

Tips and Tricks...

Joe DiPietro
Joe_DiPietro@us.ibm.com



Agenda

Operations

- What CLI commands are available?
 - Comm <string>
- GRDAPI – Datasource
- UID Chain
- Review 9.0/8.2 Release Highlights
- Enterprise reports
- Silent Installs*
- LDAP/Active directory integration
- SGATE vs STAP Terminate
- Global Profile – SIEM integration
- Change Management Reconciliation
- The GIM client can now be installed using Tivoli Provisioning Manager (TPM) as of 8.2

GIM Details

- "Discovery Agent"
- "CAS"

Helping DBA's get more visibility:

- Long running queries
- Active user last login
- Active User with No Activity
- Failed User login attempts
- SQL Errors

Reporting

- Difference reports
- Customize change management
- Customize and drill down report
- Application User Identification
- VA Tests
 - Text Exceptions
- Guardium Grid
- Dormant Accounts
 - Oracle Dormant User Report
- Linking Guardium Reporting Domain

CLI Commands

Show me all the commands that have the following string

tlab> **comm** policy

show installed security policy

store installed security policy

ok

tlab> **sh** installed security policy

Z Policy

ok

tlab>


- Show me all the commands with “policy” for example...

- You only need to type in “enough” of the command to be unique “sh” vs “show”

Useful Assets

- HowToGuides (in the product)

The screenshot shows the IBM InfoSphere Guardium web interface. At the top, the header includes the product name, a timestamp (13:49), and navigation links for 'Edit Account: admin', 'Customize', 'Logout', and 'About'. A red box highlights a help icon in the top right corner. Below the header is a navigation bar with tabs for 'System View', 'Administration Console', 'Tools', 'Daily Monitor', 'Guardium Monitor', 'Tap Monitor', 'Incident Management', and 'My New Reports'. The main content area is titled 'G2000 - Standalone Unit' and contains a 'Contents' panel on the left and a 'How-to Guide Help Book' on the right. A red arrow points to the 'How-to Guide' item in the 'Contents' panel. The 'How-to Guide Help Book' section includes a title, a description, a list of topics, and a 'Download PDF' link.

IBM InfoSphere™ Guardium™ 13:49 | [Edit Account: admin](#) | [Customize](#) | [Logout](#) | [About](#) |  **IBM.**

System View Administration Console Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management My New Reports [G2000 - Standalone Unit](#)

-Activity Report
-Exceptions Rep
-Messages Rep
- Captured Data
DB2 Priv Summ
Returned SQL E
-EF1 Report
-EF1 Report2 Ev
-UF1
-UID Chain
-object report
Export Sensitive
- Alert Status
-RecordsAffecte
-ReturnedSQLER
-appEventRepor
- DB2 on Z repo
-testNewGuardiu

Contents Search Glossary

Guardium Help Home > How-to Guide

How-to Guide Help Book

This help book presents a series of how-to topics.

The format of each how-to topic is as follows:

- What is the task?
- Why is it important?/what is added value?
- Summary of the topic
- Prerequisites
- Step procedure with screens

Click any topic in the **Contents** panel to the left to view the topics online, or click the parent book to access a PDF version.

[Download PDF](#)

How-to Guide

- Common Tools
- Monitor/Audit
- Comply
- Assess/Harden
- GuardAPI Input Gener
- Guardium Installation I
- Protect
- Capture Replay

Resources

DeveloperWorks

- <http://www.ibm.com/developerworks/data/library/techarticle/dm-1304pcidiiss/>
- Great resource for white papers, tech notes, best practices

Guardium Tech Talks

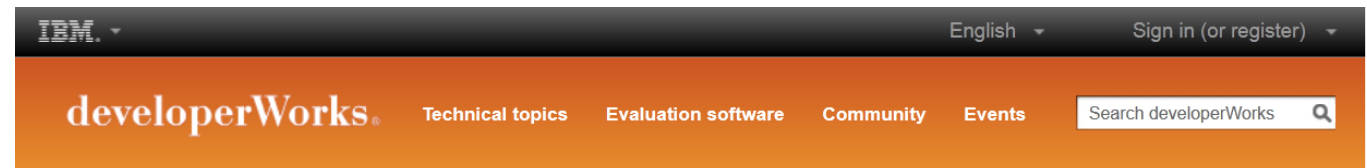
- https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Wf32fc3a2c8cb_4b9c_83e4_09b3c6f60e46/page/Guardium%20Tech%20Talks

Guardium YouTube Channel

- <http://www.youtube.com/user/InfoSphereGuardium>
- IBM InfoSphere Guardium 101 TechTalk
- Guardium demos
- Monitoring SAP with IBM InfoSphere Guardium (5:53)

Teradata Hardening Guide

- <http://www.teradata.com/white-papers/hardening-a-teradata-database-best-practices-access-rights-management/?type=WP>



developerWorks > Technical topics > Information Management > Technical library >

Accelerate the path to PCI DSS data compliance using InfoSphere Guardium

Use prebuilt reports, policies, and groups to simplify configuration

Kathryn Zeidenstein (krzeide@us.ibm.com), InfoSphere Guardium Evangelist, IBM
Shengyan Sun (sunssy@cn.ibm.com), InfoSphere Guardium QA Engineer, IBM

Date: 18 Apr 2013

Level: Intermediate

Summary for advanced users

If you are familiar with InfoSphere Guardium and don't need step-by-step instructions, here is a summary of what you need to do.

