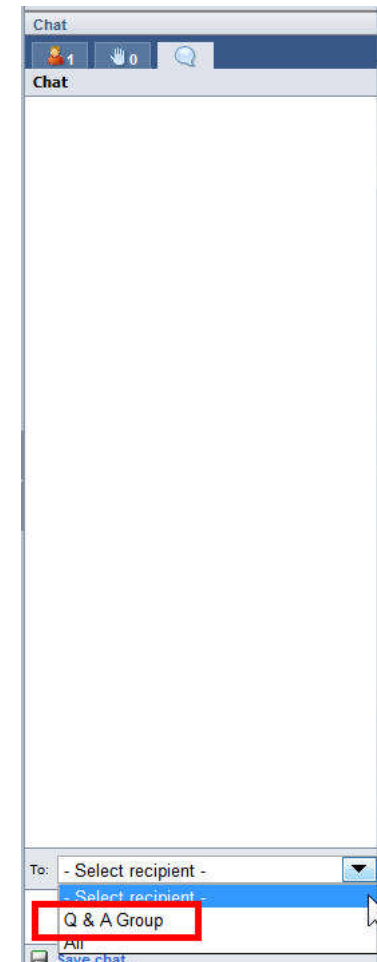
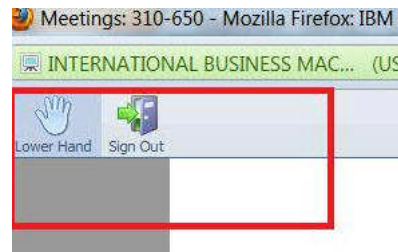


Logistics

- This tech talk is being recorded. If you object, please hang up and leave the webcast now.
- We'll post a copy of slides and link to recording on the Guardium community tech talk wiki page: <http://ibm.co/Wh9x0o>
- You can listen to the tech talk using audiocast and ask questions in the chat to the Q and A group.
- We'll try to answer questions in the chat or address them at speaker's discretion.
 - If we cannot answer your question, please do include your email so we can get back to you.
- When speaker pauses for questions:
 - We'll go through existing questions in the chat



Reminder: Guardium Tech Talks

Next tech talk: How to audit and protect SAP systems with InfoSphere Guardium Data Activity Monitor

Speakers: [Joe Dipietro](#)

Date & Time: Thursday, September 19, 2013

11:30 AM Eastern (1 hour)

Register here: <http://bit.ly/15BqkTq>

- Link to more information about this and upcoming tech talks can be found on the InfoSphere Guardium developerWorks community: <http://ibm.co/Wh9x0o>
- Please submit a comment on this page for ideas for tech talk topics.

What we'll cover today



- **30K-foot overview of InfoSphere Guardium and IBM I**
- An integrated solution for audit and compliance
- Monitoring strategy and use cases
- Step by step – getting started
- FAQ and conclusion



Polling question

The following best describes my knowledge of the topic:

1. I am most knowledgeable in the InfoSphere Guardium solution
2. I am most knowledgeable about IBM i
3. I am pretty knowledgeable about both InfoSphere Guardium and IBM i
4. I am new to both of these areas



Data is the key target for security breaches..... ... and Database Servers Are the Primary Source of Breached Data

Table 10. Compromised assets by percent of breaches and percent of records*

Type	Category	All Orgs		Larger Orgs	
POS server (store controller)	Servers	50%	1%	2%	<1%
POS terminal	User devices	35%	<1%	2%	<1%
Desktop/Workstation	User devices	18%	34%	12%	36%
Automated Teller Machine (ATM)	User devices	8%	<1%	13%	<1%
Web/application server	Servers	6%	80%	33%	82%
Database server	Servers	6%	96%	33%	98%
Regular employee/end-user	People	3%	1%	5%	<1%
Mail server	Servers	3%	2%	10%	2%
Payment card (credit, debit, etc.)	Offline data	3%	<1%	0%	<1%
Cashier/Teller/Waiter	People	2%	<1%	2%	<1%
Pay at the Pump terminal	User devices	2%	<1%	0%	<1%
File server	Servers	1%	<1%	5%	<1%
Laptop/Netbook	User devices	1%	<1%	5%	<1%
Remote access server	Servers	1%	<1%	7%	<1%
Call Center Staff	People	1%	<1%	7%	<1%

WHY?

- Database servers contain your clients' most valuable information
 - Financial records
 - Customer information
 - Credit card and other account records
 - Personally identifiable information
 - Patient records
- High volumes of structured data
- Easy to access

2012 Data Breach Report from Verizon Business RISK Team

http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf



“Go where the money is... and go there often.” - Willie Sutton

InfoSphere Guardium Value Proposition:

*Continuously monitor access to sensitive **data** including databases, data warehouses, big data environments and file shares to....*

1

Prevent data breaches

- Prevent disclosure or leakages of sensitive data



2

Ensure the integrity of sensitive data

- Monitor and control changes to data or unauthorized leakage



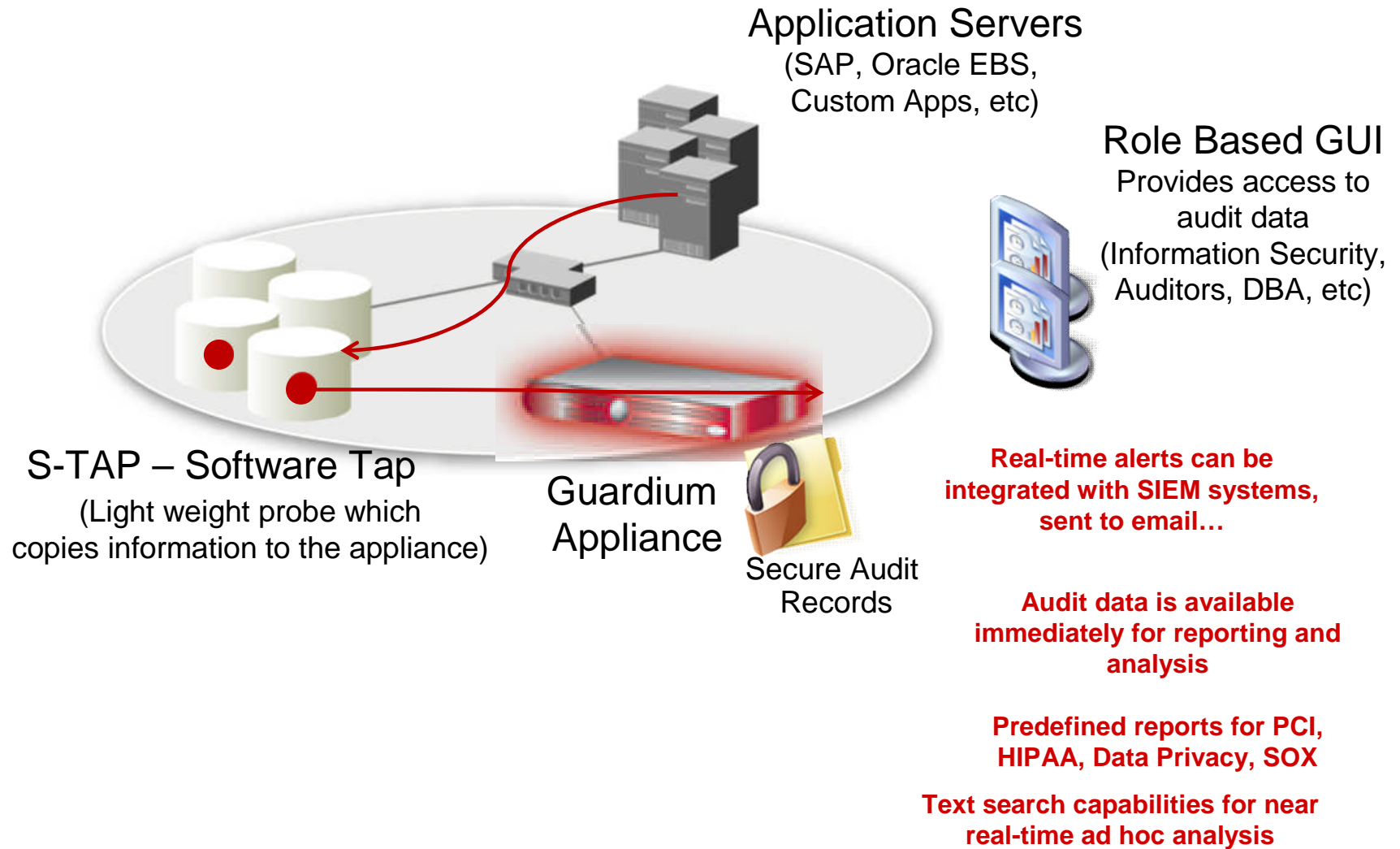
3

Reduce cost of compliance

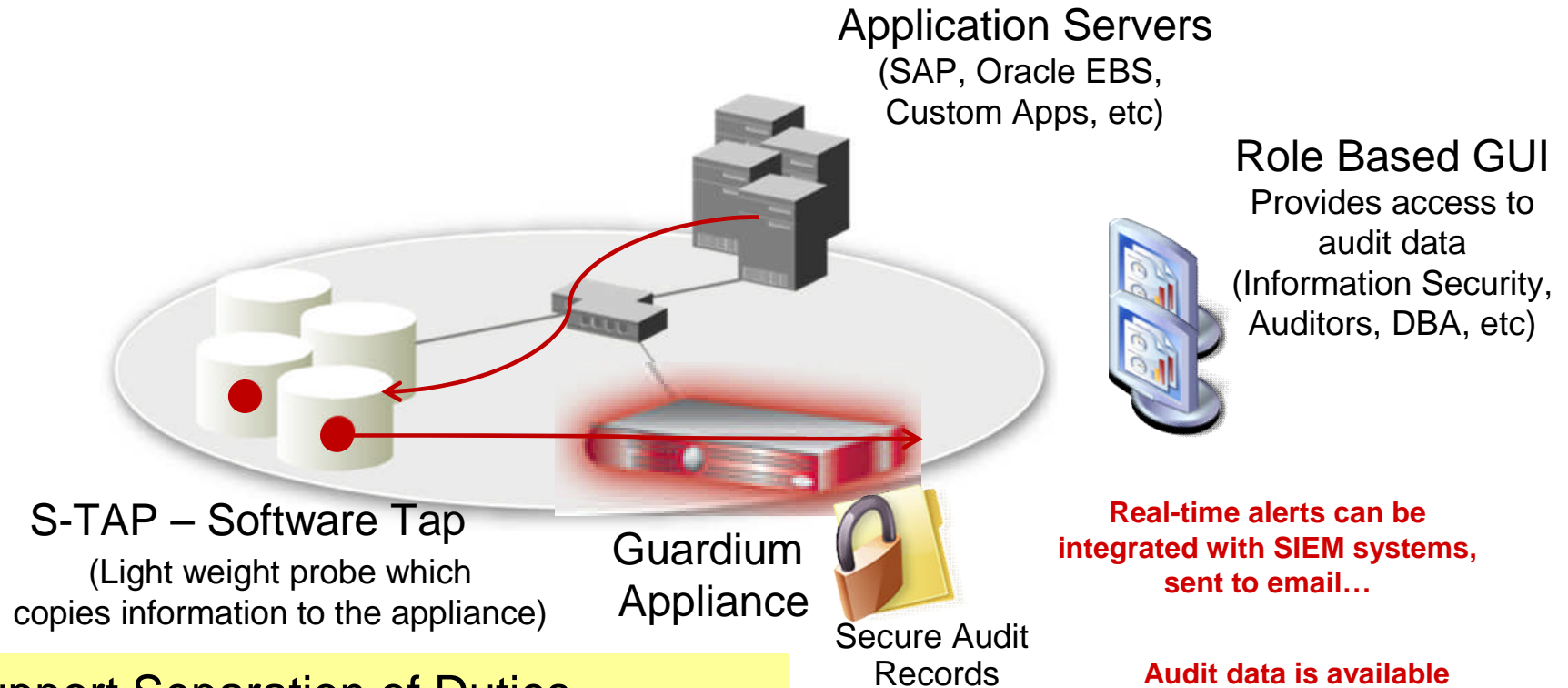
- Automate and centralize controls
 - Across diverse regulations, such as PCI DSS, data privacy regulations, HIPAA, SOX etc
 - Across heterogeneous environments such as databases, applications, data warehouses and Big Data platforms like Hadoop
- Simplify the audit review processes



InfoSphere Guardium Architecture



InfoSphere Guardium Architecture



- Support Separation of Duties
- Collect and normalize data for efficient storage
- Single repository for all audit data
- Data is immediately available and highly secure

Real-time alerts can be integrated with SIEM systems, sent to email...

Audit data is available immediately for reporting and analysis

Predefined reports for PCI, HIPAA, Data Privacy, SOX

Text search capabilities for near real-time ad hoc analysis

The IBM i Business (aka iSeries or AS/400)

More clients run IBM i than any other IBM system platform

- 100,000's of systems in 100,000+ enterprises
- 115+ countries
 - 40 language translations
 - 51 national language versions
- Cross industry



Wholesale Distribution Computer Services

Finance Retail Insurance

Consumer Package Goods Travel & Transportation

Agribusiness Automotive Construction

Manufacturing Lodging Healthcare

Education Associations Local Government

Legal Services Accounting Services

IBM i Architecture

DB2 for i & Single Level Store



Automate & optimize storage management

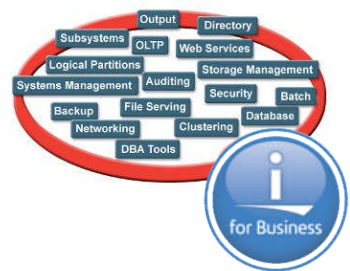
Object Based Architecture

Defined Interface			Defined Interface		
Call	TFRCTL	Display Attributes	Open	Update Record	Display Attributes
Access Authority check			Access Authority check		
↓			↓		
Program Object			File Object		

A program cannot masquerade as data and visa versa.

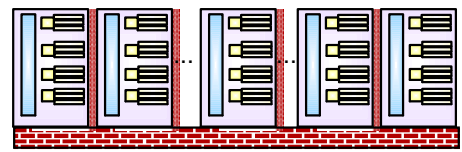
Enables integrity, security, virus-resistance

Integration



Integrates business components: DB, Web, Security

Work Management



Provides built-in application virtualization

Technology Independent Machine Interface



Ensures application compatibility across multiple technology generation.

IBM i

An **Architecture** Devoted to Business Stability, Simplicity, Security, Scalability

What we'll cover today

- 30K-foot overview of InfoSphere Guardium and IBM I
- **An integrated solution for audit and compliance**
- Monitoring strategy and use cases
- Step by step – getting started
- FAQ and conclusion



What's special about Guardium V9.0 & DB2 for i?

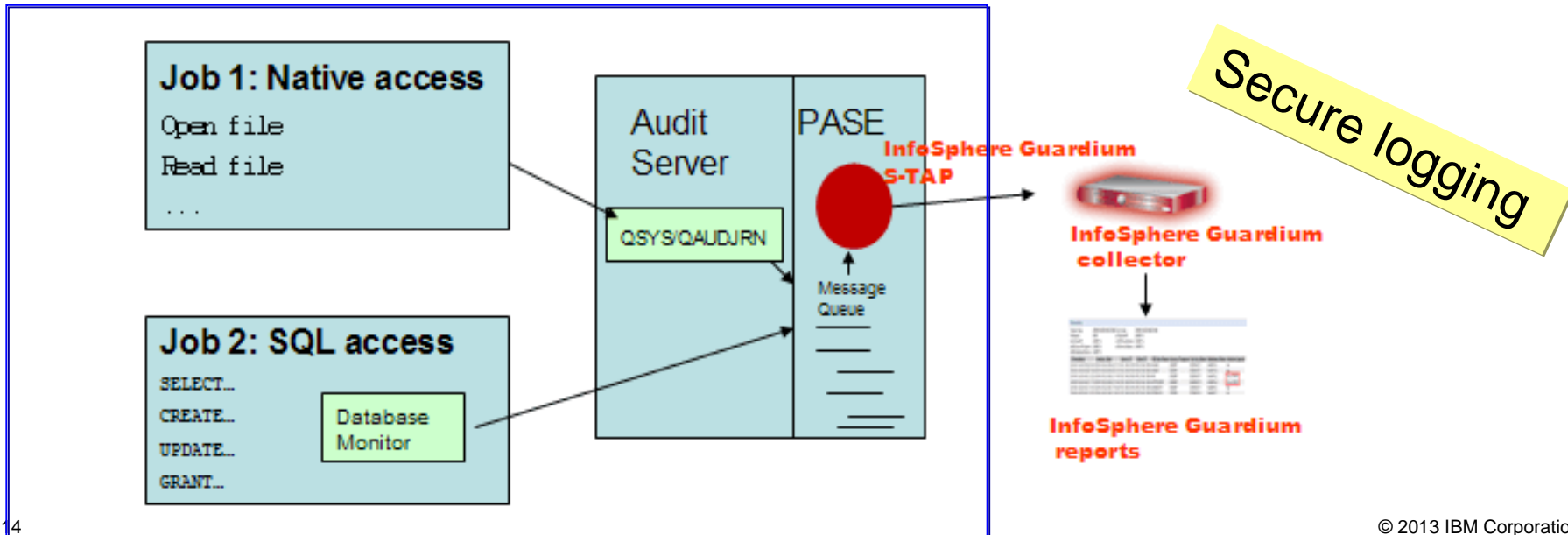
- **Comprehensive** database monitoring solution Audit Journal, inbound and host-based **SQL activity** and Data Journals
- SQL Statement Text with Bind Variables
 - ✓ Ability to reconstruct the complete SQL statement
 - ✓ Contextual detail an auditor needs
- **Real time** monitoring for database activity
 - ✓ Enables real time action and reaction
- Extensive filtering capability
- Leveraged IBM i solution in a software product that supports many DB vendors



Guardium STAP for IBM i

Both QAUDJRN and SQL information is streamed to the Guardium collector

- Global SQL Monitor using a view and instead of trigger captures SQL information and puts them on a Unix queue
- Audit server job
 - Runs in QBATCH (or your choice of subsystem)
 - Receives QAUDJRN audit entries and puts them on a Unix queue
 - Runs a Guardium UNIX executable in PASE to receive entries from the queue and send them to the collector
 - On an IPL we will restart automatically (you may have to start the subsystem)



What we'll cover today



- 30K-foot overview of InfoSphere Guardium and IBM I
- An integrated solution for audit and compliance
- **Monitoring strategy and use cases**
- Step by step – getting started
- FAQ and conclusion



Guardium & DB2 for i – Customer Requirements

Before we jump into Use Case exploration, it's important to develop the customer requirements for Activity Monitoring.

- **Whose activities do they want to watch?**
- **Which database operations are important to track?**
- **Which database objects need to be tracked?**
- **What questions need to be answered?**

In many cases, the compliance requirements will guide the answers, but take time to develop an:

Activity Monitoring Strategy

Database Monitor Filtering

Filtering option	Description
FILTER_USER	The specified user or group user profile filter, if any. Only one user name or generic user name can be specified.
FILTER_JOB	The specified job filter, if any. Only one job name or generic job name can be specified.
FILTER_TCPIP	The specified TCP/IP filter, if any. Only one TCP/IP address can be specified.
FILTER_TABLE	The specified table filter, if any. Up to ten file names or generic file names can be specified. The specified library name must be the system schema name (10 character name). The file name can be either the system table name or table name (long or short name).
FILTER_PORT	The specified port filter, if any. Only one port filter can be specified. Filtering by port is only supported in release 7.1 and above.
FILTER_CLIENT_ACCTING	The specified client accounting filter, if any. Only one client accounting filter can be specified. Filtering by client accounting is only supported in release 7.1 and above.
FILTER_CLIENT_APPLNAME	The specified client application filter, if any. Only one client application filter can be specified. Filtering by client application is only supported in release 7.1 and above.
FILTER_CLIENT_PROGRAMID	The specified client program filter, if any. Only one client program filter can be specified. Filtering by client program is only supported in release 7.1 and above.
FILTER_CLIENT_USERID	The specified client user filter, if any. Only one client user filter can be specified. Filtering by client user is only supported in release 7.1 and above.
FILTER_CLIENT_WRKSTNNAME	The specified client workstation filter, if any. Only one client workstation filter can be specified. Filtering by client workstation is only supported in release 7.1 and above.
FILTER_RDB	The specified relational database filter, if any. Up to 10 relational database filter names can be specified. Note: Case sensitive name
FILTER_SYSTEM_SQL	The specified system SQL statement filter. Specifies whether system SQL statements should be audited (Y or N) . The default is Y.
FILTER_AUDIT_ENTRY_TYPES	The specified QAUDJRN audit entry filter, if any. Specifies which audit journal entry types should be processed. The default is 'AD AF CA CO DO GD OM OR OW PG PW RA RO RZ ZC ZR'

QAUDJRN Filtering

The audit entries that we capture can be controlled by configuring which entry types should be captured. By default, the following are returned:

ZR Read object	OM Object moved or renamed
ZC Change object	PG Primary group change
CA Authority change	PW Invalid password or user ID
AD Auditing change	OW Change owner
AF Authority failure	OR Object restored
CO Create object	RA Restore authority change
DO Delete object	RO Restore owner change
GR General purpose audit record	RZ Restore primary group change
	SV System Value change

Note: CD Command string is supported, but not by default

Since the focus is primarily on database changes, we will only return entries related to objects that are database specific:

- *FILE (a table, view, index, logical file, alias, or device file)
- *SQLUDT (an SQL user-defined type)
- *SQLPKG (an SQL package)
- *PGM (a procedure, function, or program)
- *SRVPGM (a procedure, function, global variable, or service program)
- *DTAARA (an SQL sequence)

For entries that identify an object, the statement text part of the message will be constructed as follows:

XX - 30-byte-text 10-byte-library 10-byte-object-name 8-byte-object-type

For example:

ZC - Change object <library-name> <object-name> <object-type>

Quick Security Check for IBM i

Provides quick and easy check of system for major security exposures

Service Overview:

Quick Security Check performs a rapid security analysis of your IBM i system, and provides a report on key areas of security concern.

