Database Activity Monitoring vs Database Performance Monitoring

*It’s Not Just Another DB2 Monitor*

Michael Figaro
Security Engineer
Mainframe Systems
Imperva
michaelfigaro@imperva.com

June 22, 2017
Agenda

- The Activity Monitor project
- The Real Goal
  - It’s probably DCAP
- The Differences Between DCAP and Performance Monitoring
- DCAP – The Core Elements
- Controlling Monitoring
- Common Use Cases
- DCAP Reliability and Performance
- Make vs Buy
- Additional Considerations
The Activity Monitor Project
It’s easy to go to the Sun, you just have to do it at night.

https://www.pinterest.com/pin/508062401697377763/
Going to the Sun at night:
"Database activity monitoring, it’s just another monitor, right?"

https://simpleprogrammer.com/2017/03/13/dealing-with-your-boss/

Your boss walks up to your cube and says, “Hey, we’ve got this program the Security Team asked us to install. It has the ability log every activity that ever occurs on DB2. What do you think? You should be able to knock it out in a couple of days. It’s just another monitor, right?”
What are some questions that immediately come to your mind?

- What are they REALLY trying to do?
- What kind of stake should I want to have in this project?
  - Be educated about the subject. That is what we are doing right now.
- Do they really THINK they can monitor everything?
- Do they really NEED to monitor everything?
- What is this going to do to DB2 reliability?
- What is this going to do to resource consumption?
- Why don’t we make, instead of buy (using perf monitor as input)?
…more questions to consider.

• How much work is it going to be to install/maintain?
• What will my role be in the project? (identify sensitive data).
• Where is all this data going to go?
• What are some other desirable characteristics of DAM solutions?
The Real Goal
What are they really trying to do?

• Your manager and security team may not call it this, but “DCAP” is probably what they are trying to do?

• Who knows what DCAP stands for?
Big Picture Key Components

Gartner Market Guide for “Data-Centric Audit and Protection” (DCAP)

Figure 1. Summary of the Core DCAP Capabilities Offered by Vendors in Each Segment

- Data Security Policy
- Data Classification and Discovery
- Data Security Controls
- Data Activity Monitoring
- Assessment and Monitoring of User Roles and Permissions
- User Monitoring and Auditing
- Enforcement
- Behavior Analysis, Alerting, Reporting
- Block, Encrypt, Tokenize, Mask, Quarantine

Source: Gartner (December 2015)

Source: Gartner, Market Guide for Data-Centric Audit and Protection, 22 November 2014
What are they really try to do?  
What is DCAP?

• DCAP stands for Data-centric Audit and Protection

• Key Elements
  – Data Security Policy – about the enterprise
    • Discovery and Classification – Servers and Data
    • Data Security Controls (Policies Resulting from Discovery and Classification + Use case).
  – Data Activity Monitoring – about user activity against data
    • User Profiling – based on historical activity patterns
    • User Monitoring and Auditing – for compliance and forensics
  – Enforcement – about the actual protection
    • Alerting, Reporting, Behavior Analytics
    • Blocking, Masking, Encryption
  – Centralized Management Console

• Performing DCAP is different from performing Performance Monitoring
### Summary of Differences Between Activity and Performance Monitoring

<table>
<thead>
<tr>
<th></th>
<th>Activity Monitoring</th>
<th>Performance Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Who does it?</strong></td>
<td>Security Team</td>
<td>Sysprog/DBA</td>
</tr>
<tr>
<td><strong>What do they do it against?</strong></td>
<td>DBMS events of interest as defined by “Data Security Policy”</td>
<td>Badly performing SQL</td>
</tr>
<tr>
<td><strong>When do they monitor?</strong></td>
<td>Always</td>
<td>During a performance event</td>
</tr>
<tr>
<td><strong>Why do they monitor?</strong></td>
<td>Security and Compliance</td>
<td>Response time and resource use</td>
</tr>
<tr>
<td><strong>Role – Sysprog</strong></td>
<td>Installs collector</td>
<td>Installs collector/performs monitoring</td>
</tr>
<tr>
<td><strong>Role - DBA</strong></td>
<td>May help develop Data Security Policy</td>
<td>Performs monitoring</td>
</tr>
<tr>
<td><strong>Blocking of Activities</strong></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Quantity and Complexity of data retained</strong></td>
<td>More fields, more rows, details</td>
<td>Minimal, summarizations</td>
</tr>
<tr>
<td><strong>Complexity of post-analysis</strong></td>
<td>Complex, Multi Purpose</td>
<td>Simple, Performance related</td>
</tr>
</tbody>
</table>
Database Activity Monitoring Before DCAP

