

IBM InfoSphere Guardium V8.2

Lab exercises



Contents

LAB 1	DATABASE AUTO-DISCOVERY	5
	1.1 EXPLORING DATABASE AUTO-DISCOVERY	5
LAB 2	SENSITIVE DATA FINDER	20
	2.1 EXPLORING SENSITIVE DATA FINDER	20
	2.2 CONFIGURING "FIRE ONLY WITH" MARKER (OPTIONAL)	43
LAB 3	ENTITLEMENT REPORTS	60
	3.1 EXPLORING ENTITLEMENT REPORTS	60
LAB 4	GUARDIUM CLIENT INSTALLATION	94
	4.1 SILENT S-TAP AND CONFIGURATION AUDITING SYSTEM (CAS) DEPLOYMENT	94
	4.2 GUARDIUM INSTALLATION MANAGER DEPLOYMENT	115
	4.3 GIM DISCOVERY TO AUTOMATE INSPECTION ENGINE CONFIGURATION	151
	4.4 AUTOMATIC CLIENT UPGRADE (NO REBOOT REQUIRED)	173
LAB 5	CUSTOM REPORTS	190
	5.1 MONITORING USER ID CHAIN	190
	5.2 USING COMPUTED ATTRIBUTES (OPTIONAL)	217
LAB 6	POLICY BUILDER	246
	6.1 CONFIGURING ALERT POLICY	246
	6.2 CONFIGURING TERMINATE POLICY WITH S-GATE	265
	6.3 CONFIGURING QUARANTINE POLICY	293
	6.4 CONFIGURING REDACT (DATA MASKING) POLICY	319
LAB 7	VULNERABILITY ASSESSMENT	342
	7.1 EXPLORING VULNERABILITY ASSESSMENT	342
	7.2 CONFIGURING QUERY-BASED TESTS (OPTIONAL)	355
	7.3 CONFIGURING EXCEPTION TESTS (OPTIONAL)	377
LAB 8	COMPLIANCE WORKFLOW AUTOMATION	392
	8.1 EXPLORING COMPLIANCE WORKFLOW AUTOMATION	392
	8.2 CUSTOM WORKFLOW BUILDER	425
	8.3 ADVANCED COMPLIANCE WORKFLOW (OPTIONAL)	453
LAB 9	CONFIGURATION AUDIT SYSTEM (CAS)	482
	9.1 EXPLORING CAS	482
LAB 10	CORRELATION ALERTS	506
	10.1 EXPLORING CORRELATION ALERTS	506
LAB 11	STANDARD REPORTS	540
	11.1 EXPLORING STANDARD REPORTS	540
	11.2 STANDARD REPORTS LAYOUT	581
LAB 12	PAYMENT CARD INDUSTRY (PCI) ACCELERATOR	588
	12.1 EXPLORING THE PCI ACCELERATOR	588
	12.2 ADDING USERS WITH PCI ROLE (OPTIONAL)	607
LAB 13	APPLICATION END-USER IDENTIFIER	628
	13.1 CONFIGURING APPLICATION END-USER IDENTIFIER	628
	13.2 IDENTIFY USERS WITH GUARDAPPEVENTS API	657
	13.3 CUSTOM ID PROCEDURES	663
LAB 14	GUARDIUM ENTERPRISE DEPLOYMENT	676
	14.1 UPGRADE WITHOUT REBOOT (FLASH DEMO)	676
	14.2 S-TAP FAILOVER (FLASH DEMO)	679
	14.3 DRILLDOWN REPORT CONTROLS (FLASH DEMO)	681
	14.4 GRDAPI LINKAGE WITH DATABASE INSTANCE DISCOVERY (FLASH DEMO)	683
	14.5 GUARDIUM ALIAS REPORTING (FLASH DEMO)	685
	14.6 CONFIGURING QUERY-BASED TESTS (FLASH DEMO)	687
	14.7 CONFIGURING EXCEPTION TESTS (FLASH DEMO)	689
	14.8 APPLICATION END-USER IDENTIFIER (FLASH DEMO)	691
LAB 15	FREQUENTLY ASKED QUESTIONS	694
	15.1 DIAGNOSE EMPTY OR QUESTIONABLE REPORTS	695
	15.2 DIAGNOSE S-TAP COMMUNICATION ISSUES	696
	15.3 DIAGNOSE S-TAP CAPTURE ISSUES	699
	15.4 DIAGNOSE S-GATE ISSUES	700
	15.5 DIAGNOSE POLICY ISSUES	701
	15.6 DIAGNOSE NETWORK CAPTURE ISSUES	702
	15.7 DIAGNOSE COLLECTOR PERFORMANCE ISSUES	703

THIS PAGE INTENTIONALLY LEFT BLANK

Lab 1 Database Auto-Discovery

1.1 Exploring Database Auto-Discovery

Overview

Even in stable environments, where cataloging processes have historically existed, uncontrolled instances can inadvertently be introduced through mechanisms, including developers that create “temporary” test environments; business units seeking to rapidly implement local applications; and purchases of new applications with embedded databases.

The Auto-discovery application can be configured to probe specified network segments on a scheduled or on-demand basis, and can report on all databases discovered—solving the problem of identifying both legacy and newly introduced databases. Similarly, the Auto-discovery application can be used to demonstrate that a process exists to identify all new instances.

Objectives

In this lab you will learn how to:

- __1. Configure a database scan
- __2. Run the scan
- __3. View the results

- __1. Using the IBM InfoSphere® Guardium® GUI, demonstrate the ease of use within the IBM InfoSphere Guardium solution. Start the IBM InfoSphere Guardium appliance and log in.
 - __a. From your laptop, browse to <https://10.10.9.248:8443>
 - __b. Login as **pot / guardium**.

Login

Please enter your information

User name:

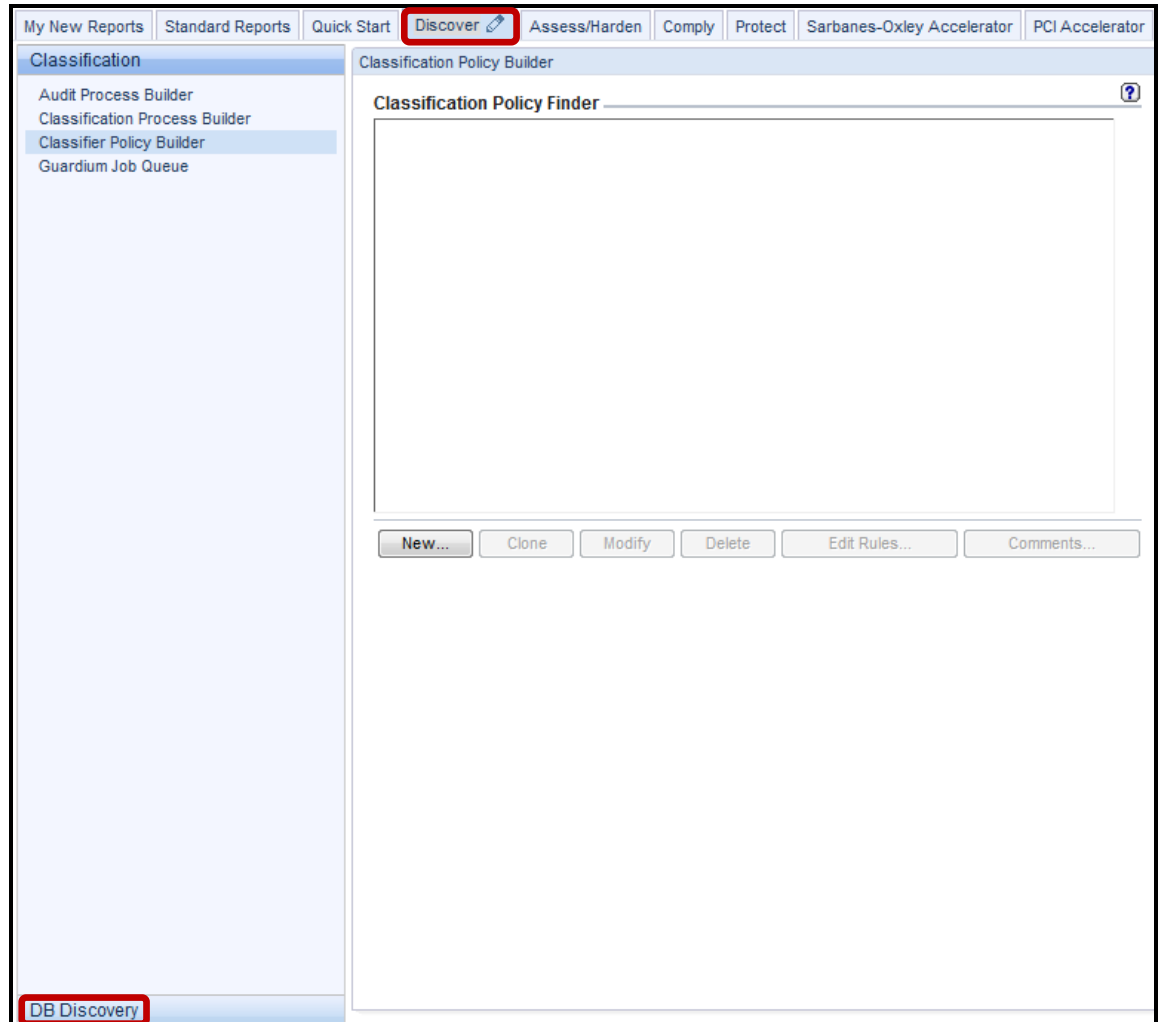
Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

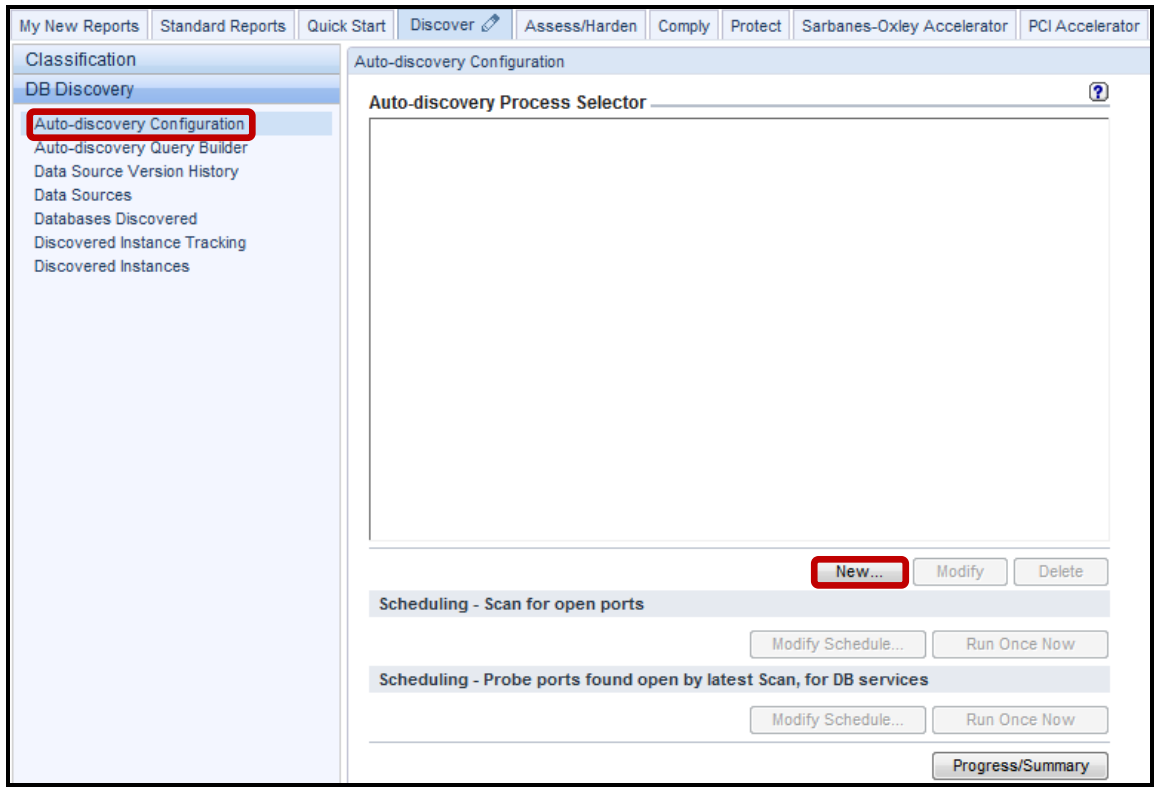
Licensed Materials - Property of IBM. 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistry/key © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

- __2. Use the IBM InfoSphere Guardium GUI to create a new Database Discovery application.
- __a. Click the **Discover** tab, then scroll down and click **DB Discovery** on the bottom left of the page.



__b. Click **Auto-discovery Configuration** under the *DB Discovery* tab, and then click **New**.



- __c. Enter '**V8 PoT Discover Databases**' for *Process name*, and click **Apply**.

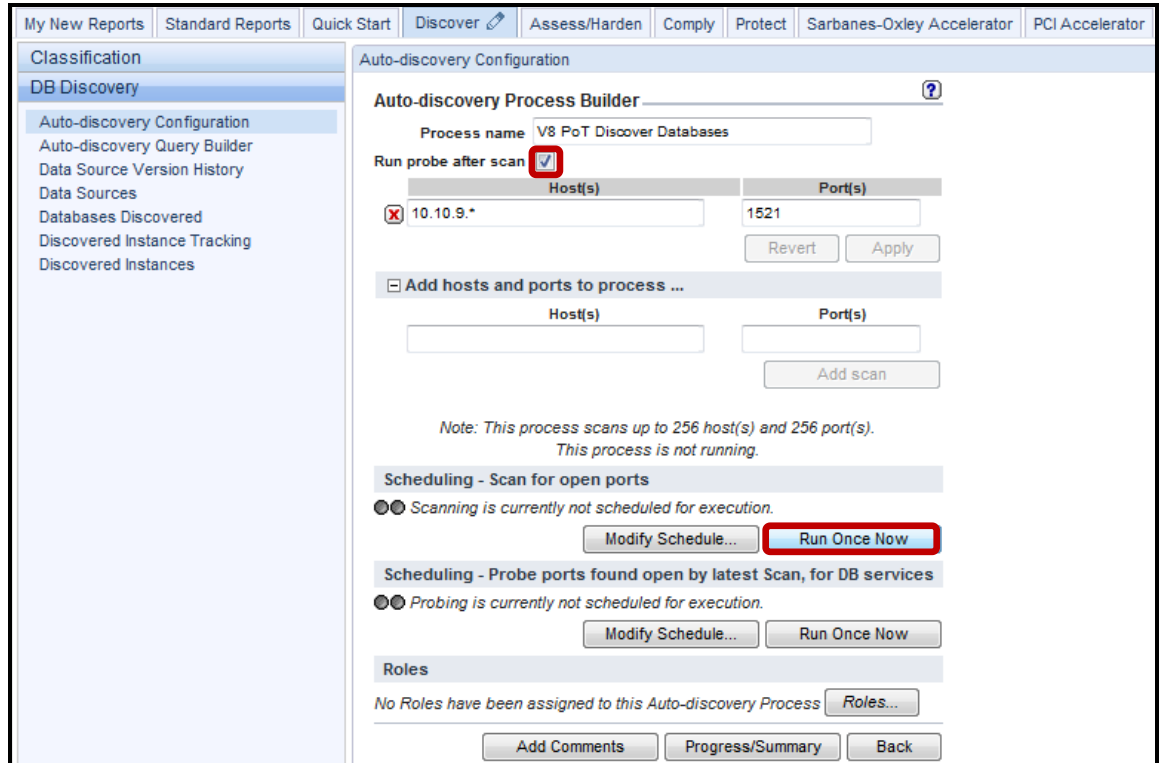
The screenshot shows the 'Auto-discovery Configuration' window. The 'Process name' field is set to 'V8 PoT Discover Databases'. The 'Run probe after scan' checkbox is checked. The 'Apply' button is highlighted in red. The 'Add hosts and ports to process ...' section is expanded, showing the status 'This process is not running.' Below this, there are two scheduling sections: 'Scheduling - Scan for open ports' and 'Scheduling - Probe ports found open by latest Scan, for DB services'. Both are currently not scheduled for execution. The 'Roles' section shows 'No Roles have been assigned to this Auto-discovery Process'.

- __d. Enter '**10.10.9.***' in the *Host(s)* field. This will result in the scanning of IP addresses 10.10.9.0 → 10.10.9.254. You can also enter just a single specific IP address.

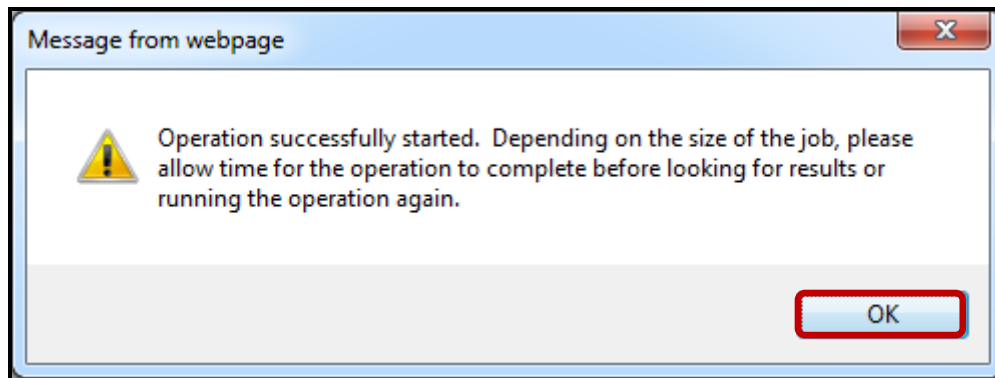
- __e. Enter '**1521**' in the *Port(s)* field and click **Add scan**. Repeat for additional scans if desired. You can also enter more than one port separated by comma(s) or a range of ports as well. You can also have multiple scan entries.

The screenshot shows the 'Auto-discovery Configuration' window. The 'Process name' field is set to 'V8 PoT Discover Databases'. The 'Run probe after scan' checkbox is checked. The 'Add hosts and ports to process ...' section is expanded, showing the 'Host(s)' field set to '10.10.9.*' and the 'Port(s)' field set to '1521'. The 'Add scan' button is highlighted in red. The 'Scheduling' and 'Roles' sections are the same as in the previous screenshot.

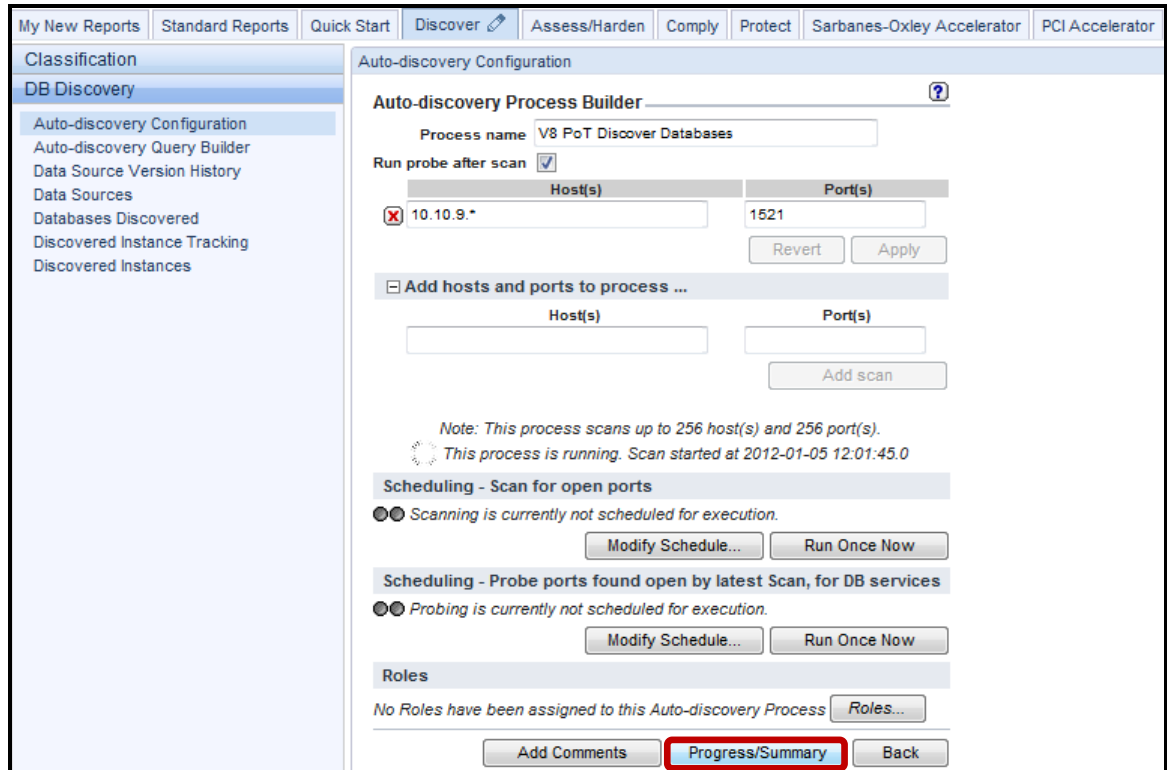
- __f. Make sure the **Run probe after scan** box is checked. This will cause the *probe* to automatically run after the scan completes.
- __g. Click **Run Once Now** under 'Scheduling – Scan for open ports' to start the scan followed by the probe.



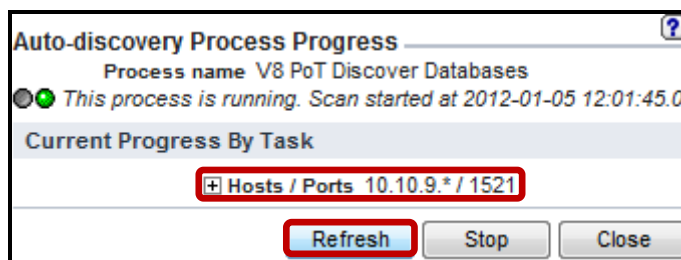
- __h. Click **OK** to acknowledge.



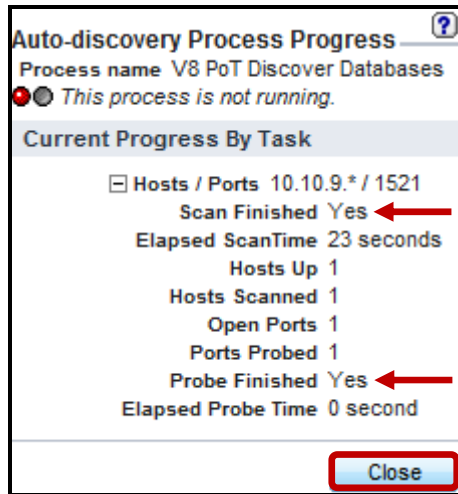
- i. Click **Progress/Summary** to view status of the scan/probe. It should complete in less than a minute. Larger scans will take longer.



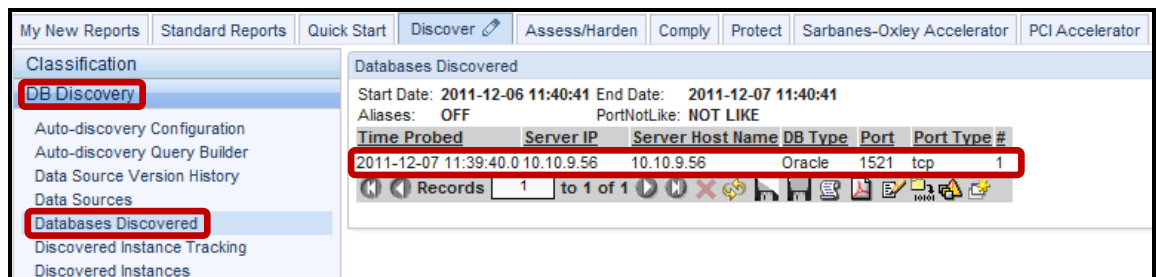
- j. Click the '+' icon to expand the **Hosts / Ports** pull-down. Click **Refresh** until the discovery process completes.



- __k. Click **Close** once the scan has completed.



- __l. Click **Databases Discovered** under the **DB Discovery** tab to view results.
- __m. Verify that the **Oracle** database has been discovered.



- __n. Now, click **Auto-discovery Configuration** under the *DB Discovery* tab once more, and then click **Modify** to modify the existing scan to scan a specific IP address.

The screenshot displays the 'Auto-discovery Configuration' window. The left-hand navigation pane is under the 'DB Discovery' tab, with 'Auto-discovery Configuration' selected. The main area shows the 'Auto-discovery Process Selector' set to 'V8 PoT Discover Databases'. Below this, there are two scheduling sections:

- Scheduling - Scan for open ports**: A radio button is selected, indicating that scanning is currently not scheduled for execution. Buttons for 'Modify Schedule...' and 'Run Once Now' are present.
- Scheduling - Probe ports found open by latest Scan, for DB services**: A radio button is selected, indicating that probing is currently not scheduled for execution. Buttons for 'Modify Schedule...' and 'Run Once Now' are present.

At the bottom right, there is a 'Progress/Summary' button.

- __o. In this case, you can simply substitute **10.10.9.56** for the **Host(s)** field and click **Apply**, and then click **Run Once Now**.

The screenshot shows the 'Auto-discovery Configuration' window. The 'Auto-discovery Process Builder' section is active, showing a process named 'V8 PoT Discover Databases'. The 'Host(s)' field is populated with '10.10.9.56' and the 'Port(s)' field with '1521'. The 'Run probe after scan' checkbox is checked. Below the fields, there are 'Revert' and 'Apply' buttons. The 'Apply' button is highlighted with a red box. Below this, there is a section for 'Scheduling - Scan for open ports' with a radio button selected for 'Scanning is currently not scheduled for execution.' and a 'Run Once Now' button highlighted in red. There is also a section for 'Scheduling - Probe ports found open by latest Scan, for DB services' with a radio button selected for 'Probing is currently not scheduled for execution.' and a 'Run Once Now' button. At the bottom, there are buttons for 'Add Comments', 'Progress/Summary', and 'Back'.

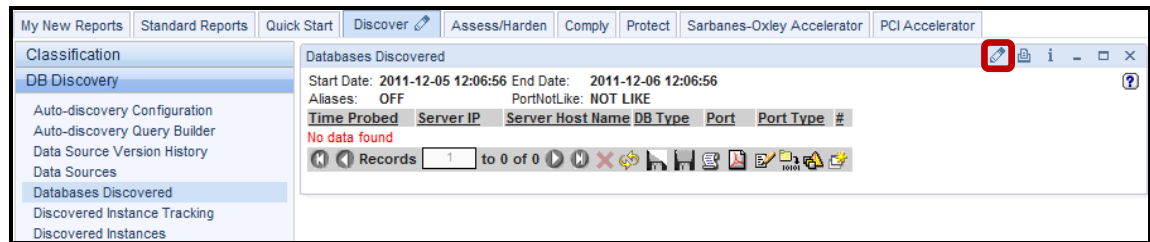
- __p. Now we see the additional scan result for the database(s) with the specific IP 10.10.9.56.

The screenshot shows the 'Databases Discovered' window. It displays a table of scan results. The table has the following columns: Time Probed, Server IP, Server Host Name, DB Type, Port, and Port Type. The data in the table is as follows:

Time Probed	Server IP	Server Host Name	DB Type	Port	Port Type	#
2011-12-07 11:39:40.0	10.10.9.56	10.10.9.56	Oracle	1521	tcp	1
2011-12-07 12:01:32.0	10.10.9.56	10.10.9.56	Oracle	1521	tcp	1

The second row of the table is highlighted with a red box. Below the table, there are navigation buttons and a record count of '1 to 2 of 2'.

- ___q. If the report does not produce any discovered databases, click the **Customize (Pencil Icon)** at the upper right.



- ___r. Make sure the **QUERY_FROM_DATE** and **QUERY_TO_DATE** *runtime parameters* are in the desired range as displayed below.
- ___s. If adjustments are necessary, simply adjust the desired date ranges and click **Update**. The new results will be projected immediately. You may need to sync system clocks.



- ___t. If the report still displays no results, then make sure the database server at 10.10.9.56 is running.
- ___u. If scanning a range of IP addresses such as 10.10.9.*, the above solution will not be practical for this lab.

Thank You

Database Auto-Discovery review

- __1. The Database Auto-discovery process runs on:
- __a. The InfoSphere Guardium collector
 - __b. The database server
 - __c. The client PC
 - __d. A network switch
- __2. Network IDS (Intrusion Detection Systems) will often view the Database Auto-discovery process as a possible threat. (**True** or **False**)
- __3. Database Auto-Discovery is a:
- __a. One-step process, scanning the network for active database ports
 - __b. Two-step process, first scanning all active ports, then querying each port with the known database protocols
 - __c. Three-step process, first verifying which IPs are active, then scanning all active ports, then querying each port with the known database protocols
- __4. The Database Auto-discovery process can be scheduled to run on a periodic basis (for example, once a week). (**True** or **False**)
- __5. Database Auto-discovery results can be:
- __a. Sent automatically through email to the admin user
 - __b. Only viewed through the GUI from the Databases Discovered report
 - __c. Viewed through the GUI from the Databases Discovered report, or automatically distributed using the Compliance Workflow capability

Database Auto-Discovery review (Answers)

__1. The Database Auto-discovery process runs on:

A – The InfoSphere Guardium Collector.

__2. Network IDS (Intrusion Detection Systems) will often view the Database Auto-discovery process as a possible threat. (**True** or **False**)

True.

__3. Database Auto-discovery is a:

B – Two-step process, first scanning all active ports, then querying each port with the known database protocols.

__4. The Database Auto-discovery process can be scheduled to run on a periodic basis (for example, once a week). (**True** or **False**)

True.

__5. Database Auto-discovery results can be:

C – Viewed through the GUI from the Databases Discovered report, or automatically distributed using the Compliance Workflow capability.

Lab 2 Sensitive Data Finder

2.1 Exploring Sensitive Data Finder

Overview

The task of securing sensitive data begins with identifying it. This can be challenging, because database environments are highly dynamic: the content of known instances is constantly changing and most organizations lack an effective means of identifying and understanding the content of unknown instances. In mature organizations, existing databases deployed before change control mechanisms had been implemented are not uncommon. Larger organizations growing through acquisition often struggle to gauge with certainty sensitive data risk in acquired infrastructures.

In roughly 20 percent of incidents, unknown data played a role in the compromise. To minimize this risk, organizations need a systematic way to identify all database instances and to determine on an ongoing basis which instances contain sensitive data, so that appropriate controls can be implemented.

The InfoSphere Guardium solution provides a complete means for addressing the entire database security and compliance life cycle. Once database instances of interest are identified by Auto-discovery, Sensitive Data Finder can be used to examine the content of each to determine whether sensitive data is included, and then take appropriate action. When a match is found, the rule can specify a wide variety of responsive actions, including:

- Logging the match.
- Sending a real-time alert detailing the match to an oversight team.
- Automatically adding the object to an existing privacy set or group (objects with similar properties, such as those containing payment card data), ensuring related security policies are automatically applied to the newly discovered object.
- Inserting a new-access rule into an existing security-policy definition.

Classification policies can be run against any specified database group on a scheduled or on-demand basis, using limited read-only credentials.

Objectives

This lab will illustrate how we can create a new Classification Policy that will search for credit card numbers and populate the *Sensitive Objects* group with the table name and column name for each detected incident.

- __1. Create a Classification Policy.
- __2. Add a Search for Data rule to the policy.
- __3. Specify an action that will populate a group when rule is triggered.
- __4. Create a Classification Process to run the Classification application.
- __5. View the results and verify that the correct group was populated.

- __1. Using the IBM InfoSphere Guardium GUI, demonstrate the ease of use within the IBM InfoSphere Guardium solution. Start the IBM InfoSphere Guardium appliance and log in.
- __a. From your laptop, browse to <https://10.10.9.248:8443>
- __b. Login as **pot / guardium**.

Login

Please enter your information

User name:

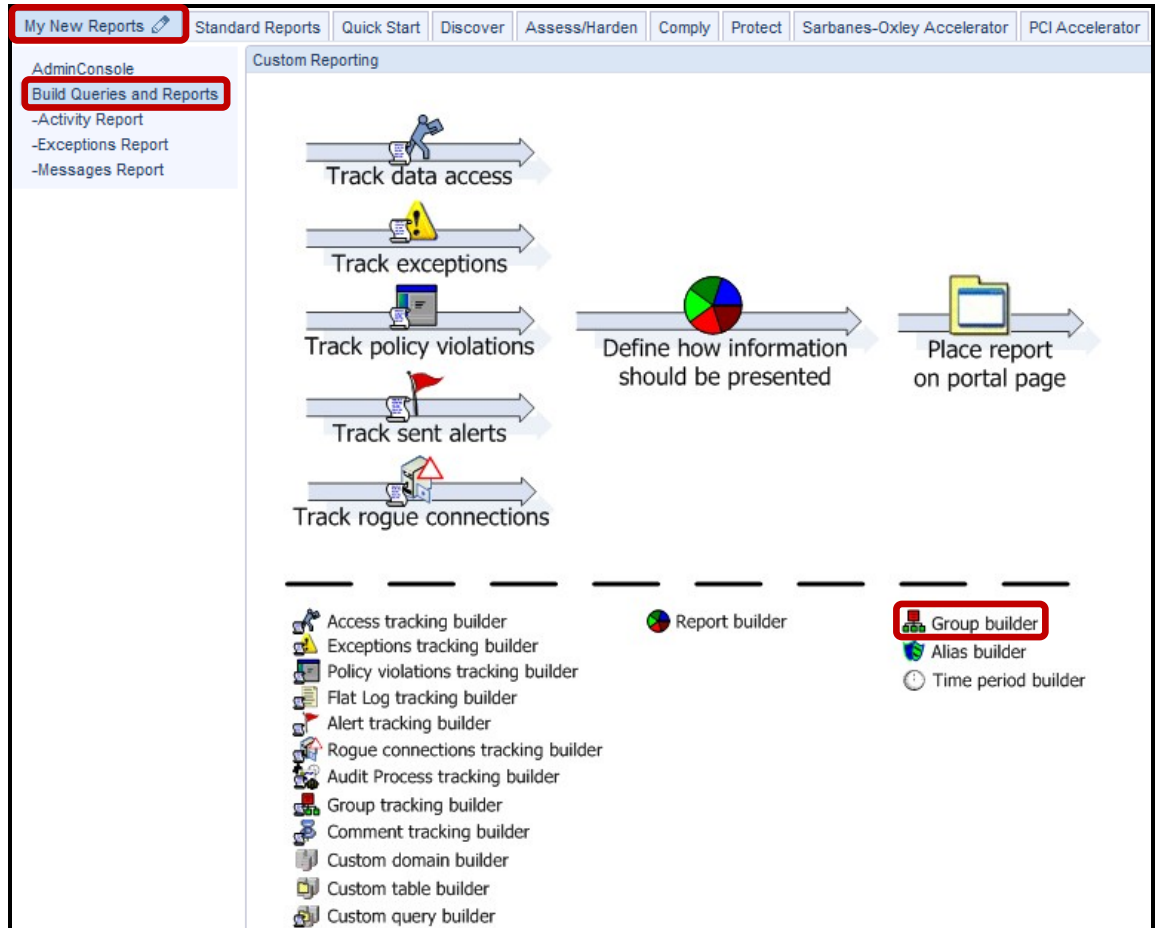
Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

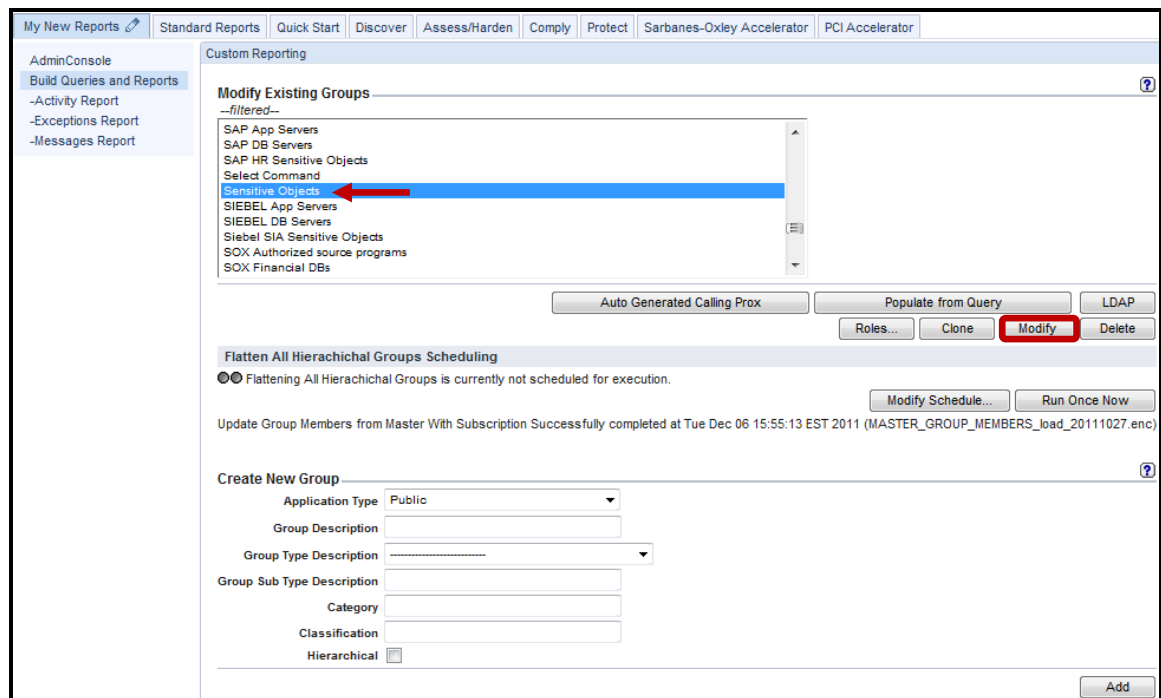
Licensed Materials - Property of IBM. 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistry/key © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

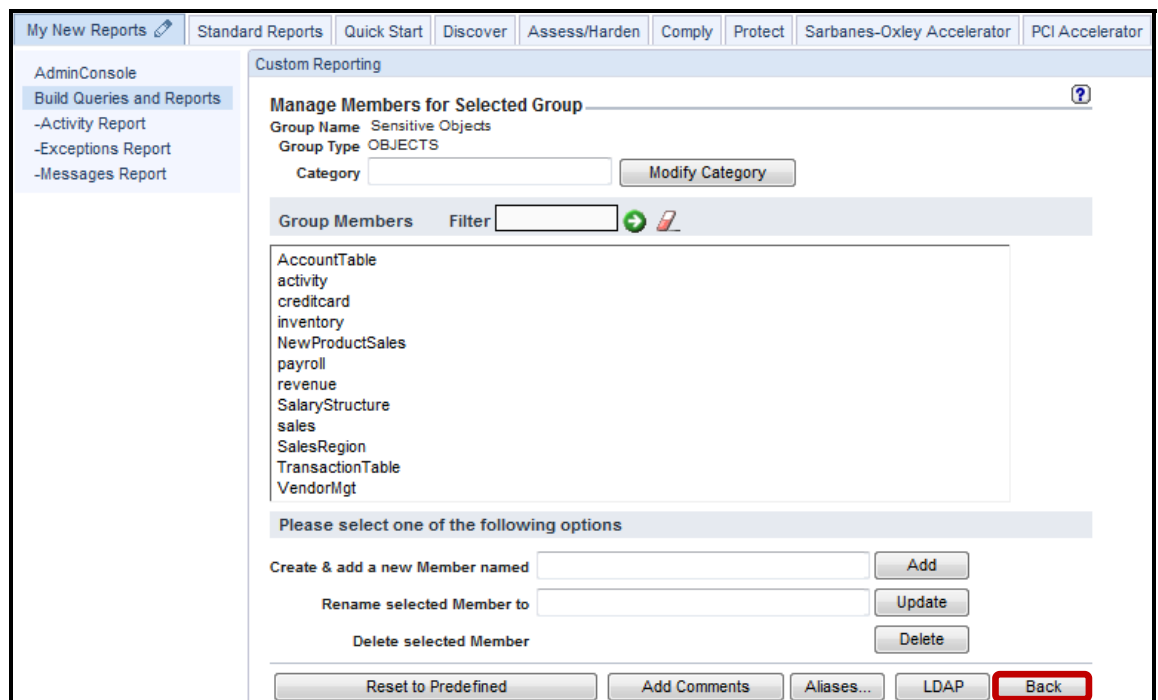
- __2. Before getting started, examine the current contents of the **Sensitive Objects** group.
 - __a. Click **Build Queries and Reports** under the **My New Reports** tab, and then click **Group builder**.



- __b. Scroll down the *Modify Existing Groups* drop-down list, select **Sensitive Objects**, and then click **Modify**.

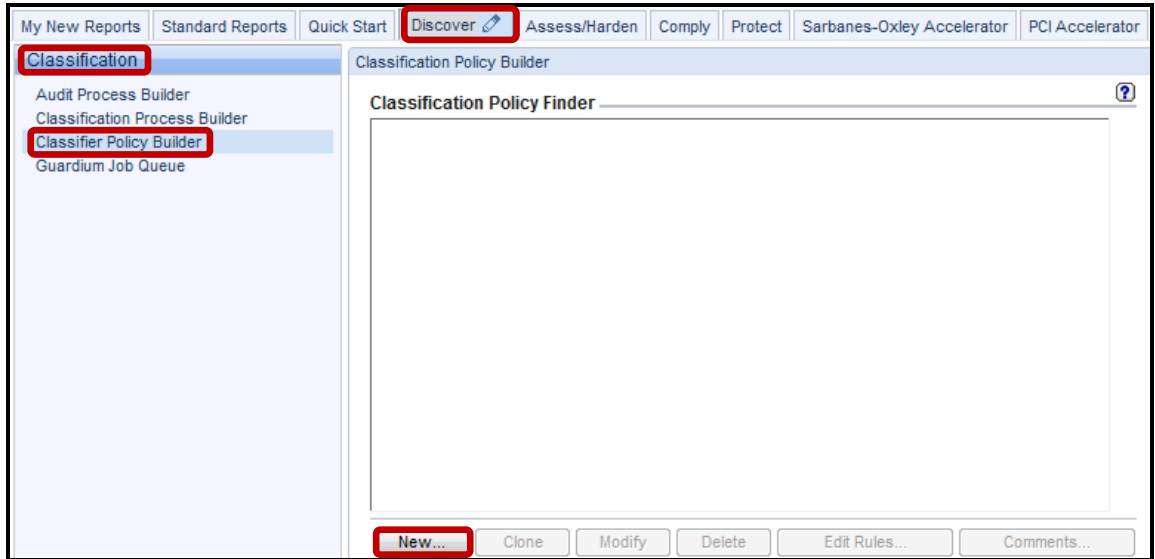


- __c. Here we can see the default **Sensitive Objects** group members provided as part of the InfoSphere Guardium Knowledgebase service. **Note these members for comparison at the end of this lab.** Click **Back** when finished examining the contents of this group.

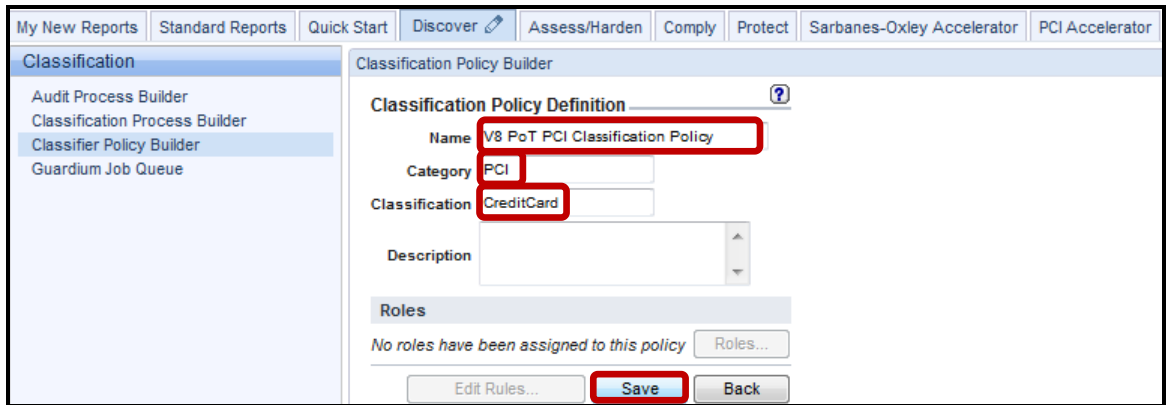


__3. Create a Classification policy

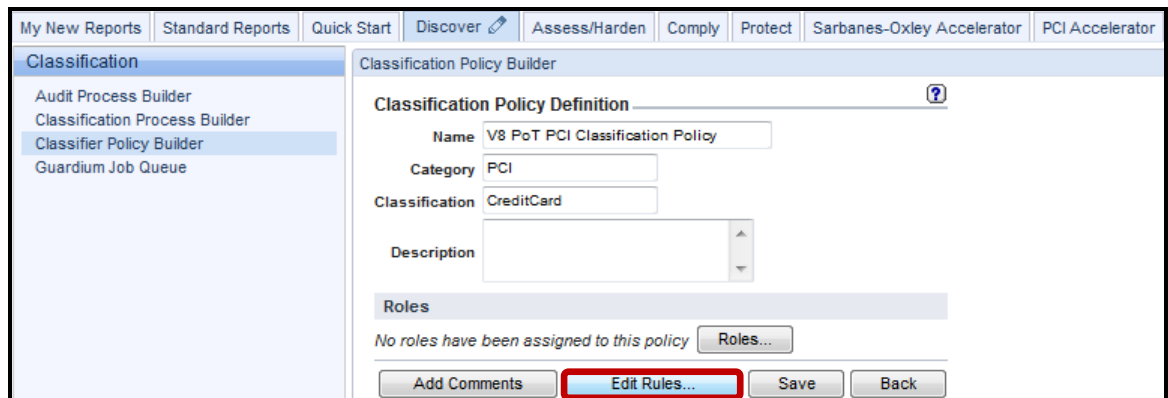
- __a. Click **Classifier Policy Builder** under the **Discover->Classification** tabs, and then click **New**.



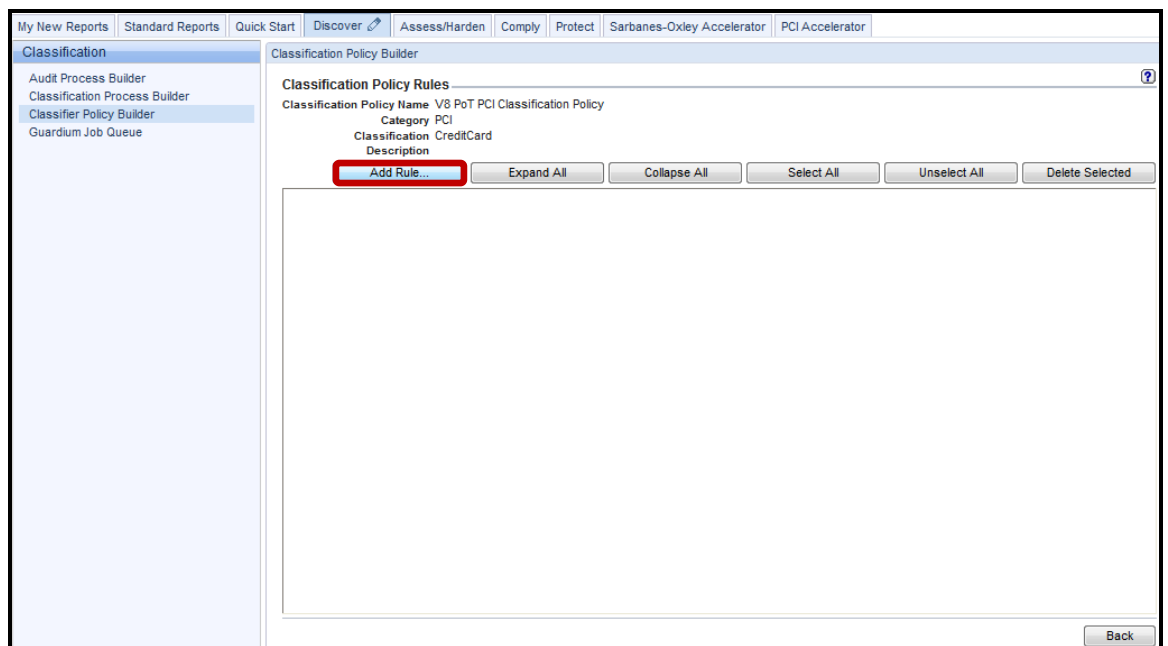
- __b. Enter '**V8 PoT PCI Classification Policy**' in the *Name* field, '**PCI**' in the *Category* field, '**CreditCard**' in the *Classification* field, and then click **Save**.



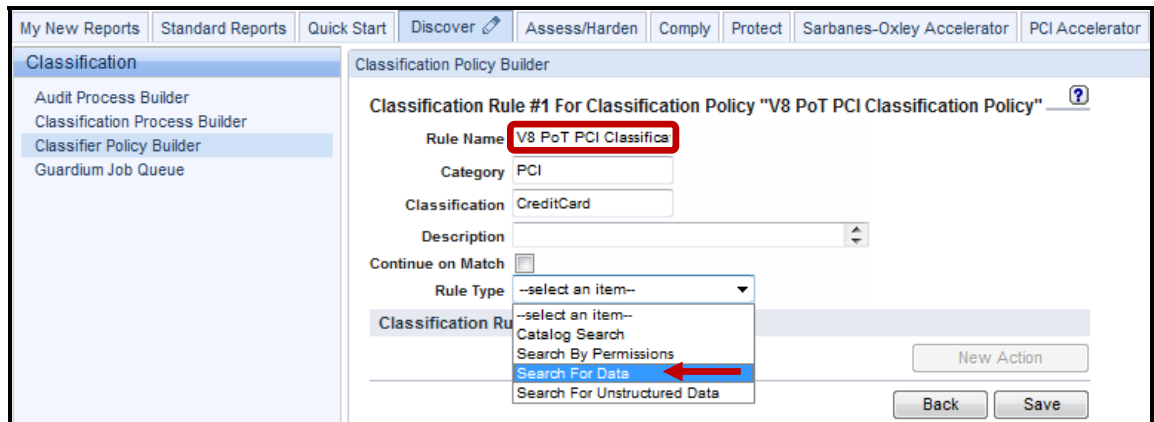
__c. Click **Edit Rules**.



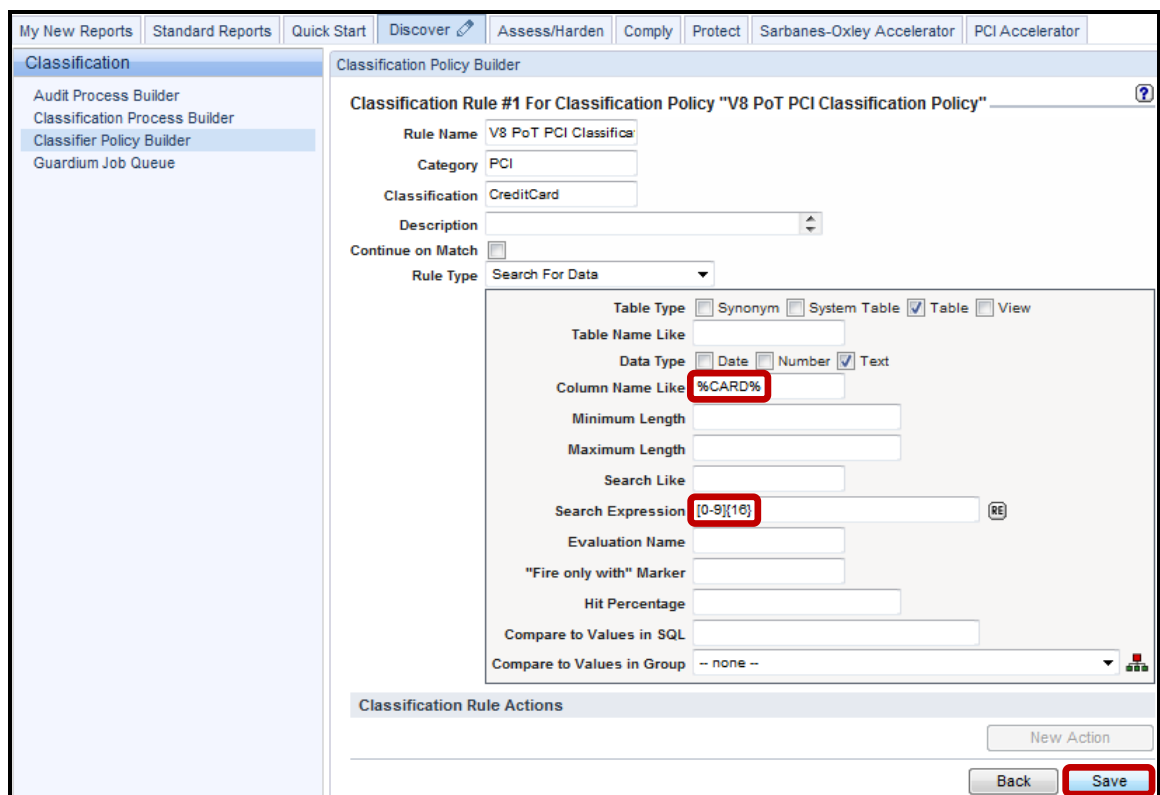
__d. Click **Add Rule**.



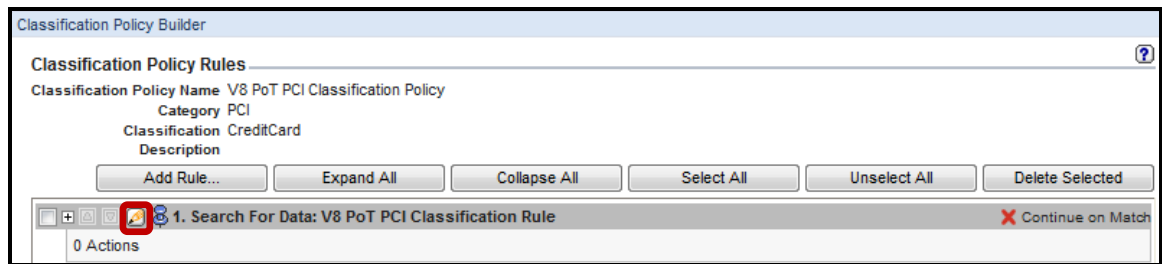
- __e. Enter 'V8 PoT PCI Classification Rule' in the *Rule Name* field, expand the *Rule Type* dropdown list, and select **Search For Data**.



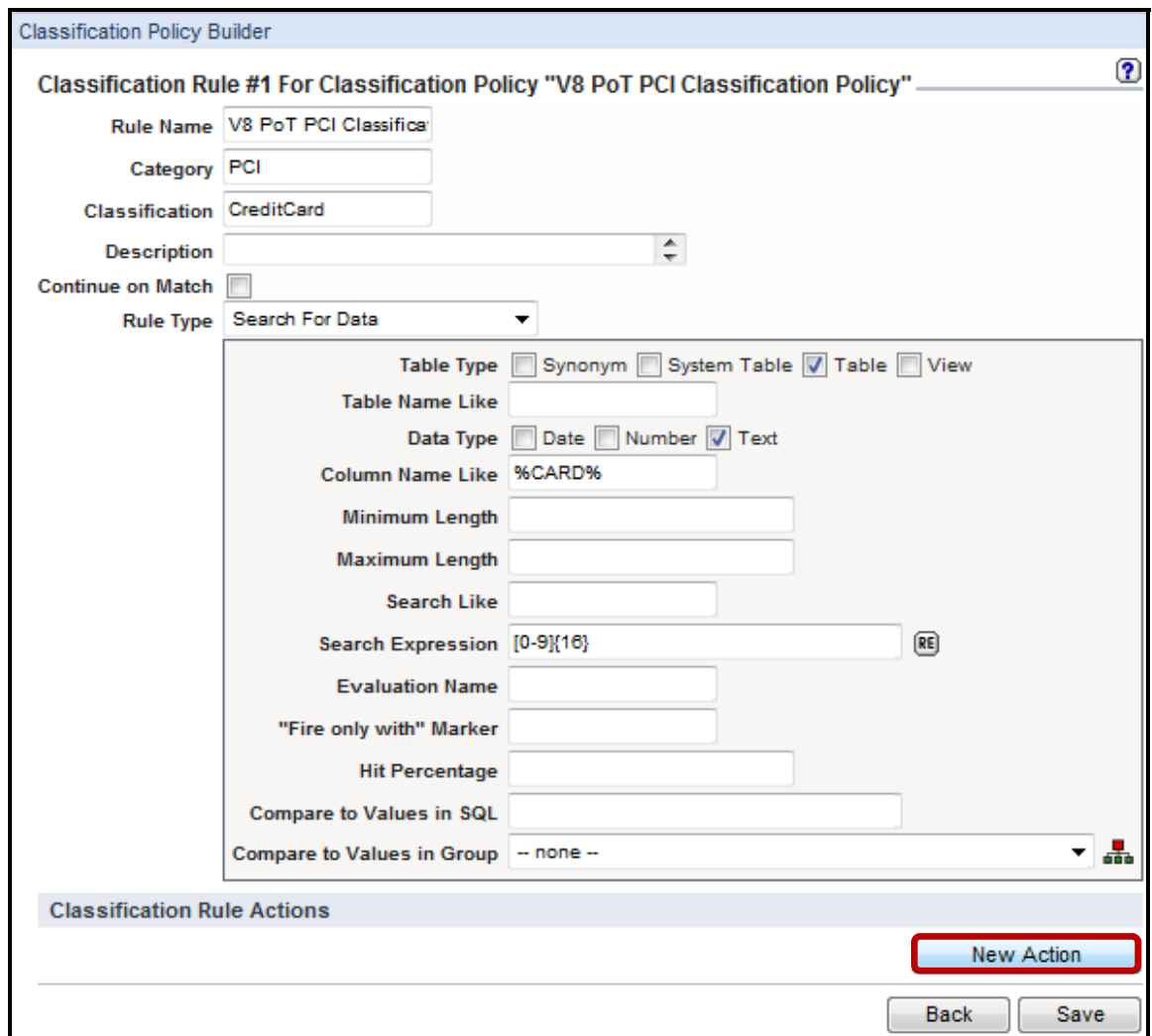
- __f. Enter **%CARD%** in the *Column Name Like* field, **[0-9]{16}** in the *Search Expression* field, and then click **Save**.



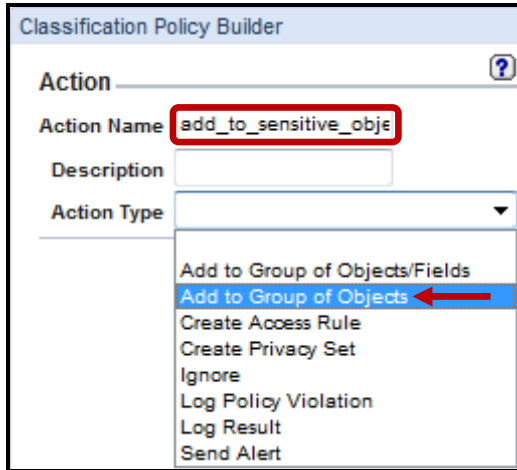
__g. Click the **Edit (pencil)** icon to add a new *Action*.



__h. Click **New Action**.



- ___i. Type 'add_to_sensitive_objects' in *Action Name* field, expand the *Action Type* dropdown list, and select **Add to Group of Objects**.



- ___j. Expand the *Object Group* dropdown list and select **(public) Sensitive Objects**.

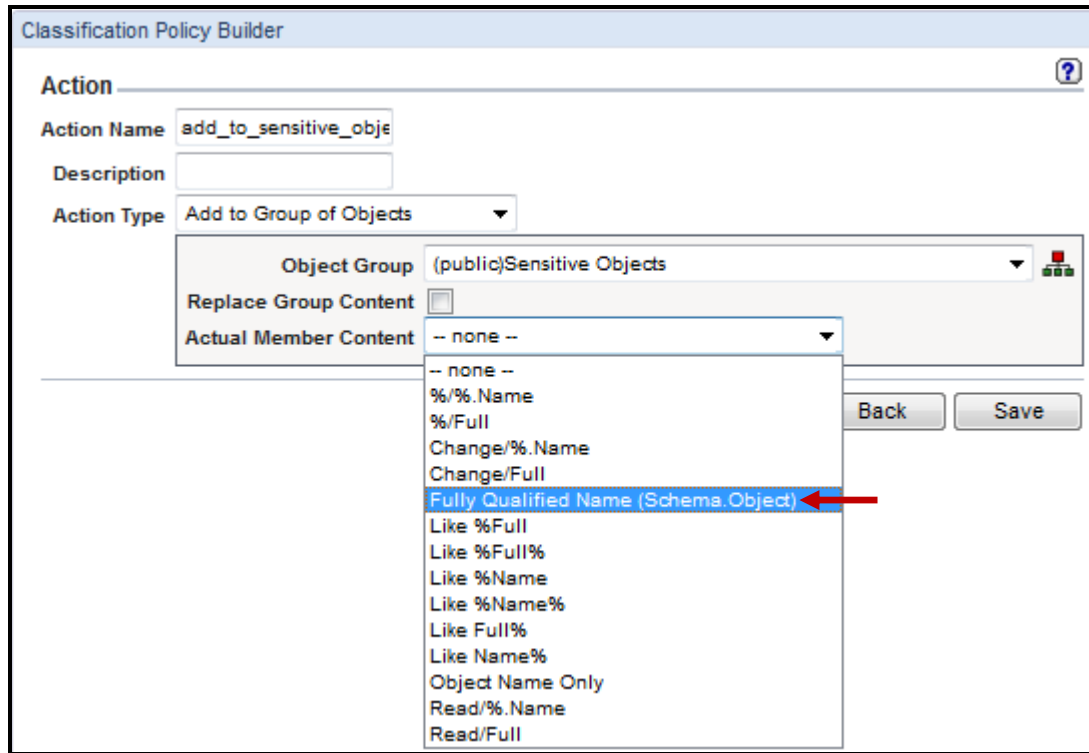
The screenshot shows the 'Classification Policy Builder' window. The 'Action' section is visible, with the following fields:

- Action Name:** add_to_sensitive_obje
- Description:** (empty)
- Action Type:** Add to Group of Objects

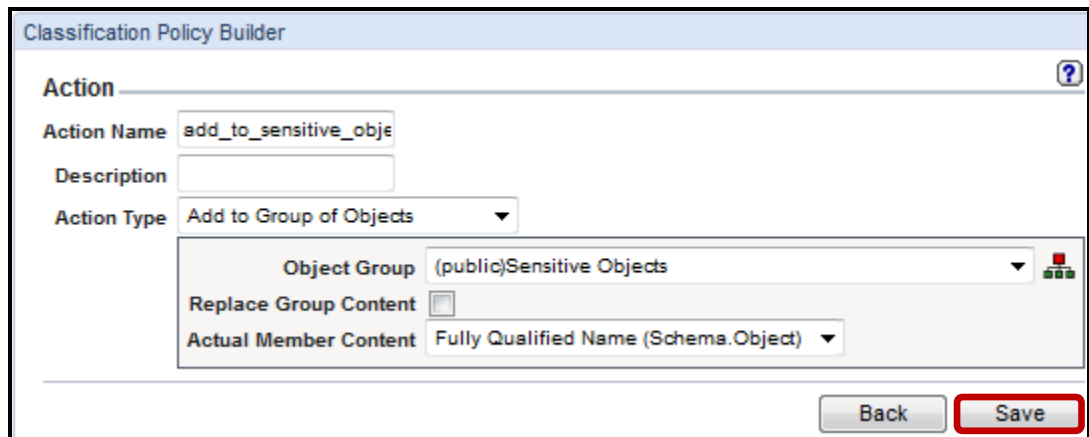
The 'Object Group' dropdown menu is expanded, showing a list of object groups. The group '(public) Sensitive Objects' is highlighted in blue, and a red arrow points to it. The list includes:

- none --
- (public)Oracle EBS - SOX
- (public)Oracle EBS HRMS Sensitive Objects
- (public)PCI Cardholder Sensitive objects
- (public)Peer Association Procedures
- (public)PeopleSoft Objects
- (public)PeopleSoft Sensitive Objects
- (public)Potential Overflow Objects
- (public)Public executable procedures
- (public)Public selectable object
- (public)Replay - Exclude from Compare
- (public)Replay - Include in Compare
- (public)SAP - PCI
- (public)SAP HR Sensitive Objects
- (public) Sensitive Objects**
- (public)Siebel SIA Sensitive Objects
- (public)SOX Financial Objects
- (public)Suspicious Objects
- (public)System Configuration Procedures
- (public)Vulnerable Objects (with wildcards)
- (public)Vulnerable Objects (with wildcards) - DB2
- (public)Vulnerable Objects (with wildcards) - DB2 iSeries
- (public)Vulnerable Objects (with wildcards) - DB2 z/OS
- (public)Vulnerable Objects (with wildcards) - Informix
- (public)Vulnerable Objects (with wildcards) - MSSQL Server
- (public)Vulnerable Objects (with wildcards) - MySQL
- (public)Vulnerable Objects (with wildcards) - Netezza
- (public)Vulnerable Objects (with wildcards) - Oracle
- (public)Vulnerable Objects (with wildcards) - PostgreSQL
- (public)Vulnerable Objects (with wildcards) - Sybase
- (public)Vulnerable Objects (with wildcards) - Teradata

- __k. Select **Fully Qualified Name (Schema.Object)** from the *Actual Member Content* dropdown list.



- __l. Click **Save**.



__m. Click **Save** one more time.

Classification Policy Builder

Classification Rule #1 For Classification Policy "V8 PoT PCI Classification Policy" ?

Rule Name: V8 PoT PCI Classifica

Category: PCI

Classification: CreditCard

Description:

Continue on Match:

Rule Type: Search For Data

Table Type: Synonym System Table Table View

Table Name Like:

Data Type: Date Number Text

Column Name Like: %CARD%

Minimum Length:

Maximum Length:

Search Like:

Search Expression: [0-9]{16} RE

Evaluation Name:





"Fire only with" Marker:

Hit Percentage:

Compare to Values in SQL:

Compare to Values in Group: -- none --

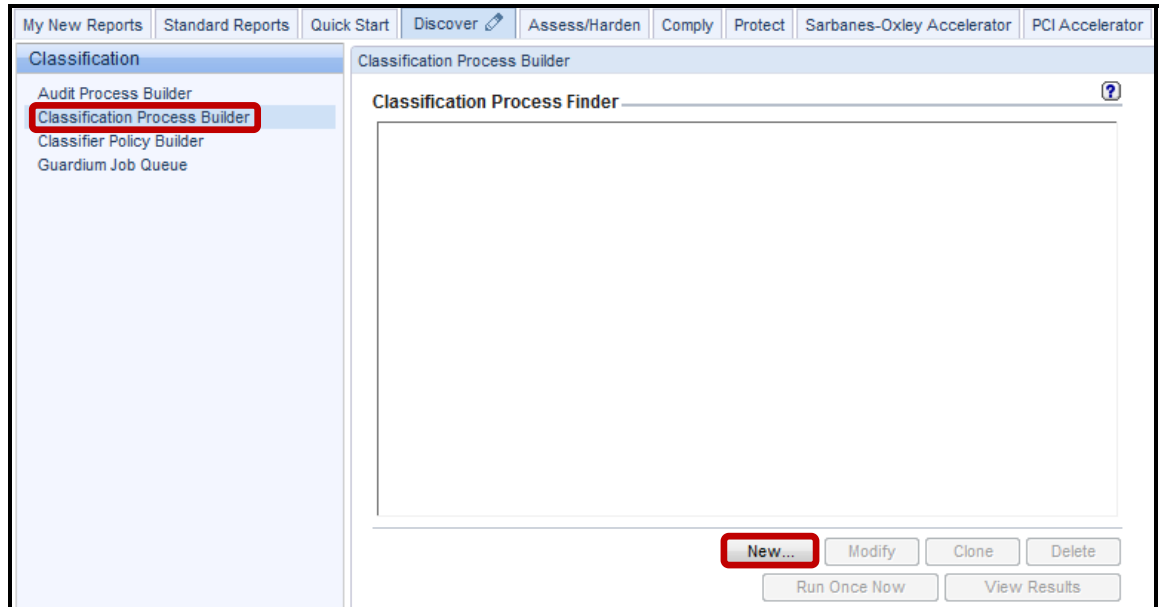
Classification Rule Actions

    1 add_to_sensitive_objects (Add to Group of Objects)

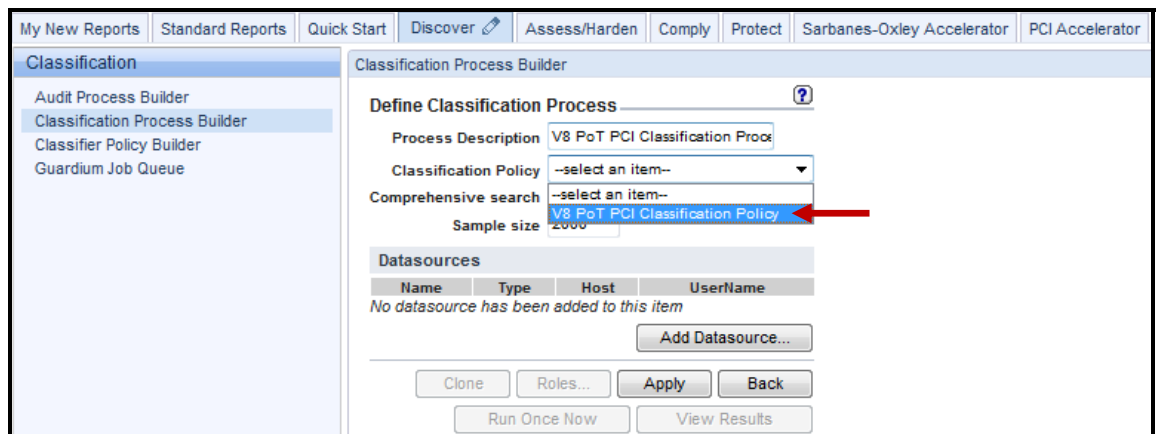
New Action

Back Save

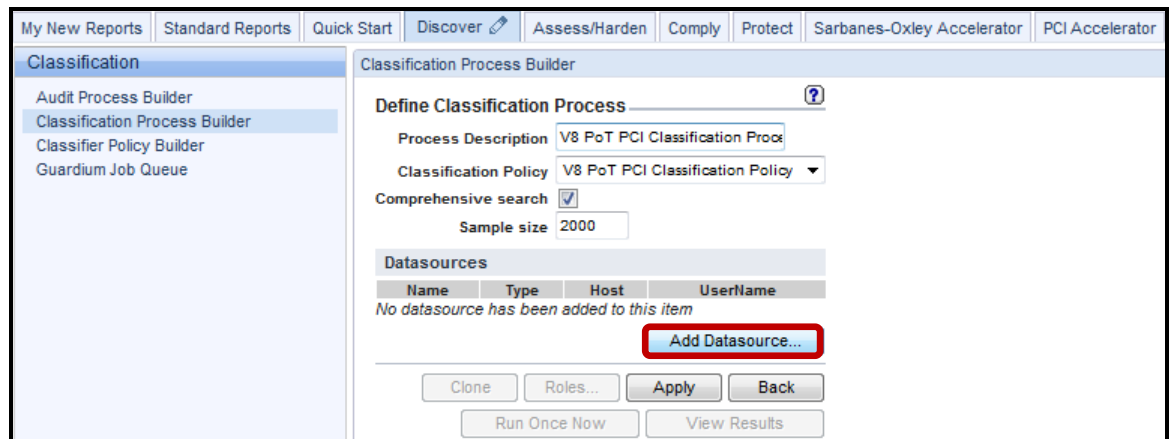
- __4. Create a Classification Process to run the Classifier Policy
 - __a. Click **Classification Process Builder**, and then click **New** to create a Classification Process for running the *Classifier Policy* that was just created.