1. Download and install the PCI DSS accelerator from Passport Advantage, assigning the PCI role to a user, and resetting the GUI layout for that user. See [Install the PCI DSS accelerator and configure the PCI role](#) for more details.
2. Using the Guardium API (See [the appendix](#)) or the Group Builder (see [Populating groups](#)), populate groups that are used to generate the reports you need, as summarized here:
 - o PCI Admin Users
 - o PCI Authorized Client IPs
 - o PCI Authorized Server IPs
 - o PCI Authorized Source Programs
 - o PCI Cardholder DBs
 - o PCI Cardholder Sensitive objects
 - o PCI Limited Access Users
3. Configure a security policy, optionally using one of the PCI policies as a template. (See [Set up the security policy.](#))



security assessments to detect common vulnerabilities or usage of bad practices for security [assessments.](#))

Automate sign-offs and review (See [Use audit processes to automate sign-offs and review.](#))

GRDAPI Example – Get Entitlement Reports Automatically

ORA Object privileges

Start Date: 2012-06-14 09:02:24 End Date: 2012-06-21 09:02:24
Aliases: ON

Grantee	Table Name	Owner	Privilege	Datasource Name	SqlGuard Timestamp
FLows_020100	CTX_DDL	CTXSYS	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
HR	SET_CTX_USER	HR	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
ANONYMOUS	WWW_FLOW_FILE_OBJECTS\$	FLows_FILES	INDEX	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
FLows_020100V	\$_TIMER	SYS	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
DON	BIN\$SPhkr9kUVUjgQAoKOakSUg==\$0	JOE	UPDATE	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
HARRY	CREDITCARD	JOE	DELETE	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
ANONYMOUS	WWW_FLOW_EPG_INCLUDE_MODULES	FLows_020100	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
FLows_020100	UTL_FILE	SYS	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
HARRY	BIN\$SPb6bFLIZIrgQAoKOakOGg==\$0	JOE	UPDATE	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
FLows_020100	FLOW_SESSIONS	SYS	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
DON	BIN\$SPb6bFLIZIrgQAoKOakOGg==\$0	JOE	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
FLows_FILES	WWW_FLOW_ID	FLows_020100	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
FLows_020100	DBMS_FLASHBACK	SYS	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
BILL	CREDITCARD	JOE	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
FLows_020100	DBA_TABLESPACES	SYS	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
XDB	USER\$	SYS	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
BILL	BIN\$SPhkr9kUVUjgQAoKOakSUg==\$0	JOE	INSERT	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
FLows_020100	WWW_FLOW_VAL	SYS	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
FLows_020100	DBA_ROLLBACK_SEGS	SYS	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0
XDB	CTX_OUTPUT	CTXSYS	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 1521	:2012-06-21 09:02:06.0

Records 1 to 20 of 115

- Create datasource
- Create entitlement report reference and link it to datasource
- Upload information from database

Alter System Privileges

ORA Accnts of ALTER SYSTEM

Start Date: **2012-06-14 09:34:10** End Date: **2012-06-21 09:34:10**
 Aliases: **ON**