- Log/IFCID based solutions – there were a number of attempts at this
- Impractical from the collecting side.
  - IFCID based was way too expensive.
- Impractical from the storage side.
  - Often stored data on DB2 tables, or generated impractical amounts of records.
- Impractical from the repository side
  - Operational complexity from keeping all those IFCIDs running.
- Impractical from the configurations side
  - Often required schema changes such as “AUDIT ALL”.
- Violated the principles of auditing – depended on management by privileged users.
- Failed to deliver use case requirements.
  - They tended to deliver data instead of the backend facilities necessary to use the data.
A Summary of DCAP Goals

• Automatic discovery of your sensitive data
• Constant automated surveillance
  • Capture everything that matters
• Low resource consumption
• Avoid the regulatory impact of non-compliance
• Avoid the financial impact of a breach
• Know the impact and scope of a breach
• Instant notification of suspicious behavior
• A single repository for all your audit data
• Protection through sophisticated blocking policies
DCAP Blocking

- DCAP blocking actually stops work in progress based on your “Data Security Policy”.
- DCAP blocking based on rules that are not part of your regular security system.
- Blocking can be at local (OS) or network level.
- Blocking can be based on user behavior analytics. (user based)
  - The user is doing something they don’t usually do.
    - Select a lot of rows.
    - Accessing an object in a way they never have before.
  - The user is accessing data from a new location or outside of their usual hours.
- Blocking can be based on an activity that is inherently dangerous (object based)
  - Selecting a large number of rows from a sensitive table. (Extrusion event).
The Differences Between DCAP and Performance Monitoring
DCAP vs Performance Monitoring – Operational Characteristics

• Always on – higher availability standards then for performance.
• Monitor access of data, not the performance of those accesses.
• **Must** be ready every time DB2 starts
• Collects larger volumes of data
• Collects a wider breadth of data (who, what, when, where, how).
• Collects different kinds of events other than just SQL.
• Collects file system events – LDS, BSDS, etc
• Classification – locate sensitive data.
• Audit and Security Policy Driven
• Joint control between systems and security (hopefully mostly security)
• Blocking can be included as part of PROTECTION.
What kind of stake should I want to have in this project? (Interested party, participant and or admin?)

• Depends on if you are a sysprog/DBA or programmer
  – A lot of DBAs end up being admins or participants. (ex oracle people, etc).

• Identify z/OS tables to monitor. (DBA’s maybe DB2 app pgmrs).

• Installer/maintainer of z/OS collector

• Reviewer
  – Performance
    • General performance
    • Application Acctg data
    • Agent CPU
  – Operational considerations
    • Console automation
    • Product startup

• There are a lot of types of involvement you don’t want to have.
Do they really THINK they can monitor everything?

• They may already be monitoring everything on smaller RDBMs (MS SQL, Oracle, DB2 LUW).
• That depends on how they define “monitor”.
  – Ignore - (don’t examine – shouldn’t incur overhead )
  – Examine (but not collect – will incur overhead)
  – Collect
• Do they really THINK they can monitor everything?
  – Monitoring everything is neither realistic or necessary
    • Consider use cases.
      – Example Use case, privileged user monitoring
    • Excluded Trusted work (batch jobs from job scheduling system)
  – There is a different between monitoring and event capture.
    • Theoretically, you could monitor everything and never capture a single event.
    • Event capture 2 Gb per appliance.
What do they actually need to monitor.?