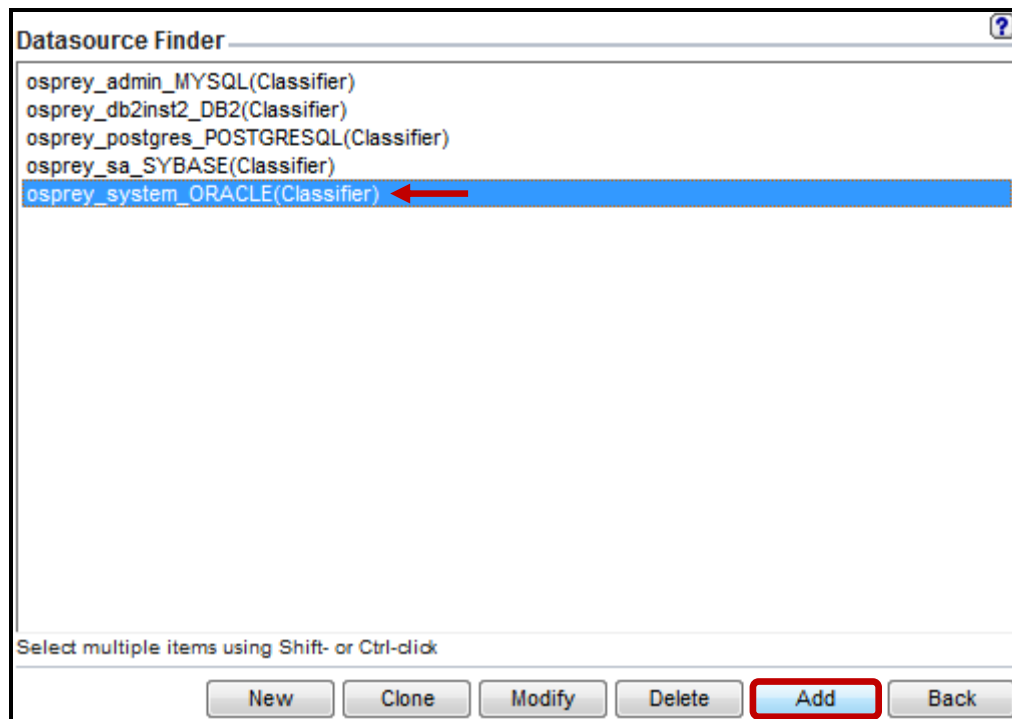
- __b. Enter '**V8 PoT PCI Classification Process**' for *Process Description*.
- __c. Expand the *Classification Policy* dropdown list and select **V8 PoT PCI Classification Policy**.



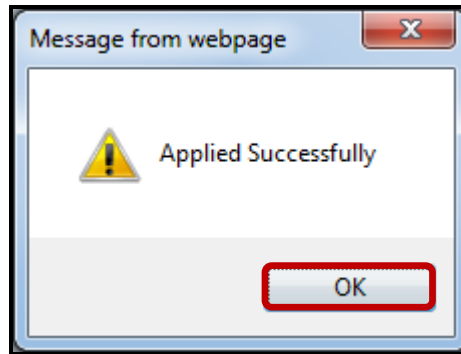
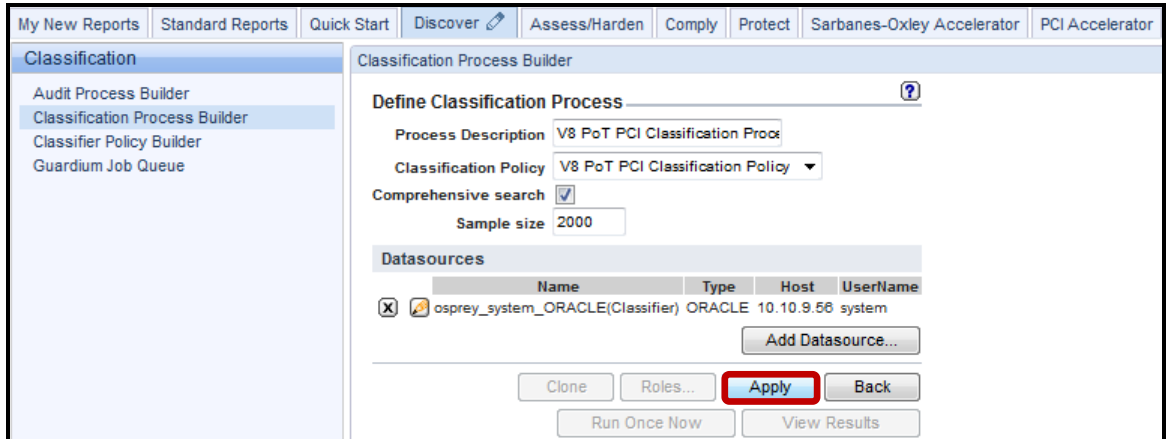
- __d. Click **Add Datasource** to specify which database(s) to search.



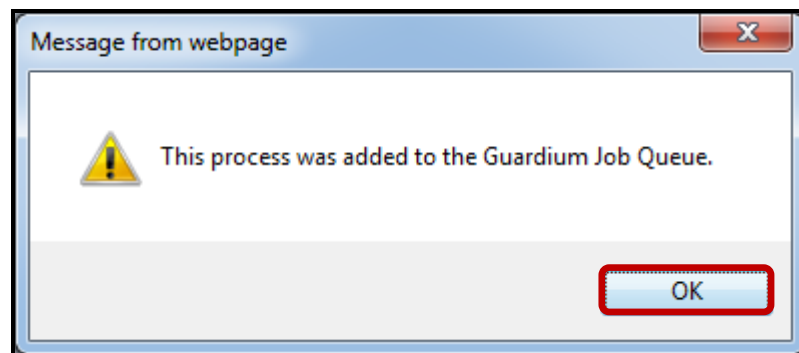
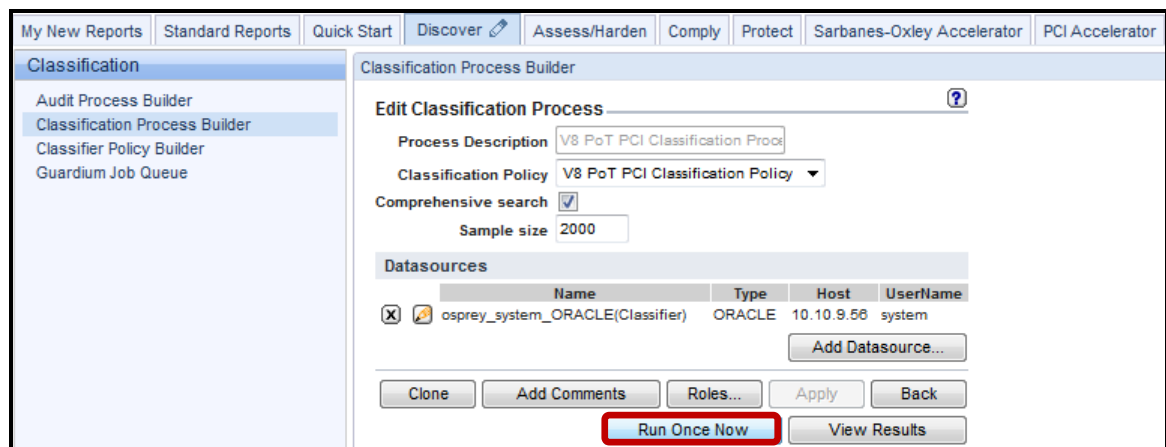
- __e. Select **osprey_system_ORACLE(Classifier)**, and then click **Add**.



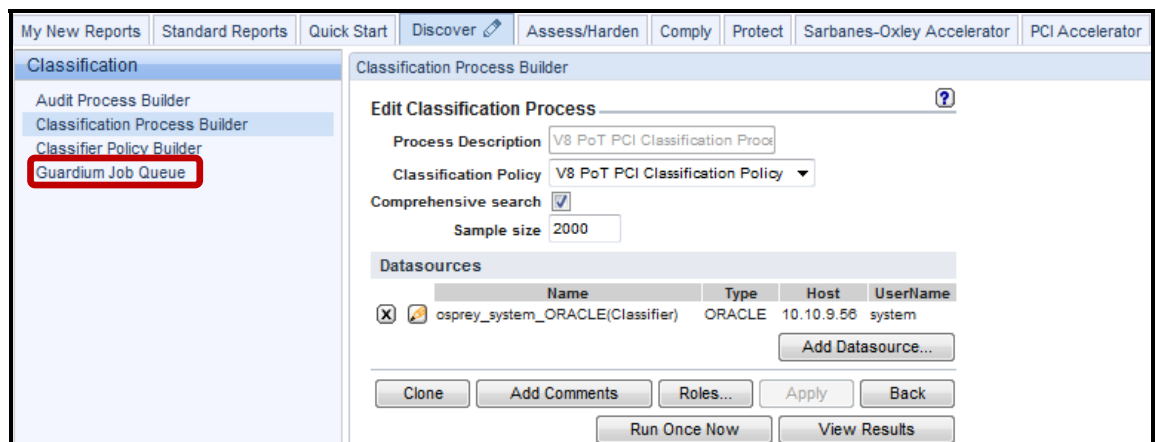
__f. Click **Apply** and then click **OK** to acknowledge.



- __5. Execute the Classification Process and review the results
- __a. Click **Run Once Now**, and then click **OK** to acknowledge.



- __b. Click **Guardium Job Queue** to check the Classification Process job status.



- c. Verify that the job is either waiting in the queue, running, or completed. If you do not see the job listed, then click the **Pencil (edit)** icon at the upper right to modify the time period.

Process Run Id	Process Type	Status	Process Id	Report Result Id	Guardium Job Description	Task Description	Queue Time	Start Time	End Time	Datasources	
1	CLASSIFICATION COMPLETED	20000	1		V8 Pot PCI Classification Process			2012-01-14 15:54:38.0	2012-01-14 15:54:54.0	2012-01-14 15:55:15.0	ORACLE osprey_system

- d. If the job never started, then make sure the **QUERY_FROM_DATE** and **QUERY_TO_DATE** are within the correct time frame. If not, adjust, and then click **Update**.

Customize Portlet

Report: **Guardium Job Queue** Based on Query: **Guardium Job Queue**

Title:

Run Time Parameters

JobEntityDesc: LIKE %

Enter Value for Job Description

QUERY_FROM_DATE: >=

Enter Period From

QUERY_TO_DATE: <=

Enter Period To

REMOTE_SOURCE:

Remote Data Source

SHOW_ALIASES: On Off Default

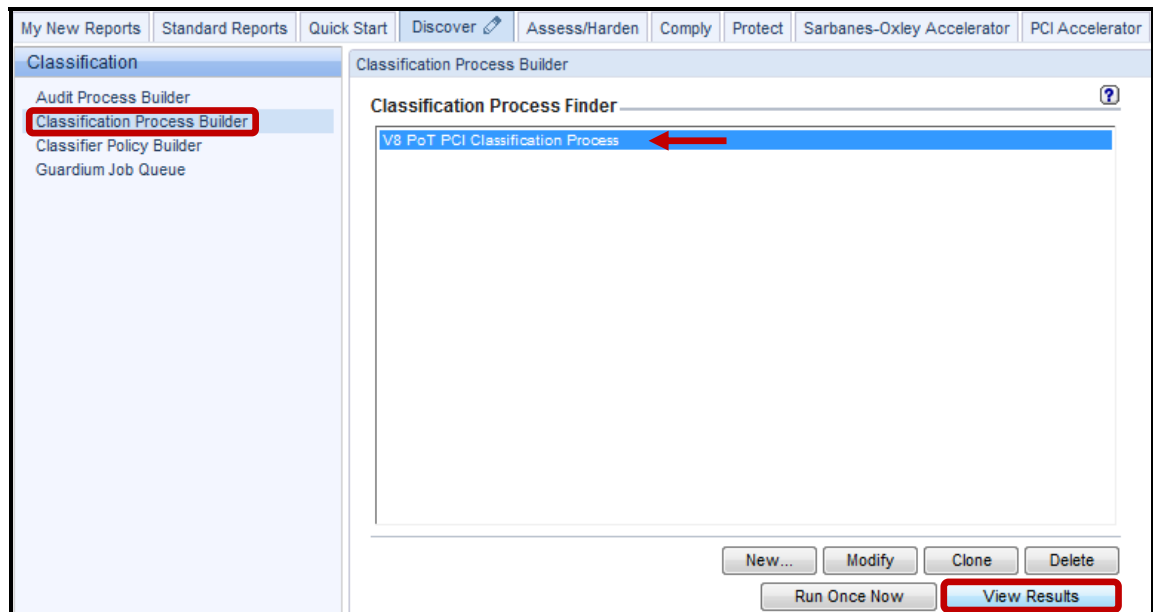
Show Aliases

Presentation Parameters

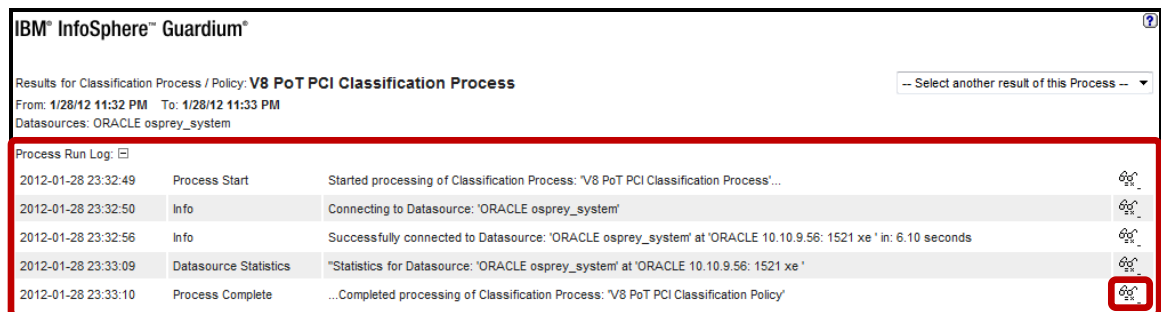
fetchSize: Max. records per page

refreshRate: Refresh rate (seconds)

- __e. Click **Classification Process Builder**, select **V8 PoT PCI Classification Process**, and then click **View Results**.



- __f. The top portion of the report will detail the process steps.



Note: Click on the eyeglasses icon on the far right column for additional details.

Detail ?

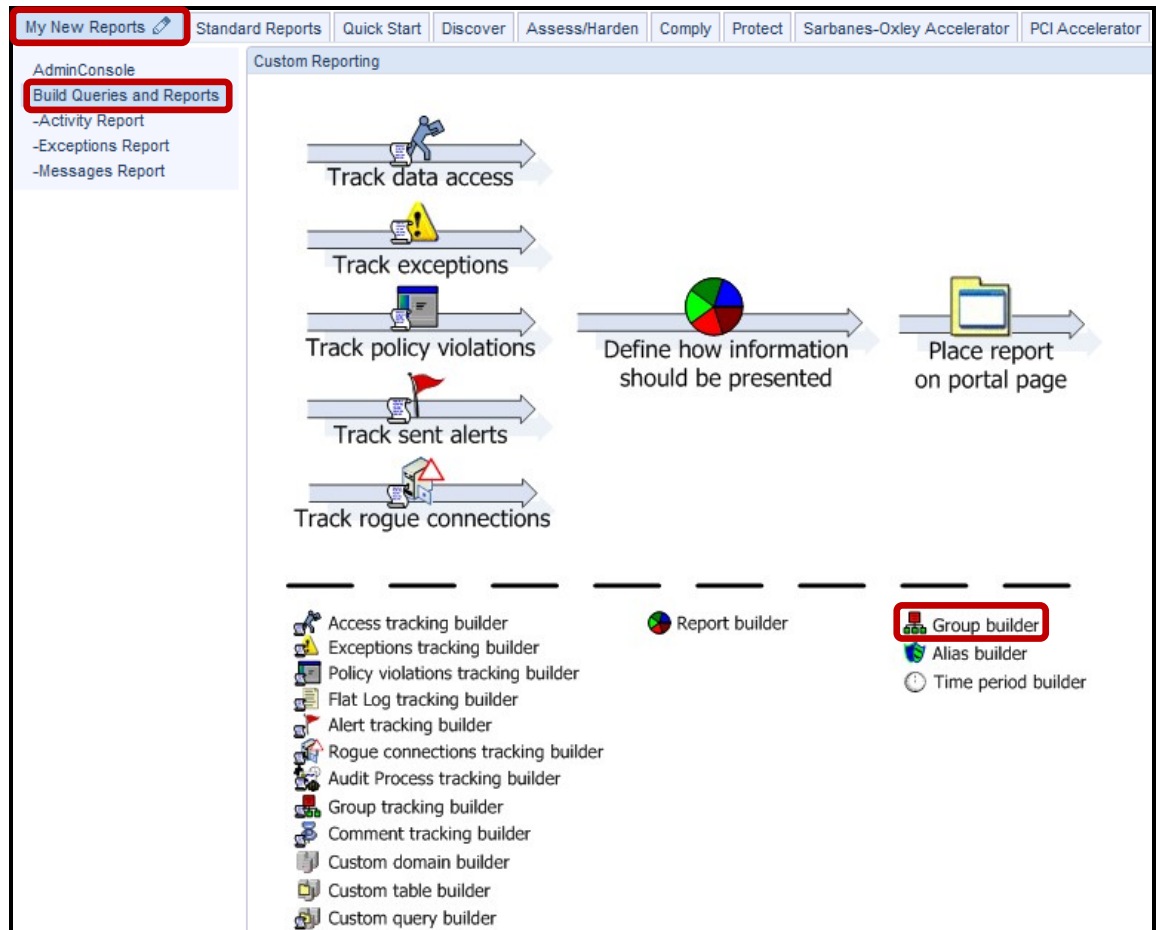
WARN
 Classification Process Run ID: 1
 Classification Process: 'V8 PoT PCI Classification Process'
 Classification Policy: 'V8 PoT PCI Classification Policy'

Started: Sat Jan 28 23:32:48 EST 2012 Ended: Sat Jan 28 23:33:10 EST 2012
 Analyzed: 1 Datasource(s) of (1) type(s)
 ORACLE: (1)
 Evaluated: 4505 Table(s) of (3) type(s)
 VIEW: (2981),SYSTEM TABLE: (841),TABLE: (683)
 Invoked: 12 Action(s) of: (1) type(s)
 Add to Group of Objects: add_to_sensitive_objects: (12)
 Assigned: 12 Category(s) of: (1) type(s)
 PCI: (12)
 Assigned: 12 Classification(s) of (1) type(s).
 CreditCard: (12)
 Encountered: 0 Error(s) of (0) type(s)

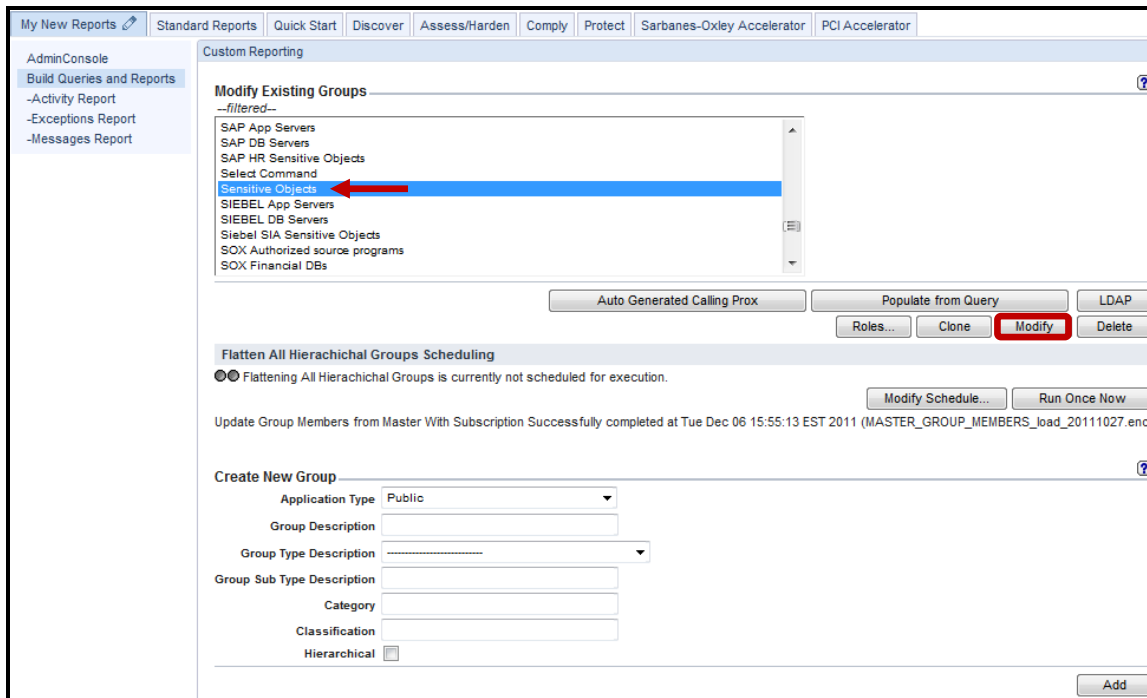
g. The remaining portion of the report will list the entire search results. If you scroll down to the bottom of the report, you will see that a total of 12 records were found. Click 'Close this window' at the bottom left of the report when finished examining the results.

Catalog	Schema	Table Name	Column Name	Rule Description	Comments	Classification Name	Category	Datasource Description
	BENI	CREDITCARD	CARDNUMBER	V8 PoT PCI Classification Rule	Date: Saturday, January 14, 2012 4:19:33 PM EST Datasource: ORACLE 10.10.9.56 :xe Object: BENI.CREDITCARD.CARDNUMBER Category: PCI Classification: 'CreditCard' Rule: Search For Data: V8 PoT PCI Classification Rule TABLE_TYPE=TABLE, DATA_TYPE=TEXT, COLUMN_NAME_LIKE='%CARD%', SEARCH_VALUE_PATTERN=[0-9]{16} Action: Add to Group of Objects: add_to_sensitive_objects Object Group=Sensitive Objects, Replace Group Content='false', Add Member Type=FULLNAME	CreditCard	PCI	osprey_system: ORACLE: 10.10.9.56 :xe : 0
	BENI	LOYALTYTRAND	CREDIT_CARD_NO	V8 PoT PCI Classification Rule	Date: Saturday, January 14, 2012 4:19:33 PM EST Datasource: ORACLE 10.10.9.56 :xe Object: BENI.LOYALTYTRAND.CREDIT_CARD_NO Category: PCI Classification: 'CreditCard' Rule: Search For Data: V8 PoT PCI Classification Rule TABLE_TYPE=TABLE, DATA_TYPE=TEXT, COLUMN_NAME_LIKE='%CARD%', SEARCH_VALUE_PATTERN=[0-9]{16} Action: Add to Group of Objects: add_to_sensitive_objects Object Group=Sensitive Objects, Replace Group Content='false', Add Member Type=FULLNAME	CreditCard	PCI	osprey_system: ORACLE: 10.10.9.56 :xe : 0
	BLL	CREDITCARD	CARDNUMBER	V8 PoT PCI Classification Rule	Date: Saturday, January 14, 2012 4:19:33 PM EST Datasource: ORACLE 10.10.9.56 :xe Object: BLL.CREDITCARD.CARDNUMBER Category: PCI Classification: 'CreditCard' Rule: Search For Data: V8 PoT PCI Classification Rule TABLE_TYPE=TABLE, DATA_TYPE=TEXT, COLUMN_NAME_LIKE='%CARD%', SEARCH_VALUE_PATTERN=[0-9]{16} Action: Add to Group of Objects: add_to_sensitive_objects Object Group=Sensitive Objects, Replace Group Content='false', Add Member Type=FULLNAME	CreditCard	PCI	osprey_system: ORACLE: 10.10.9.56 :xe : 0
	HARRY	CC	CARDNUMBER	V8 PoT PCI Classification Rule	Date: Saturday, January 14, 2012 4:19:36 PM EST Datasource: ORACLE 10.10.9.56 :xe Object: HARRY.CC.CARDNUMBER Category: PCI Classification: 'CreditCard' Rule: Search For Data: V8 PoT PCI Classification Rule TABLE_TYPE=TABLE, DATA_TYPE=TEXT, COLUMN_NAME_LIKE='%CARD%', SEARCH_VALUE_PATTERN=[0-9]{16} Action: Add to Group of Objects: add_to_sensitive_objects Object Group=Sensitive Objects, Replace Group Content='false', Add Member Type=FULLNAME	CreditCard	PCI	osprey_system: ORACLE: 10.10.9.56 :xe : 0
	JOE	BN3SP6MFL2yGaaKDAAG0g+30	CARDNUMBER	V8 PoT PCI Classification Rule	Date: Saturday, January 14, 2012 4:19:30 PM EST Datasource: ORACLE 10.10.9.56 :xe Object: JOE.BN3SP6MFL2yGaaKDAAG0g+30.CARDNUMBER Category: PCI Classification: 'CreditCard' Rule: Search For Data: V8 PoT PCI Classification Rule TABLE_TYPE=TABLE, DATA_TYPE=TEXT, COLUMN_NAME_LIKE='%CARD%', SEARCH_VALUE_PATTERN=[0-9]{16} Action: Add to Group of Objects: add_to_sensitive_objects Object Group=Sensitive Objects, Replace Group Content='false', Add Member Type=FULLNAME	CreditCard	PCI	osprey_system: ORACLE: 10.10.9.56 :xe : 0
	JOE	BN3TTT1ng8bgGaaKDAALVA+30	CARDNUMBER	V8 PoT PCI Classification Rule	Date: Saturday, January 14, 2012 4:19:30 PM EST Datasource: ORACLE 10.10.9.56 :xe Object: JOE.BN3TTT1ng8bgGaaKDAALVA+30.CARDNUMBER Category: PCI Classification: 'CreditCard' Rule: Search For Data: V8 PoT PCI Classification Rule TABLE_TYPE=TABLE, DATA_TYPE=TEXT, COLUMN_NAME_LIKE='%CARD%', SEARCH_VALUE_PATTERN=[0-9]{16} Action: Add to Group of Objects: add_to_sensitive_objects Object Group=Sensitive Objects, Replace Group Content='false', Add Member Type=FULLNAME	CreditCard	PCI	osprey_system: ORACLE: 10.10.9.56 :xe : 0
	JOE	BN3c-ExfDC0zGaaKDAAF+30	CARDNUMBER	V8 PoT PCI Classification Rule	Date: Saturday, January 14, 2012 4:19:36 PM EST Datasource: ORACLE 10.10.9.56 :xe Object: JOE.BN3c-ExfDC0zGaaKDAAF+30.CARDNUMBER Category: PCI Classification: 'CreditCard' Rule: Search For Data: V8 PoT PCI Classification Rule TABLE_TYPE=TABLE, DATA_TYPE=TEXT, COLUMN_NAME_LIKE='%CARD%', SEARCH_VALUE_PATTERN=[0-9]{16} Action: Add to Group of Objects: add_to_sensitive_objects Object Group=Sensitive Objects, Replace Group Content='false', Add Member Type=FULLNAME	CreditCard	PCI	osprey_system: ORACLE: 10.10.9.56 :xe : 0
	JOE	BN3c-FinG0mwVYgGaaKDAIq+30	CARDNUMBER	V8 PoT PCI Classification Rule	Date: Saturday, January 14, 2012 4:19:38 PM EST Datasource: ORACLE 10.10.9.56 :xe Object: JOE.BN3c-FinG0mwVYgGaaKDAIq+30.CARDNUMBER Category: PCI Classification: 'CreditCard' Rule: Search For Data: V8 PoT PCI Classification Rule TABLE_TYPE=TABLE, DATA_TYPE=TEXT, COLUMN_NAME_LIKE='%CARD%', SEARCH_VALUE_PATTERN=[0-9]{16} Action: Add to Group of Objects: add_to_sensitive_objects Object Group=Sensitive Objects, Replace Group Content='false', Add Member Type=FULLNAME	CreditCard	PCI	osprey_system: ORACLE: 10.10.9.56 :xe : 0
	JOE	CREDITCARD	CARDNUMBER	V8 PoT PCI Classification Rule	Date: Saturday, January 14, 2012 4:19:36 PM EST Datasource: ORACLE 10.10.9.56 :xe Object: JOE.CREDITCARD.CARDNUMBER Category: PCI Classification: 'CreditCard' Rule: Search For Data: V8 PoT PCI Classification Rule TABLE_TYPE=TABLE, DATA_TYPE=TEXT, COLUMN_NAME_LIKE='%CARD%', SEARCH_VALUE_PATTERN=[0-9]{16} Action: Add to Group of Objects: add_to_sensitive_objects Object Group=Sensitive Objects, Replace Group Content='false', Add Member Type=FULLNAME	CreditCard	PCI	osprey_system: ORACLE: 10.10.9.56 :xe : 0

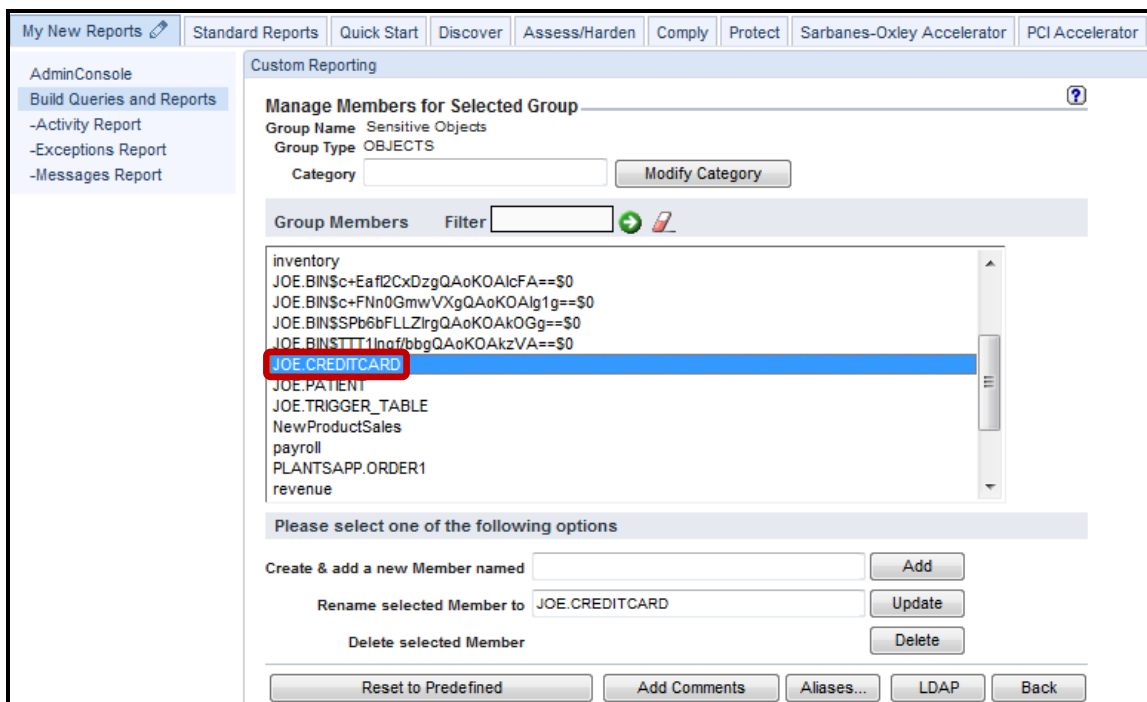
- ___6. Now let's check to see if the **Sensitive Objects** group was populated with the 12 newly discovered objects.
 - ___a. Click **Build Queries and Reports** under the **My New Reports** tab, and then click **Group builder**.



- __b. Scroll down the *Modify Existing Groups* dropdown list and select **Sensitive Objects**, and then click **Modify**.



- __c. As an example, notice that the group member '**JOE.CREDITCARD**' was automatically added by the Classifier process. This group can be referenced in a policy rule and subsequent Classifier executions can automatically maintain this group. Refer back to the beginning of this lab to compare the current group members to those in its initial state.



Thank You

2.2 Configuring “Fire only with” Marker (Optional)

Overview

The "Fire only with" Marker allows for Classifier rule types to be grouped under one common name. In addition, the entire set of rules will be logged and have their actions invoked **only if** all rules fire on the same table. Conversely, if any single rule does not fire on a table, then none of the other rules will be logged nor have their actions invoked.

Being able to have multiple rules fire together becomes important when you care about sensitive data appearing together within the same table. For example, your company may need to comply with Massachusetts Privacy Law (201 CMR 17), which requires the protection of database tables containing a Massachusetts resident's name combined with any of a social security number, a Massachusetts driver's license, or a financial account number such as a credit or debit card number.

“Fire only with” Markers require at least two rules searching data within the same table name. The "Fire only with" Marker must have the exact same value across rules within the same group. This means that if one rule has a marker of ABC, then the other rules in the group must have a marker of the same identical name. Any discrepancy in the marker value among rules invalidates the grouping.

The "Fire only with" Marker requires all members of the group to match in order to take action. As an example, if a group contains four rules, and rule #3 does not match, then no results will be returned regardless of whether the other three rules matched. This is because "Fire only with" Markers require that all rules match in order for the entire group of rules be logged and their actions to be invoked.

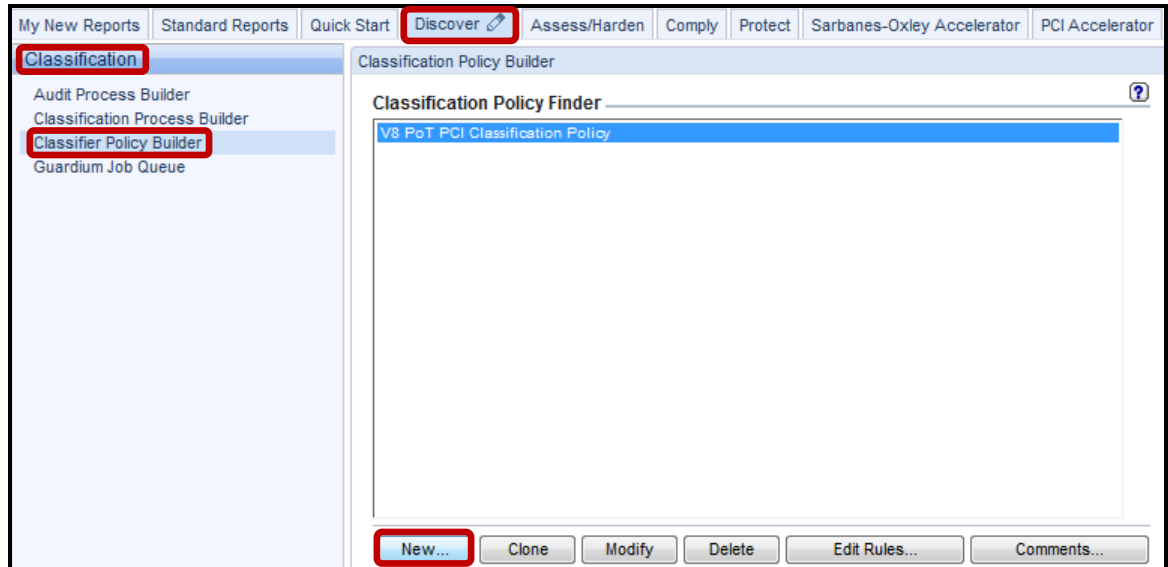
Objectives

In this lab you will learn how to:

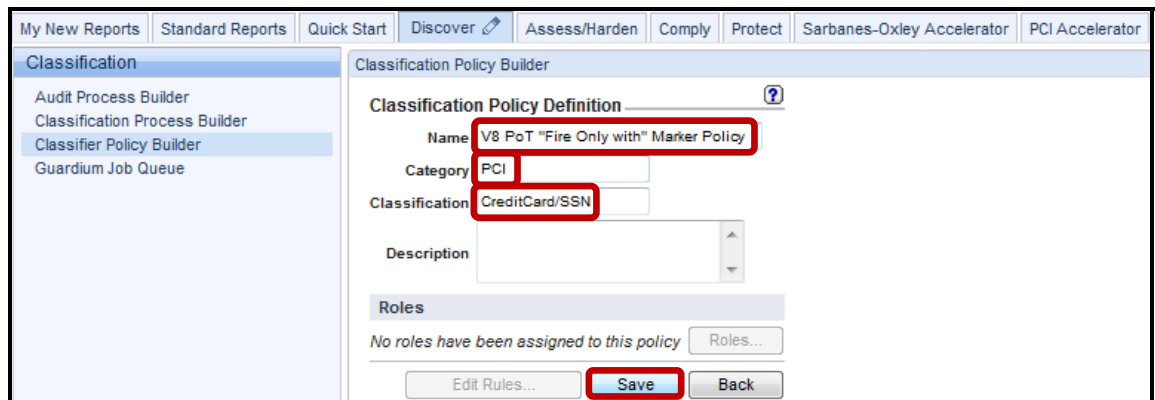
- __1. Define a Classification Policy using “Fire only with” Markers
- __2. Run the scan
- __3. View the results

__1. Illustrate how the **Fire only with marker** option works

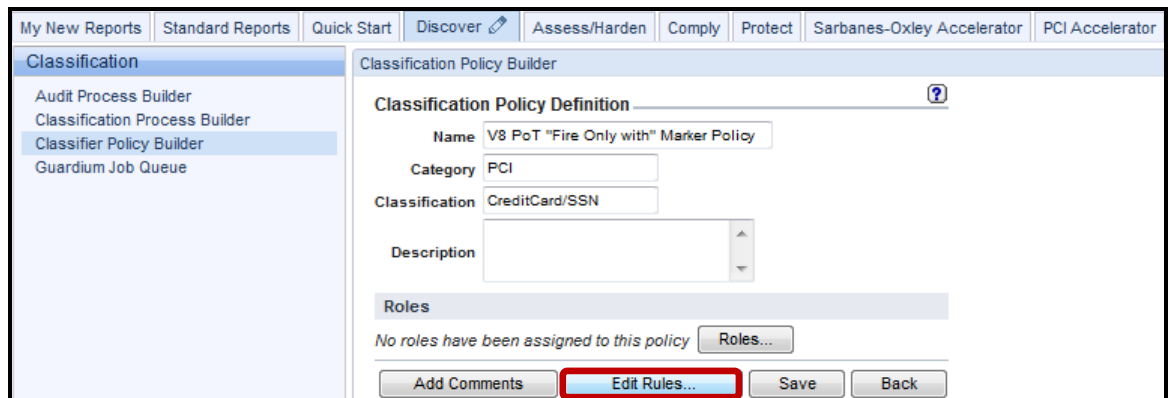
__a. Click **Classifier Policy Builder** under the **Discover->Classification** tabs, and then click **New**.



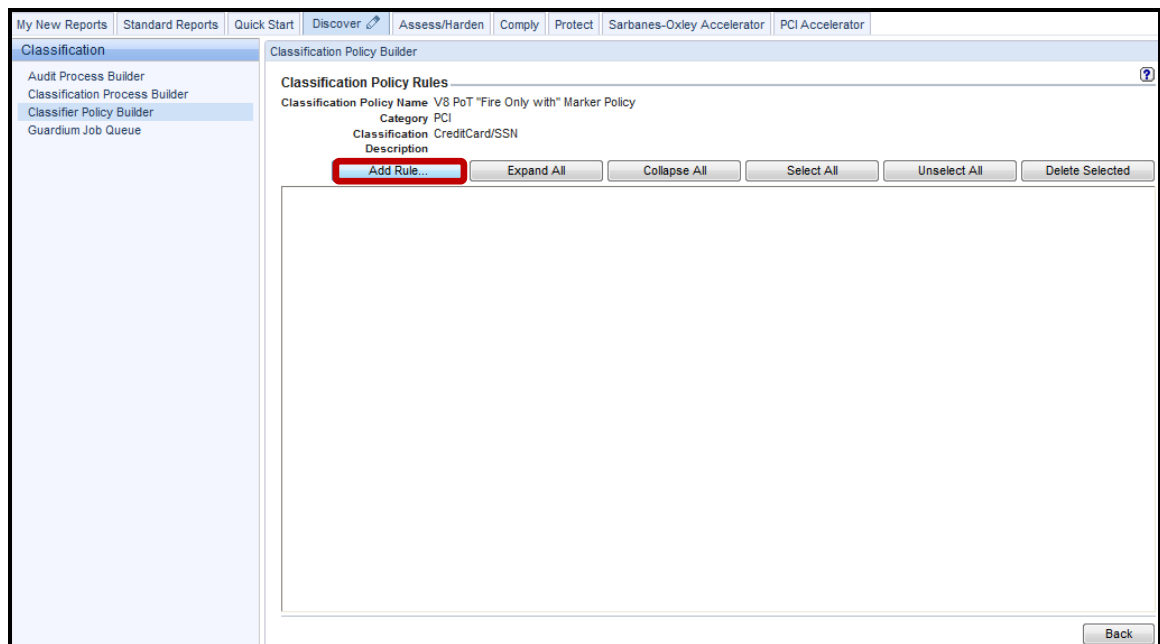
__b. Enter '**V8 PoT "Fire only with" Marker Policy**' in the *Name* field, '**PCI**' in the *Category* field, '**CreditCard/SSN**' in the *Classification* field, and then click **Save**.



__c. Click **Edit Rules**.



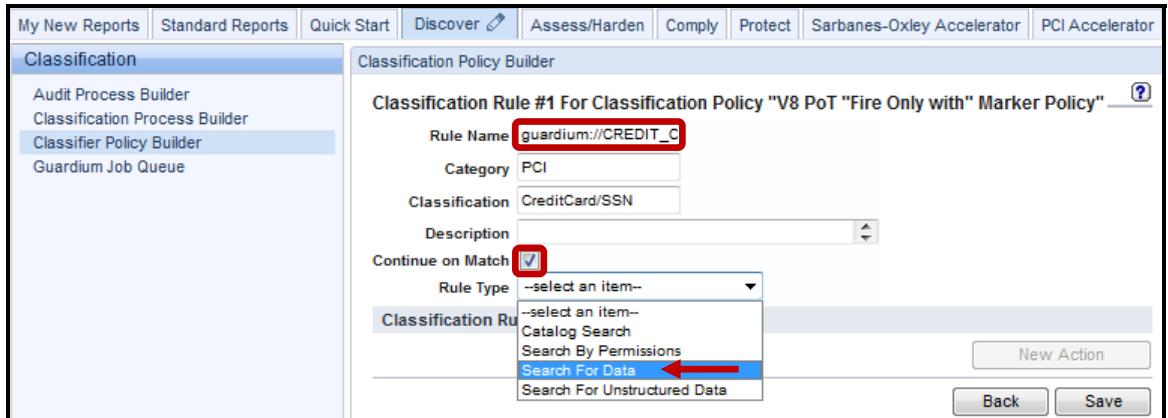
__d. Click **Add Rule**.



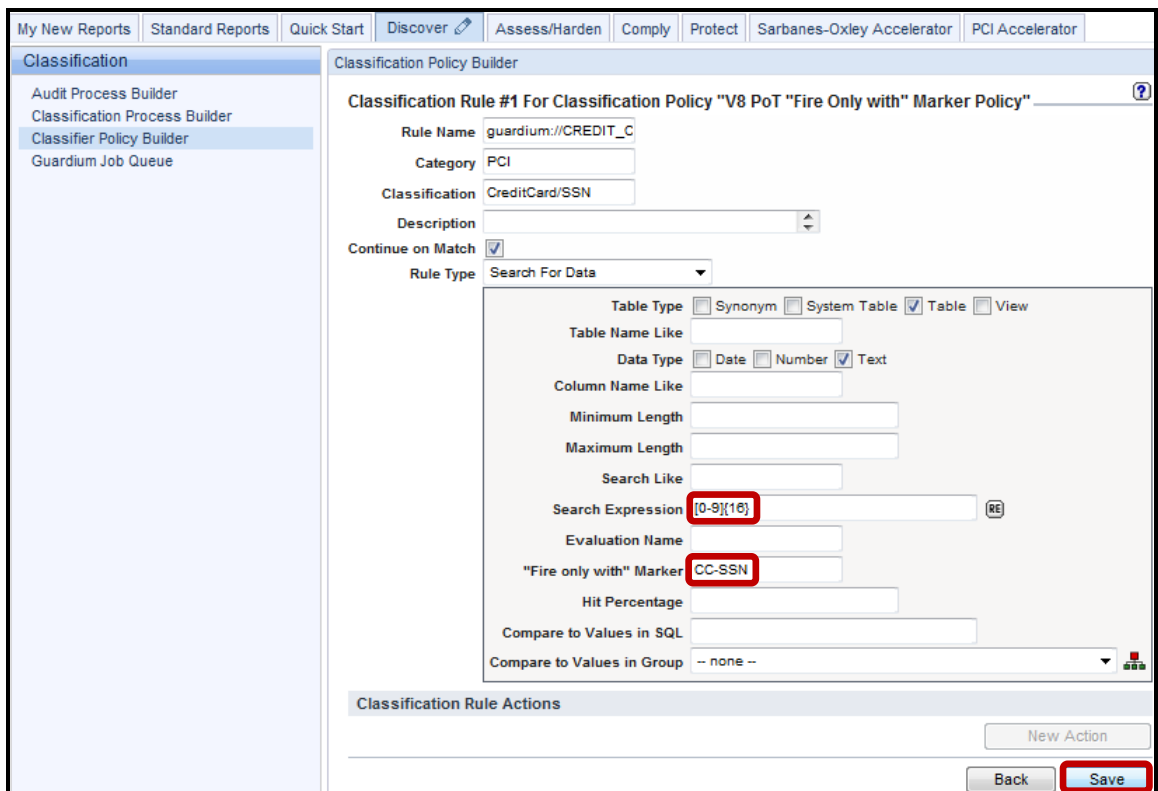
- e. Enter **'guardium://CREDIT_CARD'** in the *Rule Name* field, check the **Continue on Match** checkbox, then expand the *Rule Type* dropdown list, and select **Search For Data**.

Note: When a rule name begins with the special pattern, **'guardium://CREDIT_CARD'**, combined with a valid credit card number pattern in the Search Expression box, the classification policy will use the **Luhn algorithm** (for credit card number validation) in addition to the standard pattern matching.

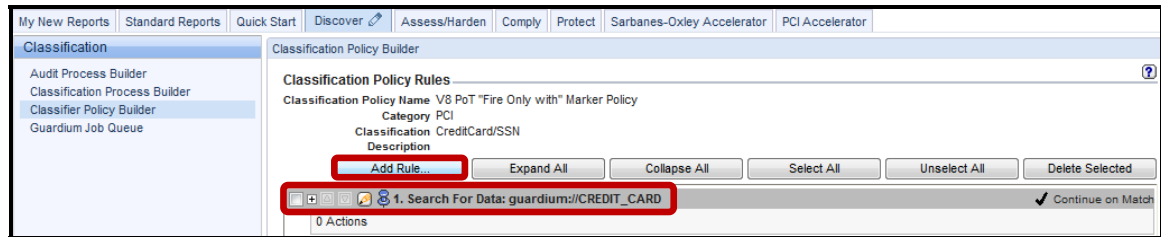
Note: Both the **guardium://CREDIT_CARD** rule name and a valid **[0-9]{16}** number in the Search Expression box **Must Be Present** to activate the Luhn algorithm validation.



- f. Enter **[0-9]{16}** in the *Search Expression* field, **CC-SSN** in the *"Fire only with" Marker* field and then click **Save**.

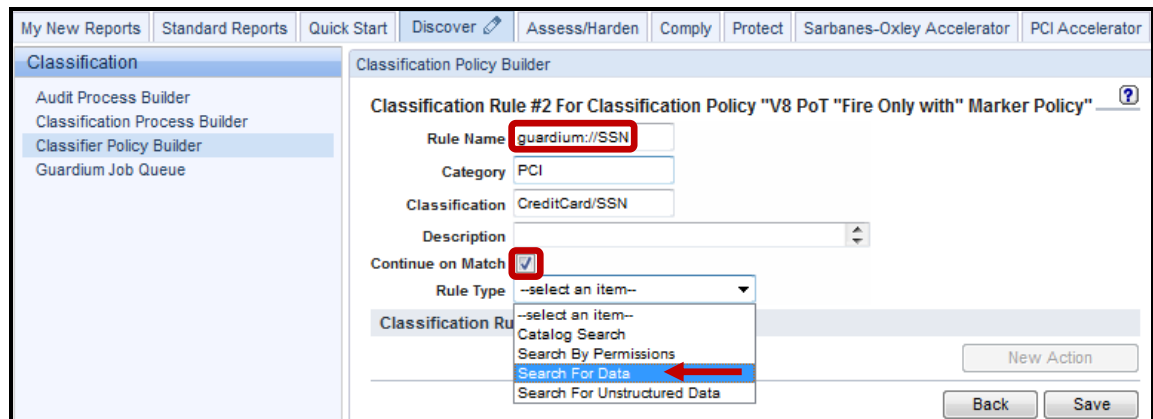


- __g. Verify that the Rule has been added and click **Add Rule** to add a second rule.

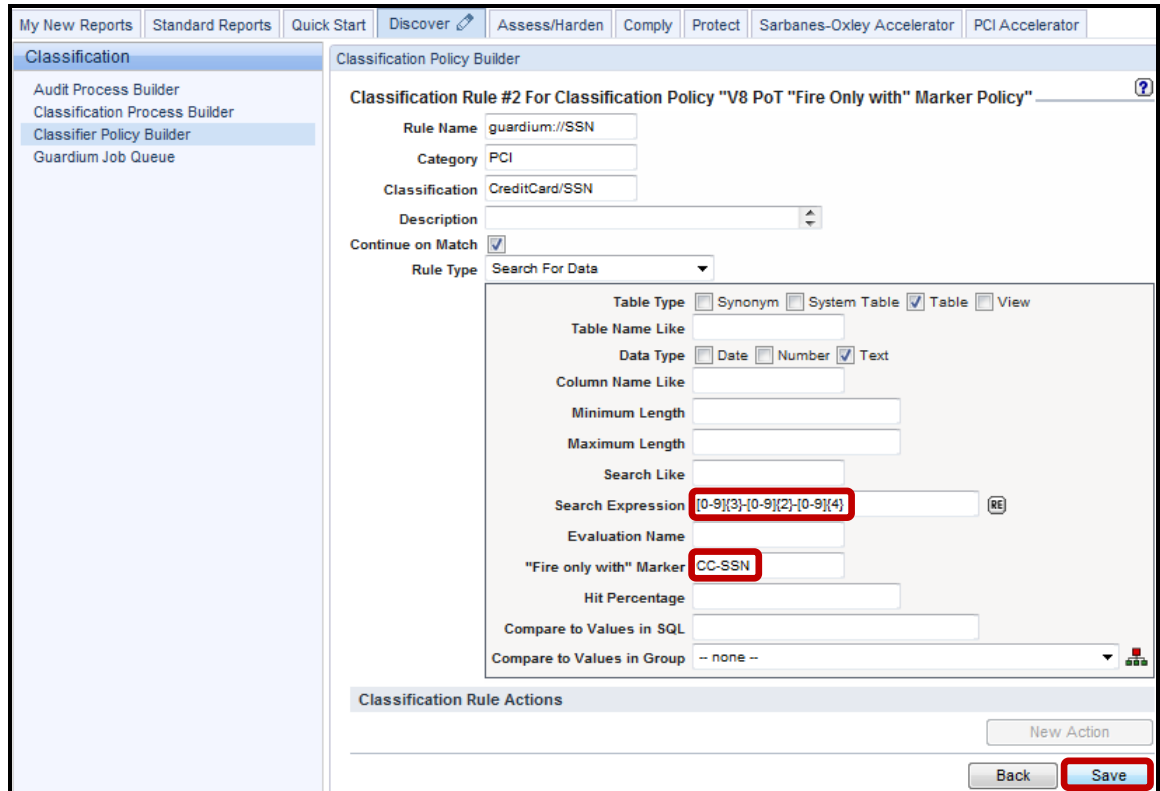


- __h. Enter '**guardium://SSN**' in the *Rule Name* field, check the **Continue on Match** checkbox, then expand the *Rule Type* dropdown list, and select **Search For Data**.

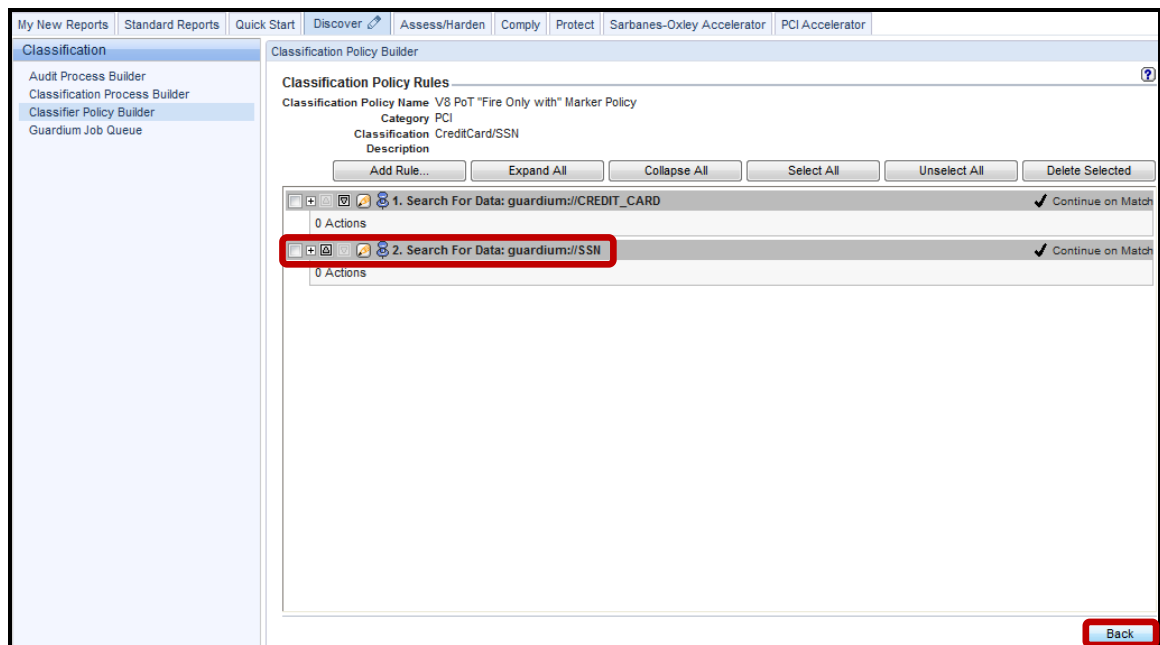
Note: Similar to the previous rule, when a rule name begins with the special pattern, '**guardium://SSN**', combined with a valid Social Security number pattern in the Search Expression box, the classification policy will use an SSN validation algorithm in addition to the standard pattern matching.



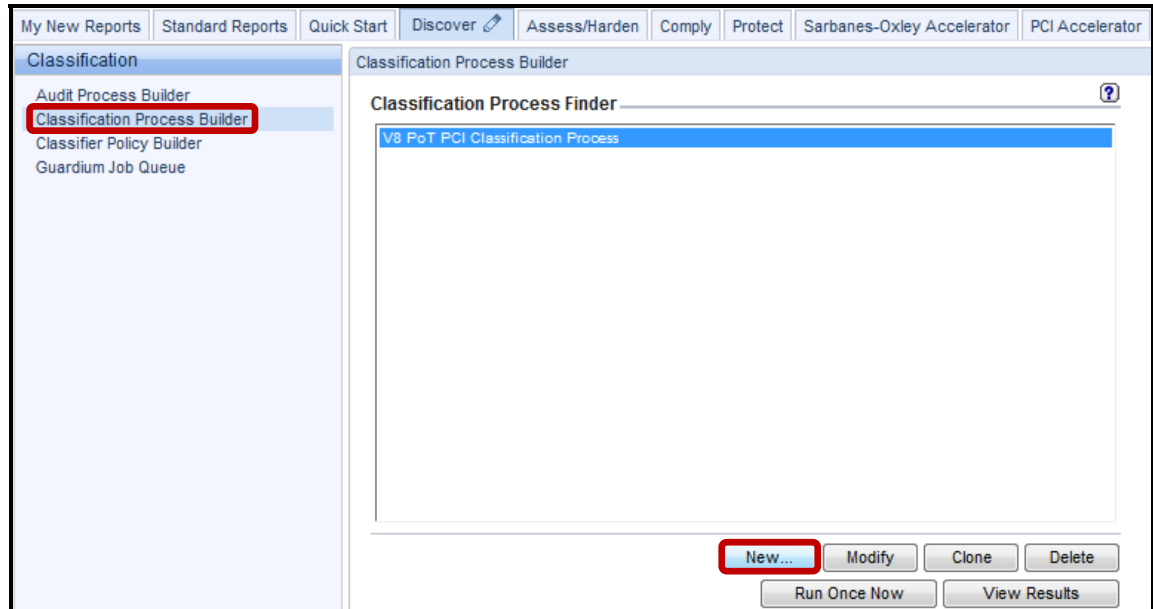
- i. Enter **[0-9]{3}-[0-9]{2}-[0-9]{4}** in the *Search Expression* field, **CC-SSN** in the “*Fire only with*” Marker field and then click **Save**. The Marker **Must Be Identical** for all rules.



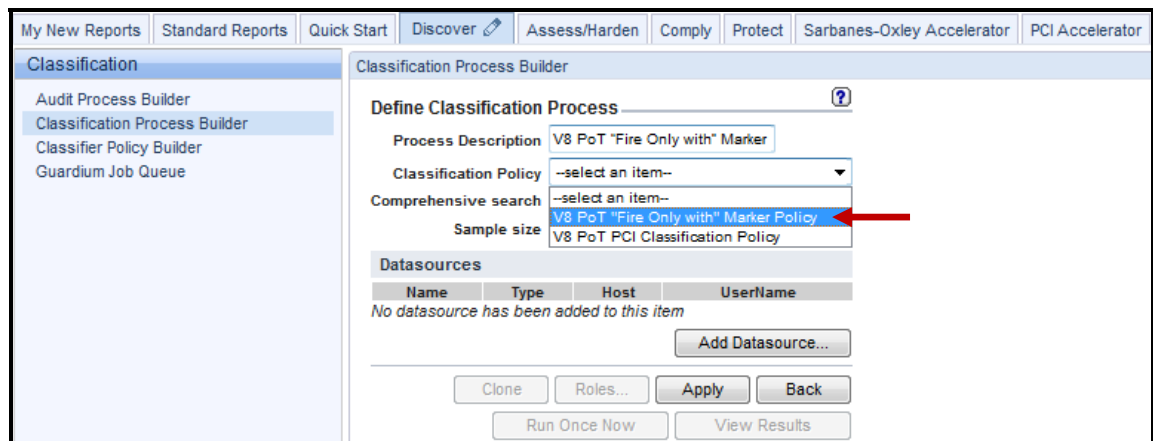
- j. Verify that the second rule has been added and click **Back**.



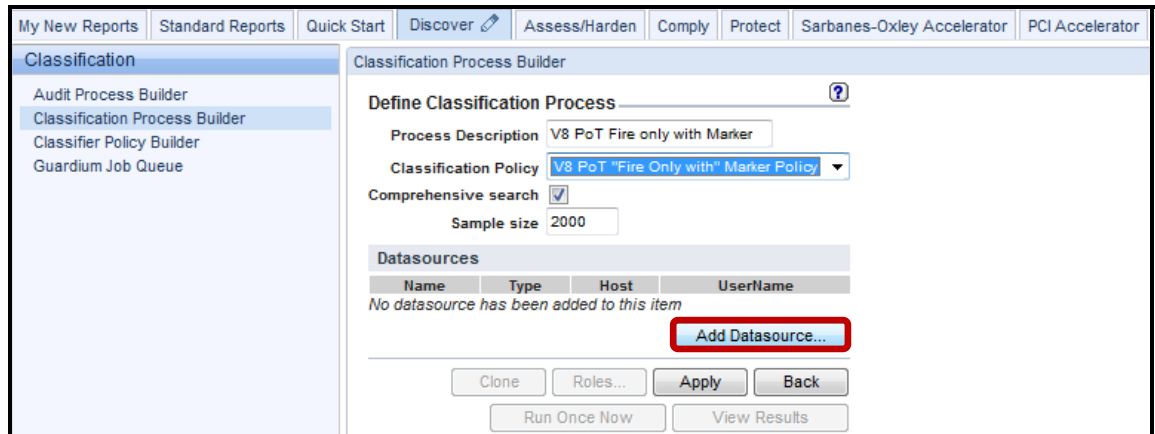
- __2. Create a Classification Process to run the Classifier Policy
- __a. Click **Classification Process Builder**, and then click **New** to create a Classification Process for running the *Classifier Policy* that was just created.



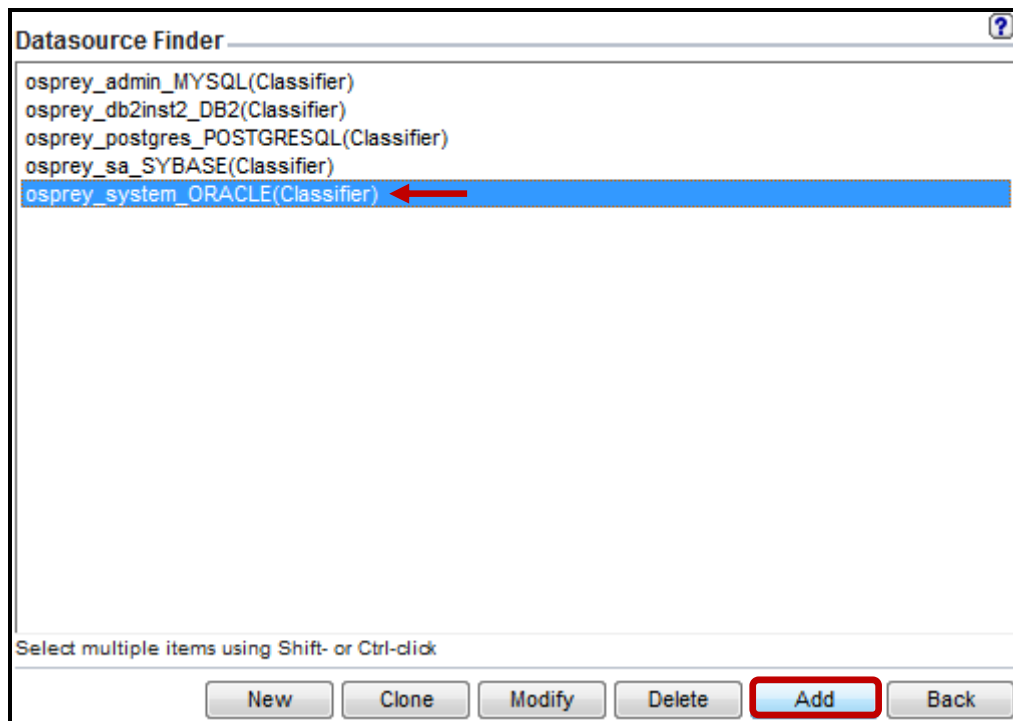
- __b. Enter '**V8 PoT Fire only with Marker**' for *Process Description*.
- __c. Expand the *Classification Policy* dropdown list and select the policy previously created, **V8 PoT "Fire Only with" Marker Policy**.



__d. Click **Add Datasource** to specify which database(s) to search.



__e. Select **osprey_system_ORACLE(Classifier)**, and then click **Add**.



__f. Click **Apply** and then click **OK** to acknowledge.

Classification Process Builder

Define Classification Process ?

Process Description: V8 PoT Fire only with Marker

Classification Policy: V8 PoT "Fire Only with" Marker Policy

Comprehensive search:

Sample size: 2000

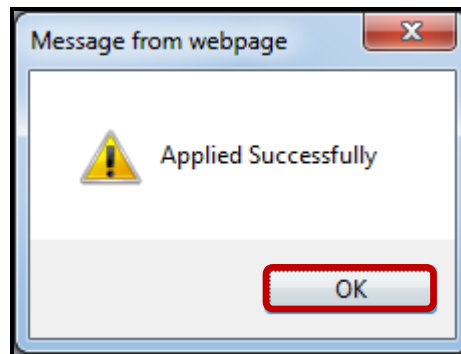
Datasources

	Name	Type	Host	UserName
<input checked="" type="checkbox"/>	osprey_system_ORACLE(Classifier)	ORACLE	10.10.9.56	system

Add Datasource...

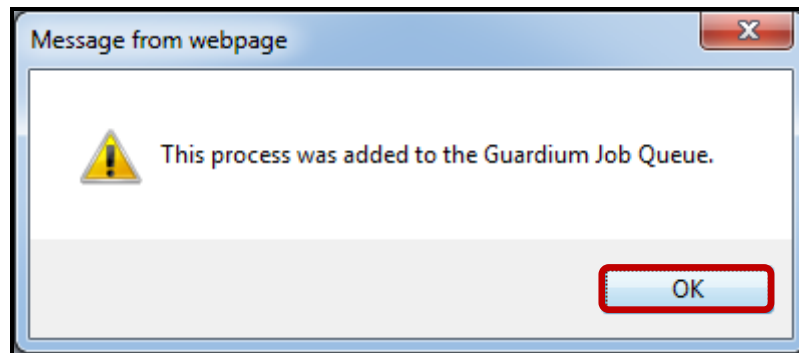
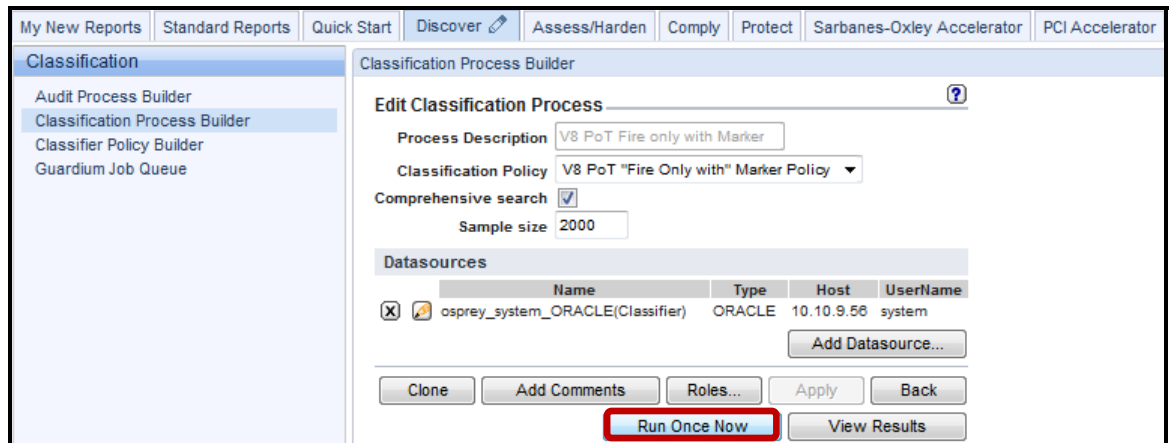
Clone Roles... **Apply** Back

Run Once Now View Results

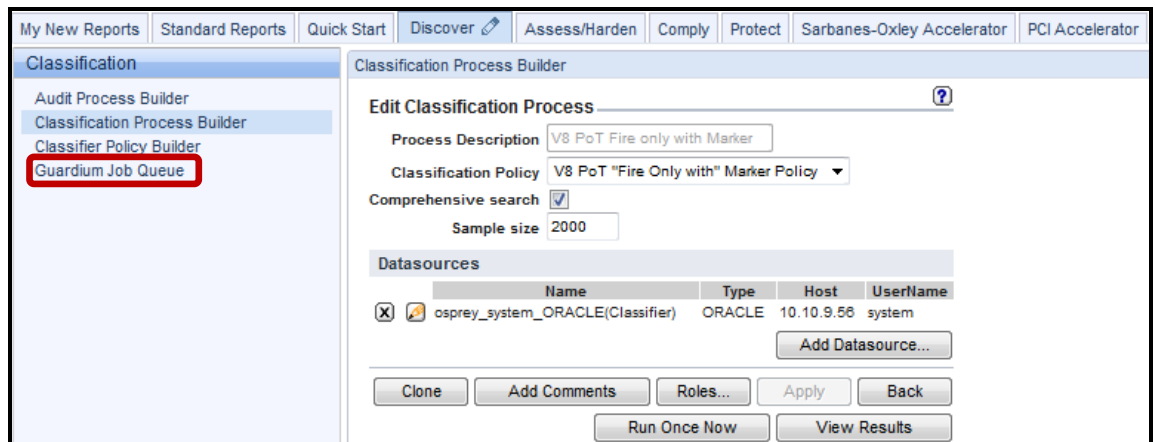


__3. Run the Classification Process and review the results

__a. Click **Run Once Now**, and then click **OK** to acknowledge.



__b. Click **Guardium Job Queue** to check job status.



- c. Verify that the job is either waiting in the queue, running, or completed. If you do not see the job listed, then click the **Pencil (edit)** icon at the upper right to modify the time period.

Process Run Id	Process Type	Status	Process Id	Report Result Id	Guardium Job Description	Task Description	Queue Time	Start Time	End Time	Datasources	
2	CLASSIFICATION COMPLETED	20001	2		V8 Pot Fire only with Marker			2012-01-14 17:12:52.0	2012-01-14 17:13:32.0	2012-01-14 17:14:10.0	ORACLE osprey_system
1	CLASSIFICATION COMPLETED	20000	1		V8 Pot PCI Classification Process			2012-01-14 16:47:00.0	2012-01-14 16:47:31.0	2012-01-14 16:47:50.0	ORACLE osprey_system

- d. If the job never started, then make sure the **QUERY_FROM_DATE** and **QUERY_TO_DATE** are within the correct time frame. If not, adjust, and then click **Update**.