Key Features:

Automated tool checks and reports hundreds of parameters in an IBM i environment

Profile Analysis:

- Special Authorities / Inherited Privileges
- Group Profiles / Ambiguous Profiles
- Default Passwords / Password Expiration
- Inactive Accounts
- *PUBLICLY and Privately Authorized Profiles
- Initial Programs, Menus, and Attention Programs
- Command Line Access

Administration / Configuration Settings:

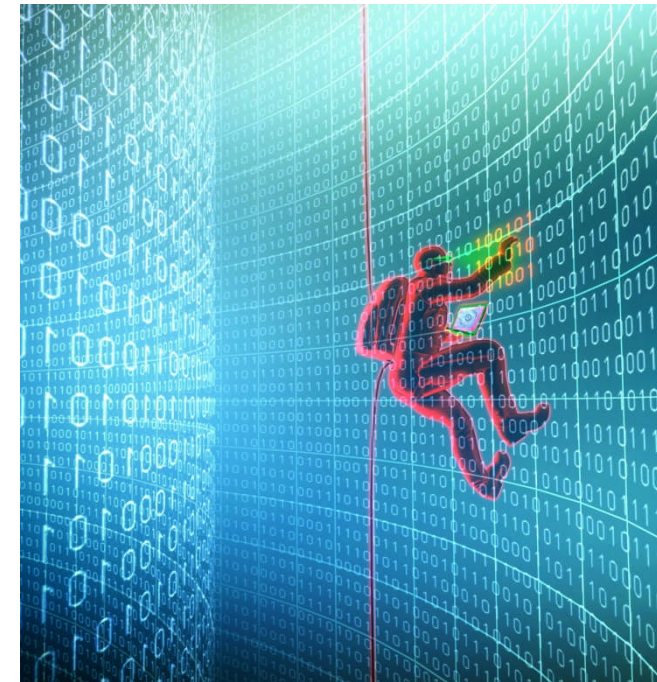
- System Values / Audit Control Settings
- Invalid Signon attempts
- Work Management Analysis
- DDM Password Requirements
- Registered Exit Points / Function Usage
- Library Analysis

Network Settings:

- Network attributes
- NetServer Configuration
- TCP/IP servers / Autostart values
- Listening ports / Network Encryption
- IP Datagram Forwarding / IP Source Routing

Service Benefits:

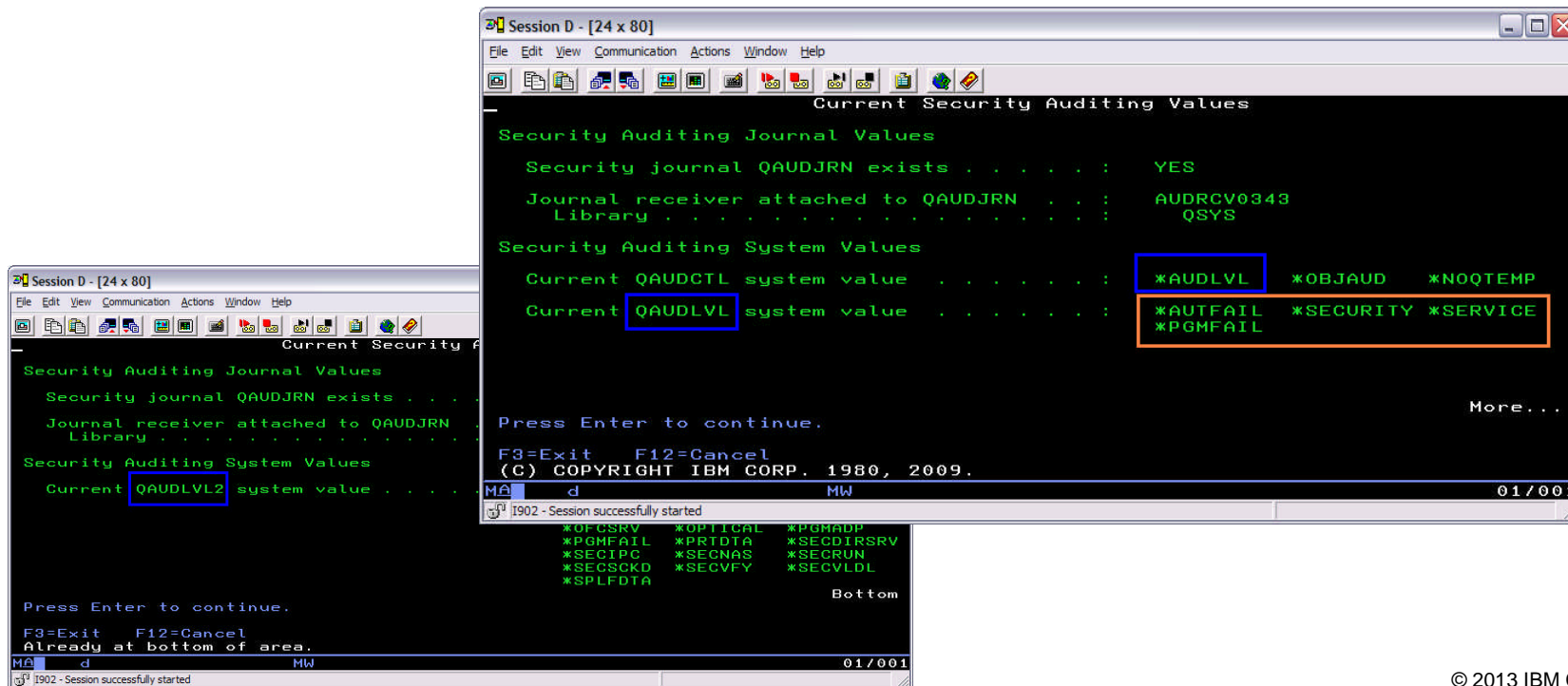
- Reduces cost and time involved in running system security checks
- Can minimize potential user errors that cause system exposures
- Offers an opportunity to review systems for security breaches and take action to address the issue
- Provides a new level of report automation and user interface that makes the tool easy-to-use, fast and accurate
- Easy enough to use that you can deploy it, and with your skills, a Business Partner's skills, or Lab Services' skills, the issues can be addressed and remediated.



Guardium and DB2 for i – Frame of reference

To set expectations of what data should be logged into the Guardium appliance, review these points:

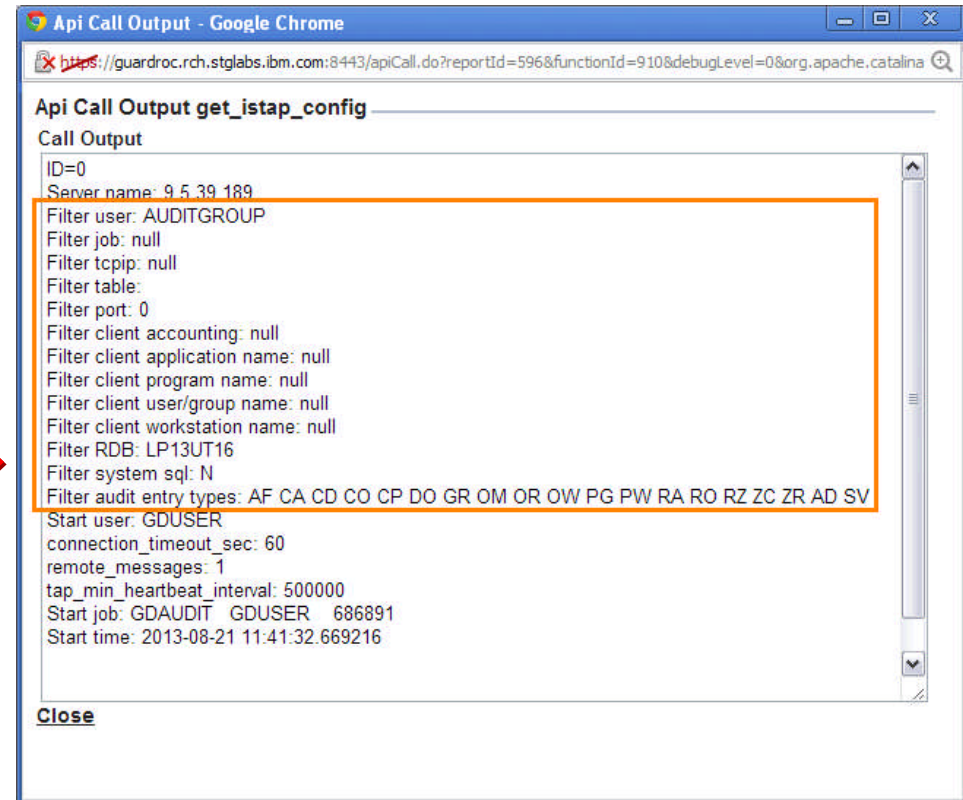
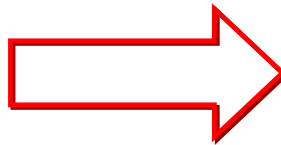
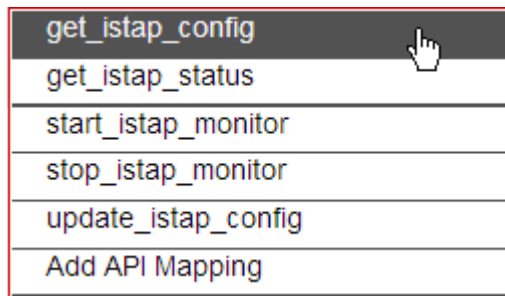
1. How is Security Auditing configured on the IBM i?
Use the **Display Security Auditing (DSPSECAUD)** command



Guardium and DB2 for i – Frame of reference

To set expectations of what data should be logged into the Guardium appliance, review these points:

2. How is the istap configured?

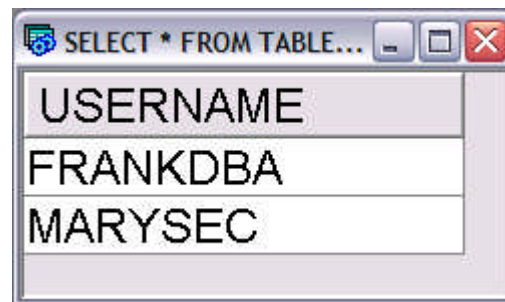


Guardium and DB2 for i – Frame of reference

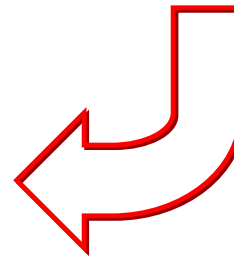
3. If Filter user is being used, is it an individual user or a group profile? If it's a group profile, who belongs to that group?

Only the users in this list will have their SQL Statements captured in the Guardium appliance.

```
SELECT * FROM TABLE(QSYS2.GROUP_USERS('AUDITGROUP')) AS A;
```

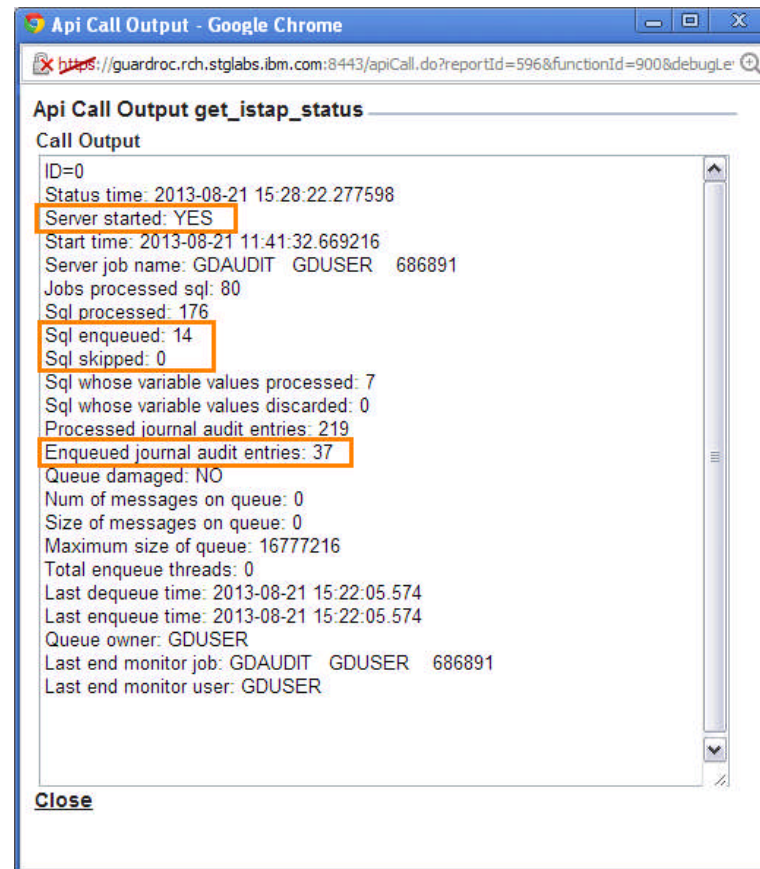
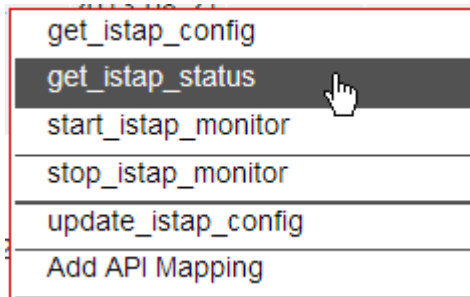


USERNAME
FRANKDBA
MARYSEC



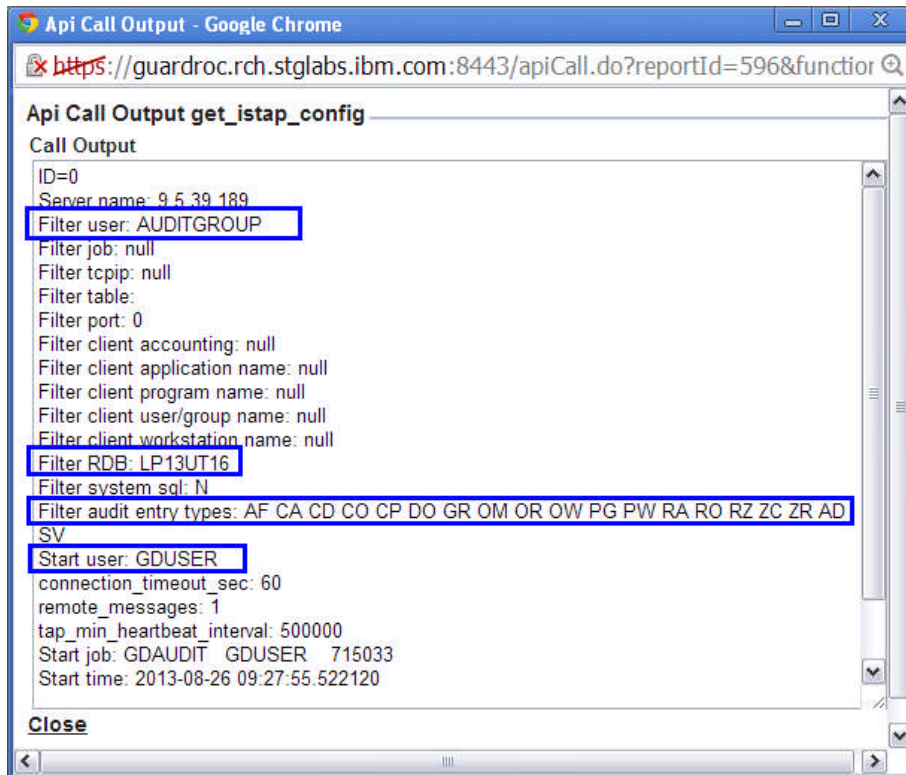
Guardium and DB2 for i – Frame of reference

4. Is the Guardium Audit Server running?



Guardium and DB2 for i – Configuration steps

Review the configuration:



IBM i configuration steps:

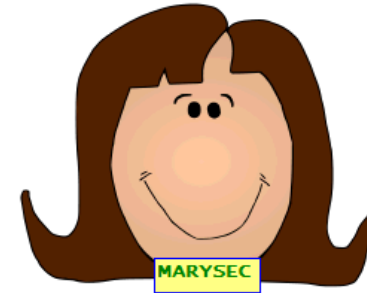
1. CRTSBSD SBSD(QGPL/GUARDSBS) POOLS((1 *BASE)) TEXT('Guardium SBS')
2. CRTJOBQ QGPL/GDJOBQ TEXT('Guardium job queue')
3. CRTUSRPRF **GDUSER** PASSWORD(*NONE) PWDEXP(*NO) STATUS(*ENABLED) SPCAUT(*ALLOBJ *JOBCTL)
4. CRTJOBQ QGPL/GDAUDIT JOBQ(GDJOBQ) JOBPTY(2) USER(GDUSER) JOBMSGQFL(*WRAP)
5. CHGUSRPRF GDUSER JOBQ(QGPL/GDAUDIT)
6. ADDJOBQE SBSD(QGPL/GUARDSBS) JOBQ(QGPL/GDJOBQ) MAXACT(10) SEQNBR(40)
7. CRTCLS CLS(GDCLS) **RUNPTY(1)** **TIMESLICE(10000)**
8. ADDRTE SBSD(QGPL/GUARDSBS) SEQNBR(800) CMPVAL(GUARDIUM) PGM(QSYS/QCMD) CLS(GDCLS)
9. STRSBS SBSD(QGPL/GUARDSBS)

Guardium and DB2 for i - Use case exploration

Meet the users:

1) **MARYSEC** – A Security Officer with authority to do anything

```
CRTUSRPRF USRPRF(MARYSEC) PASSWORD(xxxxxxxx)
USRCLS(*SECOFR)
TEXT('Security Officer')
```



1) **FRANKDBA** – A Database Administrator with authority to do everything but change security settings

```
CRTUSRPRF USRPRF(FRANKDBA) PASSWORD(xxxxxxxx)
USRCLS(*USER)
TEXT('Database Administrator')
SPCAUT(*ALLOBJ *JOBCTL *SAVSYS *SPLCTL)
```



1) **JOEUSER** – An end user with no special authority

```
CRTUSRPRF USRPRF(JOEUSER) PASSWORD(xxxxxxxx)
USRCLS(*USER)
TEXT('User with no special authorities')
```



Guardium and DB2 for i – Filtering on a group of users

Use cases – Initial setup:

1. CRTUSRPRF USRPRF(**AUDITGROUP**) PASSWORD(*NONE)
2. CRTUSRPRF USRPRF(**JOEUSER**) PASSWORD() TEXT('User with no special authorities')
3. CRTUSRPRF USRPRF(**MARYSEC**) PASSWORD() **USRCLS(*SECOFR)**
TEXT('Security Officer')
4. CRTUSRPRF USRPRF(**FRANKDBA**) PASSWORD() **USRCLS(*USER)**
TEXT('Database Administrator') **SPCAUT(*ALLOBJ *JOBCTL *SAVSYS *SPLCTL)**

Later, we'll adjust:

5. CHGUSRPRF USRPRF(**FRANKDBA**) GRPPRF(DBATEAM) SUPGRPPRF(**AUDITGROUP**)
6. CHGUSRPRF USRPRF(**MARYSEC**) GRPPRF(**AUDITGROUP**)

When in doubt, we can review the members of the group:

7. > STRSQL
> SELECT * FROM TABLE(QSYS2.GROUP_USERS('AUDITGROUP')) AS A
FRANKDBA
MARYUSER

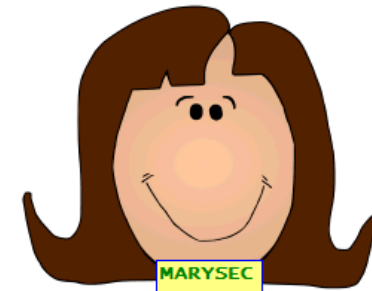
Guardium and DB2 for i - Use case exploration

What should we track?

Let's show some examples of what's possible with Guardium.

MARYSEC – As the Security Officer is supposed to limit her activity to managing user access and authorities. Mary should not be looking at data, changing data.

Let's start by adding MARYSEC to the Guardium
USER_FILTER(AUDIT_GROUP) Group Profile

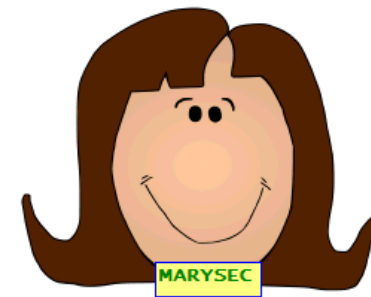


```
CHGUSRPRF USRPRF(MARYSEC) GRPPRF(AUDITGROUP)
```

Question: Do we have adequate audit coverage?

Guardium and DB2 for i - MARYSEC

Because the system includes *SECURITY as an Audit Level choice and S-TAP is configured to monitor ‘CP’ audit entries, we can see that MARYSEC’s user profile was changed.



```

Session D - [24 x 80]
File Edit View Communication Actions Window Help
Current Security Auditing Values

Security Auditing Journal Values
Security journal QAUDJRN exists . . . . . : YES
Journal receiver attached to QAUDJRN . . . : AUDRCV0343
Library . . . . . : QSYS

Security Auditing System Values
Current QAUDCTL system value . . . . . : *AUDLVL *OBJAUD *NOQTEMP
Current QAUDLVL system value . . . . . : *AUTFAIL *SECURITY *SERVICE
*PGMFAIL

Press Enter to continue.
F3=Exit F12=Cancel
(C) COPYRIGHT IBM CORP. 1980, 2009.
MA d Mw 01/001
1902 - Session successfully started
    
```

DB2 i SQL activity

Start Date: 2013-08-18 13:51:43 End Date: 2013-08-21 16:51:43
Aliases: OFF

Full SQL ID	Timestamp	DB Protocol	DB2 i/z Database	DB2 i/z Program	DB2 i Current User	Network Protocol	Succeeded	Process ID	Source Program	Full Sql
1023344	2013-08-21 10:35:30.0	DB2I	LP13UT16QSYS/QCMD	SCOTT	QAUDJRN		1	686842	SCOTT/QPADEV0004	CP - User Profile change QSYS MARYUSER *USRPRF

Guardium and DB2 for i - MARYSEC

We are configured to see all of MARYSEC’s SQL statements and that’s all.

We could easily extend the monitoring for MARYSEC to include command execution and much more.

```
> CHGUSRAUD USRPRF(MARYSEC)
  OBJAUD(*ALL)
  AUDLVL(*CREATE *DELETE *OBJMGT *SECURITY
        *SERVICE *SYSMGT *SAVRST *AUTFAIL *CMD)
```



DB2 i SQL activity										
Start Date: 2013-08-18 14:14:46 End Date: 2013-08-21 17:14:46										
Aliases: OFF										
Full SQL ID	Timestamp	DB Protocol	DB2 i/z Database	DB2 i/z Program	DB2 i Current User	Network Protocol	Succeeded	Process ID	Source Program	Full Sql
1023350	2013-08-21 10:57:13.0	DB2 I	LP13UT16	QSYS/QCMD	MARYUSERQINTER		1	686866	MARYUSER/QPADEV000	AD - Auditing change MARYSEC *USRPRF

Guardium and DB2 for i - MARYSEC

Now let's sit back and watch the data roll in...

- CRTUSRPRF NEWUSER
- DLTUSRPRF NEWUSER
- CHGSYSVAL SYSVAL(QQRYDEGREE) VALUE(*OPTIMIZE)
- STRSQL
 - > select * from store123.sales where sales_person = 'Jones'

MARYSEC's actions



And be in a position to analyze the results...

- 1) Was the process for adding a new user followed?
- 2) Why is MARYSEC changing an important DB2 for i system value?
- 3) Why is MARYSEC looking at the SALES table?