• Do they really NEED to monitor everything? - No
  – The monitoring depends on the scope of the data (which tables they want to monitor)
  – … the filtering capability of the monitor
  – … and the use cases
    • PCI
    • HIPAA
    • SOX
    • Privileged user monitoring.
    • File monitoring
  – Don’t monitor trusted workloads
    • Production Scheduled Batch Jobs
    • MQ/CICS associated with a pool userid, etc.
Low Overhead, Continuous Discovery

Automated discovery of sensitive data

Profile database access and user behavior
Constant Protection for Your Most Important Asset, Your Data

Instant alerts for suspicious data access

Monitor system related events too

Data Masking
Quickly & Easily Become Compliant and Remain There

Compliance related auditing & reporting

Understand what has been accessed, when and by whom
### Centralized Management Console – Collector List

#### Collector List Table

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Alarms</th>
<th>Running Status</th>
<th>Monitored Traffic Types</th>
<th>IP</th>
<th>Host Name</th>
<th>Service Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>990133A4A</td>
<td>Critical</td>
<td>1 Alarm</td>
<td>Disconnected</td>
<td>Database</td>
<td>10.37.100.167</td>
<td>sysa</td>
<td>Multiple</td>
</tr>
<tr>
<td>990133A00</td>
<td>Critical</td>
<td>1 Alarm</td>
<td>Disconnected</td>
<td>Database</td>
<td>10.37.100.167</td>
<td>sysa</td>
<td>Ims</td>
</tr>
<tr>
<td>990135B00</td>
<td>Critical</td>
<td>1 Alarm</td>
<td>Disconnected</td>
<td>Database</td>
<td>10.37.100.168</td>
<td>sysb</td>
<td>Ims</td>
</tr>
<tr>
<td>99014A00</td>
<td>Critical</td>
<td>1 Alarm</td>
<td>Disconnected</td>
<td>Database</td>
<td>10.37.100.167</td>
<td>sysa</td>
<td>Ims</td>
</tr>
<tr>
<td>99014B00</td>
<td>Critical</td>
<td>1 Alarm</td>
<td>Disconnected</td>
<td>Database</td>
<td>10.37.100.168</td>
<td>sysb</td>
<td>Ims</td>
</tr>
<tr>
<td>ARWAGEN3</td>
<td>Normal</td>
<td>-</td>
<td>Running</td>
<td>Database</td>
<td>10.37.100.169</td>
<td>sysc</td>
<td>Db2</td>
</tr>
<tr>
<td>ARWAGENT</td>
<td>Critical</td>
<td>1 Alarm</td>
<td>Disconnected</td>
<td>Database</td>
<td>10.37.100.169</td>
<td>sysc</td>
<td>None</td>
</tr>
</tbody>
</table>

#### Agent Name: 990133A4A

**General Details**

**Settings**

**Subsystems**

**Activity Log**

#### General Settings

Default Server Group:

#### Monitoring Policies

Monitoring Policy: **Standard Monitoring Policy**

#### Fictitious Network Parameters

- Source IP Address: 
- Destination IP Address: 10.37.100.167
- Destination Port: 

#### Blocking

Enable blocking: □
Centralized Management Console
collector configuration and status
### Centralized Management Console – Monitoring Rule

<table>
<thead>
<tr>
<th>Order</th>
<th>Rule Name</th>
<th>Service Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Sensitive Tables and Their Untrusted Users</td>
<td>DB2</td>
</tr>
<tr>
<td></td>
<td>Match:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DB2 User is [At Least One]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Table is [At Least One]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>z/OS Operations is at least one of [user_maintenance, utilities, update, insert, binding_commands, commands, user_authorization, select, object_maintenance, delete]</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Trusted Users - Exclude</td>
<td>DB2</td>
</tr>
<tr>
<td></td>
<td>Match:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DB2 User is [At Least One]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>z/OS Operations excludes all [utilities, object_maintenance, user_authorization, insert, commands, delete, binding_commands, select, user_maintenance, select_with_row_count]</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Trusted Jobs - Exclude</td>
<td>DB2</td>
</tr>
<tr>
<td></td>
<td>Match:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Job Name is at least one of [JOB0002, JOB0003]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>z/OS Operations excludes all [select, update, user_maintenance, insert, user_authorization, commands, object_maintenance, binding_commands, select_with_row_count, utilities]</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>Trusted DB2 Plans - Exclude</td>
<td>DB2</td>
</tr>
<tr>
<td></td>
<td>Match:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DB2 Plan is at least one of [^TRUSTPL2, ^TRUSTPL1, ^TRUSTPL3]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>z/OS Operations excludes all [insert, user_maintenance, update, select, user_authorization, binding_commands, object_maintenance, delete, commands, utilities]</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>Out of Scope DB2 Conn Types - Exclude</td>
<td>DB2</td>
</tr>
<tr>
<td></td>
<td>Match:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DB2 Connection Type is [DRDA]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>z/OS Operations excludes all [select, utilities, user_maintenance, binding_commands, user_authorization, commands, object_maintenance, update, delete, insert]</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>Privileged Users</td>
<td>DB2</td>
</tr>
<tr>
<td></td>
<td>Match:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DB2 User is [At Least One]</td>
<td></td>
</tr>
</tbody>
</table>
Centralized Management Console – Collection Environment Status and Security Alerts