Customize Portlet

Report: **Guardium Job Queue** Based on Query: **Guardium Job Queue**

Title:

Run Time Parameters

JobEntityDesc:

Enter Value for Job Description

QUERY_FROM_DATE

Enter Period From

QUERY_TO_DATE

Enter Period To

REMOTE_SOURCE:

Remote Data Source

SHOW_ALIASES: On Off Default

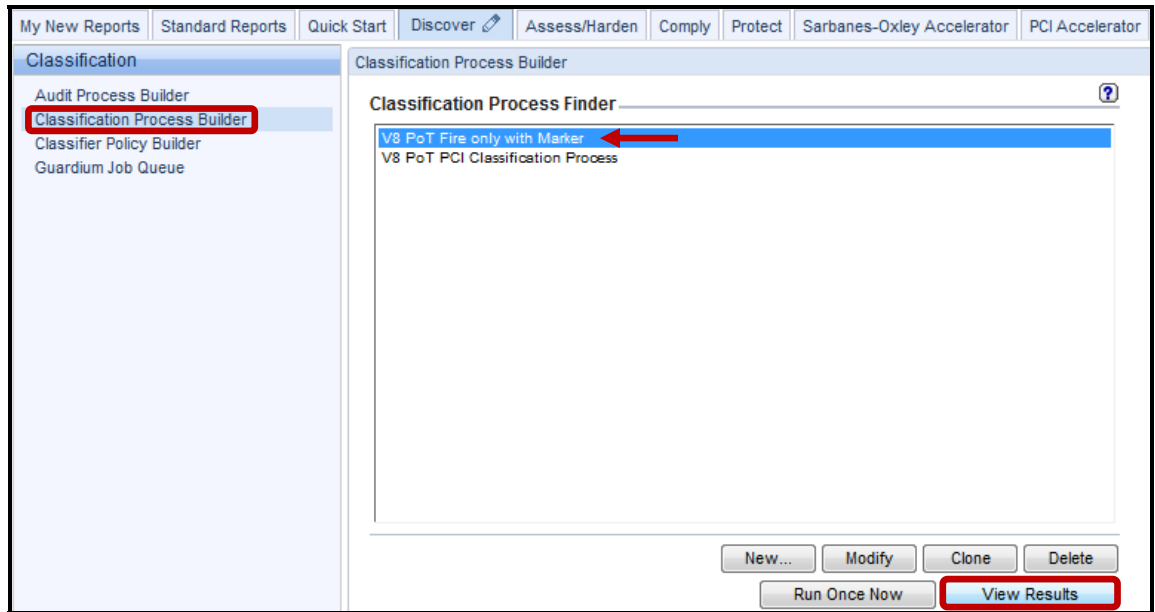
Show Aliases

Presentation Parameters

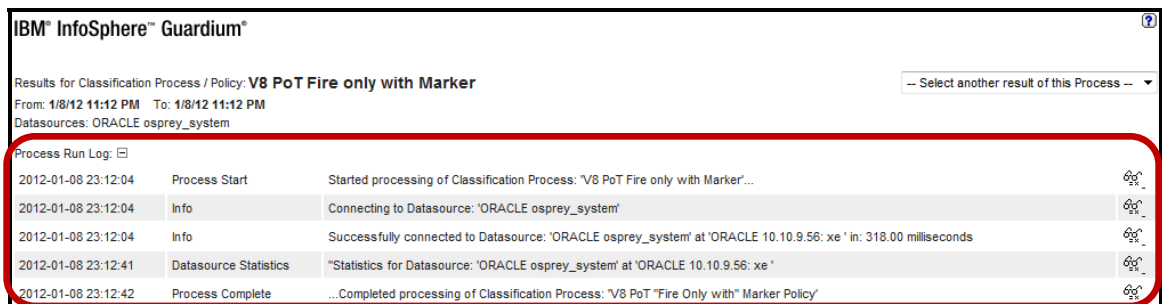
fetchSize: Max. records per page

refreshRate: Refresh rate (seconds)

- __e. From the *Classification Pane* click **Classification Process Builder**, select **V8 PoT Fire only with Marker**, and then click **View Results**.



- __f. The top portion of the report will detail the process steps.



- g. The remaining portion of the report will list the entire search results. If you scroll down to the bottom of the report, you will see that a total of six records were found. Click **Close this window** at the bottom left of the report when finished examining the results.

Note: Several tables including **JOE.PATIENT** have both Credit Card and SSN fields.

Report details: horizontal vertical Show original values Use Aliases

Catalog	Schema	Table Name	Column Name	Rule Description	Comments	Classification Name	Category	Datasource Description
	JOE	BIN\$c-EaI2Cx2z9QAoKOAlcFA==50	CARDNUMBER	guardium://CREDIT_CARD	Date: Sunday, January 8, 2012 11:12:29 PM EST Datasource: ORACLE 10.10.9.56 : xe Object: JOE BIN\$c-EaI2Cx2z9QAoKOAlcFA==50 CARDNUMBER Category: PCI Classification: 'CreditCard/SSN' Rule: Search For Data: guardium://CREDIT_CARD TABLE_TYPE=TABLE; DATA_TYPE=TEXT; SEARCH_VALUE_PATTERN=[0-9]{16}; EVALUATE_GROUP_MARKER=CC-SSN	CreditCard/SSN	PCI	osprey_system : ORACLE : 10.10.9.56 : xe :: 0 :
	JOE	BIN\$c-EaI2Cx2z9QAoKOAlcFA==50	SSN	guardium://SSN	Date: Sunday, January 8, 2012 11:12:29 PM EST Datasource: ORACLE 10.10.9.56 : xe Object: JOE BIN\$c-EaI2Cx2z9QAoKOAlcFA==50 SSN Category: PCI Classification: 'CreditCard/SSN' Rule: Search For Data: guardium://SSN TABLE_TYPE=TABLE; DATA_TYPE=TEXT; SEARCH_VALUE_PATTERN=[0-9]{3}-[0-9]{2}-[0-9]{4}; EVALUATE_GROUP_MARKER=CC-SSN	CreditCard/SSN	PCI	osprey_system : ORACLE : 10.10.9.56 : xe :: 0 :
	JOE	BIN\$c-FIn0GmwVXgQAoKOAlg1g==50	CARDNUMBER	guardium://CREDIT_CARD	Date: Sunday, January 8, 2012 11:12:29 PM EST Datasource: ORACLE 10.10.9.56 : xe Object: JOE BIN\$c-FIn0GmwVXgQAoKOAlg1g==50 CARDNUMBER Category: PCI Classification: 'CreditCard/SSN' Rule: Search For Data: guardium://CREDIT_CARD TABLE_TYPE=TABLE; DATA_TYPE=TEXT; SEARCH_VALUE_PATTERN=[0-9]{16}; EVALUATE_GROUP_MARKER=CC-SSN	CreditCard/SSN	PCI	osprey_system : ORACLE : 10.10.9.56 : xe :: 0 :
	JOE	BIN\$c-FIn0GmwVXgQAoKOAlg1g==50	SSN	guardium://SSN	Date: Sunday, January 8, 2012 11:12:29 PM EST Datasource: ORACLE 10.10.9.56 : xe Object: JOE BIN\$c-FIn0GmwVXgQAoKOAlg1g==50 SSN Category: PCI Classification: 'CreditCard/SSN' Rule: Search For Data: guardium://SSN TABLE_TYPE=TABLE; DATA_TYPE=TEXT; SEARCH_VALUE_PATTERN=[0-9]{3}-[0-9]{2}-[0-9]{4}; EVALUATE_GROUP_MARKER=CC-SSN	CreditCard/SSN	PCI	osprey_system : ORACLE : 10.10.9.56 : xe :: 0 :
	JOE	PATIENT	CARDNUMBER	guardium://CREDIT_CARD	Date: Sunday, January 8, 2012 11:12:29 PM EST Datasource: ORACLE 10.10.9.56 : xe Object: JOE PATIENT CARDNUMBER Category: PCI Classification: 'CreditCard/SSN' Rule: Search For Data: guardium://CREDIT_CARD TABLE_TYPE=TABLE; DATA_TYPE=TEXT; SEARCH_VALUE_PATTERN=[0-9]{16}; EVALUATE_GROUP_MARKER=CC-SSN	CreditCard/SSN	PCI	osprey_system : ORACLE : 10.10.9.56 : xe :: 0 :
	JOE	PATIENT	SSN	guardium://SSN	Date: Sunday, January 8, 2012 11:12:29 PM EST Datasource: ORACLE 10.10.9.56 : xe Object: JOE PATIENT SSN Category: PCI Classification: 'CreditCard/SSN' Rule: Search For Data: guardium://SSN TABLE_TYPE=TABLE; DATA_TYPE=TEXT; SEARCH_VALUE_PATTERN=[0-9]{3}-[0-9]{2}-[0-9]{4}; EVALUATE_GROUP_MARKER=CC-SSN	CreditCard/SSN	PCI	osprey_system : ORACLE : 10.10.9.56 : xe :: 0 :

Select All Unselect All Adhoc Action

Records: 1 To 6 Of 6

Close this window Download PDF

Thank You

Sensitive Data Finder review

- __1. The Sensitive Data Finder process runs on:
- __a. The InfoSphere Guardium Collector
 - __b. The database server
 - __c. The client PC
 - __d. A network switch
- __2. Only one Classifier process may be defined for each Guardium system.
(**True** or **False**)
- __3. If a table name wildcard is entered, but not a column name, then:
- __a. No columns in the table will be scanned
 - __b. All columns in the table will be scanned
 - __c. Only column names that match the table name wildcard will be scanned
- __4. Regular expressions are very flexible, but are not good at matching patterns such as:
- __a. Exactly 16 numbers
 - __b. Three uppercase letters, followed by three to six numbers
 - __c. Telephone numbers
 - __d. Name fields
- __5. Regular expressions can be useful for finding people names.
(**True** or **False**)
- __6. By default, how many rows are returned for each table that is scanned
- __a. 2,000
 - __b. 50
 - __c. 1
 - __d. All

Sensitive Data Finder review (Answers)

__1. The Sensitive Data Finder process runs on:

A – The InfoSphere Guardium Collector.

__2. Only one Classifier process may be defined for each Guardium system.
(True or False)

False.

__3. If a table name wildcard is entered, but not a column name, then:

B – All columns in the table will be scanned.

__4. Regular expressions are very flexible, but are not good at matching patterns such as:

D – Name fields.

__5. Regular expressions can be useful for finding people names.
(True or False)

False.

__6. By default, how many rows are returned for each table that is scanned

A – 2,000.

Lab 3 Entitlement Reports

3.1 Exploring Entitlement Reports

Overview

IBM InfoSphere Guardium Entitlement Reports provide a simple means of aggregating and understanding database entitlements throughout the organization. It is configured to scan all selected databases in your infrastructure on a scheduled basis, automatically collecting information on user rights, including those granted through roles and group membership. This eliminates the time-consuming process of examining each database, as well as the need to step through cascading roles (roles granted to roles) in each database to develop a true understanding of entitlements. It also enables collection of this information on a frequent, systematic basis without the use of scarce technical resources, providing timely, accurate information that will enhance your security posture and satisfy the needs of auditors, while reducing operational costs.

In recent years organizations have struggled to cope with rapidly escalating database information growth. Among the challenges associated with this trend is implementing effective data protection measures. Given the broad range of privileges available, the growth in user accounts and objects and the complexity of managing cascading roles, this has required significant labor.

Increasingly, dynamic organizations are changing roles and responsibilities more frequently than ever. Mergers and acquisitions are creating distributed, multivendor database infrastructures in which database administrators (DBAs) must cope with varying vendor entitlement models and numerous distinct systems. As a result, it has become extremely difficult to ensure that database privileges are restricted so that sensitive objects and system rights are not inappropriately exposed. This creates not only a data protection issue, but also a compliance issue.

Auditors validating compliance with major mandates require regular reviews (sometimes referred to as database-user rights-attestation reporting) to ensure that user entitlements are regularly adjusted to align with changes in personnel status, responsibilities and actual usage. Will you be better able to keep your organization safe knowing who has what database privileges?

Objectives

This lab will illustrate how to set up and view IBM InfoSphere Guardium's predefined database Entitlement (privilege) Reports. These reports will have up-to-date "snapshots" of database users and their privileges. We will use both GUI and Guardium API (GrdAPI) methods to produce these reports.

- __1. Use existing database datasources capable of extracting entitlements attributes.
- __2. Upload data into IBM InfoSphere Guardium's predefined database entitlement (privilege) data structures using the Enterprise Integrator (Custom Domain) feature of Guardium.
- __3. View the results and verify that the entitlement data was populated and appears in the Entitlements Standard Reports.

- __1. Using the IBM InfoSphere Guardium GUI, demonstrate the ease of use within the IBM InfoSphere Guardium solution. Start the IBM InfoSphere Guardium appliance and log in.
- __a. From your laptop, browse to <https://10.10.9.248:8443>
- __b. Login as **pot / guardium**.

Login

Please enter your information

User name:

Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

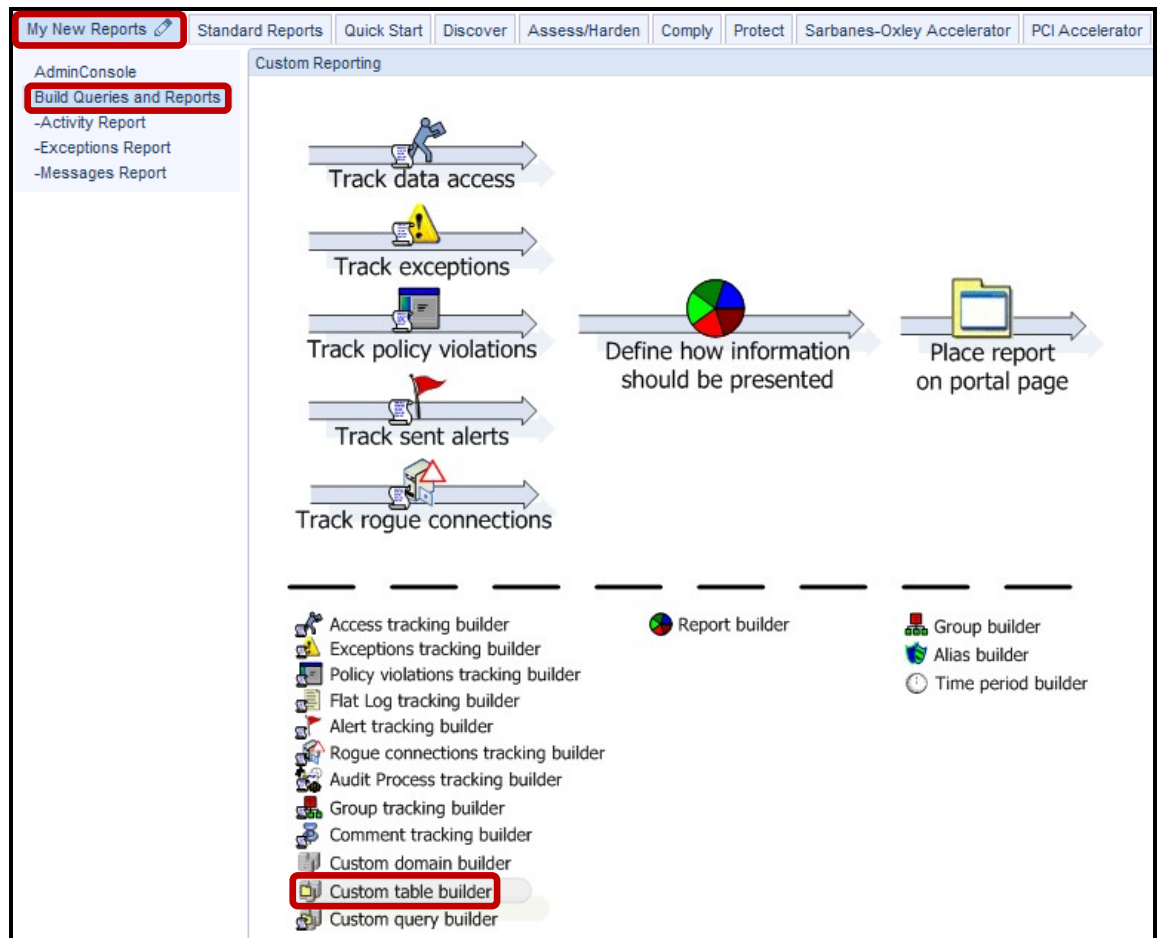
Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistrykey © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

__2. Configure an Oracle Custom table and Upload Entitlement data.

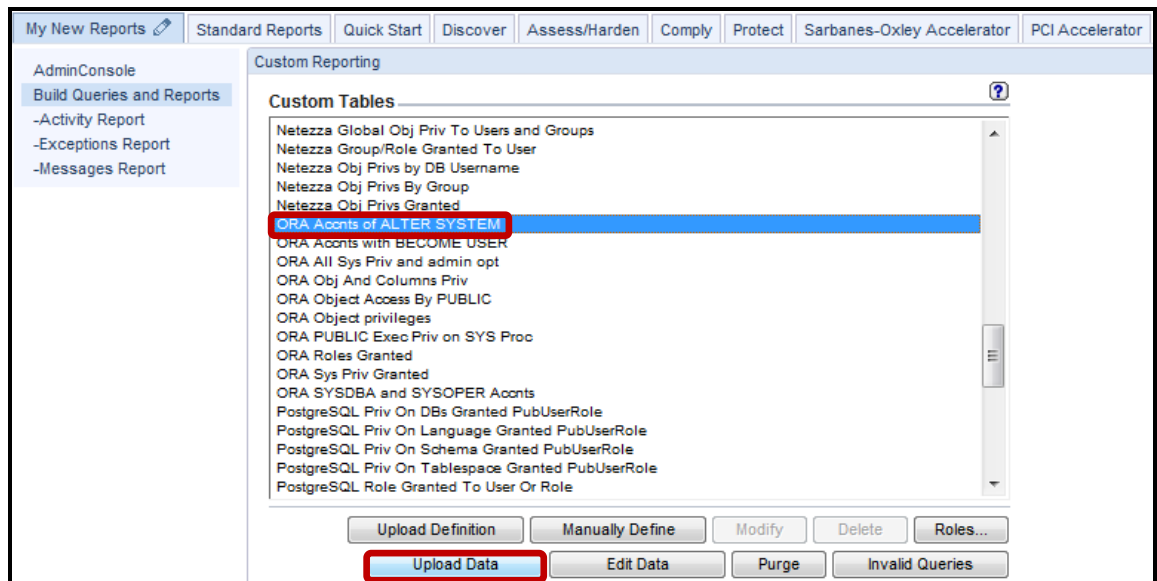
- __a. Click **Build Queries and Reports** under the **My New Reports** tab, and then click **Custom table builder**.

Our goal here is to upload entitlement data into built-in entitlement reports. This will also entail assigning datasources to the entitlement reports so that entitlement privileges can be collected from the monitored database.



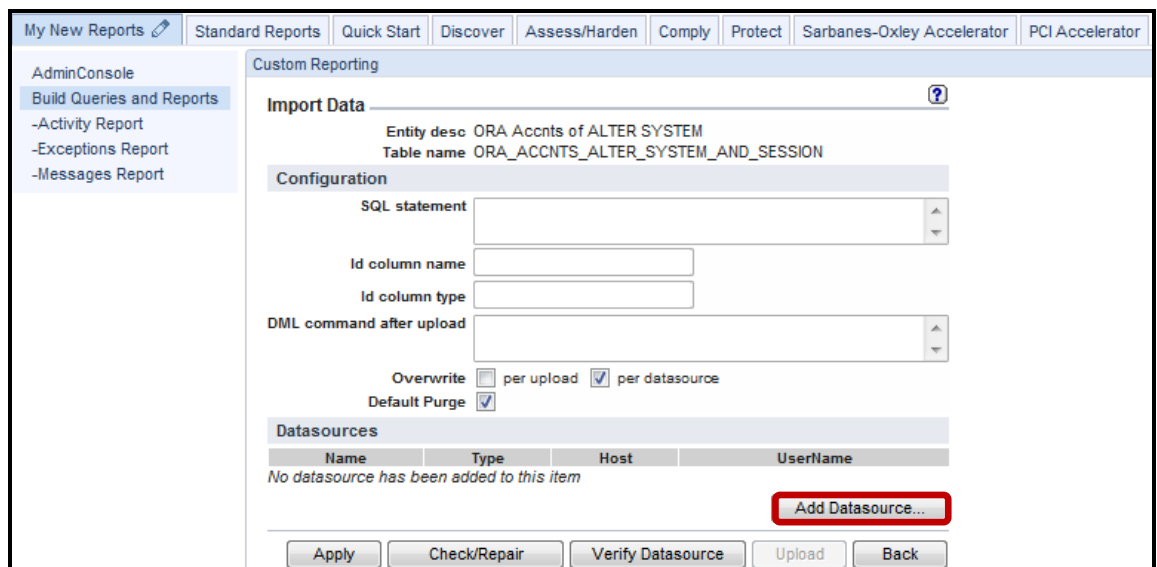
We will start with Oracle Entitlements

- __b. Scroll down the list, click ORA Accnts of ALTER SYSTEM, and then click Upload Data.



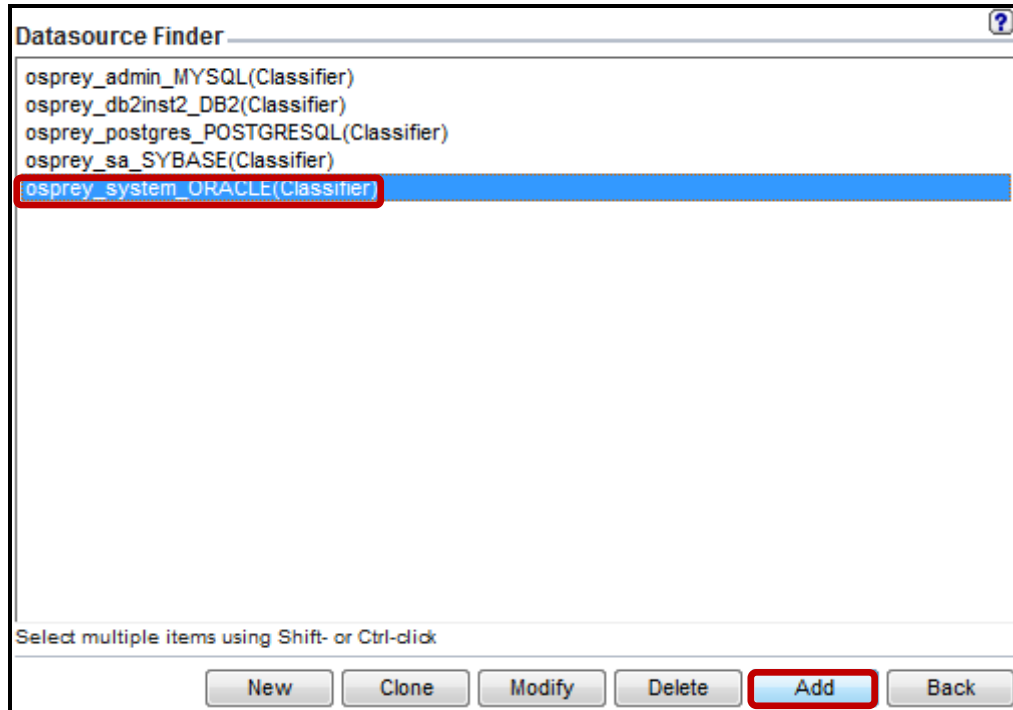
An Import Data screen will appear to allow us to associate one or multiple datasources.

- __c. Click **Add Datasource**.



- __d. Select **osprey_system_ORACLE(Classifier)** as the datasource, and click **Add**.

Note: At this point, you are generally required to click **New** to create a new datasource, but for the purposes of this lab, datasources have already been created. To learn how to create a new datasource, please refer to the product documentation or online help.



__e. Click **Apply**.

The screenshot shows the 'Import Data' configuration page in the IBM Security Center for Reporting. The page is titled 'Custom Reporting' and 'Import Data'. It displays the following information:

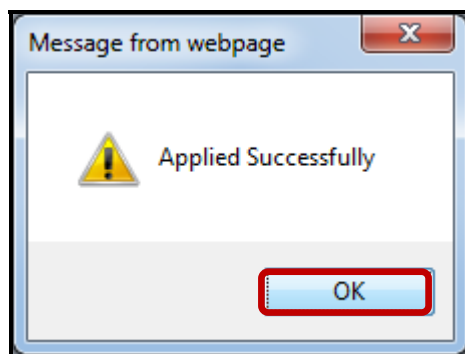
- Entity desc:** ORA Accnts of ALTER SYSTEM
- Table name:** ORA_ACCNTS_ALTER_SYSTEM_AND_SESSION
- Configuration:**
 - SQL statement:** (Empty text area)
 - Id column name:** (Empty text area)
 - Id column type:** (Empty text area)
 - DML command after upload:** (Empty text area)
 - Overwrite:** per upload, per datasource
 - Use default schedule:**
 - Default Purge:**
- Datasources:**

Name	Type	Host	UserName
osprey_system_ORACLE(Classifier)	ORACLE	10.10.9.56	system
- Scheduling:**
 - Upload is currently not scheduled for execution.
 - (Unselected)

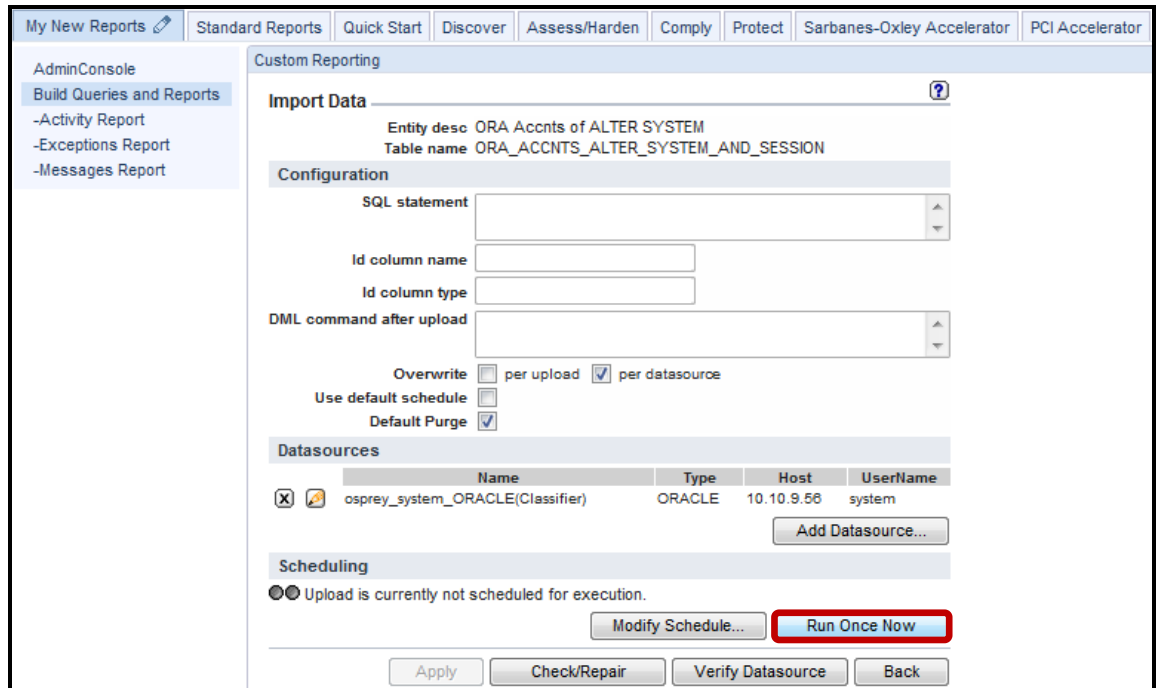
At the bottom of the page, there are several buttons: 'Apply' (highlighted with a red box), 'Check/Repair', 'Verify Datasource', and 'Back'.

Note: It is a good practice to perform **Verify Datasource** at this point, but that step is not necessary for this lab.

__f. Click **OK** to acknowledge that the Apply was successful.

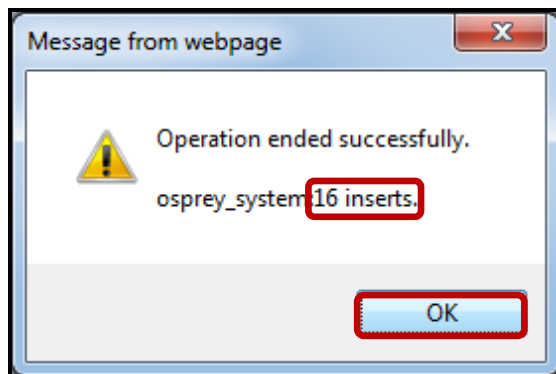


__g. Click **Run Once Now**.

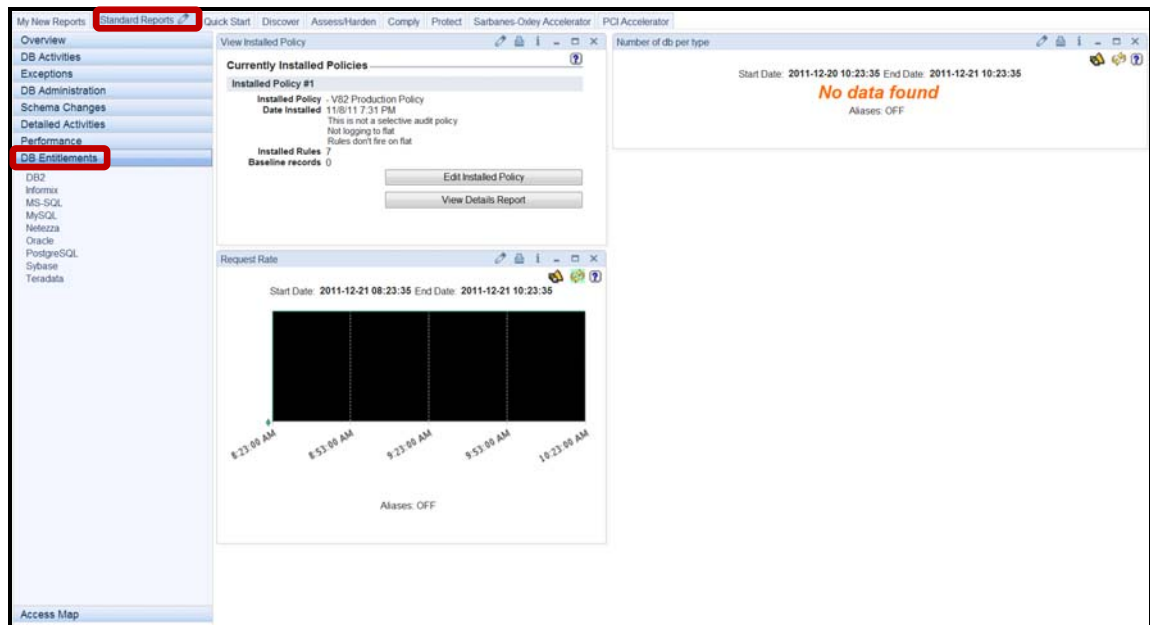


Note: The 'Operation ended successfully' dialog box includes a count of inserts of Oracle users with the Alter System privilege. Shortly, you will see that the number of inserts received will match the number of lines in the corresponding Entitlement Report.

__h. Click **OK** to acknowledge the successful insert operation.

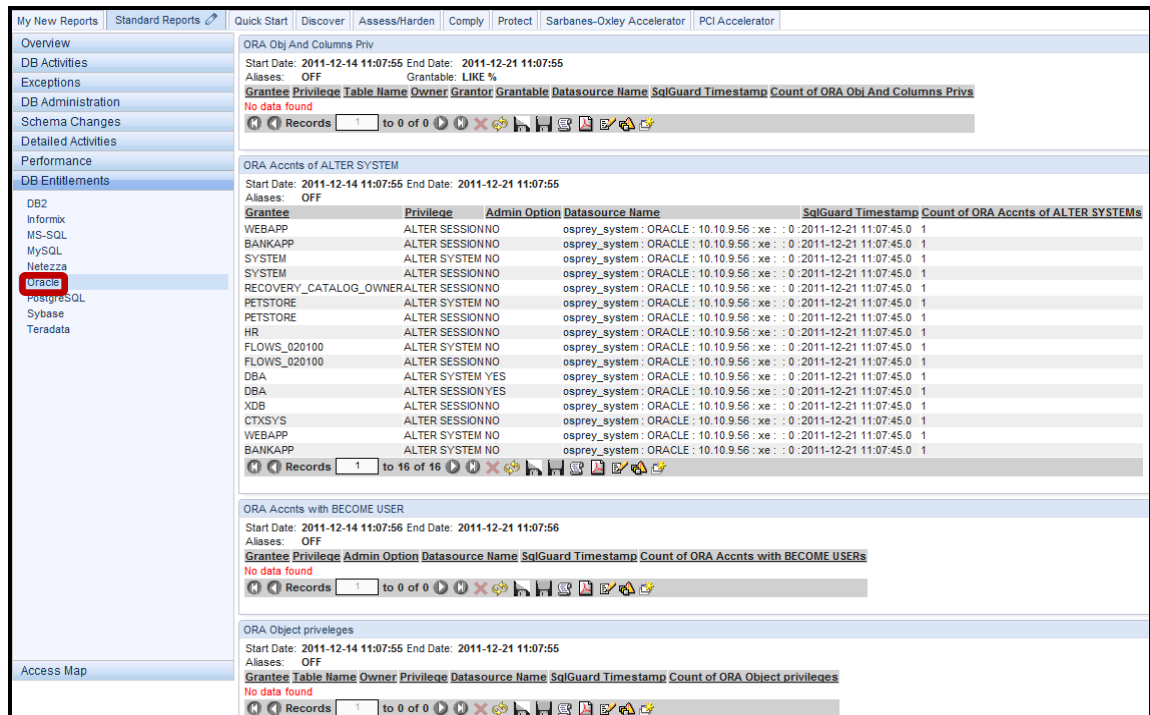


- ___3. Verify that Oracle Entitlement Report has been populated.
 - ___a. Click **DB Entitlements** under the **Standard Reports** tab.



- ___b. Click **Oracle**.

Note: Most of the reports show 'No data found' since we have yet to complete the steps to upload the other Oracle DB Entitlement data.

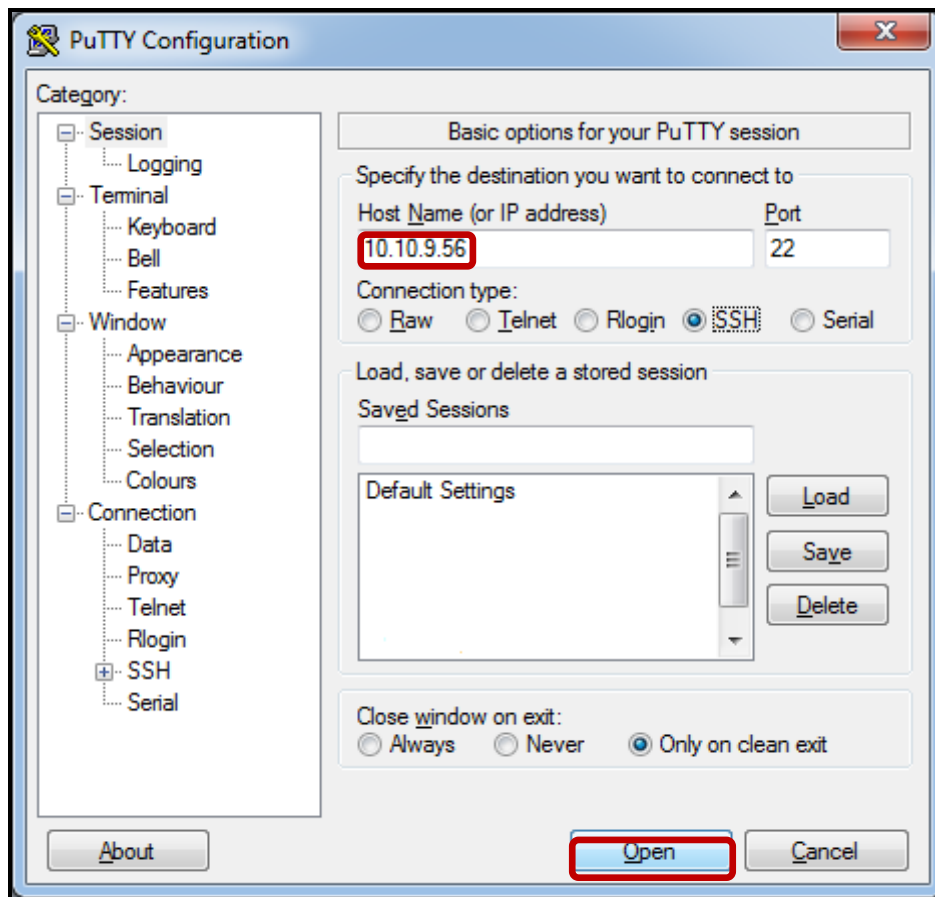


__4. Automatically configure custom tables, and upload DB Entitlement data with GrdAPI.

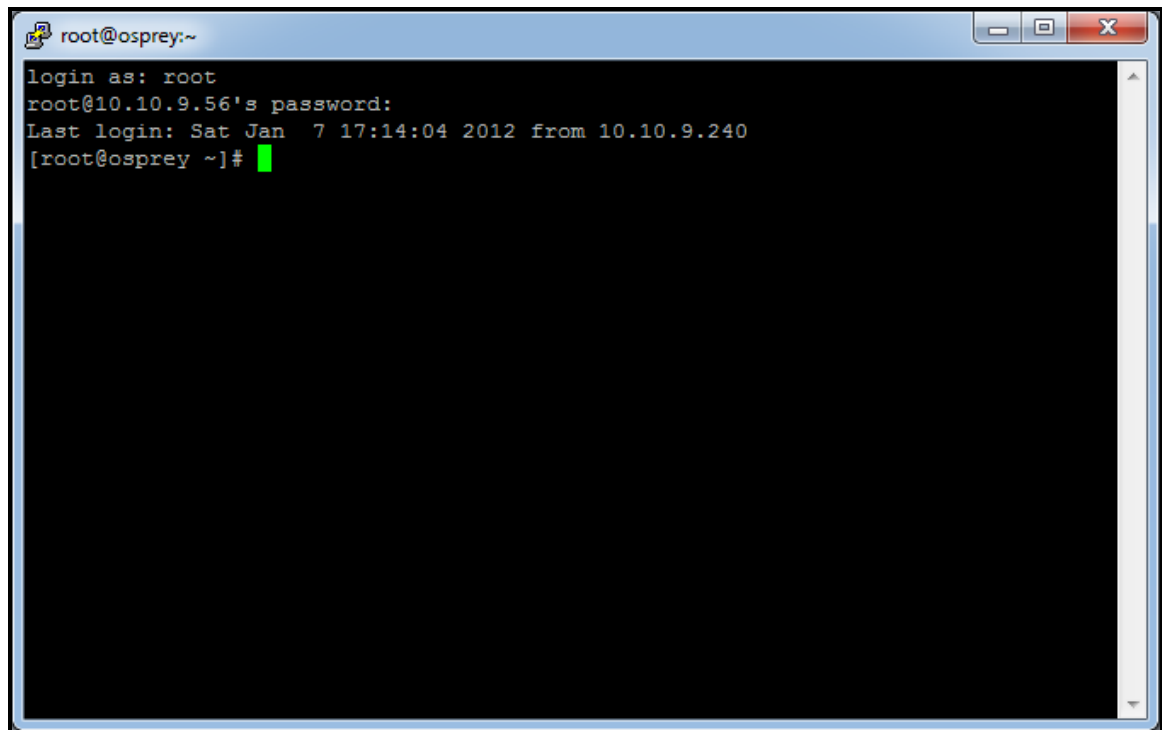
Note: Given that there are many Database Entitlement reports to use, and you may want to link them up to a multitude of datasources, now is a good time to introduce our powerful scripting capability. InfoSphere Guardium offers a powerful capability to automate routine process through its extensive library of command line features. As you will see, the **Guardium API** command line interface can streamline and speed many tasks that would otherwise take significant time to complete through the GUI.

There are many capabilities within our solution that you can either automate, or feed in with a large volume of commands, which is why the Guardium API is critical for the success of any Enterprise Database Activity Monitoring deployment.

- __a. Using a PuTTY SSH client, access the VM database server to demonstrate the ease with which the IBM InfoSphere Guardium solution can automatically and silently populate Database Entitlement Reports.
- __b. Start the PuTTY SSH client login.
- __c. From your laptop, launch PuTTY, enter **10.10.9.56**, and click **Open**.

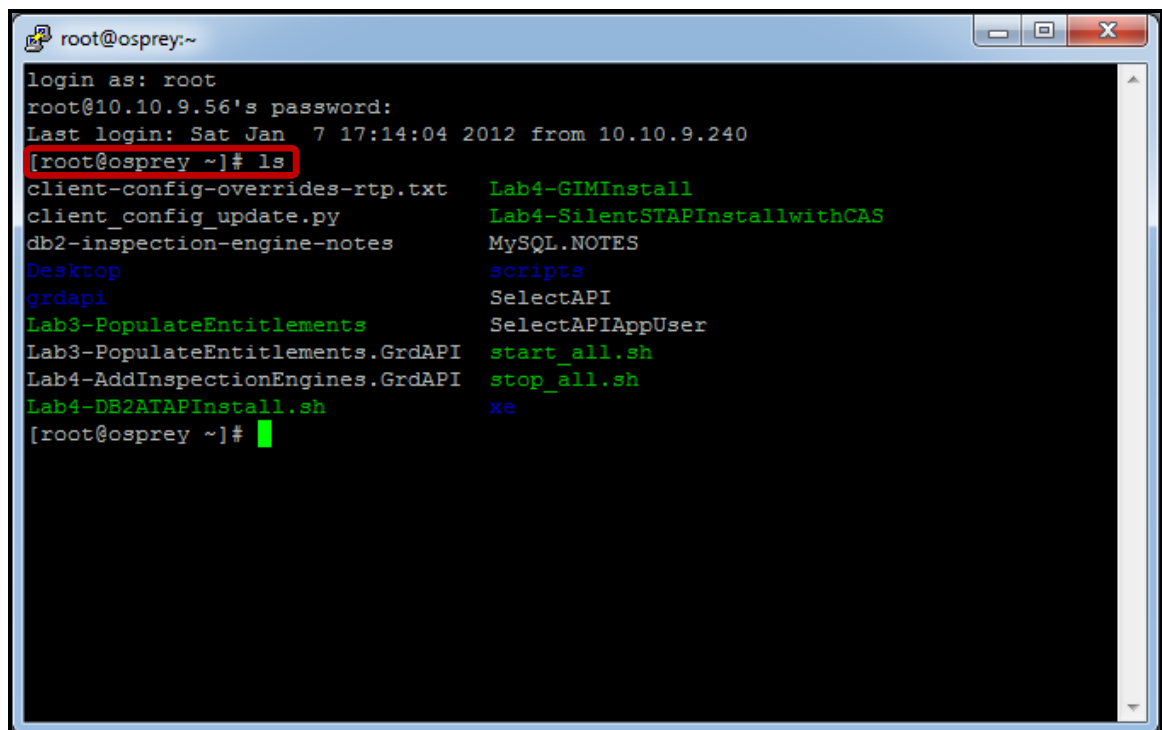


- __d. Login as **root** / **guardium**. After logging in, the following prompt will be displayed.



```
root@osprey:~  
login as: root  
root@10.10.9.56's password:  
Last login: Sat Jan 7 17:14:04 2012 from 10.10.9.240  
[root@osprey ~]#
```

- __e. Type **ls** to get a list of available files.

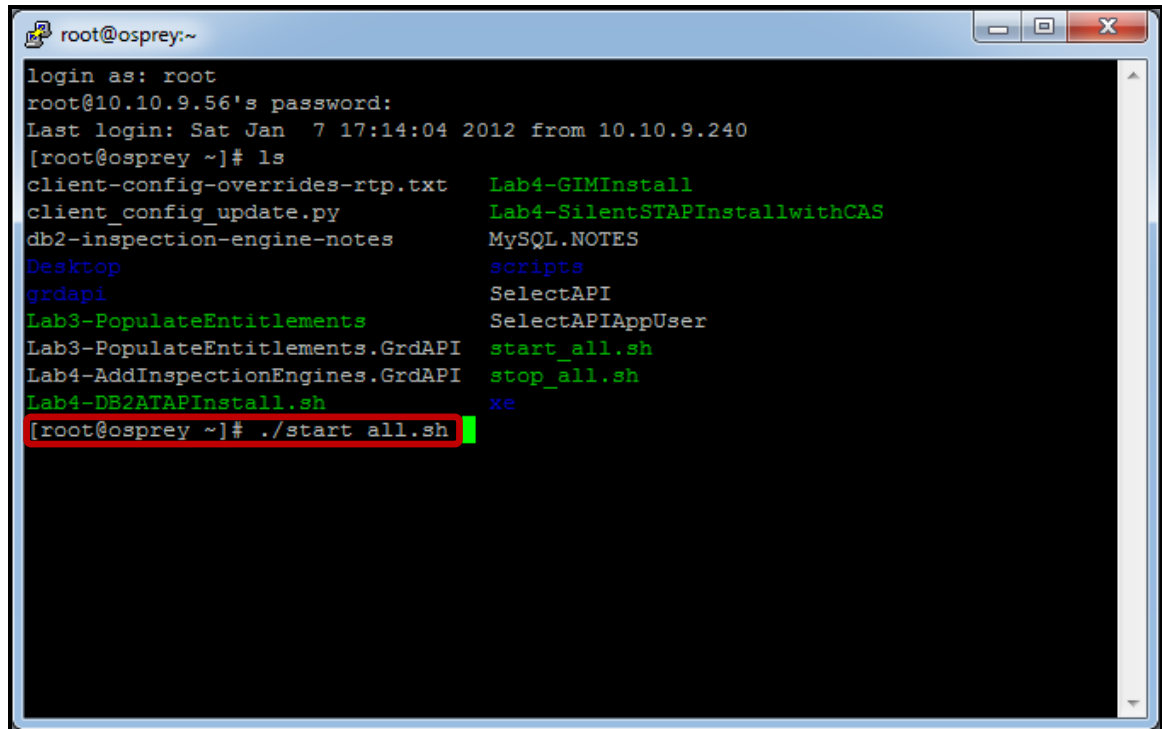


```
root@osprey:~  
login as: root  
root@10.10.9.56's password:  
Last login: Sat Jan 7 17:14:04 2012 from 10.10.9.240  
[root@osprey ~]# ls  
client-config-overrides-rtp.txt      Lab4-GIMInstall  
client_config_update.py             Lab4-SilentSTAPInstallwithCAS  
db2-inspection-engine-notes         MySQL.NOTES  
Desktop                             scripts  
grdapi                              SelectAPI  
Lab3-PopulateEntitlements           SelectAPIAppUser  
Lab3-PopulateEntitlements.GrdAPI     start_all.sh  
Lab4-AddInspectionEngines.GrdAPI    stop_all.sh  
Lab4-DB2ATAPInstall.sh             xe  
[root@osprey ~]#
```

Check that you see the files listed above in the /root directory.

- __f. **Critical Step** – Start all of the database servers by executing the following script:

./start_all.sh

A terminal window titled 'root@osprey:~' showing a root user login. The user runs 'ls' and lists files including 'Lab4-DB2ATAPInstall.sh'. The command './start all.sh' is entered and highlighted with a red box.

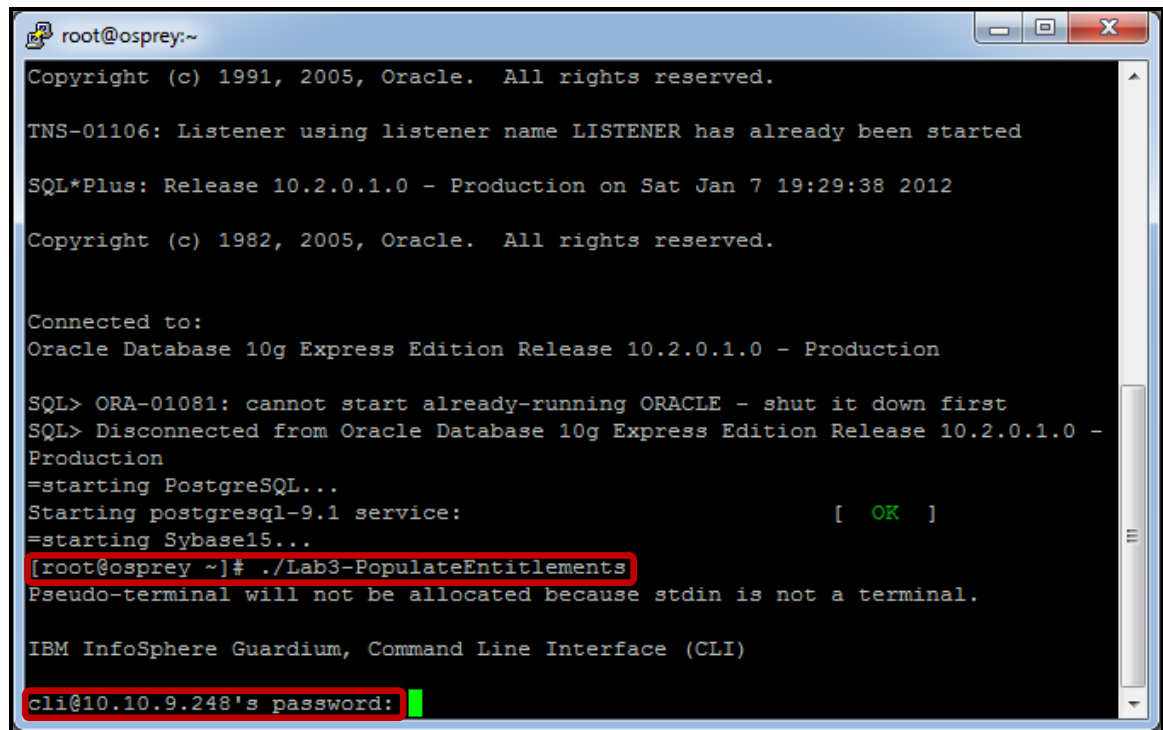
```
root@osprey:~  
login as: root  
root@10.10.9.56's password:  
Last login: Sat Jan 7 17:14:04 2012 from 10.10.9.240  
[root@osprey ~]# ls  
client-config-overrides-rtp.txt      Lab4-GIMInstall  
client_config_update.py              Lab4-SilentSTAPInstallwithCAS  
db2-inspection-engine-notes          MySQL.NOTES  
Desktop                               scripts  
grdapi                                SelectAPI  
Lab3-PopulateEntitlements             SelectAPIAppUser  
Lab3-PopulateEntitlements.GrdAPI      start_all.sh  
Lab4-AddInspectionEngines.GrdAPI     stop_all.sh  
Lab4-DB2ATAPInstall.sh               xe  
[root@osprey ~]# ./start all.sh
```

Note: The IBM DB2®, MySQL, Oracle, PostgreSQL, and Sybase datasources require their databases to be started to communicate to upload their respective Database Entitlement data.

__g. Start the GrdAPI populate process by executing the following script:

./Lab3-PopulateEntitlements

__h. **Critical Step** – Type **guardium** when prompted for **cli@10.10.9.248's password:**.

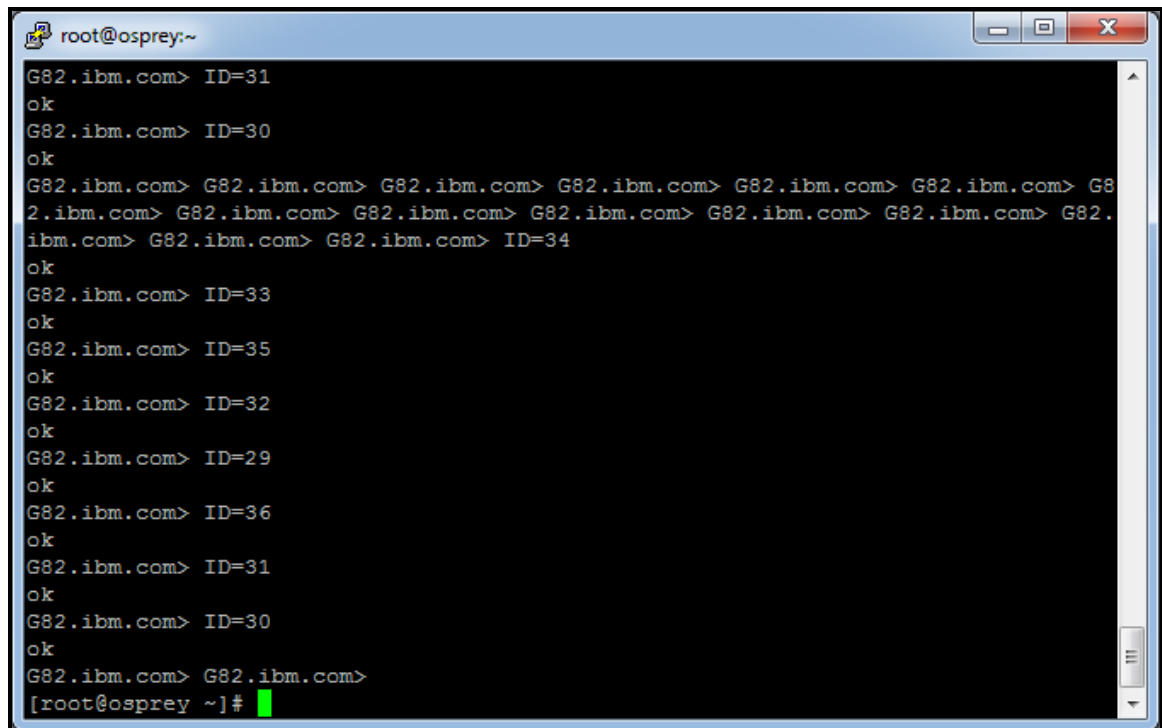


```
root@osprey:~  
Copyright (c) 1991, 2005, Oracle. All rights reserved.  
  
TNS-01106: Listener using listener name LISTENER has already been started  
  
SQL*Plus: Release 10.2.0.1.0 - Production on Sat Jan 7 19:29:38 2012  
  
Copyright (c) 1982, 2005, Oracle. All rights reserved.  
  
Connected to:  
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production  
  
SQL> ORA-01081: cannot start already-running ORACLE - shut it down first  
SQL> Disconnected from Oracle Database 10g Express Edition Release 10.2.0.1.0 -  
Production  
=starting PostgreSQL...  
Starting postgresql-9.1 service: [ OK ]  
=starting Sybase15...  
[root@osprey ~]# ./Lab3-PopulateEntitlements  
Pseudo-terminal will not be allocated because stdin is not a terminal.  
  
IBM InfoSphere Guardium, Command Line Interface (CLI)  
cli@10.10.9.248's password: █
```

__i. DB Entitlement Population complete.

This will populate DB Entitlement data for DB2, MySQL, Oracle and Sybase. This script can be run as frequently as necessary to collect and update the current DB Entitlement data for reporting purposes. As we have seen, this method takes seconds to perform, and is a tremendous time saver in comparison to the InfoSphere Guardium GUI method.

Custom tables can also be populated using the automated schedule facility, when editing each custom table there is a "Modify Schedule ..." button where you can set how often to upload the data.

A terminal window titled 'root@osprey:~' showing the execution of a script. The script consists of multiple lines of commands, each followed by 'ok' or a return code. The commands are: 'G82.ibm.com> ID=31', 'G82.ibm.com> ID=30', 'G82.ibm.com> ID=33', 'G82.ibm.com> ID=35', 'G82.ibm.com> ID=32', 'G82.ibm.com> ID=29', 'G82.ibm.com> ID=36', 'G82.ibm.com> ID=31', 'G82.ibm.com> ID=30', and 'G82.ibm.com> G82.ibm.com>'. The terminal ends with a prompt '[root@osprey ~]#'.

```
root@osprey:~  
G82.ibm.com> ID=31  
ok  
G82.ibm.com> ID=30  
ok  
G82.ibm.com> G82.ibm.com> G82.ibm.com> G82.ibm.com> G82.ibm.com> G82.ibm.com> G8  
2.ibm.com> G82.ibm.com> G82.ibm.com> G82.ibm.com> G82.ibm.com> G82.ibm.com> G82.  
ibm.com> G82.ibm.com> G82.ibm.com> ID=34  
ok  
G82.ibm.com> ID=33  
ok  
G82.ibm.com> ID=35  
ok  
G82.ibm.com> ID=32  
ok  
G82.ibm.com> ID=29  
ok  
G82.ibm.com> ID=36  
ok  
G82.ibm.com> ID=31  
ok  
G82.ibm.com> ID=30  
ok  
G82.ibm.com> G82.ibm.com>  
[root@osprey ~]#
```

Note: If your screen shows any errors or does not look very similar to this one, it is likely that you didn't run the `./start_all.sh` script earlier in this section. If this is the case, please run the `./start_all.sh` script first, followed by the `./Lab3-PopulateEntitlements` script.

The contents of the **start_all.sh** script:

```
#!/bin/bash
echo "=starting DB2..."
su - db2inst2 -c "db2start"
echo "=starting MySQL..."
/etc/init.d/mysql start
echo "=starting Oracle10g..."
su - oracle -c "./start.sh"
echo "=starting PostgreSQL..."
/etc/init.d/postgresql-9.1 start
echo "=starting Sybase15..."
su - sybase15 -c "source /home/sybase15/.bash_profile; /home/sybase15/start_it.sh"
```

The contents of the **Lab3-PopulateEntitlements** script

```
# Populate Entitlement Reports
ssh cli@10.10.9.248 < Lab3-PopulateEntitlements.GrdAPI
```

The contents of the **Lab3-PopulateEntitlements.GrdAPI** script:

```
# DB2 - Create Datasource Bindings
grdapi create_datasourceRef_by_name application=CustomTables objName="DB2 Column Level Privs" datasourceName=osprey_db2inst2
grdapi create_datasourceRef_by_name application=CustomTables objName="DB2 DB Level Privs" datasourceName=osprey_db2inst2
grdapi create_datasourceRef_by_name application=CustomTables objName="DB2 Index Level Privs" datasourceName=osprey_db2inst2
grdapi create_datasourceRef_by_name application=CustomTables objName="DB2 Package Level Privs" datasourceName=osprey_db2inst2
grdapi create_datasourceRef_by_name application=CustomTables objName="DB2 Table Level Privs" datasourceName=osprey_db2inst2
grdapi create_datasourceRef_by_name application=CustomTables objName="DB2 Priv Summary" datasourceName=osprey_db2inst2

# DB2 - Upload Entitlement Data
grdapi upload_custom_data tableName=DB2_COLUMN_PRIVS
grdapi upload_custom_data tableName=DB2_DB_PRIVS
grdapi upload_custom_data tableName=DB2_INDEX_PRIVS
grdapi upload_custom_data tableName=DB2_PACKAGE_PRIVS
grdapi upload_custom_data tableName=DB2_TABLE_PRIVS
grdapi upload_custom_data tableName=DB2_PRIVS_SUMMARY

# MySQL - Create Datasource Bindings
grdapi create_datasourceRef_by_name application=CustomTables objName="MYSQL DB Privs 40" datasourceName=osprey_admin
grdapi create_datasourceRef_by_name application=CustomTables objName="MYSQL DB Privs 500" datasourceName=osprey_admin
grdapi create_datasourceRef_by_name application=CustomTables objName="MYSQL DB Privs 502" datasourceName=osprey_admin
grdapi create_datasourceRef_by_name application=CustomTables objName="MYSQL Host Privs 40" datasourceName=osprey_admin
grdapi create_datasourceRef_by_name application=CustomTables objName="MYSQL Host Privs 500" datasourceName=osprey_admin
grdapi create_datasourceRef_by_name application=CustomTables objName="MYSQL Host Privs 502" datasourceName=osprey_admin
grdapi create_datasourceRef_by_name application=CustomTables objName="MYSQL Table Privs 40" datasourceName=osprey_admin
grdapi create_datasourceRef_by_name application=CustomTables objName="MYSQL Table Privs 500" datasourceName=osprey_admin
grdapi create_datasourceRef_by_name application=CustomTables objName="MYSQL Table Privs 502" datasourceName=osprey_admin
grdapi create_datasourceRef_by_name application=CustomTables objName="MYSQL User Privs 40" datasourceName=osprey_admin
grdapi create_datasourceRef_by_name application=CustomTables objName="MYSQL User Privs 500" datasourceName=osprey_admin
grdapi create_datasourceRef_by_name application=CustomTables objName="MYSQL User Privs 502" datasourceName=osprey_admin

# MySQL - Upload Entitlement Data
grdapi upload_custom_data tableName=MYSQL_DB_PRIVS_40
grdapi upload_custom_data tableName=MYSQL_DB_PRIVS_500
grdapi upload_custom_data tableName=MYSQL_DB_PRIVS_502
grdapi upload_custom_data tableName=MYSQL_HOST_PRIVS_40
grdapi upload_custom_data tableName=MYSQL_HOST_PRIVS_500
grdapi upload_custom_data tableName=MYSQL_HOST_PRIVS_502
grdapi upload_custom_data tableName=MYSQL_TABLE_PRIVS_40
grdapi upload_custom_data tableName=MYSQL_TABLE_PRIVS_500
grdapi upload_custom_data tableName=MYSQL_TABLE_PRIVS_502
grdapi upload_custom_data tableName=MYSQL_USER_PRIVS_40
grdapi upload_custom_data tableName=MYSQL_USER_PRIVS_500
grdapi upload_custom_data tableName=MYSQL_USER_PRIVS_502
```

```

# Oracle - Create Datasource Bindings
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA Acnts of ALTER SYSTEM" datasourceName=osprey_system
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA Acnts with BECOME USER" datasourceName=osprey_system
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA All Sys Priv and admin opt" datasourceName=osprey_system
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA Obj And Columns Priv" datasourceName=osprey_system
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA Object Access By PUBLIC" datasourceName=osprey_system
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA Object privileges" datasourceName=osprey_system
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA PUBLIC Exec Priv on SYS Proc" datasourceName=osprey_system
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA Roles Granted" datasourceName=osprey_system
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA Sys Priv Granted" datasourceName=osprey_system
grdapi create_datasourceRef_by_name application=CustomTables objName="ORA SYSDBA and SYSDOPER Acnts" datasourceName=osprey_system

# Oracle - Upload Entitlement Data
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_ALL_SYSTEM_PRIVILEGE
grdapi upload_custom_data tableName=ORA_OBJECT_AND_COLUMNS_PRIVILEGES
grdapi upload_custom_data tableName=ORA_OBJECT_ACCESS_BY_PUBLIC
grdapi upload_custom_data tableName=ORA_OBJECT_PRIVILEGES_BY_DB
grdapi upload_custom_data tableName=ORA_EXEC_PRIV_ON_SYS_PROC
grdapi upload_custom_data tableName=ORA_ROLES_TO_USERS_AND_ROLES
grdapi upload_custom_data tableName=ORA_HIERARCHICAL_SYS_PRIV_GRANTED
grdapi upload_custom_data tableName=ORA_SYSDBA_SYSDOPER_PRIV_ACCNT

# PostgreSQL - Create Datasource Bindings
grdapi create_datasourceRef_by_name application=CustomTables objName="PostgreSQL Priv On DBs Granted PubUserRole" datasourceName=osprey_postgres
grdapi create_datasourceRef_by_name application=CustomTables objName="PostgreSQL Priv On Language Granted PubUserRole"
datasourceName=osprey_postgres
grdapi create_datasourceRef_by_name application=CustomTables objName="PostgreSQL Priv On Schema Granted PubUserRole"
datasourceName=osprey_postgres
grdapi create_datasourceRef_by_name application=CustomTables objName="PostgreSQL Priv On Tablespace Granted PubUserRole"
datasourceName=osprey_postgres
grdapi create_datasourceRef_by_name application=CustomTables objName="PostgreSQL Role Granted To User Or Role" datasourceName=osprey_postgres
grdapi create_datasourceRef_by_name application=CustomTables objName="PostgreSQL Super User Granted To User Or Role"
datasourceName=osprey_postgres
grdapi create_datasourceRef_by_name application=CustomTables objName="PostgreSQL Sys Privs Granted To User And Role"
datasourceName=osprey_postgres
grdapi create_datasourceRef_by_name application=CustomTables objName="PostgreSQL TabViewSeqFun Granted To Public" datasourceName=osprey_postgres
grdapi create_datasourceRef_by_name application=CustomTables objName="PostgreSQL TabViewSeqFun Privs Granted To Login"
datasourceName=osprey_postgres
grdapi create_datasourceRef_by_name application=CustomTables objName="PostgreSQL TabViewSeqFun Privs Granted To Roles"
datasourceName=osprey_postgres
grdapi create_datasourceRef_by_name application=CustomTables objName="PostgreSQL TabViewSeqFun Privs Granted with Grant"
datasourceName=osprey_postgres

# PostgreSQL - Upload Entitlement Data
grdapi upload_custom_data tableName=POSTGRESQL_PRIV_ON_DBS_GRANTED_PUBUSERROLE
grdapi upload_custom_data tableName=POSTGRESQL_PRIV_ON_LANGUAGE_GRANTED_PUBUSERROLE
grdapi upload_custom_data tableName=POSTGRESQL_PRIV_ON_SCHEMA_GRANTED_PUBUSERROLE
grdapi upload_custom_data tableName=POSTGRESQL_PRIV_ON_TABLESPACE_GRANTED_PUBUSERROLE
grdapi upload_custom_data tableName=POSTGRESQL_ROLE_GRANTED_TO_USER_OR_ROLE
grdapi upload_custom_data tableName=POSTGRESQL_SUPER_USER_GRANTED_TO_USER_OR_ROLE
grdapi upload_custom_data tableName=POSTGRESQL_SYS_PRIVS_GRANTED_TO_USER_AND_ROLE
grdapi upload_custom_data tableName=POSTGRESQL_TABVIEWSEQFUN_GRANTED_TO_PUBLIC
grdapi upload_custom_data tableName=POSTGRESQL_TABVIEWSEQFUN_PRIVS_GRANTED_TO_LOGIN
grdapi upload_custom_data tableName=POSTGRESQL_TABVIEWSEQFUN_PRIVS_GRANTED_TO_ROLES
grdapi upload_custom_data tableName=POSTGRESQL_TABVIEWSEQFUN_PRIVS_GRANTED_WITH_GRANT

# Sybase - Create Datasource Bindings
grdapi create_datasourceRef_by_name application=CustomTables objName="SYBASE Acnts With Sys Or Sec Admin Roles" datasourceName=osprey_sa
grdapi create_datasourceRef_by_name application=CustomTables objName="SYBASE Execute Priv On Proc Func To Public" datasourceName=osprey_sa
grdapi create_datasourceRef_by_name application=CustomTables objName="SYBASE Obj Col Privs Granted With Grant" datasourceName=osprey_sa
grdapi create_datasourceRef_by_name application=CustomTables objName="SYBASE Object Access By Public" datasourceName=osprey_sa
grdapi create_datasourceRef_by_name application=CustomTables objName="SYBASE Object Privs By DB Acct" datasourceName=osprey_sa
grdapi create_datasourceRef_by_name application=CustomTables objName="SYBASE Role Granted To User" datasourceName=osprey_sa
grdapi create_datasourceRef_by_name application=CustomTables objName="SYBASE Role Granted To User And Sys Privs Granted" datasourceName=osprey_sa
grdapi create_datasourceRef_by_name application=CustomTables objName="SYBASE Sys Priv And Role Granted To User" datasourceName=osprey_sa

# Sybase - Upload Entitlement Data
grdapi upload_custom_data tableName=SYBASE_ACCNTS_WITH_SYS_OR_SEC_ADMIN_ROLES
grdapi upload_custom_data tableName=SYBASE_EXECUTE_PRIV_ON_PROC_FUNC_TO_PUBLIC
grdapi upload_custom_data tableName=SYBASE_OBJ_COL_PRIVS_GRANTED_WITH_GRAN
grdapi upload_custom_data tableName=SYBASE_OBJECT_ACCESS_BY_PUBLIC
grdapi upload_custom_data tableName=SYBASE_OBJECT_PRIVS_BY_DB_ACCNT
grdapi upload_custom_data tableName=SYBASE_ROLE_GRANTED_TO_USER
grdapi upload_custom_data tableName=SYBASE_ROLE_GRANTED_TO_USER_AND_SYS_PRIVS_GRANTED
grdapi upload_custom_data tableName=SYBASE_SYS_PRIV_AND_ROLE_GRANTED_TO_USER
exit

```

__5. Verify that DB2 Entitlement Reports have been populated.

__a. Click **DB2**.

The screenshot shows the 'Entitlement Reports' application with the 'DB2' category selected in the left-hand navigation pane. The main window displays four report sections:

- DB2 Column Level Privs:** Shows a table with columns for GRANTEE, GRANTEETYPE, TABSCHEMA, TABNAME, COLNAME, COLNO, PRIVTYPE, GRANTABLE, and Datasource Name. A single record is visible for user 'JOE' on table 'CREDITCARD.CARDID'.
- DB2 DB Level Privs:** Shows a table with columns for GRANTEE, GRANTEETYPE, INDSHEMA, INDDNAME, CONTROLAUTH, and Datasource Name. Multiple records are shown for users like 'DB2INST2', 'PUBLIC', and 'COMMON' across various system tables.
- DB2 Index Level Privs:** Shows a table with columns for GRANTEE, GRANTEETYPE, INDSHEMA, INDNAME, CONTROLAUTH, and Datasource Name. Records are shown for users like 'DB2INST2' and 'PUBLIC' on system tables.
- DB2 Package Level Privs:** Shows a table with columns for GRANTEE, GRANTEETYPE, INDSHEMA, INDDNAME, CONTROLAUTH, and Datasource Name. Records are shown for users like 'DB2INST2' and 'PUBLIC' on various system packages.