Grantee	Privilege	Admin Option	Datasource Name ▲	SqlGuard Timestamp
BANKAPP	ALTER SYSTEM	NO	10.10.9.56-sqlguard : ORACLE : 10.10.9.56 : xe : : null1521	2012-06-21 09:31:56.0
WEBAPP	ALTER SYSTEM	NO	10.10.9.56-sqlguard : ORACLE : 10.10.9.56 : xe : : null1521	2012-06-21 09:29:22.0
DBA	ALTER SYSTEM	YES	10.10.9.56-sqlguard : ORACLE : 10.10.9.56 : xe : : null1521	2012-06-21 09:31:56.0
BANKAPP	ALTER SYSTEM	NO	10.10.9.56-sqlguard : ORACLE : 10.10.9.56 : xe : : null1521	2012-06-21 09:29:22.0
HR	ALTER SESSION	NO	10.10.9.56-sqlguard : ORACLE : 10.10.9.56 : xe : : null1521	2012-06-21 09:31:56.0
DBA	ALTER SYSTEM	YES	10.10.9.56-sqlguard : ORACLE : 10.10.9.56 : xe : : null1521	2012-06-21 09:29:22.0
RECOVERY_CATALOG_OWNER	ALTER SESSION	NO	10.10.9.56-sqlguard : ORACLE : 10.10.9.56 : xe : : null1521	2012-06-21 09:31:56.0
HR	ALTER SESSION	NO	10.10.9.56-sqlguard : ORACLE : 10.10.9.56 : xe : : null1521	2012-06-21 09:29:22.0
WEBAPP	ALTER SESSION	NO	10.10.9.56-sqlguard : ORACLE : 10.10.9.56 : xe : : null1521	2012-06-21 09:31:56.0
RECOVERY_CATALOG_OWNER	ALTER SESSION	NO	10.10.9.56-sqlguard : ORACLE : 10.10.9.56 : xe : : null1521	2012-06-21 09:29:22.0
BANKAPP	ALTER SESSION	NO	10.10.9.56-sqlguard : ORACLE : 10.10.9.56 : xe : : null1521	2012-06-21 09:31:56.0
WEBAPP	ALTER SESSION	NO	10.10.9.56-sqlguard : ORACLE : 10.10.9.56 : xe : : null1521	2012-06-21 09:29:22.0
FLows_020100	ALTER SYSTEM	NO	osprey_system : ORACLE : : xe : : 1521	2012-06-21 09:29:22.0
SYSTEM	ALTER SYSTEM	NO	osprey_system : ORACLE : : xe : : 1521	2012-06-21 09:31:55.0
PETSTORE	ALTER SYSTEM	NO	osprey_system : ORACLE : : xe : : 1521	2012-06-21 09:29:22.0
XDB	ALTER SESSION	NO	osprey_system : ORACLE : : xe : : 1521	2012-06-21 09:31:55.0
SYSTEM	ALTER SYSTEM	NO	osprey_system : ORACLE : : xe : : 1521	2012-06-21 09:29:22.0
CTXSYS	ALTER SESSION	NO	osprey_system : ORACLE : : xe : : 1521	2012-06-21 09:31:55.0
XDB	ALTER SESSION	NO	osprey_system : ORACLE : : xe : : 1521	2012-06-21 09:29:22.0
FLows_020100	ALTER SESSION	NO	osprey_system : ORACLE : : xe : : 1521	2012-06-21 09:31:55.0

Records 21 to 40 of 64

GRDAPI Example – Get Entitlement Reports Automatically

create the datasource

```
G82.ibm.com> grdapi create_datasource type=ORACLE name=10.10.9.56-sqlguard
description=< > host=10.10.9.56 port=1521 serviceName=xe user=joe password=guardium
dbName=< > shared=true conProperty=< > dbInstanceDirectory=< > dbInstanceAccount=< >
application=Classifier owner=admin customURL=< > severity=< > api_target_host=< >
ID=20017
ok
G82.ibm.com>
```

Create the datasource bindings for Oracle Entitlement reports

```
G82.ibm.com> grdapi create_datasourceRef_by_name application=CustomTables
objName="ORA Accnts of ALTER SYSTEM" datasourceName="10.10.9.56-sqlguard"
ID=7
ok
G82.ibm.com>
```

Upload custom data into the entitlement reports

```
G82.ibm.com> grdapi upload_custom_data
tableName=ORA_ACCNTS_ALTER_SYSTEM_AND_SESSION
ID=7
ok
G82.ibm.com>
```


GRDAPI Example – Get Entitlement Reports Automatically

create the datasource (Only once)

```
grdapi create_datasource type=ORACLE name=10.10.9.56-sqlguard description=< > host=10.10.9.56 port=1521 serviceName=xe user=joe
password=guardium dbName=< > shared=true conProperty=< > dbInstanceDirectory=< > dbInstanceAccount=< > application=Classifier owner=admin
customURL=< > severity=< > api_target_host=< >
```

Create the datasource bindings for Oracle Entitlement reports

```
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA Acnts of ALTER SYSTEM" datasourceName="10.10.9.56-sqlguard"
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA Acnts with BECOME USER" datasourceName="10.10.9.56-sqlguard"
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA All Sys Priv and admin opt" datasourceName="10.10.9.56-sqlguard"
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA Obj And Columns Priv" datasourceName="10.10.9.56-sqlguard"
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA Object Access By PUBLIC" datasourceName="10.10.9.56-sqlguard"
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA Object privileges" datasourceName="10.10.9.56-sqlguard"
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA PUBLIC Exec Priv on SYS Proc" datasourceName="10.10.9.56-
sqlguard"
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA Roles Granted" datasourceName="10.10.9.56-sqlguard"
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA Sys Priv Granted" datasourceName="10.10.9.56-sqlguard"
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA SYSDBA and SYSOPER Acnts" datasourceName="10.10.9.56-
sqlguard"
```