- Status of the Gateway Collector Appliances
- Collector Performance
- Real-Time Security Alerts
- Status of the DB Servers being Monitored
- Real-Time Collector System Events
Profiling - Threat Management – Abnormal Behavior

Database and Schema Accessed

Database User

Database Access Method

Operation Performed

Database Objects Accessed
Data Classification…

Scans scheduled regularly to locate sensitive data that is new on the database
• Metadata – for sensitive data formats and names
• Data – possibly sampling

• DBAs may be asked to participate in the creation and analysis of these scans
• The scan may need to have sufficient privilege to read the data and the catalog.
  • DB2 DATAACCESS privilege is one option
Data Classification…

After classification scan has been done, activity against sensitive objects s/b clear
Capture and Alert On Access to Specific Data…2

An Alert is triggered and posted whenever a matching value is found in the specified dictionary

<table>
<thead>
<tr>
<th>No.</th>
<th>Updated</th>
<th>#</th>
<th>Alert Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>28036</td>
<td>05:54:09</td>
<td>2</td>
<td>SG Test 3</td>
</tr>
<tr>
<td>28037</td>
<td>05:54:09</td>
<td>1</td>
<td>VIP Client Accessed</td>
</tr>
<tr>
<td>28034</td>
<td>10/4/16</td>
<td>1</td>
<td>Unauthorized Source Application cicsd51a by cics from 255.255.255.255</td>
</tr>
<tr>
<td>28035</td>
<td>10/4/16</td>
<td>1</td>
<td>Unauthorized Database and Schema cics by cics</td>
</tr>
</tbody>
</table>
Detailed Audit Trail – Retained Permanently

Comprehensive Audit Trail for DB2

<table>
<thead>
<tr>
<th>Reported Period:</th>
<th>02/29/2016, 16:00-03/30/2016, 16:08 (29 Days, 23 hrs)</th>
</tr>
</thead>
</table>

**Select Columns**

<table>
<thead>
<tr>
<th>Time Group - 1 Minute</th>
<th>Source Application</th>
<th>User</th>
<th>Service</th>
<th>Database</th>
<th>Operation</th>
<th>DB Schema</th>
<th>Object</th>
<th>Parsed Query</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 18, 2016 1:05:00 PM</td>
<td>dga2dist</td>
<td>nlm2</td>
<td>DB2 svc</td>
<td>dga2</td>
<td>insert</td>
<td>nsu1 md</td>
<td>2</td>
<td>insert into nsu1 md values (?, ?, ?, ?, current_timestamp)</td>
</tr>
<tr>
<td>March 18, 2016 1:05:00 PM</td>
<td>dga2dist</td>
<td>ses1</td>
<td>DB2 svc</td>
<td>dga2</td>
<td>Select</td>
<td>NSU1 emp</td>
<td>2</td>
<td>select firstname, midinit, lastname into ?, ?, ? from nsu1 emp where empno = ?</td>
</tr>
<tr>
<td>March 18, 2016 1:05:00 PM</td>
<td>dga2dist</td>
<td>nsu1</td>
<td>DB2 svc</td>
<td>dga2</td>
<td>Delete</td>
<td>NSU1 emp</td>
<td>2</td>
<td>delete from nsu1 emp where empno = ?</td>
</tr>
<tr>
<td>March 18, 2016 1:05:00 PM</td>
<td>dga2dist</td>
<td>nlm2</td>
<td>DB2 svc</td>
<td>dga2</td>
<td>Delete</td>
<td>NSU1 emp</td>
<td>2</td>
<td>delete from nsu1 emp where empno = ?</td>
</tr>
<tr>
<td>March 18, 2016 1:05:00 PM</td>
<td>dga2dist</td>
<td>ses1</td>
<td>DB2 svc</td>
<td>dga2</td>
<td>insert</td>
<td>NSU1 emp</td>
<td>2</td>
<td>insert into nsu1 emp values (?, ?, ?, ?, current_timestamp)</td>
</tr>
<tr>
<td>March 18, 2016 1:05:00 PM</td>
<td>dga2dist</td>
<td>nsu1</td>
<td>DB2 svc</td>
<td>dga2</td>
<td>Select</td>
<td>NSU1 emp</td>
<td>2</td>
<td>select firstname, midinit, lastname from nsu1 emp where empno = ?</td>
</tr>
</tbody>
</table>