__b. DB2 Entitlements for 'DB2 Column Level Privs'.

This view shows a detailed record from the 'DB2 Column Level Privs' report:

GRANTEE	GRANTEETYPE	TABSCHEMA	TABNAME	COLNAME	COLNO	PRIVTYPE	GRANTABLE	Datasource Name	SqlGuard Timestamp	Count of DB2 Column Level Privs
JOE	U	DB2INST2	CREDITCARD	CARDID	0	U	N	osprey_db2inst2 : DB2 : 10.10.9.56 : : sample2 : 50001 : 2011-12-21 17:48:01.0	1	

__c. DB2 Entitlements for 'DB2 DB Level Privs'.

This view shows a detailed record from the 'DB2 DB Level Privs' report:

GRANTEE	GRANTEETYPE	INDSCHEMA	INDNAME	CONTROLAUTH	Datasource Name	SqlGuard Timestamp	Count of DB2 DB Level Privs
DB2INST2	U	SYSTOOLS	ATM_UNIQ	Y	osprey_db2inst2 : DB2 : 10.10.9.56 : : sample2 : 50001 : 2011-12-21 17:48:02.0	1	
PUBLIC	G	SYSTOOLS	POLICY_UNQY	N	osprey_db2inst2 : DB2 : 10.10.9.56 : : sample2 : 50001 : 2011-12-21 17:48:01.0	1	
COMMON	G	SYSTOOLS	HL_OBJ_UNIQY	N	osprey_db2inst2 : DB2 : 10.10.9.56 : : sample2 : 50001 : 2011-12-21 17:48:01.0	1	

__d. DB2 Entitlements for 'DB2 Index Level Privs'.

This view shows a detailed record from the 'DB2 Index Level Privs' report:

GRANTEE	GRANTEETYPE	INDSCHEMA	INDNAME	CONTROLAUTH	Datasource Name	SqlGuard Timestamp	Count of DB2 Index Level Privs
DB2INST2	U	SYSTOOLS	ATM_UNIQ	Y	osprey_db2inst2 : DB2 : 10.10.9.56 : : sample2 : 50001 : 2011-12-21 17:48:02.0	1	
DB2INST2	U	SYSTOOLS	POLICY_UNQY	Y	osprey_db2inst2 : DB2 : 10.10.9.56 : : sample2 : 50001 : 2011-12-21 17:48:02.0	1	
DB2INST2	U	SYSTOOLS	HL_OBJ_UNIQY	Y	osprey_db2inst2 : DB2 : 10.10.9.56 : : sample2 : 50001 : 2011-12-21 17:48:02.0	1	

e. DB2 Entitlements for 'DB2 Package Level Privs'.

DB2 Package Level Privs										
Start Date: 2011-12-14 18:02:56 End Date: 2011-12-21 18:02:56										
Aliases: OFF										
GRANTEE	GRANTEETYPE	PKGSHEMA	PKGNAME	CONTROLAUTH	BINDAUTH	EXECUTEAUTH	Datasource Name	SqlGuard Timestamp	Count of DB2 Package Level Privs	
PUBLIC	G	NULLID	SYSLN400	N	Y	Y	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
DB2INST2	U	NULLID	SYSSN302	Y	G	G	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
DB2INST2	U	NULLID	SQLE3F01	Y	G	G	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
PUBLIC	G	NULLID	SYSSN302	N	Y	Y	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
PUBLIC	G	NULLID	SQLE3F01	N	Y	Y	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
DB2INST2	U	NULLID	SYSLH200	Y	G	G	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
PUBLIC	G	NULLID	SYSLH200	N	Y	Y	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
DB2INST2	U	NULLID	SYSSH102	Y	G	G	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
DB2INST2	U	NULLID	DB2XDBM	Y	G	G	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
DB2INST2	U	NULLID	SQUCF03	Y	G	G	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
PUBLIC	G	NULLID	SYSSH102	N	Y	Y	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
DB2INST2	U	NULLID	TUPLEWRT	Y	G	G	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
PUBLIC	G	NULLID	TUPLEWRT	N	Y	Y	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
PUBLIC	G	NULLID	SQUCF03	N	Y	Y	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
DB2INST2	U	NULLID	SYSLH302	Y	G	G	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
PUBLIC	G	NULLID	SYSLH302	N	Y	Y	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
DB2INST2	U	NULLID	SYSSH301	Y	G	G	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
DB2INST2	U	NULLID	SQLA1F00	Y	G	G	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
PUBLIC	G	NULLID	SYSSH301	N	Y	Y	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		
PUBLIC	G	NULLID	SPIMPL	N	Y	Y	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:02.0	1		

f. DB2 Entitlements for 'DB2 Table Level Privs'.

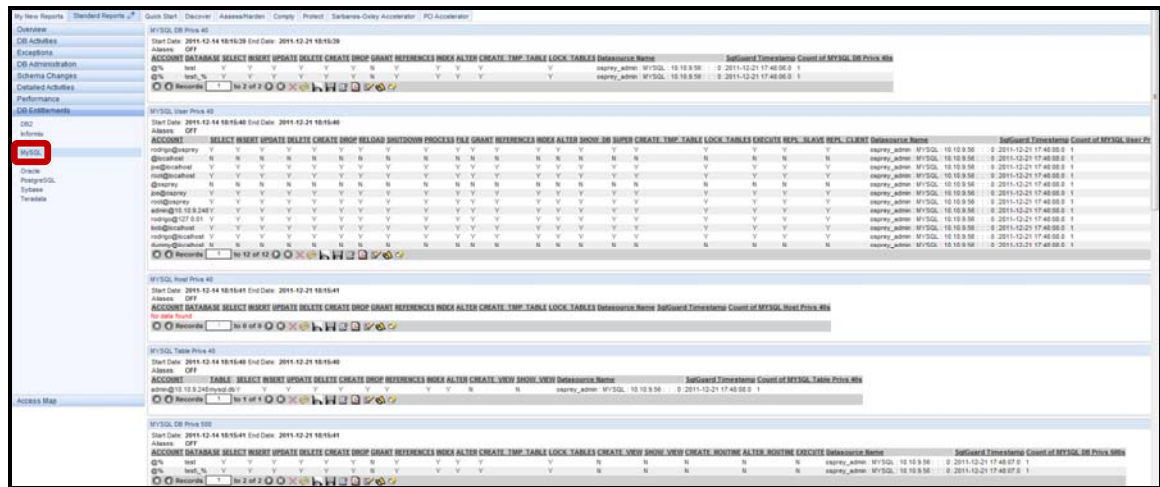
DB2 Table Level Privs													
Start Date: 2011-12-14 18:02:57 End Date: 2011-12-21 18:02:57													
Aliases: OFF													
GRANTEE	GRANTEETYPE	TABSCHEMA	TABNAME	CONTROLAUTH	ALTERAUTH	DELETEAUTH	INSERTAUTH	REFAUTH	SELECTAUTH	UPDATEAUTH	Datasource Name	SqlGuard Timestamp	Count of DB2 Table Level Privs
PUBLIC	G	SYSCAT	SEQUENCEAUTH	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSCAT	COLLUSE	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSEADM	OBJECTOWNERS	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSESM	SYSECURITYLABELS	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSESM	SYSCOLGROUPSCOLS	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSESM	SYSCOLNAMS	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSCAT	SERVERS	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSCAT	DATAPARTITIONS	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSEADM	QUERY_PREF_COST	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSESM	SYSECURITYPOLYEXEMPTIONS	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSESM	SYSESERVEROPTIONS	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSESM	SYSCONGTOP	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSCAT	TABAUTH	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSCAT	DBPARTITIONGROUPDEF	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
DB2INST2	U	DB2INST2	CC	Y	G	G	G	G	G	G	G	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSEADM	SNAPAGENT_MEMORY_POOL	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSEADM	SNLSP	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSESM	SYSSURROGATEAUTHDS	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSESM	SYSDATAVES	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1
PUBLIC	G	SYSCAT	TABDEFINITIONS	N	N	N	N	N	N	Y	N	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:03.0	1

g. DB2 Entitlements for 'DB2 Priv Summary'.

DB2 Priv Summary					
Start Date: 2011-12-14 18:02:56 End Date: 2011-12-21 18:02:56					
Aliases: OFF					
GRANTEE	GRANTEETYPE	PRIVILEGETYPE	Datasource Name	SqlGuard Timestamp	Count of DB2 Priv Summaries
DB2INST2	U	DATABASE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
DB2INST2	U	ROUTINE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
GDENT	G	DATABASE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
GDMMON	G	DATABASE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
GDMMON	G	TABLE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
PUBLIC	G	DATABASE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
PUBLIC	G	SCHEMA	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
DB2INST2	U	PACKAGE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
DB2INST2	U	TBLSPACE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
GDENT	G	TABLE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
GDMMON	G	ROUTINE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
JOE	U	TABLE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
PUBLIC	G	ROUTINE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
PUBLIC	G	TBLSPACE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
DB2INST2	U	INDEX	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
DB2INST2	U	TABLE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
GDENT	G	PACKAGE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
GDMMON	G	PACKAGE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
JOE	U	COLUMN	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	
PUBLIC	G	PACKAGE	osprey_db2inst2 : DB2 : 10.10.9.56 : sample2 : 50001 : 2011-12-21 17:48:04.0	1	

6. Verify that MySQL Entitlement Reports have been populated.

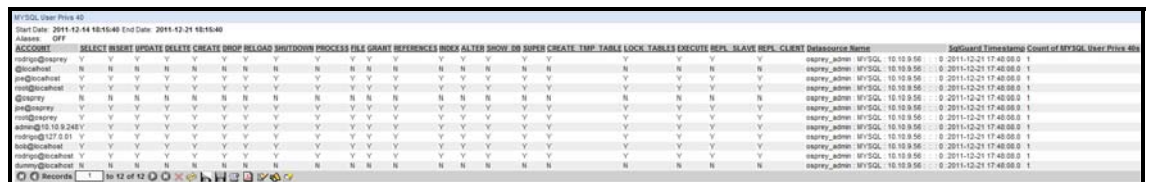
a. Click **MySQL**.



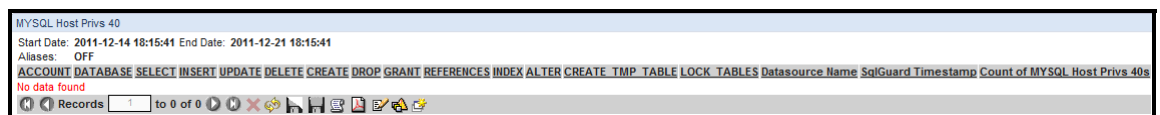
b. MySQL Entitlements for 'MySQL DB Privs 40'.



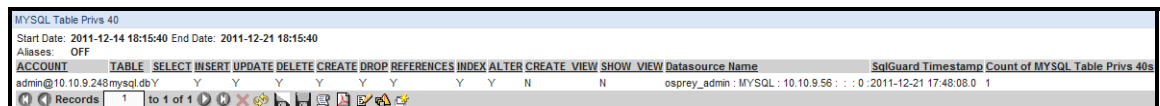
c. MySQL Entitlements for 'MySQL User Privs 40'.



d. MySQL Entitlements for 'MySQL Host Privs 40'.



e. DB2 Entitlements for 'MySQL Table Privs 40'.



__k. MySQL Entitlements for 'MYSQL User Privs 502/up'.

GRANTEE	TABLE CATALOG	PRIVILEGE TYPE	IS GRANTABLE	Datasource Name	SqGuard Timestamp	Count of MYSQL User Privs 502/up
'@localhost'	def	USAGE	NO	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'@osprey'	def	USAGE	NO	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	ALTER	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	ALTER ROUTINE	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	CREATE	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	CREATE ROUTINE	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	CREATE TABLESPACE	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	CREATE TEMPORARY TABLES	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	CREATE USER	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	CREATE VIEW	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	DELETE	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	DROP	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	EVENT	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	EXECUTE	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	FILE	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	INDEX	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	INSERT	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	LOCK TABLES	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	PROCESS	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	REFERENCES	YES	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1

__l. MySQL Entitlements for 'MYSQL Host Privs 502/up'.

GRANTEE	TABLE CATALOG	TABLE SCHEMA	TABLE NAME	PRIVILEGE TYPE	IS GRANTABLE	Datasource Name	SqGuard Timestamp	Count of MYSQL Host Privs 502/up
No data found								

__m. MySQL Entitlements for 'MYSQL Table Privs 502/up'.

GRANTEE	TABLE CATALOG	TABLE SCHEMA	TABLE NAME	PRIVILEGE TYPE	IS GRANTABLE	Datasource Name	SqGuard Timestamp	Count of MYSQL Table Privs 502/up
'admin'@'10.10.9.248'	def	mysql	db	ALTER	NO	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	mysql	db	CREATE	NO	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	mysql	db	DELETE	NO	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	mysql	db	DROP	NO	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	mysql	db	INDEX	NO	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	mysql	db	INSERT	NO	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	mysql	db	REFERENCES	NO	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	mysql	db	SELECT	NO	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1
'admin'@'10.10.9.248'	def	mysql	db	UPDATE	NO	osprey_admin : MYSQL : 10.10.9.56 : : 0	2011-12-21 17:48:08.0	1

__7. Verify that Oracle Entitlements Reports have been populated.

- __a. The Oracle database Entitlement report “ORA Accnts of ALTER SYSTEM’ displays all user accounts (16) with Alter System privilege.

ORA Accnts of ALTER SYSTEM						
Start Date: 2011-12-14 11:07:55 End Date: 2011-12-21 11:07:55						
Aliases: OFF						
Grantee	Privilege	Admin Option	Datasource Name	SqlGuard Timestamp	Count of ORA Accnts of ALTER SYSTEMS	
WEBAPP	ALTER SESSIONNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 11:07:45.0	1	
BANKAPP	ALTER SESSIONNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 11:07:45.0	1	
SYSTEM	ALTER SYSTEM NO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 11:07:45.0	1	
SYSTEM	ALTER SESSIONNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 11:07:45.0	1	
RECOVERY_CATALOG_OWNER	ALTER SESSIONNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 11:07:45.0	1	
PETSTORE	ALTER SYSTEM NO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 11:07:45.0	1	
PETSTORE	ALTER SESSIONNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 11:07:45.0	1	
HR	ALTER SESSIONNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 11:07:45.0	1	
FLows_020100	ALTER SYSTEM NO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 11:07:45.0	1	
FLows_020100	ALTER SESSIONNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 11:07:45.0	1	
DBA	ALTER SYSTEM YES		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 11:07:45.0	1	
DBA	ALTER SESSIONYES		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 11:07:45.0	1	
XDB	ALTER SESSIONNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 11:07:45.0	1	
CTXSYS	ALTER SESSIONNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 11:07:45.0	1	
WEBAPP	ALTER SYSTEM NO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 11:07:45.0	1	
BANKAPP	ALTER SYSTEM NO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 11:07:45.0	1	

- __b. Oracle Entitlements for ‘ORA Accnts with BECOME USER’.

ORA Accnts with BECOME USER						
Start Date: 2011-12-14 12:19:43 End Date: 2011-12-21 12:19:43						
Aliases: OFF						
Grantee	Privilege	Admin Option	Datasource Name	SqlGuard Timestamp	Count of ORA Accnts with BECOME USERS	
WEBAPP	BECOME USERNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 12:05:36.0	1	
BANKAPP	BECOME USERNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 12:01:17.0	1	
WEBAPP	BECOME USERNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 12:01:17.0	1	
SYSTEM	BECOME USERNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 12:05:36.0	1	
SYSTEM	BECOME USERNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 12:01:17.0	1	
PETSTORE	BECOME USERNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 12:05:36.0	1	
PETSTORE	BECOME USERNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 12:01:17.0	1	
JBROWN	BECOME USERYES		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 12:05:36.0	1	
JBROWN	BECOME USERYES		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 12:01:17.0	1	
IMP_FULL_DATABASE	BECOME USERNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 12:05:36.0	1	
IMP_FULL_DATABASE	BECOME USERNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 12:01:17.0	1	
DBA	BECOME USERYES		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 12:05:36.0	1	
DBA	BECOME USERYES		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 12:01:17.0	1	
BANKAPP	BECOME USERNO		osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2011-12-21 12:05:36.0	1	

- __c. Oracle Entitlements for ‘ORA Obj and Columns Priv’.

ORA Obj And Columns Priv									
Start Date: 2011-12-31 22:06:27 End Date: 2012-01-07 22:06:27									
Aliases: OFF Grantable: LIKE %									
Grantee	Privilege	Table Name	Owner	Grantor	Grantable	Datasource Name	SqlGuard Timestamp	Count of ORA Obj And Columns Privs	
ANONYMOUS	ALTER	WWW_FLOW_FILE_OBJECTS\$	FLows_FILES	FLows_FILES	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
ANONYMOUS	ALTER	WWW_FLOW_FILE_OBJECTS\$	FLows_FILES	FLows_FILES	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
ANONYMOUS	DEBUG	WWW_FLOW_FILE_OBJECTS\$	FLows_FILES	FLows_FILES	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
ANONYMOUS	DELETE	WWW_FLOW_FILE_OBJECTS\$	FLows_FILES	FLows_FILES	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
ANONYMOUS	EXECUTE	WWW_FLOW_EPG_INCLUDE_MODULES	FLows_FILES	FLows_FILES	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
ANONYMOUS	FLASHBACK	WWW_FLOW_FILE_OBJECTS\$	FLows_FILES	FLows_FILES	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
ANONYMOUS	INDEX	WWW_FLOW_FILE_OBJECTS\$	FLows_FILES	FLows_FILES	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
ANONYMOUS	INSERT	WWW_FLOW_FILE_OBJECTS\$	FLows_FILES	FLows_FILES	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
ANONYMOUS	ON COMMIT REFRESH	WWW_FLOW_FILE_OBJECTS\$	FLows_FILES	FLows_FILES	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
ANONYMOUS	QUERY REWRITE	WWW_FLOW_FILE_OBJECTS\$	FLows_FILES	FLows_FILES	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
ANONYMOUS	REFERENCES	WWW_FLOW_FILE_OBJECTS\$	FLows_FILES	FLows_FILES	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
ANONYMOUS	SELECT	WWW_FLOW_FILE_OBJECTS\$	FLows_FILES	FLows_FILES	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
ANONYMOUS	UPDATE	WWW_FLOW_FILE_OBJECTS\$	FLows_FILES	FLows_FILES	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
AQ_ADMINISTRATOR_ROLE	EXECUTE	DBMS_AQ	SYS	SYS	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
AQ_ADMINISTRATOR_ROLE	EXECUTE	DBMS_AQADM	SYS	SYS	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
AQ_ADMINISTRATOR_ROLE	EXECUTE	DBMS_AQELM	SYS	SYS	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
AQ_ADMINISTRATOR_ROLE	EXECUTE	DBMS_AQIN	SYS	SYS	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
AQ_ADMINISTRATOR_ROLE	EXECUTE	DBMS_AQJMS_INTERNAL	SYS	SYS	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
AQ_ADMINISTRATOR_ROLE	EXECUTE	DBMS_AQ_IMPORT_INTERNAL	SYS	SYS	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
AQ_ADMINISTRATOR_ROLE	EXECUTE	DBMS_RULE_EXMP	SYS	SYS	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	
AQ_ADMINISTRATOR_ROLE	EXECUTE	DBMS_TRANSFORM	SYS	SYS	NO	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	: 2012-01-07 22:01:11.0	1	

d. Oracle Entitlements for 'ORA Object Access By PUBLIC'.

ORA Object Access By PUBLIC						
Start Date: 2011-12-14 12:19:42 End Date: 2011-12-21 12:19:42						
Aliases: OFF						
Owner	Object Name	Privilege	Datasource Name	SqlGuard Timestamp	Count of ORA Object Access By PUBLICS	
MDSYS	USER_SDO_THEMES	UPDATE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:23.0		1	
SYS	DBMS_TRANSACTION	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:43.0		1	
SYS	USER_IND_STATISTICS	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:24.0		1	
SYS	KU\$_PKGBODY_VIEW	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:24.0		1	
PETSTORE	CATEGORY	DELETE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:23.0		1	
CTXSYS	CTX_PREFERENCES	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:23.0		1	
SYS	EXPCOMPRESSED_TAB	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:43.0		1	
SYS	USER_OPBINDINGS	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:24.0		1	
SYS	KU\$_PROCOBJ_LOCS	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:24.0		1	
PETSTORE	LINEITEM	DEBUG	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:23.0		1	
CTXSYS	CTX_USER_THESAURI	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:23.0		1	
SYS	EXU10TABU	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:43.0		1	
SYS	USER_REGISTRY	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:24.0		1	
SYS	KU\$_RESOCOST_LIST_T	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:24.0		1	
PETSTORE	PRODUCT	ALTER	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:23.0		1	
CTXSYS	DRVPARX	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:23.0		1	
SYS	USER_REWRITE_EQUIVALENCES	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:43.0		1	
SYS	EXU81SPOKU	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:43.0		1	
SYS	KU\$_SPIND_STATS_LIST_T	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:24.0		1	
PETSTORE	SUPPLIER	UPDATE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:24.0		1	

Records 1 to 20 of 5476

e. Oracle Entitlements for 'ORA Object privileges'.

ORA Object privileges						
Start Date: 2011-12-14 12:19:39 End Date: 2011-12-21 12:19:39						
Aliases: OFF						
Grantee	Table Name	Owner	Privilege	Datasource Name	SqlGuard Timestamp	Count of ORA Object privileges
HARRY	CREDITCARD	JOE	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
BILL	BIN\$SPHkr9kUVUjgQAoKOAkSug==#0	JOE	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
FLows_020100	DBA_TAB_COLUMNS	SYS	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
FLows_FILES	WWW_FLOW	FLows_020100	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
ANONYMOUS	WWW_FLOW_FILE_OBJECTS\$	FLows_FILES	DEBUG	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
XDB	UTL_FILE	SYS	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
DON	CREDITCARD	JOE	INSERT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
FLows_020100	UTLSMTP	SYS	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
BILL	BIN\$SPHkr9kUVUjgQAoKOAkSug==#0	JOE	DELETE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:25.0		1
FLows_020100	DBA_TABLES	SYS	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:25.0		1
FLows_020100	WWW_FLOW_FILE_OBJECTS\$	FLows_FILES	UPDATE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:25.0		1
ANONYMOUS	WWW_FLOW_EPG_INCLUDE_MODULES	FLows_020100	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:25.0		1
XDB	SET_TABLESPACE	SYS	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:25.0		1
DON	BIN\$SPHkr9kUVUjgQAoKOAkSug==#0	JOE	UPDATE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:25.0		1
FLows_020100	UTL_FILE	SYS	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:25.0		1
HARRY	CREDITCARD	JOE	DELETE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:25.0		1
FLows_020100	DBA_SEGMENTS	SYS	SELECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
FLows_020100	WWW_FLOW_FILE_OBJECTS\$	FLows_FILES	QUERY REWRITE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
XDB	DBMS_REGISTRY	SYS	EXECUTE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
DON	BIN\$SPHkr9kUVUjgQAoKOAkSug==#0	JOE	DELETE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1

Records 1 to 20 of 230

__f. Oracle Entitlements for 'ORA PUBLIC Exec Priv on SYS Proc'.

ORA PUBLIC Exec Priv On SYS Proc					
Start Date: 2011-12-14 12:19:43 End Date: 2011-12-21 12:19:43					
Aliases: OFF					
Object Name	Object Type	Grantor	Datasource Name	SqlGuard Timestamp	Count of ORA PUBLIC Exec Priv on SYS Proc
URIFACTORY	PACKAGE	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
OWA_COOKIE	PACKAGE	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
IS_ALTER_COLUMN	FUNCTION	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
DBMS_STATS	PACKAGE	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
DBMS_REPUTIL2	PACKAGE	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
DBMS_FREQUENT_ITEMSET	PACKAGE	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
DATABASE_NAME	FUNCTION	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
TIMESTAMP_TO_SCN	FUNCTION	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
OWA_CACHE	PACKAGE	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
ISXMLTYPETABLE	FUNCTION	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
DBMS_STANDAR	PACKAGE	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
DBMS_REPUTIL	PACKAGE	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
DBMS_FILE_GROUP_IMP	PACKAGE	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
CLIENT_IP_ADDRESS	FUNCTION	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:44.0		1
TIMESTAMP_TO_SCN	FUNCTION	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
OWA_CACHE	PACKAGE	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
ISXMLTYPETABLE	FUNCTION	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
DBMS_STANDAR	PACKAGE	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
DBMS_REPUTIL	PACKAGE	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
DBMS_FILE_GROUP_IMP	PACKAGE	SYS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1

__g. Oracle Entitlements for 'ORA Roles Granted'.

ORA Roles Granted					
Start Date: 2011-12-14 12:19:43 End Date: 2011-12-21 12:19:43					
Aliases: OFF					
Grantee	User Or Role	Granted Role	Datasource Name	SqlGuard Timestamp	Count of ORA Roles Granted
SYSTEM	User	PLUSTRACE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
SQLGUARD	User	OEM_MONITOR	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
FLows_020100	User	SCHEDULER_ADMIN	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
BENJI	User	XDBADMIN	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
WEBAPP	User	CONNECT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
SYS	User	EXECUTE_CATALOG_ROLE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
HR	User	RESOURCE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
DBA	Role	HS_ADMIN_ROLE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
APPUSER	User	DBA	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
SYS	User	OEM_MONITOR	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
JOE	User	GATHER_SYSTEM_STATISTICS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
EXECUTE_CATALOG_ROLE	Role	HS_ADMIN_ROLE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
APPUSER	User	SCHEDULER_ADMIN	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
SYSTEM	User	AQ_ADMINISTRATOR_ROLE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
LOGSTDBY_ADMINISTRATOR	Role	RESOURCE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
FLows_020100	User	DELETE_CATALOG_ROLE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
BENJI	User	EXECUTE_CATALOG_ROLE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:01:26.0		1
FLows_020100	User	EXP_FULL_DATABASE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:45.0		1
BENJI	User	GATHER_SYSTEM_STATISTICS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:45.0		1
SYSTEM	User	SELECT_CATALOG_ROLE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0 : 2011-12-21 12:05:45.0		1

__h. Oracle Entitlements for 'ORA Sys Priv Granted'.

ORA Sys Priv Granted		
Start Date: 2011-12-14 12:19:42 End Date: 2011-12-21 12:19:42		
Aliases: OFF		
User Role Privilege	Datasource Name	SqlGuard Timestamp
>ANONYMOUS	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
->CREATE SESSION	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
>APPUSER	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
->CREATE VIEW	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
->DBA	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
-->CREATE OPERATOR	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
-->CREATE PROCEDURE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
-->CREATE PROFILE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
-->CREATE PUBLIC DATABASE LINK	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
-->CREATE PUBLIC SYNONYM	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
-->CREATE ROLE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
-->CREATE ROLLBACK SEGMENT	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
-->CREATE RULE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
-->CREATE RULE SET	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
-->CREATE SEQUENCE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
-->CREATE SESSION	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
-->CREATE SYNONYM	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
-->CREATE TABLE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
-->CREATE TABLESPACE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0
-->CREATE TRIGGER	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:26.0

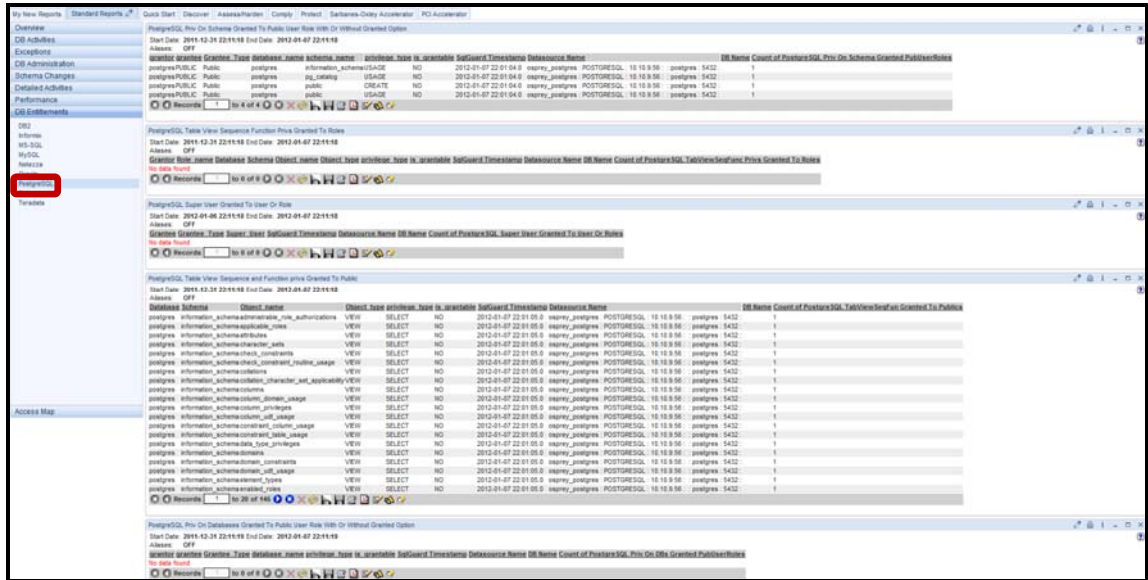
__i. Oracle Entitlements for 'ORA SYSDBA and SYSOPER Accnts'.

ORA SYSDBA and SYSOPER Accnts						
Start Date: 2011-12-14 12:19:39 End Date: 2011-12-21 12:19:39						
Aliases: OFF						
Username	Is Sysdba	Is Sysoper	Is External Password	Datasource Name	SqlGuard Timestamp	Count of ORA SYSDBA and SYSOPER Accnts
OLGA	TRUE	FALSE	FALSE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:29.0	1
SYS	TRUE	TRUE	FALSE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:01:29.0	1
OLGA	TRUE	FALSE	FALSE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:05:47.0	1
SYS	TRUE	TRUE	FALSE	osprey_system : ORACLE : 10.10.9.56 : xe : : 0	:2011-12-21 12:05:47.0	1

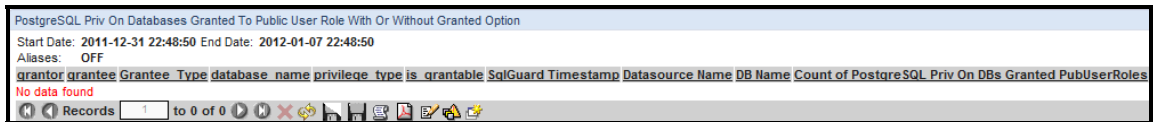
__8. Verify that PostgreSQL Entitlements Reports have been populated.

Note: Since this lab uses a new installation of PostgreSQL with very little data, only a small number of the PostgreSQL Entitlement Reports are populated with data.

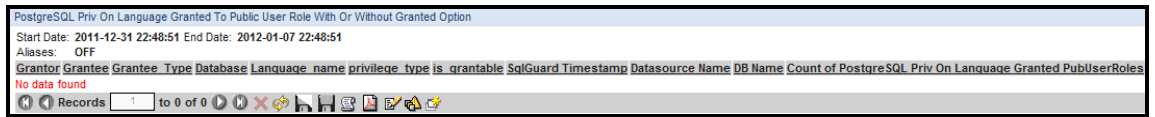
__a. Click **PosgreSQL**.



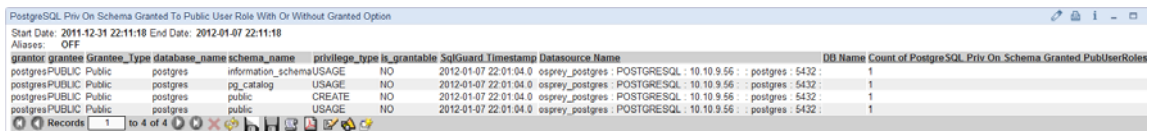
__b. PostgreSQL Entitlements for 'PostgreSQL Priv On DBs Granted PubUserRole'.



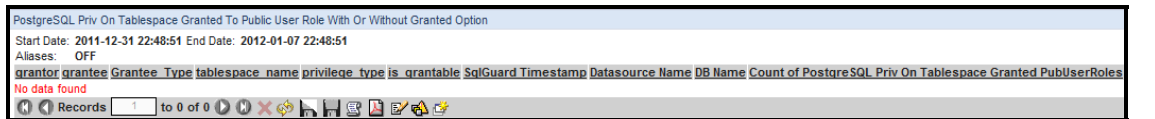
__c. PostgreSQL Entitlements for 'PostgreSQL Priv On Language Granted PubUserRole'.



__d. PostgreSQL Entitlements for 'PostgreSQL Priv On Schema Granted PubUserRole'.



__e. PostgreSQL Entitlements for 'PostgreSQL Priv On Tablespace Granted PubUserRole'.



f. PostgreSQL Entitlements for 'PostgreSQL Role Granted To User Or Role'.

PostgreSQL Role Granted To User Or Role												
Start Date: 2011-12-31 22:48:50 End Date: 2012-01-07 22:48:50												
Aliases: OFF												
grantee	grantee_type	role	name	role	or	login	is	grantable	SqlGuard Timestamp	Datasource Name	DB Name	Count of PostgreSQL Role Granted To User Or Roles
No data found												

g. PostgreSQL Entitlements for 'PostgreSQL Super User Granted To User Or Role'.

PostgreSQL Super User Granted To User Or Role									
Start Date: 2012-01-06 22:48:50 End Date: 2012-01-07 22:48:50									
Aliases: OFF									
grantee	grantee_type	super	user	SqlGuard Timestamp	Datasource Name	DB Name	Count of PostgreSQL Super User Granted To User Or Roles		
No data found									

h. PostgreSQL Entitlements for 'PostgreSQL Sys Privs Granted To User And Role'.

PostgreSQL Sys Privs Granted To User And Role																
Start Date: 2011-12-31 22:11:20 End Date: 2012-01-07 22:11:20																
Aliases: OFF																
grantee	grantee_type	super	user	inherits	privileges	create	role	create	database	update	system	catalog	SqlGuard Timestamp	Datasource Name	DB Name	Count of PostgreSQL Sys Privs Granted To User And Roles
postgres	User	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1

i. PostgreSQL Entitlements for 'PostgreSQL TabViewSeqFun Privs Granted To Public'.

PostgreSQL Table View Sequence and Function privs Granted To Public											
Start Date: 2011-12-31 22:11:10 End Date: 2012-01-07 22:11:10											
Aliases: OFF											
Database	Schema	Object name	Object type	privilege	type	is	grantable	SqlGuard Timestamp	Datasource Name	DB Name	Count of PostgreSQL TabViewSeqFun Granted To Public
postgres	information_schema	administrable_role_authorizations	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	asizable_roles	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	attributes	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	character_sets	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	check_constraints	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	check_constraint_routine_usage	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	collations	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	collation_character_set_applicability	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	columns	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	column_domain_usage	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	column_privileges	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	column_usage	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	constraint_catalog_usage	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	constraint_table_usage	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	data_type_privileges	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	domains	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	domain_constraints	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	domain_usage	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	element_types	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1
postgres	information_schema	enabled_roles	VIEW	SELECT		NO	NO	2012-01-07 22:01:05.0	osprey_postgres : PostgreSQL : 10.10.9.56	postgres : 5432	1

j. PostgreSQL Entitlements for 'PostgreSQL TabViewSeqFun Privs Granted To Login'.

PostgreSQL Table Views Sequence and Functions Privs Granted To Login													
Start Date: 2011-12-31 22:48:51 End Date: 2012-01-07 22:48:51													
Aliases: OFF													
grantor	user	database	schema	object name	object type	privilege	type	is	grantable	SqlGuard Timestamp	Datasource Name	DB Name	Count of PostgreSQL TabViewSeqFun Privs Granted To Logins
No data found													

k. PostgreSQL Entitlements for 'PostgreSQL TabViewSeqFun Privs Granted To Roles'.

PostgreSQL Table View Sequence Function Privs Granted To Roles														
Start Date: 2011-12-31 22:48:49 End Date: 2012-01-07 22:48:49														
Aliases: OFF														
grantor	role	name	database	schema	object name	object type	privilege	type	is	grantable	SqlGuard Timestamp	Datasource Name	DB Name	Count of PostgreSQL TabViewSeqFunc Privs Granted To Roles
No data found														

l. PostgreSQL Entitlements for 'PostgreSQL TabViewSeqFun Privs Granted with Grant'.

PostgreSQL Table View Sequence and Function Privs Granted With Grant Option														
Start Date: 2011-12-31 22:48:50 End Date: 2012-01-07 22:48:50														
Aliases: OFF														
grantor	grantee	grantee_type	database	schema	object name	object type	privilege	type	is	grantable	SqlGuard Timestamp	Datasource Name	DB Name	Count of PostgreSQL TabViewSeqFun Privs Granted with Grants
No data found														

__9. Verify that Sybase Entitlement Reports have been populated.

__a. Click **Sybase**.

The screenshot shows the IBM Security Guardium console interface. In the left-hand navigation pane, the 'Sybase' link is highlighted with a red rectangular box. The main content area displays three reports related to Sybase entitlements:

- SYBASE Object Privs by DB Acct:** Shows a table with columns: Grantee, Object, Type, Privilege, Role, Type of Grant, SqlGuard Timestamp, Datasource Name, DB Name, and Count. The report indicates 'No data found'.
- SYBASE Sys Priv And Role Granted To User:** Shows a table with columns: User, Privilege, Role, Type, Type of Grant, SqlGuard Timestamp, Datasource Name, DB Name, and Count. It lists several roles (oper_role, sa_role, sso_role, sybase_ts_role) granted to users (joe) on the 'sa_role' database.
- SYBASE Role Granted To User And Sys Privs Granted:** Shows a table with columns: Grantee, Grantee Type, Privilege, Role, Type, Type of Grant, SqlGuard Timestamp, Datasource Name, DB Name, and Count. It lists roles granted to users (joe) on the 'sa_role' database.

__b. Sybase Entitlements for 'SYBASE Object Privs by DB Acct'.

This screenshot shows a detailed view of the 'SYBASE Object Privs by DB Acct' report. The table has the following columns: Grantee, Object, Type, Privilege, Role, Type of Grant, SqlGuard Timestamp, Datasource Name, DB Name, and Count. The report indicates 'No data found'.

__c. Sybase Entitlements for 'SYBASE Sys Priv And Role Granted To User'.

This screenshot shows a detailed view of the 'SYBASE Sys Priv And Role Granted To User' report. The table has the following columns: User, Privilege, Role, Type, Type of Grant, SqlGuard Timestamp, Datasource Name, DB Name, and Count. The report lists roles granted to users (joe) on the 'sa_role' database.

User	Privilege	Role	Type	Type of Grant	SqlGuard Timestamp	Datasource Name	DB Name	Count of SYBASE Sys Priv And Role Granted To Users
dbo	oper_role	Role	Grant	2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56	: sn5u3000 : 4200		1
dbo	sa_role	Role	Grant	2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56	: sn5u3000 : 4200		1
dbo	sso_role	Role	Grant	2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56	: sn5u3000 : 4200		1
dbo	sybase_ts_role	Role	Grant	2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56	: sn5u3000 : 4200		1
joe	Create table	PrivilegesGrant		2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56	: sn5u3000 : 4200		1
joe	sa_role	Role	Grant	2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56	: sn5u3000 : 4200		1

d. Sybase Entitlements for 'SYBASE Role Granted To User And Sys Privs Granted'.

Grantee	Grantee Type	Privilege	Role Type	Type of Grant	SqlGuard Timestamp	Datasource Name	DB Name	Count of SYBASE Role Granted To User And Sys Privs Granted
dbo User	oper_role	Role	Grant	2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :			1
dbo User	sa_role	Role	Grant	2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :			1
dbo User	sso_role	Role	Grant	2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :			1
dbo User	sybase_ts_role	Role	Grant	2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :			1
joe User	Create table	Privilege	Grant	2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :			1
joe User	sa_role	Role	Grant	2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :			1

e. Sybase Entitlements for 'SYBASE Object Access By Public'.

Owner	Object Name	Object Type	Privileges	Grant Type	SqlGuard Timestamp	Datasource Name	DB Name	Count of SYBASE Object Access By Publics
dbo	sysreferences	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	sysalternates	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	syspartitions	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	sysusers	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	syskeys	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	sysabstats	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	sysdepends	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	sysroles	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	sysattributes	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	sysprocedures	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	syskypes	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	syslogs	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	systhresholds	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	sysencryptkeys	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	syssegments	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	syscolumns	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	sysprotects	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	sysobjects	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	sysotypes	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	sysindexes	System table	Select	Grant	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1

f. Sybase Entitlements for 'SYBASE Execute Priv On Proc Func To Public'.

Schema	Owner	Grantor	Object Name	Object Type	Privileges	Grant Type	SqlGuard Timestamp	Datasource Name	DB Name	Count of SYBASE Execute Priv On Proc Func To Publics
No data found										

g. Sybase Entitlements for 'SYBASE Accnts With Sys Or Sec Admin Roles'.

Login	Role	SqlGuard Timestamp	Datasource Name	Count of SYBASE Accnts With Sys Or Sec Admin Roles
joe	sa_role	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :	1
sa	sybase_ts_role	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :	1
sa	sso_role	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :	1
sa	sa_role	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :	1
sa	oper_role	2011-12-21 17:48:26.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :	1

h. Sybase Entitlements for 'SYBASE Obj Col Privs Granted With Grant'.

Grantee	Privileges	Object Name	Object Type	Schema	Owner	Grantor	SqlGuard Timestamp	Datasource Name	DB Name	Count of SYBASE Obj Col Privs Granted With Grants
No data found										

__i. Sybase Entitlements for 'SYBASE Role Granted To User'.

SYBASE Role Granted To User					
Start Date: 2011-12-14 19:12:17 End Date: 2011-12-21 19:12:17					
Aliases: OFF					
Grantee	Role	SqlGuard Timestamp	Datasource Name	DB Name	Count of SYBASE Role Granted To Users
dbo	oper_role	2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
joe	sa_role	2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	sybase_ts_role	2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	sso_role	2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1
dbo	sa_role	2011-12-21 17:48:27.0	osprey_sa : SYBASE : 10.10.9.56 : : sn5u3000 : 4200 :		1

Records 1 to 5 of 5

Thank You

Entitlement Reports review

- __1. Entitlement reports run on:
- __a. The InfoSphere Guardium Collector
 - __b. The database server
 - __c. The client PC
 - __d. Part of IBM S-TAP™.
- __2. Database Entitlement Reports use the Enterprise Integrator (Custom Domain) feature of Guardium.
(**True or False**)
- __3. Where does the Entitlement Reports audit data originate?
- __a. Before running the reports, data is restored from the database
 - __b. A direct connection to database system tables
 - __c. The report data is based upon the entitlement custom domain.
 - __d. The reports collect the data from internal GDM tables.
- __4. Why does Guardium require a Datasource to be assigned to each relevant entitlement report?
- __a. To organize the Guardium reports
 - __b. The Datasource points Guardium to the source of database system tables
 - __c. Datasource is required for database admin
- __5. Database Entitlements Reports are an optional component enabled by the product key.
(**True or False**)

Entitlement Reports review (Answers)

__1. Entitlement Reports run on:

A – The InfoSphere Guardium Collector.

__2. DB Entitlement Reports use the Enterprise Integrator (Custom Domain) feature of Guardium.
(**True** or **False**)

True.

__3. From where does the Entitlement Reports audit data originate?

C – The report data is based upon the entitlement custom domain.

__4. Why do we need to assign a Datasource to the relevant entitlement reports?

B – The Datasource points Guardium to the source of database system tables.

__5. DB Entitlements Reports are an optional component enabled by the product key.
(**True** or **False**)

True.

Lab 4 Guardium Client Installation

4.1 Silent S-TAP and Configuration Auditing System (CAS) deployment

Overview

Unique in the industry, S-TAPs are non-intrusive software probes that monitor both network and local database protocols (for example, shared memory, named pipes) at the operating system level of the database server. S-TAPs minimize any effect on server performance by relaying all traffic to separate InfoSphere Guardium appliances for real-time analysis and reporting, rather than relying on the database itself to process and store log data. S-TAPs are often preferred because they eliminate the need for dedicated hardware appliances in remote locations or available SPAN ports in your data center.

The CAS module can be installed as part of an S-TAP installation or as a separate installation. The CAS agent runs as a Java program and thus needs Java 1.4 or above installed on the host. Java is a prerequisite and the CAS agent installer asks for the location of the Java installation.

The IBM InfoSphere Guardium solution enables customers to:

- Deploy a lightweight software probe that monitors all local and network database activity while requiring minimal resource usage and maintenance.
- Scale across enterprise heterogeneous database and operating system platforms.
- Avoid the risks associated with database or application changes.
- Continuously monitor access and changes to high value databases.
- Block unauthorized changes to sensitive objects..

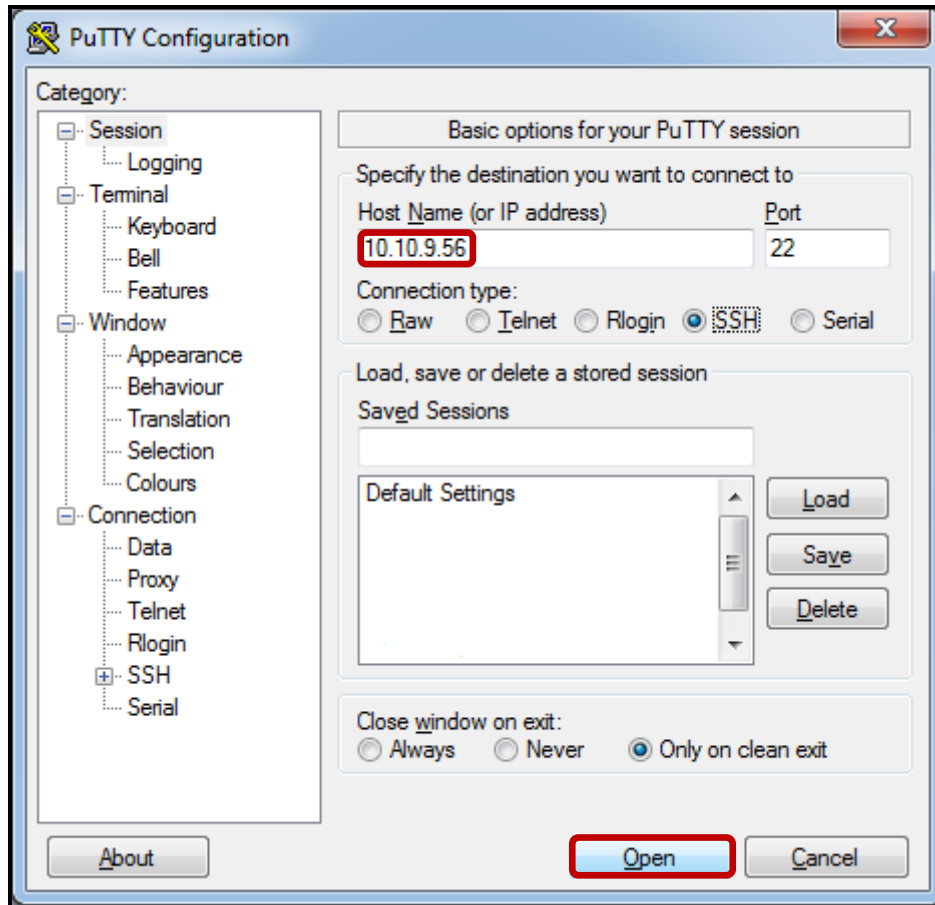
Objectives

This lab will demonstrate the ease with which the IBM InfoSphere Guardium solution can be deployed in an enterprise environment. We will focus on using standard shell scripts and the IBM InfoSphere Guardium GrdAPI command line interface to perform silent, scripted installations and configurations of the Guardium S-TAP and CAS software probes.

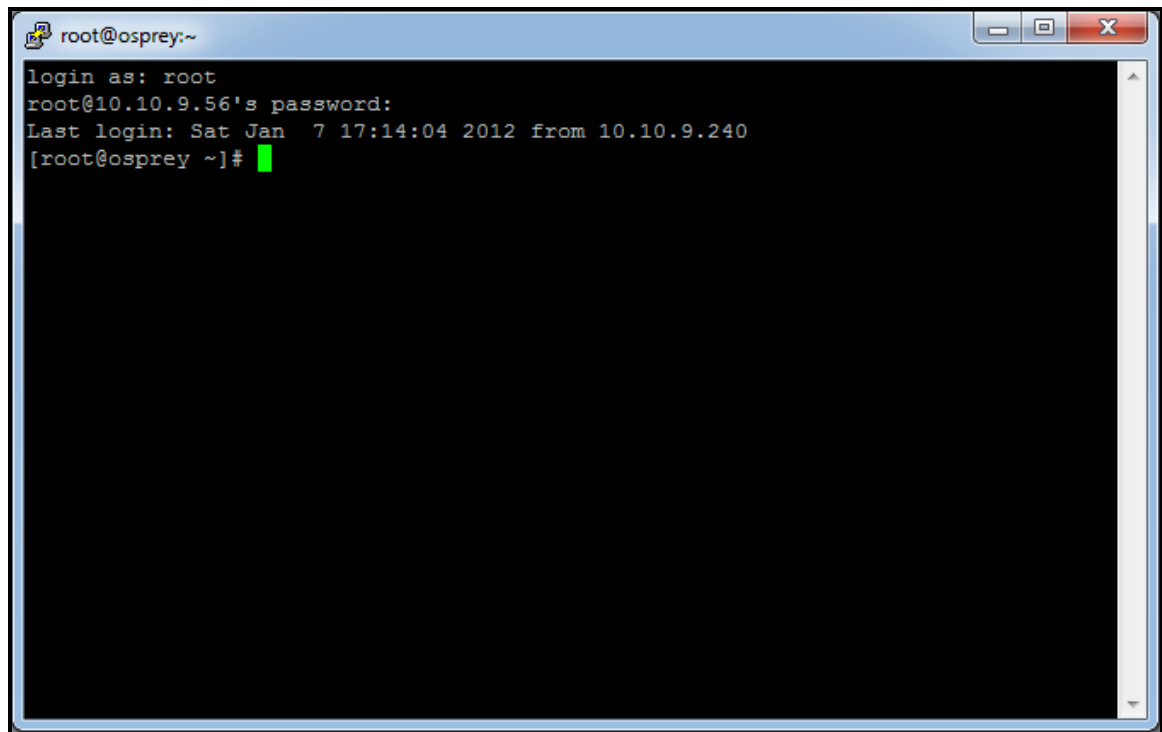
The following steps will guide us through the lab:

- __1. Install the IBM InfoSphere Guardium lightweight software probe (S-TAP)
- __2. Install the IBM InfoSphere Guardium Change Audit System (CAS)
- __3. Silently configure the IBM InfoSphere Guardium Inspection Engine for each database platform (Oracle, DB2 and Sybase) using the GrdAPI command line interface
- __4. Use the Browser-based interface to validate a successful installation

- __1. Using a PuTTY SSH client, access the VM database server to demonstrate the ease with which the IBM InfoSphere Guardium solution can be automatically and silently deployed.
 - __a. Start the PuTTY SSH client login.
 - __b. From your laptop, launch PuTTY, enter **10.10.9.56**, and click **Open**.

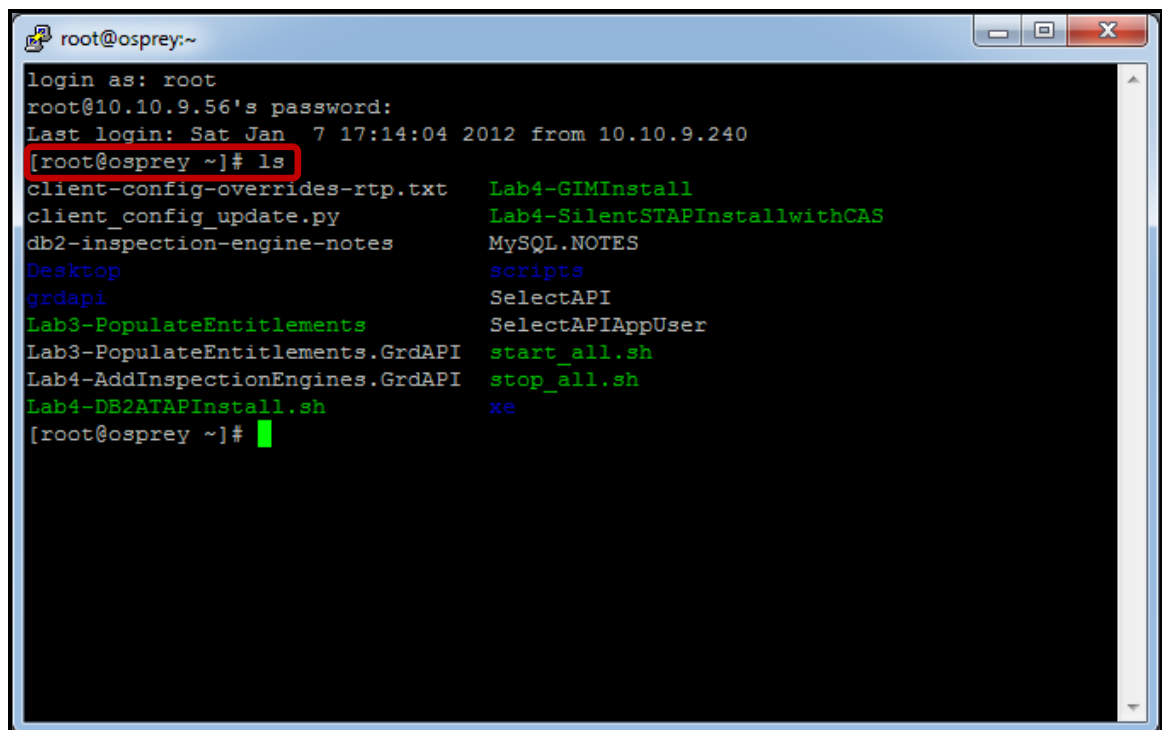


- __c. Login as **root** / **guardium**. After logging in, the following prompt will be displayed.



```
root@osprey:~  
login as: root  
root@10.10.9.56's password:  
Last login: Sat Jan 7 17:14:04 2012 from 10.10.9.240  
[root@osprey ~]#
```

- __d. Type **ls** to get a list of available files.

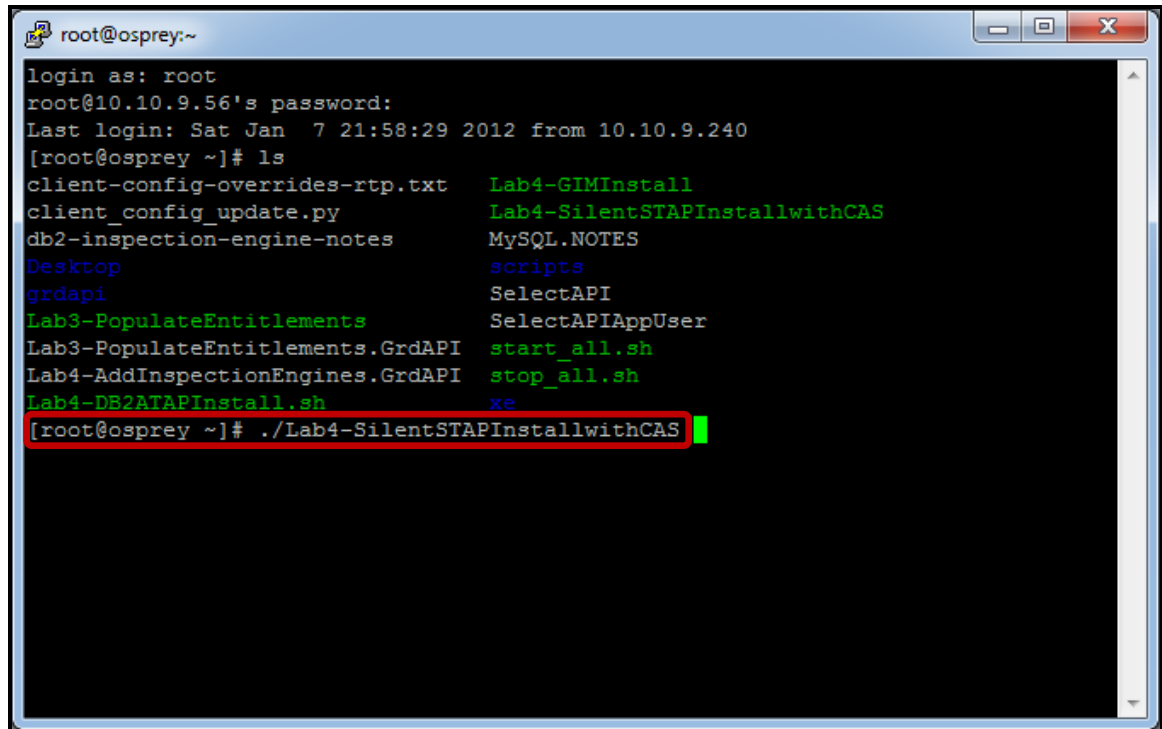


```
root@osprey:~  
login as: root  
root@10.10.9.56's password:  
Last login: Sat Jan 7 17:14:04 2012 from 10.10.9.240  
[root@osprey ~]# ls  
client-config-overrides-rtp.txt    Lab4-GIMInstall  
client_config_update.py           Lab4-SilentSTAPInstallwithCAS  
db2-inspection-engine-notes       MySQL.NOTES  
Desktop                            scripts  
grdapi                             SelectAPI  
Lab3-PopulateEntitlements         SelectAPIAppUser  
Lab3-PopulateEntitlements.GrdAPI  start_all.sh  
Lab4-AddInspectionEngines.GrdAPI  stop_all.sh  
Lab4-DB2ATAPInstall.sh           xe  
[root@osprey ~]#
```

Check that you see the files listed above in the /root directory.

- __e. Start the Silent install process by executing the following script:

./Lab4-SilentSTAPInstallwithCAS

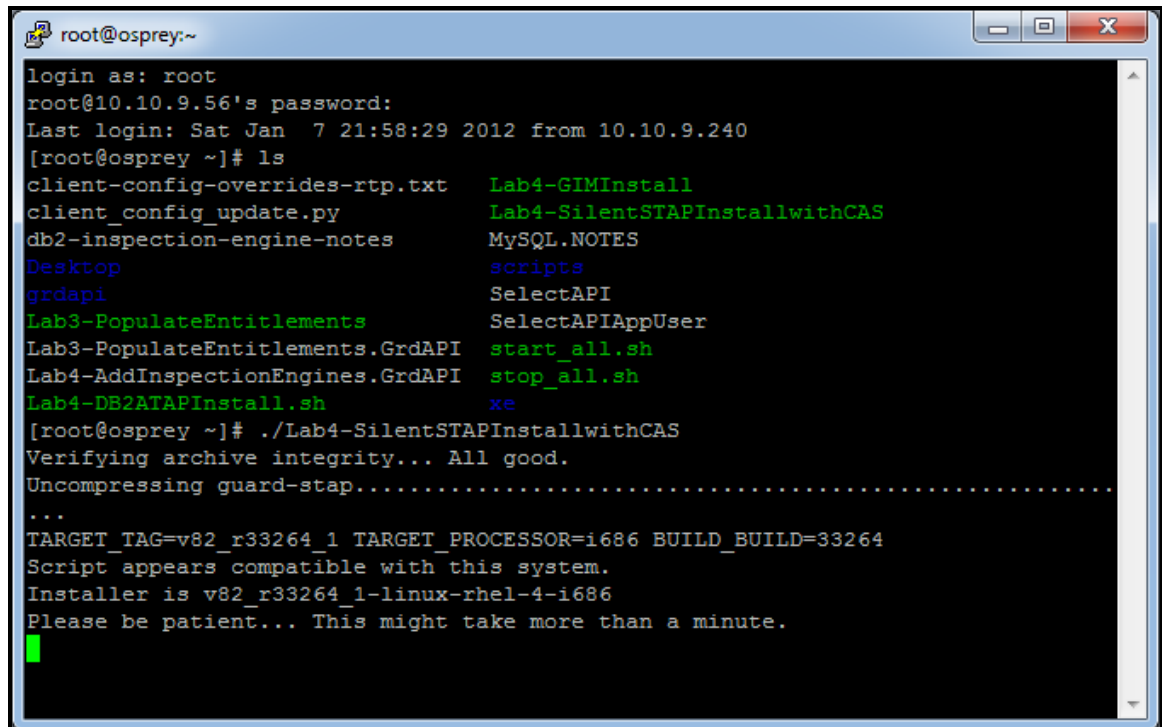


```

root@osprey:~
login as: root
root@10.10.9.56's password:
Last login: Sat Jan 7 21:58:29 2012 from 10.10.9.240
[root@osprey ~]# ls
client-config-overrides-rtp.txt      Lab4-GIMInstall
client_config_update.py              Lab4-SilentSTAPInstallwithCAS
db2-inspection-engine-notes          MySQL.NOTES
Desktop                               scripts
grdapi                               SelectAPI
Lab3-PopulateEntitlements             SelectAPIAppUser
Lab3-PopulateEntitlements.GrdAPI      start_all.sh
Lab4-AddInspectionEngines.GrdAPI     stop_all.sh
Lab4-DB2ATAPInstall.sh               xe
[root@osprey ~]# ./Lab4-SilentSTAPInstallwithCAS

```

- __f. Silent Install Progress – Starting S-TAP install



```

root@osprey:~
login as: root
root@10.10.9.56's password:
Last login: Sat Jan 7 21:58:29 2012 from 10.10.9.240
[root@osprey ~]# ls
client-config-overrides-rtp.txt      Lab4-GIMInstall
client_config_update.py              Lab4-SilentSTAPInstallwithCAS
db2-inspection-engine-notes          MySQL.NOTES
Desktop                               scripts
grdapi                               SelectAPI
Lab3-PopulateEntitlements             SelectAPIAppUser
Lab3-PopulateEntitlements.GrdAPI      start_all.sh
Lab4-AddInspectionEngines.GrdAPI     stop_all.sh
Lab4-DB2ATAPInstall.sh               xe
[root@osprey ~]# ./Lab4-SilentSTAPInstallwithCAS
Verifying archive integrity... All good.
Uncompressing guard-stap.....
...
TARGET_TAG=v82_r33264_1 TARGET_PROCESSOR=i686 BUILD_BUILD=33264
Script appears compatible with this system.
Installer is v82_r33264_1-linux-rhel-4-i686
Please be patient... This might take more than a minute.

```

The contents of the **Lab4-SilentSTAPInstallwithCAS** script:

```
# STAP Installation
/tmp/guard-stap-v82_r33264_1-rhel-4-linux-i686.sh -- --modules /tmp/modules-
v82_r33264_1.tgz --ni --tls 1 -k --dir /usr/local --tapip 10.10.9.56 --sqlguardip
10.10.9.248 --presets firewall_installed=1 hunter_trace=1

# CAS Installation
/tmp/guard-cas-v82_r33264_1-rhel-4-linux-i686.sh -- install --java-home /usr/java
--stap-conf /usr/local/guardium/guard_stap/guard_tap.ini

# Create Inspection Engines
ssh cli@10.10.9.248 < Lab4-AddInspectionEngines.GrdAPI
```

The contents of the **Lab4-AddInspectionEngines.GrdAPI** script:

```
# DB2
grdapi create_stap_inspection_engine stapHost=10.10.9.56 protocol=DB2
portMin=50001 portMax=50001 dbInstallDir=/home/db2inst2
procName=/home/db2inst2/sqllib/adm/db2sysc client=0.0.0.0/0.0.0.0
db2SharedMemAdjustment=20 db2SharedMemClientPosition=61440
db2SharedMemSize=131072 ktapDbPort=50001

# MySQL
grdapi create_stap_inspection_engine stapHost=10.10.9.56 protocol=MySQL
portMin=3306 portMax=3306 dbInstallDir=NULL procName=mysql
client=0.0.0.0/0.0.0.0 ktapDbPort=3306

# Oracle
grdapi create_stap_inspection_engine stapHost=10.10.9.56 protocol=Oracle
portMin=1521 portMax=1521 dbInstallDir=/usr/lib/oracle/xe
procName=/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/bin/oracle
client=0.0.0.0/0.0.0.0 ktapDbPort=1521

# PostgreSQL
grdapi create_stap_inspection_engine stapHost=10.10.9.56
protocol=PostgreSQL portMin=5432 portMax=5432 dbInstallDir=NULL
procName=PostgreSQL client=0.0.0.0/0.0.0.0 ktapDbPort=5432

# Sybase
grdapi create_stap_inspection_engine stapHost=10.10.9.56 protocol=Sybase
portMin=4200 portMax=4200 client=0.0.0.0/0.0.0.0 ktapDbPort=4200

exit
```

__g. Silent Install Progress – KTAP installed

```

root@osprey:~
grdapi                               SelectAPI
Lab3~PopulateEntitlements             SelectAPIAppUser
Lab3~PopulateEntitlements.GrdAPI      start_all.sh
Lab4~AddInspectionEngines.GrdAPI     stop_all.sh
Lab4~DB2ATAPInstall.sh               xe
[root@osprey ~]# ./Lab4-SilentSTAPInstallwithCAS
Verifying archive integrity... All good.
Uncompressing guard-stap.....
...
TARGET_TAG=v82_r33264_1 TARGET_PROCESSOR=i686 BUILD_BUILD=33264
Script appears compatible with this system.
Installer is v82_r33264_1-linux-rhel-4-i686
Please be patient... This might take more than a minute.
Copying installation files...
Current ktap is:
lrwxrwxrwx  1 root root 5 Jan  8 00:47 /usr/local/guardium/guard_stap/ktap/current -> 33264
Testing guard_stap -
STAP-v82_r33264_1-20110812_0001

No missing dependencies
Installing Ktap module
KTAP installed

```

__h. Silent Install Progress – Searching for KTAP module

```

root@osprey:~
IP for 10.10.9.56 is 38090a0a
Tap Debug level = 3
Parsed param list:
  <connection_pool_size> = <0>
  <primary> = <1>
  <sqlguard_ip> = <10.10.9.248>
  <sqlguard_port> = <16016>
Parsing SQLGuard section SQLGuard_0
IP for 10.10.9.248 is f8090a0a
hostname is osprey
Local IPs
ip = 127.0.0.1
ip = 10.10.9.56
Using inifile /usr/local/guardium/guard_stap/guard_tap.ini, backup file /usr/local/guardium/guard_stap/guard_tap.ini.bak
Buffer attached, starting at 16(0x10), next free 16(10)
Guardium STAP config file OK.

Your configuration has been validated.

We have been able to provide you with a working copy of LSOF, it has run
Starting Ktap module
Searching for modules in /tmp/modules-v82_r33264_1.tgz

```


__i. Silent Install Progress – Extracting RedHat KTAP module

```

root@osprey:~
    <primary> = <1>
    <sqlguard_ip> = <10.10.9.248>
    <sqlguard_port> = <16016>
Parsing SQLGuard section SQLGuard_0
IP for 10.10.9.248 is f8090a0a
hostname is osprey
Local IPs
ip = 127.0.0.1
ip = 10.10.9.56
Using inifile /usr/local/guardium/guard_stap/guard_tap.ini, backup file /usr/local/guardium/guard_stap/guard_tap.ini.bak
Buffer attached, starting at 16(0x10), next free 16(10)
Guardium STAP config file OK.

Your configuration has been validated.

We have been able to provide you with a working copy of LSOF, it has run
Starting Ktap module
Searching for modules in /tmp/modules-v82_r33264_1.tgz
guard_ktap_loader: Module ktap-v82_r33264_1-rh4u4x32m-2.6.9-42.0.3.EL-i686-UP.ko
selected for kernel 2.6.9-42.0.3.EL.
Extracted module ktap-v82_r33264_1-rh4u4x32m-2.6.9-42.0.3.EL-i686-UP.ko from /tmp/modules-v82_r33264_1.tgz

```

__j. Silent Install Progress – STAP install finished

```

root@osprey:~
IP for 10.10.9.248 is f8090a0a
hostname is osprey
Local IPs
ip = 127.0.0.1
ip = 10.10.9.56
Using inifile /usr/local/guardium/guard_stap/guard_tap.ini, backup file /usr/local/guardium/guard_stap/guard_tap.ini.bak
Buffer attached, starting at 16(0x10), next free 16(10)
Guardium STAP config file OK.

Your configuration has been validated.

We have been able to provide you with a working copy of LSOF, it has run
Starting Ktap module
Searching for modules in /tmp/modules-v82_r33264_1.tgz
guard_ktap_loader: Module ktap-v82_r33264_1-rh4u4x32m-2.6.9-42.0.3.EL-i686-UP.ko
selected for kernel 2.6.9-42.0.3.EL.
Extracted module ktap-v82_r33264_1-rh4u4x32m-2.6.9-42.0.3.EL-i686-UP.ko from /tmp/modules-v82_r33264_1.tgz
KTAP loaded
guard_hnt is using this perl binary: /usr/bin/perl
guard_hnt is using this lsof binary: /usr/sbin/lsof
Install finished

```

__k. Silent Install Progress – Starting CAS install

```

root@osprey:~
ip = 127.0.0.1
ip = 10.10.9.56
Using inifile /usr/local/guardium/guard_stap/guard_tap.ini, backup file /usr/local/guardium/guard_stap/guard_tap.ini.bak
Buffer attached, starting at 16(0x10), next free 16(10)
Guardium STAP config file OK.

Your configuration has been validated.

We have been able to provide you with a working copy of LSOF, it has run
Starting Ktap module
Searching for modules in /tmp/modules-v82_r33264_1.tgz
guard_ktap_loader: Module ktap-v82_r33264_1-rh4u4x32m-2.6.9-42.0.3.EL-i686-UP.ko
selected for kernel 2.6.9-42.0.3.EL.
Extracted module ktap-v82_r33264_1-rh4u4x32m-2.6.9-42.0.3.EL-i686-UP.ko from /tmp/modules-v82_r33264_1.tgz
KTAP loaded
guard_hnt is using this perl binary: /usr/bin/perl
guard_hnt is using this lsof binary: /usr/sbin/lsof
Install finished
Verifying archive integrity... All good.
Uncompressing guard-cas.....
.....

```

__l. Silent Install Progress – CAS install finished

```

root@osprey:~
Starting Ktap module
Searching for modules in /tmp/modules-v82_r33264_1.tgz
guard_ktap_loader: Module ktap-v82_r33264_1-rh4u4x32m-2.6.9-42.0.3.EL-i686-UP.ko
selected for kernel 2.6.9-42.0.3.EL.
Extracted module ktap-v82_r33264_1-rh4u4x32m-2.6.9-42.0.3.EL-i686-UP.ko from /tmp/modules-v82_r33264_1.tgz
KTAP loaded
guard_hnt is using this perl binary: /usr/bin/perl
guard_hnt is using this lsof binary: /usr/sbin/lsof
Install finished
Verifying archive integrity... All good.
Uncompressing guard-cas.....
.....
Running bin/guard-executor-32
bin conf etc lib scripts
Platform runs bin/guard-executor-32
Java location verified -
Installing CAS under /usr/local/guardium/guard_stap/cas using Java in /usr/java
Using /usr/local/guardium/guard_stap/guard_tap.ini as guard_tap.ini
Edited /etc/inittab.guard-20111216_103552 original is preserved in /etc/inittab.guard-20111216_103552.guard-save-20111216_103552
CAS install finished.
Pseudo-terminal will not be allocated because stdin is not a terminal.