DB2 i SQL activity

Start Date: 2013-08-18 14:56:03 End Date: 2013-08-21 17:56:03
Aliases: OFF

Full SQL ID	Timestamp	DB Protocol	DB2 i/z Database	DB2 i/z Program	DB2 i Current User	Network Protocol	Succeeded	Process ID	Source Program	Full Sql	Bind Variables Values
1023355	2013-08-21 10:57:13.0	DB2 I	LP13UT16QSQL/QSQIMAIN		MARYUSERQINTER		1	686866	MARYUSER/QPADEV000L	select * from store123.sales where sales_person = ?	'Jones'
1023354	2013-08-21 10:57:13.0	DB2 I	LP13UT16QSYS/QCMD		MARYUSERQINTER		1	686866	MARYUSER/QPADEV000L	SV - System value change QQRYDEGREE	NEW VALUE: *OPTIMIZE OLD VALUE: *NONE
1023353	2013-08-21 10:57:13.0	DB2 I	LP13UT16QSYS/QCMD		MARYUSERQINTER		1	686866	MARYUSER/QPADEV000L	DO - Delete object NEWUSER *USRPRF	QSYS
1023352	2013-08-21 10:57:13.0	DB2 I	LP13UT16QSYS/QCMD		MARYUSERQINTER		1	686866	MARYUSER/QPADEV000L	CP - User Profile change QSYS NEWUSER *USRPRF	
1023351	2013-08-21 10:57:13.0	DB2 I	LP13UT16QSYS/QCMD		MARYUSERQINTER		1	686866	MARYUSER/QPADEV000L	CA - Authority change QSYS NEWUSER *USRPRF	

Guardium and DB2 for i - Use case exploration

What should we track?

FRANKDBA – As the database administrator, FRANKDBA needs to manage the database. He needs to all authorities to data, including create/drop/save/restore/reorganize/and more.

This capability implies a tremendous amount of trust. His actions need to be monitored to identify accidents/mistakes or intentional bad behavior.

Definitely want to add him to the auditing group profile.

```
CHGUSRPRF USRPRF(FRANKDBA)  
GRPPRF(AUDITGROUP)
```

Question: Do we have adequate audit coverage?



Guardium and DB2 for i - Use case exploration

- **Do we care to monitor Native Database access or IBM i Command manipulation of critical database objects?**

Restoring a library

```
RSTLIB SAVLIB(STORE123) DEV(*SAVF)  
SAVF(QGPL/STORE123)
```

Deleting a file (aka table)

```
DLTF FILE(STORE123/dept )
```

Renaming a table

```
RNMOBJ OBJ(STORE123/SALES) OBJTYPE(*FILE) NEWOBJ(SALESSAVED)
```

Moving a table

```
MOV OBJ(STORE123/EMP) OBJTYPE(*FILE) TOLIB(FRANKLIB)
```



- **The Audit Control & Audit Level System Values determines which of these operations will appear in the Data Activity Monitor**

Guardium and DB2 for i - Use case exploration

- Lets add *SAVRST and *OBJMGT to QAUDLVL.
 → WRKSYSVAL SYSVAL(QAUD*)
 By enabling more Audit Journal options → The Guardium Activity Monitor will have the chance to see more data

```

Session E - [24 x 80]
File Edit View Communication Actions Window Help

Change System Value
-----
Auditing options - Help

-
current auditing value. You cannot change the system value to not
available (*NOTAVL).

*OBJMGT
Generic object tasks are audited. The following are some examples:
o Moves of objects
o Renames of objects

*OFCSRV
OfficeVision are audited. The following are some examples:
o Changes to the system distribution directory
o Tasks involving electronic mail

*OPTICAL
All optical functions are audited. The following are some examples:
More...
F2=Extended help F3=Exit help F10=Move to top F12=Cancel
F13=Information Assistant F14=Print help

-----

*PGMFAIL
Program failures are audited. The following are some examples:
o Blocked instruction
o Validation value failure
o Domain violation

*PRDTA
Printing functions are audited. The following are some examples:
o Printing a spooled file
o Printing with parameter SPOOL(*NO)

*SAVRST
Save and restore information is audited. The following are some
examples:
o When programs that adopt their owner's user profile are restored
more...
F2=Extended help F3=Exit help F10=Move to top F12=Cancel
F13=Information Assistant F14=Print help
    
```

```

Session E - [24 x 80]
File Edit View Communication Actions Window Help

Change System Value
-----
Auditing options - Help

-
current auditing value. You cannot change the system value to not
available (*NOTAVL).

*OBJMGT
Generic object tasks are audited. The following are some examples:
o Moves of objects
o Renames of objects

*OFCSRV
OfficeVision are audited. The following are some examples:
o Changes to the system distribution directory
o Tasks involving electronic mail

*OPTICAL
All optical functions are audited. The following are some examples:
More...
F2=Extended help F3=Exit help F10=Move to top F12=Cancel
F13=Information Assistant F14=Print help

-----

MA e MW 04/005
1902 - Session successfully started
    
```



Guardium and DB2 for i - Use case exploration



- After these changes, we see some audit entries appear.
- The information is accurate, but we can do better.
- We didn't see an entry for the Delete File (DLTF) command and we didn't see an explanation of what was driving the changes other than QSYS/QCMD was being used.

DB2 I SQL activity											
Start Date: 2013-08-23 10:10:24 End Date: 2013-08-26 13:10:24											
Aliases: OFF											
Full SQL ID	Timestamp	DB Protocol	DB2 i/z Database	DB2 i/z Program	DB2 i Current User	Network Protocol	Succeeded	Process ID	Source Program	Full Sql	Bind Variables Values
1039829	2013-08-26 09:39:56.0	DB2 I	LP13UT16	QSYS/QCMD	FRANKDBA	QAUDJRN	1	715262	FRANKDBA/QPADEV0004	OM - Object moved or renamed STORE123 EMP *FILE	NEW LIBRARY: FRANKLIB
1039828	2013-08-26 09:39:56.0	DB2 I	LP13UT16	QSYS/QCMD	FRANKDBA	QAUDJRN	1	715262	FRANKDBA/QPADEV0004	OM - Object moved or renamed STORE123 SALES *FILE	NEW NAME: SALESSAVED
1039827	2013-08-26 09:39:56.0	DB2 I	LP13UT16	QSYS/QCMD	FRANKDBA	QAUDJRN	1	715262	FRANKDBA/QPADEV0004	OR - Object restored STORE123 SYSVIEWS *FILE	
1039826	2013-08-26 09:39:56.0	DB2 I	LP13UT16	QSYS/QCMD	FRANKDBA	QAUDJRN	1	715262	FRANKDBA/QPADEV0004	OR - Object restored STORE123 SYSVIEWDEP*FILE	
	2013-08-26									OR - Object restored	

Guardium and DB2 for i - Use case exploration

- **Enable Object auditing for all existing objects within the STORE123 library**
`CHGOBJAUD OBJ(STORE123/*ALL) OBJTYPE(*ALL) OBJAUD(*USRPRF)`

OBJAUD(*USRPRF): The user profile of the user accessing this object is used to determine if an audit record is created. The OBJAUD keyword on the CHGUSRAUD command controls whether a specific user should be audited.

Also, change FRANKDBA to have command and object level auditing enabled

- `CHGUSRAUD USRPRF(FRANKDBA)`
`OBJAUD(*CHANGE) AUDLVL(*CMD)`



Guardium and DB2 for i - Use case exploration

After these changes, we see the **delete operation** and **the commands** used to drive the auditable entries



DB2 i SQL activity											
Start Date: 2013-08-23 10:21:03 End Date: 2013-08-26 13:21:03											
Aliases: OFF											
Full SQL ID	Timestamp	DB Protocol	DB2 i/z Database	DB2 i/z Program	DB2 i Current User	Network Protocol	Succeeded	Process ID	Source Program	Full Sql	Bind Variables Values
1039975	2013-08-26 09:39:56.0	DB2 I	LP13UT16	QSYS/QCMD	FRANKDBA	QAUDJRN1		715264	FRANKDBA/QPADEV0004	OM - Object moved or renamed STORE123 EMP *FILE	NEW LIBRARY: FRANKLIB
1039974	2013-08-26 09:39:56.0	DB2 I	LP13UT16	QSYS/QCMD	FRANKDBA	QAUDJRN1		715264	FRANKDBA/QPADEV0004	CD - Command string QSYS MOV OBJ *CMD	MOV OBJ OBJ(STORE123/EMP) OBJTYPE(*FILE) TOLIB(FRANKLIB)
1039973	2013-08-26 09:39:56.0	DB2 I	LP13UT16	QSYS/QCMD	FRANKDBA	QAUDJRN1		715264	FRANKDBA/QPADEV0004	OM - Object moved or renamed STORE123 SALES *FILE	NEW NAME: SALESSAVED
1039972	2013-08-26 09:39:56.0	DB2 I	LP13UT16	QSYS/QCMD	FRANKDBA	QAUDJRN1		715264	FRANKDBA/QPADEV0004	CD - Command string QSYS RNM OBJ *CMD	RNM OBJ OBJ(STORE123/SALES) OBJTYPE(*FILE) NEW OBJ(SALESSAVED)
1039971	2013-08-26 09:39:56.0	DB2 I	LP13UT16	QSYS/QCMD	FRANKDBA	QAUDJRN1		715264	FRANKDBA/QPADEV0004	DO - Delete object STORE123 DEPT *FILE	
1039970	2013-08-26 09:39:56.0	DB2 I	LP13UT16	QSYS/QCMD	FRANKDBA	QAUDJRN1		715264	FRANKDBA/QPADEV0004	CD - Command string QSYS DLTF *CMD	DLTF FILE(STORE123/DEPT)

Guardium and DB2 for i - Use case exploration

Digging deeper...

The Process ID combined with the Source Program is the Qualified Job Name on the IBM i.



Full SQL ID	Timestamp	DB Protocol	DB2 i/z Database	DB2 i/z Program	DB2 i Current User	Network Protocol	Succeeded	Process ID	Source Program	Full Sql	Bind Variables Values
1039975	2013-08-26 09:39:56.0	DB2 I	LP13UT16QSYS/QCMD	FRANKDBAQAUDJRN1				715264	FRANKDBA/QPADEV0004	DM - Object moved or renamed STORE123 EMP FILE	NEW LIBRARY: FRANKLIB

DSPJOB JOB(715264/FRANKDBA/QPADEV0004) and choose option 10

```

Session E - [24 x 80]
File Edit View Communication Actions Window Help
Display All Messages
Job . . . : QPADEV0004      User . . . : FRANKDBA      System: LP13UT16
Number . . . : 715264
> DLTFF FILE(STORE123/dept )
Object DEPT in STORE123 type *FILE deleted.
> RNM OBJ(STORE123/SALES) OBJTYPE(*FILE) NEWOBJ(SALESSAVED)
Object SALES in STORE123 type *FILE renamed SALESSAVED.
>> MOV OBJ(STORE123/EMP) OBJTYPE(*FILE) TOLIB(FRANKLIB)
Object EMP in STORE123 type *FILE moved to library FRANKLIB.
    
```

Guardium and DB2 for i - Use case exploration

What should we track?

JOEUSER – This user has no special authorities. They have access to the machine to be able to use a subset of well defined applications. If the object authorization strategy is sound, this user can do no accidental or intentional harm.

Should be no need to add this user to the auditing group profile.

Unless this user shows up in the Guardium Exception Report, we will make no additional monitoring configuration.



Question: Do we have adequate audit coverage?

Guardium and DB2 for i - Use case exploration

The Activity and Exception reports surface similar detail, driven by Audit Journal Authorization Failures (AF) and Password Failures (PW)

Since this user is not part of AUDITGROUP and isn't setup for Command auditing, we only see the failed attempts to signon and authorization failures.



To study JOEUSER more closely, reconsider the auditing and filtering choices.

DB2 I SQL activity

Start Date: 2013-08-23 18:39:03 End Date: 2013-08-26 21:39:03
Aliases: OFF

Full SQL ID	Timestamp	DB Protocol	DB2 i/z Database	DB2 i/z Program	DB2 i Current User	Network Protocol	Succeeded	Process ID	Source Program	Full Sql	Bind Variables Values	Records Affected	DB2 Client Info	Client IP
1040096	2013-08-26 18:32:25.0	DB2 I	LP13UT16	QSYS/QCMD	JOEUSER	QAUDJRN	0	715472	JOEUSER/QPADEV000L	AF - Authority failure QSYS STORE123 *LIB		-1	0	9.10.110.143
1040095	2013-08-26 18:32:25.0	DB2 I	LP13UT16	QSYS/QCMD	JOEUSER	QAUDJRN	0	715472	JOEUSER/QPADEV000L	AF - Authority failure QSYS STORE123 *LIB		-1	0	9.10.110.143

Detailed Exception Report

Start Date: 2013-08-26 05:38:01 End Date: 2013-08-27 07:38:01
Aliases: OFF

Exception Timestamp	DB Protocol	DB2 i/z Database	DB2 i Current User	DB2 i/z Program	Network Protocol	Exception Type	Process ID	Source Program	Error Code	Exception Description	Database Error Text	SQL string that caused the Exception	Client IP	Exception Description
2013-08-26 18:39:12.0	DB2 I	LP13UT16	JOEUSER	QSYS/QLESPI	QAUDJRN	LOGIN_FAILED	714521	QSYS/QINTER	N/A	PW - Invalid password or user ID	N/A		9.10.110.143	Login Failed
2013-08-26 18:38:36.0	DB2 I	LP13UT16	JOEUSER	QSYS/QCMD	QAUDJRN	SQL_ERROR	715472	JOEUSER/QPADEV000L	-551	42501:-551	The authorization ID does not have the privilege to perform the specified operation on the identified object.	AF - Authority failure QSYS STORE123 *LIB	9.10.110.143	Database Server returned an error

Guardium & DB2 for i – Frequently Asked Monitoring Questions

1. Can this product monitor ftp traffic?

Answer: Yes.

- Topic explained in the “Guardium Activity Monitor & DB2 for i Serviceability Guide”

<http://bit.ly/GuardiumDB2foriServiceabilityDocument>

2. What about Native database access from RPG?

Answer: Yes

- Native access appears through the audit journal as ZR (Read Object) and ZC (Change Object)

3. What about Data Journals, are they used?

Answer: Up to you.

- Guardium maintains the ability to have data journals included through a scheduled upload. (not real time)

4. I want to monitor all activity with no filtering, is that supported?

Answer: Yes

- Recent enhancements are explained on the next slide

Guardium & DB2 for i – Entire system auditing



1. Install the recommended IBM i service: <http://bit.ly/GuardiumOni>
2. Install the updated Audit Server PASE program (to be released soon)
3. Tune the Audit Server to have RUNPTY(1) and TIMESLICE(1000)
“Tuning the performance of the audit server” section of the white paper:
http://www.ibm.com/developerworks/ibmi/library/i-infosphere_guardium_db2/index.html
4. Stop and Restart the Audit Server
5. Regularly review the get_istap_status status and watch the “**Sql Skipped**” value.
6. SQL Skipped > 0 indicates that the Audit Server cannot keep up with the amount of monitored activity. On a very busy machine with no filtering, this could be encountered.
7. To direct the Audit Server to avoid skipping, the following SQL statement needs to be executed on the IBM i:

```
UPDATE QSYS2/SYSAUDIT SET PREVENT_SKIPPED_ENTRIES = 'Y'
```

Note: By choosing this option, you are directing the audit server to potentially impact the performance of workloads. The size of Sql Skipped will provide insight into the anticipated workload performance degradation. This is a processor bound decision that can be managed by enabling more cores (CPUs) on the machine.

What we'll cover today



- 30K-foot overview of InfoSphere Guardium and IBM I
- An integrated solution for audit and compliance
- Monitoring strategy and use cases
- **Step by step – getting started**
- FAQ and conclusion



DB2 i Guardium Implementation

- Getting Started (install & config)
- Policies (Alerting)
- Custom reporting for DB2 i
- Enhancing DB2 i Reports

IBM PASE for i

IBM Portable Application Solutions Environment for i (PASE for I) allows you to port IBM AIX applications to the IBM i platform with minimal effort.

Provides an integrated runtime environment that allows you to run selected applications without the complexity of managing operating systems, such as AIX or Linux

Provides industry-standard and defacto-standard shells and utilities that provide you with a powerful scripting environment

Install PASE

- 1. On an IBM i command line, enter GO LICPGM**
- 2. Select 11 (Install licensed program)**
- 3. Select Option 33 (5770-SS1 - Portable Application Solutions Environment)**
- 4. Optional: Install additional locales**

Install the DB2 i S-TAP

1. In the PASE shell environment on IBM i server, create a temporary directory to put the S-TAP installation script (such as /tmp). You can use a 5250 emulator software to connect to system i remotely and enter the PASE shell by entering “**call qp2term**”.
2. FTP the following S-TAP installation shell script to that temporary directory: **guard-itap-9.0.0_rnnnnn-aix-5.3-aix-powerpc.sh**
3. In the same directory, run the following command:

guard-itap-9.0.0_rnnnnn-aix-5.3-aix-powerpc.sh guardium_host_IP where guardium_host_IP

Where **guardium_host_IP** is the IP address of the InfoSphere Guardium collector. The installation program will install under **/usr/local/guardium**.

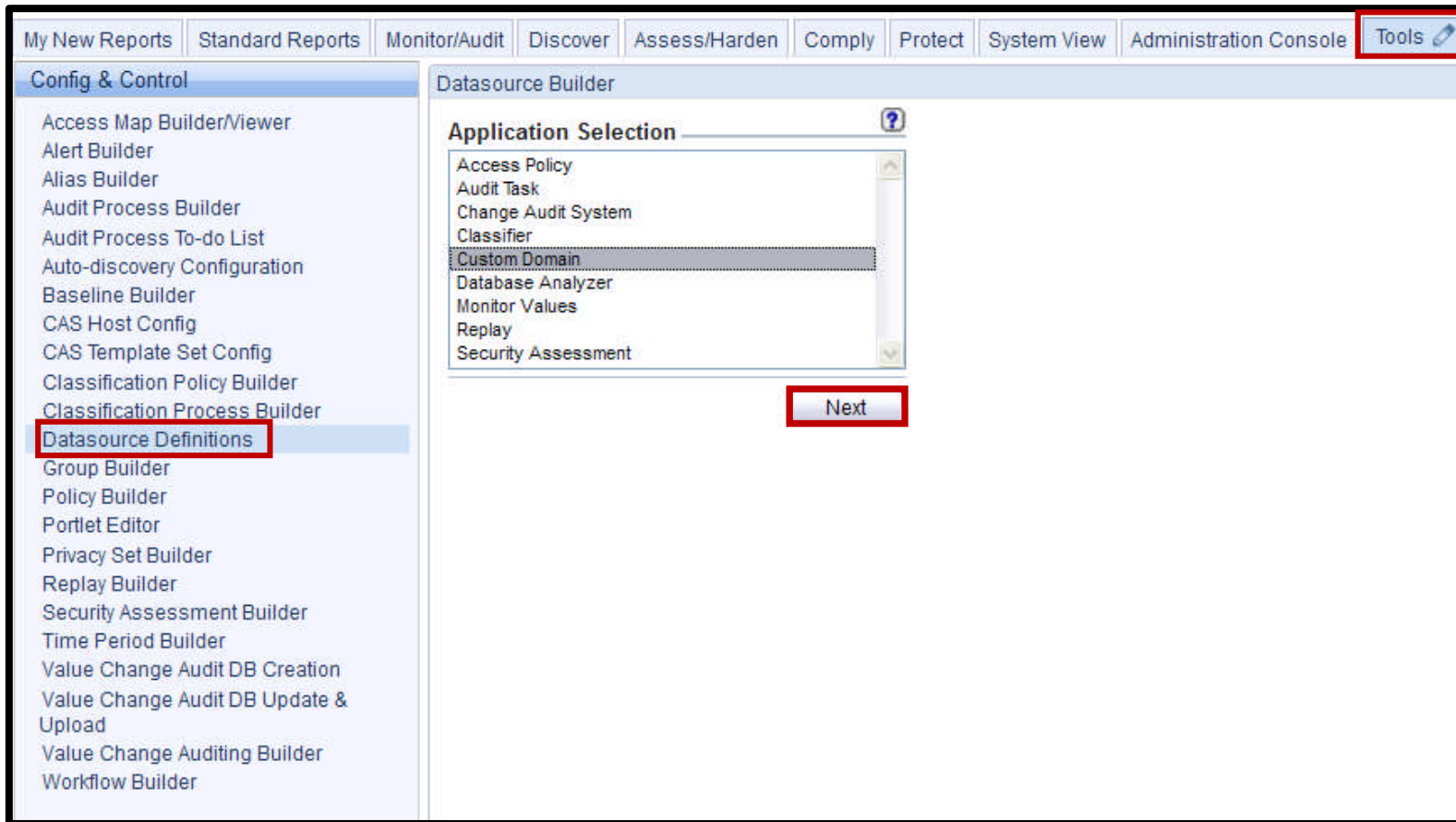
Configure the DB2 i S-TAP

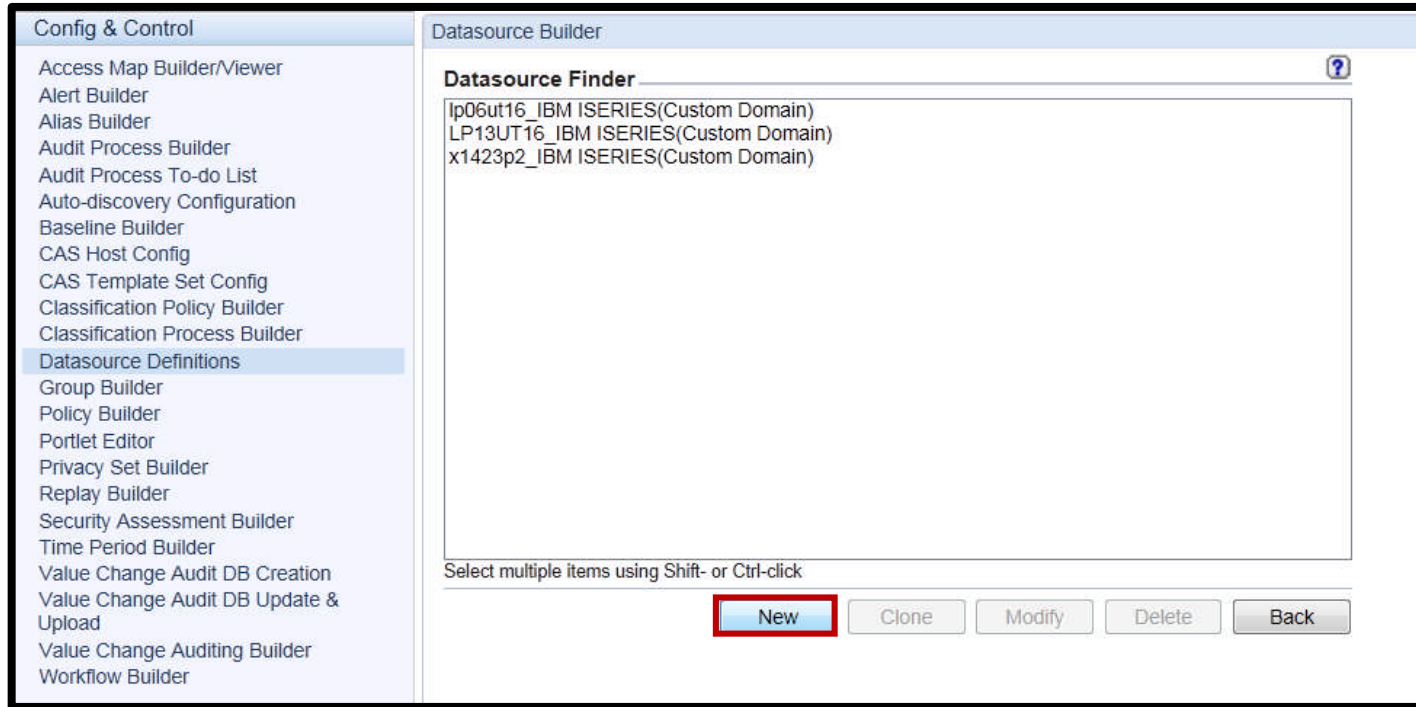
To configure and start audit processing on DB2 for i, you will be using the Guardium user Interface to **update the configuration settings** in the configuration file on IBM i and to start the **auditing process**.

