors: ID based

Parser example: Site Protector DB Connector

maxid.query = select max(SensorDataRowID) from SensorData
• Current id, from where it start retrieving the events

query = select SensorData.SensorGUID, SensorData.SensorDataRowID as RowID, ...
FROM AlertType WITH (NOLOCK).....WHERE SensorData.SensorDataRowID > ? ORDER BY SensorData.SensorDataRowID
• Retrieves data using the above query starting from value greater than max id value
Types of Database Connectors: Time based

- Timestamp used to retrieve events from the device database
- Sample database

<table>
<thead>
<tr>
<th>EventId</th>
<th>Incident Time</th>
<th>Signature</th>
<th>SourceIP</th>
<th>Destination IP</th>
<th>Priority</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCC-DDD</td>
<td>09/01/05 12:56:00</td>
<td>Port Scan</td>
<td>9.10.11.12</td>
<td>13.14.15.16</td>
<td>1</td>
<td>TCP</td>
</tr>
<tr>
<td>AAA-BBB</td>
<td>09/01/05 12:54:00</td>
<td>ICMP Failure</td>
<td>1.2.3.4</td>
<td>5.6.7.8</td>
<td>3</td>
<td>ICMP</td>
</tr>
</tbody>
</table>

- Examples of Time based connectors are:
  - Microsoft Audit Collection System DB
  - Microsoft Sharepoint Server DB
  - Flex Connector: Time Based (<product_name>.sdktbdatabase.properties)
Types of Database Connectors: Time based

Parser example: Sharepoint DB Connector

version.order=0
• when multiple parsers are in place, tells the connector which one to try first

version.id=2013
• If the version.query succeeds, the deviceVersion field is set to the value of version.id

version.query=SELECT top 1 SiteId from AllWebs
• Version query specifies a unique entity in the database schema that differentiates it from other database versions
• Version query used only at startup time
Types of Database Connectors: Time based

Parser example: Sharepoint DB Connector

\[ \text{lastdate.query}=\text{select max(Occurred) from AuditData} \]

• Current timestamp, from where it start retrieving the events

\[ \text{query}=\text{select TOP 1000 AuditData.Siteid Site_ID, AuditData.ItemID as Item_ID, ...} \]
\[ \text{FROM AuditData.....WHERE AuditData.Occurred } \geq ? \  \text{ORDER BY AuditData.Occurred} \]

• Retrieves data using the above query starting from value greater than max timestamp value
Types of Database Connectors: Blend of DB & file

Microsoft SQL Server Multiple Instance Audit DB

• Access the database only to find the version
  – fn_trace_gettable is Microsoft developed function which returns trace file information in a table format. This system function provides a mechanism for querying trace data stored in a file (trace_filename.trc).

• Reads the trace files locally or remotely

• Current file cannot be accessed by connector till the lock is released by SQL server.

• After processing the trace file, connector has the option to rename or delete the trace file.
## Types of Database Connectors: Blend of DB & file

### Microsoft SQL Server Multiple Instance Audit DB  
(Configuration path)

<table>
<thead>
<tr>
<th></th>
<th>Trace File Local Folder</th>
<th>Connector Data Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local</strong></td>
<td>C:\Program Files\SQL Server\MS SQL\Data</td>
<td>C:\Program Files\SQL Server\MS SQL\Data</td>
</tr>
<tr>
<td><strong>Remote (Connector on Windows)</strong></td>
<td>C:\Program Files\SQL Server\MS SQL\Data</td>
<td>Mapped (z:\Data)</td>
</tr>
<tr>
<td><strong>Remote (Connector on Linux)</strong></td>
<td>C:\Program Files\SQL Server\MS SQL\Data</td>
<td>/mnt/mssql</td>
</tr>
</tbody>
</table>

**Note:** When running the SmartConnector as a service, mapped drives do not work. For a service, use the remote network shared drives in the UNC Notation. (For example \servername.name.domain.com\foldername)
Types of Database Connectors: Blend of DB & file

Parser example: Microsoft SQL Server Multiple Instance Audit DB

version.order=0
• when multiple parsers are in place, tells the connector which one to try first

version.id=2005/2008/2012/2014
• If the version.query succeeds, the deviceVersion field is set to the value of version.id

version.query=select count(*) from master.sys.dm_exec_connections
• Version query specifies a unique entity in the database schema that differentiates it from other database versions
• Version query used only at startup time
Types of Database Connectors: Blend of DB & file

Parser example: Microsoft SQL Server Multiple Instance Audit DB

SELECT TOP 1 * FROM ::fn_trace_gettable('$TRACE_FILE_FULL_PATH$', 1)
• This query is used to check if the trace file under consideration is the current trace file SQL Server is writing to. If it is the current trace file, then attempt to execute this query will result in non-writeable query exception or something like that

SELECT CAST(TextData as varchar(1000)) as TextData, NTUserName, NTDomainName, HostName, ServerName, ApplicationName, LoginName, SessionLoginName, SPID, StartTime, …
FROM ::fn_trace_gettable('$TRACE_FILE_FULL_PATH$', 1) where StartTime >= ?
• Retrieves data using the query after the current connector system time.
How to retrieve historical data

• Database Connectors retrieve current data from the device DB by default

• Configuration change needed to enable retrieving historical data from device DB
  − For ID based DB connectors, add the following property in agent.properties file
    Example: agents[0].startatid=2534
  − For Time based DB connectors, add the following property in agent.properties file
    Example: agents[0].startatdate=06/06/2014 09:00:00

• Restart database connector for the change to take effect
Exploration of HP ArcSight Database Connectors and best practices

Common issues and troubleshooting tips
Common issues

- Database drivers
- Network communication
- Authentication
- Configuration
Common issues and troubleshooting tips (1)