```

- __m. **Critical Step** – Silent Install Progress – Appliance Login. Type **guardium** when prompted for **cli@10.10.9.248's password:**.

```

root@osprey:~
selected for kernel 2.6.9-42.0.3.EL.
Extracted module ktap-v82_r33264_1-rh4u4x32m-2.6.9-42.0.3.EL-i686-UP.ko from /tm
p/modules-v82_r33264_1.tgz
KTAP loaded
guard_hnt is using this perl binary: /usr/bin/perl
guard_hnt is using this lsof binary: /usr/sbin/lsof
Install finished
Verifying archive integrity... All good.
Uncompressing guard-cas.....
.....
Running bin/guard-executor-32
bin conf etc lib scripts
Platform runs bin/guard-executor-32
Java location verified -
Installing CAS under /usr/local/guardium/guard_stap/cas using Java in /usr/java
Using /usr/local/guardium/guard_stap/guard_tap.ini as guard_tap.ini
Edited /etc/inittab.guard-20111216_103552 original is preserved in /etc/inittab.
guard-20111216_103552.guard-save-20111216_103552
CAS install finished.
Pseudo-terminal will not be allocated because stdin is not a terminal.

IBM InfoSphere Guardium, Command Line Interface (CLI)

cli@10.10.9.248's password:

```

- __n. Silent Install Progress – Silently configuring Inspection Engines using GrdAPI on Appliance

```

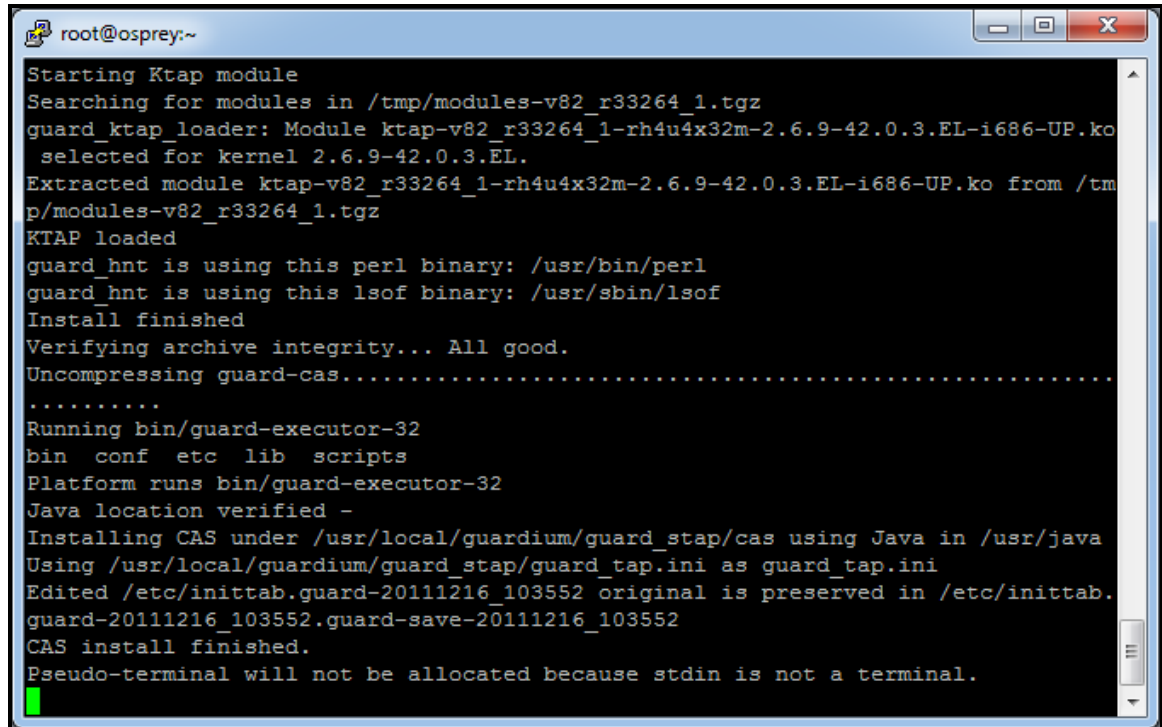
root@osprey:~
p/modules-v82_r33264_1.tgz
KTAP loaded
guard_hnt is using this perl binary: /usr/bin/perl
guard_hnt is using this lsof binary: /usr/sbin/lsof
Install finished
Verifying archive integrity... All good.
Uncompressing guard-cas.....
.....
Running bin/guard-executor-32
bin conf etc lib scripts
Platform runs bin/guard-executor-32
Java location verified -
Installing CAS under /usr/local/guardium/guard_stap/cas using Java in /usr/java
Using /usr/local/guardium/guard_stap/guard_tap.ini as guard_tap.ini
Edited /etc/inittab.guard-20111216_103552 original is preserved in /etc/inittab.
guard-20111216_103552.guard-save-20111216_103552
CAS install finished.
Pseudo-terminal will not be allocated because stdin is not a terminal.

IBM InfoSphere Guardium, Command Line Interface (CLI)

cli@10.10.9.248's password:
Welcome cli - your last login was Thu Dec  8 18:07:49 2011
G82.ibm.com> G82.ibm.com>

```

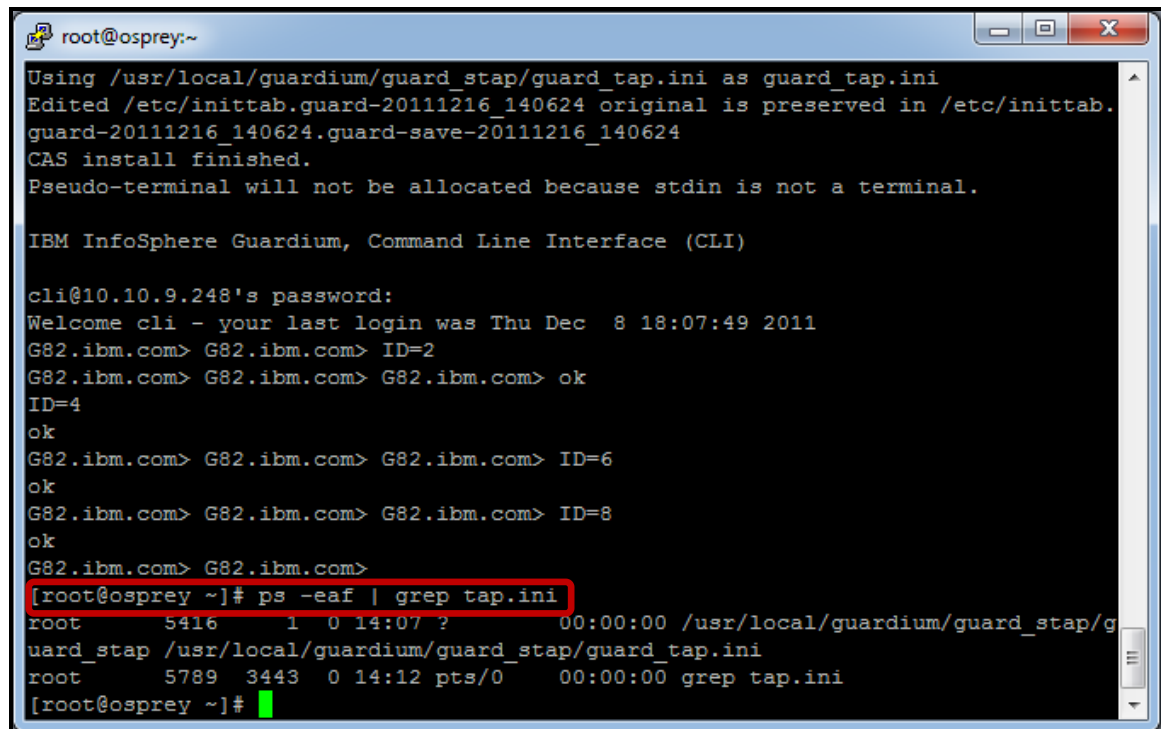
- __o. Silent Install Progress – Silent install complete. An “ID=N” for each GrdAPI command. A total of four Inspection Engines have been created.



```
root@osprey:~  
Starting Ktap module  
Searching for modules in /tmp/modules-v82_r33264_1.tgz  
guard_ktap_loader: Module ktap-v82_r33264_1-rh4u4x32m-2.6.9-42.0.3.EL-i686-UP.ko  
selected for kernel 2.6.9-42.0.3.EL.  
Extracted module ktap-v82_r33264_1-rh4u4x32m-2.6.9-42.0.3.EL-i686-UP.ko from /tm  
p/modules-v82_r33264_1.tgz  
KTAP loaded  
guard_hnt is using this perl binary: /usr/bin/perl  
guard_hnt is using this lsof binary: /usr/sbin/lsof  
Install finished  
Verifying archive integrity... All good.  
Uncompressing guard-cas.....  
.....  
Running bin/guard-executor-32  
bin conf etc lib scripts  
Platform runs bin/guard-executor-32  
Java location verified -  
Installing CAS under /usr/local/guardium/guard_stap/cas using Java in /usr/java  
Using /usr/local/guardium/guard_stap/guard_tap.ini as guard_tap.ini  
Edited /etc/inittab.guard-20111216_103552 original is preserved in /etc/inittab.  
guard-20111216_103552.guard-save-20111216_103552  
CAS install finished.  
Pseudo-terminal will not be allocated because stdin is not a terminal.
```

__2. Verify that S-TAP is running

__a. Type `ps -eaf | grep tap.ini` to confirm that the S-TAP process is running.



```
root@osprey:~  
Using /usr/local/guardium/guard_stap/guard_tap.ini as guard_tap.ini  
Edited /etc/inittab.guard-20111216_140624 original is preserved in /etc/inittab.  
guard-20111216_140624.guard-save-20111216_140624  
CAS install finished.  
Pseudo-terminal will not be allocated because stdin is not a terminal.  
  
IBM InfoSphere Guardium, Command Line Interface (CLI)  
  
cli@10.10.9.248's password:  
Welcome cli - your last login was Thu Dec  8 18:07:49 2011  
G82.ibm.com> G82.ibm.com> ID=2  
G82.ibm.com> G82.ibm.com> G82.ibm.com> ok  
ID=4  
ok  
G82.ibm.com> G82.ibm.com> G82.ibm.com> ID=6  
ok  
G82.ibm.com> G82.ibm.com> G82.ibm.com> ID=8  
ok  
G82.ibm.com> G82.ibm.com>  
[root@osprey ~]# ps -eaf | grep tap.ini  
root    5416      1  0 14:07 ?        00:00:00 /usr/local/guardium/guard_stap/g  
uard_stap /usr/local/guardium/guard_stap/guard_tap.ini  
root    5789    3443  0 14:12 pts/0    00:00:00 grep tap.ini  
[root@osprey ~]#
```

__3. Verify that CAS is running

- __a. Type `ps -eaf | grep cas` to confirm that the CAS process is running.

```

root@osprey:~
Using /usr/local/guardium/guard_stap/guard_tap.ini as guard_tap.ini
Edited /etc/inittab.guard-20111216_140624 original is preserved in /etc/inittab.
guard-20111216_140624.guard-save-20111216_140624
CAS install finished.
Pseudo-terminal will not be allocated because stdin is not a terminal.

IBM InfoSphere Guardium, Command Line Interface (CLI)

cli@10.10.9.248's password:
Welcome cli - your last login was Thu Dec  8 18:07:49 2011
G82.ibm.com> G82.ibm.com> ID=2
G82.ibm.com> G82.ibm.com> G82.ibm.com> ok
ID=4
ok
G82.ibm.com> G82.ibm.com> G82.ibm.com> ID=6
ok
G82.ibm.com> G82.ibm.com> G82.ibm.com> ID=8
ok
G82.ibm.com> G82.ibm.com>
[root@osprey ~]# ps -eaf | grep tap.ini
root      5416      1  0 14:07 ?          00:00:00 /usr/local/guardium/guard_stap/g
uard_stap /usr/local/guardium/guard_stap/guard_tap.ini
root      5789    3443  0 14:12 pts/0    00:00:00 grep tap.ini
[root@osprey ~]# ps -eaf | grep cas

```

```

root@osprey:~
root      5333    5316  0 14:06 ?          00:00:00 /usr/java/bin/java -Djava.class.
path=/usr/local/guardium/guard_stap/cas/lib/terajdbc4.jar:/usr/local/guardium/gu
ard_stap/cas/lib/postgresql-8.3-604.jdbc3.jar:/usr/local/guardium/guard_stap/cas
/lib/ojdbc14.jar:/usr/local/guardium/guard_stap/cas/lib/ifxjdbc.jar:/usr/local/g
uardium/guard_stap/cas/lib/jconn3.jar:/usr/local/guardium/guard_stap/cas/lib/jtd
s-1.2.2.jar:/usr/local/guardium/guard_stap/cas/lib/tdgssconfig.jar:/usr/local/gu
ardium/guard_stap/cas/lib/ddSqlServer.jar:/usr/local/guardium/guard_stap/cas/lib
/db2jcc.jar:/usr/local/guardium/guard_stap/cas/lib/jRegistryKey.jar:/usr/local/g
uardium/guard_stap/cas/lib/log4j-1.2.6.jar:/usr/local/guardium/guard_stap/cas/li
b/EccpressoFIPsJca.jar:/usr/local/guardium/guard_stap/cas/lib/cas_client.jar:/us
r/local/guardium/guard_stap/cas/lib/EccpressoFIPs.jar:/usr/local/guardium/guard
_stap/cas/lib/Text_JDBC30.jar:/usr/local/guardium/guard_stap/cas/lib/jt400.jar:/u
sr/local/guardium/guard_stap/cas/lib/nativeloader-200505172341.jar:/usr/local/gu
ardium/guard_stap/cas/lib/db2jcc_license_cu.jar:/usr/local/guardium/guard_stap/c
as/lib/bcprov-jdk14-144.jar:/usr/local/guardium/guard_stap/cas/lib/ddOracle.jar:
/usr/local/guardium/guard_stap/cas/lib/jcifs.jar:/usr/local/guardium/guard_stap/
cas/lib/tarbz2.jar:/usr/local/guardium/guard_stap/cas/lib/nzjdbc.jar:/usr/local/
guardium/guard_stap/cas/lib/jconn2.jar:/usr/local/guardium/guard_stap/cas/lib/td
gssjava.jar:/usr/local/guardium/guard_stap/cas/lib/nativecall-0.4.1.jar:/usr/loc
al/guardium/guard_stap/cas/lib/mysql-connector-java-5.0.5-bin.jar: -Djava.library
.path=/usr/local/guardium/guard_stap/cas/lib -Xms128M -Xmx512M -Dpre.exe.env1=V
UE="" -DcasRestartTimer=1440 com.guardium.cas.client.CASClient
root      5867    3443  0 14:13 pts/0    00:00:00 grep cas
[root@osprey ~]#

```

- __4. Now, launch the InfoSphere Guardium GUI to verify the installation, and Inspection Engines.
- __a. From your laptop, browse to <https://10.10.9.248:8443>
- __b. Login as user **pot** / **guardium**.

Login

Please enter your information

User name:

Password:

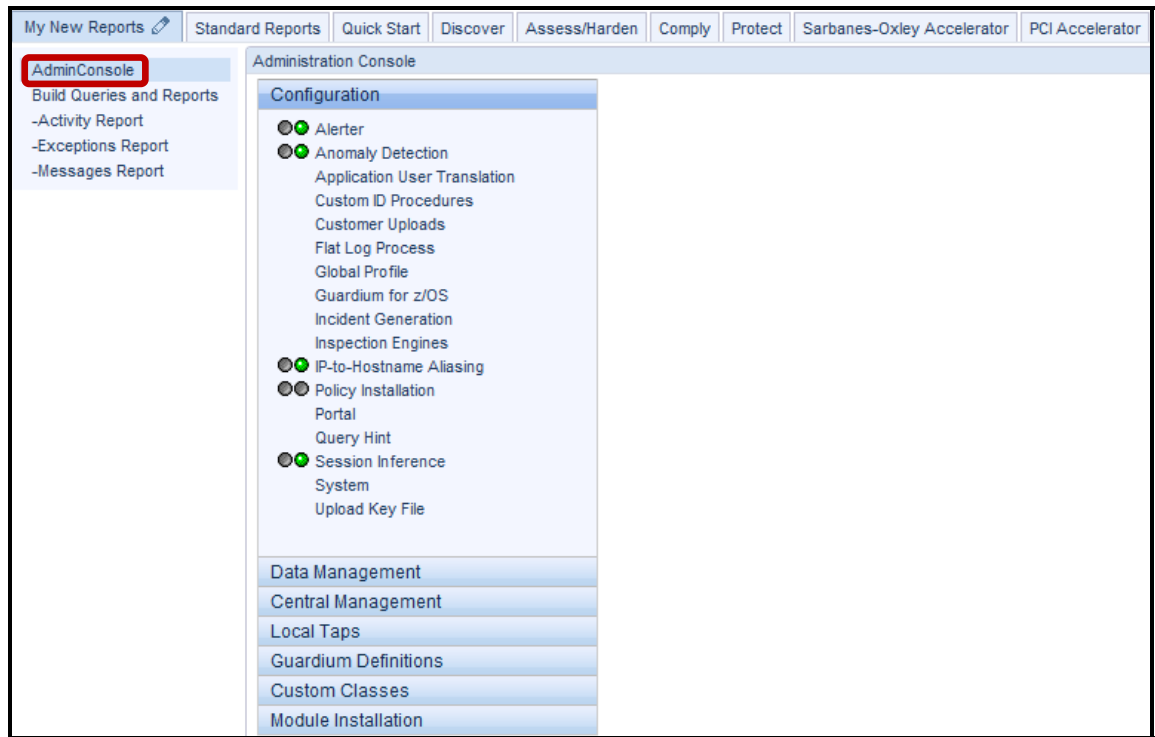
Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

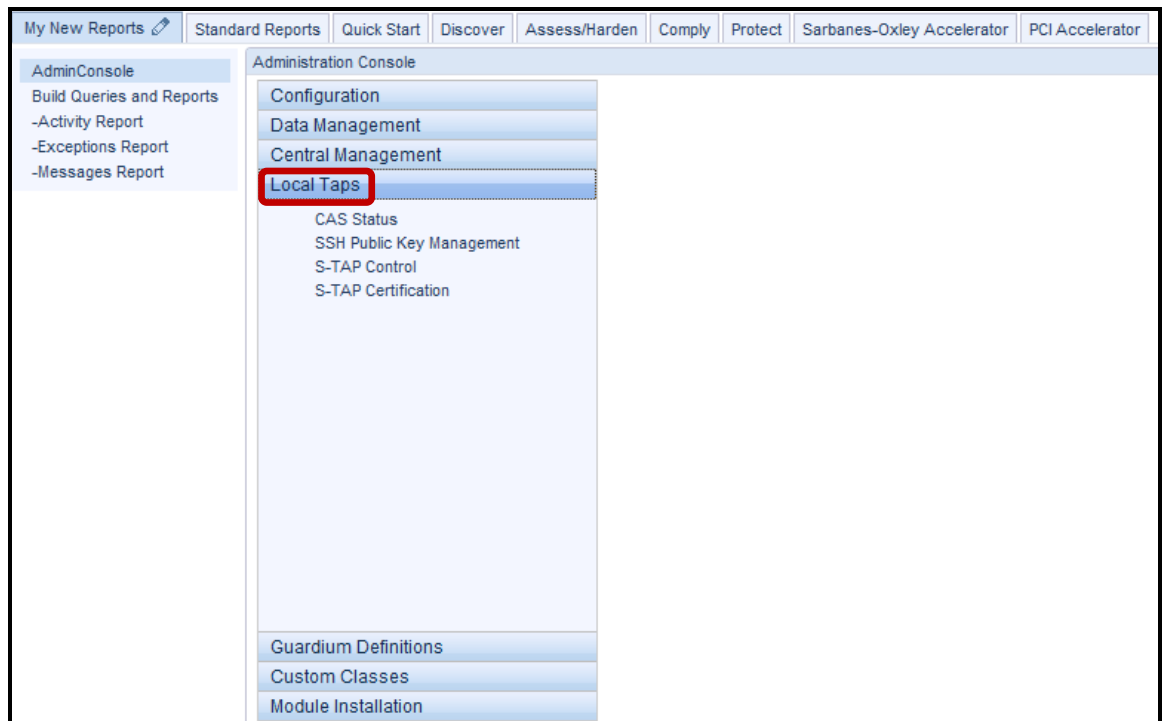
CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistry/key © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com, Zthread © Copyright 2000-2003, Eric Crahen.

Verify CAS and S-TAP configuration for DB2, MySQL, Oracle, PostgreSQL, and Sybase.

__c. Click **Admin Console** under the **My New Reports** tab.



__d. Click **Local Taps**.



- __e. Click **CAS Status** under **Local Taps**. It may take a few moments to display.

The screenshot shows the Administration Console interface. The left sidebar contains 'AdminConsole' and 'Build Queries and Reports' with sub-items: '-Activity Report', '-Exceptions Report', and '-Messages Report'. The main navigation pane is titled 'Administration Console' and includes sections for 'Configuration', 'Data Management', 'Central Management', 'Local Taps', 'Guardium Definitions', 'Custom Classes', and 'Module Installation'. Under 'Local Taps', 'CAS Status' is highlighted with a red box. The right pane displays 'Configuration Auditing System Status' with a help icon. The status text reads: 'CAS is active on this Guardium server.' Below this, there are three green status indicators, a server icon, the IP address '10.10.9.56 (10.10.9.56) (UNIX)', and a red 'X' icon. A 'Refresh' button is located at the bottom right of the status area.

- __f. Click **S-TAP Control** under **Local Taps**.

The screenshot shows the Administration Console interface with 'S-TAP Control' selected under 'Local Taps' in the left pane. The right pane displays 'S-TAP Control' with a help icon and a 'Refresh' button. Below the title is a table with columns: 'S-TAP Host', 'Status', and 'Last Response'. The table contains one row with the following data: '10.10.9.56', a green status indicator, and '2011-12-16 14:20:12.0'. Below the table are several expandable sections: 'Details', 'Change Auditing', 'Application Server User Identification', 'Guardium Hosts', and 'Inspection Engines'. At the bottom right, there are 'Refresh' and 'Comments...' buttons.

S-TAP Host	Status	Last Response
10.10.9.56		2011-12-16 14:20:12.0

The green status indicators above confirm that the IBM InfoSphere Guardium appliance is communicating with the S-TAP and CAS processes on the database server.

__g. Expand the '+' icon alongside "Inspection Engines" to see the Inspection Engine details.

The screenshot displays the Administration Console interface. On the left is a navigation menu with sections like 'AdminConsole', 'Build Queries and Reports', and 'Local Taps'. The main area shows the 'Inspection Engines' section, which is expanded to show details for five different database protocols. Each engine configuration is presented in a structured table format with red borders around the data blocks.

Protocol	Port Range	KTAP DB Real Port
DB2	50001-50001	50001
Ip	Mask	
0.0.0.0	0.0.0.0	
DB Install Dir	Process Name	
/home/db2inst2	/home/db2inst2/sqlib/adm/db2sysc	
DB2 Shared Memory Adjustment	DB2 Shared Memory Client Position	DB2 Shared Memory Size
20	61440	131072
Intercept Types		
NULL		

Protocol	Port Range	KTAP DB Real Port
Mysql	3306-3306	3306
Ip	Mask	
0.0.0.0	0.0.0.0	
DB Install Dir	Process Name	
NULL	mysql	
Intercept Types		
NULL		

Protocol	Port Range	KTAP DB Real Port
Oracle	1521-1521	1521
Ip	Mask	
0.0.0.0	0.0.0.0	
DB Install Dir	Process Name	
/usr/lib/oracle/xe	/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/bin/oracle	
Intercept Types		
NULL		

Protocol	Port Range	KTAP DB Real Port
PostgreSQL	5432-5432	5432
Ip	Mask	
0.0.0.0	0.0.0.0	
DB Install Dir	Process Name	
NULL	PostgreSQL	
Intercept Types		
NULL		

Protocol	Port Range	KTAP DB Real Port
Sybase	4200-4200	4200
Ip	Mask	
0.0.0.0	0.0.0.0	
DB Install Dir	Process Name	
NULL	NULL	
Intercept Types		
NULL		

The CAS status, S-TAP status, and associated Inspection Engines for DB2, MySQL, Oracle, PostgreSQL, and Sybase confirm a successful silent installation and Inspection Engine configuration.

- __5. Now, verify that the IBM InfoSphere Guardium Appliance is capturing SQL statements.
- __a. Return to the PuTTY ssh session and login as the Oracle DBA account (**su - oracle**). Then, login to Oracle by typing: **sqlplus system/guardium**.

```

root@osprey:~
stap/cas/lib/Text_JDBC30.jar:/usr/local/guardium/guard_stap/cas/lib/jt400.jar:/u
sr/local/guardium/guard_stap/cas/lib/nativeloader-200505172341.jar:/usr/local/gu
ardium/guard_stap/cas/lib/db2jcc_license_cu.jar:/usr/local/guardium/guard_stap/c
as/lib/bcprov-jdk14-144.jar:/usr/local/guardium/guard_stap/cas/lib/ddOracle.jar:
/usr/local/guardium/guard_stap/cas/lib/jcifs.jar:/usr/local/guardium/guard_stap/
cas/lib/tarbz2.jar:/usr/local/guardium/guard_stap/cas/lib/nzjdbc.jar:/usr/local
guardium/guard_stap/cas/lib/jconn2.jar:/usr/local/guardium/guard_stap/cas/lib/td
gssjava.jar:/usr/local/guardium/guard_stap/cas/lib/nativecall-0.4.1.jar:/usr/loc
al/guardium/guard_stap/cas/lib/mysql-connector-java-5.0.5-bin.jar: -Djava.librar
y.path=/usr/local/guardium/guard_stap/cas/lib -Xms128M -Xmx512M -Dpre.exe.env1=V
UE="" -DcasRestartTimer=1440 com.guardium.cas.client.CASClient
root      5867   3443   0 14:13 pts/0    00:00:00 grep cas
[root@osprey ~]# su - oracle
-bash-3.00$ sqlplus system/guardium

SQL*Plus: Release 10.2.0.1.0 - Production on Fri Dec 16 14:18:15 2011

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

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

SQL> select * from dba_users;

```

- __b. Type the SQL Query 'select * from dba_users;'

```

root@osprey:~
-----
EXTERNAL_NAME
-----
XDB                                27 E76A6BD999EF9FF1
EXPIRED & LOCKED                    31-JAN-06
SYSAUX                              TEMP                                31-JAN-06

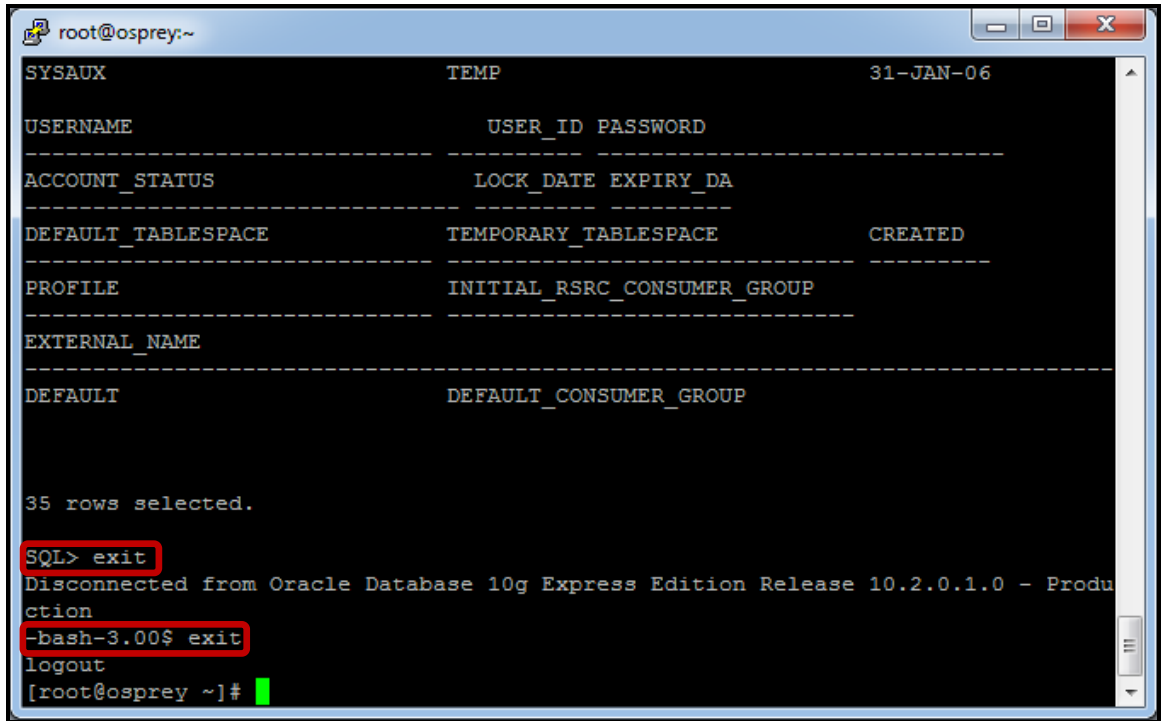
USERNAME                            USER_ID PASSWORD
-----
ACCOUNT_STATUS                      LOCK_DATE EXPIRY_DA
-----
DEFAULT_TABLESPACE                  TEMPORARY_TABLESPACE          CREATED
-----
PROFILE                             INITIAL_RSRC_CONSUMER_GROUP
-----
EXTERNAL_NAME
-----
DEFAULT                             DEFAULT_CONSUMER_GROUP

35 rows selected.

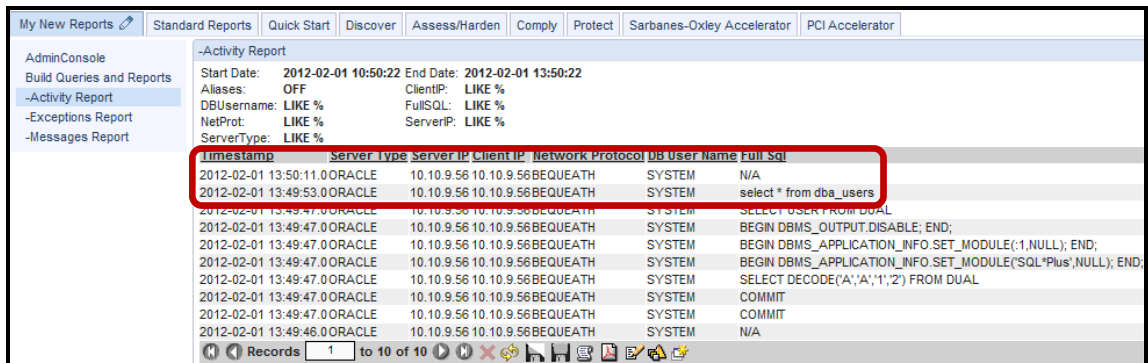
SQL>

```

- c. After receiving the result set, type **exit** to exit Oracle sqlplus, and then type **exit** to return to the root user account shell.



- d. From the IBM InfoSphere Guardium GUI, verify that Oracle SQL is being captured. Click **-Activity Report** under the **My New Reports** tab.



Note: The logged SQL statement from your query will appear in the **Full_Sql** column along with additional details captured at the time that the SQL statement was executed.

Thank You

4.2 Guardium Installation Manager Deployment

Overview

The purpose of the InfoSphere Guardium Installation Manager is to provide an automatic installation capability for Guardium software modules such as S-TAP and KTAP. Every database server can periodically check the Guardium appliance for new version updates. Upon finding a new release the installer agent running on the Guardium appliance (Guardium Installation Manager server) shall retrieve the new version software, either from its local database or by fetching it from a remote central manager machine, and sending it to the installer client (Guardium Installation Manager Client) on the database server.

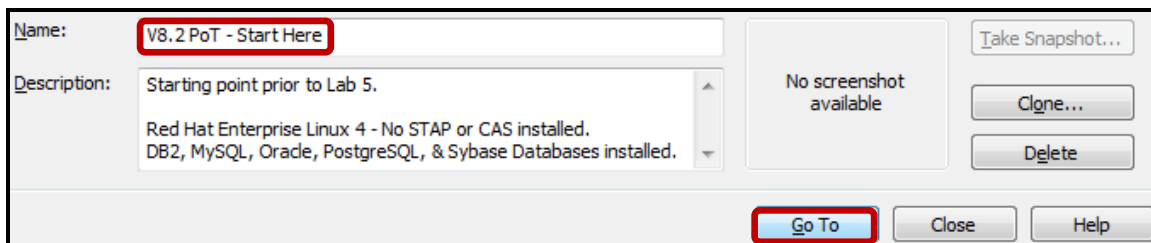
Objectives

This lab will demonstrate the ease with which the IBM InfoSphere Guardium solution can be deployed in an enterprise environment. We will focus on utilizing the IBM InfoSphere Guardium Installation Manager interface to perform automated installations and configurations of the Guardium S-TAP, CAS, and DISCOVERY software probes.

The following steps will guide us through the lab:

- __1. Install the IBM InfoSphere Guardium Installation Manager client software
- __2. Make use of the Guardium Installation Manager software modules for S-TAP, CAS and DISCOVERY that have been previously uploaded for this lab.
- __3. Deploy the lightweight S-TAP, CAS, and DISCOVERY software probes by means of the Guardium Installation Manager GUI
- __4. Configure an IBM InfoSphere Guardium Inspection Engine for the Oracle database platform
- __5. Use the Browser-based interface to validate a successful installation

- __1. **Critical Step** – Before beginning this section, ensure that the Database Server VM snapshot is reset back to the “V8.2 PoT – Start Here” snapshot, and then restarted. This is critical since a fresh system (no prior S-TAP install) is required before we can install the Guardium software probe again (which was already performed in the previous section of this lab). There is no need to reset the Appliance VM image because it will automatically detect the presence of the S-TAP.



- __a. Also, ensure that both the IBM InfoSphere Guardium appliance and database server VMs are up and running. You can easily confirm this by “pinging” the appliance and database server IP addresses.
- __b. Open a command prompt and type:
- __c. *ping 10.10.9.248* (Appliance VM IP address).

```
Pinging 10.10.9.248 with 32 bytes of data:
Reply from 10.10.9.248: bytes=32 time<1ms TTL=64
Reply from 10.10.9.248: bytes=32 time<1ms TTL=64
Reply from 10.10.9.248: bytes=32 time<1ms TTL=64
Reply from 10.10.9.248: bytes=32 time<1ms TTL=64

Ping statistics for 10.10.9.248:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

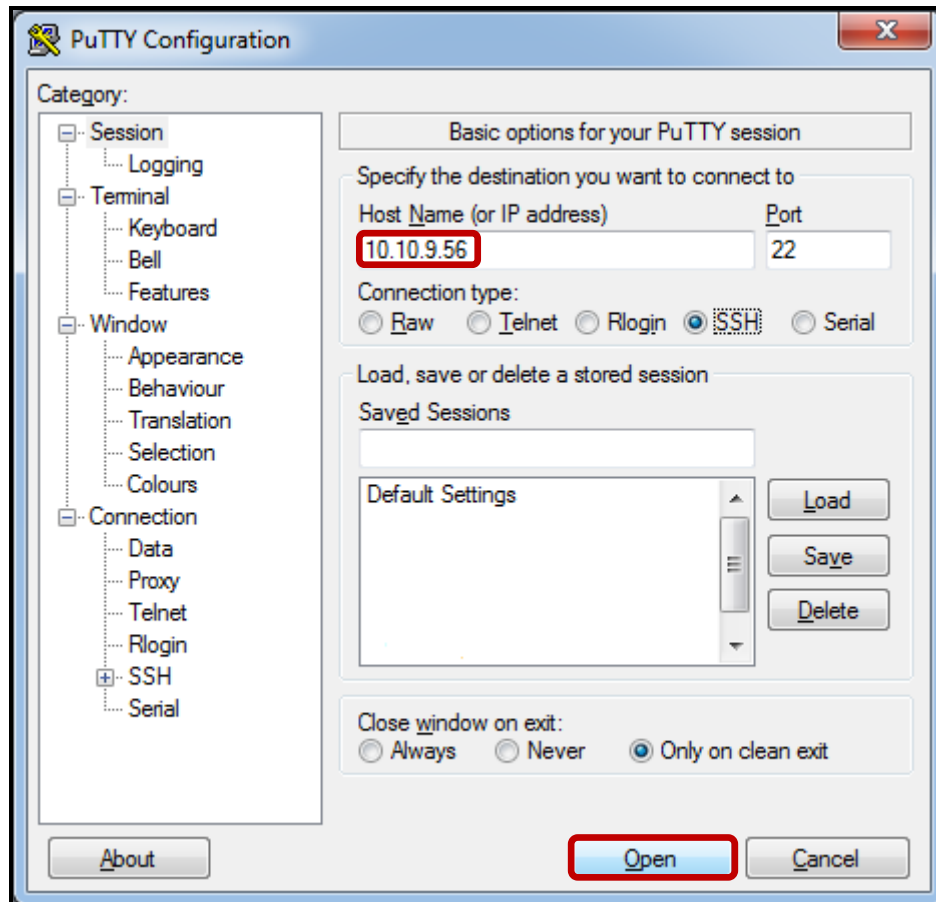
- __d. *ping 10.10.9.56* (Database Server VM IP address)

```
Pinging 10.10.9.56 with 32 bytes of data:
Reply from 10.10.9.56: bytes=32 time<1ms TTL=64
Reply from 10.10.9.56: bytes=32 time<1ms TTL=64
Reply from 10.10.9.56: bytes=32 time<1ms TTL=64
Reply from 10.10.9.56: bytes=32 time<1ms TTL=64

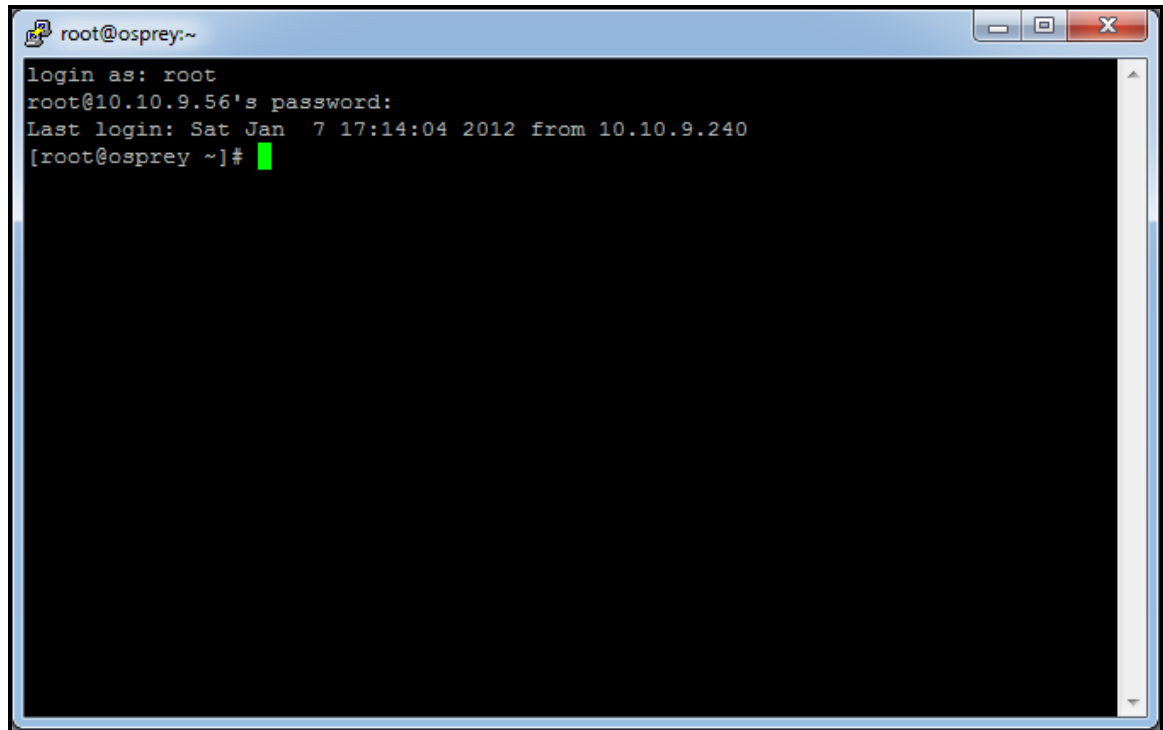
Ping statistics for 10.10.9.56:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If both of these steps are successful, please proceed to the next step. Otherwise, please refer to the Instructor Guide for further instructions or restart the associated VM.

- __2. Using a PuTTY SSH client, access the VM database server to demonstrate the ease with which the IBM InfoSphere Guardium solution can be automatically deployed using Guardium Installation Manager client software.
- __a. Start the PuTTY SSH client login.
 - __b. From your laptop, launch PuTTY, enter **10.10.9.56**, and click **Open**.

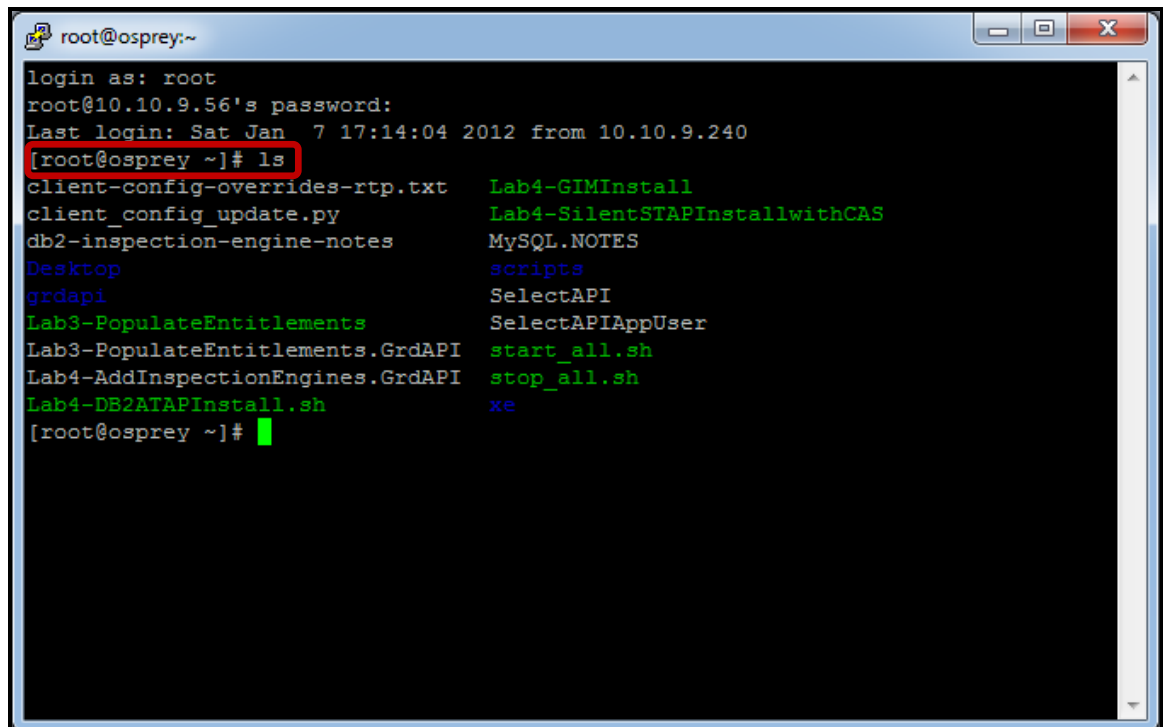


- __c. Login as **root** / **guardium**. After logging in, the following prompt will be displayed.



```
root@osprey:~  
login as: root  
root@10.10.9.56's password:  
Last login: Sat Jan 7 17:14:04 2012 from 10.10.9.240  
[root@osprey ~]#
```

- __d. Type **ls** to get a list of available files.

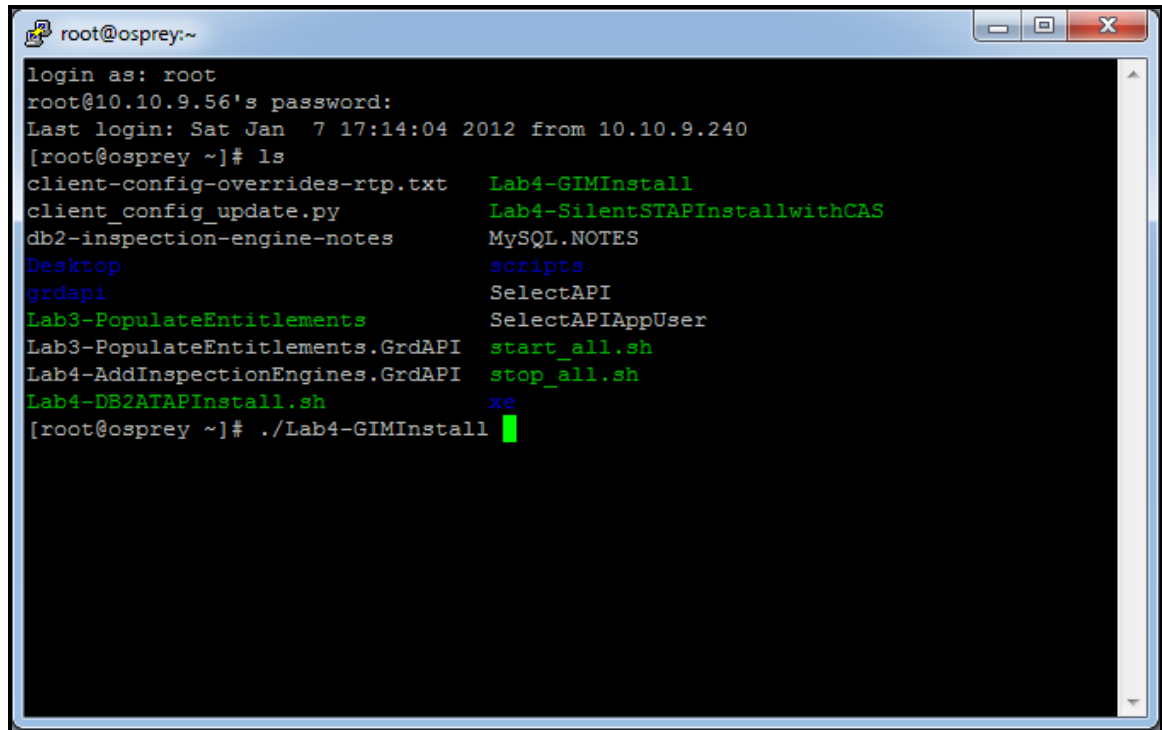


```
root@osprey:~  
login as: root  
root@10.10.9.56's password:  
Last login: Sat Jan 7 17:14:04 2012 from 10.10.9.240  
[root@osprey ~]# ls  
client-config-overrides-rtp.txt      Lab4-GIMInstall  
client_config_update.py              Lab4-SilentSTAPInstallwithCAS  
db2-inspection-engine-notes          MySQL.NOTES  
Desktop                               scripts  
grdapi                               SelectAPI  
Lab3-PopulateEntitlements             SelectAPIAppUser  
Lab3-PopulateEntitlements.GrdAPI      start_all.sh  
Lab4-AddInspectionEngines.GrdAPI     stop_all.sh  
Lab4-DB2ATAPInstall.sh               xe  
[root@osprey ~]#
```

Check that you see the files listed above in the /root directory.

- __e. Start the Guardium Installation Manager installation process by executing the following script:

`./Lab4-GIMInstall`



```

root@osprey:~
login as: root
root@10.10.9.56's password:
Last login: Sat Jan 7 17:14:04 2012 from 10.10.9.240
[root@osprey ~]# ls
client-config-overrides-rtp.txt  Lab4-GIMInstall
client_config_update.py          Lab4-SilentSTAPInstallwithCAS
db2-inspection-engine-notes      MySQL.NOTES
Desktop                           scripts
grdapi                             SelectAPI
Lab3-PopulateEntitlements         SelectAPIAppUser
Lab3-PopulateEntitlements.GrdAPI  start_all.sh
Lab4-AddInspectionEngines.GrdAPI stop_all.sh
Lab4-DB2ATAPInstall.sh          xe
[root@osprey ~]# ./Lab4-GIMInstall

```

The contents of the **Lab4-GIMInstall** script:

```

# GIM Installation
/tmp/guard-bundle-GIM-v82_r33264_1-rhel-4-linux-i686.gim.sh -- --dir
/usr/local/guardium --sqlguardip 10.10.9.248 --tapip 10.10.9.56

```

__f. Guardium Installation Manager Client Software Install Progress – Starting installation

```

root@osprey:~
login as: root
root@10.10.9.56's password:
Last login: Sat Jan  7 17:14:04 2012 from 10.10.9.240
[root@osprey ~]# ls
client-config-overrides-rtp.txt  Lab4-GIMInstall
client_config_update.py         Lab4-SilentSTAPIInstallwithCAS
db2-inspection-engine-notes     MySQL.NOTES
Desktop                          scripts
grdapi                           SelectAPI
Lab3-PopulateEntitlements        SelectAPIAppUser
Lab3-PopulateEntitlements.GrdAPI  start_all.sh
Lab4-AddInspectionEngines.GrdAPI  stop_all.sh
Lab4-DB2ATAPInstall.sh          xe
[root@osprey ~]# ./Lab4-GIMInstall
Verifying archive integrity... All good.
Uncompressing Guard BUNDLE-GIM Installer...

```

__g. Guardium Installation Manager Client Software Install Progress – International Program License Agreement

__h. Type 'q' to proceed with the installation.

```

root@osprey:~
perl used : /usr/bin/perl
International Program License Agreement

Part 1 - General Terms

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT" BUTTON,
OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT.
IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT AND WARRANT
T THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AG
REE TO THESE TERMS,

- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR USE TH
E PROGRAM; AND

- PROMPTLY RETURN THE UNUSED MEDIA, DOCUMENTATION, AND PROOF OF ENTITLEMENT TO T
HE PARTY FROM WHOM IT WAS OBTAINED FOR A REFUND OF THE AMOUNT PAID. IF THE PROGR
AM WAS DOWNLOADED, DESTROY ALL COPIES OF THE PROGRAM.

1. Definitions

"Authorized Use" - the specified level at which Licensee is authorized to execut
e or run the Program. That level may be measured by number of users, millions of
service units ("MSUs"), Processor Value Units ("PVUs"), or other level of use s
--More-- (1%)

```

- __i. Guardium Installation Manager Client Software Install Progress – Installation completed successfully

```

root@osprey:~
Part 1 - General Terms

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT" BUTTON,
OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT.
IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT AND WARRANT
T THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AG
REE TO THESE TERMS,

- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR USE TH
E PROGRAM; AND

- PROMPTLY RETURN THE UNUSED MEDIA, DOCUMENTATION, AND PROOF OF ENTITLEMENT TO T
HE PARTY FROM WHOM IT WAS OBTAINED FOR A REFUND OF THE AMOUNT PAID. IF THE PROGR
AM WAS DOWNLOADED, DESTROY ALL COPIES OF THE PROGRAM.

1. Definitions

"Authorized Use" - the specified level at which Licensee is authorized to execut
e or run the Program. That level may be measured by number of users, millions of
service units ("MSUs"), Processor Value Units ("PVUs"), or other level of use s
Installing modules ...
Installation completed successfully
[root@osprey ~]# █

```

- __j. Verify that Guardium Installation Manager client software is running
- __k. Type **ps -eaf | grep gim** to confirm that the Guardium Installation Manager client software process is running.

```

root@osprey:~
IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT AND WARRANT
T THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AG
REE TO THESE TERMS,

- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR USE TH
E PROGRAM; AND

- PROMPTLY RETURN THE UNUSED MEDIA, DOCUMENTATION, AND PROOF OF ENTITLEMENT TO T
HE PARTY FROM WHOM IT WAS OBTAINED FOR A REFUND OF THE AMOUNT PAID. IF THE PROGR
AM WAS DOWNLOADED, DESTROY ALL COPIES OF THE PROGRAM.

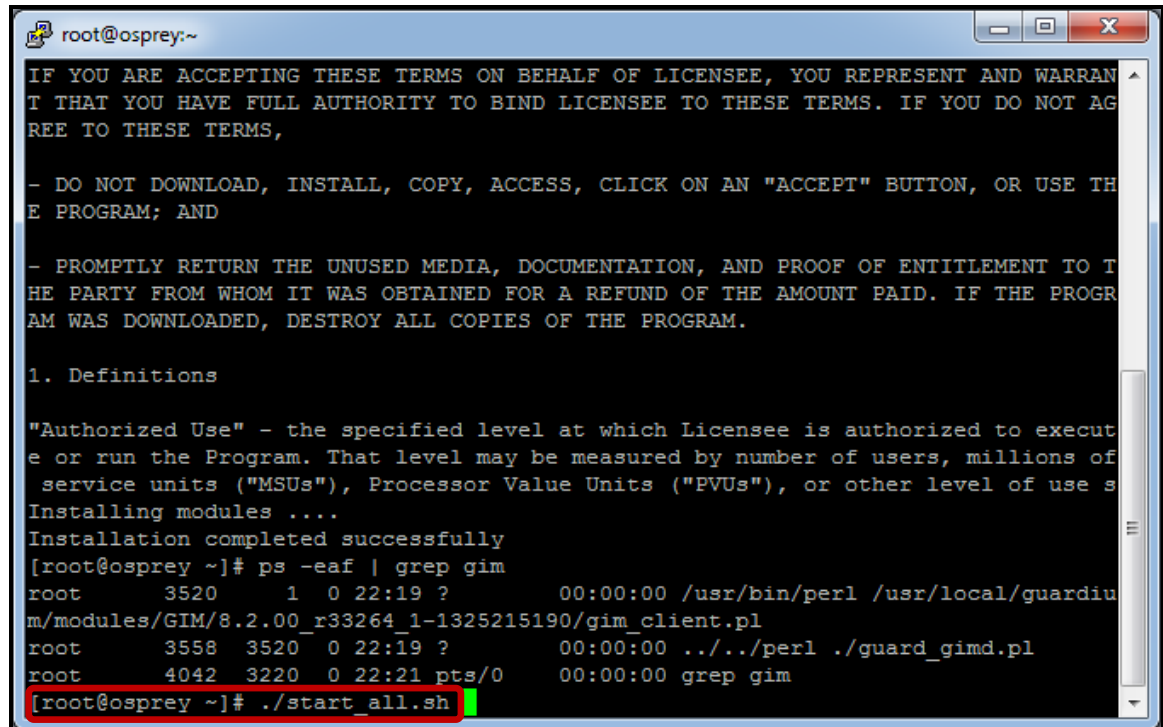
1. Definitions

"Authorized Use" - the specified level at which Licensee is authorized to execut
e or run the Program. That level may be measured by number of users, millions of
service units ("MSUs"), Processor Value Units ("PVUs"), or other level of use s
Installing modules ...
Installation completed successfully
[root@osprey ~]# ps -eaf | grep gim
root      3520      1  0  22:19 ?                00:00:00 /usr/bin/perl /usr/local/guardium
m/modules/GIM/8.2.00_r33264_1-1325215190/gim_client.pl
root      3558    3520  0  22:19 ?                00:00:00 ../../perl ./guard_gimd.pl
root      4042    3220  0  22:21 pts/0          00:00:00 grep  gim
[root@osprey ~]# █

```

- __I. **Critical Step** – Start all of the database servers. by executing the following script:

```
./start_all.sh
```



```

root@osprey:~
IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,

- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR USE THE PROGRAM; AND

- PROMPTLY RETURN THE UNUSED MEDIA, DOCUMENTATION, AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM IT WAS OBTAINED FOR A REFUND OF THE AMOUNT PAID. IF THE PROGRAM WAS DOWNLOADED, DESTROY ALL COPIES OF THE PROGRAM.

1. Definitions

"Authorized Use" - the specified level at which Licensee is authorized to execute or run the Program. That level may be measured by number of users, millions of service units ("MSUs"), Processor Value Units ("PVUs"), or other level of use s
Installing modules ...
Installation completed successfully
[root@osprey ~]# ps -eaf | grep gim
root      3520      1  0 22:19 ?                00:00:00 /usr/bin/perl /usr/local/guardium/modules/GIM/8.2.00_r33264_1-1325215190/gim_client.pl
root      3558    3520  0 22:19 ?                00:00:00 ../../perl ./guard_gimd.pl
root      4042    3220  0 22:21 pts/0          00:00:00 grep  gim
[root@osprey ~]# ./start_all.sh

```

We will need these running for later sections of this lab after the Guardium Installation Manager Discovery software has been installed so that all instances will be properly discovered.

The contents of the **start_all.sh** script:

```

#!/bin/bash
echo "=starting MySQL..."
/etc/init.d/mysql start
echo "=starting DB2..."
su - db2inst2 -c "db2start"
echo "=starting Sybase15..."
su - sybase15 -c "source /home/sybase15/.bash_profile;
/home/sybase15/start_it.sh"
echo "=starting Oracle10g..."
su - oracle -c "./start.sh"

```

- __3. Now, launch the InfoSphere Guardium GUI to verify the GIM client software installation, and to begin the process of deploying software through the GIM GUI.
- __a. Login as user **pot** / **guardium**.

Login

Please enter your information

User name:

Password:

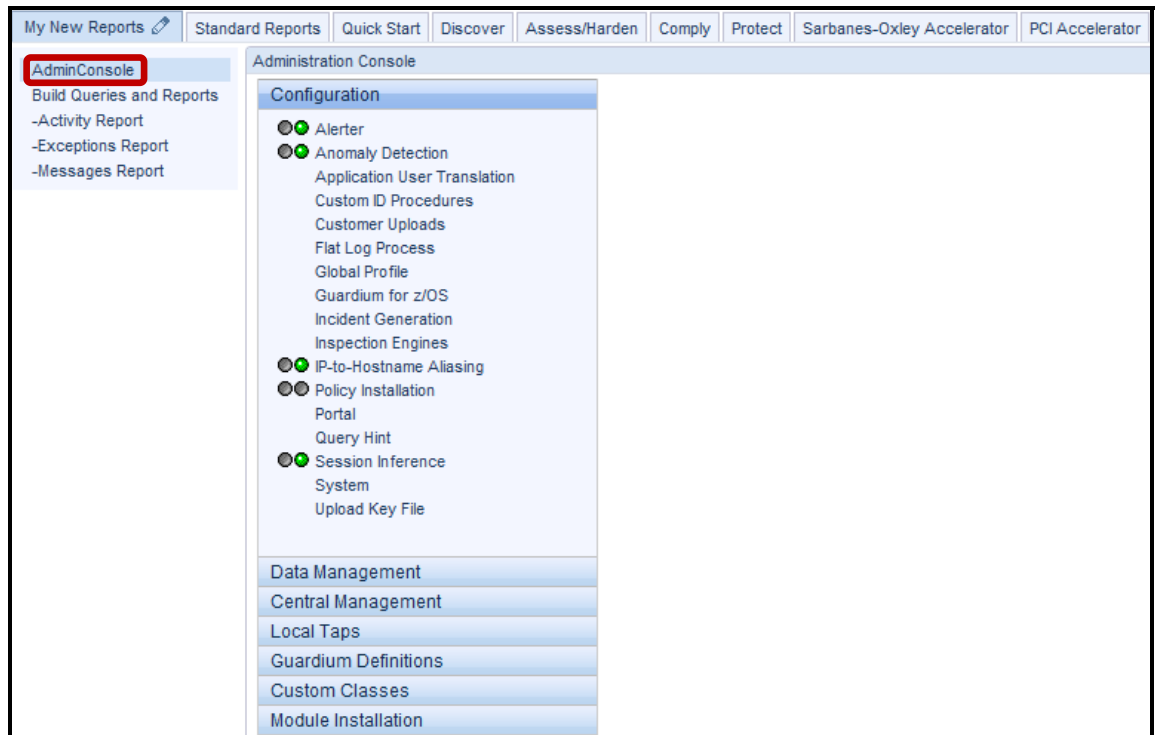
Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

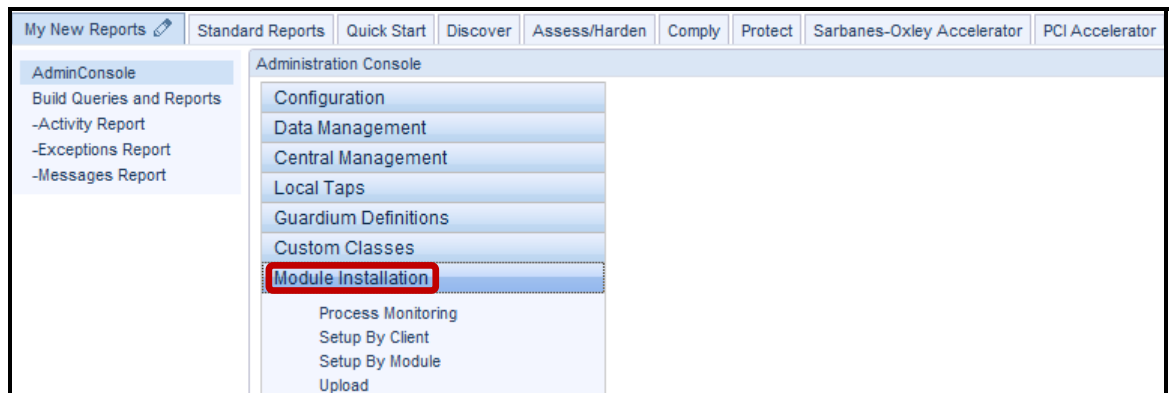
CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistry/key © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

Verify GIM process communication.

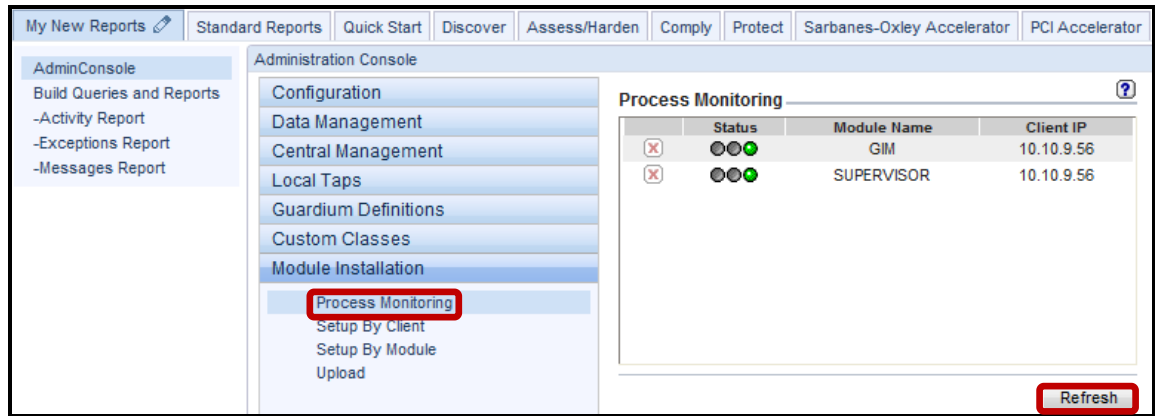
__b. Click **Admin Console** under the **My New Reports** tab.



__c. Click **Module Installation**.

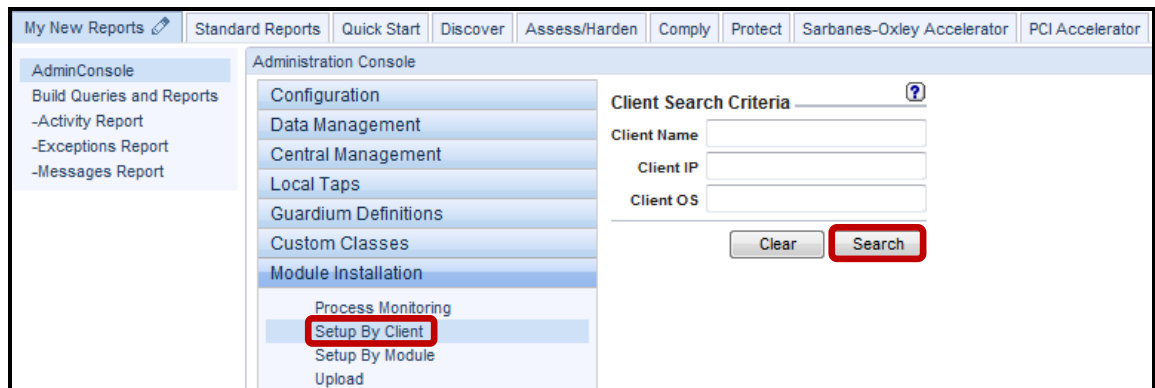


- __d. Click **Process Monitoring** under the **Module Installation** tab. Click **Refresh** until your screen appears as below. This may take a couple of minutes.

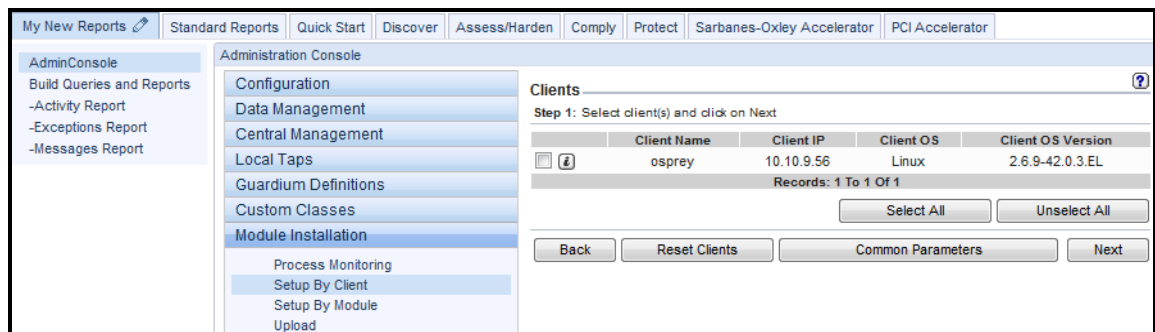


The green status lights should appear for 'GIM' and 'SUPERVISOR' modules which are now running on the database server. A corresponding pair of 'GIM' and 'SUPERVISOR' processes will appear for each client IP being managed by GIM.

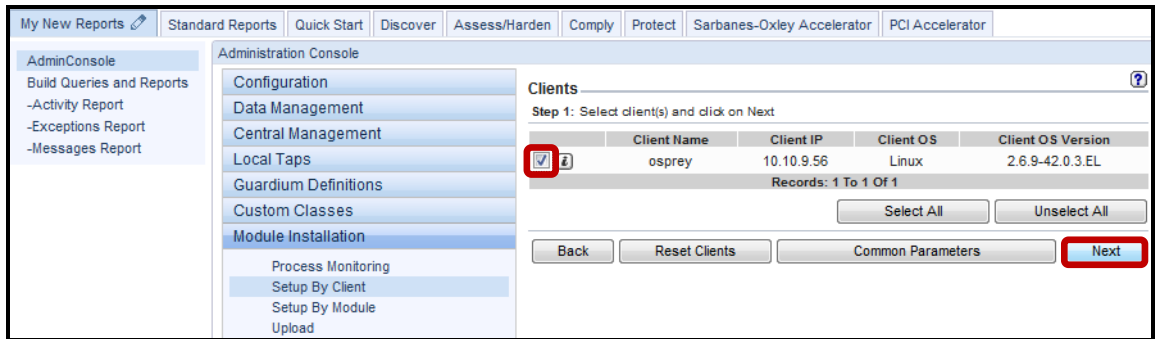
- __e. Click **Setup By Client** under the **Module Installation** tab, and click **Search**.



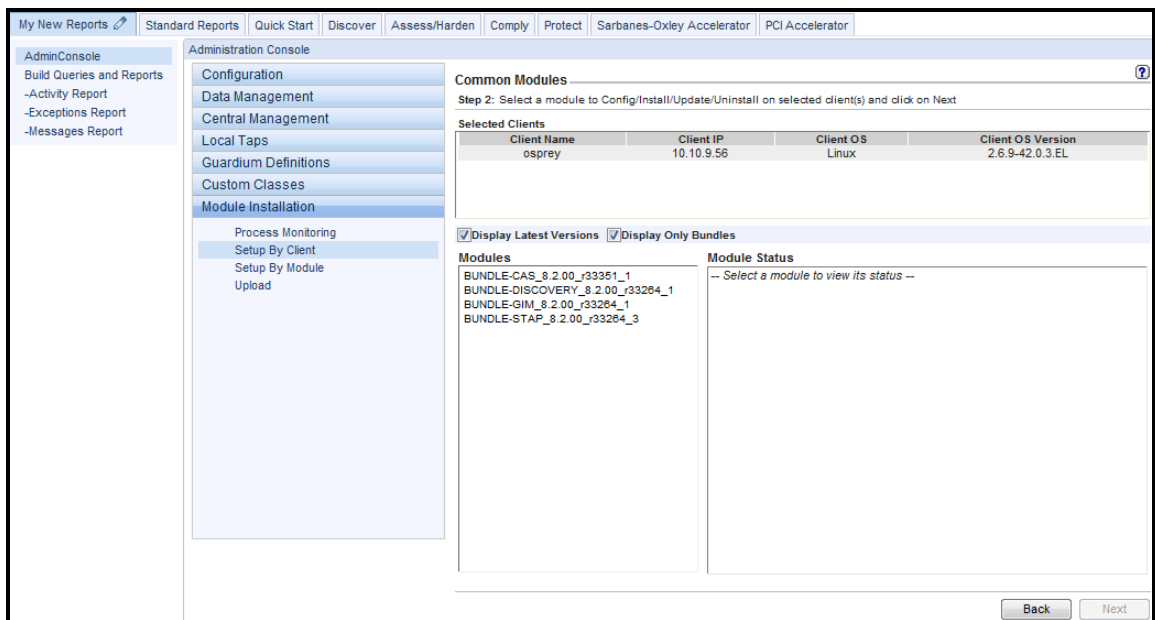
A list of available GIM clients will display.



__f. Check the left hand checkbox, and click **Next**.

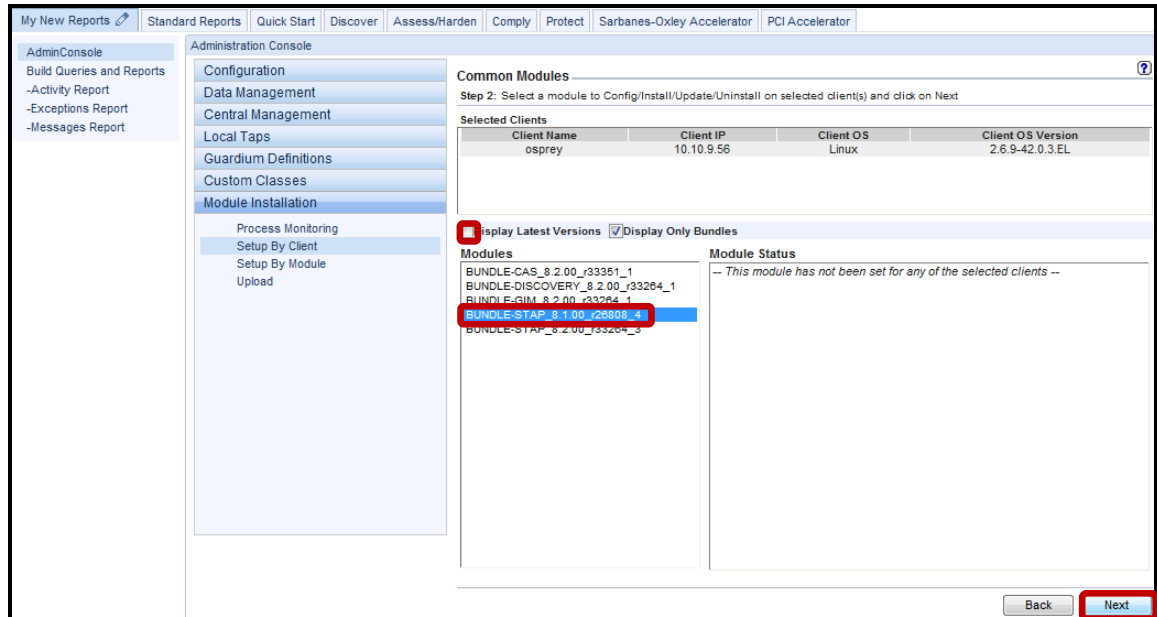


A list of uploaded modules currently available for the targeted platform(s) will appear.