The following 3 steps are to be executed:

- 1) Define DB2 for i as a recognized data source to Guardium (and test connection).
- 2) Populate Guardium collector with information from the configuration file on IBM i (that was automatically created when DB2 for i S-TAP was installed) using Custom Table Builder
- 3) Create DB2 for i configuration report. From this report interface you can invoke the APIs that start and stop the monitoring process, get status information, and update configuration

1 - Create datasource for DB2 for i





Config & Control

- Access Map Builder/Viewer
- Alert Builder
- Alias Builder
- Audit Process Builder
- Audit Process To-do List
- Auto-discovery Configuration
- Baseline Builder
- CAS Host Config
- CAS Template Set Config
- Classification Policy Builder
- Classification Process Builder
- Datasource Definitions**
- Group Builder
- Policy Builder
- Portlet Editor
- Privacy Set Builder
- Replay Builder
- Security Assessment Builder
- Time Period Builder
- Value Change Audit DB Creation
- Value Change Audit DB Update & Upload
- Value Change Auditing Builder
- Workflow Builder

Datasource Builder

Datasource Finder ?

- ip06ut16_IBM ISERIES(Custom Domain)
- LP13UT16_IBM ISERIES(Custom Domain)
- x1423p2_IBM ISERIES(Custom Domain)

Select multiple items using Shift- or Ctrl-click

New Clone Modify Delete Back

Datasource Builder

Datasource Definition

Name: _____

Database Type: _____

Severity classification: NONE

Description: _____

Share Datasource:

Authentication

Save Password:

Login Name: _____

Password: _____

Location

Host Name/IP: _____

Port: _____

Service Name: _____

Informix Server: _____

Database: _____

Connection Property: _____

Custom Url: _____

Datasource Builder

Datasource Definition

Name: x1423p2

Database Type: DB2 for i

Severity classification: NONE

Description: _____

Share Datasource:

Authentication

Save Password:

Login Name: LARKINB

Password: ●●●●●●

Location

Host Name/IP: x1423p2.rch.stglabs.ibm.com

Port: 446

Service Name: X1423P2

Informix Server: _____

Schema: _____

Connection Property: _____

Custom Url: _____

CAS

Database Instance Account: _____

Database Instance Directory: _____

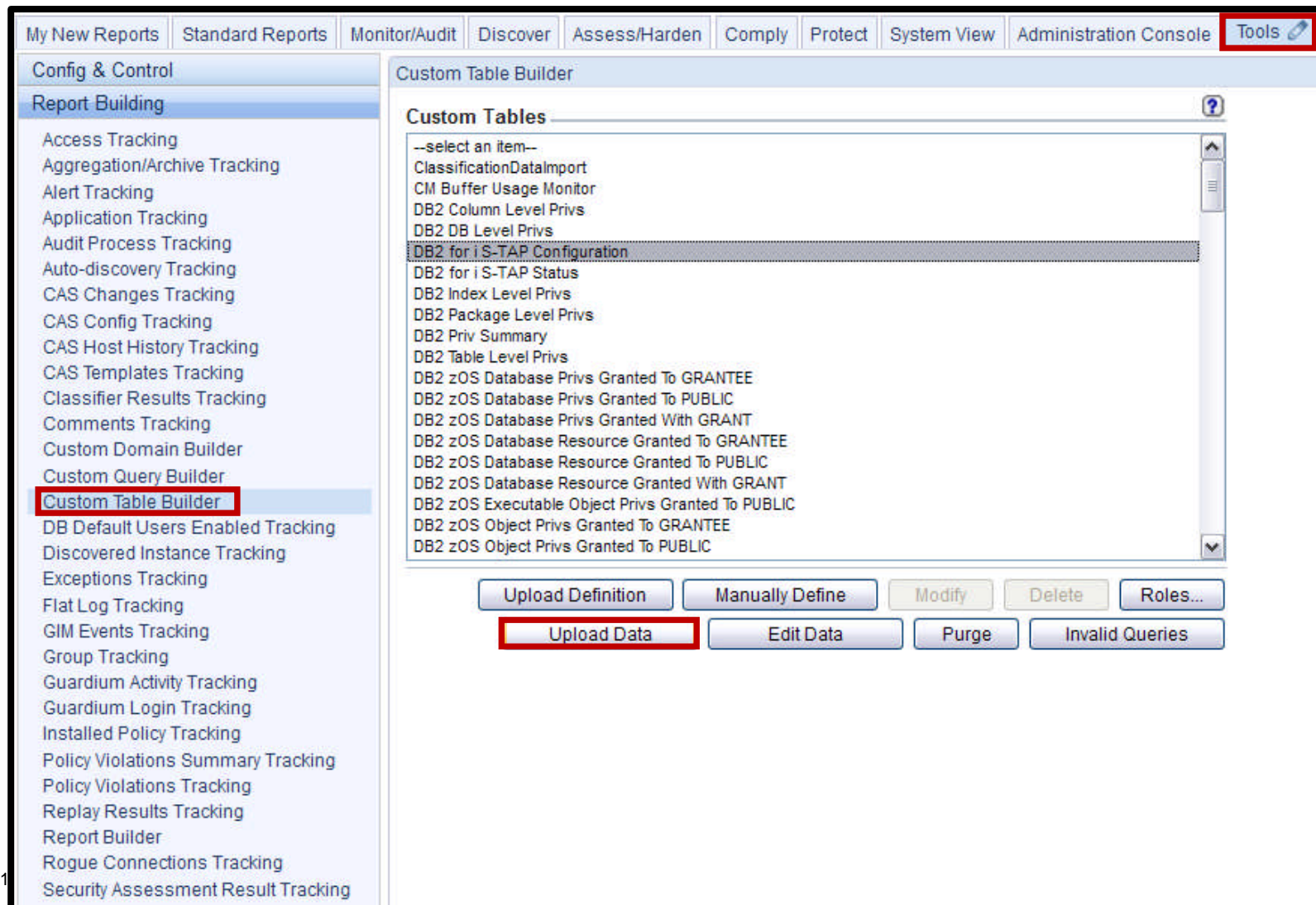
Roles

No roles have been assigned to this datasource

- DB2
- DB2 for i ←
- DB2 z/OS
- Informix
- MS SQL SERVER (DataDirect)
- MySQL
- Netezza
- Oracle (DataDirect)
- PostgreSQL
- Sybase
- Sybase IQ
- TERADATA
- TEXT
- TEXT:FTP
- TEXT:HTTP
- TEXT:HTTPS
- TEXT:SAMBA

This datasource can be successfully connected

2 - Upload the DB2 for i configuration settings to Guardium collector using custom table builder



Config & Control

Report Building

- Access Tracking
- Aggregation/Archive Tracking
- Alert Tracking
- Application Tracking
- Audit Process Tracking
- Auto-discovery Tracking
- CAS Changes Tracking
- CAS Config Tracking
- CAS Host History Tracking
- CAS Templates Tracking
- Classifier Results Tracking
- Comments Tracking
- Custom Domain Builder
- Custom Query Builder
- Custom Table Builder**
- DB Default Users Enabled Tracking
- Discovered Instance Tracking
- Exceptions Tracking
- Flat Log Tracking
- GIM Events Tracking
- Group Tracking
- Guardium Activity Tracking
- Guardium Login Tracking
- Installed Policy Tracking
- Policy Violations Summary Tracking
- Policy Violations Tracking
- Replay Results Tracking
- Report Builder
- Rogue Connections Tracking
- Security Assessment Result Tracking

Custom Table Builder ?

Import Data ?

Entity desc DB2 for i S-TAP Configuration
Table name ITAP_CONFIG

Configuration

SQL statement

Id column name

Id column type

DML command after upload

Overwrite per upload per datasource

Use default schedule

Default Purge

Datasources

Name	Type	Host	UserName
<i>No datasource has been added to this item</i>			

[Add Datasource...](#)

Scheduling

Upload is currently not scheduled for execution.

Datasource Finder

- Ip06ut16 IBM ISERIES(Custom Domain)
- LP13UT16 IBM ISERIES(Custom Domain)
- x1423p2 IBM ISERIES(Custom Domain)**

Select multiple items using Shift- or Ctrl-click

Custom Table Builder

Upload Data

Entity desc: DB2 for i S-TAP Configuration
Table name: ITAP_CONFIG

Configuration

SQL statement:

Id column name:

Id column type:

DML command after upload:

Overwrite per upload per datasource

Use default schedule

Default Purge

Datasources

	Name	Type	Host	UserName
<input checked="" type="checkbox"/>	x1423p2 IBM ISERIES(Custom Domain)	IBM ISERIES	x1423p2.rch.stglabs.ibm.com	LARKINB

Scheduling

Upload is currently not scheduled for execution.


Operation ended successfully.

svli5k:1 inserts.

3 – Create report to Invoke an api:

The screenshot shows the IBM InfoSphere Guardium interface. At the top, there is a navigation bar with tabs: System View, Administration Console, Tools (highlighted with a red box), Daily Monitor, Guardium Monitor, Tap Monitor, Incident Management, and My New Reports. On the left side, there is a 'Config & Control' sidebar with a 'Report Building' section. Under 'Report Building', a list of report types is shown, with 'Report Builder' highlighted by a red box. The main area is titled 'Report Builder' and contains a 'Report Finder' section. This section has a search bar with a help icon (?), and four input fields: 'Query', 'Report Title', 'Monitor' (with a checkbox), and 'Chart Type' (with a dropdown menu). Below these fields are two buttons: 'New...' and 'Search' (highlighted with a red box).

Report Builder

Report Search Results 

- DB Predefined Users Sessions
- DB Server List
- DB Server Throughput
- DB Server Throughput-Chart
- DB Users Mapping List
- DB2 Column Level Privs
- DB2 DB Level Privs
- DB2 for i S-TAP configuration**
- DB2 for i S-TAP Status
- DB2 i SQL activity
- DB2 Index Level Privs
- DB2 Package Level Privs
- DB2 Priv Summary
- DB2 Table Level Privs
- DB2 z/OS Database Privileges Granted To GRANTEE
- DB2 z/OS Database Privileges Granted To GRANTEE With GRANT Option
- DB2 z/OS Database Privileges Granted To PUBLIC
- DB2 z/OS Database Resource Granted To GRANTEE
- DB2 z/OS Database Resource Granted To GRANTEE With GRANT Option
- DB2 z/OS Database Resource Granted To PUBLIC

New... Clone Modify Delete Roles... Comments...

Add to My New Reports Add to Pane... Regenerate Portlet

API Assignment Drilldown Control

Back

Double click a row in the report to invoke API Options

The screenshot shows the IBM InfoSphere Guardium interface. At the top, there's a navigation bar with 'My New Reports' and 'Standard Reports'. Below that, a menu bar includes 'Monitor/Audit', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'System View', 'Administration Console', 'Tools', 'Daily Monitor', 'Guardium Monitor', 'Tap Monitor', and 'Incident Management'. The main area displays a report titled 'DB2 for i S-TAP configuration'. The report header includes columns for 'Datasource Name', 'SqlGuard Timestamp', 'Guard Host Name', and various filter options like 'FILTER USER', 'FILTER JOB', 'FILTER TCP/IP', 'FILTER TABLE', 'FILTER PORT', 'FILTER CLIENT ACCOUNTING', 'FILTER CLIENT APPLNAME', 'FILTER CLIENT PROGRAMID', 'FILTER CLIENT USERID', 'FILTER CLIENT WRKSTNNAME', 'FILTER RDB', 'FILTER SYSTEM SQL', and 'FILTER AUDIT ENTRY TYPES'. A row with 'svli5k' as the datasource name is selected, and a context menu is open over it, listing API functions: 'get_istap_config', 'get_istap_status', 'start_istap_monitor', 'stop_istap_monitor', and 'update_istap_config'. The 'get_istap_config' option is highlighted.

get_istap_config API Function

The screenshot shows the configuration dialog for the 'get_istap_config' API function. It includes the following fields and options:

- Report: DB2 for i S-TAP configuration
- Api Function: get_istap_config
- datasourceName: svli5k (marked as a required parameter)
- Log level: 0 (dropdown menu)
- Parameter Encryption not enabled - shared secret not set.
- Buttons: 'Generate script' and 'Invoke now' (highlighted with a red border).

Api Call Output get_istap_config

The screenshot shows the output of the 'get_istap_config' API call. The output is as follows:

```

Call Output
ID=0
Server name: 9.30.174.72
Filter user: null
Filter job: null
Filter tcpip: null
Filter table: null
Filter port: 0
Filter client accounting: null
Filter client application name: null
Filter client program name: null
Filter client user/group name: null
Filter client workstation name: null
Filter RDB: null
Filter system sql: Y
Filter audit entry types: AD AF CA CO DO GR OM OR OW PG PW RA RO RZ ZC ZR
Start user: MJA
connection_timeout_sec: 61
remote_messages: 0
Start job: QBATCH MJA 039768
Start time: 2012-08-23 11:51:37.739863
    
```

Close

start_istap_monitor Api function

IBM InfoSphere™ Guardium® 00:21 | Edit Account: larry | Customize | Logout | About | IBM

My New Reports | Standard Reports | Monitor/Audit | Discover | Assess/Harden | Comply | Protect | System View | Administration Console | Tools | Daily Monitor | Guardium Monitor | Tap Monitor | Incident Management | Standalone Unit

Build Queries and Reports
-Activity Report
DB2 for i S-TAP configuration

DB2 for i S-TAP configuration
Start Date: 2012-08-25 20:58:35 End Date: 2012-08-25 23:58:35
Aliases: OFF

Datasource Name	SqlGuard Timestamp	Guard Host Name	FILTER USER	FILTER JOB	FILTER TCPIP	FILTER TABLE	FILTER PORT	FILTER CLIENT ACCTING	FILTER CLIENT APPLNAME	FILTER CLIENT PROGRAMID	FILTER CLIENT USERID	FILTER CLIENT WRKSTNNAME	FILTER RDB	FILTER SYSTEM SQL	FILTER AUDIT ENTRY TYPES	Start User	ConnectionTimeout Sec	Remote Messages	Start Job	Start Time
svli5k	2012-08-20 10:57:45.0	9.30.174.72					0							Y	AD AF CA CO DO GR OM OR OW PG PW RA RO RZ ZC ZR	MJA	61	0	QBATCH MJA 038571	2012-08-11 00:01:49.0

Records 1 to 1 of 1

- get_istap_config
- get_istap_status
- start_istap_monitor**
- stop_istap_monitor
- update_istap_config

Api Call Output start_istap_monitor

Call Output

ID=0

S-TAP Status Monitor

Aliases: OFF

S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response Received	Primary Host Name	KTAP	TEE	MSS Shm	Win DB2 Shm	Win Local TCP	Pipes	Encrypted?	Firewall Installed
SVLI5K.SVL.IBM.COM	Guardium_S-Tap for IBM i_1		Active	2012-08-26 06:45:04	9.30.174.72	Yes	No	No	N/A	N/A	No	Unencrypted	No

Records 1 to 1 of 1

Build Queries and Reports
-Activity Report
DB2 for i S-TAP configuration

DB2 for i S-TAP configuration

Start Date: 2012-08-25 20:58:35 End Date: 2012-08-25 23:58:35
Aliases: OFF

Datasource Name	SqlGuard Timestamp	Guard Host Name	FILTER USER	FILTER JOB	FILTER TCP/IP	FILTER TABLE	FILTER PORT	FILTER CLIENT ACCTING	FILTER CLIENT APPLNAME	FILTER CLIENT PROGRAMID	FILTER CLIENT USERID	FILTER CLIENT WRKSTNNAME	FILTER RDB	FILTER SYSTEM SQL	FILTER AUDIT ENTRY TYPES	Start User	ConnectionTimeout Sec	Remote Messages	Start Job	Start Time
svli5k	2012-08-20 10:57:45.0	9.30.174.72					0							Y	AD AF CA CO DO GR OM OR OW PG PW RA RO RZ ZC ZR	MJA	61	0	QBATCH MJA 038571	2012-08-11 00:01:49.0

Records 1 to 1 of 1

get_istap_config
get_istap_status
start_istap_monitor
stop_istap_monitor
update_istap_config

Report: IBM iSeries S-TAP configuration
Api Function: update_istap_config

datasourceName: svli5k-new *

guardium_host: 9.30.174.72

filter_user: unchange

filter_job: unchange

filter_tcpip: unchange

filter_table: unchange

filter_port: 0

filter_client_acct: unchange

filter_client_appl: unchange

filter_client_prog: unchange

filter_client_user: unchange

filter_client_wkstn: unchange

filter_rdb: SVLI5K

filter_system_sql: Y

filter_audit_entry_types: AF CA CO DO OM OR OW PG

connection_timeout_sec: 61

remote_messages: 0

start_monitor: 1

*Required parameter

Log level: 0

Parameter Encryption not enabled - shared secret not set.

Generate script Invoke now

Update_istap_config API

When **start_monitor** is set **1** (default), the auditing process will start (or restart) the DB2 i server after the configuration table is updated from **Invoke now**

Policies for DB2 i

My New Reports Administration Console System View Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management Standard Reports Monitor/Audit Comply **Protect** Standalone Unit

Security Policies Correlation Alerts Incident Management

Data Access Policy Application

Policy builder Baseline builder Group builder Time Period builder

View Installed Policy

Currently Installed Policies

Installed Policy #1

Installed Policy DB2 i Log Full Details
Date Installed 8/24/13 7:53 PM
This is not a selective audit policy
Not logging to flat
Rules don't fire on flat

Installed Rules 2
Baseline records 0

Edit Installed Policy
View Details Report

Policy Violation Count

Start Date: 2013-08-23 20:32:48 End Date: 2013-08-24 20:32:48

Data Access Policy Application

Policy Definition

Policy description DB2 i Log Full Details
Policy category
Log flat
Rules on flat
Selective audit trail
Audit pattern


Roles

No roles have been assigned to this policy Roles...

Back Add Comments **Edit Rules...** Reinstall Apply

Data Access Policy Application

Policy Rules ?

DB2 i Log Full Details Filter: 

Rule Suggestion

Rule min. ct. Object Group min. ct.

Access Rule Definition

Rule #1 of policy DB2 i Log Full Details

Description

Category Classification Severity

Not Server IP / and/or Group

Not Client IP / and/or Group

Not Client MAC

Net Prtcl. and/or Group

DB Type

Not Svc. Name and/or Group

Not DB Name and/or Group

Not DB User and/or Group

Not Client IP/Src App./DB User/Server IP/Svc. Name

Not App. User and/or Group

Not OS User and/or Group

Not Src App. and/or Group

Not Field and/or Group Every

Not Object and/or Group Every

Not Command and/or Group Every

Not Object/Cmd. Group

Not Object/Field Group

Pattern (RE)

XML Pattern (RE)

App Event Exists Event Type Event User Name

App Event Values Text and/or Group

Numeric Date

Masking Pattern (RE) Replacement Character

Time Period

Minimum Count Reset Interval minutes Trigger Once Per Session

Quarantine for minutes Records Affected Threshold Rec. Vals. Cont. to next rule

Actions


LOG FULL DETAILS

Add Action


Back Add Comments Save

- ALERT DAILY
- ALERT ONCE PER SESSION
- ALERT ONLY
- ALERT PER MATCH
- ALERT PER TIME GRANULARITY
- ALLOW
- Do Not RECORD VALUES SEPARATELY
- IGNORE RESPONSES PER SESSION
- IGNORE S-TAP SESSION
- IGNORE SESSION
- IGNORE SQL PER SESSION
- LOG FULL DETAILS**
- LOG FULL DETAILS PER SESSION
- LOG MASKED DETAILS
- LOG ONLY
- MARK AS AUTO-COMMIT OFF
- MARK AS AUTO-COMMIT ON
- NO PARSE
- QUARANTINE
- QUICK PARSE
- QUICK PARSE NATIVE
- QUICK PARSE NO FIELDS
- RECORD VALUES SEPARATELY
- S-GATE ATTACH
- S-GATE DETACH
- S-GATE TERMINATE
- S-TAP TERMINATE
- SKIP LOGGING

Granular Access Policy


Rule #4 Description 

Category **Classification** **Severity**


Not **Server IP** / and/or Group 


Not **Client IP** / and/or Group


Not **Client MAC** **Net. Protocol** and/or Group

DB Type  **Not** **Service Name** and/or Group


Not **DB Name** and/or Group


Not **DB User** and/or Group 


Not **App. User** and/or Group 

Not **OS User** and/or Group 

Not **Src App.** and/or Group

Not **Field Name** and/or Group 

Not **Object** and/or Group 

Not **Command** and/or Group 

Min. Ct. **Reset Interval (minutes)**

Continue to next Rule **Rec. Vals.**

Action

Which Servers

Which Databases

Which Users

Which Fields

Which Tables

Which SQL Commands

Access Rule Definition

Rule #2 of policy DB2 i Log Full Details

Description

Category Classification Severity HIGH

Not Server IP / and/or Group

Not Client IP / and/or Group

Not Client MAC

Net Prtcl. and/or Group

DB Type

Not Svc. Name and/or Group

Not DB Name and/or Group

Not DB User and/or Group

Not Client IP/Src App./DB User/Server IP/Svc. Name

Not App. User and/or Group

Not OS User and/or Group

Not Src App. and/or Group

Not Field and/or Group Every

Not Object and/or Group Every

Not Command and/or Group Every

Not Object/Cmd. Group

Not Object/Field Group

Pattern RE

XML Pattern RE

App Event Exists Event Type Event User Name

App Event Values Text and/or Group

Numeric Date

Masking Pattern RE Replacement Character

Time Period

Minimum Count Reset Interval minutes Trigger Once Per Session

Quarantine for minutes Records Affected Threshold Rec. Vals. Cont. to next rule

Actions

ALERT PER MATCH

Add Action

Back Add Comments Save

IBM® InfoSphere™ Guardium®

Manage Members for Selected Group

Group Name DB2i Delete/Update

Group Type COMMANDS

Category

Group Members Filter

DELETE UPDATE

Modify Group Type

Modify Category

My New Reports Administration Console System View Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management