Upload custom data into the entitlement reports

```
grdapi upload_custom_data tableName=ORA_OBJECT_PRIVILEGES_BY_DB
grdapi upload_custom_data tableName=ORA_HIERARCHICAL_SYS_PRIV_GRANTED debug=5
grdapi upload_custom_data tableName=ORA_ALL_SYSTEM_PRIVILEGE
grdapi upload_custom_data tableName=ORA_OBJECT_ACCESS_BY_PUBLIC debug=5
grdapi upload_custom_data tableName=ORA_EXEC_PRIV_ON_SYS_PROC debug=4
grdapi upload_custom_data tableName=ORA_SYSDBA_SYSOPER_PRIV_ACCNT
grdapi upload_custom_data tableName=ORA_ACCNTS ALTER_SYSTEM_AND_SESSION
grdapi upload_custom_data tableName=ORA_ACCOUNTS_WITH_BECOME_USER
grdapi upload_custom_data tableName=ORA_OBJECT_AND_COLUMNS_PRIVILEGES
grdapi upload_custom_data tableName=ORA_ROLES_TO_USERS_AND_ROLES
```

Encrypting Passwords with GrdAPI

-- In our example, we will use "guardium" as the password to encrypt

```
g8.ibm.com> grdapi encrypt_value valueToEncrypt="guardium" key=guardium
```

```
ID=0
```

```
-----BEGIN PGP MESSAGE-----
```

```
Version: GnuPG v1.4.5 (GNU/Linux)
```

```
jA0EAgMCovmWMCNrcsRgyTsz2oWR6nw67F+efUx/eQrH1qkVP61+9V3DFYv/3DW1
```

```
PLbouzfkbaiGRIjyK0KAaJI31Jbcg+Awhqr3JQ==
```

```
=xeNP
```

```
-----END PGP MESSAGE-----
```

```
ok
```

```
g8.ibm.com>
```

```
g8.ibm.com> grdapi create_datasource type=oracle name=OracleDataSourceEncrypted host=10.10.9.57
```

```
shared=true application=AuditTask owner=admin user=system serviceName=xencryptedParam=password
```

```
-----BEGIN PGP MESSAGE-----
```

```
Version: GnuPG v1.4.5 (GNU/Linux)
```

```
jA0EAgMCovmWMCNrcsRgyTsz2oWR6nw67F+efUx/eQrH1qkVP61+9V3DFYv/3DW1
```

```
PLbouzfkbaiGRIjyK0KAaJI31Jbcg+Awhqr3JQ==
```

```
=xeNP
```

```
-----END PGP MESSAGE-----
```

```
ok
```

```
ID=20023
```

```
g8.ibm.com>
```

Heterogeneous Database Entitlement Reports – Oracle Sample Reports

IBM InfoSphere™ Guardium® 02:24 | [Edit Account](#)

My New Reports Standard Reports Discover Assess/Harden Comply Protect Quick Start Sarbanes-Oxley Accelerator PCI Accelerator Data Privacy Accelerator

Overview

DB Activities

Exceptions

DB Administration

Schema Changes

Detailed Activities

Performance

DB Entitlements

DB2

Informix

MS-SQL

MySQL

Netezza

Oracle

PostgreSQL

Sybase

Teradata

Access Map

ORA Obj And Columns Priv

ORA Acnts of ALTER SYSTEM

ORA Acnts with BECOME USER

ORA Object privileges

ORA SYSDBA and SYSOPER Acnts

ORA All Sys Priv and admin opt

Managing the information...

Custom Reporting

Custom Tables ?

- Netezza Obj Privs by DB Username
- Netezza Obj Privs By Group
- Netezza Obj Privs Granted
- ORA Acnts of ALTER SYSTEM**
- ORA Acnts with BECOME USER
- ORA All Sys Priv and admin opt
- ORA Obj And Columns Priv
- ORA Object Access By PUBLIC
- ORA Object privileges
- ORA PUBLIC Exec Priv on SYS Proc
- ORA Roles Granted
- ORA Sys Priv Granted
- ORA SYSDBA and SYSOPER Acnts
- PostgreSQL Priv On DBs Granted PubUserRole
- PostgreSQL Priv On Language Granted PubUserRole
- PostgreSQL Priv On Schema Granted PubUserRole
- PostgreSQL Priv On Tablespace Granted PubUserRole
- PostgreSQL Role Granted To User Or Role
- PostgreSQL Super User Granted To User Or Role
- PostgreSQL Sys Privs Granted To User And Role

Upload Definition Manually Define Modify Delete Roles...

Upload Data Edit Data Purge Invalid Queries

Schedule, Purge, Overwrite, etc...

Custom Reporting

Import Data ?

Entity desc ORA Acnts of ALTER SYSTEM
Table name ORA_ACCNTS_ALTER_SYSTEM_AND_SESSION

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"/>	osprey_system_ORACLE(Classifier)	ORACLE	10.10.9.56	system
<input checked="" type="checkbox"/>	10.10.9.56-sqlguard_ORACLE(Classifier)	ORACLE	10.10.9.56	joe

Scheduling

Upload is currently not scheduled for execution.