© 2016 Imperva, Inc. All rights reserved.
## z/OS File Monitoring

### Table 1: z/OS File Audit Rule - All Events - Data

<table>
<thead>
<tr>
<th>Gateway None</th>
<th>User Name</th>
<th>Operation</th>
<th>Folder Path</th>
<th>OS Group Owner</th>
<th>OS User Owner</th>
<th>Object Type</th>
<th>User ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlonPrimary</td>
<td>greg</td>
<td>Read</td>
<td>SV115C</td>
<td>GCG1</td>
<td>TSTX0020</td>
<td>Data Set</td>
<td>0</td>
</tr>
<tr>
<td>AlonPrimary</td>
<td>greg</td>
<td>Read</td>
<td>SV115C</td>
<td>GCG1</td>
<td>TSTX0060</td>
<td>Data Set</td>
<td>0</td>
</tr>
<tr>
<td>AlonPrimary</td>
<td>greg</td>
<td>Read</td>
<td>SV115C</td>
<td>GCG1</td>
<td>TSTX0080</td>
<td>Data Set</td>
<td>0</td>
</tr>
<tr>
<td>AlonPrimary</td>
<td>greg</td>
<td>Read</td>
<td>SV115C</td>
<td>GCG1</td>
<td>TSTX0070</td>
<td>Data Set</td>
<td>0</td>
</tr>
<tr>
<td>AlonPrimary</td>
<td>greg</td>
<td>Read</td>
<td>SV115C</td>
<td>GCG1</td>
<td>TSTX0080</td>
<td>Data Set</td>
<td>0</td>
</tr>
<tr>
<td>AlonPrimary</td>
<td>greg</td>
<td>Rename</td>
<td>/usr/lb/rsa/msgC</td>
<td>0</td>
<td>TSTX0100</td>
<td>File</td>
<td>0</td>
</tr>
<tr>
<td>AlonPrimary</td>
<td>greg</td>
<td>Read</td>
<td>/usr/lb/rsa/msgC</td>
<td>0</td>
<td>TSTX0100</td>
<td>File</td>
<td>0</td>
</tr>
<tr>
<td>AlonPrimary</td>
<td>greg</td>
<td>Modify</td>
<td>/usr/lb/rsa/msgC</td>
<td>0</td>
<td>TSTX0110</td>
<td>File</td>
<td>0</td>
</tr>
<tr>
<td>AlonPrimary</td>
<td>greg</td>
<td>Read</td>
<td>/usr/lb/rsa/msgC</td>
<td>0</td>
<td>TSTX0110</td>
<td>File</td>
<td>0</td>
</tr>
<tr>
<td>AlonPrimary</td>
<td>greg</td>
<td>Read</td>
<td>/usr/lb/rsa/msgC</td>
<td>0</td>
<td>TSTX0120</td>
<td>File</td>
<td>0</td>
</tr>
<tr>
<td>AlonPrimary</td>
<td>greg</td>
<td>Read</td>
<td>/usr/lb/rsa/msgC</td>
<td>0</td>
<td>TSTX0120</td>
<td>File</td>
<td>0</td>
</tr>
<tr>
<td>AlonPrimary</td>
<td>greg</td>
<td>Read</td>
<td>/usr/lb/rsa/msgC</td>
<td>0</td>
<td>TSTX0130</td>
<td>Data Set</td>
<td>0</td>
</tr>
</tbody>
</table>
Controlling Monitoring With Filtering
Desirable characteristics of monitoring policies.