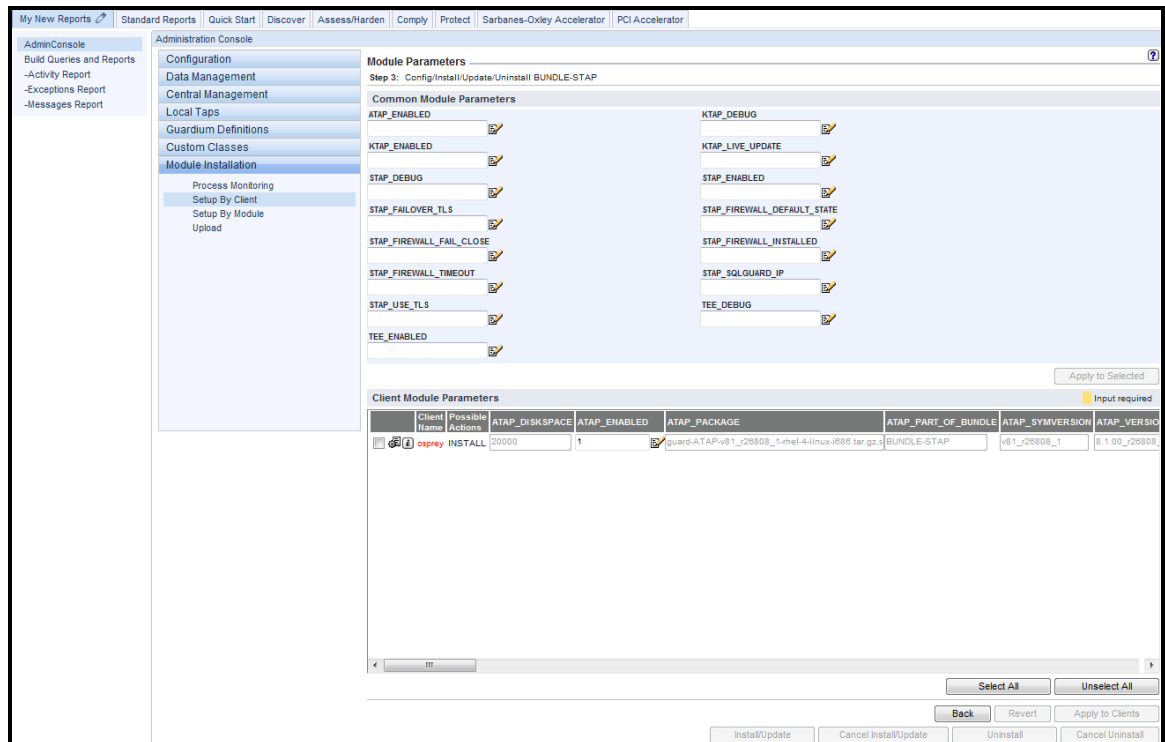


4. S-TAP Installation using GIM.

- a. **Critical Step.** This step must be performed properly to ensure that the S-TAP Upgrade will work in a later section of this lab. Before proceeding, uncheck the **Display Latest Version** checkbox, select **BUNDLE-STAP_8.1.00_r26808_4**, and click **Next**.

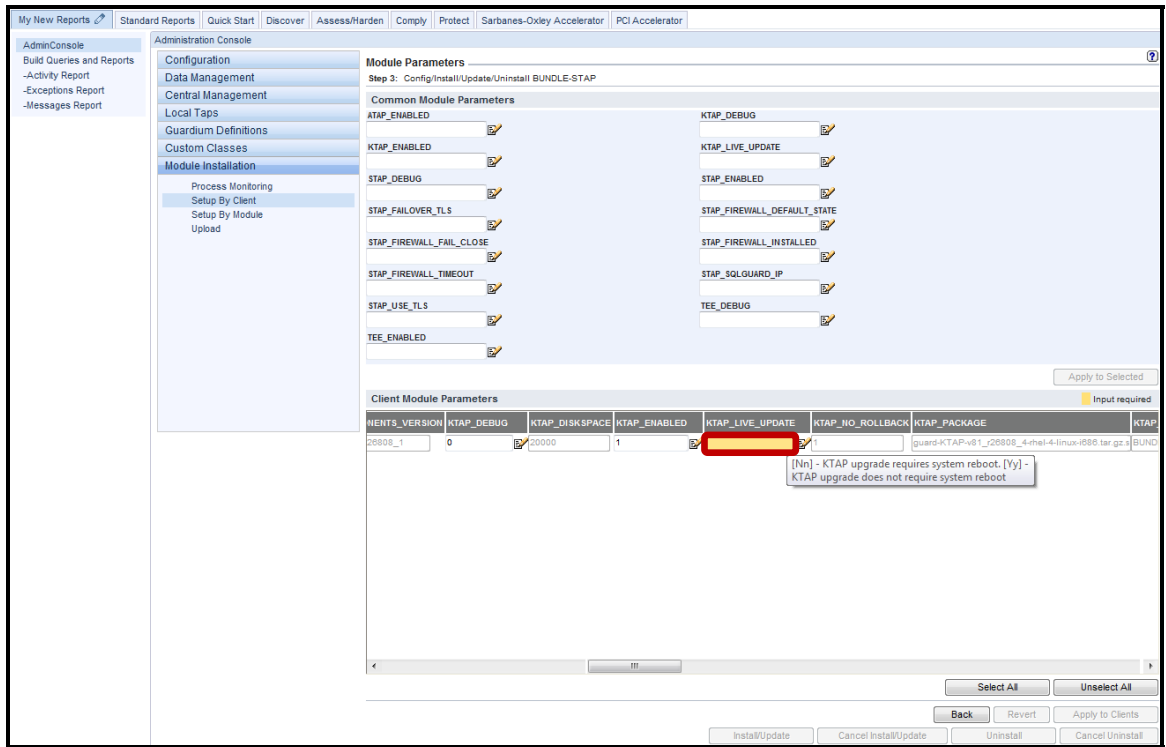


A Module Parameters screen will appear enabling the configuration of a variety of properties before installing new software or updating existing software installations.

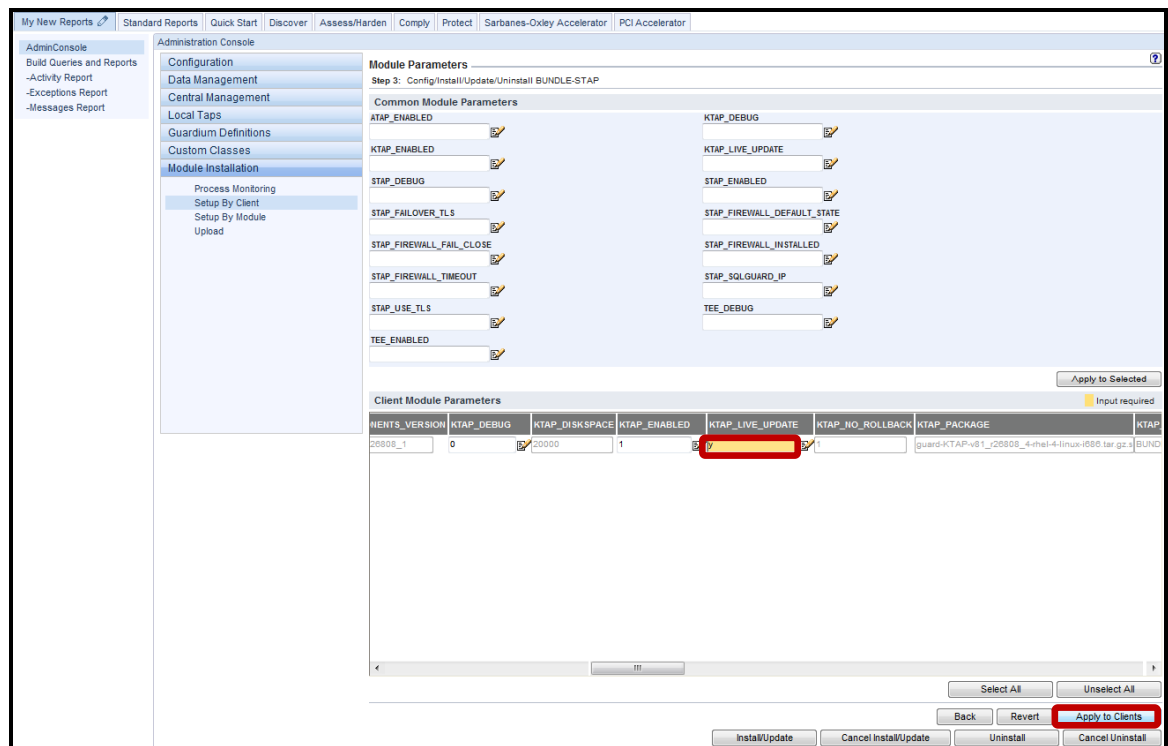


- __b. Scroll to the right until the golden **KTAP_LIVE_UPDATE** box appears which indicates that a property value must be provided before the installation can proceed.

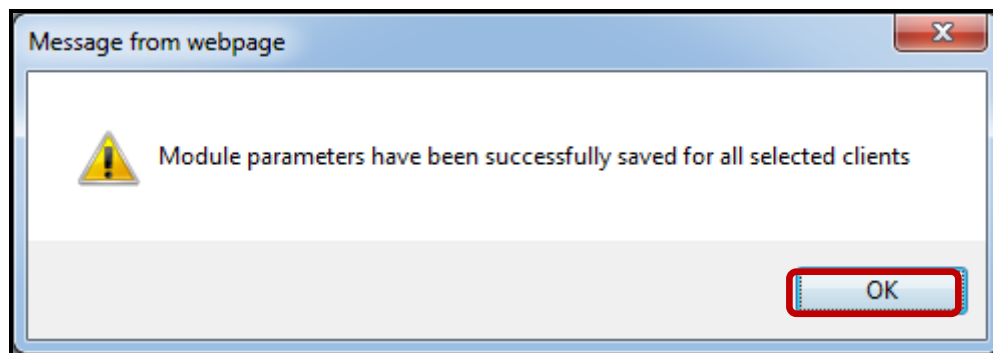
Hover over any of the property boxes to see details on valid values. A property content dialog can also be accessed by clicking on the pencil and paper icon alongside some the property boxes.



- ___c. Enter 'y', and click **Apply to Clients** to specify that a KTAP upgrade does not require a system reboot.



- ___d. Click **OK** to acknowledge.

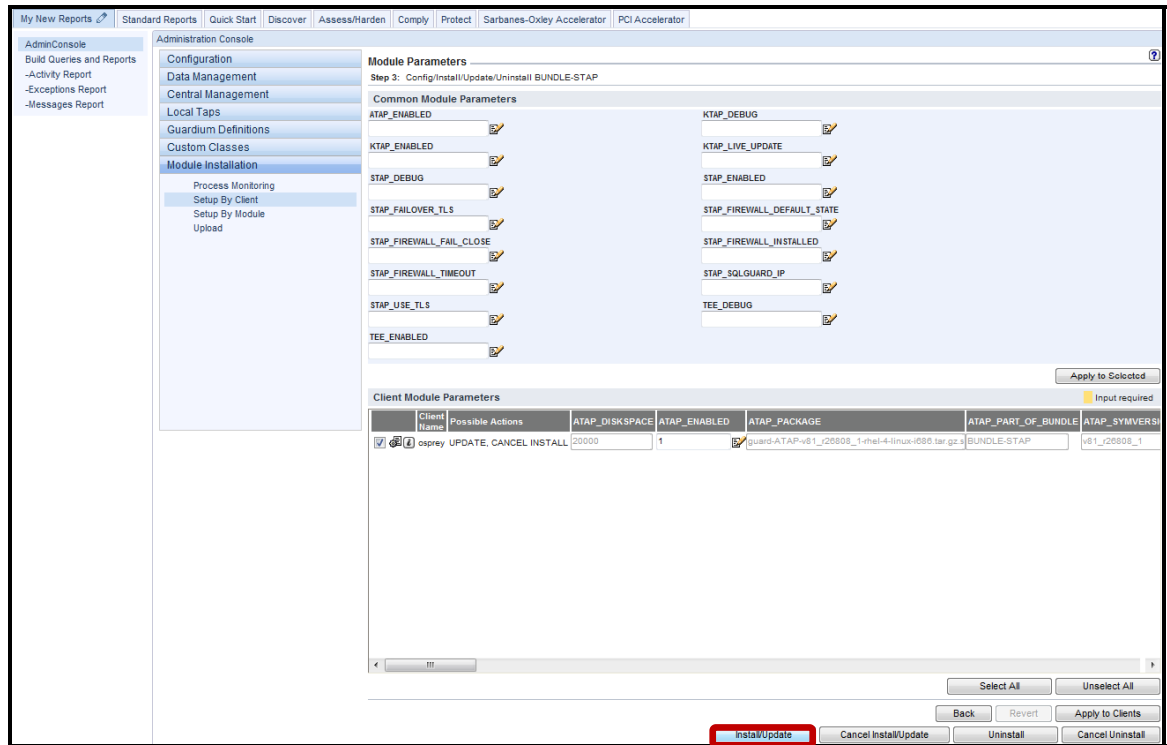


Note: While not required, this is the same location to set additional properties such as:

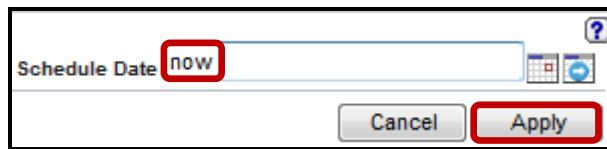
STAP_FIREWALL_INSTALLED=1 – S-GATE Blocking Enabled (0 by Default)

In a later lab section, this value will be required to be set.

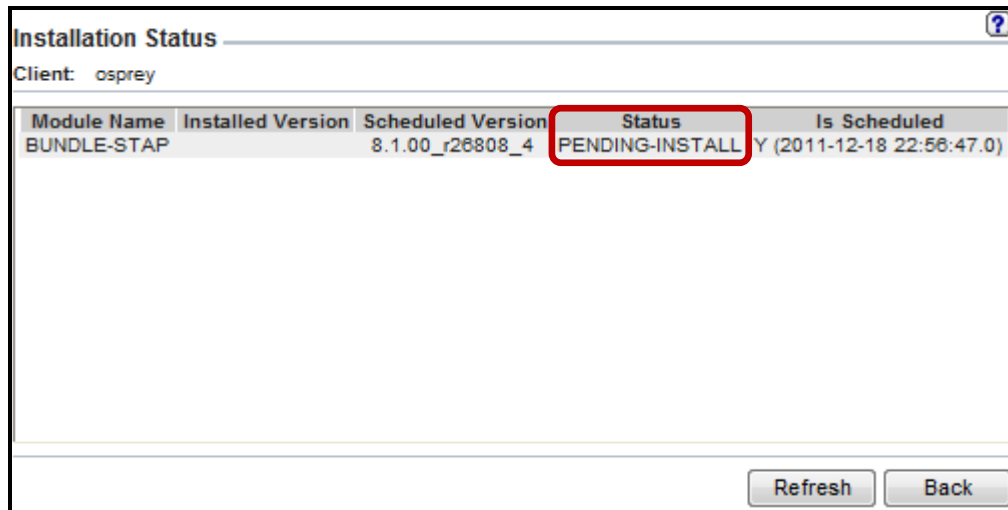
__e. Click **Install/Update**.



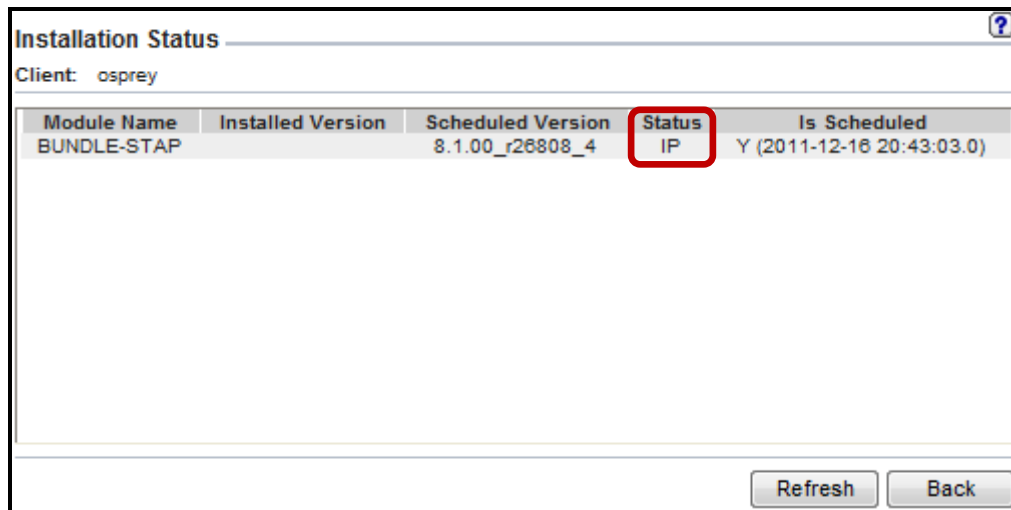
__f. Enter '**now**' for the Schedule Date, and click **Apply**.



__g. Click on the  icon to check the status of the installation.



“IP” indicates that the installation is “In Progress”.

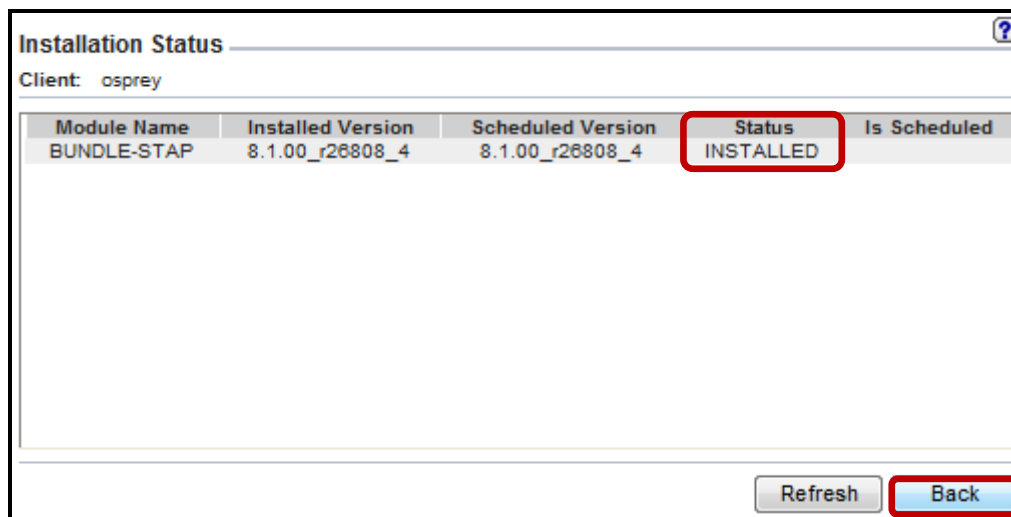


Installation Status ?

Client: osprey

Module Name	Installed Version	Scheduled Version	Status	Is Scheduled
BUNDLE-STAP		8.1.00_r26808_4	IP	Y (2011-12-16 20:43:03.0)

- __h. Once the installation has completed successfully, click **Back** to return to the **Module Parameters** screen.



Installation Status ?

Client: osprey

Module Name	Installed Version	Scheduled Version	Status	Is Scheduled
BUNDLE-STAP	8.1.00_r26808_4	8.1.00_r26808_4	INSTALLED	

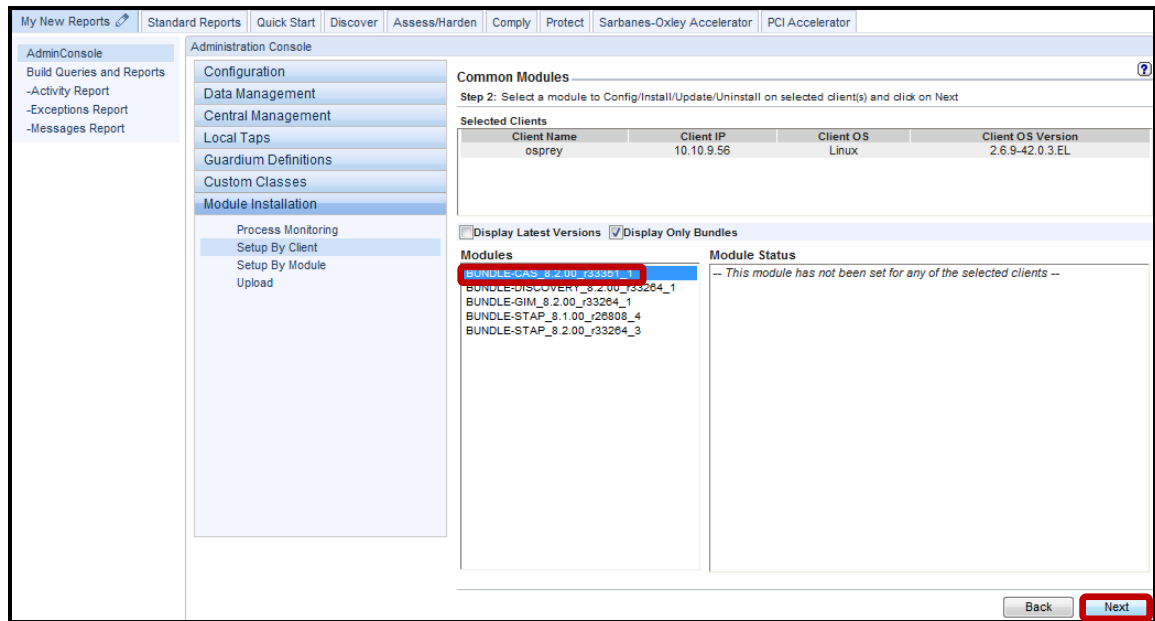
__i. Click **Back** once more to return to the **Common Modules** screen.

The screenshot shows the Administration Console interface for Guardium. The left sidebar contains navigation options like 'AdminConsole', 'Build Queries and Reports', and 'Configuration'. The main area is titled 'Module Parameters' and shows configuration options for 'BUNDLE-STAP'. Below the configuration options is a table for 'Client Module Parameters' with one row of data. At the bottom right, a 'Back' button is highlighted with a red box, along with other buttons like 'Revert', 'Apply to Clients', 'Install/Update', 'Cancel Install/Update', 'Uninstall', and 'Cancel Uninstall'.

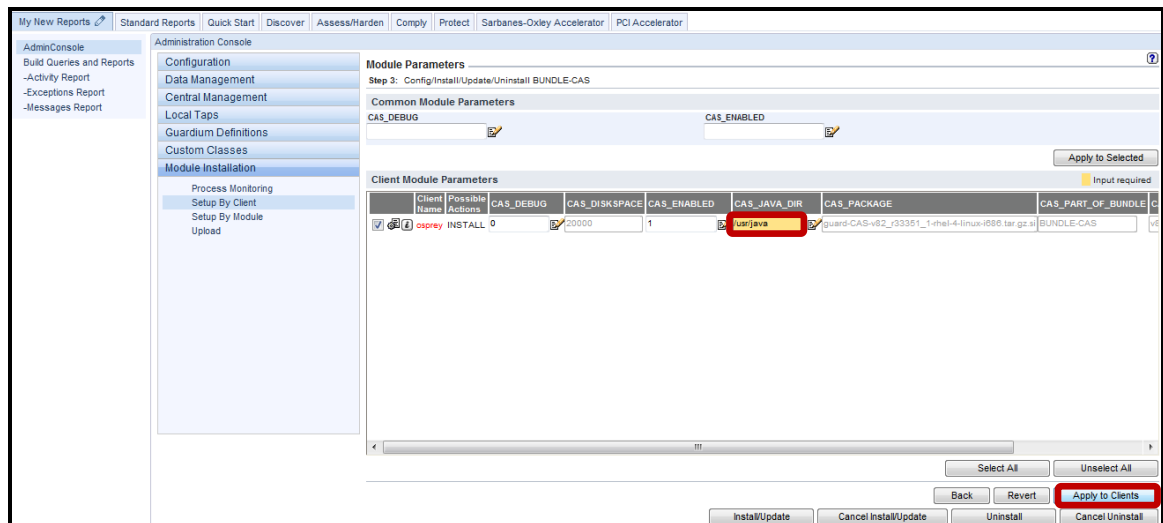
Client Name	Possible Actions	ATAP_DISKSPACE	ATAP_ENABLED	ATAP_PACKAGE	ATAP_PART_OF_BUNDLE	ATAP_SYMVERSION	ATAP_VERSION
osprey	UPDATE, UNINSTALL	20000	1	guard-ATAP-v81_28808_1-shel-4-linux-i686.tar.gz	BUNDLE-STAP	v81_28808_1	8.1

__5. CAS installation using GIM.

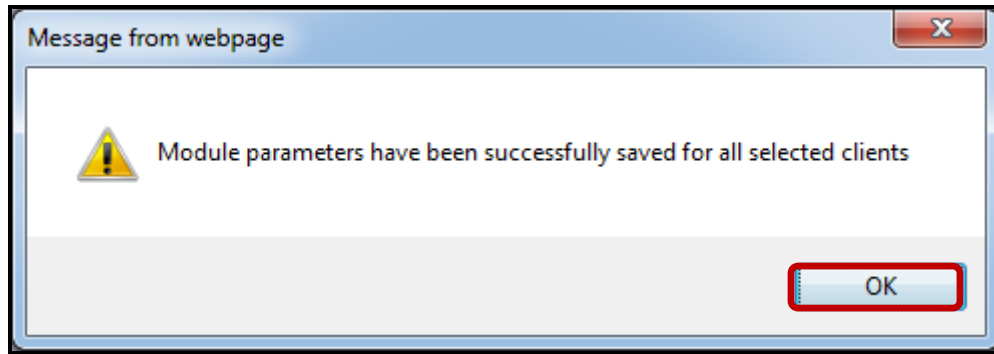
__a. Next, select **BUNDLE-CAS_8.2.00_r33351_1**, and click **Next**.



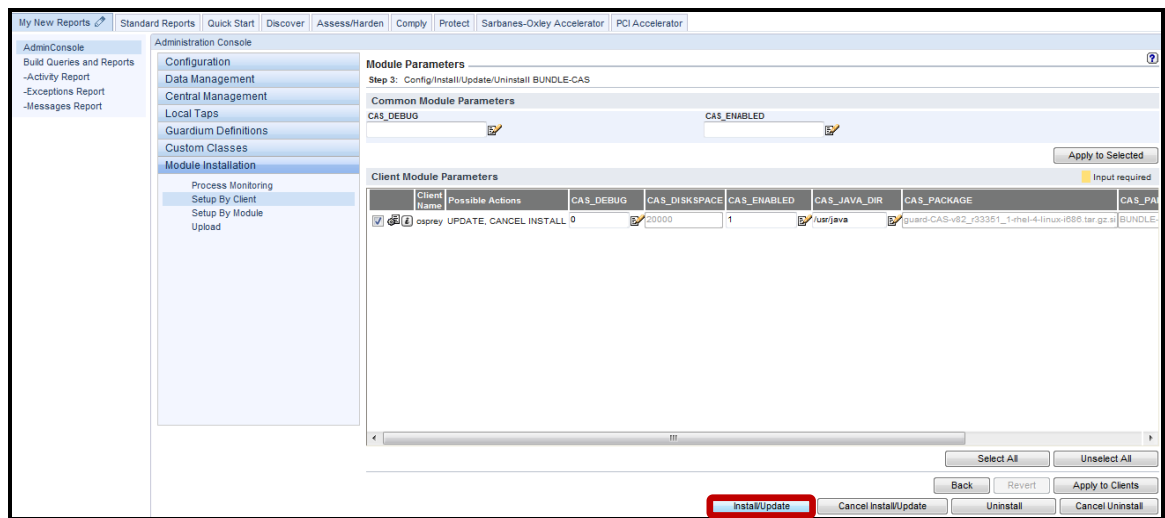
__b. Enter **'/usr/java'** in the golden **CAS_JAVA_DIR** box which indicates that a property value must be provided before the installation can proceed. Then, click **Apply to Clients** to specify the correct JAVA HOME directory.



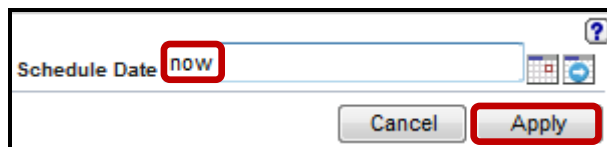
__c. Click **OK** to acknowledge.



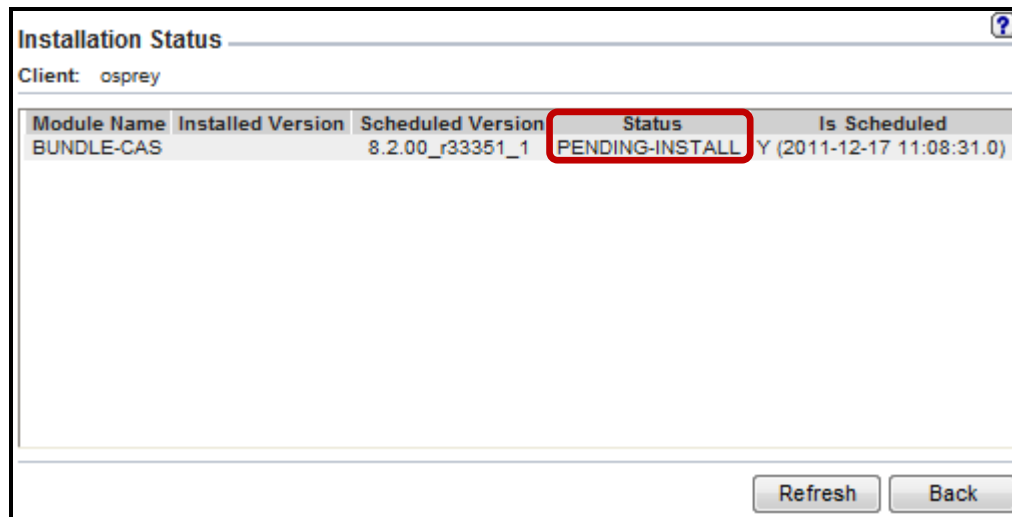
__d. Click **Install/Update**.



__e. Enter '**now**' for the Schedule Date, and click **Apply**.



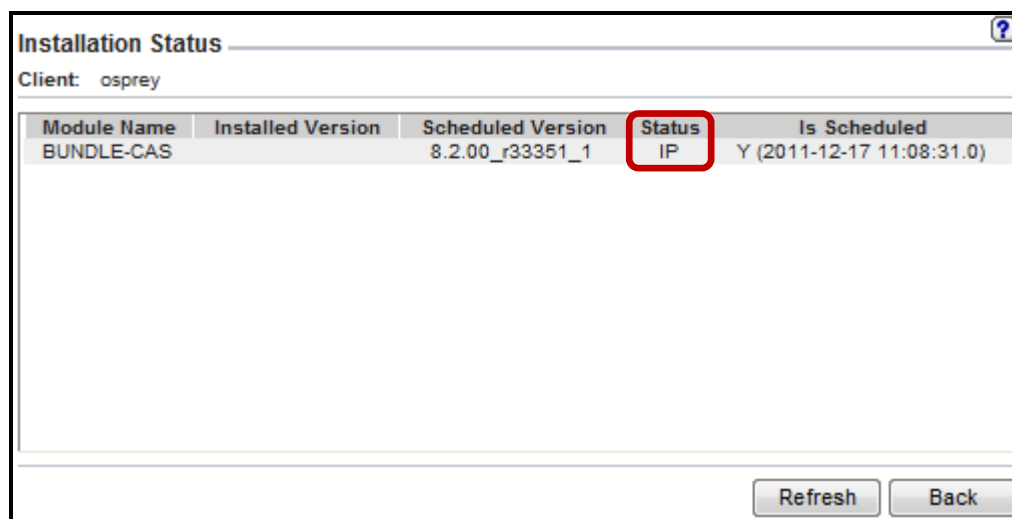
__f. Click on the ⓘ icon to check the status of the installation.



The screenshot shows a window titled "Installation Status" with a help icon in the top right corner. Below the title bar, it says "Client: osprey". A table with the following columns is displayed: "Module Name", "Installed Version", "Scheduled Version", "Status", and "Is Scheduled". The table contains one row for "BUNDLE-CAS" with "Installed Version" blank, "Scheduled Version" "8.2.00_r33351_1", "Status" "PENDING-INSTALL", and "Is Scheduled" "Y (2011-12-17 11:08:31.0)". The "Status" cell is highlighted with a red box. At the bottom right, there are "Refresh" and "Back" buttons.

Module Name	Installed Version	Scheduled Version	Status	Is Scheduled
BUNDLE-CAS		8.2.00_r33351_1	PENDING-INSTALL	Y (2011-12-17 11:08:31.0)

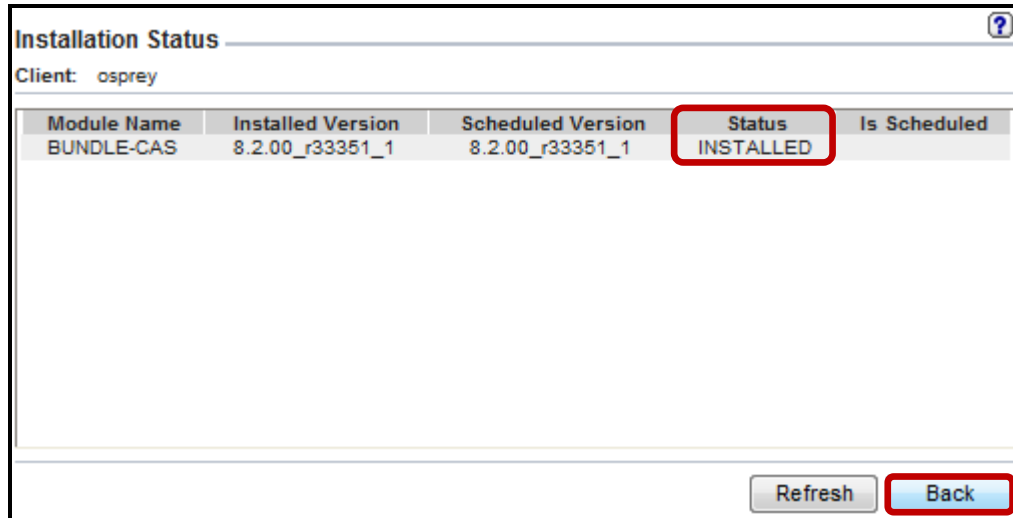
“IP” indicates that the installation is “In Progress”.



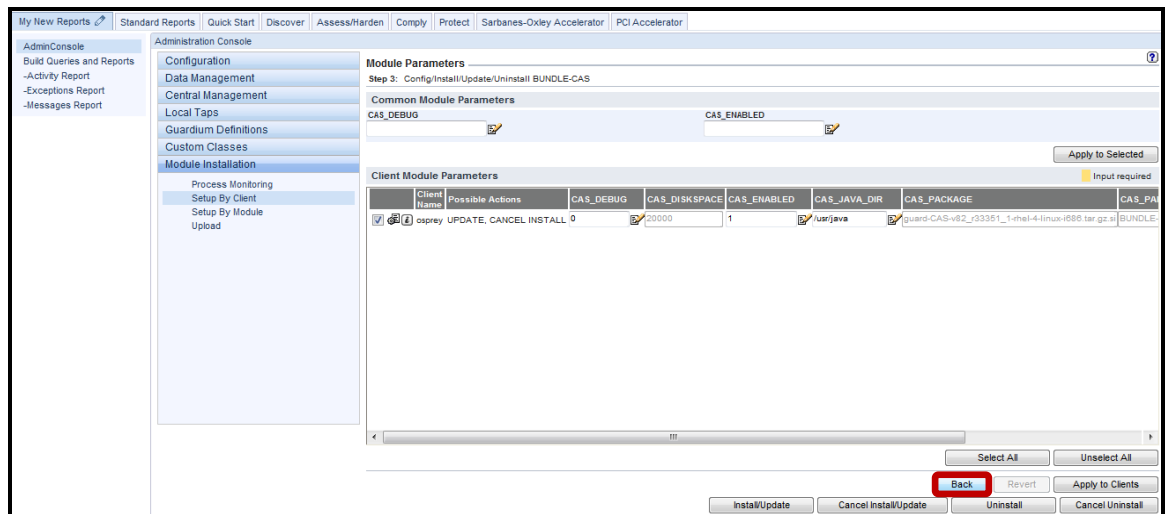
The screenshot shows the same "Installation Status" window. The table now shows the "Status" for "BUNDLE-CAS" as "IP", which is highlighted with a red box. All other data in the table remains the same. The "Refresh" and "Back" buttons are still present at the bottom right.

Module Name	Installed Version	Scheduled Version	Status	Is Scheduled
BUNDLE-CAS		8.2.00_r33351_1	IP	Y (2011-12-17 11:08:31.0)

- __g. Once the installation has completed successfully, click **Back** to return to the **Module Parameters** screen.

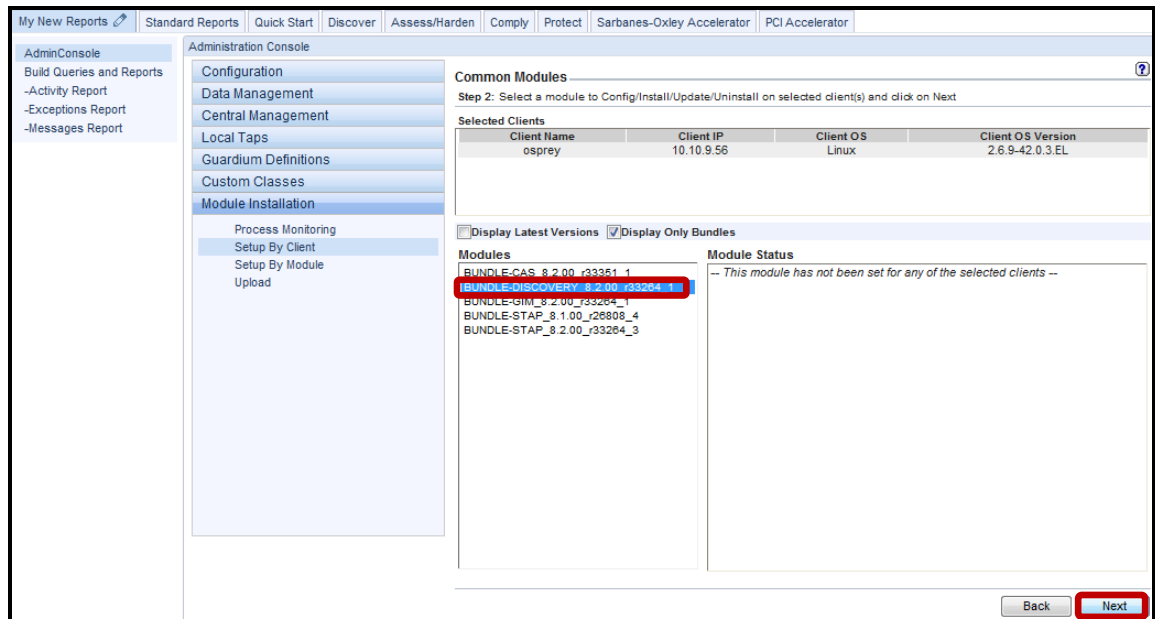


- __h. Click **Back** once more to return to the **Common Modules** screen.

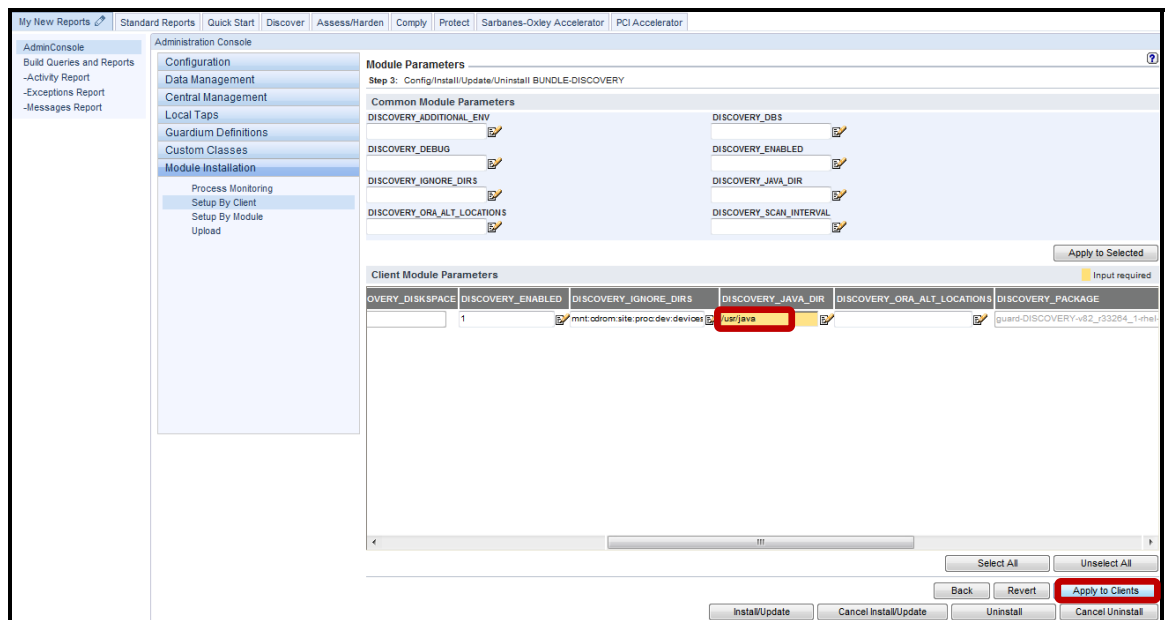


__6. DISCOVERY installation using GIM.

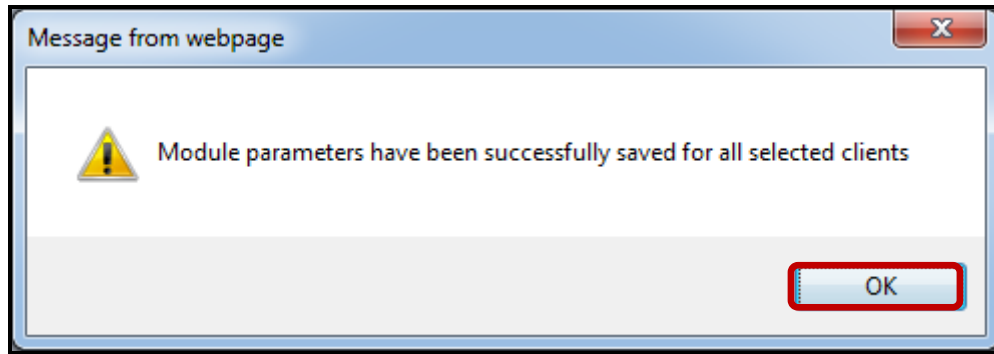
__a. Next, select **BUNDLE-DISCOVERY_8.2.00_r33264_1**, and click **Next**.



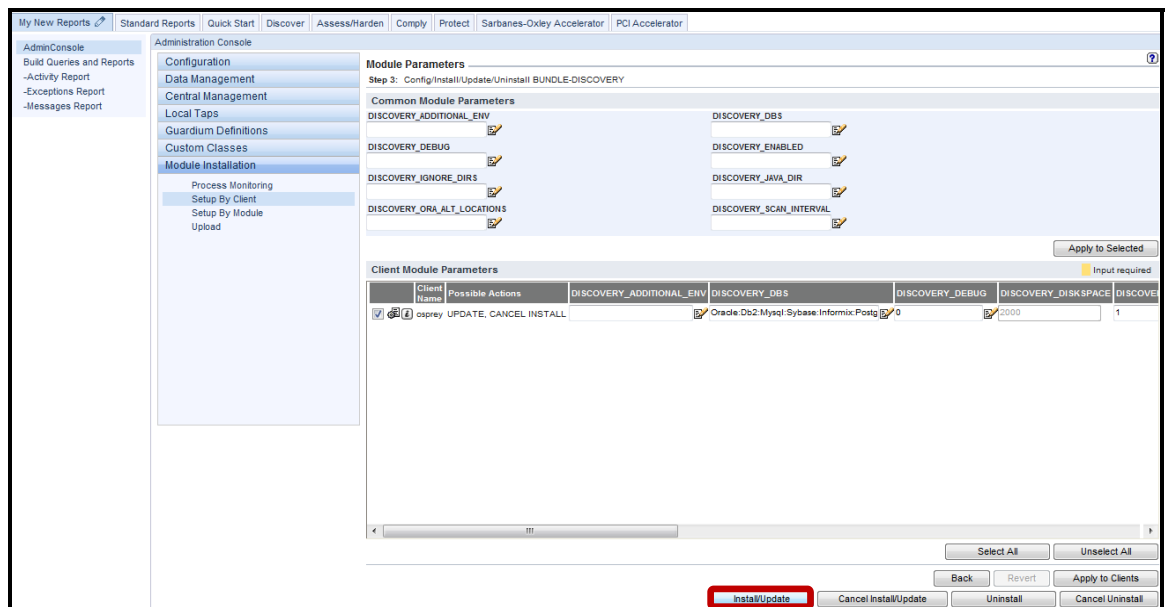
__b. Scroll to the right, and enter **'/usr/java'** in the golden **DISCOVERY_JAVA_DIR** box which indicates that a property value must be provided before the installation can proceed. Then, click **Apply to Clients** to specify the correct JAVA HOME directory.



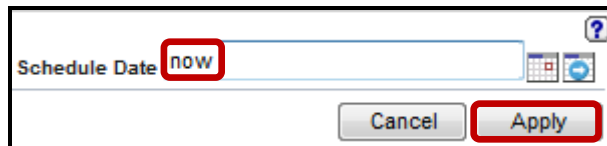
__c. Click **OK** to acknowledge.



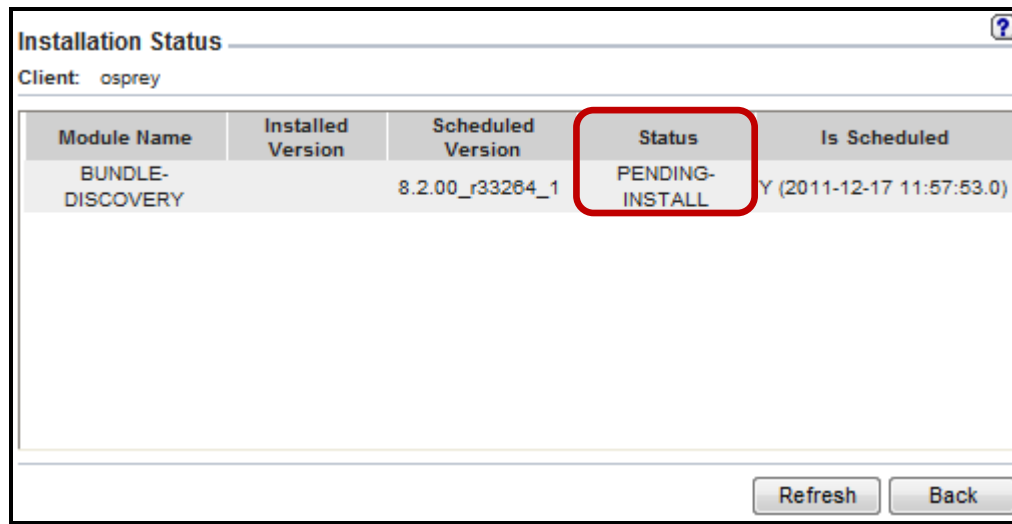
__d. Click **Install/Update**.



__e. Enter '**now**' for the Schedule Date, and click **Apply**.



__f. Click on the ⓘ icon to check the status of the installation.



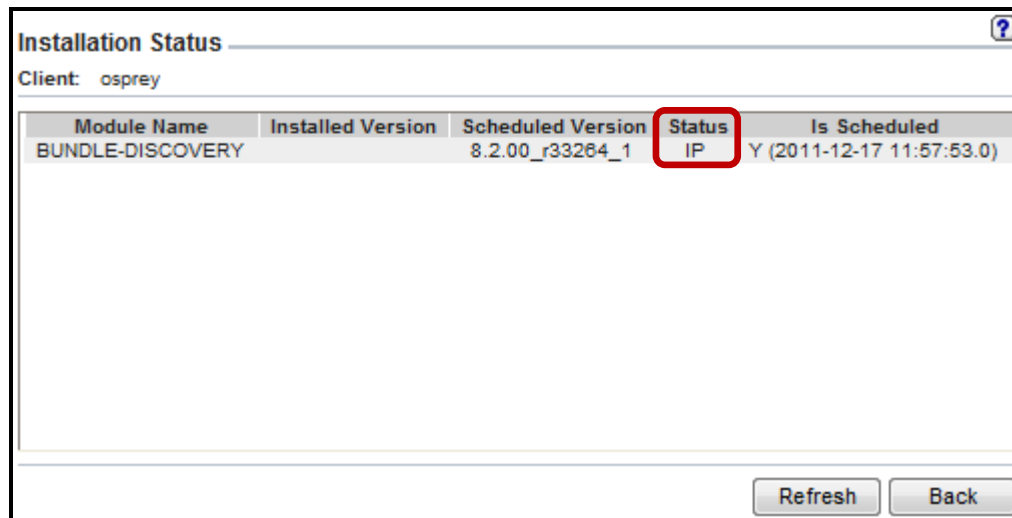
Installation Status ⓘ

Client: osprey

Module Name	Installed Version	Scheduled Version	Status	Is Scheduled
BUNDLE-DISCOVERY		8.2.00_r33264_1	PENDING-INSTALL	Y (2011-12-17 11:57:53.0)

Refresh Back

“IP” indicates that the installation is “In Progress”.



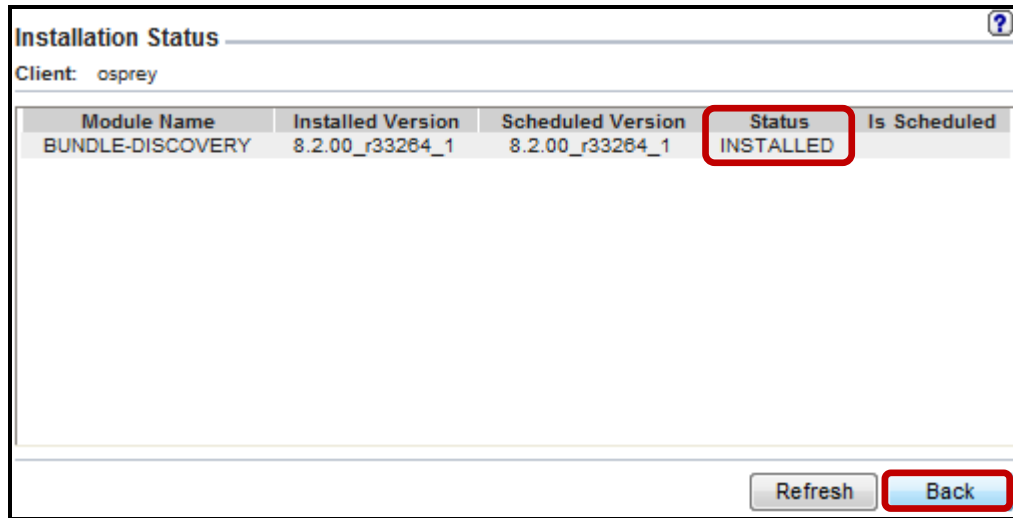
Installation Status ⓘ

Client: osprey

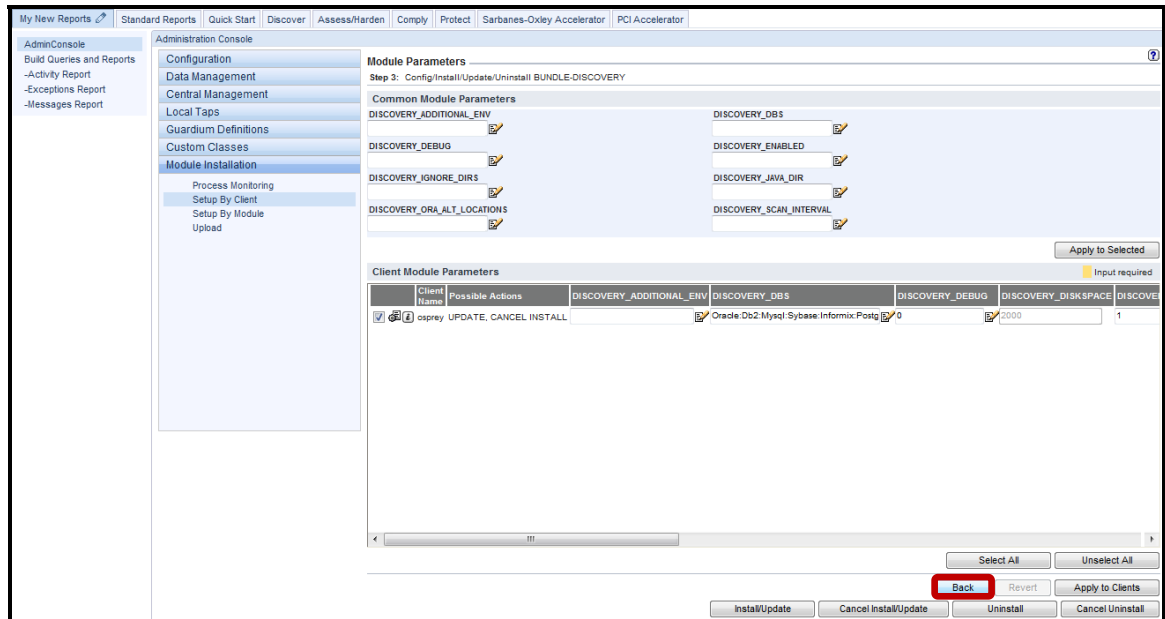
Module Name	Installed Version	Scheduled Version	Status	Is Scheduled
BUNDLE-DISCOVERY		8.2.00_r33264_1	IP	Y (2011-12-17 11:57:53.0)

Refresh Back

- __g. Once the installation has completed successfully, click **Back** to return to the **Module Parameters** screen.

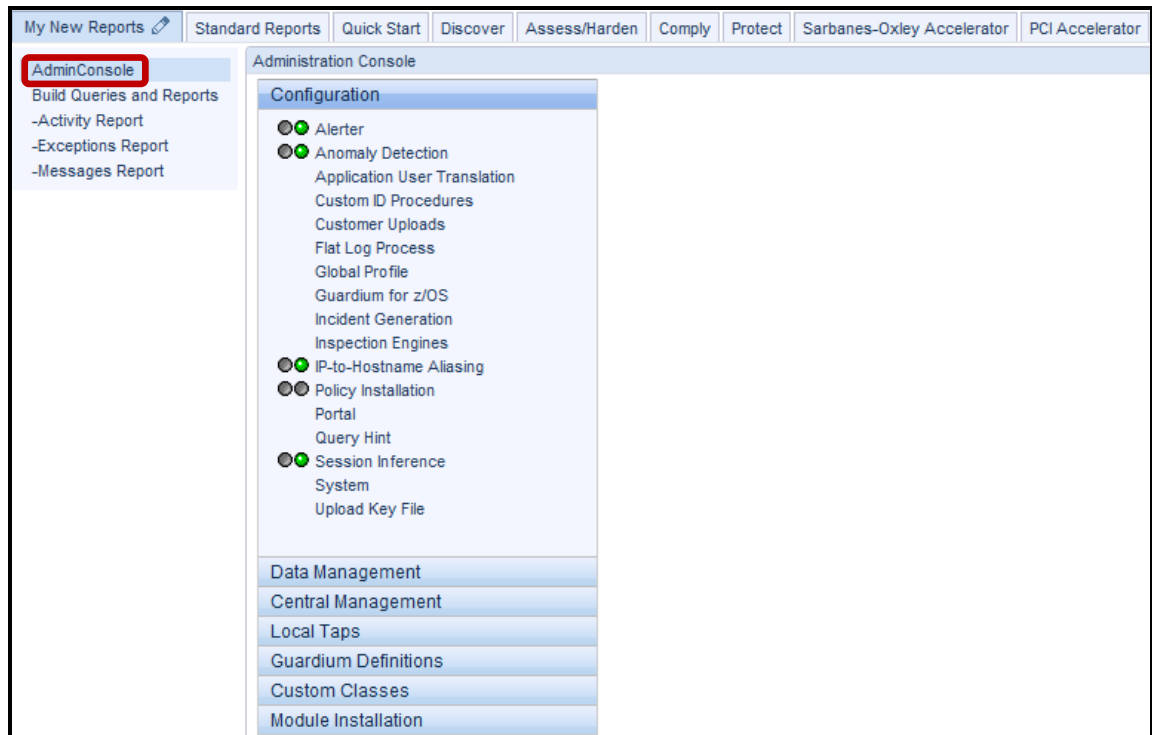


- __h. Click **Back** once more to return to the **Common Modules** screen.

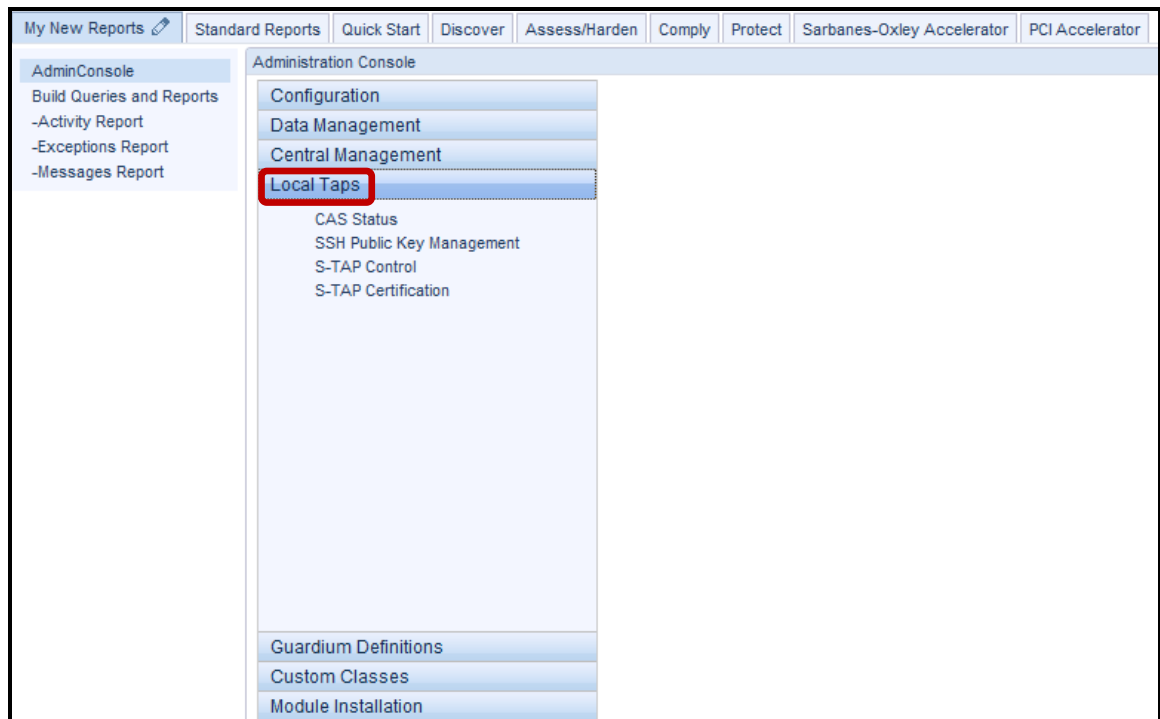


__7. Verify that CAS and S-TAP processes are communicating with the Appliance.

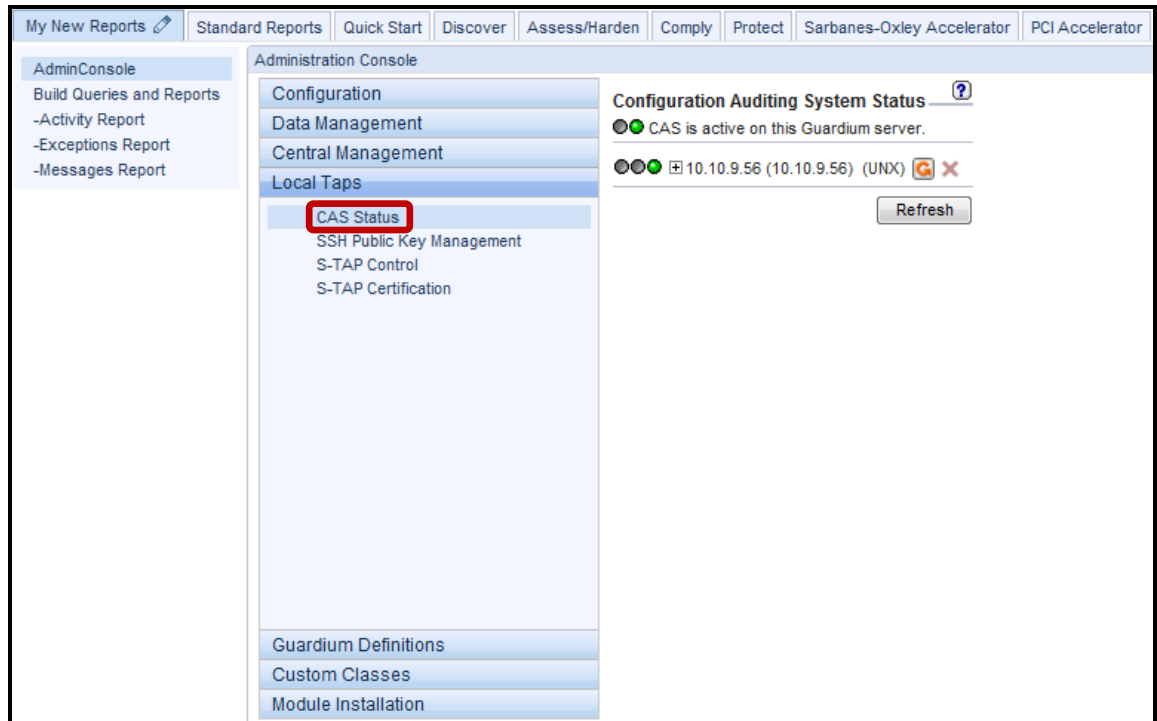
__a. Click **Admin Console** under the **My New Reports** tab.



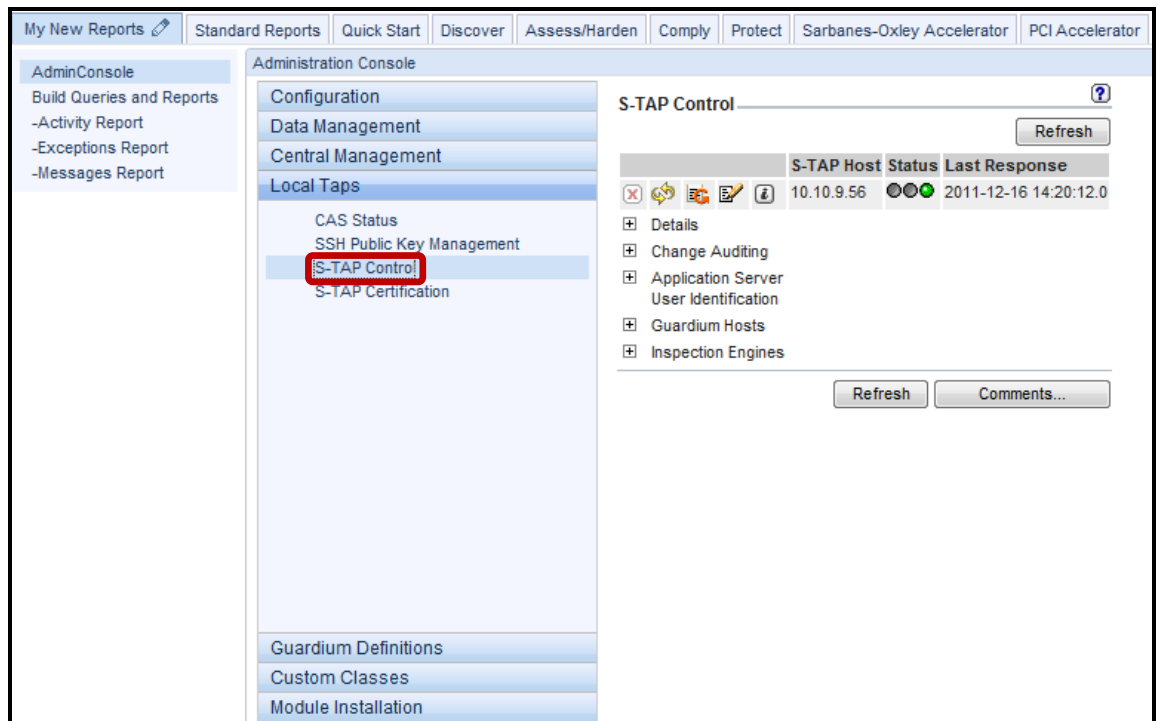
__b. Click **Local Taps**.



__c. Click **CAS Status** under **Local Taps**. It may take a few moments to display.




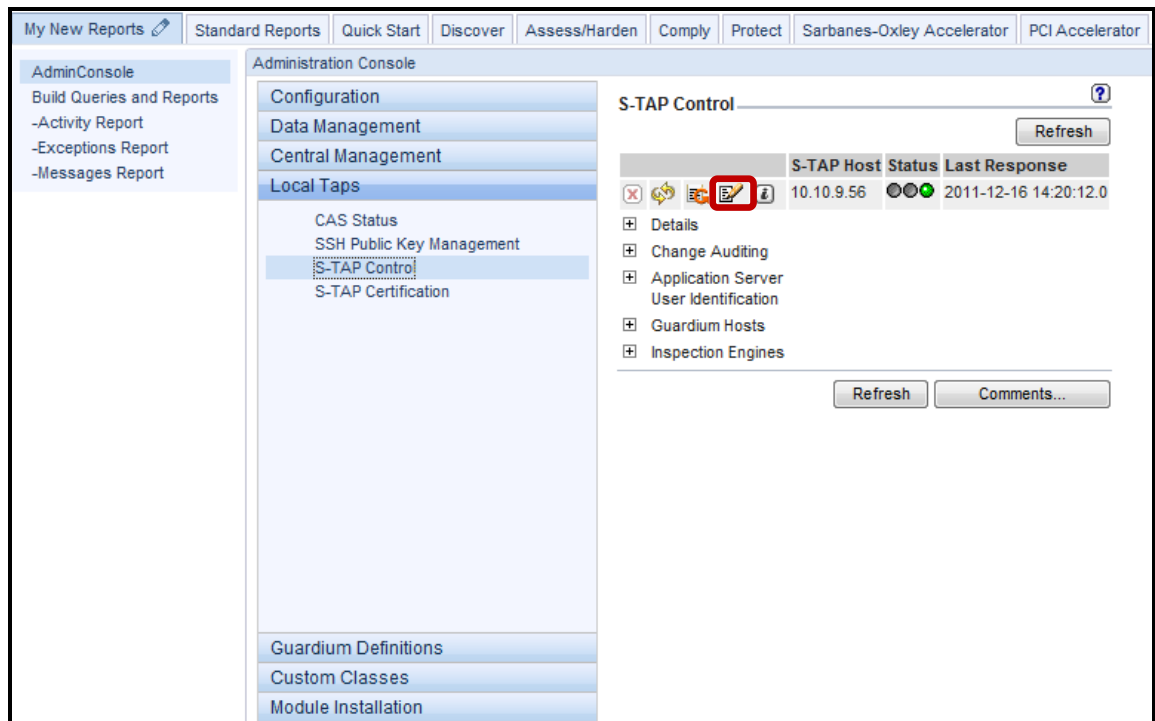
__d. Click **S-TAP Control** under **Local Taps**.



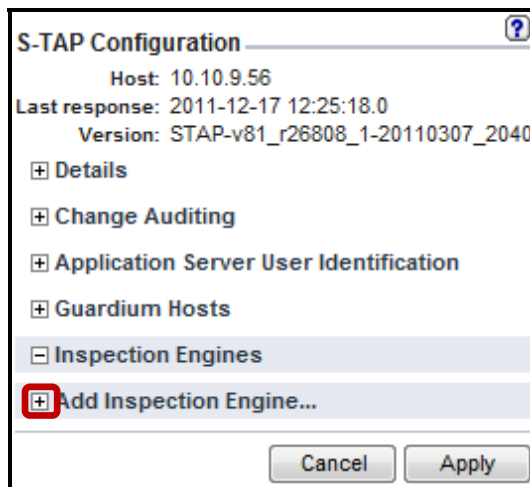
The green status indicators above confirm that the IBM InfoSphere Guardium appliance is communicating with the S-TAP and CAS processes on the database server.

__8. Configure Oracle Inspection Engine

__a. Click the  icon to edit the S-TAP Configuration.



__b. Click the '+' icon alongside **Add Inspection Engine** to create a new Inspection Engine.



- c. Enter the following values for the specified attributes to configure an Oracle Inspection Engine, and click **Add**.