The page at https://10.10.9.248:8443 says:

Operation ended successfully.
32 total inserts.
osprey_system:16 inserts.
10.10.9.56-sqlguard:16 inserts.

UID Chaining to Identify Unique Individual with “Generic” Accounts

- Problem:
 - Generic accounts like “System”, “SA”, “Sys” don’t have individual accountability to identify who performed the database transactions
 - Etc
- Solution
 - Use Guardium UID Chain feature. Need (hunter_trace=1) in guard_tap.ini
- Use Case
 - Uniquely identify “joe” as the user that logged into Oracle using the “system” account, from the OS User of “Oracle”

Developers/SAs/Analysts - Access to Live Production Systems

Start Date: 2010-03-07 20:53:45 End Date: 2010-03-12 17:53:45

Timestamp	Client IP	Server IP	Network Protocol	Uid Chain Compressed	OS User	DB User Name	Source Program	Full Sql	Uid Chain
2010-03-11 20:47:40.0	10.10.9.56	10.10.9.56	BEQUEATH	joe	ORACLE	SYSTEM	SQLPLUS@OSPREY	select * from creditcard	(1,root,init [3])->(2267,root,/usr/sbin/sshd)->(20063,root,sshd: joe [priv])->(20065, joe,sshd: joe@pts/3)->(20066,joe,-bash)->(20142,joe,su-oracle)->(20149,oracle,-bash)->(20175, oracle,sqlplus)->(20182,oracle,oracleXE (DESCRIPTION=(LOCAL=YES)(ADDRESS=(PROTOCOL=beq))))

```

joe@osprey:~
Using username "joe".
joe@10.10.9.56's password:
Last login: Fri Sep 25 13:31:39 2009 from jdi
[joe@osprey ~]$ su - oracle
Password:
-bash-3.00$ sqlplus system

SQL*Plus: Release 10.2.0.1.0 - Production on Fri Mar 12 16:39:53 2010

Copyright (c) 1982, 2005, Oracle. All rights reserved.

Enter password:

Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

SQL> select * from creditcard;

NAME                                CARDNUMBER                                CARDID
-----                                -
Joe D                                1234567890123456                                1
Harry S                                2345678901234567                                2

SQL> quit
Disconnected from Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production
-bash-3.00$
    
```

hunter_trace=1



Change Management Reconciliation

- Problem:
 - It's a manual and time consuming process to reconcile database changes to appropriate change tickets
- Solution
 - Use Guardium Select API to link DBA activity with change ticket number
- Use Case
 - Oracle DBA uses SQLPlus to change database based on change ticket. A report is required for auditors to identify the appropriate ticket with actual changes to the database
 - ** See attached document