**Database drivers**
- Drivers used by the DB connector to communicate to the vendor DB
- For MS SQL server DB, driver needs to be downloaded and copied to the connector folder
  
  $ARCSIGHT_HOME/current/user/agent/lib

**Observations:**
- In the agent.log file, we find the following error:

  Tried version [virusscan/epo3.x]. ERROR: [java.sql.SQLException: No suitable driver found for jdbc:sqlserver://xxxx.org;DatabaseName=xxx
  at java.sql.DriverManager.getConnection(DriverManager.java:602)
  at java.sql.DriverManager.getConnection(DriverManager.java:185)
Common issues and troubleshooting tips (1)

**Possible causes**

- ODBC drivers used in the Non Windows environment where the connector is installed
- JDBC/ODBC URL incorrectly configured (format not as suggested in the connector configuration guide)
- JDBC driver for MS SQL Server placed at incorrect location instead of `<connector home>/current/user/agent/lib`
- JDBC version incompatible with the vendor DB version and type
Common issues and troubleshooting tips (2)

Connection between the connector and the device DB
• Connector not able to communicate to the Database.

Observation
• In the agent.log we find the following error


  INFO  | jvm 1  | 2013/09/12 13:31:33 | Tried version [5.0]. ERROR: [The TCP/IP connection to the host xxxx, port 1433 has failed. Error: “Connection refused: connect. Verify the connection properties. Make sure that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port. Make sure that TCP connections to the port are not blocked by a firewall.”.]
Common issues and troubleshooting tips (2)

Possible causes

• Network port used for communication is blocked by firewall
• Database name or port is wrongly configured on the connector DB
• Connector server IP is not configured in the DB for it to allow to communicate with the connector server
• Query timed out
  • Result retrieved is too large leading to time out because of the time taken to generate and return results
  • Database unindexed
Common issues and troubleshooting tips (3)

Authentication
• User used in the connector needs privilege to make connection to the DB

Observation
• In the agent.log we find the following error

```
INFO | jvm 1 | 2014/08/06 10:09:09 | Tried version [viruscan8.x/epo4.5&5.0]. ERROR: [[Microsoft] [ODBC SQL Server Driver][SQL Server]Login failed for user ‘xxxxxx’.]
```
Common issues and troubleshooting tips (3)

Possible causes
Required privilege is not provided to user which is used in the connector configuration, it should have the below privileges.

- SELECT
- CONNECT
Common issues and troubleshooting tips (4)

Configuration

• For Symantec Endpoint Protection (SEP) & McAfee ePO there are many modules with different versions are supported by connector:

• Example: For SEP Connector
  - alerts, agent-security, agent-traffic and more modules are supported

Observation

• In the agent.log we find the following error for modules not configured

  Example 1: INFO | jvm 1 | 2012/03/06 15:30:22 | [Tue Mar 06 15:30:21 BRT 2012] [ERROR] Device connection to [jdbc:sqlserver://10.14.0.37\sepm:1433;DatabaseName=sem5\xxxxx] down. (Unable to detect database version.

  INFO | jvm 1 | 2012/03/06 15:30:22 | Tried version [12]. ERROR: [Invalid object name 'AGENT_TRAFFIC_LOG_1'.]

  INFO | jvm 1 | 2012/03/06 15:30:22 | Tried version [11]. ERROR: [Invalid object name 'ALERTS'.]
Common issues and troubleshooting tips (4)

Tried version [policy_auditor5.1/epo4.x]. ERROR: [Query returned 0 rows]

Possible causes

• By default all the event types (module) are selected in the configuration without the knowledge of which module and version configured in the environment
• Configure only those module/version which are installed in the environment
Exploration of HP ArcSight Database Connectors and best practices

Best practices
Best practices

• ODBC Driver should be used for Windows environment only
• User used in the connector configuration should have the required permission to connect and retrieve the data from the device database
• The JDBC Driver version should be compatible with the device vendor DB version/type
• JDBC Driver for MS SQL Server should be placed in <connector home>/current/user/agent/lib
• Firewall should not block the port used for communication between the connector server and the database server
• Connector server should be geographically close to the DB server to avoid network latency
• The modules/event types configured in the connector should match the modules/event types configured in the device DB
Best practices (continued)

- Confirm that the connector supports all configured event types for the DB version in use
- When expected events are not being retrieved by the connector, run the DB connector query with a DB client and examine the records returned
- To isolate permission issues, use third party JDBC client to test the credentials configured in the DB connector
- To use JDBC driver with SmartConnectors that connect to Microsoft SQL Servers using Windows Authentication only.
  - Use the sqljdbc4.jar driver.
  - Add “integratedSecurity=true” to the JDBC URL entry for the connection to your database.
  - Copy the sqljdbc_4.0\enu\auth\x86\sqljdbc_auth.dll file from the driver to the $ARCSIGHT_HOME/jre/bin directory.
  - For the sqljdbc_auth.dll, the x86 version is used as the connector JVM is only 32-bit.
  - Example: jdbc:sqlserver://mysqlserver:1433;DatabaseName=mydatabase;integratedSecurity=true
Q&A
For more information

Attend these sessions

• TB3259, Gain tips, tricks and best practices for assessing the health of your HP ArcSight ESM Solution (Thursday, 9:00 AM)

After the event

• Stop by at the Support Booth and meet the expert engineers
• Provide valuable feedback on how support can serve you better

Your feedback is important to us. Please take a few minutes to complete the session T3113 survey.
Please give me your feedback

**Session** TT3113  **Speakers** Farid Merchant & Neela Jorapur

Please fill out a survey.

Hand it to the door monitor on your way out.

Thank you for providing your feedback, which helps us enhance content for future events.
Thank you