- Easy to specify – The admin probably doesn’t want to be a programmer.
- Good boilerplate examples
  - Something that fits real world
- Exclude by connection type.
- Highly filtering to minimize connection and when possible, overhead.
  - For example things that don’t change during the life the connection should avoid overhead.
Don’t forget Ignore, Examine, Collect

• Just because an event is not collected doesn’t mean it doesn’t cost anything to monitor it.
• For each filter field in the monitoring policy, determine if it can:
  – **Ignore** - (don’t examine – avoid most overhead )
  – **Examine** (but not collect – will incur overhead)
  – **Collect** (will incur more overhead, including network adapter)
What to Monitor => How To Filter => What To Collect =>

Monitor
- Connections: local remote
- SQL (all): static dynamic
- Stored procedures external native
- DDL
- DB2 Utilities
- DB2 Commands
- Plan activity bind/free
- LDS Opens

Filter
- SSID
- Userid
- Object name
- Jobname
- Plans
- Package
- DBRM
- Connection Type
- Qualify with patterns, masking, and lists
- REGEX
- LDS names

Collect
- User: primary secondary remote
- SQL text
- Host variables
- SQL return codes
- Object names
- Jobname
- Timestamp
### An Example Boiler Plate z/OS Agent Monitoring Policy

<table>
<thead>
<tr>
<th>Order</th>
<th>Rule Name</th>
<th>Service Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Sensitive Tables and Their Untrusted Users</td>
<td>DB2</td>
</tr>
<tr>
<td></td>
<td><strong>Match:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- DB2 User is [AtLeastOne]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Table is [AtLeastOne]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- z/OS Operations is at least one of [user_maintenance, utilities, update, insert, binding_commands, commands, user_authorization, select, object_maintenance, delete]</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Trusted Users - Exclude</td>
<td>DB2</td>
</tr>
<tr>
<td></td>
<td><strong>Match:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- DB2 User is [AtLeastOne]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- z/OS Operations excludes all [utilities, object_maintenance, user_authorization, insert, commands, delete, binding_commands, select, user_maintenance, select_with_row_count]</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Trusted Jobs - Exclude</td>
<td>DB2</td>
</tr>
<tr>
<td></td>
<td><strong>Match:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Job Name is at least one of [JOB0002, JOB0003]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- z/OS Operations excludes all [select, update, user_maintenance, insert, user_authorization, commands, object_maintenance, binding_commands, select_with_row_count, utilities]</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>Trusted DB2 Plans - Exclude</td>
<td>DB2</td>
</tr>
<tr>
<td></td>
<td><strong>Match:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- DB2 Plan is at least one of [*TRUSTPL2, *TRUSTPL1, ^TRUSTPL3]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- z/OS Operations excludes all [insert, user_maintenance, update, select, user_authorization, binding_commands, object_maintenance, delete, commands, utilities]</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>Out of Scope DB2 Conn Types - Exclude</td>
<td>DB2</td>
</tr>
<tr>
<td></td>
<td><strong>Match:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- DB2 Connection Type is [DRDA]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- z/OS Operations excludes all [select, utilities, user_maintenance, binding_commands, user_authorization, commands, object_maintenance, update, delete, insert]</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>Privileged Users</td>
<td>DB2</td>
</tr>
<tr>
<td></td>
<td><strong>Match:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- DB2 User is [AtLeastOne]</td>
<td></td>
</tr>
</tbody>
</table>
Common Use Cases
Common Use Cases and their Monitoring requirements.