Change Management Systems Overview

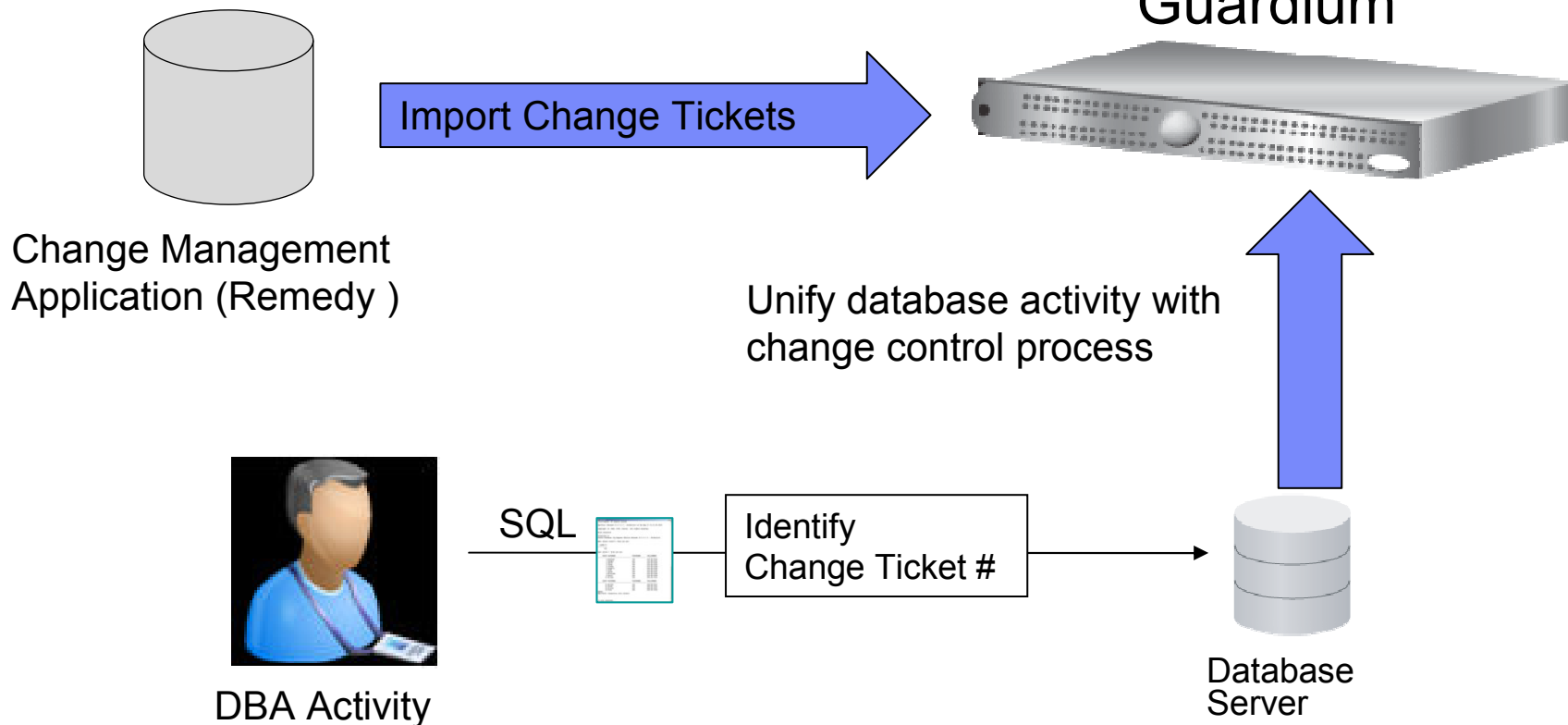
Authorized Change

Unauthorized Change

Timestamp	Server IP	DB User Name	CR Owner	CR Number - observed	Actual SQL	CR Number - CMDB	CR Instruction
2008-09-22 17:33:30.0	192.168.8.129	SYSTEM	allen	crq000000000027	CREATE TABLE pci_data (owner_name varchar(?), cc_number varchar(?))	CRQ000000000027	Plase create a table called PC data
2008-09-22 17:34:02.0	192.168.8.129	SYSTEM			drop table pci_data		

Records: 1 to 2 of 2

Aliases: ON



Change Control Process

Change CRQ000000000042 (Modify)

BMC REMEDY IT SERVICE MANAGEMENT - Change Management Help

Infrastructure Change bmcsoftware

Quick Links

- CI Search
- Select Operational
- Select Product
- View Broadcasts
- View Calendar

Functions

- Advanced
- Create Other Requests
- Consoles

Change ID*+

Process Flow Status

Initiate > Review & Authorize > **Plan & Schedule** > Implement > Closed

Approval Status

Current Overall

Change Request Information

Change Type* Change **Status*** Scheduled For Approval **Impact*** 4-Minor/Localized

Summary* Alter SOX revenue table **Status Reason** **Urgency*** 4-Low

Risk Level* Risk Level 1 **Priority** Low

Notes

Requester Classification Work Info Tasks Assignment Relationships Approvers SLM Financials Dates

Requested By **Requested For**

Support Company*+ Calbro Financial Services **First Name+**

Start Date: 2009-01-22 15:00:00 End Date: 2009-01-22 16:00:00

Timestamp	Server Type	risk level	priority	description	change id	change id entered	Assigned To	DB User Name	Client IP	Server IP	Sql
2009-01-22 15:08:12.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	SELECT ? from dual
2009-01-22 15:08:21.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_east add total_revenue float
2009-01-22 15:08:29.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_central add total_revenue float
2009-01-22 15:08:36.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_west add total_revenue float
2009-01-22 15:08:44.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_revenue float
2009-01-22 15:12:39.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	alter table allen.sox_sales_east add sum_total float
2009-01-22 15:14:19.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	insert into allen.sox_sales_east (customer_zipcode,revenue,total_revenue,sum_total) values(?,?,?,?,?)
2009-01-22 15:41:44.0	ORACLE	0	0			crq000000000232	allen	SYSTEM	192.168.8.129	192.168.8.129	SELECT ? from dual
2009-01-22 15:41:55.0	ORACLE	0	0			crq000000000232	allen	SYSTEM	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_rev float

Sample login.sql for oracle environments

- Change Management Integration

Start Date: 2009-01-27 22:36:04 End Date: 2009-01-27 23:36:04

Timestamp	Event User Name	Event Value Str	Event Type	Client IP	Server IP	DB User Name	Sql
2009-01-27 23:33:11.0	finance	changerequest	crq000054	10.10.9.56	10.10.9.56	JOE	alter table salesregion add latinamerica float

```

root@osprey:~/jsql
[root@osprey jsql]# sqlplus joe

SQL*Plus: Release 10.2.0.1.0 - Production on Tue Jan 27 23:32:26 2009

Copyright (c) 1982, 2005, Oracle. All rights reserved.

Enter password:

Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

Enter Business Owner: Finance
Enter Change Request (ticket) Number: CRQ000054
SQL> alter table salesregion add latinamerica float;

Table altered.

SQL> quit
Disconnected from
[root@osprey jsql]
    
```