Security Policies Correlation Alerts Incident Management

Data Access Policy Application

Not Server IP / and/or Group

Not Client IP / and/or Group

Not Client MAC

Net Prtl. and/or Group

DB Type

Not Svc. Name and/or Group

Not DB Name and/or Group

Not DB User LARKINB and/or Group

Not Client IP/Src App./DB User/Server IP/Svc. Name

Not App. User and/or Group

Not OS User and/or Group

Not Src App. and/or Group

Not Field and/or Group Every

Not Object and/or Group Every

Not Command and/or Group (Public) DB2i Delete/Update Every

Not Object/Cmd. Group

Not Object/Field Group

Pattern RE

XML Pattern RE

App Event Exists Event Type Event User Name

App Event Values Text and/or Group

Numeric Date

Masking Pattern RE Replacement Character *

Time Period

Minimum Count 0 Reset Interval 0 minutes Trigger Once Per Session

Quarantine for 0 minutes Records Affected Threshold 0 Rec. Vals. Cont. to next rule

Actions

Add New Action

Action ALERT PER MATCH

Message Template Default

Notification




Notification Type







Alert Receiver

- MAIL
- SNMP
- CUSTOM
- SYSLOG**

Add

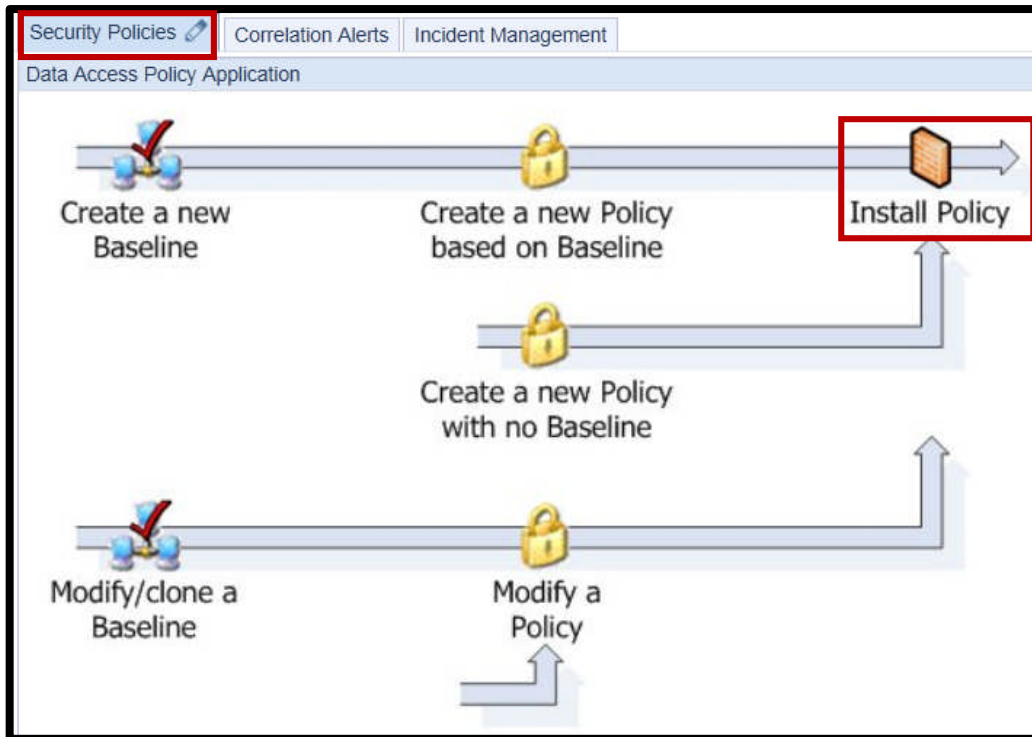
Policy Rules ?

DB2 i Log Full Details Filter:   

<input type="checkbox"/>				<input checked="" type="checkbox"/>	1 Access Rule: Log Full Details (Installed)
<input type="checkbox"/>				<input checked="" type="checkbox"/>	2 Access Rule: Alert on Delete/Update (Installed)

Rule Suggestion

Rule min. ct. Object Group min. ct.



View Installed Policy

Currently Installed Policies

Installed Policy #1

Installed Policy DB2 i Log Full Details
Date Installed 8/24/13 7:53 PM
This is not a selective audit policy
Not logging to flat
Rules don't fire on flat
Installed Rules 2
Baseline records 0

Edit Installed Policy
View Details Report

Policy Installer

- Allow-All
- Basel II
- Capture and Replay - DB2-to-DB2
- Capture and Replay - Heterogeneous
- Data Privacy
- Data Privacy - PII
- DB2 i Log Full Details**
- Default - Ignore Data Activity for Unknown Connections
- Default Sharepoint Auditing
- Hadoop Policy
- HIPAA
- log full det
- PCI
- PCI, Oracle EBS
- PCI, SAP
- Privileged Users Monitoring (black list)

-- Select an installation action --
-- Select an installation action --
Install & Override
Install before policy.log full det
Install last

Scheduled for execution.

Modify Schedule... Run Once Now

Are you sure you want to install this policy and apply it to all Inspection Engines?

OK Cancel

My New Reports	Administration Console	System View	Tools	Daily Monitor	Guardium Monitor	Tap Monitor	Incident Management	Standard Reports	Monitor/Audit	Comply	Protect
Policy Violations / Incident Management											
Start Date: 2013-08-25 11:43:46 End Date: 2013-08-26 14:43:46											
Aliases: OFF											
Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity	Description	Incident Number	Count of Policy Rule Violations
490	2013-08-25 14:42:08.0		Alert on Delete/Update	9.56.49.185	9.5.50.69	LARKINB	DELETE FROM EMPSAL WHERE EMPNO = ?	HIGH		0	1
489	2013-08-25 14:39:28.0		Alert on Delete/Update	9.56.49.185	9.5.50.69	LARKINB	UPDATE EMPSAL SET SALARY = ? WHERE EMPNO = ?	HIGH		0	1
Records 1 to 2 of 2											

INSERT into EMPSAL values ('11111','White',95000)
 INSERT into EMPSAL values ('22222','Jones,82000)
 INSERT into EMPSAL values ('33333','Smith',77000)

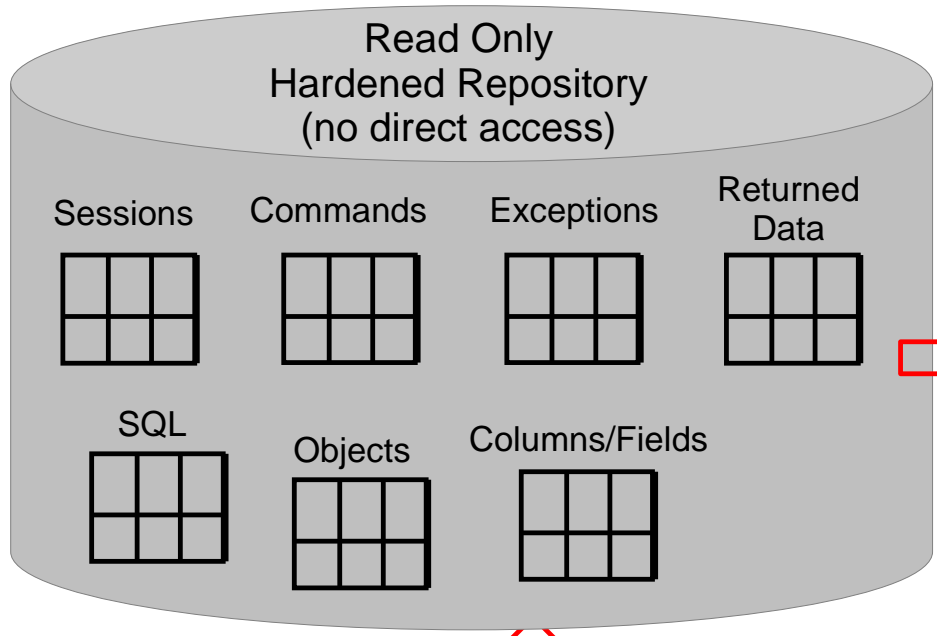
UPDATE EMPSAL set salary = 85000 where empno = '33333'

DELETE from EMPSAL where empno = '33333'

DB2 i Reports

Reporting

Session Id	DB User Name	SQL Verb	Object Name	Full Sql
16091	JOE	SELECT	creditcard	select name,cardid from creditcard



Logged in repository

Query builder for reports

Entity List

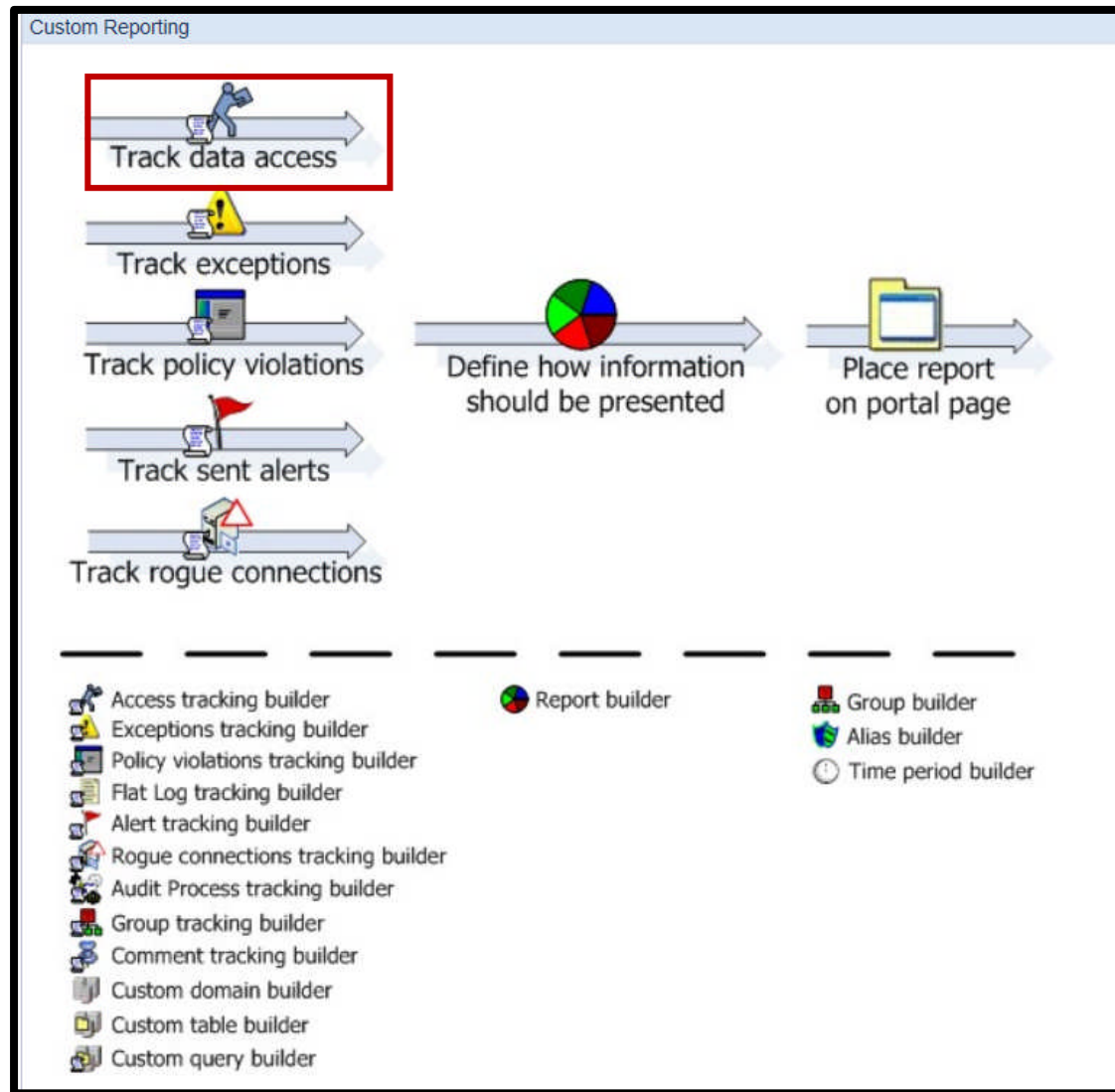
- Client/Server
- Server IP/Server Port
- Session
- Access Period
- SQL
- FULL SQL
- Full Sql
- Timestamp
- Response Time
- Records Affected
- Returned Data
- 7AX5 Full SQL ID
- 7AX5 Instance ID
- Successful
- Records Affected (Desc)
- Access Rule Description
- Returned Data Count
- Auto-Commit
- 7AX5 Response Time
- 7AX5 Statement Type
- Bind Variables Values
- Original Timezone
- FULL SQL Values
- Application Events
- App User Name
- Command
- Object
- Object/Command
- Join
- Field
- Object/Field
- Qualified Object
- Field SQL Value

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
1	Client/Server	DB User Name	Value			
2	FULL SQL	Full SQL ID	Value		1	
3	Access Period	Session Id				
4	FULL SQL					
5	SQL					
6	SQL	Construct Id				
7	Access Period	Instance Id				
8	Command	SQL Verb				
9	Object	Object Name				
10	Field	Field Name				

Entities and attributes

Entity	Agg.	Attribute	Operator	Runtime Param.
WHERE FULL SQL		Full Sql	LIKE	Parameter FullSQLLike
AND Session		Session Id	LIKE	Parameter SessionIDLike
AND Session		Access Id	LIKE	Parameter AccessIDLike
AND FULL SQL		Instance ID	LIKE	Parameter InstanceIDLike
AND SQL		Construct Id	LIKE	Parameter ConstructIDLike
AND Client/Server		Client IP	LIKE	Parameter ClientIPLike
AND Client/Server		Server IP	LIKE	Parameter ServerIPLike
AND Client/Server		Network Protocol	LIKE	Parameter NetProtoLike
AND Client/Server		DB User Name	LIKE	Parameter DBUserLike

DB2 for i message forwarded from the Audit Server...



Custom Reporting

New Query - Overall Details [?](#)

Query Name

Main Entity

Custom Reporting

New Query - Overall Details [?](#)

Query Name

Main Entity

- Select an Entity --
- Client/Server By Session
- Client/Server
- Session
- Server IP/Server Port
- Application Events
- Changed Data Value
- App User Name
- FULL SQL Values
- FULL SQL
- SQL**
- Access Period
- Command
- Object
- Object/Command
- Join
- Object/Field
- Qualified Object
- Field
- Field SQL Value
- Session Start
- Session End

Access Tracking

Entity List

- Client/Server
- Session
- Server IP/Server Port
- Application Events
- Changed Data Value
- App User Name
- FULL SQL Values
- FULL SQL
- SQL
- Access Period
- Command
- Object
- Object/Command
- Join
- Object/Field
- Qualified Object
- Field
- Field SQL Value

Activity Report

Main Entity: SQL

Add Count Add Distinct Sort by count

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend

Addition mode: AND OR HAVING

Entity	Agg.	Attribute	Operator	Runtime Param.

Entity List

- Client/Server
- Server IP/Server Port
- Session
- Access Period
 - 7AX5 Session Id
 - 7AX5 Instance Id
 - 7AX5 Construct Id
 - Total access
 - Period Start
 - Period Start Date
 - Period Start Weekday
 - Period Start Time
 - Timestamp
 - Add Field
 - Add Condition
 - Timestamp WeekDay
 - Timestamp Year
 - Period End
 - Period End Date
 - Period End Weekday
 - Period End Time
 - Application User

-Activity Report ?

Main Entity: SQL
 Add Count
 Add Distinct
 Sort by count
 Run In Two Stages

Query Fields						
Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend

Addition mode: AND
 OR
 HAVING

Query Conditions				
Entity	Agg.	Attribute	Operator	Runtime Param.

Delete Clone Roles... Save Back

Data Mart Generate Tabular Regenerate Add to Pane... Add to My New Reports

Entity List

- Client/Server
- Server IP/Server Port
- Session
- Access Period
 - 7AX5 Session Id
 - 7AX5 Instance Id
 - 7AX5 Construct Id
- Total access
- Period Start
- Period Start Date
- Period Start Weekday
- Period Start Time
- Timestamp
- Timestamp Date
- Timestamp Time
- Timestamp WeekDay
- Timestamp Year
- Period End
- Period End Date
- Period End Weekday
- Period End Time
- Application User

-Activity Report ?

Main Entity: SQL
 Add Count
 Add Distinct
 Sort by count
 Run In Two Stages

Query Fields						
Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
1	Access Period	Timestamp	Value ▾	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>

Addition mode: AND
 OR
 HAVING

Query Conditions				
Entity	Agg.	Attribute	Operator	Runtime Param.

Delete Clone Roles... Save Back

Data Mart Generate Tabular Regenerate Add to Pane... Add to My New Reports

Entity List

- Client/Server
- Server
- IP/Server Port
- Session
- Access Period
- SQL
- FULL SQL
- FULL SQL Values
- Changed Data Value
- Application Events
- App User Name
- Command
- Object
- Object/Command
- Join
- Field
- Object/Field
- Qualified Object
- Field SQL Value

-Activity Report ?

Main Entity: **SQL**
 Add Count
 Add Distinct
 Sort by count
 Run In Two Stages

Query Fields

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Access Period	Timestamp	Value ▾	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Client IP	Value ▾	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	3	Access Period	DB2 i/z Database	Value ▾	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	4	Access Period	DB2 i/z Program	Value ▾	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	5	Access Period	DB2 i Current User	Value ▾	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	6	Client/Server	Source Program	Value ▾	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	7	FULL SQL	Full Sql	Value ▾	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	8	Session	Client Port	Value ▾	<input type="checkbox"/>	<input type="checkbox"/>

Addition mode: AND
 OR
 HAVING

Query Conditions

Entity	Agg.	Attribute	Operator	Runtime Param.

Entity List

- Client/Server
- Server
- IP/Server Port
- Session
- Access Period
- SQL
- FULL SQL
- Full Sql
- Add Field
- Add Condition
- # Records Affected
- Returned Data
- 7AX5 Full SQL ID
- 7AX5 Instance ID
- ✓ Succeeded
- # Records Affected (Desc)
- desc: Access Rule Description
- # Returned Data Count
- # Auto-Commit
- # Ack Response Time
- 7AX5 Statement Type
- Bind Variables Values
- Original Timezone

-Activity Report ?

Main Entity: **SQL**
 Add Count
 Add Distinct
 Sort by count
 Run In Two Stages

Query Fields							
Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend	
<input type="checkbox"/>	1	Access Period	Timestamp	Value ▾	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Client IP	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	3	Access Period	DB2 i/z Database	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	4	Access Period	DB2 i/z Program	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	5	Access Period	DB2 i Current User	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	6	Client/Server	Source Program	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	7	FULL SQL	Full Sql	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	8	Session	Client Port	Value ▾	<input type="checkbox"/>		

Query Conditions				
Entity	Agg.	Attribute	Operator	Runtime Param.
(X) (I) (J) Addition mode: <input checked="" type="radio"/> AND <input type="radio"/> OR <input type="checkbox"/> HAVING				

Entity List

- Client/Server
- Server IP/Server
- Port
- Session
- Access Period
- SQL
- FULL SQL
- Full Sql
- Timestamp
- Response Time
- # Records Affected
- Returned Data
- 7AX5 Full SQL ID
- 7AX5 Instance ID
- Succeeded
- # Records Affected (Desc)
- desc: Access Rule Description
- # Returned Data Count
- # Auto-Commit
- # Ack Response Time
- 7AX5 Statement Type
- Bind Variables Values

-Activity Report ?

Main Entity: SQL
 Add Count
 Add Distinct
 Sort by count
 Run In Two Stages

Query Fields							
Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend	
<input type="checkbox"/>	1	Access Period	Timestamp	Value ▾	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Client IP	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	3	Access Period	DB2 i/z Database	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	4	Access Period	DB2 i/z Program	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	5	Access Period	DB2 i Current User	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	6	Client/Server	Source Program	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	7	FULL SQL	Full Sql	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	8	FULL SQL	Bind Variables Values	Value ▾	<input type="checkbox"/>		

Query Conditions					
	Entity	Agg.	Attribute	Operator	Runtime Param.
<input type="checkbox"/>	WHERE	FULL SQL	-----	Full Sql	----- ▾

Delete Clone Roles... Save Back

Data Mart Generate Tabular Regenerate Add to Pane... Add to My New Reports

Entity List

- Client/Server
- Server IP/Server
- Port
- Session
- Access Period
- SQL
- FULL SQL
- Full Sql
- Timestamp
- Response Time
- Records Affected
- Returned Data
- Full SQL ID
- Instance ID
- Succeeded
- Records Affected (Desc)
- Access Rule Description
- Returned Data Count
- Auto-Commit
- Ack Response Time
- Statement Type
- Bind Variables Values

-Activity Report ?

Main Entity: SQL
 Add Count
 Add Distinct
 Sort by count
 Run In Two Stages

Query Fields							
Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend	
<input type="checkbox"/>	1	Access Period	Timestamp	Value	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Client IP	Value	<input type="checkbox"/>		
<input type="checkbox"/>	3	Access Period	DB2 i/z Database	Value	<input type="checkbox"/>		
<input type="checkbox"/>	4	Access Period	DB2 i/z Program	Value	<input type="checkbox"/>		
<input type="checkbox"/>	5	Access Period	DB2 i Current User	Value	<input type="checkbox"/>		
<input type="checkbox"/>	6	Client/Server	Source Program	Value	<input type="checkbox"/>		
<input type="checkbox"/>	7	FULL SQL	Full Sql	Value	<input type="checkbox"/>		
<input type="checkbox"/>	8	FULL SQL	Bind Variables Values	Value	<input type="checkbox"/>		

AND
 OR
 HAVING

Query Conditions					
	Entity	Agg.	Attribute	Operator	Runtime Param.
<input type="checkbox"/>	WHERE		FULL SQL	Full Sql	

- <
- <=
- <>
- =
- >
- >=
- IN ALIASES GROUP
- IN DYNAMIC ALIASES GROUP
- IN DYNAMIC GROUP
- IN GROUP
- IS NOT NULL
- IS NULL
- LIKE
- LIKE GROUP
- NOT IN ALIASES GROUP
- NOT IN DYNAMIC ALIASES GROUP
- NOT IN DYNAMIC GROUP
- NOT IN GROUP
- NOT LIKE**
- NOT LIKE GROUP
- NOT REGEXP

Data Mart
Generate Tabular
one
Roles...
Save
Back

Add to My New Reports

Entity List

- Client/Server
- Server IP/Server
- Port
- Session
- Access Period
- SQL
- FULL SQL
- Full Sql
- Timestamp
- Response Time
- Records Affected
- Returned Data
- Full SQL ID
- Instance ID
- Succeeded
- Records Affected (Desc)
- Access Rule Description
- Returned Data Count
- Auto-Commit
- Ack Response Time
- Statement Type
- Bind Variables

-Activity Report

Main Entity: SQL Add Count Add Distinct Sort by count Run In Two Stages

Query Fields							
Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend	
<input type="checkbox"/>	1	Access Period	Timestamp	Value	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Client IP	Value	<input type="checkbox"/>		
<input type="checkbox"/>	3	Access Period	DB2 i/z Database	Value	<input type="checkbox"/>		
<input type="checkbox"/>	4	Access Period	DB2 i/z Program	Value	<input type="checkbox"/>		
<input type="checkbox"/>	5	Access Period	DB2 i Current User	Value	<input type="checkbox"/>		
<input type="checkbox"/>	6	Client/Server	Source Program	Value	<input type="checkbox"/>		
<input type="checkbox"/>	7	FULL SQL	Full Sql	Value	<input type="checkbox"/>		
<input type="checkbox"/>	8	FULL SQL	Bind Variables Values	Value	<input type="checkbox"/>		

Addition mode: AND OR HAVING

Query Conditions					
	Entity	Agg.	Attribute	Operator	Runtime Param.
<input type="checkbox"/>	WHERE	FULL SQL	Full Sql	NOT LIKE	<div style="border: 1px solid red; padding: 2px;"> Value Value Parameter Attribute </div>

Delete Clone Roles... Save Back

Data Mart Generate Tabular Regenerate Add to Pane... Add to My New Reports

Entity List

- Client/Server
- Server IP/Server
- Port
- Session
- Access Period
- SQL
- FULL SQL
- FULL SQL Values
- Changed Data
- Value
- Application
- Events
- App User Name
- Command
- Object
- Object/Command
- Join
- Field
- Object/Field
- Qualified Object
- Field SQL Value

-Activity Report ?