Protocol: Oracle
Port Range: 1521 / 1521
KTAP DB Real Port: 1521
Client Ip/Mask: 0.0.0.0 / 0.0.0.0
DB Install Dir: /usr/lib/oracle/xe
Process Name: /usr/lib/oracle/xe/app/oracle/product/10.2.0/server/bin/oracle

The screenshot shows the 'S-TAP Configuration' dialog box. At the top, it displays system information: Host: 10.10.9.56, Last response: 2011-12-17 12:25:18.0, and Version: STAP-v81_r26808_1-20110307_2040. Below this is a list of expandable sections: Details, Change Auditing, Application Server User Identification, Guardium Hosts, Inspection Engines, and Add Inspection Engine... The 'Add Inspection Engine...' section is expanded, showing the following fields: Protocol (Oracle), Port Range (1521 - 1521), KTAP DB Real Port (1521), Client Ip/Mask (0.0.0.0 / 0.0.0.0), Exclude Client Ip/Mask, DB Install Dir (/usr/lib/oracle/xe), Process Name (/oracle/product/10.2.0/server/bin/oracle), Encryption (checkbox), and Intercept Types. There are 'Add Pair' buttons next to the Client Ip/Mask and Exclude Client Ip/Mask fields. At the bottom right, there is an 'Add' button, and at the bottom center, there are 'Cancel' and 'Apply' buttons. Red boxes highlight the Protocol dropdown, the Port Range and KTAP DB Real Port fields, the DB Install Dir and Process Name fields, and the Add button.

__d. Click **Apply**.

S-TAP Configuration ?

Host: 10.10.9.56
Last response: 2011-12-17 12:25:18.0
Version: STAP-v81_r26808_1-20110307_2040

- Details
- Change Auditing
- Application Server User Identification
- Guardium Hosts
- Inspection Engines**

Protocol: Oracle

Port Range: 1521 - 1521

KTAP DB Real Port: 1521

Client Ip/Mask: 0.0.0.0 / 0.0.0.0 Add Pair

Exclude Client Ip/Mask Add Pair

DB Install Dir: /usr/lib/oracle/xe

Process Name: /usr/lib/oracle/xe/app/oracle/product/10

Encryption:

Intercept Types:

Delete

Add Inspection Engine...

Protocol:

Port Range: -

KTAP DB Real Port:

Client Ip/Mask: / Add Pair

Exclude Client Ip/Mask: / Add Pair

DB Install Dir:

Process Name:

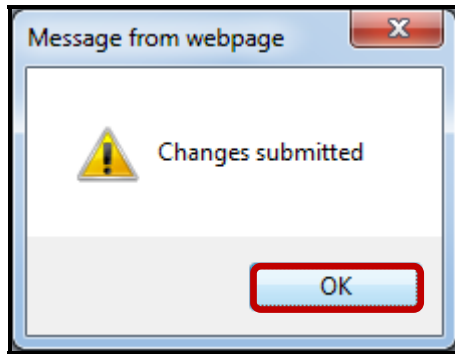
Encryption:

Intercept Types:

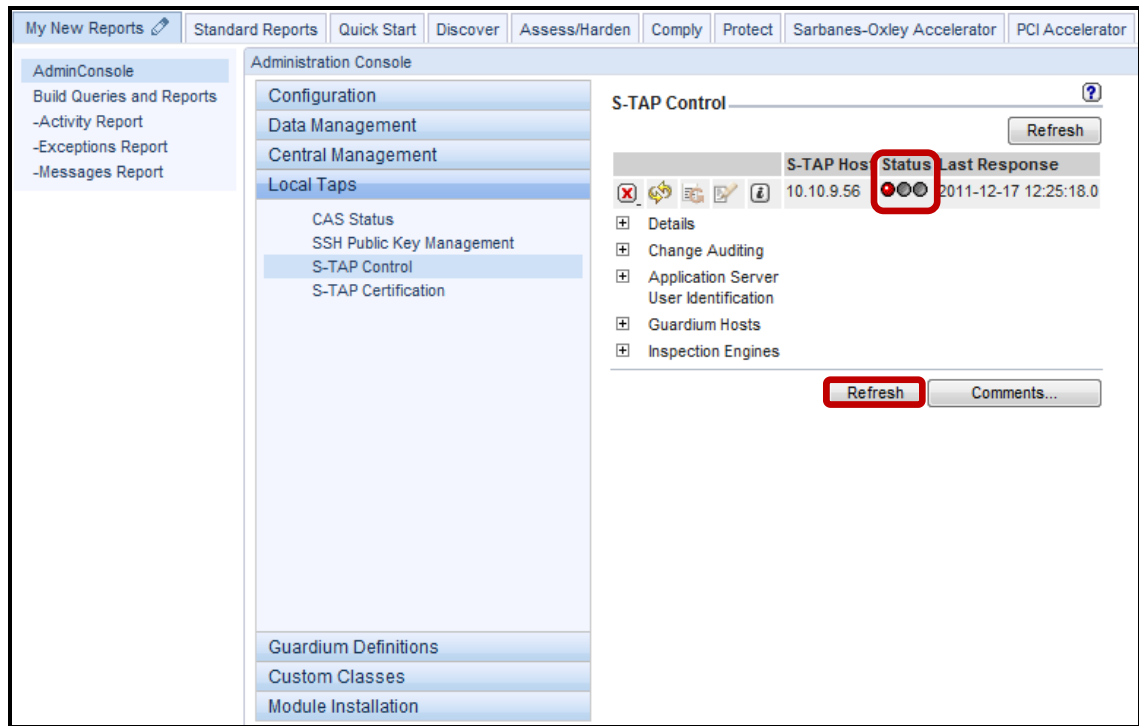
Add

Cancel **Apply**

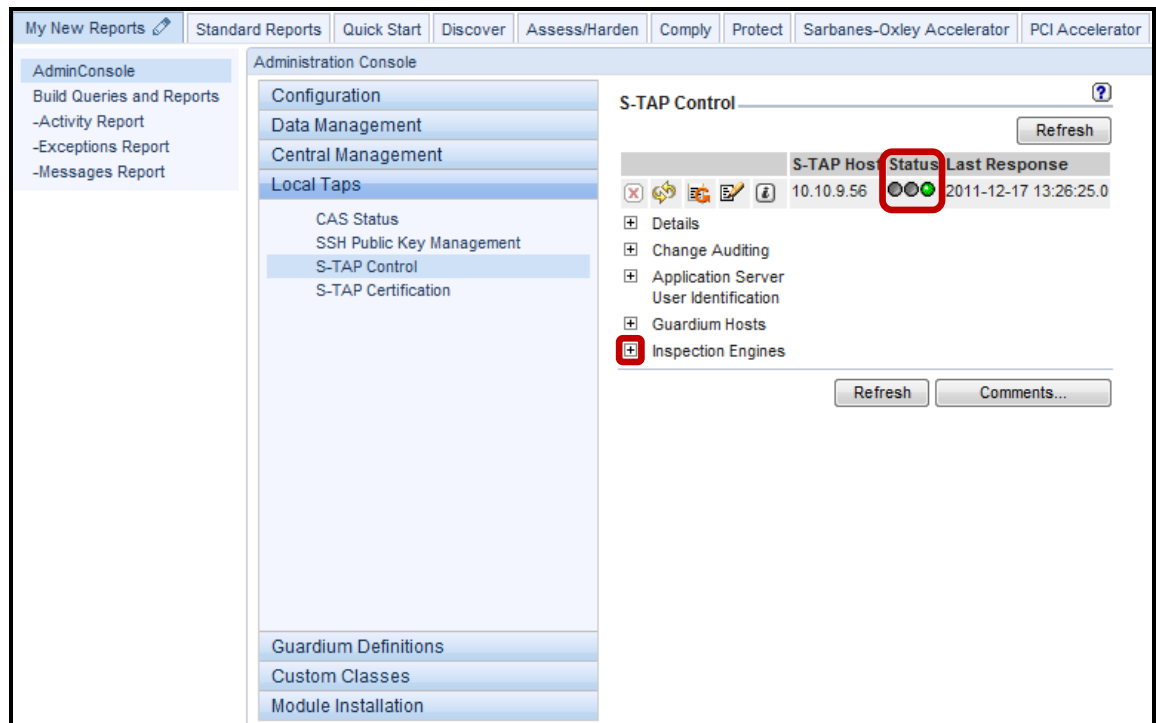
__e. Click **OK** to acknowledge changes have been submitted.



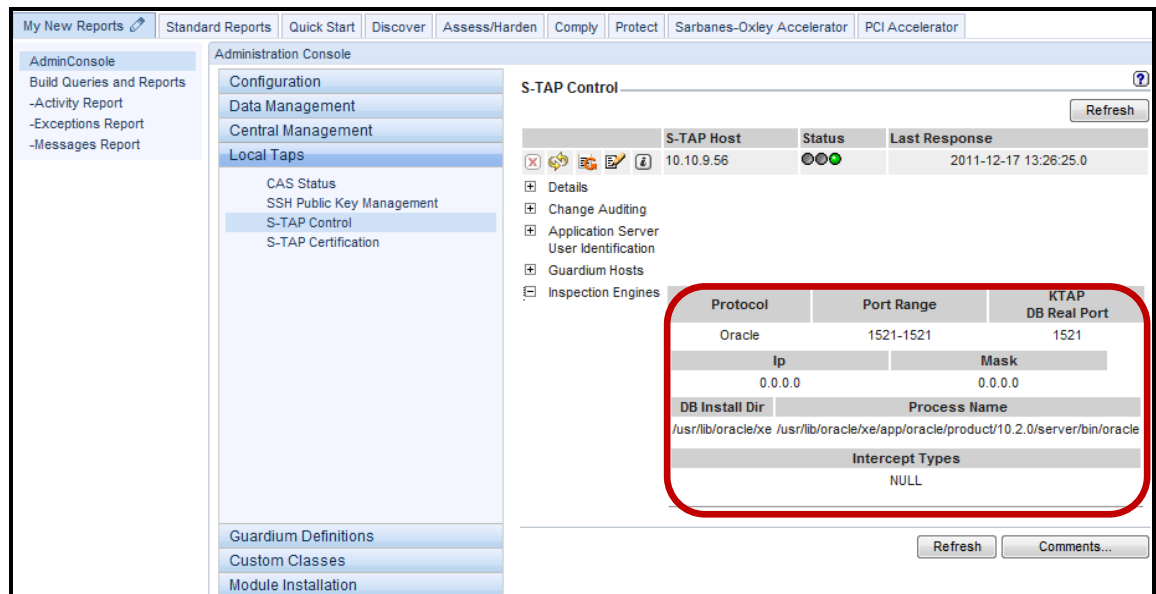
__f. The S-TAP will restart to apply the new Inspection Engine.



__g. Click **Refresh** until the color changes back to green.



__h. Click the '+' icon alongside **Inspection Engines** to confirm that the new Oracle Inspection Engine has been added correctly.



- __9. Now, verify that the IBM InfoSphere Guardium Appliance is capturing SQL statements.
- __a. Return to the PuTTY ssh session and login as the Oracle DBA account (**su - oracle**).

```

root@osprey:~
=starting Oracle10g...

LSNRCTL for Linux: Version 10.2.0.1.0 - Production on 08-JAN-2012 09:57:55

Copyright (c) 1991, 2005, Oracle. All rights reserved.

TNS-01106: Listener using listener name LISTENER has already been started

SQL*Plus: Release 10.2.0.1.0 - Production on Sun Jan 8 09:57:55 2012

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

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

SQL> ORA-(1081: cannot start already-running ORACLE - shut it down first
SQL> Disconnected from Oracle Database 10g Express Edition Release 10.2.0.1.0 -
Production
=starting PostgreSQL...
Starting postgresql-9.1 service: [ OK ]
=starting Sybase15...
[root@osprey ~]# su - oracle
-bash-3.00$

```

- __b. Then, login to Oracle by typing: **sqlplus system/guardium**, and type the SQL Query **'select * from dba_users;'**.

```

root@osprey:~
Copyright (c) 1982, 2005, Oracle. All rights reserved.

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

SQL> ORA-01081: cannot start already-running ORACLE - shut it down first
SQL> Disconnected from Oracle Database 10g Express Edition Release 10.2.0.1.0 -
Production
=starting PostgreSQL...
Starting postgresql-9.1 service: [ OK ]
=starting Sybase15...
[root@osprey ~]# su - oracle
-bash-3.00$ sqlplus system/guardium

SQL*Plus: Release 10.2.0.1.0 - Production on Sun Jan 8 09:59:54 2012

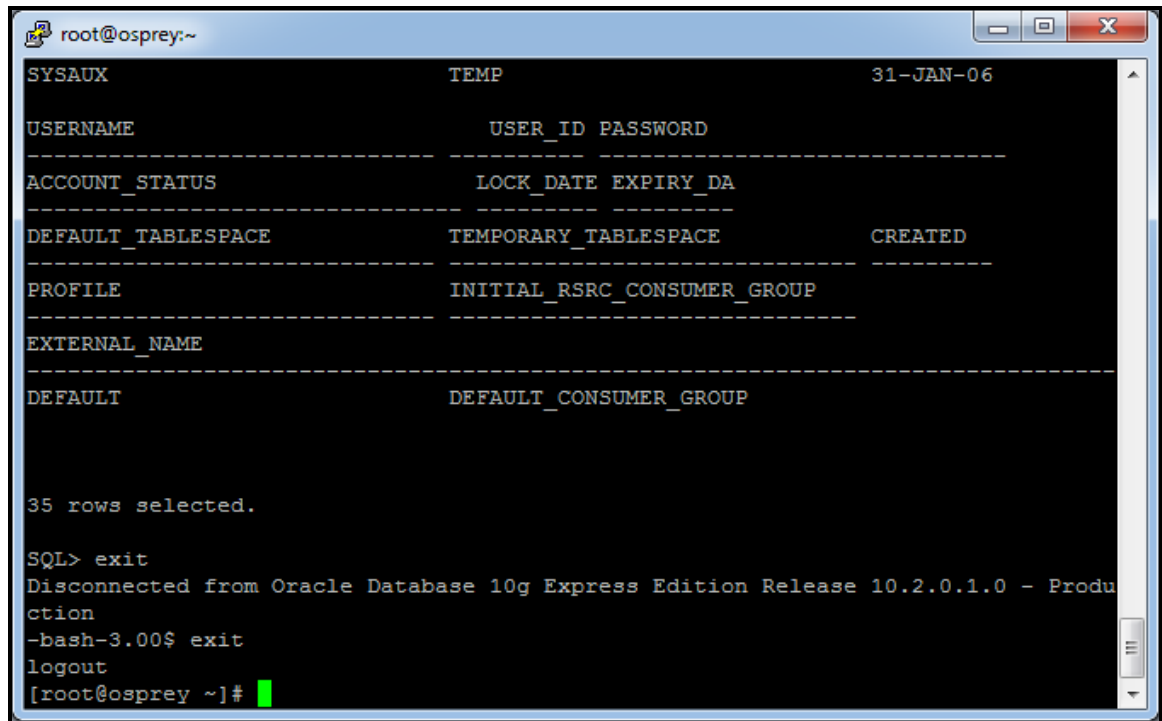
Copyright (c) 1982, 2005, Oracle. All rights reserved.

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

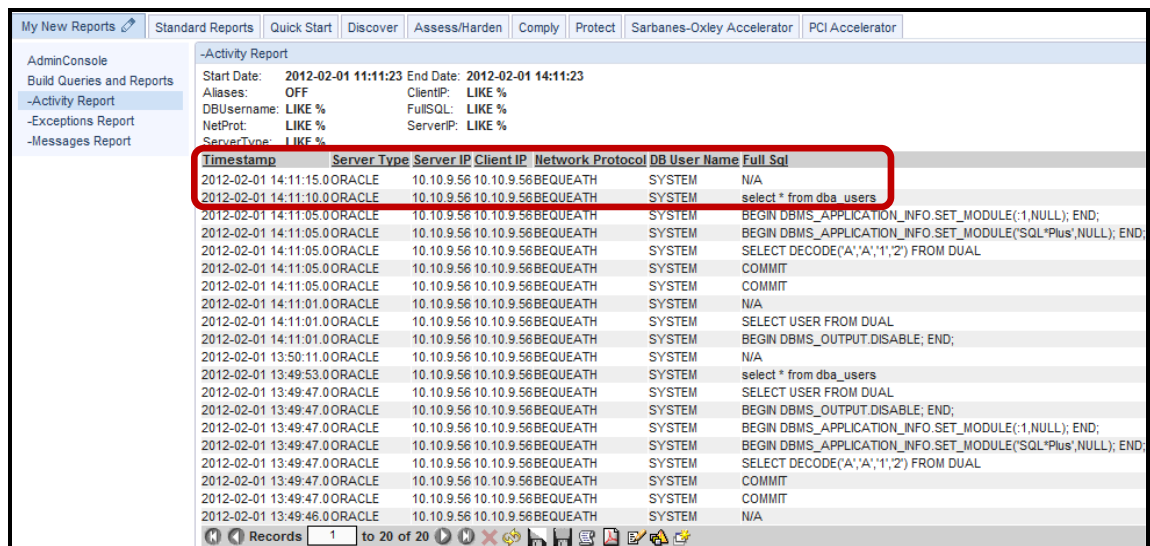
SQL> select * from dba_users;

```


- c. After receiving the result set, type **exit** to exit Oracle sqlplus, and then type **exit** to return to the root user account shell.



- d. From the IBM InfoSphere Guardium GUI, verify that Oracle SQL is being captured. Click **-Activity Report** under the **My New Reports** tab.



Note: The logged SQL statement from your query will appear in the **Full_Sql** column along with additional details captured at the time that the SQL statement was executed.

Thank You

4.3 GIM Discovery to Automate Inspection Engine Configuration

Overview

The GIM Discovery module requires an existing S-TAP installation, and provides the powerful capability to scan and detect multiple, active database instances. The results of these scans can be viewed by the “Database Instances” report. Since, the information gathered by GIM Discovery is sufficient to create an Inspection Engine, the InfoSphere Guardium drilldown feature has been enhanced to enable the results from a Discovery scan to automatically “invoke” the GrdAPI command line interface, and create an Inspection Engine.

One of the key advantages of leveraging this capability is that it saves time by eliminating the risk of manual error caused by a typing error or by using bad information that was errantly produced. The end result is that in a matter of minutes, one or many Inspection Engines can be automatically created, and no time is wasted debugging an incorrect parameter on a manually created Inspection Engine.

Note that GIM Discovery has no connection to Database Auto-Discovery (which requires no software).

Objectives

This lab will demonstrate the ease with which the IBM InfoSphere Guardium solution can be deployed in an enterprise environment. We will focus on leveraging capabilities of the IBM InfoSphere Guardium Installation Manager (GIM) Discovery software module to perform automated database instance scans on database servers, and to automate the creation of a DB2 Inspection Engine.

The following steps will guide us through the lab:

- __1. Make use of the GIM Discovery Module (deployed in the last section) to scan the Database Server and produce a list of discovered database instances.
- __2. Use the InfoSphere Guardium capability to drill down to invoke a GrdAPI command and automatically create a DB2 Inspection Engine.

Key Benefit: Through the GUI, quickly discover new databases and add inspection engines without system level commands or requiring additional external group (DBAs, system administrators and others) intervention.
- __3. Use the browser-based interface to validate the automatically generated DB2 Inspection Engine.
- __4. Demonstrate how to set up a Compliance Workflow Automation job to discover new database instances, and create associated Inspection Engines as necessary.

- __1. Launch the InfoSphere Guardium GUI to verify the GIM client software installation performed during the previous lab section.
 - __a. Login as user **pot** / **guardium**.

Login

Please enter your information

User name:

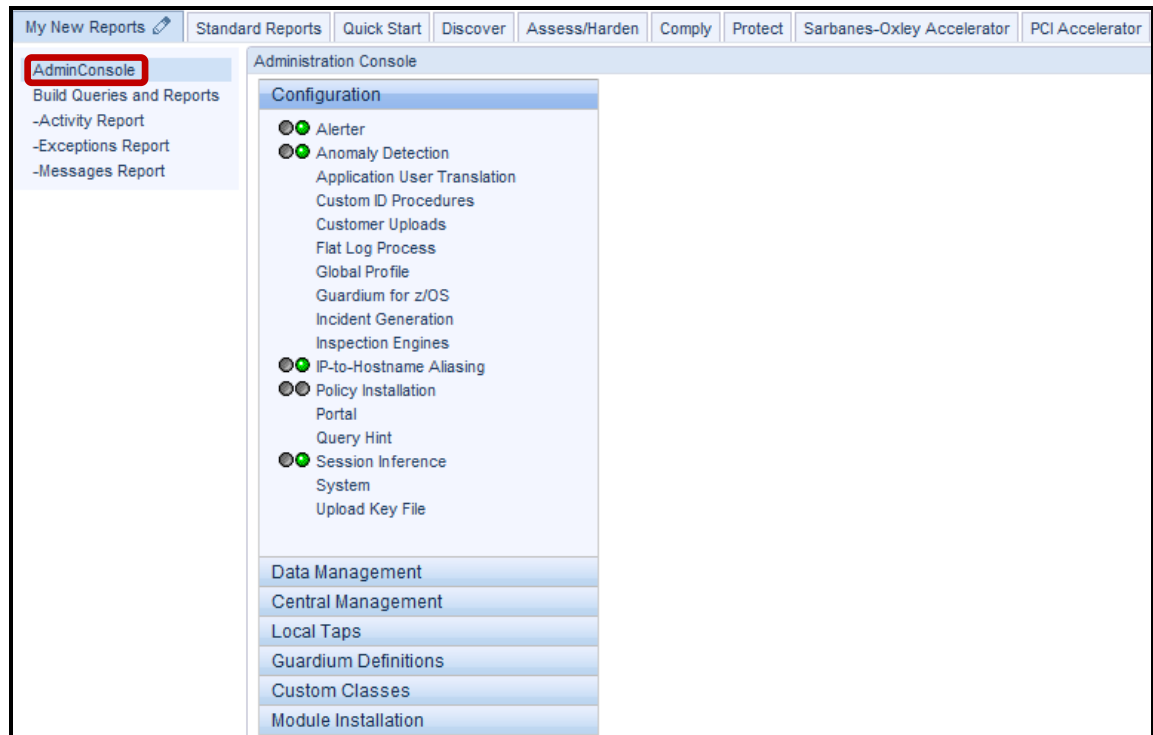
Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

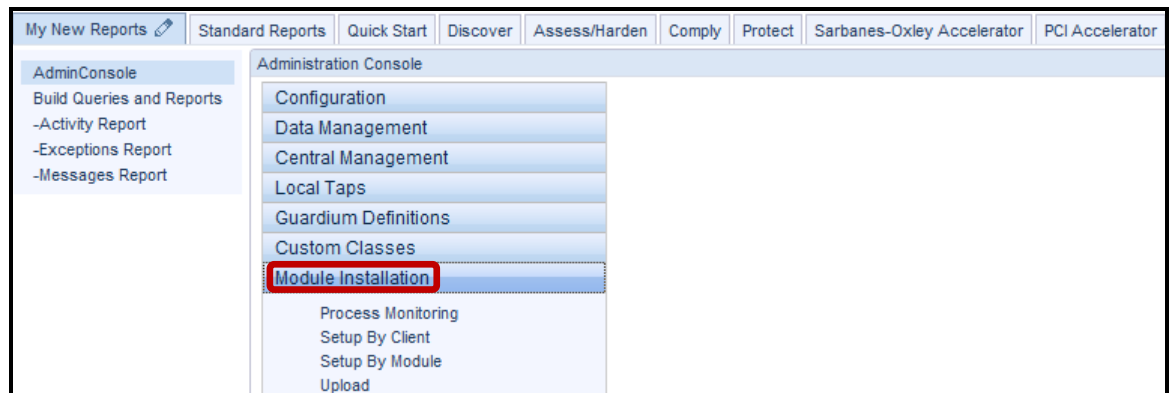
Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistry/key © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com, Zthread © Copyright 2000-2003, Eric Crahen.

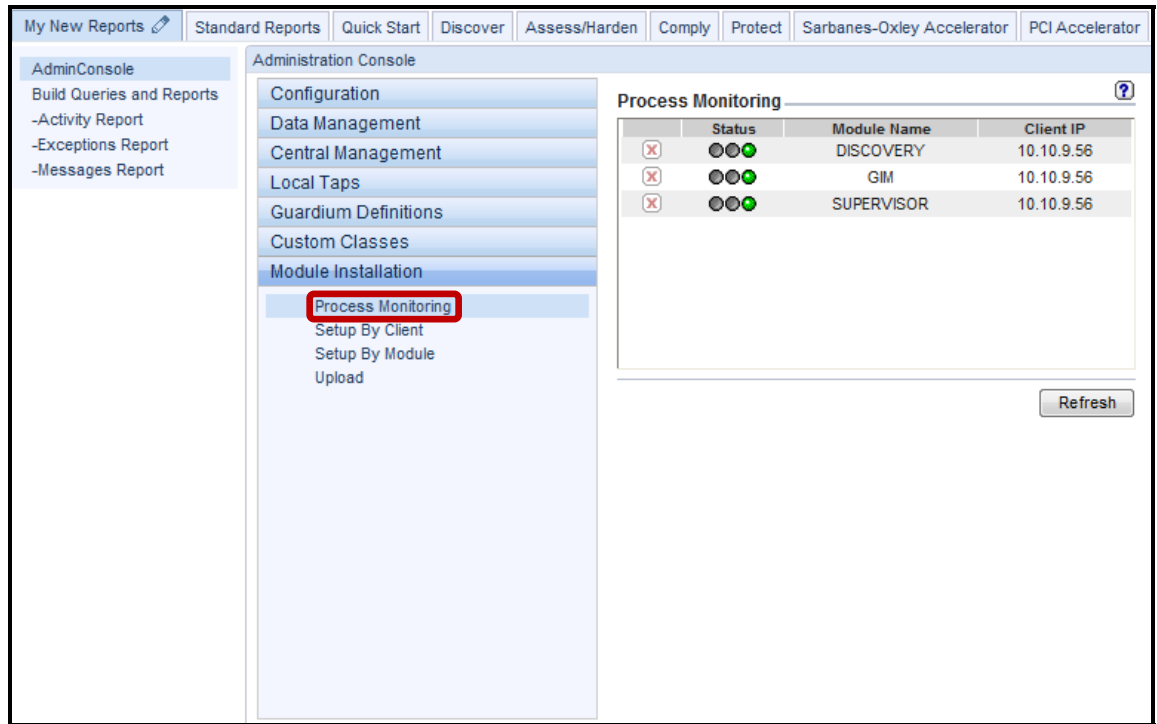
- __b. Verify GIM process communication.
- __c. Click **Admin Console** under the **My New Reports** tab.



- __d. Click **Module Installation**.

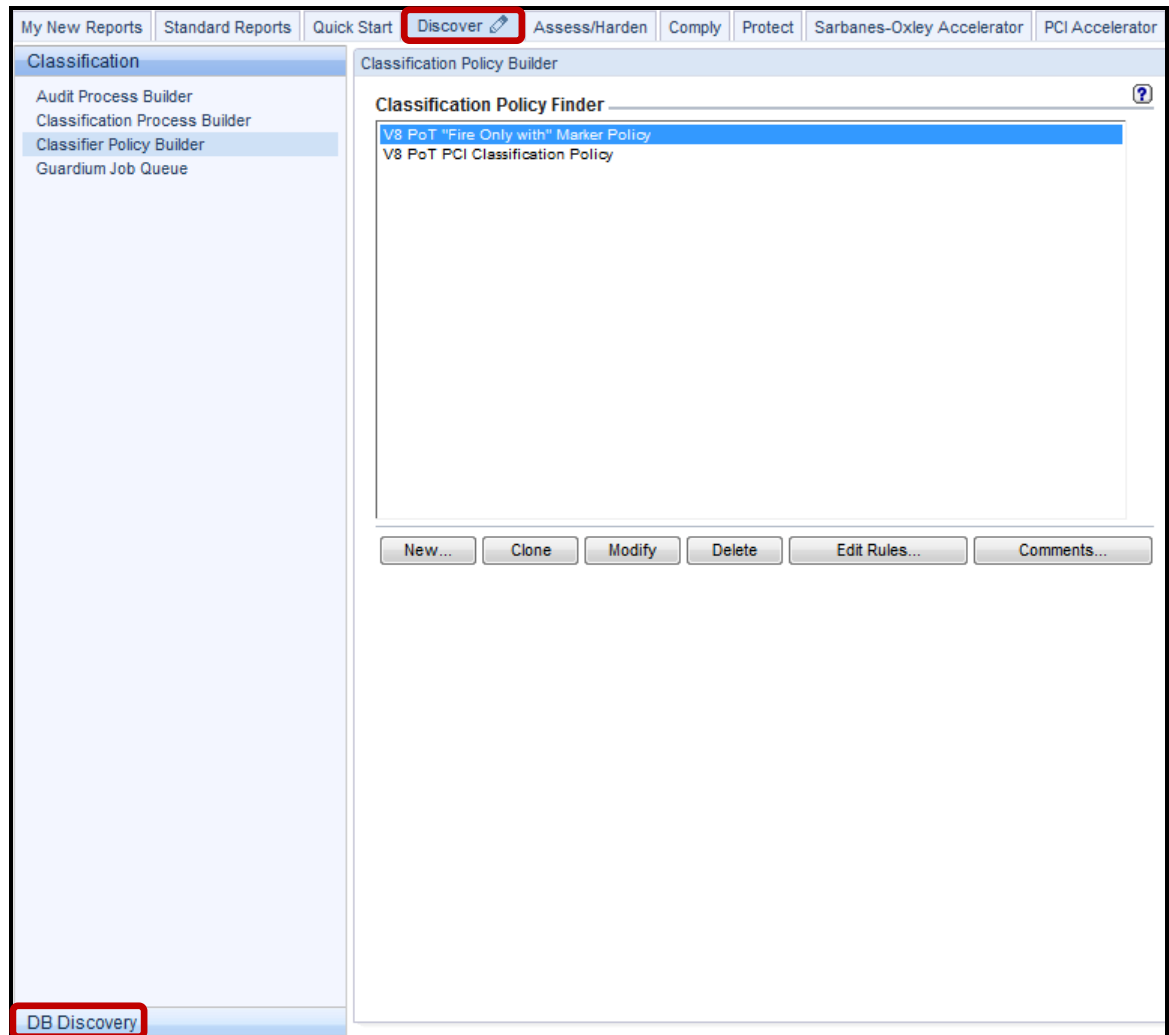


__e. Click **Process Monitoring** under the **Module Installation** tab.



The green status lights should appear for 'DISCOVERY', 'GIM', and 'SUPERVISOR' modules which are now running on the database server. A corresponding pair of 'DISCOVERY', 'GIM', and 'SUPERVISOR' processes will appear for each client IP being managed by GIM.

- __2. Check for Instances discovered by the GIM Discovery Module
- __a. Click the **Discover** tab, then scroll down and click **DB Discovery** on the bottom left of the page.



b. Click **Discovered Instances** under the **DB Discovery** tab.

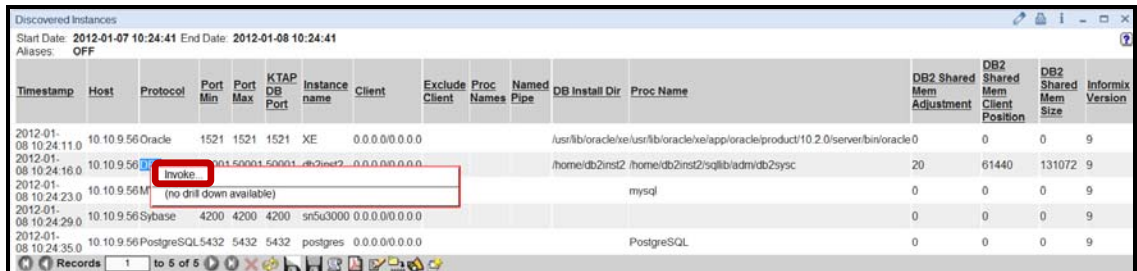
Note: Inspection Engines are discovered ONCE by the GIM Discovery module. In order to see all discovered instances the date filter in this screen should be set to wide range.



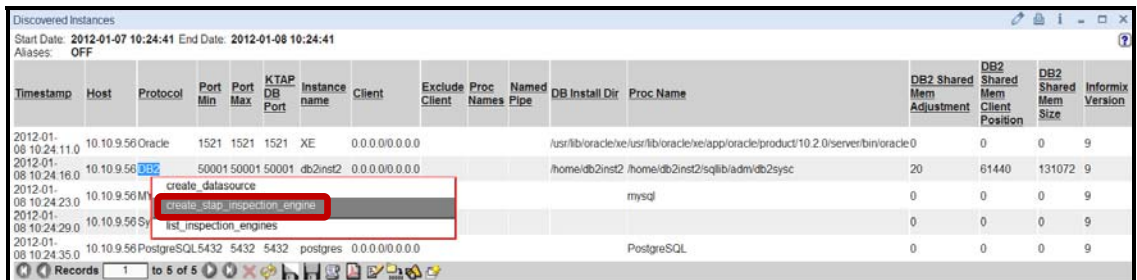
c. Locate the entry for DB2.



d. Double-click **DB2** beneath the Protocol column heading to access the Guardium drilldown menu, and first select 'Invoke'.



e. Then, select 'create_stap_inspection_engine' from the Invoke submenu.



__f. Click **Invoke now** from the dialog box.

IBM® InfoSphere™ Guardium®

Report: Discovered Instances
Api Function: create_stap_inspection_engine

stapHost	10.10.9.56
protocol	DB2
portMin	50001
portMax	50001
teeListenPort	
teeRealPort	
connectToIp	127.0.0.1
client	0.0.0.0/0.0.0.0
excludeClient	
procNames	
namedPipe	
ktapDbPort	50001
dbInstallDir	/home/db2inst2
procName	/home/db2inst2/sqllib/adm/c
db2SharedMemAdjustment	20
db2SharedMemClientPosition	61440
db2SharedMemSize	131072
instanceName	db2inst2
informixVersion	9
encryption	0
interceptTypes	
api_target_host	

*Required parameter

Log level: 0

Parameter to encrypt: -----

Generate script **Invoke now**

__g. Click **Close** once the 'ID=N' appears, and cancel the previous 'Invoke now' dialog box.

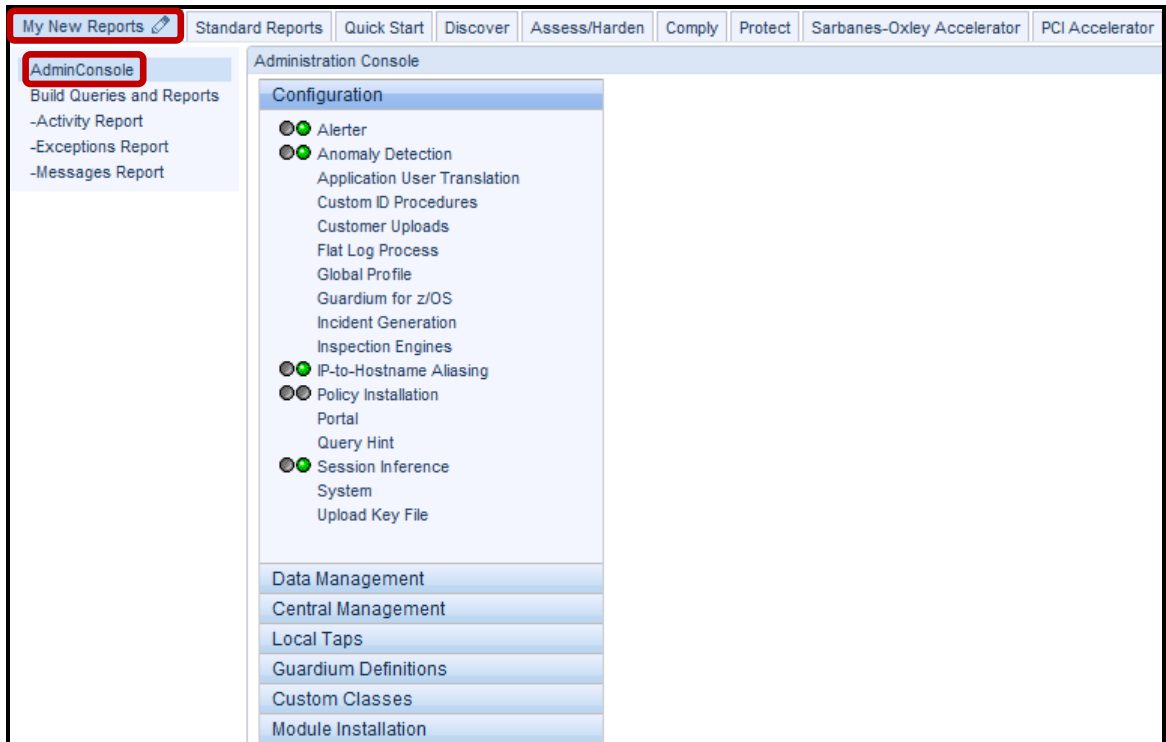
Api Call Output create_stap_inspection_engine

Call Output

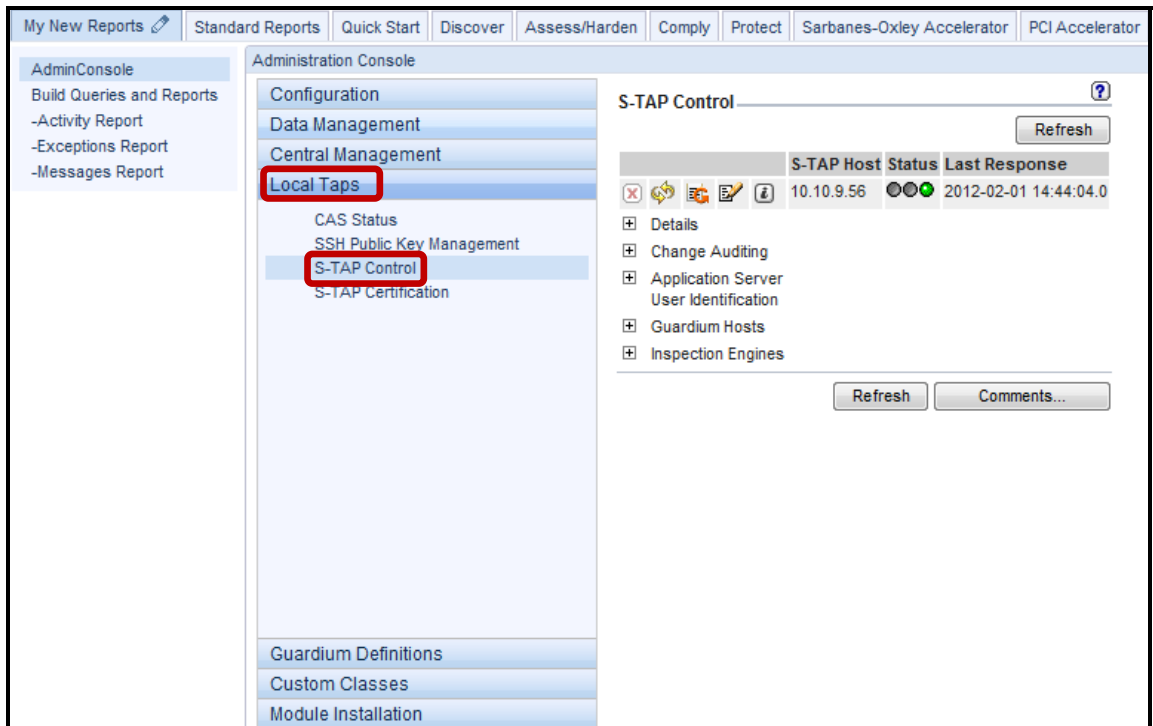
ID=5

Close

__h. Now, click **AdminConsole** under the **My New Reports** tab.



__i. Click **S-TAP Control** under the **Local Taps** tab.



- j. Click the '+' icon alongside **Inspection Engines** to reveal the new DB2 Inspection Engine automatically created using GIM Discovery, and the GrdAPI.

The screenshot shows the Administration Console interface. On the left is a navigation menu with sections like 'AdminConsole', 'Local Taps', and 'Guardium Definitions'. The main area is titled 'S-TAP Control' and contains a table of hosts and their configurations. A red box highlights the configuration for a DB2 engine.

S-TAP Host	Status	Last Response
10.10.9.56		2012-02-01 14:44:04.0

Protocol	Port Range	KTAP DB Real Port
Oracle	1521-1521	1521

Ip	Mask
0.0.0.0	0.0.0.0

DB Install Dir	Process Name
/usr/lib/oracle/xe	/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/bin/oracle

Intercept Types		
NULL		

Protocol	Port Range	KTAP DB Real Port
DB2	50001-50001	50001

Ip	Mask
0.0.0.0	0.0.0.0

DB Install Dir	Process Name
/home/db2inst2	/home/db2inst2/sqllib/adm/db2sysc

DB2 Shared Memory Adjustment	DB2 Shared Memory Client Position	DB2 Shared Memory Size
20	61440	131072

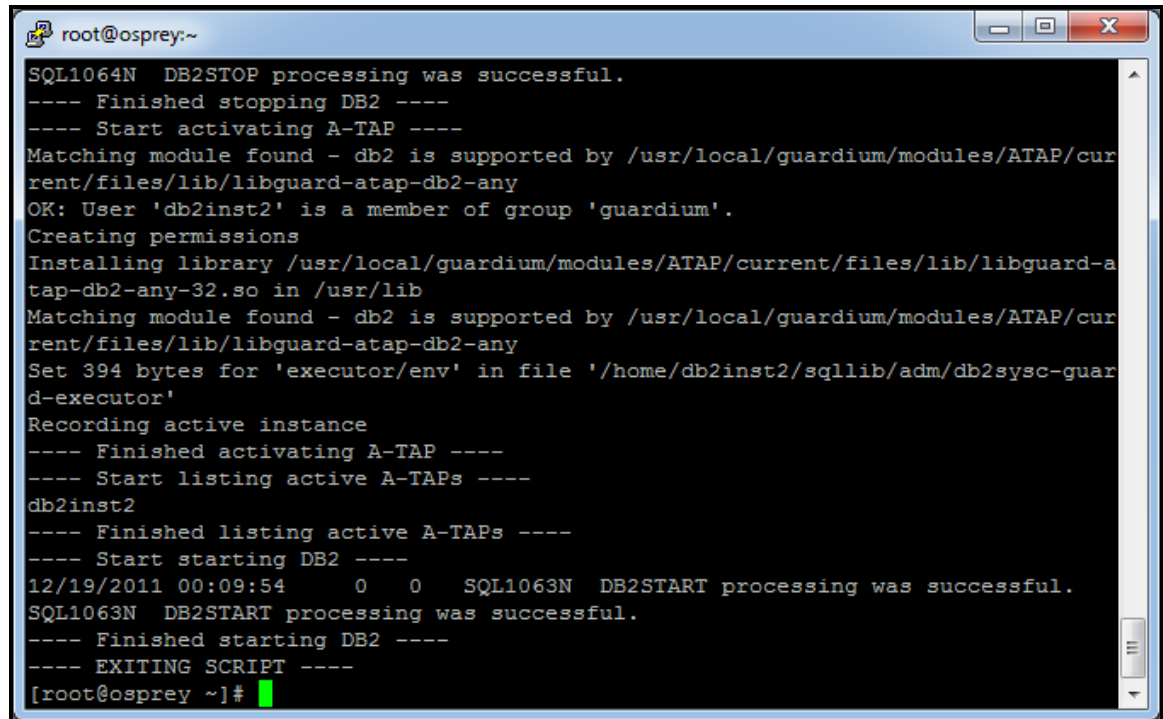
Intercept Types		
NULL		

- __3. Now, verify that the IBM InfoSphere Guardium Appliance is capturing SQL statements.
- __a. **Critical Step.** In the case of DB2 on Linux, there is an additional step that must be taken to enable the monitoring of DB2 Shared Memory (ATAP).

Make sure you are at the root account shell before running this script.

Return the PuTTY ssh session and execute the following script (**Must be run as root**):

./Lab4-DB2ATAPInstall.sh



```
root@osprey:~  
SQL1064N  DB2STOP processing was successful.  
---- Finished stopping DB2 ----  
---- Start activating A-TAP ----  
Matching module found - db2 is supported by /usr/local/guardium/modules/ATAP/current/files/lib/libguard-ata  
tap-db2-any-32.so in /usr/lib  
OK: User 'db2inst2' is a member of group 'guardium'.  
Creating permissions  
Installing library /usr/local/guardium/modules/ATAP/current/files/lib/libguard-a  
tap-db2-any-32.so in /usr/lib  
Matching module found - db2 is supported by /usr/local/guardium/modules/ATAP/current/files/lib/libguard-ata  
tap-db2-any-32.so in /usr/lib  
Set 394 bytes for 'executor/env' in file '/home/db2inst2/sqllib/adm/db2sysc-guard  
d-executor'  
Recording active instance  
---- Finished activating A-TAP ----  
---- Start listing active A-TAPs ----  
db2inst2  
---- Finished listing active A-TAPs ----  
---- Start starting DB2 ----  
12/19/2011 00:09:54    0    0    SQL1063N  DB2START processing was successful.  
SQL1063N  DB2START processing was successful.  
---- Finished starting DB2 ----  
---- EXITING SCRIPT ----  
[root@osprey ~]#
```

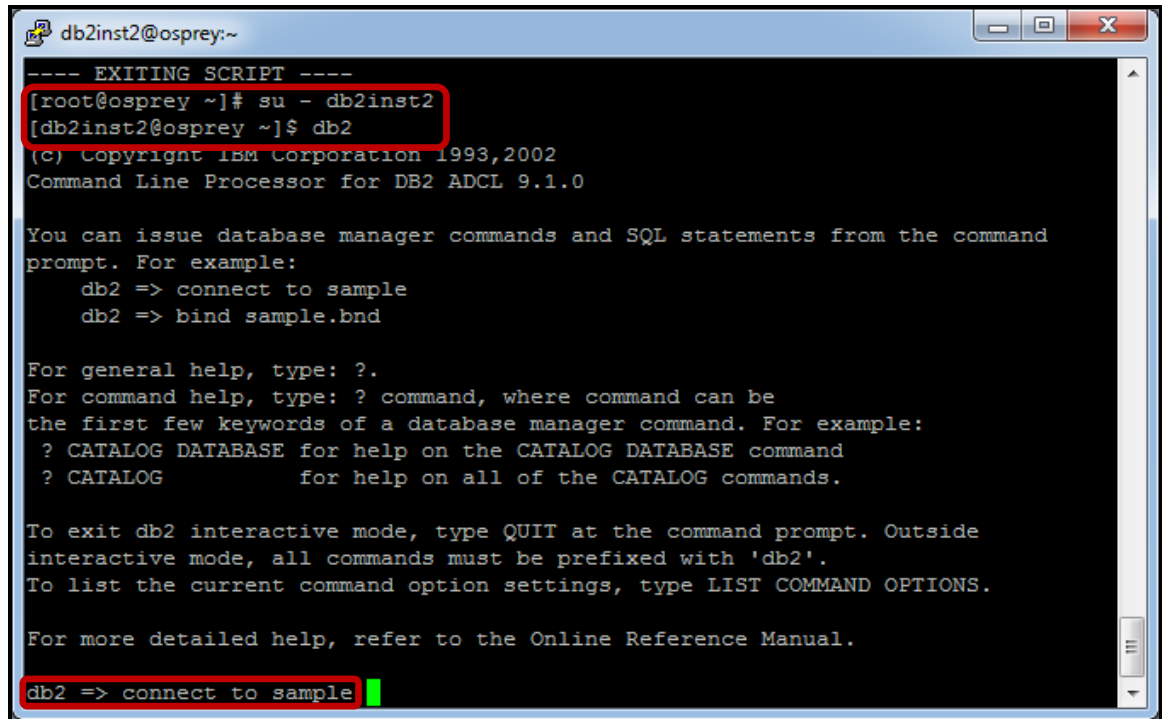
The contents of the **DB2ATAPInstall.sh** script:

```
#!/bin/sh

echo '---- Adding Guardium to db2inst2 Group ----'
usermod -G guardium db2inst2

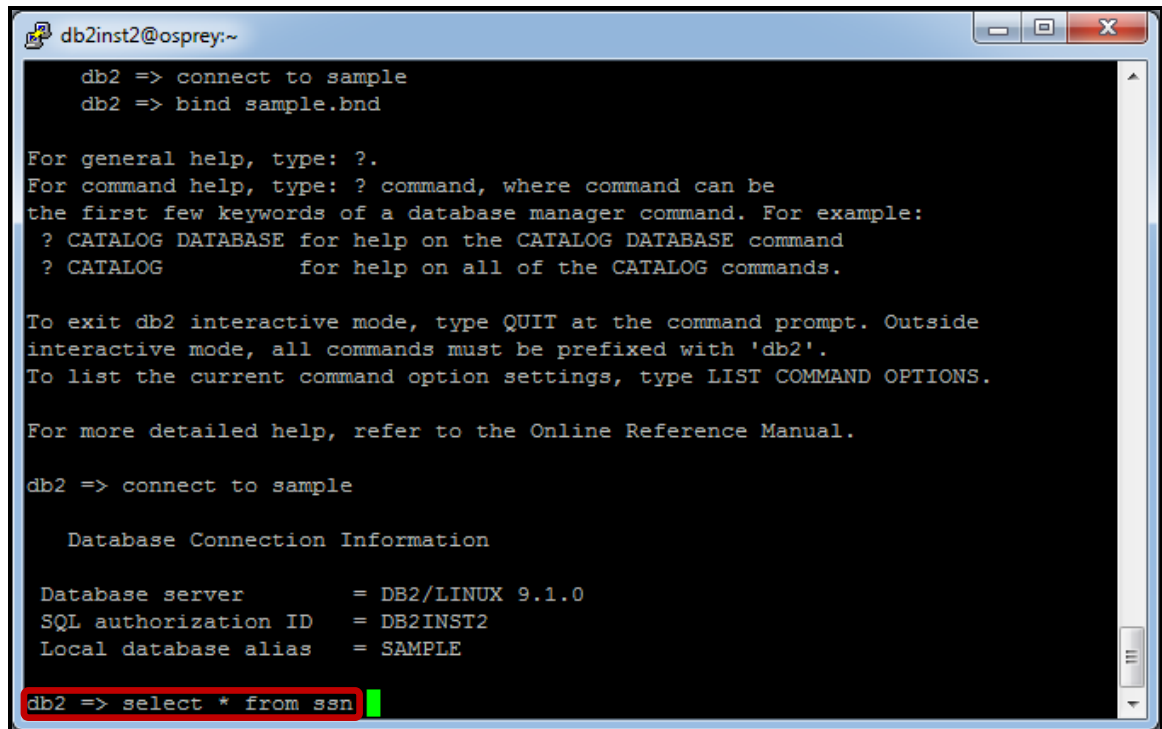
# Sets the A-TAP configuration parameters
echo '---- Start setting the A-TAP configuration parameters ----'
/usr/local/guardium/modules/ATAP/current/files/bin/guardctl db-instance=db2inst2
db-user=db2inst2 db-type=db2 db2-shmsize=131072 db2-c2soffset=61440 db2-
header_offset=20 db-home=/home/db2inst2 db-version=any store-conf
echo '---- Finished setting the A-TAP configuration parameters ----'
echo '---- Start stopping DB2 ----'
# Stop db2, need to switch to db2inst2 to do that
su - db2inst2 -c db2stop
echo '---- Finished stopping DB2 ----'
echo '---- Start activating A-TAP ----'
# Activate the A-TAP
/usr/local/guardium/modules/ATAP/current/files/bin/guardctl db-instance=db2inst2
db-type=db2 activate
echo '---- Finished activating A-TAP ----'
echo '---- Start listing active A-TAPs ----'
# List active A-TAPs to confirm
/usr/local/guardium/modules/ATAP/current/files/bin/guardctl list-active
echo '---- Finished listing active A-TAPs ----'
echo '---- Start starting DB2 ----'
# Start db2, need to switch to db2inst9 to do that
su - db2inst2 -c db2start
echo '---- Finished starting DB2 ----'
```

- __b. Next, log in as the DB2 DBA account (**su – db2inst2**). Then, initiate a *Shared Memory* connection to DB2 by typing: **db2** followed by **connect to sample**.



```
db2inst2@osprey:~  
---- EXITING SCRIPT ----  
[root@osprey ~]# su - db2inst2  
[db2inst2@osprey ~]$ db2  
(c) Copyright IBM Corporation 1993,2002  
Command Line Processor for DB2 ADCL 9.1.0  
  
You can issue database manager commands and SQL statements from the command  
prompt. For example:  
    db2 => connect to sample  
    db2 => bind sample.bnd  
  
For general help, type: ?.  
For command help, type: ? command, where command can be  
the first few keywords of a database manager command. For example:  
    ? CATALOG DATABASE for help on the CATALOG DATABASE command  
    ? CATALOG           for help on all of the CATALOG commands.  
  
To exit db2 interactive mode, type QUIT at the command prompt. Outside  
interactive mode, all commands must be prefixed with 'db2'.  
To list the current command option settings, type LIST COMMAND OPTIONS.  
  
For more detailed help, refer to the Online Reference Manual.  
  
db2 => connect to sample
```

- __c. Type the **select * from ssn**.



```
db2inst2@osprey:~  
db2 => connect to sample  
db2 => bind sample.bnd  
  
For general help, type: ?.  
For command help, type: ? command, where command can be  
the first few keywords of a database manager command. For example:  
    ? CATALOG DATABASE for help on the CATALOG DATABASE command  
    ? CATALOG           for help on all of the CATALOG commands.  
  
To exit db2 interactive mode, type QUIT at the command prompt. Outside  
interactive mode, all commands must be prefixed with 'db2'.  
To list the current command option settings, type LIST COMMAND OPTIONS.  
  
For more detailed help, refer to the Online Reference Manual.  
  
db2 => connect to sample  
  
Database Connection Information  
  
Database server      = DB2/LINUX 9.1.0  
SQL authorization ID = DB2INST2  
Local database alias = SAMPLE  
  
db2 => select * from ssn
```

- __d. Now, type **connect to sample2 user db2inst2 using guardium** to initiate a *TCP* connection to DB2, and type **select * from ssn** once more.

```

db2inst2@osprey:~
35 Dole                Bob                234-56-7835
36 Dunn                Bob                234-56-7836
37 OLeary              Bob                234-56-7837
38 OTool               Bob                234-56-7838
39 Peterson            Bob                234-56-7839
40 Parke               Bob                234-56-7840
41 Wadsworth           Bob                234-56-7841
42 Anthony             John               234-56-7842
43 Thomas              John               234-56-7843
44 Smith               John               234-56-7844
45 Jones               John               234-56-7845
46 Craven              John               234-56-7846

47 record(s) selected.

db2 => connect to sample2 user db2inst2 using guardium

Database Connection Information

Database server          = DB2/LINUX 9.1.0
SQL authorization ID    = DB2INST2
Local database alias    = SAMPLE2

db2 => select * from ssn

```

- __e. Type **quit** to exit the db2 command prompt, and then **exit** to return to the root user account shell.

```

db2inst2@osprey:~
29 Williams           Bob                234-56-7829
30 Davis              Bob                234-56-7830
31 Wilson             Bob                234-56-7831
32 Miller             Bob                234-56-7832
33 Brown              Bob                234-56-7833
34 Dillon             Bob                234-56-7834
35 Dole               Bob                234-56-7835
36 Dunn              Bob                234-56-7836
37 OLeary            Bob                234-56-7837
38 OTool             Bob                234-56-7838
39 Peterson          Bob                234-56-7839
40 Parke             Bob                234-56-7840
41 Wadsworth         Bob                234-56-7841
42 Anthony           John               234-56-7842
43 Thomas            John               234-56-7843
44 Smith             John               234-56-7844
45 Jones            John               234-56-7845
46 Craven           John               234-56-7846

47 record(s) selected.

db2 => quit
DB200001 The QUIT command completed successfully.
[db2inst2@osprey ~]$ exit

```

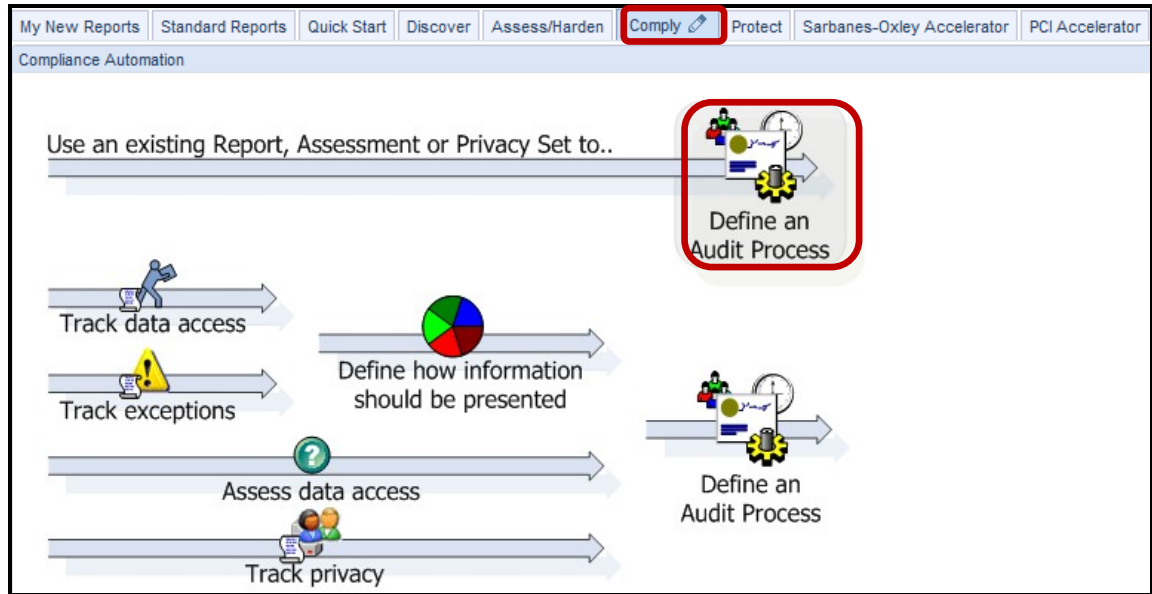
- f. From the IBM InfoSphere Guardium GUI, verify that both *Shared Memory* and *TCP SQL* are being captured. Click '**-Activity Report**' under the **My New Reports** tab.

Timestamp	Server Type	Server IP	Client IP	Network Protocol	DB User Name	Full Sql
2012-02-01 14:56:04.0DB2	DB2	10.10.9.56	10.10.9.56	TCP	DB2INST2	N/A
2012-02-01 14:55:49.0DB2	DB2	10.10.9.56	10.10.9.56	TCP	DB2INST2	SET CURRENT LOCALE LC_CTYPE = 'en_US'
2012-02-01 14:55:49.0DB2	DB2	10.10.9.56	10.10.9.56	TCP	DB2INST2	select * from ssn
2012-02-01 14:55:49.0DB2	DB2	10.10.9.56	10.10.9.56	TCP	DB2INST2	CALL SQLCZP0A
2012-02-01 14:55:45.0DB2	DB2	10.10.9.56	10.10.9.56	TCP	DB2INST2	N/A
2012-02-01 14:55:41.0DB2	DB2	10.10.9.56	10.10.9.56	SHARED MEMORY	DB2INST2	N/A
2012-02-01 14:55:24.0DB2	DB2	10.10.9.56	10.10.9.56	SHARED MEMORY	DB2INST2	select * from ssn
2012-02-01 14:55:24.0DB2	DB2	10.10.9.56	10.10.9.56	SHARED MEMORY	DB2INST2	CALL SQLCZP0A
2012-02-01 14:55:19.0DB2	DB2	10.10.9.56	10.10.9.56	SHARED MEMORY	DB2INST2	SET CURRENT LOCALE LC_CTYPE = 'en_US'
2012-02-01 14:55:18.0DB2	DB2	10.10.9.56	10.10.9.56	SHARED MEMORY	DB2INST2	N/A
2012-02-01 14:11:15.0ORACLE	ORACLE	10.10.9.56	10.10.9.56	BEQUEATH	SYSTEM	N/A
2012-02-01 14:11:10.0ORACLE	ORACLE	10.10.9.56	10.10.9.56	BEQUEATH	SYSTEM	select * from dba_users
2012-02-01 14:11:05.0ORACLE	ORACLE	10.10.9.56	10.10.9.56	BEQUEATH	SYSTEM	BEGIN DBMS_APPLICATION_INFO.SET_MODULE(:1,NULL); END;
2012-02-01 14:11:05.0ORACLE	ORACLE	10.10.9.56	10.10.9.56	BEQUEATH	SYSTEM	BEGIN DBMS_APPLICATION_INFO.SET_MODULE('SQL*Plus',NULL); END;
2012-02-01 14:11:05.0ORACLE	ORACLE	10.10.9.56	10.10.9.56	BEQUEATH	SYSTEM	SELECT DECODE('A','A','1','2') FROM DUAL
2012-02-01 14:11:05.0ORACLE	ORACLE	10.10.9.56	10.10.9.56	BEQUEATH	SYSTEM	COMMIT
2012-02-01 14:11:05.0ORACLE	ORACLE	10.10.9.56	10.10.9.56	BEQUEATH	SYSTEM	COMMIT
2012-02-01 14:11:01.0ORACLE	ORACLE	10.10.9.56	10.10.9.56	BEQUEATH	SYSTEM	N/A
2012-02-01 14:11:01.0ORACLE	ORACLE	10.10.9.56	10.10.9.56	BEQUEATH	SYSTEM	SELECT USER FROM DUAL
2012-02-01 14:11:01.0ORACLE	ORACLE	10.10.9.56	10.10.9.56	BEQUEATH	SYSTEM	BEGIN DBMS_OUTPUT.DISABLE; END;

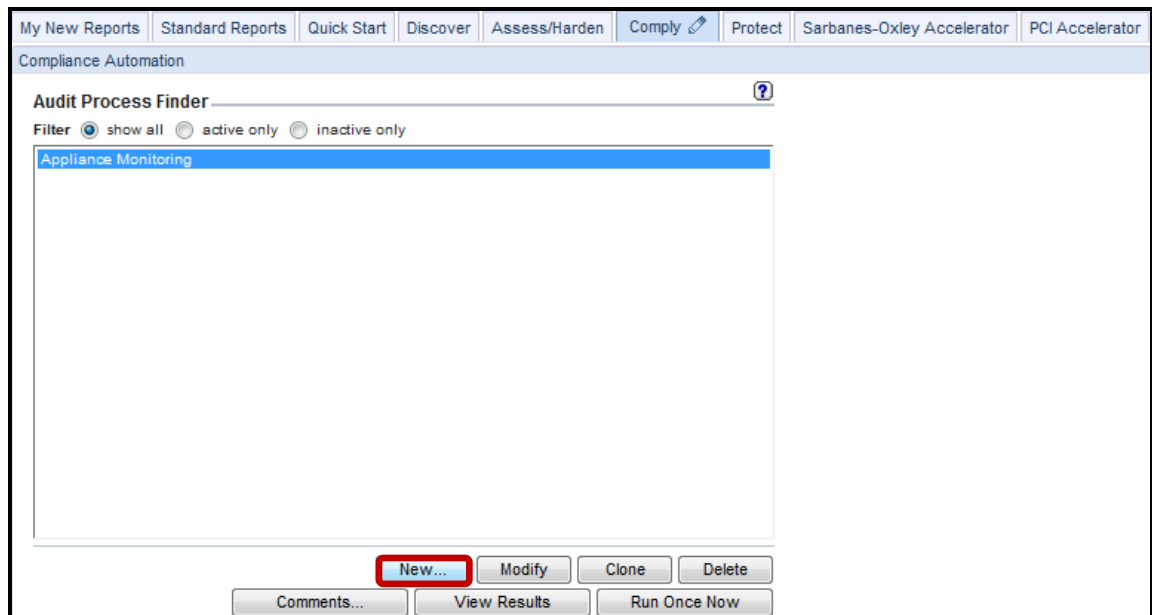
Note: The logged SQL statement from your query will appear in the **Full_Sql** column along with additional details captured at the time that the SQL statement was executed.

___4. Finally, use Compliance Workflow Automation (more detail to come in a subsequent lab) to automate the process of adding new Inspection Engines whenever new database instances are discovered.

___a. Click **Define an Audit Process** under the **Comply** tab.



___b. Click **New**.



- c. Enter 'V8 PoT Inspection Engines for new instances' for the Audit Process Definition Description, enter 'Discovered Instances' for the Audit Tasks Description in the lower section of the dialog, and click 'Report' for the Task Type.

The screenshot displays the 'Compliance Automation' interface. At the top, there are navigation tabs: 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. The main section is titled 'Audit Process Definition'. The 'Description' field contains the text 'V8 PoT Inspection Engines for new inst.'. Below this, there are options for 'Active' (unchecked), 'Archive Results' (unchecked), and 'Keep for a minimum of' (0 days or 5 runs). There is also a 'CSV/CEF File Label' field and a checked 'Zip CSV for mail' option. An 'Email Subject' field is present. Buttons for 'View', 'Run Once Now', and 'Modify Schedule...' are located below the email subject field. The 'Receiver Table' section has columns for 'Receiver', 'Action Req.', 'To-Do List', 'Email Notif.', 'Cont.', and 'Appv. if Empty'. Below the table is an 'Add Receiver' section with a 'Receiver name' dropdown, a 'Search users' button, and radio buttons for 'Action Required' (Review, Sign), 'To-Do List' (Add), 'Email Notification' (None, Link Only, Full Results), 'Continuous' (checked), and 'Approve if Empty' (Yes). An 'Add' button is at the bottom right of this section. The 'Audit Tasks' section features an 'Add New Task' dialog box. The 'Description' field in the dialog contains 'Discovered Instances', and the 'Task Type' is set to 'Report'. Other task types include 'Security Assessment', 'Entity Audit Trail', 'Privacy Set', and 'Classification Process'. An 'Apply' button is at the bottom right of the dialog. Below the dialog is an 'Add Audit Task' button. The 'Roles' section shows 'No roles have been assigned to this Process' and a 'Roles...' button. At the bottom of the interface are buttons for 'Refresh', 'Delete', 'Clone', 'Apply', and 'Back'.

- __d. Select '**Discovered Instances**' from the Report dropdown list, '**create_stap_inspection_engine**' from the API for automatic execution dropdown list, enter '**now -1 day**' for Period From, '**now**' for Period To, and then click **Apply**.

Audit Tasks
 Report: Discovered Instances [Discovered Instances]

Description: Discovered Instances

Task Type: Report Security Assessment Entity Audit Trail Privacy Set Classification Process

Report

Report: **Discovered Instances**

CSV/CEF File Label: Discovered_Instances

Export CSV file:
 Export CEF file:
 Export PDF file:
 Write to Syslog:
 Compress:
 PDF Content: Report Diff Report and Diff

API for automatic execution: **create_stap_inspection_engine**

Task Parameters

* On aggregators, only reports not exceeding the maximum merge period will be executed.

Enter Period From: **now -1 day**
 Enter Period To: **now**

Show Aliases: On Off Default

Remote Data Source: -- none --

Apply

Add Audit Task

- __e. Check the '**Active**' checkbox.

Audit Process Builder

Audit Process Definition

Description: V8 PoT Inspection Engines for new inst

Active: There is no schedule associated with this process

Archive Results:

Keep for a minimum of 0 days or 5 runs

CSV/CEF File Label: V8_PoT_Inspection_E Zip CSV for mail

Email Subject:

View Run Once Now Modify Schedule...

- __f. Click **Apply** at the bottom of the dialog to apply the Audit Process, and then **Back** to return to the main Audit Process Builder screen.

Roles

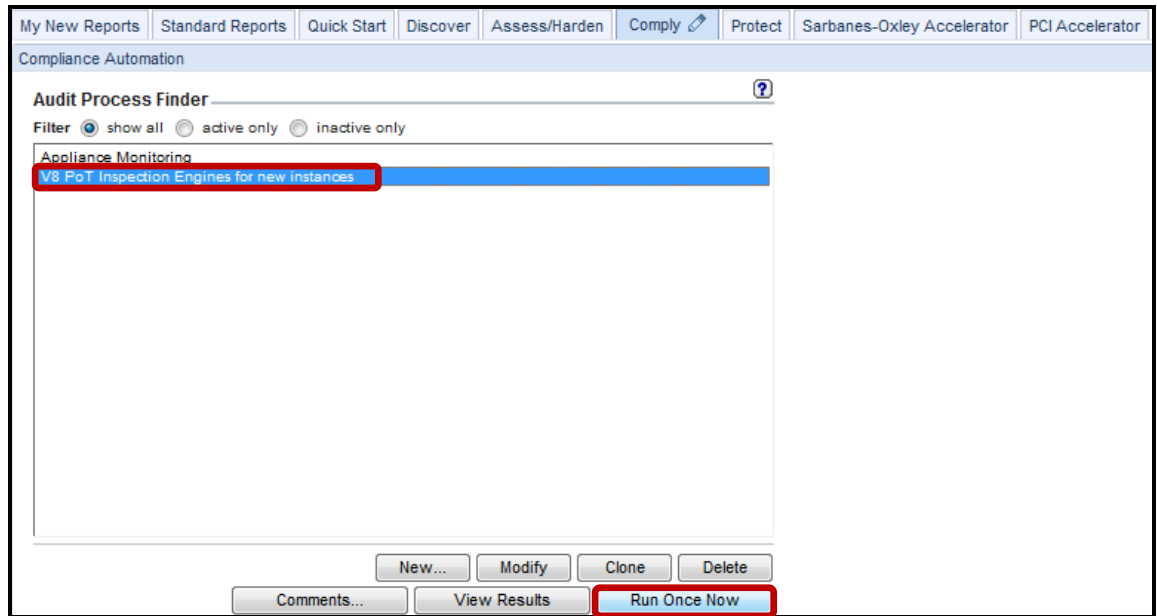
No roles have been assigned to this Process

Roles...