Portions of login.sql

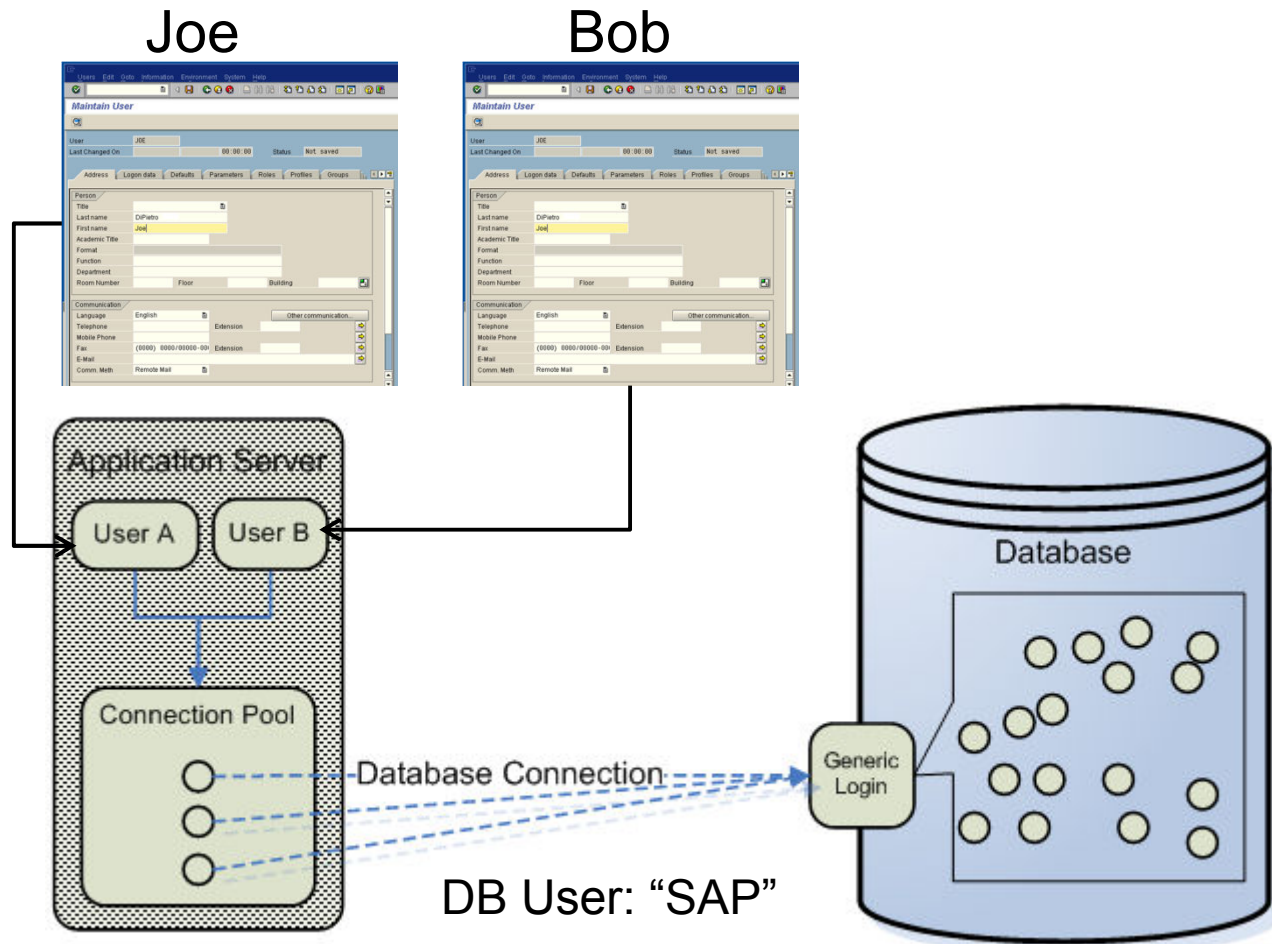
```

accept EventUserName char prompt "Enter Business Owner: "
accept TicketNumber char prompt "Enter Change Request (ticket) Number: "
select 'GuardAppEvent:Start', 'GuardAppEventType:&TicketNumber',
'GuardAppEventUserName:&EventUserName',
'GuardAppEventStrValue:ChangeRequest' from dual;
    
```