Main Entity: **SQL** Add Count Add Distinct Sort by count Run In Two Stages

Query Fields

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Access Period	Timestamp	Value ▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Client IP	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	3	Access Period	DB2 i/z Database	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	4	Access Period	DB2 i/z Program	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	5	Access Period	DB2 i Current User	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	6	Client/Server	Source Program	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	7	FULL SQL	Full Sql	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	8	FULL SQL	Bind Variables Values	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>

Addition mode: AND OR HAVING

	Entity	Agg.	Attribute	Operator	Runtime Param.	
<input type="checkbox"/>	WHERE	FULL SQL	Full Sql	NOT LIKE	Value ▼	%GuardAppEvent%

Delete Clone Roles... Save Back

Data Mart Generate Tabular Regenerate Add to Pane... Add to My New Reports

Entity List

- Client/Server
- 7AX5 Access Id
- Timestamp
- Timestamp
- Date
- Timestamp
- Time
- Timestamp
- WeekDay
- Timestamp
- Year
- Server Type
- 123 Client IP
- 321 Server IP
- Network Protocol
- DB Protocol
- DB Protocol Version
- DB User Name
- Source Program
- 7AX5 Client MAC
- *host:X* Client Host Name
- svcX Service Name
- Server OS
- Client OS
- OS User
- *host:X* Server Host Name

-Activity Report

Main Entity: SQL
 Add Count
 Add Distinct
 Sort by count
 Run In Two Stages

Query Fields						
Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Access Period	Timestamp	Value	<input checked="" type="checkbox"/>	1 <input checked="" type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Client IP	Value	<input type="checkbox"/>	
<input type="checkbox"/>	3	Access Period	DB2 i/z Database	Value	<input type="checkbox"/>	
<input type="checkbox"/>	4	Access Period	DB2 i/z Program	Value	<input type="checkbox"/>	
<input type="checkbox"/>	5	Access Period	DB2 i Current User	Value	<input type="checkbox"/>	
<input type="checkbox"/>	6	Client/Server	Source Program	Value	<input type="checkbox"/>	
<input type="checkbox"/>	7	FULL SQL	Full Sql	Value	<input type="checkbox"/>	
<input type="checkbox"/>	8	Session	Client Port	Value	<input type="checkbox"/>	

Query Conditions						
Addition mode: <input checked="" type="radio"/> AND <input type="radio"/> OR <input type="checkbox"/> HAVING						
	Entity	Agg.	Attribute	Operator	Runtime Param.	
<input type="checkbox"/>	WHERE	FULL SQL	Full Sql	NOT LIKE	Value	%GuardAppEvent%
<input type="checkbox"/>	AND	Client/Server	Client IP	LIKE	Value	

Entity List

Client/Server

7AX5 Access Id

Timestamp

Timestamp

Date

Timestamp

Time

Timestamp

WeekDay

Timestamp

Year

Server Type

123 Client IP

321 Server IP

Network Protocol

DB Protocol

DB Protocol Version

DB User Name

Source Program

7AX5 Client MAC

host.X Client Host Name

svcX Service Name

Server OS

Client OS

OS User

host.X Server Host Name

-Activity Report

Main Entity: SQL Add Count Add Distinct Sort by count Run In Two Stages

Query Fields

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Access Period	Timestamp	Value ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Client IP	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	3	Access Period	DB2 i/z Database	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	4	Access Period	DB2 i/z Program	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	5	Access Period	DB2 i Current User	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	6	Client/Server	Source Program	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	7	FULL SQL	Full Sql	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	8	Session	Client Port	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>

Addition mode: AND OR HAVING

	Entity	Agg.	Attribute	Operator	Runtime Param.
<input type="checkbox"/>	WHERE FULL SQL	-----	Full Sql	NOT LIKE ▼	Value ▼ %GuardAppEvent%
<input type="checkbox"/>	AND Client/Server	-----	Client IP	LIKE ▼	Parameter ▼ ClientIP

Entity List

- Client/Server
- Server IP/Server
- Port
- Session
- Access Period
- SQL
- FULL SQL
- FULL SQL
- Values
- Changed Data Value
- Application Events
- App User Name
- Command
- Object
- Object/Command
- Join
- Field
- Object/Field
- Qualified Object
- Field SQL Value

-Activity Report ?





Main Entity: **SQL**
 Add Count
 Add Distinct
 Sort by count
 Run In Two Stages


Query Fields

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Access Period	Timestamp	Value ▾	<input checked="" type="checkbox"/>	1 <input type="text"/>
<input type="checkbox"/>	2	Client/Server	Client IP	Value ▾	<input type="checkbox"/>	
<input type="checkbox"/>	3	Access Period	DB2 i/z Database	Value ▾	<input type="checkbox"/>	
<input type="checkbox"/>	4	Access Period	DB2 i/z Program	Value ▾	<input type="checkbox"/>	
<input type="checkbox"/>	5	Access Period	DB2 i Current User	Value ▾	<input type="checkbox"/>	
<input type="checkbox"/>	6	Client/Server	Source Program	Value ▾	<input type="checkbox"/>	
<input type="checkbox"/>	7	FULL SQL	Full Sql	Value ▾	<input type="checkbox"/>	
<input type="checkbox"/>	8	Session	Client Port	Value ▾	<input type="checkbox"/>	

X
 ()
 Addition mode:
 AND
 OR
 HAVING

Query Conditions

Entity	Agg.	Attribute	Operator	Runtime Param.				
<input type="checkbox"/>	WHERE	FULL SQL	-----	Full Sql	NOT LIKE	Value ▾	%GuardAppEvent%	
<input type="checkbox"/>	AND	Client/Server	-----	Client IP	LIKE	Parameter ▾	ClientIP	
<input type="checkbox"/>	AND	Access Period	-----	DB2 i/z Database	LIKE	Parameter ▾	DB2iDatabase	
<input type="checkbox"/>	AND	Client/Server	-----	DB User Name	LIKE	Parameter ▾	DBUserName	

My New Reports  Administration Console System View Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management Standard Reports

Build Queries and Reports


- Activity Report
- DB2 for i S-TAP configuration
- Command Tracking


-Activity Report

Start Date: **2013-08-22 14:54:57** End Date: **2013-08-24 14:54:57**
 Aliases: **OFF** ClientIP: **LIKE**
 DB2iDatabase: **LIKE** DBUserName: **LIKE**

Timestamp Client IP DB2 i/z Database DB2 i/z Program DB2 i Current User Source Program Full Sql Client Port

No data found


Records to 0 of 0 

-Activity Report 

Start Date: **2013-08-22 14:54:57** End Date: **2013-08-24 14:54:57**
 Aliases: **OFF** ClientIP: **LIKE**
 DB2iDatabase: **LIKE** DBUserName: **LIKE**


Timestamp Client IP DB2 i/z Database DB2 i/z Program DB2 i Current User Source Program Full Sql Client Port

No data found

Records to 0 of 0 






IBM® InfoSphere™ Guardium®

Customize Portlet


Report: **-Activity Report** Based on Query: **-Activity Report** 

Title -Activity Report

Run Time Parameters


ClientIP Enter Value for Client IP	LIKE <input type="text"/>
DB2iDatabase Enter Value for DB2 i/z Database	LIKE <input type="text"/>
DBUserName Enter Value for DB User Name	LIKE <input type="text"/>
QUERY_FROM_DATE Enter Period From	>= NOW -1 DAY  
QUERY_TO_DATE Enter Period To	<= NOW  
REMOTE_SOURCE Remote Data Source	-- none -- 
SHOW_ALIASES Show Aliases	<input type="radio"/> On <input type="radio"/> Off <input type="radio"/> Default

Presentation Parameters

fetchSize Max. records per page	20 
refreshRate Refresh rate (seconds)	<input type="text" value="0"/>

IBM InfoSphere™ Guardium™

Customize Portlet

Report: **-Activity Report** Based on Query: **-Activity Report** 



Title



Run Time Parameters

ClientIP **Enter Value for Client IP** LIKE %

DB2iDatabase **Enter Value for DB2 i/z Database** LIKE %

DBUserName **Enter Value for DB User Name** LIKE %

QUERY_FROM_DATE **Enter Period From** >= NOW -1 DAY  

QUERY_TO_DATE **Enter Period To** <= NOW  


REMOTE_SOURCE **Remote Data Source** -- none --

SHOW_ALIASES **Show Aliases** On Off Default

Presentation Parameters


fetchSize **Max. records per page** 20

refreshRate **Refresh rate (seconds)** 0

-Activity Report 

Start Date: **2013-08-27 12:46:24** End Date: **2013-08-28 12:46:24**
 Aliases: **OFF** ClientIP: **LIKE %**
 DB2iDatabase: **LIKE %** DBUserName: **LIKE %**

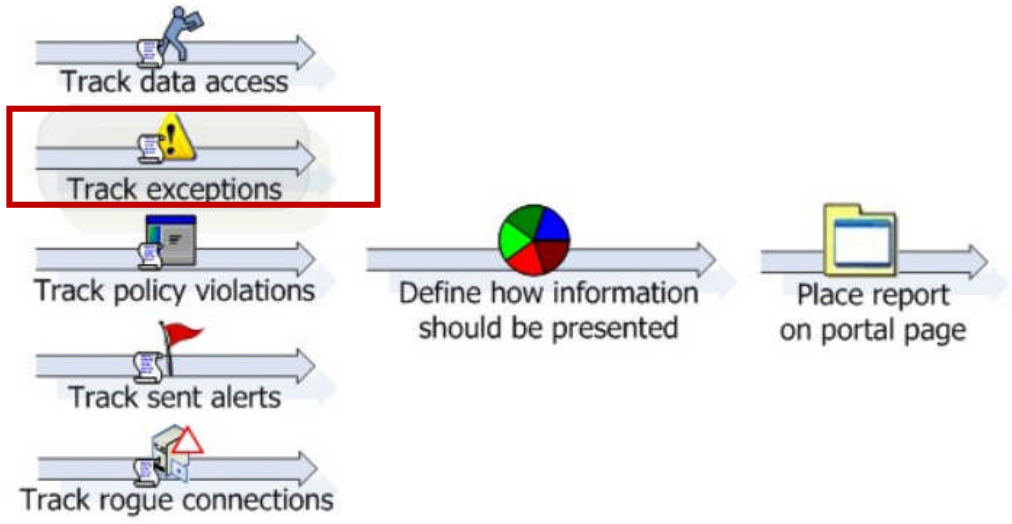
Timestamp	Client IP	DB2 i/z Database	DB2 i/z Program	DB2 i Current User	Source Program	Full Sql	Bind Variables Values
2013-08-28 12:12:30.0	9.10.111.49	LP13UT16	QSYS/QCMD	MJA	MJA/QPADEV000D	CA - Authority change MJATST QTNNTX *PGM	
2013-08-28 12:12:30.0	9.10.111.49	LP13UT16	QSYS/QCMD	MJA	MJA/QPADEV000D	CA - Authority change MJATST QTNNTX *PGM	
2013-08-28 12:12:30.0	9.10.111.49	LP13UT16	QSYS/QCMD	MJA	MJA/QPADEV000D	CA - Authority change MJATST QTNNTX *PGM	
2013-08-28 12:12:30.0	9.10.111.49	LP13UT16	QSYS/QCMD	MJA	MJA/QPADEV000D	CA - Authority change MJATST QTNNTX *PGM	
2013-08-28 12:12:30.0	9.10.111.49	LP13UT16	QSYS/QZDASOINIT	MJA	QUSER/QZDASOINIT	CA - Authority change QSYS2 QSQPDTBL *FILE	
2013-08-28 12:12:17.0	9.5.37.48	LP06UT16	QSYS/QS9UTIL	QSRVAGT	QSRVAGT/QS9PALMONINSERT INTO QSRVAGT / QAS9AUDLOG (LOGDATA) VALUES (: H)	'13/08/28 12:10:45 QS9PALMON: running	
2013-08-28 12:12:17.0	9.5.37.48	LP06UT16	QSYS/QS9UTIL	QSRVAGT	QSRVAGT/QS9PALMONINSERT INTO QSRVAGT / QAS9AUDLOG (LOGDATA) VALUES (: H)	'13/08/28 12:10:45 QS9PALMON: ready for cycle	
2013-08-28 12:10:59.0	9.10.111.49	LP13UT16	QTCP/QTMFSRVR	MJA	QTCP/QTFTP00044	CA - Authority change QRECOVERY QDBRG27147*FILE	
2013-08-28 12:10:59.0	9.10.111.49	LP13UT16	QTCP/QTMFSRVR	MJA	QTCP/QTFTP00044	CA - Authority change QRECOVERY QDBRG27147*FILE	
2013-08-28 12:10:59.0	127.0.0.1	LP06UT16/		QSECOFR	QUSER/QSQSRVR	COMMIT	
2013-08-28 12:10:59.0	127.0.0.1	LP06UT16/		QSECOFR	QUSER/QSQSRVR	COMMIT	
2013-08-28 12:10:59.0	127.0.0.1	LP06UT16/		QSECOFR	QUSER/QSQSRVR	COMMIT	
2013-08-28 12:10:59.0	127.0.0.1	LP06UT16/		QSECOFR	QUSER/QSQSRVR	COMMIT	
2013-08-28 12:10:59.0	127.0.0.1	LP06UT16/		QSECOFR	QUSER/QSQSRVR	COMMIT	
2013-08-28 12:10:59.0	127.0.0.1	LP06UT16/		QSECOFR	QUSER/QSQSRVR	COMMIT	
2013-08-28 12:10:59.0	127.0.0.1	LP06UT16/		QSECOFR	QUSER/QSQSRVR	COMMIT	
2013-08-28 12:10:59.0	127.0.0.1	LP06UT16/		QSECOFR	QUSER/QSQSRVR	COMMIT	
2013-08-28 12:10:59.0	127.0.0.1	LP06UT16/		QSECOFR	QUSER/QSQSRVR	COMMIT	
2013-08-28 12:10:59.0	127.0.0.1	LP06UT16/		QSECOFR	QUSER/QSQSRVR	COMMIT	
2013-08-28 12:10:59.0	127.0.0.1	LP06UT16/		QSECOFR	QUSER/QSQSRVR	COMMIT	
2013-08-28 12:10:59.0	127.0.0.1	LP06UT16/		QSECOFR	QUSER/QSQSRVR	COMMIT	
2013-08-28 12:10:59.0	127.0.0.1	LP06UT16/		QSECOFR	QUSER/QSQSRVR	COMMIT	
2013-08-28 12:10:59.0	127.0.0.1	LP06UT16/		QSECOFR	QUSER/QSQSRVR	COMMIT	

Records to 20 of 3307 

My New Reports Administration Console System View Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management Standard Reports Monitor/Audit Comply Protect

Build Queries and Reports
 -Activity Report
 DB2 for i S-TAP configuration
 Command Tracking

Custom Reporting



Track data access

Track exceptions

Track policy violations

Track sent alerts

Track rogue connections


Define how information should be presented

Place report on portal page

- Access tracking builder
- Exceptions tracking builder
- Policy violations tracking builder
- Flat Log tracking builder
- Alert tracking builder
- Rogue connections tracking builder
- Audit Process tracking builder
- Group tracking builder
- Comment tracking builder
- Custom domain builder
- Custom table builder
- Custom query builder

- Report builder

- Group builder
- Alias builder
- Time period builder


My New Reports Administration Console System View **Tools**  Daily Monitor Guardium Monitor Tap Monitor Incident Management Standard Reports Monitor/Audit Comply Protect

Config & Control

Report Building

- Access Policy Tracking
- Access Tracking
- Aggregation/Archive Tracking
- Alert Tracking
- Application Tracking
- Audit Process Tracking
- Auto-discovery Tracking
- CAS Changes Tracking
- CAS Config Tracking
- CAS Host History Tracking
- CAS Templates Tracking
- Classifier Results Tracking
- Comments Tracking
- Custom DB Usage Tracking
- Custom Domain Builder
- Custom Query Builder
- Custom Table Builder
- Data Marts
- DB Default Users Enabled Tracking
- Discovered Instance Tracking
- Exceptions Tracking**
- Flat Log Tracking
- GIM Events Tracking
- Group Tracking
- Guardium Activity Tracking
- Guardium Login Tracking
- Installed Policy Tracking
- Policy Violations Summary Tracking
- Policy Violations Tracking
- Replay Results Tracking
- Report Builder

Exceptions Tracking

New Query - Overall Details 

Query Name Exceptions Report

Main Entity -- Select an Entity --

- Select an Entity --
- Client/Server
- Session
- Exception Type
- Database Error Text**
- Exception

My New Reports Administration Console System View Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management Standard Reports Monitor/Audit Comply Protect

Config & Control Report Building

- Access Policy Tracking
- Access Tracking
- Aggregation/Archive Tracking
- Alert Tracking
- Application Tracking
- Audit Process Tracking
- Auto-discovery Tracking
- CAS Changes Tracking
- CAS Config Tracking
- CAS Host History Tracking
- CAS Templates Tracking
- Classifier Results Tracking
- Comments Tracking
- Custom DB Usage Tracking
- Custom Domain Builder
- Custom Query Builder
- Custom Table Builder
- Data Marts
- DB Default Users Enabled Tracking
- Discovered Instance Tracking
- Exceptions Tracking
- Flat Log Tracking
- GIM Events Tracking
- Group Tracking
- Guardium Activity Tracking
- Guardium Login Tracking
- Installed Policy Tracking
- Policy Violations Summary Tracking
- Policy Violations Tracking
- Replay Results Tracking
- Report Builder
- Rogue Connections Tracking
- Security Assessment Result Tracking
- Sniffer Buffer Usage Tracking
- Step Statistics Tracking
- STAP/Z Files Tracking
- Unit Utilization Levels Tracking
- User/Role/Application Tracking

Exceptions Tracking

Exceptions Report ?

Main Entity: **Database Error Text** Add Count Add Distinct Sort by count

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend

Query Fields

Entity Agg. Attribute Operator Runtime Param.

Entity: 123 Source Address

Entity: 321 Destination Address

Entity: Destination Port

Entity: Session Id

Entity: Database Protocol

Entity: New TTL value

Entity: Exception Description

Entity: SQL string that caused the Exception

Entity: User Name

7AX5 Exception ID

Exception Type ID

Exception Timestamp

Exception Date

Exception Time

Exception WeekDay

Exception Year

Source Address

Source Port

Destination Address

Destination Port

Session Id

Database Protocol

New TTL value

Exception Description

SQL string that caused the Exception

User Name

Additional mode: AND OR HAVING

Delete Clone Roles... Save Back

Data Mart Generate Tabular Regenerate Add to Pane... Add to My New Reports

Exception Report – Recommended Report Definition

This report will show you the failures in descending time order. Beware of the “SESSION TIMEOUT” rows as they only indicate that an active session has not produced any new audit data (~ 60 minutes) and the Exception Timestamp value comes from the collector. If your collector’s time does not match the IBM i’s time, the resulting report can look confusing.

Exception Report definition:

Detailed Exception Report ?