Depending on your industry, there are a variety of regulations that affect you monitoring requirements. The requirements affect the quantity of data that you monitor and the number of events you collect. This directly correlates to overhead.
PCI Monitoring Requirements

• Falls under Requirement 10 – Regularly monitor and test networks
• **Monitor access to PII**, account and card information
  – Type of event (10.3.2)
  – Date and time (10.3.3)
  – Success or failure (10.3.4)
  – Origin of event (10.3.5)
  – Affected data, component or resource (10.3.6)
• Each user/process should have a unique account solely for their use
• **Privileged** user monitoring
• Monitor access to logs and audit trails of PCI accesses
• Ensure systems and applications are using the correct time
HIPAA monitoring requirements

• HIPAA monitoring requirements
  – 164.308(a)(5)(ii)(C) – Login
  – 164.312(b) – Auditing of accesses to health information
  – 164.308(a)(1)(ii)(D) – Regular review of audit/log information relating to HIPPA

• Tracking repository of access to each customer’s data.
• Masking of PHI from applications and users without a need to know.
SOX monitoring requirements

- SOX sections 302, 404 & 409 require the following to be audited
  - Internal controls (potentially through the COBIT framework)
  - Network activity
  - Database activity (changes, i.e. DDL, and access to logs)
  - Login activity (successful and failed)
  - Account activity
  - User activity
  - SOX relevant Information access

- Audit **updates** to accounting data.
File Monitoring

- All access to DB2 tablespaces outside of DB2 (LDS)
  - Monitor for low level utility access such as DSN1COPY or REPRO
    - This could indicate illicit copying of data
- System configuration file reads and updates
  - Also important for USS
- FTP access to files
  - Where are files being moved to?
- Not a DB2 thing but some customer still keep a lot of data on VSAM. Key value monitoring can produce a lot of events.
- Open close monitoring is cheap
Privileged User Monitoring Requirements

• A pervasive use case
  – Not just for misbehavior, but the loss of credentials too

• Managing the Insider Threat

• All accesses to all DB2
  – Include utility access (specific interest in UNLOAD, DSNTIAUL and COPY)
  – Specifically target ‘LOG NO’ events (i.e REPAIR LOG NO)
  – Object changes (e.g. ALTERing tables to switch AUDIT off)
  – Consider use of DB2 controls, like SECADM, TRUSTED CONTEXTS and DATAACCESS

• All accesses to z/OS file which contain databases (LDSs).
  – Doesn’t have to be a lot of collection since only OPEN needs to be logged.
  – Accesses to configuration files such as DSNZPARM and DSNHDECP
Use cases and the amount of monitoring vs collection they require.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Amount of monitoring</th>
<th>Amount of collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI</td>
<td>Large, all data that if taken could result in credit card abuse.</td>
<td>Large due to the high volume of transactions.</td>
</tr>
<tr>
<td>SOX</td>
<td>All accounting table access, usually a small subset of the DB</td>
<td>Small (Update only, usually a small subset of tables on the system)</td>
</tr>
<tr>
<td>HIPAA</td>
<td>PHI Data + Medical Records</td>
<td>Large, can include history of who accessed an individual's records.</td>
</tr>
<tr>
<td>General PII</td>
<td>Varies, depending on the industry.</td>
<td>Medium, depending on the industry, customer count and transaction rate</td>
</tr>
<tr>
<td>Privileged User</td>
<td>Small if only against privileged objects, otherwise medium</td>
<td>Medium, in general, batch processess/b trusted except for priv user</td>
</tr>
</tbody>
</table>
DCAP – Reliability and Performance
How do I make sure this will not affect DB2 reliability?

• Find out about the architecture of the product
  – The few moving parts the better
  – Make sure the vendor supports their own agent and it is not through a partnership. The software business makes for strange bedfellows.

• Does the installation modify DB2? STEPLIB?

• Make sure the vendor supports their own agent.
  – The software business makes for strange bedfellows.

• Look for a significant install base.

• Watch out for interdependencies with other programs, particularly performance monitors.

• Look for signs of operational maturity
  – Exception handling
    • DB2 starts and stops handled automatically
    • What happens during excessive event collection
z/OS Activity Monitor for DB2 - Single STC per LPAR - Output to appliance.
z/OS Activity Monitor for DB2 - Single STC per DB2 - Output to appliance.
z/OS Activity Monitor for DB2 - Single STC per DB2 – IFICDS - Output to DB2 tables.
z/OS Activity Monitor for DB2 - Single STC per DB2 – IFCIDS - Output to SIEM.
Does anyone knows what SIEM standard for?
System Information and Event Management
What is this going to do to resource consumption?

- What is the going to do to resource consumption?
  - Limit the subsystem, tables and applications monitored
  - Measure DB2 acctg data, db2 subsystems and servers.