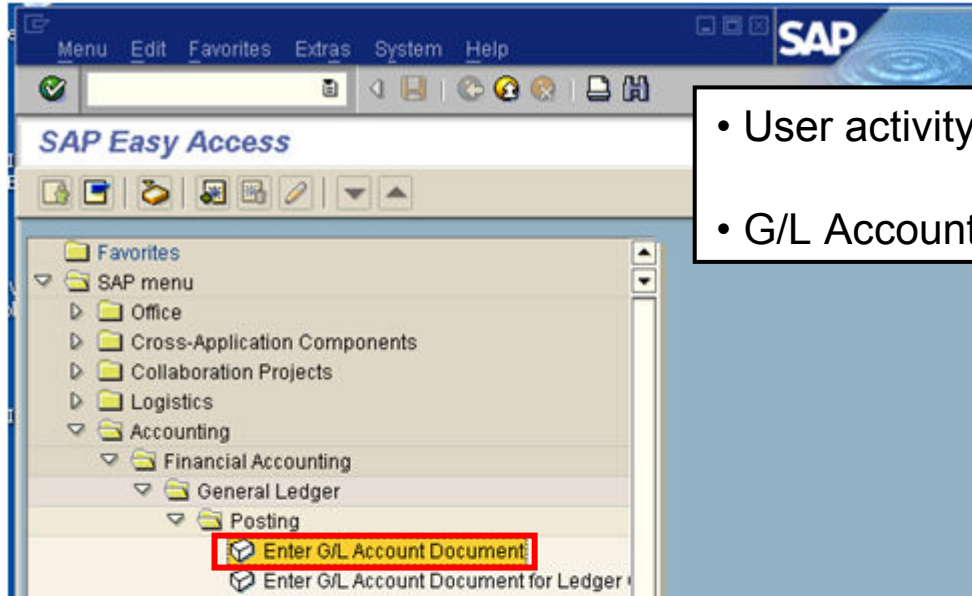
Application User Identification

- Problem:
 - Identify the actual user that performed a transaction to the database through a pooled user account
- Solution
 - Depending on the application architecture, Guardium can help identify the actual user through the pooled connection
- Use Case
 - Need to identify the SAP user that performs that transactions and the SAP transaction codes
 - Out of the box, SAP, Siebel, Oracle EBS, etc
 - Custom Applications
 - Depends on the architecture, but there are different methods that we can use. Stored Procedure Scraping, Custom API's, etc

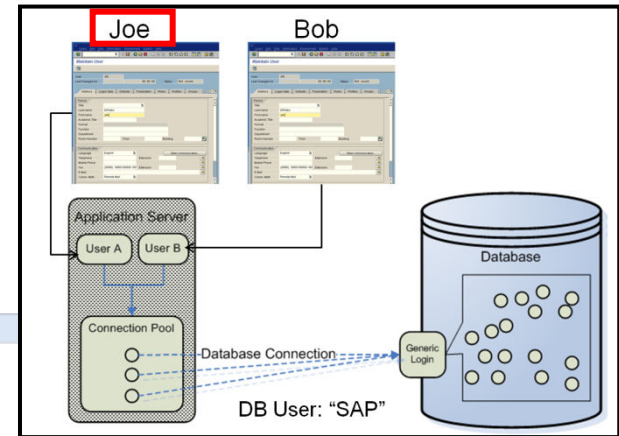
Identifying the End User of the Transaction Through a Pooled Database User



SAP Transactions to G/L Account



- User activity is based on transactions
- G/L Account Posting = FB50 transaction



- sql trace

Start Date: 2010-09-22 10:08:22:52
 Aliases: ON
 DBUserLike: LIKE %
 NetProtoLike: LIKE %
 SourceProgLike: LIKE %

Pooled SAP Database User (SAPE6A) → **Unique SAP User that executed the transaction** (JOE)

Timestamp	Client IP	Server IP	Network Protocol	Database Name	DB User Name	Application User	Full Sql
2010-09-22 17:24:10.0	10.10.10.10	10.10.10.10	SHARED MEMORY	E6A	SAPE6A	JOE	SELECT * FROM "TSTC" WHERE "TCODE" = 'FB50' FETCH FIRST 1 ROWS ONLY OPTIMIZE FOR 1 ROWS WITH CS -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLSMTR_NAVIGATION_MODULES , 621) -- SYSTEM(E6A, SAPE6A)
2010-09-22 17:24:10.0	10.10.10.10	10.10.10.10	SHARED MEMORY	E6A	SAPE6A	JOE	SELECT * FROM "TSTCT" WHERE "SPRS" = 'E' AND "TCODE" = 'FB50' FETCH FIRST 1 ROWS ONLY OPTIMIZE FOR 1 ROWS WITH CS -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLSMTR_NAVIGATION_MODULES , 1416) -- SYSTEM(E6A, SAPE6A)

Reference Documents: Document, Account, Master Records, Statistical Key Figures, Periodic Processing

You are not authorized to use transaction FB50

Tesekkur Ederiz!