Main Entity: Database Error Text
 Add Count
 Add Distinct
 Sort by count
 Run In Two Stages

Query Fields							
Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend	
<input type="checkbox"/>	1	Exception	Exception Timestamp	Value ▾	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	DB Protocol	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	3	Exception	DB2 i/z Database	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	4	Exception	DB2 i Current User	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	5	Exception	DB2 i/z Program	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	6	Client/Server	Network Protocol	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	7	Exception Type	Exception Type	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	8	Session	Process ID	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	9	Client/Server	Source Program	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	10	Database Error Text	Error Code	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	11	Exception	Exception Description	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	12	Database Error Text	Database Error Text	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	13	Exception	SQL string that caused the Exception	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	14	Client/Server	Client IP	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	15	Exception Type	Exception Description	Value ▾	<input type="checkbox"/>		

Exception Timestamp	DB Protocol	DB2 i/z Database	DB2 i Current User	DB2 i/z Program	Network Protocol	Exception Type	Process ID	Source Program	Error Code	Exception Description
2013-08-28 08:11:41.0	DB2 I	X1423P2	SCOTTFF	QSYS/QSQSAMPL	TOOLBOX.JDBC:07010009	SQL_ERROR	155558	QUSER/QZDASOINIT-601	42710:-601	
2013-08-28 08:11:41.0	DB2 I	X1423P2	SCOTTFF	QSYS/QSQSAMPL	TOOLBOX.JDBC:07010009	SQL_ERROR	155558	QUSER/QZDASOINIT-443	38I01:-443	
2013-08-28 06:01:30.0	DB2 I	LP13UT16	QQSMART	QSYS/QZSOSIGN	QAUDJRN	LOGIN_FAILED	726873	QUSER/QZSOSIGN	N/A	PW - Invalid password or user ID
2013-08-28 00:01:02.0	DB2 I	LP13UT16	QIJS	QIJS/QIJSC3AUT	QAUDJRN	SQL_ERROR	727895	QIJS/RMVHSTJS	-551	42501:-551
2013-08-28 00:01:02.0	DB2 I	LP13UT16	QIJS	QIJS/QIJSC3AUT	QAUDJRN	SQL_ERROR	727896	QIJS/RMVLOGEJS	-551	42501:-551

Database Error Text	SQL string that caused the Exception	Client IP	Exception Description
A duplicate object or constraint name was detected.	CREATE SCHEMA INDEXADVIC	9.10.110.20	Database Server returned an error
Error occurred while calling a user-defined function, procedure, or trigger (using the SIMPLE CALL or SIMPLE CALL WITH NULLS calling convention).	CALL QSYS.CREATE_SQL_SAMPLE(?)	9.10.110.20	Database Server returned an error
N/A		127.0.0.1	Login Failed
The authorization ID does not have the privilege to perform the specified operation on the identified object.	AF - Authority failure QUSRIJS QAIJSAUT *FILE	9.26.120.179	Database Server returned an error
The authorization ID does not have the privilege to perform the specified operation on the identified object.	AF - Authority failure QUSRIJS QAIJSAUT *FILE	9.26.120.179	Database Server returned an error

Entity List

- Client/Server
- Server
- IP/Server Port
- Session
- Access Period
- SQL
- FULL SQL
- FULL SQL
- Values
- Changed Data
- Value
- Application
- Events
- App User
- Name
- Command
- Object
- Object/Command
- Join
- Field
- Object/Field
- Qualified
- Object
- Field SQL
- Value

Object Tracking

Main Entity: **Object/Command**

Add Count
 Add Distinct
 Sort by count
 Run In Two Stages

Query Fields							
	Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Client/Server	Timestamp	Value ▾	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Client IP	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	3	Access Period	DB2 i/z Database	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	4	Access Period	DB2 i Current User	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	5	Command	SQL Verb	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	6	Object	Object Name	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	7	FULL SQL	Full Sql	Value ▾	<input type="checkbox"/>		
<input type="checkbox"/>	8	FULL SQL	Bind Variables Values	Value ▾	<input type="checkbox"/>		

AND
 OR
 HAVING

Query Conditions						
	Entity	Agg.	Attribute	Operator	Runtime Param.	
<input type="checkbox"/>	WHERE	FULL SQL	Full Sql	NOT LIKE	Value ▾	%GuardAppEvent%
<input type="checkbox"/>	AND	Access Period	DB2 i/z Database	LIKE	Parameter ▾	DB2iDatabase
<input type="checkbox"/>	AND	Client/Server	DB User Name	LIKE	Parameter ▾	DBUserName
<input type="checkbox"/>	AND	Command	SQL Verb	NOT LIKE	Value ▾	%CONNECT%

Drill Down Capability

Object Tracking

Start Date: **2013-08-25 09:41:16** End Date: **2013-08-28 09:41:16**
 Aliases: **OFF** DB2iDatabase: **LIKE %**
 DBUserName: **LIKE %LARKINB**

Timestamp	Client IP	DB2 i/z Database	DB2 i Current User	SQL Verb	Object Name	Full Sql	Bind Variables Values
2013-08-22 08:13:01.0	9.56.49.185X1423P2		LARKINB	DROP TABLE	empsal	drop table empsal	
2013-08-22 08:13:01.0	9.56.49.185X1423P2		LARKINB	CREATE TABLE	empsal	create table empsal (EMPNO CHAR(5), NAME CHAR(10), SALARY INT)	
2013-08-22 08:13:01.0	9.56.49.185X1423P2		LARKINB	INSERT	empsal	INSERT INTO EMPSAL VALUES (?, ?, ?)	'11111', 'WHITE', 95000
2013-08-22 08:13:01.0	9.56.49.185X1423P2		LARKINB	INSERT	empsal	INSERT INTO EMPSAL VALUES (?, ?, ?)	'22222', 'JONES', 82000
2013-08-22 08:13:01.0	9.56.49.185X1423P2		LARKINB	INSERT	empsal	INSERT INTO EMPSAL VALUES (?, ?, ?)	'33333', 'SMITH', 77000
2013-08-22 08:13:01.0	9.56.49.185X1423P2		LARKINB	INSERT	empsal	INSERT INTO EMPSAL VALUES (?, ?, ?)	'33333', 'SMITH', 77000
2013-08-22 08:13:01.0	9.56.49.185X1423P2		LARKINB	UPDATE	EMPSAL	UPDATE EMPSAL SET SALARY = ? WHERE EMPNO = ?	85000, '33333'
2013-08-22 08:13:01.0	9.56.49.185X1423P2		LARKINB	SELECT	empsal	SELECT * FROM EMPSAL	
2013-08-22 08:13:01.0	9.56.49.185X1423P2		LARKINB	SELECT	empsal	SELECT * FROM EMPSAL	
2013-08-22 08:13:01.0	9.56.49.185X1423P2		LARKINB	DELETE	EMPSAL	DELETE FROM EMPSAL WHERE EMPNO = ?	'33333'

Records 1 to 10 of 10

- Client IP Activity Summary
- Command Details
- Full SQL By Client IP
- Object Activity Summary
- Object Details
- Optim - Request Execution per Optim Server
- Optim - Request Execution per User
- Sensitive Objects List
- Add API Mapping

Enhancing Reports

Do we want to see all these records ?

-Activity Report							
Start Date: 2013-08-24 14:50:26		End Date: 2013-08-25 14:50:26					
Aliases: OFF		ClientIP: LIKE %					
DB2iDatabase: LIKE %		DBUserName: LIKE %					
Timestamp	Client IP	DB2 i/z Database	DB2 i/z Program	DB2 i Current User	Source Program	Full Sql	Bind Variables Values
2013-08-25 14:42:12.0	9.56.49.185X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB	LARKINB/QPADEV000R	INSERT INTO EMPNSAL VALUES (?, ?, ?)	'11111', 'WHITE', 95000
2013-08-25 14:42:12.0	9.56.49.185X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB	LARKINB/QPADEV000R	INSERT INTO EMPNSAL VALUES (?, ?, ?)	'22222', 'JONES', 82000
2013-08-25 14:42:12.0	9.56.49.185X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB	LARKINB/QPADEV000R	INSERT INTO EMPNSAL VALUES (?, ?, ?)	'33333', 'SMITH', 77000
2013-08-25 14:42:12.0	9.56.49.185X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB	LARKINB/QPADEV000R	INSERT INTO EMPNSAL VALUES (?, ?, ?)	'33333', 'SMITH', 77000
2013-08-25 14:40:25.0	9.56.49.185X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB	LARKINB/QPADEV000R	SELECT * FROM EMPNSAL	
2013-08-25 14:40:25.0	9.56.49.185X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB	LARKINB/QPADEV000R	SELECT * FROM EMPNSAL	
2013-08-25 14:40:21.0	9.56.49.185X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB	LARKINB/QPADEV000R	DELETE FROM EMPNSAL WHERE EMPNO = ?	'33333'
2013-08-25 14:37:41.0	9.56.49.185X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB	LARKINB/QPADEV000R	UPDATE EMPNSAL SET SALARY = ? WHERE EMPNO = ?	85000, '33333'
2013-08-25 14:12:39.0	9.56.49.185X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB	LARKINB/QPADEV000R	create table empnsal (EMPNO CHAR(5), NAME CHAR(10), SALARY INT)	
2013-08-25 14:03:00.0	9.56.49.185X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB	LARKINB/QPADEV000R	drop table empnsal	
2013-08-25 13:33:51.0	9.5.37.48	LP06UT16 QSYS/QS9UTIL	QSRVAGT	QSRVAGT	QSRVAGT/QS9PALMON	INSERT INTO QSRVAGT / QAS9AUDLOG (LOGDATA) VALUES (: H)	'13/08/25 12:11:51 QS9PALMON: running
2013-08-25 13:33:51.0	9.5.37.48	LP06UT16 QSYS/QS9UTIL	QSRVAGT	QSRVAGT	QSRVAGT/QS9PALMON	INSERT INTO QSRVAGT / QAS9AUDLOG (LOGDATA) VALUES (: H)	'13/08/25 12:11:51 QS9PALMON: ready for cycle
2013-08-25 13:33:51.0	9.56.49.185X1423P2	/	LARKINB	LARKINB	LARKINB/QPADEV000R	CONNECT	
2013-08-25 11:58:56.0	127.0.0.1	LP13UT16 QSYS/QCMD	DHQB	DHQB	DHQB/ANZDFTPWD2	CP - User Profile change	QSYS GDAUDIT2 *USRPRF
2013-08-25 11:58:56.0	127.0.0.1	LP13UT16 QSYS/QCMD	DHQB	DHQB	DHQB/ANZDFTPWD2	CP - User Profile change	QSYS GRPVISUAL *USRPRF
2013-08-25 11:58:56.0	127.0.0.1	LP13UT16 QSYS/QCMD	DHQB	DHQB	DHQB/ANZDFTPWD2	CP - User Profile change	QSYS IT_DATA *USRPRF
2013-08-25 11:58:56.0	127.0.0.1	LP13UT16 QSYS/QCMD	DHQB	DHQB	DHQB/ANZDFTPWD2	CP - User Profile change	QSYS IT_SEC *USRPRF
2013-08-25 11:58:56.0	127.0.0.1	LP13UT16 QSYS/QCMD	DHQB	DHQB	DHQB/ANZDFTPWD2	CP - User Profile change	QSYS ITGRP *USRPRF
2013-08-25 11:58:56.0	127.0.0.1	LP13UT16 QSYS/QCMD	DHQB	DHQB	DHQB/ANZDFTPWD2	CP - User Profile change	QSYS ITSEC *USRPRF
2013-08-25 11:58:56.0	127.0.0.1	LP13UT16 QSYS/QCMD	DHQB	DHQB	DHQB/ANZDFTPWD2	CP - User Profile change	QSYS PERFTEAM *USRPRF

Filter on database X1423P2

-Activity Report							
Start Date: 2013-08-24 14:49:06		End Date: 2013-08-25 14:49:06					
Aliases: OFF		ClientIP: LIKE %					
DB2iDatabase: LIKE %X1423P2		DBUserName: LIKE %					
Timestamp	Client IP	DB2 i/z Database	DB2 i/z Program	DB2 i Current User	Source Program	Full Sql	Bind Variables Values
2013-08-25 14:42:12.0	9.56.49.185	X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	INSERT INTO EMPALS VALUES (?, ?, ?)	'11111', 'WHITE', 95000
2013-08-25 14:42:12.0	9.56.49.185	X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	INSERT INTO EMPALS VALUES (?, ?, ?)	'22222', 'JONES', 82000
2013-08-25 14:42:12.0	9.56.49.185	X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	INSERT INTO EMPALS VALUES (?, ?, ?)	'33333', 'SMITH', 77000
2013-08-25 14:42:12.0	9.56.49.185	X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	INSERT INTO EMPALS VALUES (?, ?, ?)	'33333', 'SMITH', 77000
2013-08-25 14:40:25.0	9.56.49.185	X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	SELECT * FROM EMPALS	
2013-08-25 14:40:25.0	9.56.49.185	X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	SELECT * FROM EMPALS	
2013-08-25 14:40:21.0	9.56.49.185	X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	DELETE FROM EMPALS WHERE EMPNO = ?	'33333'
2013-08-25 14:37:41.0	9.56.49.185	X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	UPDATE EMPALS SET SALARY = ? WHERE EMPNO = ?	85000, '33333'
2013-08-25 14:12:39.0	9.56.49.185	X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	create table empals (EMPNO CHAR(5), NAME CHAR(10), SALARY INT)	
2013-08-25 14:03:00.0	9.56.49.185	X1423P2	QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	drop table empals	
2013-08-25 13:33:51.0	9.56.49.185	X1423P2	/	LARKINB	LARKINB/QPADEV000R	CONNECT	
2013-08-25 08:13:41.0	9.5.50.69	X1423P2	MJBNQEAPIP/NQECANAPI2	C2USER	C2SECOFR/\$AUDNQEAPI	AF - Authority failure	MJBNQEAPI TESTTBL *FILE
2013-08-25 08:13:41.0	9.5.50.69	X1423P2	MJBNQEAPIP/NQECANAPI2	C2USER	C2SECOFR/\$AUDNQEAPI	AF - Authority failure	MJBNQEAPI TESTTBL *FILE
2013-08-25 08:13:41.0	9.5.50.69	X1423P2	MJBNQEAPIP/NQECANAPI2	C2USER	C2SECOFR/\$AUDNQEAPI	AF - Authority failure	MJBNQEAPI TESTTBL *FILE
2013-08-25 08:13:41.0	9.5.50.69	X1423P2	MJBNQEAPIP/NQECANAPI2	C2USER	C2SECOFR/\$AUDNQEAPI	AF - Authority failure	MJBNQEAPI TESTTBL *FILE
2013-08-25 08:13:41.0	9.5.50.69	X1423P2	QSYS/QSECCHSA	C2SECOFR	C2SECOFR/\$AUDNQEAPI	SV - System value change	QAUDCTL NEW VALUE: *NONE OLD VALUE: *NONE
2013-08-25 08:13:41.0	9.5.50.69	X1423P2	QSYS/QSECCHSA	C2SECOFR	C2SECOFR/\$AUDNQEAPI	SV - System value change	QAUDCTL NEW VALUE: *NONE OLD VALUE: *NONE
2013-08-25 08:13:41.0	9.5.50.69	X1423P2	QSYS/QSECCHSA	C2SECOFR	C2SECOFR/\$AUDNQEAPI	SV - System value change	QAUDCTL NEW VALUE: *NONE OLD VALUE: *NONE
2013-08-25 08:13:41.0	9.5.50.69	X1423P2	QSYS/QSECCHSA	C2SECOFR	C2SECOFR/\$AUDNQEAPI	SV - System value change	QAUDCTL NEW VALUE: *NONE OLD VALUE: *NONE
2013-08-25 08:13:41.0	9.5.50.69	X1423P2	QSYS/QSECCHSA	C2SECOFR	C2SECOFR/\$AUDNQEAPI	SV - System value change	QAUDCTL NEW VALUE: *NONE OLD VALUE: *NONE



-Activity Report

Start Date: **2013-08-24 14:50:02** End Date: **2013-08-25 14:50:02**
 Aliases: **OFF** ClientIP: **LIKE %**
 DB2iDatabase: **LIKE %X1423P2** DBUserName: **LIKE %LARKINB**

Timestamp	Client IP	DB2 i/z Database	DB2 i/z Program	DB2 i Current User	Source Program	Full Sql	Bind Variables Values
2013-08-25 14:42:12.09.56.49.185X1423P2			QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	INSERT INTO EMPSPAL VALUES (?, ?, ?)	'11111', 'WHITE', 95000
2013-08-25 14:42:12.09.56.49.185X1423P2			QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	INSERT INTO EMPSPAL VALUES (?, ?, ?)	'22222', 'JONES', 82000
2013-08-25 14:42:12.09.56.49.185X1423P2			QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	INSERT INTO EMPSPAL VALUES (?, ?, ?)	'33333', 'SMITH', 77000
2013-08-25 14:42:12.09.56.49.185X1423P2			QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	INSERT INTO EMPSPAL VALUES (?, ?, ?)	'33333', 'SMITH', 77000
2013-08-25 14:40:25.09.56.49.185X1423P2			QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	SELECT * FROM EMPSPAL	
2013-08-25 14:40:25.09.56.49.185X1423P2			QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	SELECT * FROM EMPSPAL	
2013-08-25 14:40:21.09.56.49.185X1423P2			QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	DELETE FROM EMPSPAL WHERE EMPNO = ?	'33333'
2013-08-25 14:37:41.09.56.49.185X1423P2			QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	UPDATE EMPSPAL SET SALARY = ? WHERE EMPNO = ?	85000, '33333'
2013-08-25 14:12:39.09.56.49.185X1423P2			QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	create table empstal (EMPNO CHAR(5), NAME CHAR(10), SALARY INT)	
2013-08-25 14:03:00.09.56.49.185X1423P2			QSQL/QSQIMAIN	LARKINB	LARKINB/QPADEV000R	drop table empstal	
2013-08-25 13:33:51.09.56.49.185X1423P2			/	LARKINB	LARKINB/QPADEV000R	CONNECT	

Records 1 to 11 of 11

Customize Portlet

Report: **-Activity Report** Based on Query: **-Activity Report**

Title: -Activity Report

Run Time Parameters

ClientIP: LIKE %LARKINB

DB2iDatabase: LIKE %X1423P2

DBUserName: LIKE %

QUERY_FROM_DATE: >= NOW -1 DAY

QUERY_TO_DATE: <= NOW

REMOTE_SOURCE: -- none --

SHOW_ALIASES: On Off Default

Presentation Parameters

fetchSize: 20

Max. records per page

Monitoring istap

-Activity Report

Start Date: 2012-08-23 08:13:14 End Date: 2012-08-23 14:13:14

Aliases: OFF ClientIP: LIKE %

DBUsername: LIKE %LARKINB NetProt: LIKE %

SQL: LIKE % ServerIP: LIKE %

ServerType: LIKE %

Timestamp	Server Type	Server IP	Client IP	Network Protocol	DB User Name	Sql
2012-08-23 10:55:22.0DB2		9.30.174.989.56.117.164	QAUDJRN	LARKINB	select EXTRUSION_RULE from sysDummy	
2012-08-23 10:55:22.0DB2		9.30.174.989.56.117.164	QAUDJRN	LARKINB	select KBYTE_COUNT from SESSION_COUNTERS	
2012-08-23 10:55:22.0DB2		9.30.174.989.56.117.164	QAUDJRN	LARKINB	CO - Create object QGPL TSETEST *FILE	

Records 1 to 3 of 3

Api Call Output get_istap_status

Call Output

ID=0

Status time: 2012-08-23 11:50:19.939887

Server started: NO

Start time: 2012-08-11 00:01:49.470323

Server job name: QBATCH MJA 038571

Jobs processed sql: 40

Sql processed: 176

Sql enqueued: 168

Sql skipped: 0

Sql whose variable values processed: 2

Sql whose variable values discarded: 0

Processed journal audit entries: 35984

Enqueued journal audit entries: 58

Queue damaged: NO

Num of messages on queue: 0

Size of messages on queue: 0

Maximum size of queue: 16777216

Total enqueue threads: 0

Last dequeue time: 2012-08-23 18:50:19.37

Last enqueue time: 2012-08-23 18:50:19.37

Queue owner: MJA

Close

Api Call Output start_istap_monitor

Call Output

ID=0

Api Call Output get_istap_status

Call Output

ID=0

Status time: 2012-08-23 12:03:09.332259

Server started: YES

Start time: 2012-08-23 11:51:37.739863

Server job name: QBATCH MJA 039768

Jobs processed sql: 13

Sql processed: 51

Sql enqueued: 40

Sql skipped: 0

Sql whose variable values processed: 8

Sql whose variable values discarded: 0

Processed journal audit entries: 23

Enqueued journal audit entries: 6

Queue damaged: NO

Num of messages on queue: 0

Size of messages on queue: 0

Maximum size of queue: 16777216

Total enqueue threads: 0

Last dequeue time: 2012-08-23 19:03:09.168

Last enqueue time: 2012-08-23 19:03:09.168

Queue owner: MJA

Close

What we'll cover today

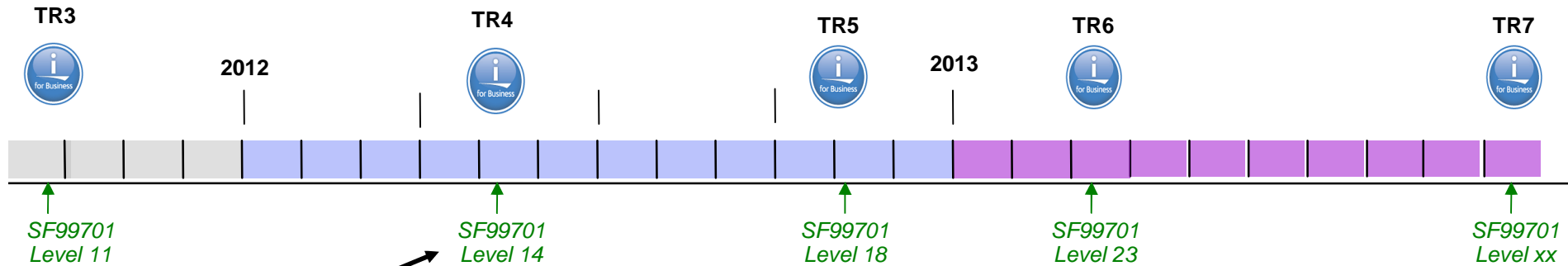


- 30K-foot overview of InfoSphere Guardium and IBM I
- An integrated solution for audit and compliance
- Monitoring strategy and use cases
- Step by step – getting started
- **FAQ and conclusion**



DB2 for i – Enhancements delivered via DB2 PTF Groups

IBM i 7.1



TR4 timed Enhancements:

- XMLTable
- RUNSQL command
- Performance enhancements for large numbers of row locks
- Automatic management of SQL Plan Cache size
- Many Others...

TR5 timed Enhancements:

- Named and Default Parameters for Procedures
- **InfoSphere Guardium V9.0 – DB2 for i**
- SQE enhancement for Encoded Vector Indexes defined with INCLUDE
- Many Others...

TR6 timed Enhancements:

- HTTP functions
- Database Reorganization (User specified starting point)
- Tracking System Limits (Phase 1)
- Many Others...

TR7 timed Enhancements:

- Coming later in 2013

Future Plans are subject to change

Enhancements delivered by PTF are documented here:

www.ibm.com/developerworks/ibmi/techupdates/db2

DB2 for i – Enhancements delivered by DB2 PTF Groups

- The developerWorks IBM i Technology Updates wiki includes the schedule, status and enhancement breakdown.
www.ibm.com/developerworks/ibmi/techupdates/db2/groupptf
- Stay current and you'll be rewarded

The Guardium on IBM i fact page (<http://bit.ly/GuardiumOni>) is the single, best place to look to understand the service level requirements.