- Where the data goes affect resource consumption
  - If DB2 tables, that means that there could be one SQL statement executed for each SQL statement collected.
  - If TCP/IP, consider adapter capacity
  - If SMFfiles…
$3000 to $8000 increase in MLC charges per year for each additional MSU consumed
Considerations for z/OS DAM - Resource Cost

• Frequency of monitored events
  – SQL statement
  – Fetch
  – DDL
  – Privileged user only
  – Utilities
  – Commands

• Collection technique – no IFCIDs please

• Filtering
  – minimize collection, memorize CPU on monitored but not collected work

• Where the data goes - staging to a DB2 table can be expensive.

• Don’t forget network costs.
Considerations for z/OS DAM - Monitoring costs
Most frequent overhead measurement mistakes.

• No measuring at all – then making assumptions.
  – Remember examine, monitor, collect
• Measuring response time, not resource consumption.
• Measuring use a load inducing tool that attempts to achieve a TPS, not a fixed amount of work, the reporting CPU vs TIME instead of CPU vs WORKLOAD
• Measuring in a non-isolated environment, the
• Measuring with an invalid mix.
• Measuring with an invalid monitoring rule – (more or less collection than is realistic.
• Reporting on the wrong address spaces.
• Not reporting on DB2 accounting data.
Make vs Buy
Why don’t we make, instead of buy? (using Perf Monitor data as input)?
Make vs Buy - Challenges

• Separation of duties is difficult to maintain
  – The privileged user built and manages the audit process

• Real time monitoring is difficult to provide
  – Many sources of audit data are batch oriented

• Time, effort, and expertise required to build
  – Security/compliance knowledge
  – Programming skill to integrate data and present to auditor

• Resource usage
  – Some traces have big CPU cost, impact to MLC costs
  – Disk space to store audit data

• DB2 audit data is isolated from other audit data
Build Your Own

DB2 Trace data
- Many different traces
- ALTER Table(s)
- Balance data vs. overhead

Logs/SMF
- Could read trace data here
- RACF, etc.
- no SELECT activity

Repurposed Performance data
- Use a SQL monitoring product to track DML

Work to do:
- Join or rationalize data
- Batch reporting
- Console/GUI
How much work is it going to be to install/maintain?

• Does it require coordinated configurations on other products
  – DB2
  – Performance Monitors
• Does it require modification of applications
• Does it require ongoing operational procedures.
  – IFCIDS starting and stopping, run offloads of data, etc…
  – Alters of DB2 objects?
• Interdependencies on other monitors?
• SMPE or non-SMPE?
• Can it be started and restarted without affecting DB2 or applications
• Who will have the ongoing responsibility of determining that it’s working?
Installation Should be a Task, Not a project.
What will my role be in the project? (identify sensitive data).

• Maintain the agent software
• What will my role be in the project? (identify sensitive data).
  – Identify DB2 specific things they will care about
    • Utilities, commands, connection info, program prep, file system objects.
• Review Monitoring Policies before they are implemented
• Ideally, your solution will integrate with change control systems
  – You want to be brought into the loop on monitoring policy changes
Where is all this data going to go and how will it be used?

- **DB2 Tables**
  - If DB2 tables, that means that there could be one SQL statement executed for each SQL statement collected.

- **SMF**
  - Mics/Homegrown/MXG – usually a “build” home grown solution.

- **DAM product repository**
  - as part of a full on DCAP implementation (auditing and security)

- **SIEM**
  - The loosely defined magic bullet that can supposedly do everything.
  - I think of a SIEM as a security data warehouse on steroids.

- **SOC – do you know what SOC stands for?**
SOC – Security Operations Center
Where is all this data going to go and how will it be used? (An example of a full on DAM implementation)
Actually, it can get crazier than that…

- There can be a lot of pieces to full on Database + **Application** monitoring
- There projects can have a lot of momentum by the time you find out about them
What are some other desirable characteristics of DAM solutions?

• System event monitoring (events that affect the collectors operations)
  – Data stops arriving
  – Audit policy loaded.
  – High collection rate
  – Low collection rate
  – Network adapter saturation
  – New monitoring policy loaded

• Most configuration is by Security team
• Security event analysis and alerts are handled by Security team, not by you.