♦ **The recommended service level is:**

Release 6.1 SF99601 Level 30 (or higher)

On IBM i 6.1, additional PTFs to install: PTF 5761SS1 SI50446, SI50447, SI50578, SI50580 & SI50582

Release 7.1 SF99701 Level 25 (or higher)

On IBM i 7.1, additional PTFs to install: PTF 5770SS1 SI50438, SI50439, SI50579, SI50581 & SI50583

Closing thoughts

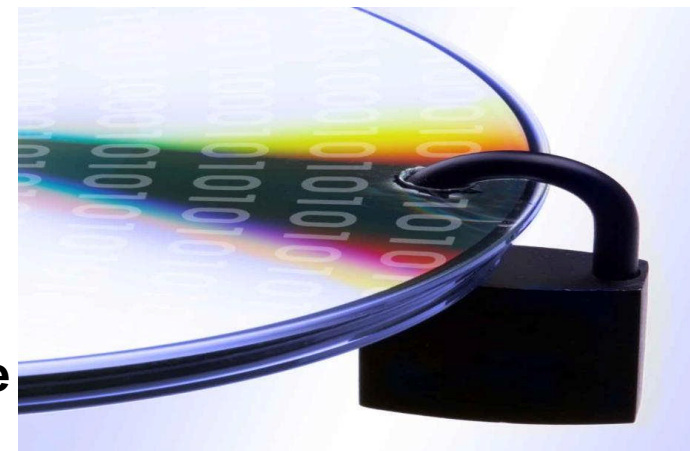


It's critical to secure high value data and validate compliance

Traditional log management, SIEM and DLP solutions are only part of the solution

InfoSphere Guardium is the most widely-deployed solution, with ongoing feedback from the most demanding data center environments worldwide

- **Scalable enterprise architecture**
- **Broad heterogeneous support**
- **Complete visibility and granular control**
- **Deep automation to reduce workload and total cost of operations**
- **Holistic approach to security and compliance**



Information, training, and community

- [DB2 for i and Guardium serviceability guide](#) (You must have this!)
- [DB2 for i and Guardium developerWorks article](#) (aka ‘the white paper’)
- [InfoSphere Guardium Tech Talks](#) – at least one per month. Suggestions welcome!
- [InfoSphere Guardium YouTube Channel](#) – includes overviews, technical demos, tech talk replays
- [InfoSphere Guardium newsletter](#)
- [developerWorks forum](#) (very active)
- [Guardium DAM User Group on Linked-In](#) (very active)
- [Community on developerWorks](#) (includes discussion forum, content and links to a myriad of sources, developerWorks articles, tech talk materials and schedules)
- [Guardium Info Center](#) (Installation, System Z S-TAPs, how-tos, more to come)
- [Technical training courses](#) (classroom and self-paced)



InfoSphere Guardium Virtual User Group.
Open, technical discussions with other users.
Not recorded!
Send a note to bamealm@us.ibm.com if
interested.

Reminder: Guardium Tech Talks

Next tech talk: How to audit and protect SAP systems with InfoSphere Guardium Data Activity Monitor

Speakers: Joe Dipietro

Date & Time: Thursday, September 19, 2013

11:30 AM Eastern (1 hour)

Register here: <http://bit.ly/15BqkTq>

- Link to more information about this and upcoming tech talks can be found on the InfoSphere Guardium developerWorks community: <http://ibm.co/Wh9x0o>
- Please submit a comment on this page for ideas for tech talk topics.

धन्यवाद
Hindi

多謝
Traditional Chinese

Dziękuję
Polish

ขอบพระคุณ
Thai

Gracias
Spanish



Merci
French

Спасибо
Russian

شكراً
Arabic

Obrigado
Brazilian Portuguese

Danke
German

多谢
Simplified Chinese

Tack
Swedish

நன்றி
Tamil

ありがとうございました
Japanese

Grazie
Italian

Backup

My New Reports Administration Console System View Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management Standard Reports Monitor/Audit Comply Protect

Security Policies Correlation Alerts Incident Management

Data Access Policy Application

Not Server IP / and/or Group
 Not Client IP / and/or Group
 Not Client MAC
 Net Prtol. and/or Group
 DB Type
 Not Svc. Name and/or Group
 Not DB Name and/or Group
 Not DB User LARKINB and/or Group
 Not Client IP/Src App./DB User/Server IP/Svc. Name
 Not App. User and/or Group
 Not OS User and/or Group
 Not Src App. and/or Group
 Not Field and/or Group Every
 Not Object and/or Group Every
 Not Command and/or Group (Public) DB2 Delete/Update Every
 Not Object/Cmd. Group
 Not Object/Field Group
 Pattern RE
 XML Pattern RE
 App Event Exists Event Type Event User Name
 App Event Values Text and/or Group
 Numeric Date
 Masking Pattern RE Replacement Character
 Time Period
 Minimum Count 0 Reset Interval 0 minutes Trigger Once Per Session
 Quarantine for 0 minutes Records Affected Threshold 0 Rec. Vals. Cont. to next rule

Actions

Add New Action

Action

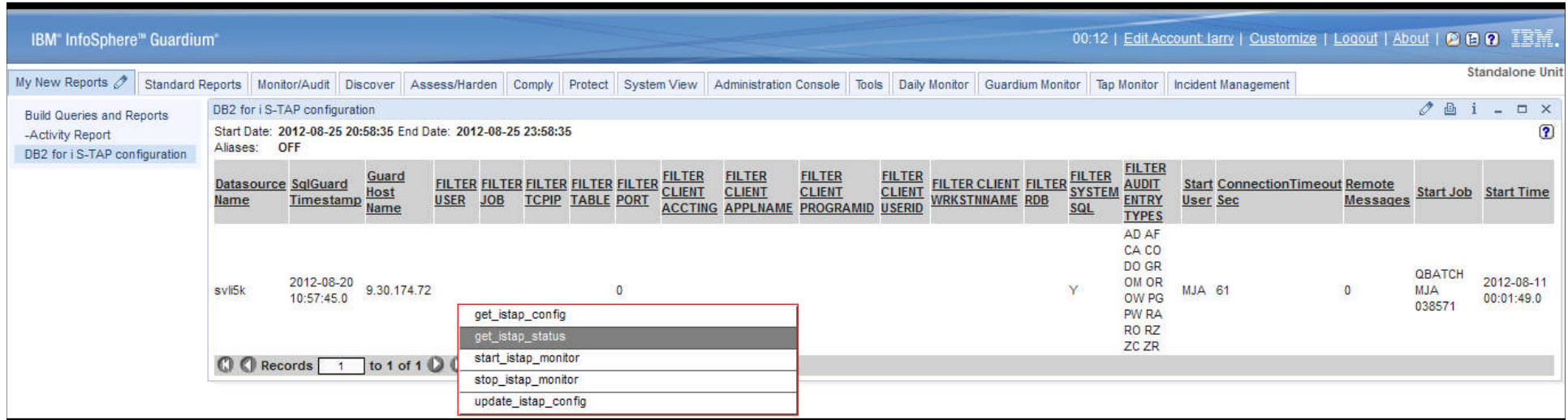
- ALERT DAILY
- ALERT ONCE PER SESSION
- ALERT ONLY
- ALERT PER MATCH**
- ALERT PER TIME GRANULARITY
- ALLOW
- Do Not RECORD VALUES SEPARATELY
- IGNORE RESPONSES PER SESSION
- IGNORE S-TAP SESSION
- IGNORE SESSION
- IGNORE SQL PER SESSION
- LOG FULL DETAILS
- LOG FULL DETAILS PER SESSION
- LOG MASKED DETAILS
- LOG ONLY
- MARK AS AUTO-COMMIT OFF
- MARK AS AUTO-COMMIT ON
- NO PARSE
- QUARANTINE
- QUICK PARSE
- QUICK PARSE NATIVE
- QUICK PARSE NO FIELDS
- RECORD VALUES SEPARATELY
- S-GATE ATTACH
- S-GATE DETACH
- S-GATE TERMINATE
- S-TAP TERMINATE
- SKIP LOGGING


Guardium community on developerWorks

Bit.ly/guardwiki

The screenshot shows the InfoSphere Guardium community page on developerWorks. At the top, there's a navigation bar with 'Technical topics', 'Evaluation software', 'Community', and 'Events'. Below that, the 'Communities' section is active, showing 'InfoSphere Guardium'. A green notification box states: 'We have upgraded the developerWorks community applications to the latest version of IBM Connections. Get a glimpse of the improvements!'. The 'Community Description' section explains that the community is for users, developers, and partners to share information about using IBM InfoSphere Guardium. The 'Forums' section lists several topics, including 'Submitting product enhancement requests - new automated system' and 'Tech Talk on June 20: Planning a successful Guardium deployment'. On the left, there's a circular diagram with four quadrants: 'Monitor & Enforce', 'Audit & Report', 'Find & Classify', and 'Assess & Harden', with 'Critical Data Infrastructure' in the center. The right sidebar contains 'Important Bookmarks', 'Members' (with 35 people), and 'Related bookmarks'.

get_istap_status Api function



IBM InfoSphere™ Guardium™ 00:12 | Edit Account: larry | Customize | Logout | About |  IBM

My New Reports | Standard Reports | Monitor/Audit | Discover | Assess/Harden | Comply | Protect | System View | Administration Console | Tools | Daily Monitor | Guardium Monitor | Tap Monitor | Incident Management | Standalone Unit

Build Queries and Reports
-Activity Report
DB2 for i S-TAP configuration

DB2 for i S-TAP configuration
Start Date: 2012-08-25 20:58:35 End Date: 2012-08-25 23:58:35
Aliases: OFF

Datasource Name	SqlGuard Timestamp	Guard Host Name	FILTER USER	FILTER JOB	FILTER TCPIP	FILTER TABLE	FILTER PORT	FILTER CLIENT ACCTING	FILTER CLIENT APPLNAME	FILTER CLIENT PROGRAMID	FILTER CLIENT USERID	FILTER CLIENT WRKSTNNAME	FILTER RDB	FILTER SYSTEM SQL	FILTER AUDIT ENTRY TYPES	Start User	ConnectionTimeout Sec	Remote Messages	Start Job	Start Time
svl5k	2012-08-20 10:57:45.0	9.30.174.72					0							Y	AD AF CA CO DO GR OM OR OW PG PW RA RO RZ ZC ZR	MJA 61		0	QBATCH MJA 038571	2012-08-11 00:01:49.0

Records 1 to 1 of 1

- get_istap_config
- get_istap_status**
- start_istap_monitor
- stop_istap_monitor
- update_istap_config

Api Call Output get_istap_status

Call Output

```

ID=0
Status time: 2012-08-26 00:22:09.983872
Server started: YES
Start time: 2012-08-23 11:51:37.739863
Server job name: QBATCH MJA 039768
Jobs processed sql: 116
Sql processed: 650
Sql enqueued: 555
Sql skipped: 0
Sql whose variable values processed: 28
Sql whose variable values discarded: 0
Processed journal audit entries: 7282
Enqueued journal audit entries: 17
Queue damaged: NO
Num of messages on queue: 0
Size of messages on queue: 0
Maximum size of queue: 16777216
Total enqueue threads: 0
Last dequeue time: 2012-08-26 07:22:09.811
Last enqueue time: 2012-08-26 07:22:09.811
Queue owner: MJA
    
```

[Close](#)

Guardium community-Tech Talk wiki page

You are in: [InfoSphere Guardium Community](#) > [InfoSphere Guardium Wiki](#) > [Guardium Tech Talks](#)

Guardium Tech Talks

| Updated 6/24/13 by KRZ | Tags:

- [guardium](#),
- [webcast](#)

[Page Actions](#) ▾

Guardium Tech Talks



No budget for education or conference travel this year? Do you want the opportunity to interact with product experts from the labs? Join us for a series of low key, informal tech talks about Guardium data activity monitoring. Speakers will include product management, support rep, development and QA, and lab services.

These talks will include both deeply technical talks for more experienced users as well as “101” sessions to provide the opportunity for those new to the offering to get up to speed and have an environment where their questions can be answered.

The sessions will be recorded.

If you have additional questions, or have ideas for tech talks you’d like to see, send an email to [krzeide at us.ibm.com](mailto:krzeide@us.ibm.com) or add a comment to this page.

- [Upcoming tech talks](#)
- [Previous tech talks and recordings](#)

Upcoming Tech Talks

July 16 Tech Talk: Planning an InfoSphere Guardium deployment, Part 2: Monitoring setup and guidelines

11:30 AM Eastern Daylight, 8:30 AM Pacific Daylight

Speakers: Boaz Barkai InfoSphere Guardium WW Practice Lead and Yosef Rozenblit, InfoSphere Guardium WW Services Lead

We can all use a little advice from those who have gone before. If you are planning a new deployment of InfoSphere Guardium or are expanding an existing one, Our speakers have years of experience in guiding customer deployments, and in this talk they will provide a blueprint to help you plan for a deployment. They will also offer advice on how to manage the environment post-deployment. You'll learn:

- What architecture options need to be considered
- What team members need to be involved
- What IT infrastructure requirements to consider
- What business requirements and drivers need to be understood

Guardium community – Quick Reference

Bit.ly/guardwiki

You are in: [InfoSphere Guardium Community](#) > [InfoSphere Guardium Wiki](#) > Quick Reference

Quick Reference

| Updated 5/8/13 by KRZ | Tags: None

Page Actions ▾

Quick Reference

- [InfoSphere Guardium Data Security product web page](#)
- [System requirements and supported data sources](#)
 - [8.2](#)
 - [9.0](#)
- [Software appliance technical requirements \(V9\)](#)
- [V9 Sizing portal](#)
- [Upgrading from 8.2 to 9.0](#)
- [Announcement dates and lifecycle information](#)
- [Product support portal](#)
- [Articles and videos](#)
- [Tech Talk schedule and recordings](#)
- [Customer case studies](#)
- [Information Center \(product documentation\)](#)
- **Important:** Not all product information is available in the online Information Center. It includes installation, some "how tos" and the S-TAP information for the System z S-TAPS. The rest of the product information is available in the online help book.
- [Education and training \(classes\)](#)
- [Submitting product enhancement requests](#)

Filtering Which Data to Capture

There are several places where audit data is filtered:

- Normal auditing controls filter what data goes into QSYS/QAUDJRN
 - Filtering only specific Journal Entry Types can be configured
 - Only certain journal entry types are processed and sent to Guardium
 - Only certain attributes of the journal entries are processed and sent to Guardium
- The database monitor can filter data
 - The same filtering available on STRDBMON can be configured
 - Only certain monitor entries are processed and sent to Guardium
 - Only certain attributes of the monitor entries are captured and sent to Guardium
- The Guardium collector can perform additional filtering via Policies.
For example:
 - Only capture security failures
 - Only capture failures for certain users or objects
 - Etc. Etc. Etc.

Attribute filtering

Audit Data	SQL Monitor	Audit Journal
Job name	Yes	Yes
Job user	Yes	Yes
Job number	Yes	Yes
Start time	Yes	Yes
End time	Yes	Always the same as the Start time
SQLSTATE	Yes	08001 for invalid password (PW) and audit records (GR) 42501 for authority failure (AF) 00000 everything else
SQLCODE	Yes	-30080 for invalid password (PW) and audit records (GR) -551 for authority failure. (AF) 0 everything else
SQL statement	Yes – limited to 60K	No - basic journal entry description instead
SQL variables	Yes - limited to 1000 bytes	No
Interface	Yes	Always QAUDJRN
Client application name	Yes,	No
Client user ID	Yes	No
Client workstation	Yes	No
Client accounting	Yes	No
Client program	Yes	No
Current user	Yes	Yes
Thread ID	Yes	Yes
Program schema	Yes, if the statement is executed from a PGM or SRVPGM	Yes, if the statement is executed from a PGM or SRVPGM
Program name	Yes, if the statement is executed from a PGM or SRVPGM	Yes, if the statement is executed from a PGM or SRVPGM
Client IP Address	Yes	Yes
Local or server port number	Yes	Yes
RDB name	Yes	Yes
Number of rows	Yes, only for INSERT, DELETE, UPDATE, MERGE, OPEN*, VALUES INTO, CREATE TABLE AS, DECLARE GLOBAL TEMPORARY TABLE AS and SET VARIARI F	No

Audit Server Status information

STATUS_TIME	Timestamp of this request for status
SERVER_STARTED	Indicates whether the server is currently started or not (YES or NO)
START_TIME	Timestamp of the last time the server was started
SERVER_JOB	Job name of the server
NUMBER_JOBS_AUDITED_USING_SQL	Number of jobs that have processed an SQL statements since the server was started
NUMBER_PROCESSED_SQL_STATEMENTS	Number of SQL statements that have been processed since the server was started. This does not include SQL statements filtered out by STRDBMON
NUMBER_ENQUEUED_SQL_STATEMENTS	Number of SQL statements that have been enqueued since the server was started. This does not include SQL statements filtered out.
NUMBER_SKIPPED_SQL_STATEMENTS	Each job will attempt to put an SQL statement on the queue up to three times. This indicates that some number of SQL statements could not be audited. Rare...typically indicates a queue problem.
NUMBER_PROCESSED_VARIABLE_SETS	Number of SQL statements that have variables since the server was started. Some SQL statements have variables and some not. This does not include SQL statements filtered out.
NUMBER_SKIPPED_VARIABLE_SETS	Number of SQL statements whose variable values were discarded. Since the variable values are written to the monitor PRIOR to the actual SQL statement, It is possible that several sets of variables will have to be saved until the SQL statement shows up. Up to 300 sets of variables are saved so this is extremely unlikely.
NUMBER_PROCESSED_QAUDJRN_ENTRIES	Number of journal audit entries that have been processed since the server was started. This does not include audit entries filtered out.
NUMBER_ENQUEUED_QAUDJRN_ENTRIES	Number of journal audit entries that have been enqueued since the server was started. This does not include entries filtered out.
QUEUE_DAMAGED	Indicates whether or not the queue is damaged. (YES or NO)
NUMBER_MESSAGES_ON_QUEUE	Number of messages currently on the queue
SIZE_OF_MESSAGES_ON_QUEUE	Size of the queue
MAXIMUM_SIZE_OF_QUEUE	Maximum size of the queue (this is always 16 meg)
116 TOTAL_ENQUEUING_THREADS	Total number of threads enqueueing messages

Command Tracking (Command Main Entity)

Entity List

- Client/Server
- Server IP/Server
- Port
- Session
- Access Period
- SQL
- FULL SQL
- FULL SQL Values
- Changed Data Value
- Application Events
- App User Name
- Command
- Object
- Object/Command
- Join
- Field
- Object/Field
- Qualified Object

Command Tracking

Main Entity: **Command** Add Count Add Distinct Sort by count Run In Two Stages

Query Fields						
Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Client/Server	Timestamp	Value	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Client IP	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	3	Access Period	DB2 i/z Database	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	4	Access Period	DB2 i Current User	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	5	Command	SQL Verb	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	6	FULL SQL	Full Sql	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	7	FULL SQL	Bind Variables Values	Value	<input type="checkbox"/>	<input type="checkbox"/>

Addition mode: AND OR HAVING

Query Conditions						
	Entity	Agg.	Attribute	Operator	Runtime Param.	
<input type="checkbox"/>	WHERE	FULL SQL	Full Sql	NOT LIKE	Value	%GuardAppEvent%
<input type="checkbox"/>	AND	Access Period	DB2 i/z Database	LIKE	Parameter	DB2iDatabase
<input type="checkbox"/>	AND	Client/Server	DB User Name	LIKE	Parameter	DBUsername
<input type="checkbox"/>	AND	Command	SQL Verb	NOT LIKE	Value	%CONNECT%

Command Tracking						
Start Date:	2013-08-23 19:41:03	End Date:	2013-08-25 20:41:03			
Aliases:	OFF	DB2iDatabase:	LIKE %X1423P2			
DBUsername:	LIKE %LARKINB					
Timestamp	Client IP	DB2 i/z Database	DB2 i Current User	SQL Verb	Full Sql	Bind Variables Values
2013-08-22 08:13:01.09.56.49.185X1423P2			LARKINB	SELECT	select * from empsal	
2013-08-22 08:13:01.09.56.49.185X1423P2			LARKINB	SELECT	select * from empsal	
2013-08-22 08:13:01.09.56.49.185X1423P2			LARKINB	DROP TABLE	drop table empsal	
2013-08-22 08:13:01.09.56.49.185X1423P2			LARKINB	CREATE TABLE	create table empsal (EMPNO CHAR(5), NAME CHAR(10), SALARY INT)	
2013-08-22 08:13:01.09.56.49.185X1423P2			LARKINB	INSERT	INSERT INTO EMPSAL VALUES (?, ?, ?)	'11111', 'WHITE', 95000
2013-08-22 08:13:01.09.56.49.185X1423P2			LARKINB	INSERT	INSERT INTO EMPSAL VALUES (?, ?, ?)	'22222', 'JONES', 82000
2013-08-22 08:13:01.09.56.49.185X1423P2			LARKINB	INSERT	INSERT INTO EMPSAL VALUES (?, ?, ?)	'33333', 'SMITH', 77000
2013-08-22 08:13:01.09.56.49.185X1423P2			LARKINB	INSERT	INSERT INTO EMPSAL VALUES (?, ?, ?)	'33333', 'SMITH', 77000
2013-08-22 08:13:01.09.56.49.185X1423P2			LARKINB	UPDATE	UPDATE EMPSAL SET SALARY = ? WHERE EMPNO = ?	85000, '33333'
2013-08-22 08:13:01.09.56.49.185X1423P2			LARKINB	SELECT	SELECT * FROM EMPSAL	
2013-08-22 08:13:01.09.56.49.185X1423P2			LARKINB	SELECT	SELECT * FROM EMPSAL	
2013-08-22 08:13:01.09.56.49.185X1423P2			LARKINB	DELETE	DELETE FROM EMPSAL WHERE EMPNO = ?	'33333'

Records 1 to 12 of 12

Object Tracking (Object Main Entity)

Drill Down Capability – What Table Are You Interested In?

IBM® InfoSphere™ Guardium®

Client IP	Source Program	SQL Verb	Depth	Object Name	Total access
10.10.10.10	DISP+WORK.EXE	INSERT	0	TUCON	48
10.10.10.10	DISP+WORK.EXE	SELECT	0	T_01	1458
10.10.10.10	DISP+WORK.EXE	INSERT	0	UCMP000	4
10.10.10.10	DISP+WORK.EXE	SELECT	0	URL_EXITS	1
10.10.10.10	DISP+WORK.EXE	SET CLIENT APPLNAME	0	US01	2
10.10.10.10	DISP+WORK.EXE	SELECT	0	USERS_SSM	6
10.10.10.10	DISP+WORK.EXE	SELECT	0	USGRP_USER	4
10.10.10.10	DISP+WORK.EXE	INSERT	0	USH02	5
10.10.10.10	DISP+WORK.EXE	SELECT	0	USH02	6
10.10.10.10	DISP+WORK.EXE	UPDATE	0	USH02	4
10.10.10.10	DISP+WORK.EXE	SELECT	0	USOBX_C	21
10.10.10.10	DISP+WORK.EXE	SELECT	0	USR01	2
10.10.10.10	DISP+WORK.EXE	UPDATE	0	USR01	5
10.10.10.10	DISP+WORK.EXE	INSERT	0	USR01	2
10.10.10.10	DISP+WORK.EXE	UPDATE	0	USR02	9
10.10.10.10	DISP+WORK.EXE	SELECT	0	USR02	24
10.10.10.10	DISP+WORK.EXE	INSERT	0	USR02	1
10.10.10.10	DISP+WORK.EXE	SELECT	0	USR04	104
10.10.10.10	DISP+WORK.EXE	INSERT	0	USR04	1
10.10.10.10	DISP+WORK.EXE	SELECT	0	USR05	6

- Client IP Activity Summary
- Command Details
- Full SQL By Client IP
- Object Activity Summary
- Object Details
- Sensitive Objects List
- Alias Definition
- Show SQL
- Show SQL with Values

```

SQL String
INSERT INTO "USR04" VALUES( '000' , 'JOE' , '20100922' , '171641' , 'DDIC' , 2 , 'C' ) -- OPTLEVEL( 5 ) -- QUERY_DEGREE( 1 ) -- LOCATION( SAPLSUU2 , 1292 ) -- SYSTEM( E6A , SAPE6A )
    
```