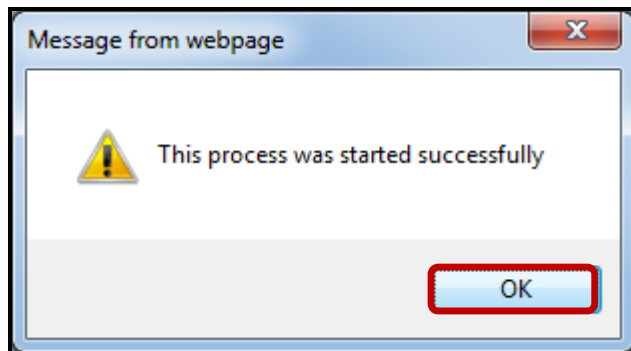
Delete Clone

Refresh **Apply** **Back**

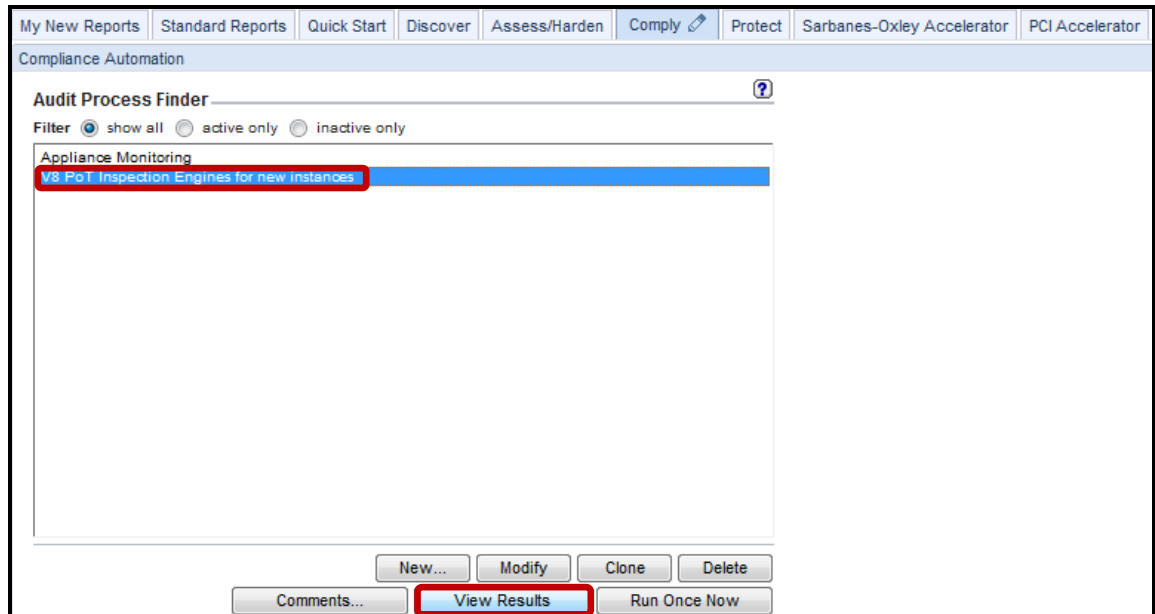
- __g. Select '**V8 PoT Inspection Engines for new instances**' and click **Run Once Now** to execute the new Audit Process.



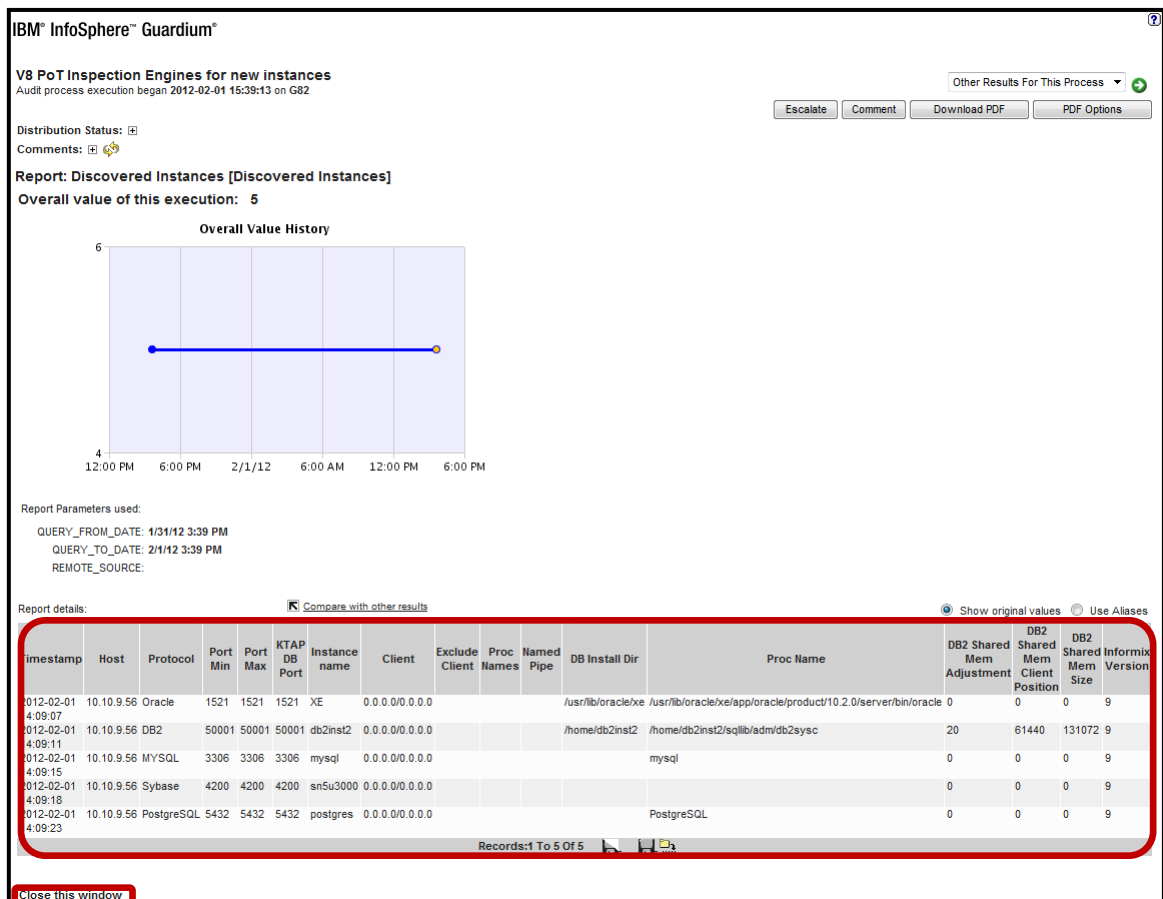
- __h. Click **OK** to acknowledge the process has started successfully.



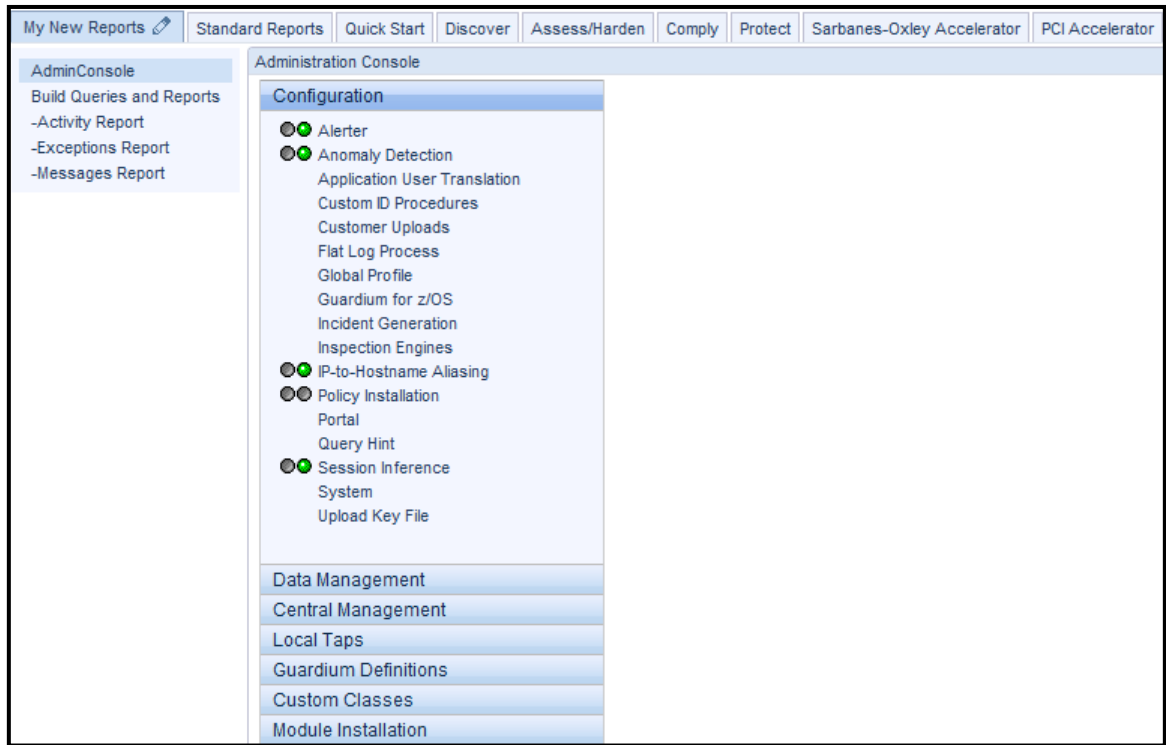
i. Click **View Results** to display the results of the Audit Process.



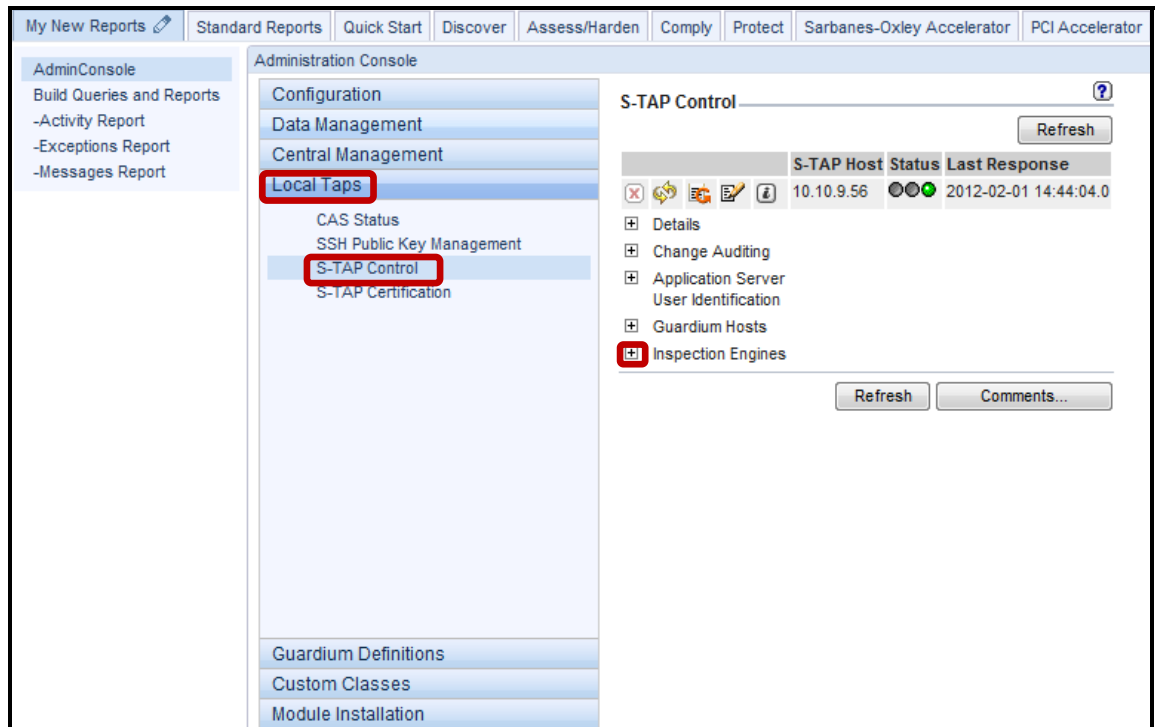
j. As expected, we see identical result as with the Discovered Instances report we ran earlier during this lab. Click **Close this window** at the bottom left when finished.



__k. Once again, click **AdminConsole** under the **My New Reports** tab.



__l. Click **S-TAP Control** under the **Local Taps** tab.



- __m. Click the '+' icon alongside **Inspection Engines**, and scroll down to the bottom to reveal the newly added inspection engines for MySQL, Sybase, and PostgreSQL.

Protocol	Port Range	KTAP DB Real Port
Mysql	3306-3306	3306
Ip	Mask	
0.0.0.0	0.0.0.0	
DB Install Dir	Process Name	
NULL	mysql	
Intercept Types		
NULL		
Protocol	Port Range	KTAP DB Real Port
Sybase	4200-4200	4200
Ip	Mask	
0.0.0.0	0.0.0.0	
DB Install Dir	Process Name	
NULL	NULL	
Intercept Types		
NULL		
Protocol	Port Range	KTAP DB Real Port
PostgreSQL	5432-5432	5432
Ip	Mask	
0.0.0.0	0.0.0.0	
DB Install Dir	Process Name	
NULL	PostgreSQL	
Intercept Types		
NULL		

Thank You

4.4 Automatic Client Upgrade (No Reboot Required)

Overview

The purpose of Guardium Installation Manager (GIM) is to provide an automatic installation capability for Guardium modules such as S-TAP and KTAP. Every database server can periodically check the Guardium appliance for new versions updates. Upon finding a new release the installer agent running on the Guardium appliance (GIM server) shall retrieve the new version software, either from its local database or by fetching it from a remote Central Manager machine, and sending it to the installer client (GIM Client) on the database server.

InfoSphere Guardium provides the capability to upgrade S-TAP version across the enterprise without impact to production services.

Objectives

This lab will demonstrate the ease with which the IBM InfoSphere Guardium solution can be upgraded in an enterprise environment. The lab will focus on upgrading the S-TAP software probe from the Guardium Installation Manager GUI.

The following steps will guide us through the lab:

- __1. Upgrade the IBM InfoSphere Guardium lightweight software probe (STAP)
- __2. Use the browser-based interface to validate a successful installation

CRITICAL NOTE: THIS LAB REQUIRES THE SUCCESSFUL COMPLETION OF LAB SECTION 4.2.

- __1. Launch the InfoSphere Guardium GUI to verify the GIM client software installation performed during a previous lab section.
 - __a. Login as user **pot** / **guardium**.

Login

Please enter your information

User name:

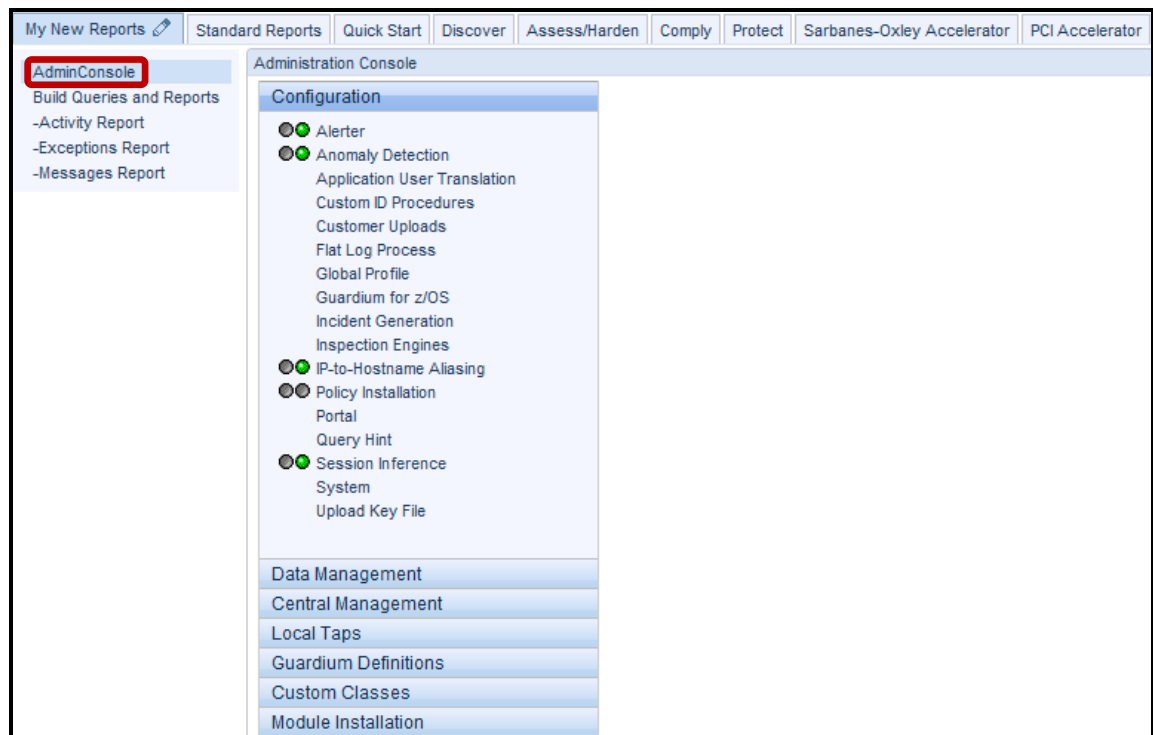
Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

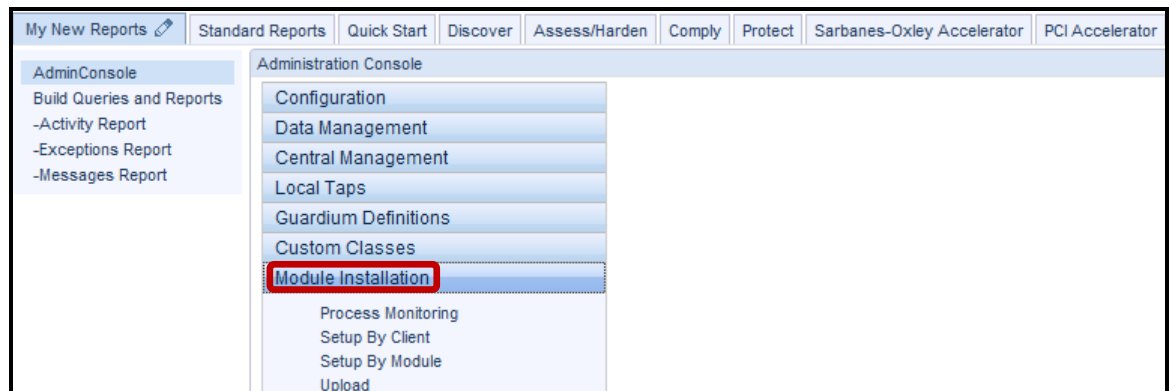
Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistry/key © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com, Zthread © Copyright 2000-2003, Eric Crahen.

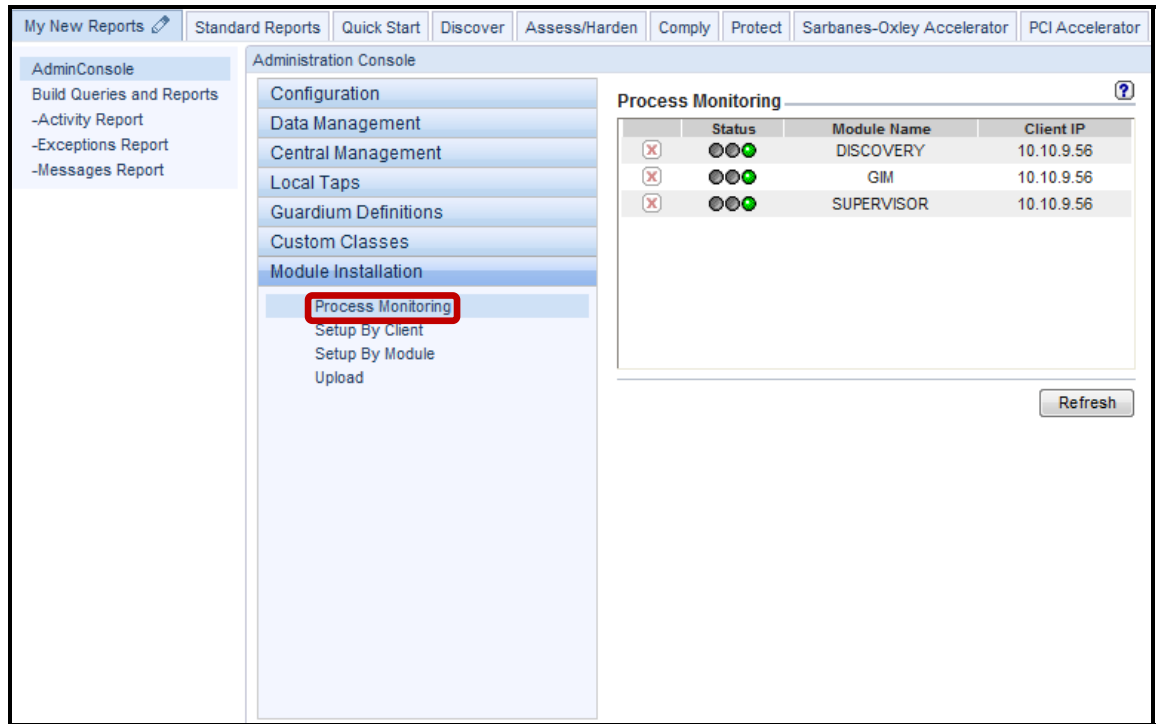
- __b. Verify GIM process communication.
- __c. Click **Admin Console** under the **My New Reports** tab.



- __d. Click **Module Installation**.



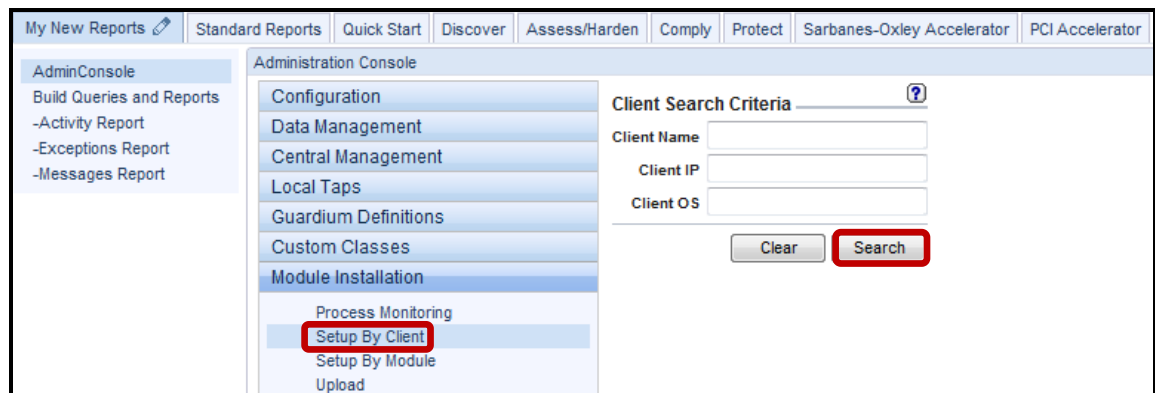
__e. Click **Process Monitoring** under the **Module Installation** tab.



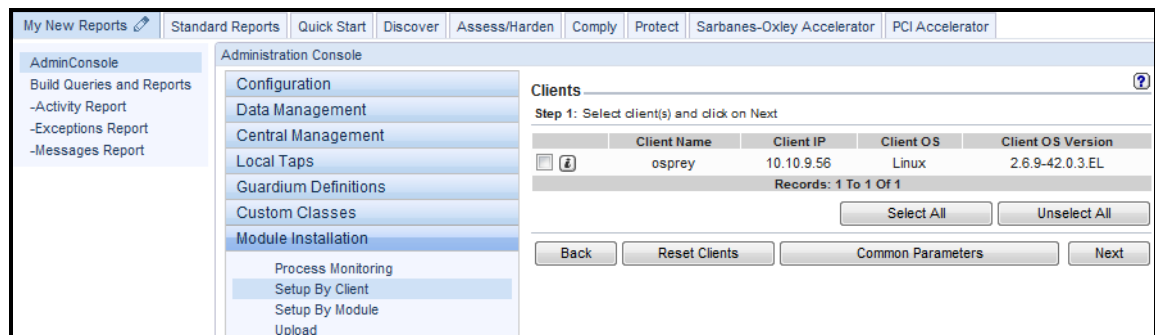
The green status lights should appear for 'DISCOVERY', 'GIM', and 'SUPERVISOR' modules which are now running on the database server. A corresponding pair of 'DISCOVERY', 'GIM', and 'SUPERVISOR' processes will appear for each client IP being managed by GIM.

__2. S-TAP Upgrade using GIM.

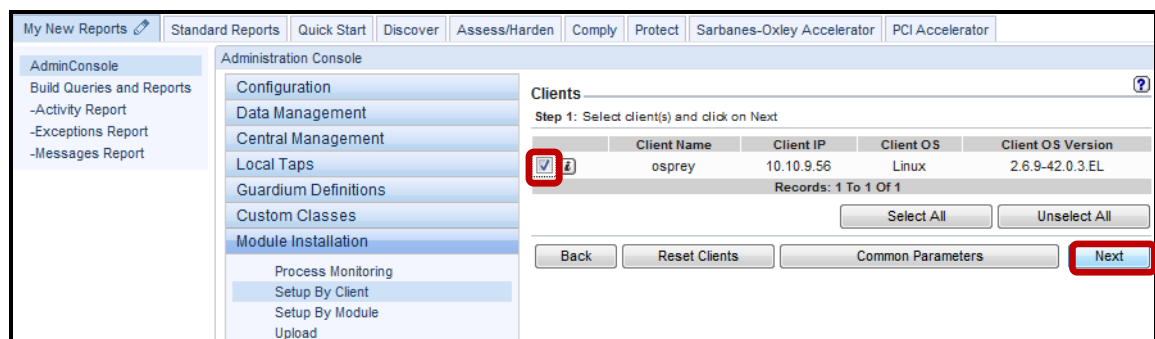
__a. Click **Setup By Client** under the **Module Installation** tab, and click **Search**.



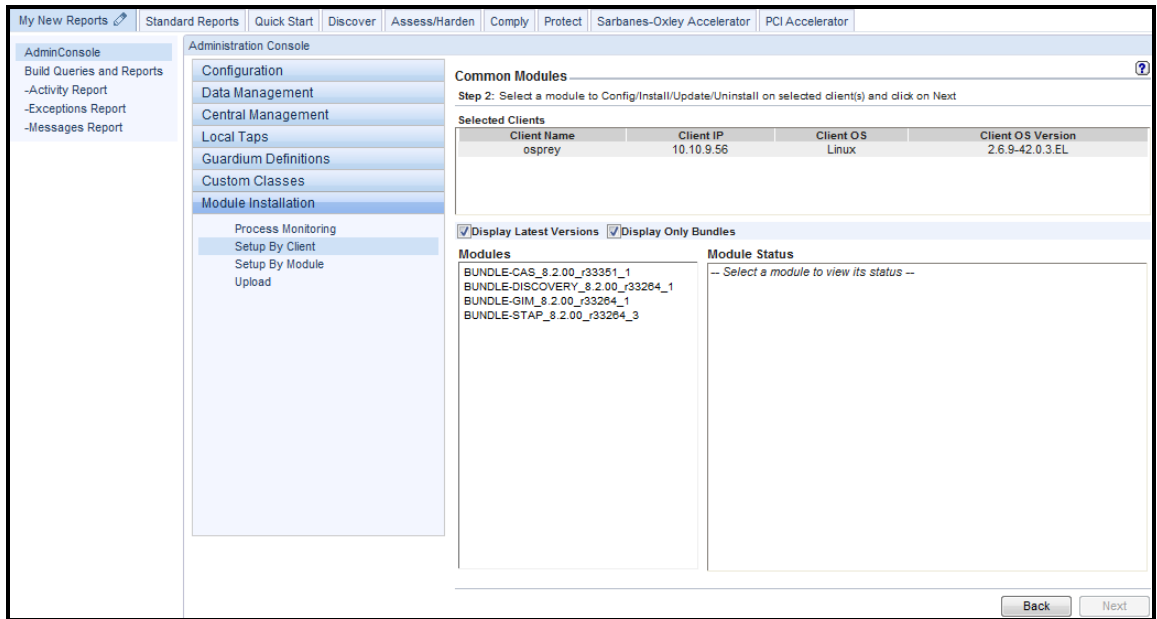
A list of available GIM clients will display.



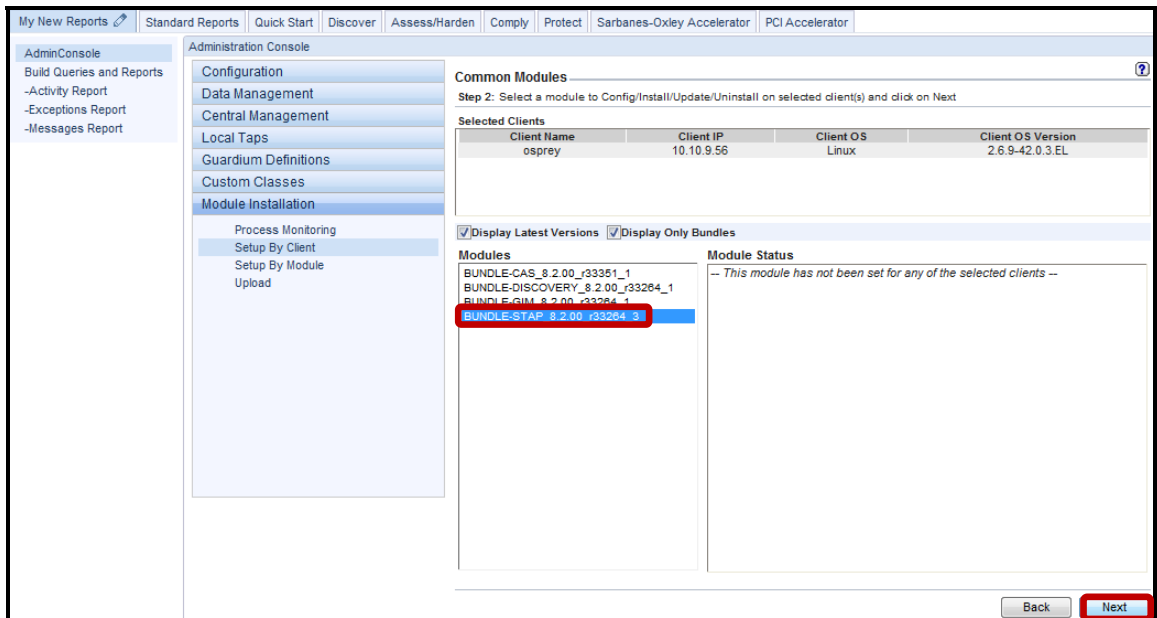
__b. Check the left-hand checkbox, and click **Next**.



A list of uploaded modules currently available for the targeted platform(s) will appear.



 c. Select **BUNDLE-STAP_8.2.00_r33264_3**, and click **Next**.



A Module Parameters screen will appear enabling the configuration of a variety of properties before Installing new software or Updating existing software installations.

The screenshot displays the 'Module Parameters' configuration interface. The top navigation bar includes options like 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. The left sidebar shows the 'Administration Console' with a tree view including 'Configuration', 'Data Management', 'Central Management', 'Local Taps', 'Guardium Definitions', 'Custom Classes', and 'Module Installation'. The main area is titled 'Module Parameters' and shows 'Step 3: Config/Install/Update/Uninstall BUNDLE-STAP'. It features two sections: 'Common Module Parameters' with a grid of toggle switches for parameters like ATAP_ENABLED, KTAP_DEBUG, STAP_ENABLED, and TEE_DEBUG; and 'Client Module Parameters' which is a table with the following data:

Client Name	Possible Actions	ATAP_DISKSPACE	ATAP_ENABLED	ATAP_PACKAGE	ATAP_PART_OF_BUNDLE	ATAP_SYMVERSION	ATAP_VERSION
osprey	INSTALL	20000	1	guard-A.TAP-v82_r33204_1-rhel-4-linux-i686.tar.gz	BUNDLE-STAP	v82_r33204_1	8.2.00_r33204

At the bottom of the screen, there are buttons for 'Install/Update', 'Cancel Install/Update', 'Uninstall', and 'Cancel Uninstall', along with 'Back', 'Revert', and 'Apply to Clients' buttons.

- d. Scroll to the right until the golden **KTAP_LIVE_UPDATE** box appears which indicates that a property value must be provided before the installation can proceed.

Hover over any of the property boxes to see details on valid values. A property content dialog can also be accessed by clicking on the pencil and paper icon alongside some the property boxes.

The screenshot shows the 'Module Parameters' configuration page for 'BUNDLE-STAP'. The 'Common Module Parameters' section contains various properties like ATAP_ENABLED, STAP_DEBUG, and KTAP_LIVE_UPDATE. The 'Client Module Parameters' table below has a red highlight on the 'KTAP_LIVE_UPDATE' column for the first row. A tooltip is displayed over the table, containing the text: '[Nn] - KTAP upgrade requires system reboot. [Yy] - KTAP upgrade does not require system reboot'.

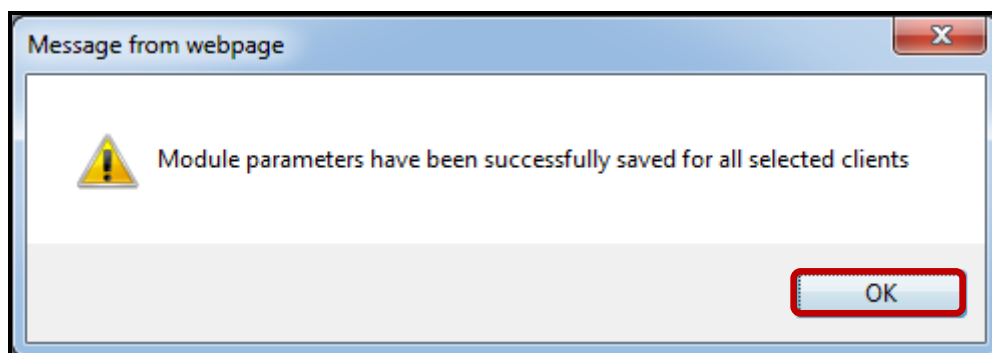
CLIENTS_VERSION	KTAP_DEBUG	KTAP_DISKSPACE	KTAP_ENABLED	KTAP_LIVE_UPDATE	KTAP_NO_ROLLBACK	KTAP_PACKAGE	KTAP
28888_1	0	20000	1			guard-KTAP-v81_28888_4-4hel-4-linux-i888.tar.gz	BUND

- __e. **Critical Step** – Enter 'y' for KTAP_LIVE_UPDATE, and scroll to the right to change the value for STAP_FIREWALL_INSTALLED from '0' to '1'. Click **Apply to Clients** to specify that a KTAP upgrade does not require a system reboot, and to enable S-GATE Blocking.

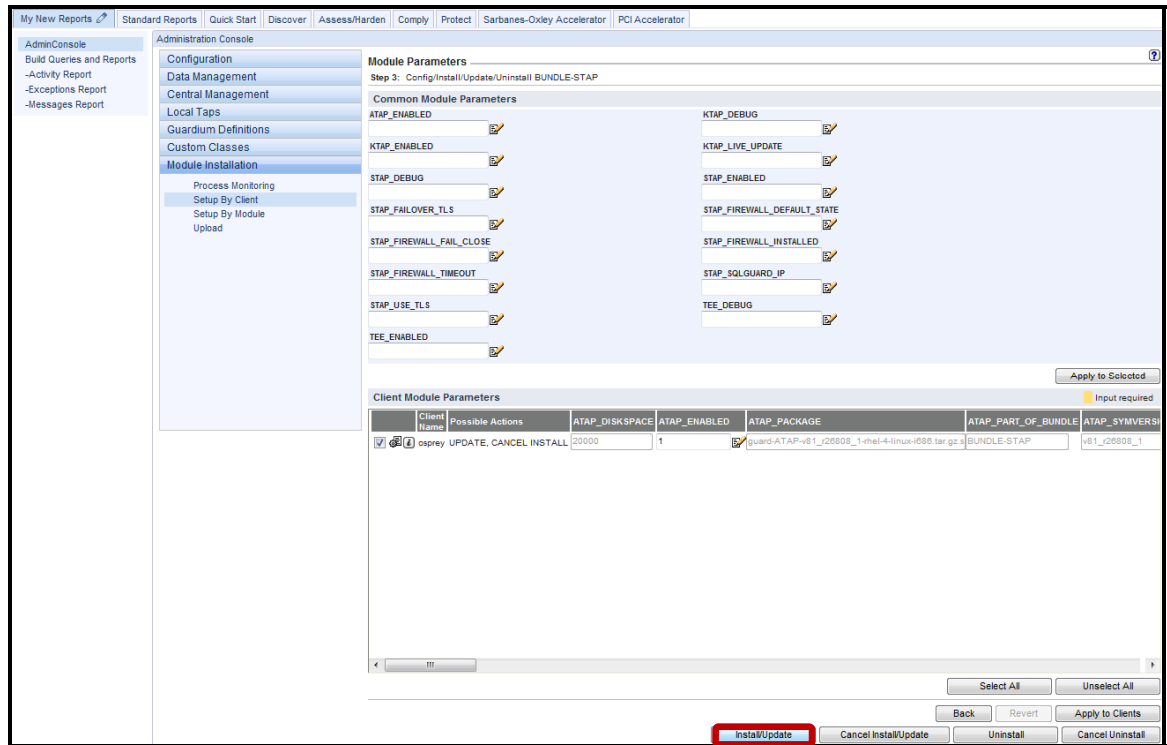
Note: This is the same location to set additional properties. We are enabling the S-GATE Blocking feature here since it will be required in a later lab section.

The screenshot shows the Administration Console interface for configuring module parameters. The left sidebar contains navigation options like AdminConsole, Build Queries and Reports, and Module Installation. The main area is titled 'Module Parameters' and shows a configuration step for 'Config/Install/Update/Uninstall BUNDLE-STAP'. Under 'Common Module Parameters', various settings are listed, including KTAP_ENABLED, STAP_DEBUG, and STAP_FIREWALL_INSTALLED. The 'Apply to Clients' button is highlighted with a red box. Below the parameters is a table for 'Client Module Parameters' with columns for CLIENTS_VERSION, KTAP_DEBUG, KTAP_DISKSPACE, KTAP_ENABLED, KTAP_LIVE_UPDATE, KTAP_NO_ROLLBACK, and KTAP_PACKAGE. The 'Apply to Clients' button is also highlighted with a red box at the bottom right of the console.

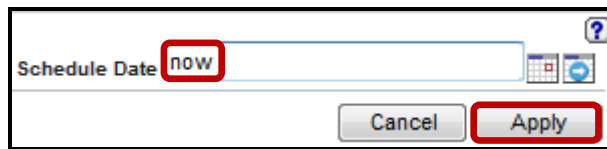
- __f. Click **OK** to acknowledge.



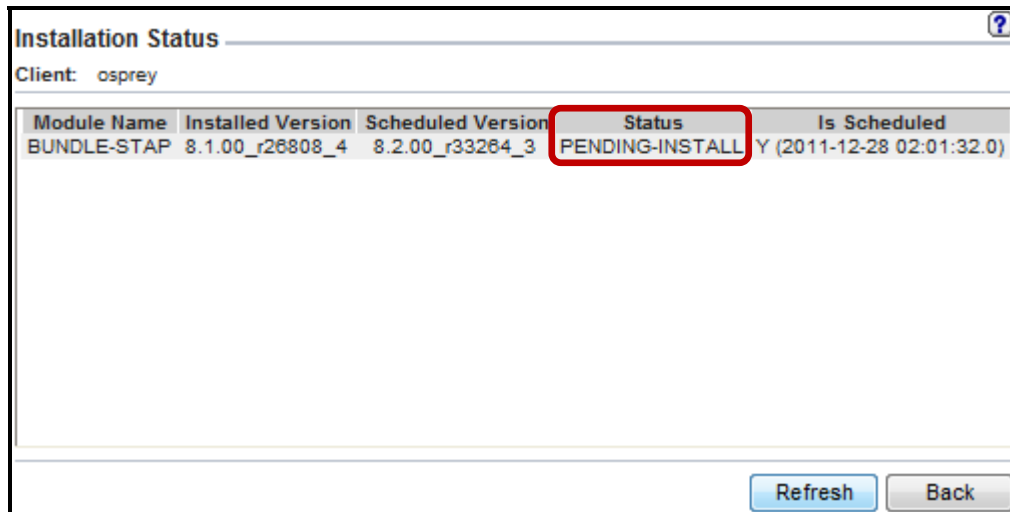
__g. Click **Install/Update**.



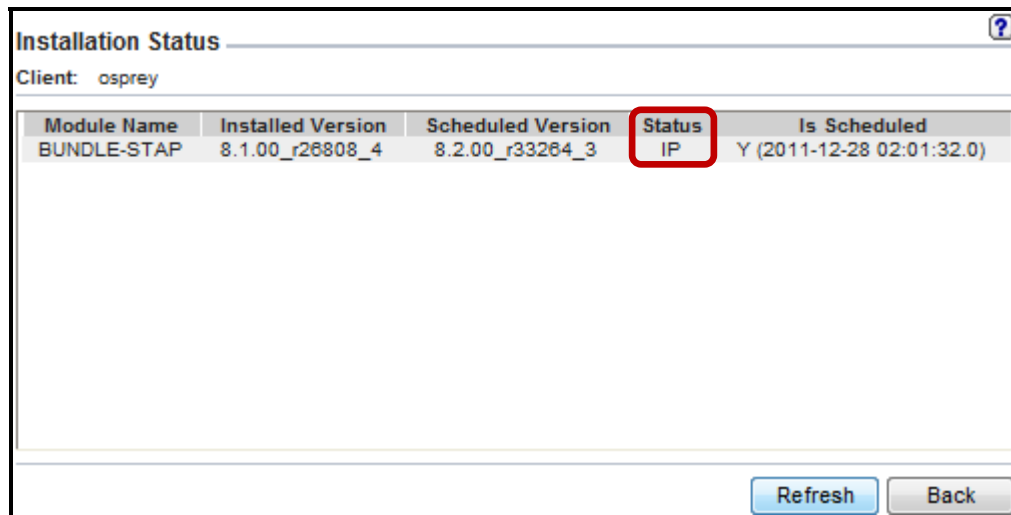
__h. Enter '**now**' for the Schedule Date, and click **Apply**.



__i. Click on the  icon to check the status of the installation.



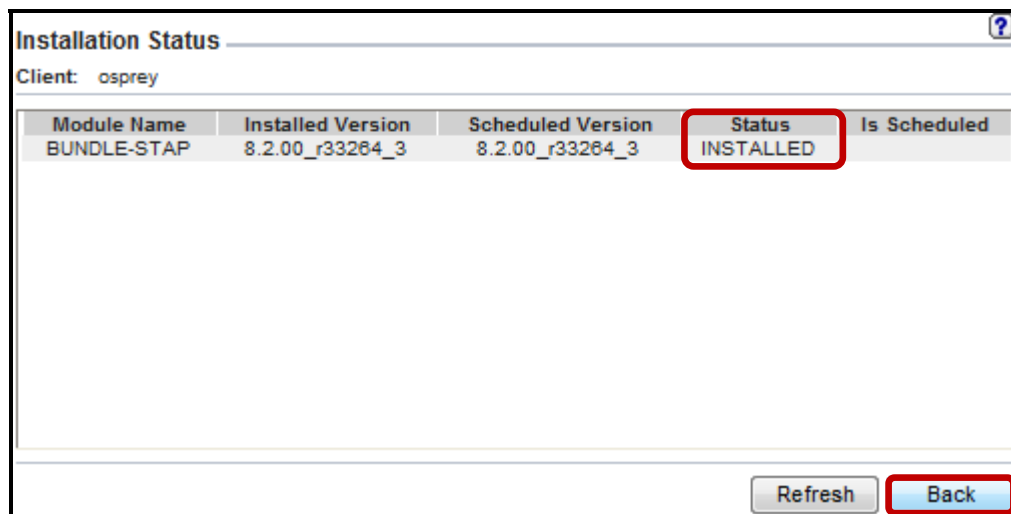
“IP” indicates that the installation is “In Progress”.



The screenshot shows a window titled "Installation Status" with a help icon in the top right corner. Below the title bar, it says "Client: osprey". A table displays the installation details for the BUNDLE-STAP module. The "Status" column is highlighted with a red box and contains the value "IP". At the bottom right, there are "Refresh" and "Back" buttons.

Module Name	Installed Version	Scheduled Version	Status	Is Scheduled
BUNDLE-STAP	8.1.00_r26808_4	8.2.00_r33264_3	IP	Y (2011-12-28 02:01:32.0)

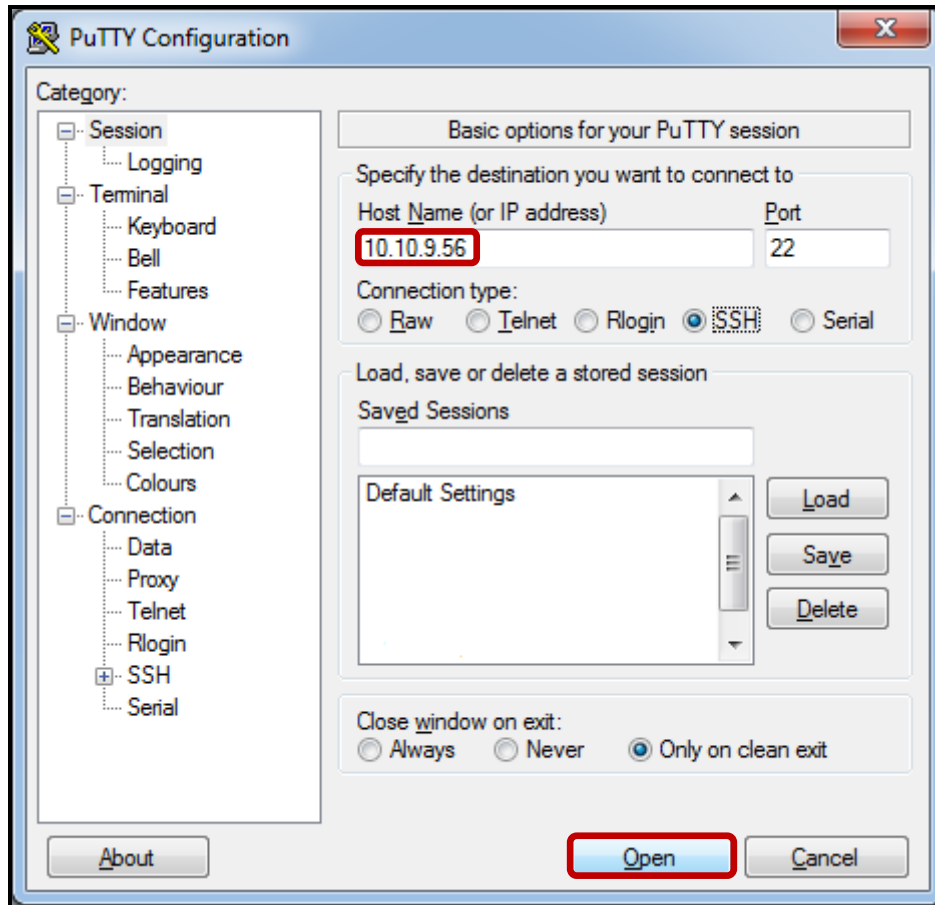
- __j. Once the installation has completed successfully, click **Back** to return to the **Module Parameters** screen.



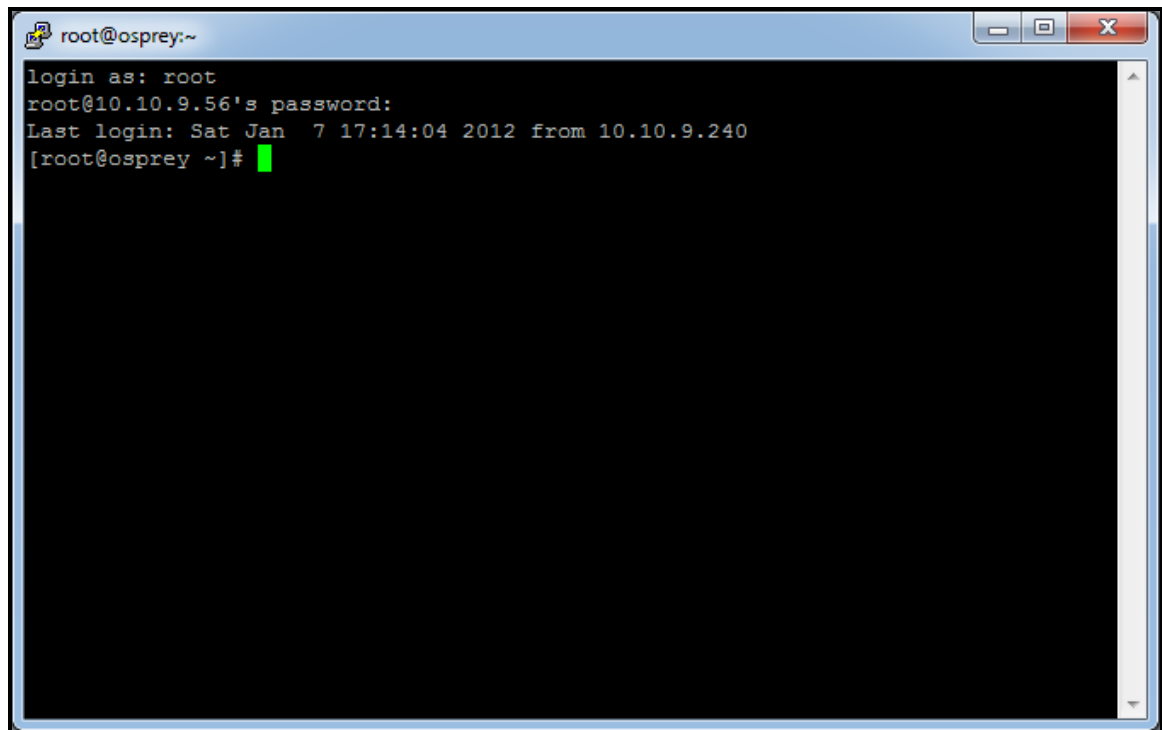
The screenshot shows the same "Installation Status" window. The "Status" column is now highlighted with a red box and contains the value "INSTALLED". The "Back" button at the bottom right is also highlighted with a red box. The "Refresh" button remains visible.

Module Name	Installed Version	Scheduled Version	Status	Is Scheduled
BUNDLE-STAP	8.2.00_r33264_3	8.2.00_r33264_3	INSTALLED	

- __3. Using a PuTTY SSH client, access the VM database server to verify the ease with which the IBM InfoSphere™ Guardium® solution has been automatically upgraded.
 - __a. Start the PuTTY SSH client login.
 - __b. From your laptop, launch PuTTY, enter **10.10.9.56**, and click **Open**.

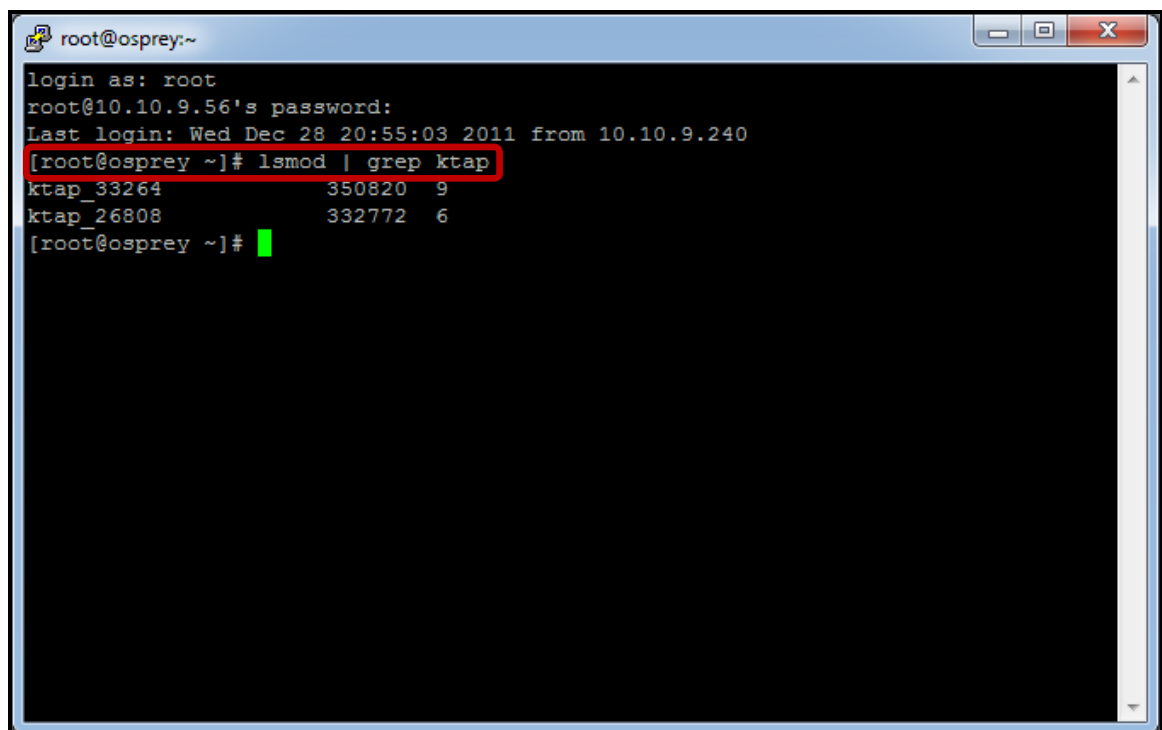


- __c. Login as **root** / **guardium**. After logging in, the following prompt will be displayed.



```
root@osprey:~  
login as: root  
root@10.10.9.56's password:  
Last login: Sat Jan 7 17:14:04 2012 from 10.10.9.240  
[root@osprey ~]#
```

- __d. Type **lsmod | grep ktap** to get a list of currently loaded KTAP module files. The previously loaded KTAP (ktap_26808) is now inactive. Once the database server is rebooted, this kernel module will be removed.



```
root@osprey:~  
login as: root  
root@10.10.9.56's password:  
Last login: Wed Dec 28 20:55:03 2011 from 10.10.9.240  
[root@osprey ~]# lsmod | grep ktap  
ktap_33264          350820  9  
ktap_26808         332772  6  
[root@osprey ~]#
```

Thank You

Guardium Client Installation review

- __1. The S-TAP process runs on:
 - __a. The InfoSphere Guardium Collector
 - __b. The database server
 - __c. The client PC
- __2. CAS requires the S-TAP process.
(**True** or **False**)
- __3. The KTAP_LIVE_UPDATE parameter should be set up to:
 - __a. Database IP address
 - __b. Y or N
 - __c. Guardium IP address
 - __d. A and C
- __4. When installing CAS on a UNIX system, there are two requirements:
 - __a. Locate the JAVA_HOME directory, and determine the Java version.
 - __b. Locate the JAVA_HOME directory, and determine the Perl version
 - __c. Install Perl and locate C++ lib
- __5. What ports does CAS use to connect to Guardium?
 - __a. 16017 and 16019
 - __b. 16016 and 16018
 - __c. 8075 and 9500
- __6. S-TAP uses the “Inspection engines” setup from admin console.
(**True** or **False**)
- __7. Can S-TAP and CAS be managed from the Central manager?
 - __a. Yes
 - __b. No

- __8. Status of the S-TAP. One of the three lights will be illuminated:
- __a. Green, blue and black
 - __b. Green, red and orange
 - __c. Green, red and yellow
 - __d. White, red and green

Guardium Client Installation review (Answers)

__1. The S-TAP process runs on:

B – The database server.

__2. CAS requires the S-TAP process.
(True or False)

False.

__3. The KTAP_LIVE_UPDATE parameter should be set up to:

B – Y or N.

__4. When installing CAS on a UNIX system, there are two requirements:

A – Locate the JAVA_HOME directory, and determine the Java version.

__5. What ports does CAS use to connect to Guardium?

A – 16017 and 16019

__6. S-TAP uses the “Inspection engines” setup from the admin console.
(True or False)

False.

__7. Can S-TAP and CAS be managed from the Central manager?

B – No.

__8. Status of the S-TAP. One of the three lights will be illuminated:

C – Green, red, and yellow.

Lab 5 Custom Reports

5.1 Monitoring User ID Chain

Overview

InfoSphere Guardium's Chain UID feature provides the capability to identify multiple user IDs utilized during an access operation. Often when a privileged user accesses sensitive information, it is difficult to identify the actual user. With Chain UID, the actual user who first logged on to the operating system is easily identified so that an appropriate investigation can occur.

The UNIX command "su" (short for substitute user) is used to run the shell of another user without logging out. It is commonly used to change to root user permissions for administrative work without logging off and back on; it is also used to switch to other users in the same way. When invoked without a target user, the root user is assumed (identical to su root).

It is possible that this UNIX feature may be misused by a user trying to "cover his or her tracks" by logging in as one user, then switching to another user and connecting to a database. IBM InfoSphere Guardium recognizes this possible security threat and audits this activity completely.

Objectives

IBM InfoSphere Guardium continuously monitors the databases to reduce operational costs and simplify governance and compliance. This lab will demonstrate how to use the IBM InfoSphere Guardium GUI to create a simple UID Chaining Report using the following steps.

- __1. Open a browser and login to the IBM InfoSphere Guardium appliance.
- __2. Use track data access to define a query.
- __3. Generate a report.
- __4. Place the report on the InfoSphere Guardium GUI.
- __5. Customize the parameters of the report in the GUI.
- __6. View the report.

- __1. Using the IBM InfoSphere Guardium GUI, demonstrate the ease of use within the IBM InfoSphere Guardium solution. Start the IBM InfoSphere Guardium appliance and login.
 - __a. From your laptop, browse to <https://10.10.9.248:8443>
 - __b. Login as **pot /guardium**.

Login

Please enter your information

User name:

Password:

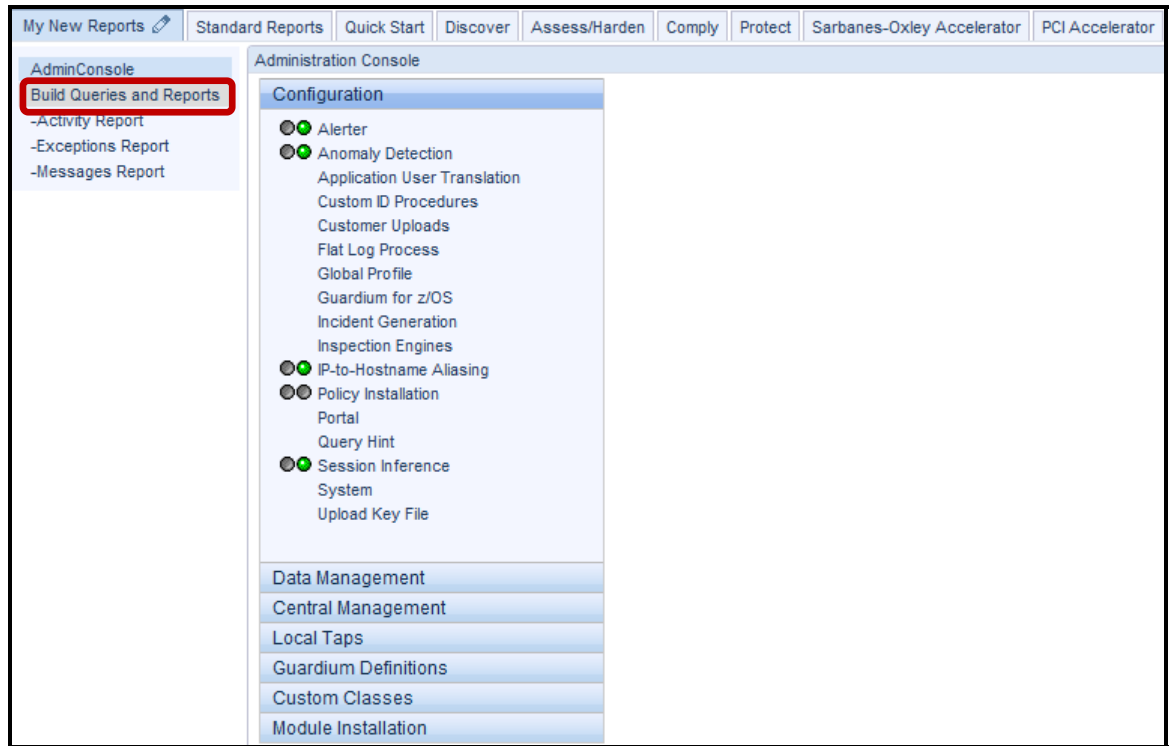
Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

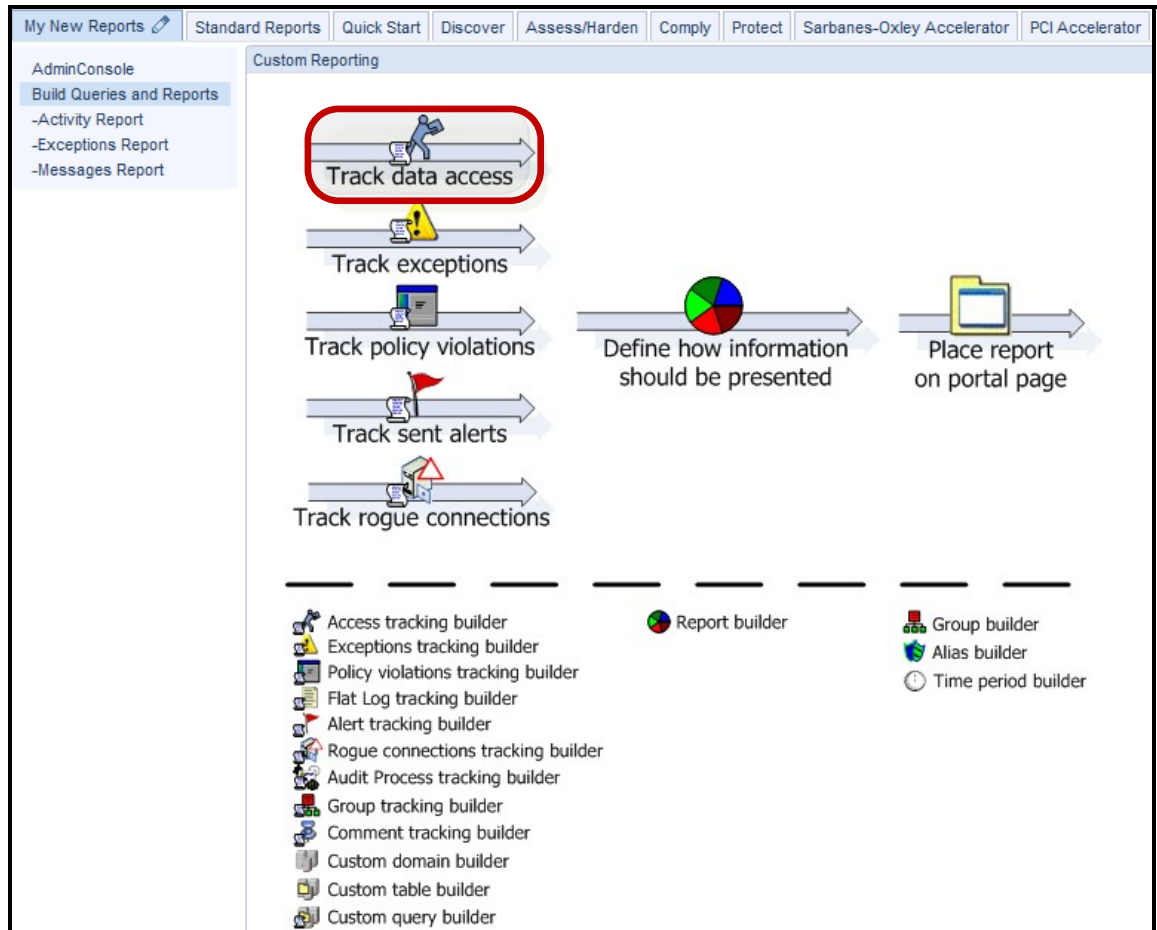
CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistrykey © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

__2. Use the IBM InfoSphere Guardium GUI to create a UID Chaining report.

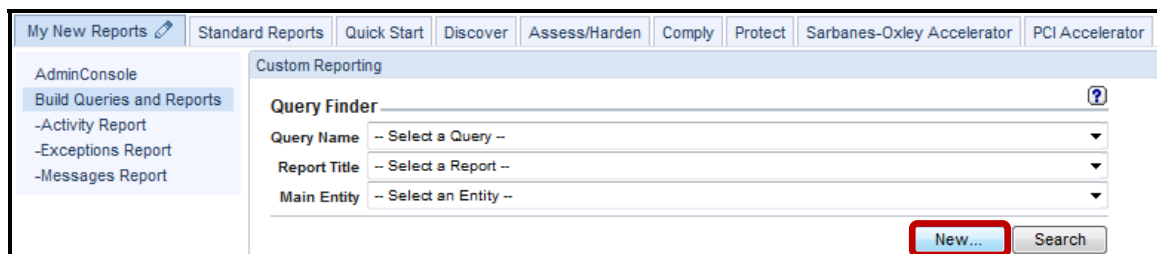
__a. Click **Build Queries and Reports** under the **My New Reports** tab.



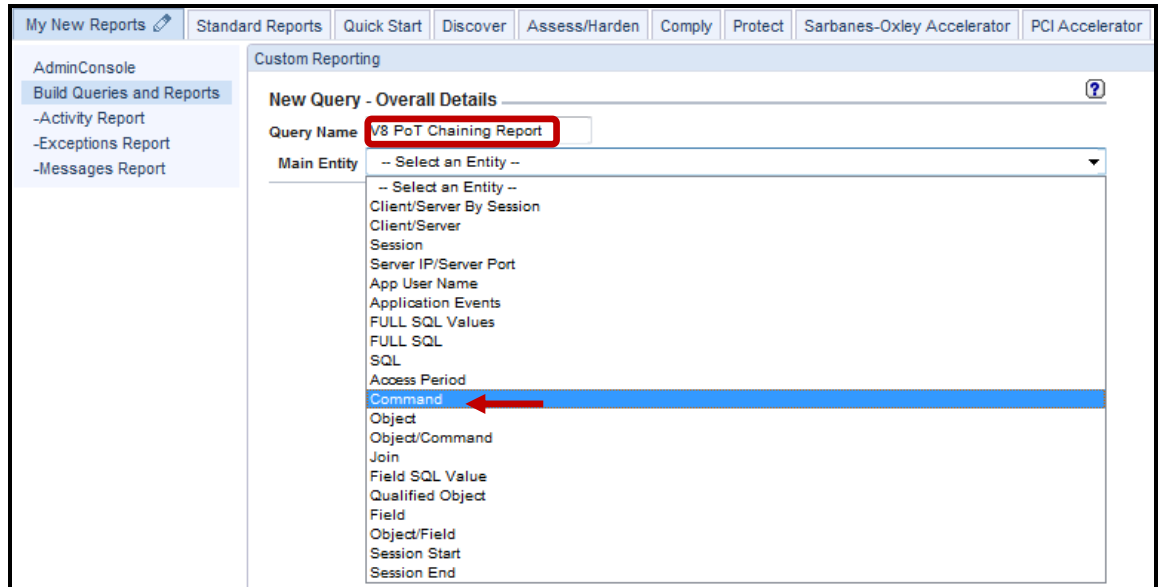
__b. Click **Track data access**.



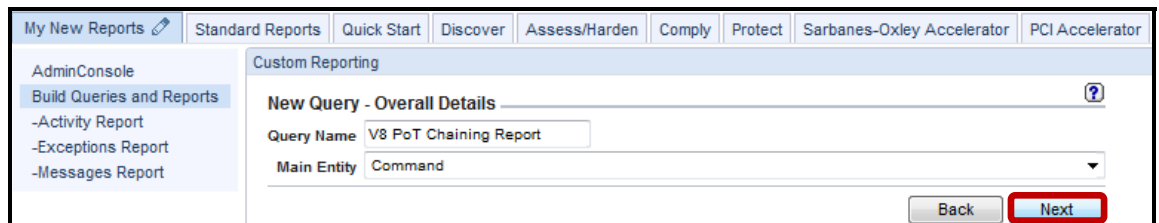
__c. Click **New**.



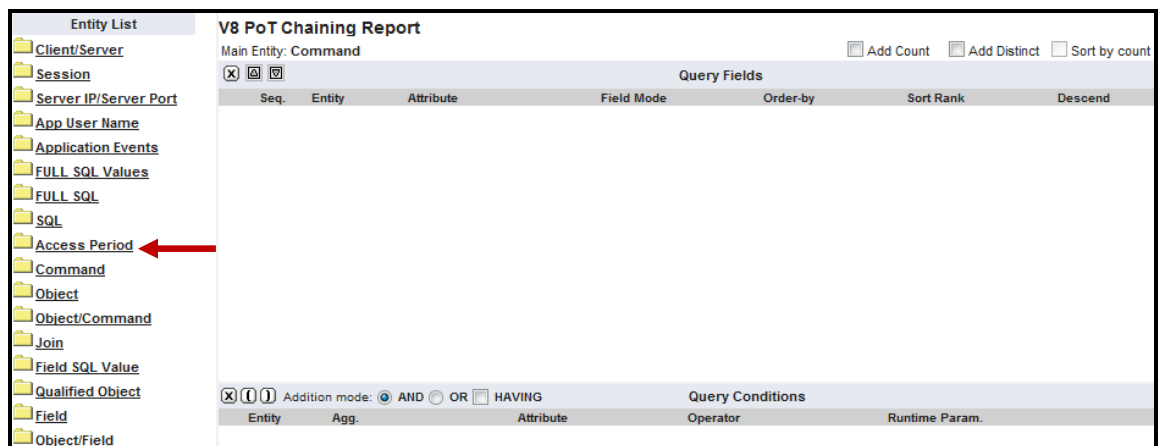
- d. Enter 'V8 PoT Chaining Report' for the *Query Name* and Select **Command** from the *Main Entity* dropdown.



- e. Click **Next**.

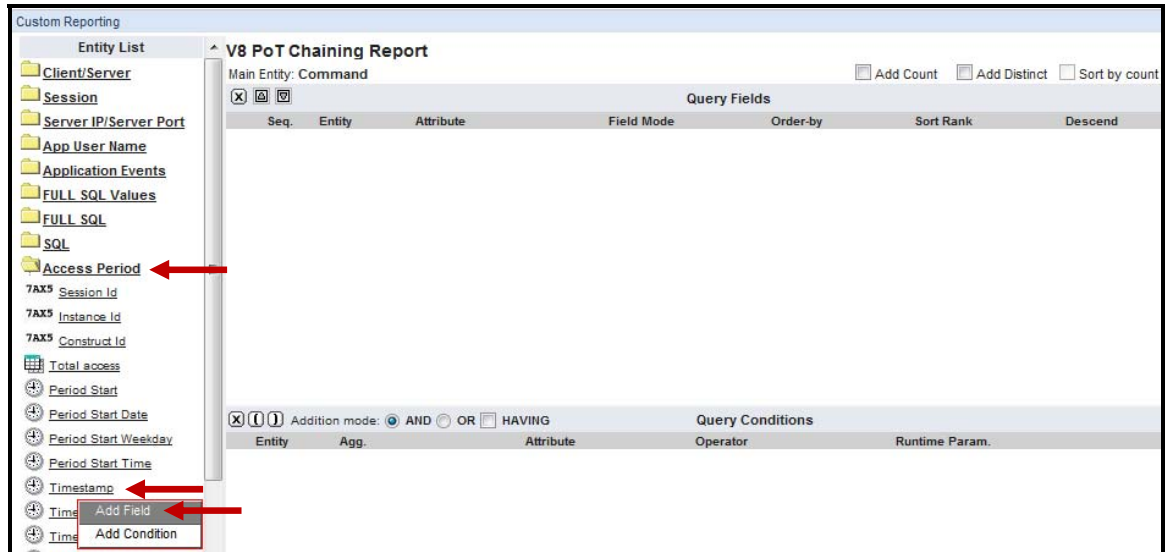


- f. Select **Access Period** from *Entity List*.



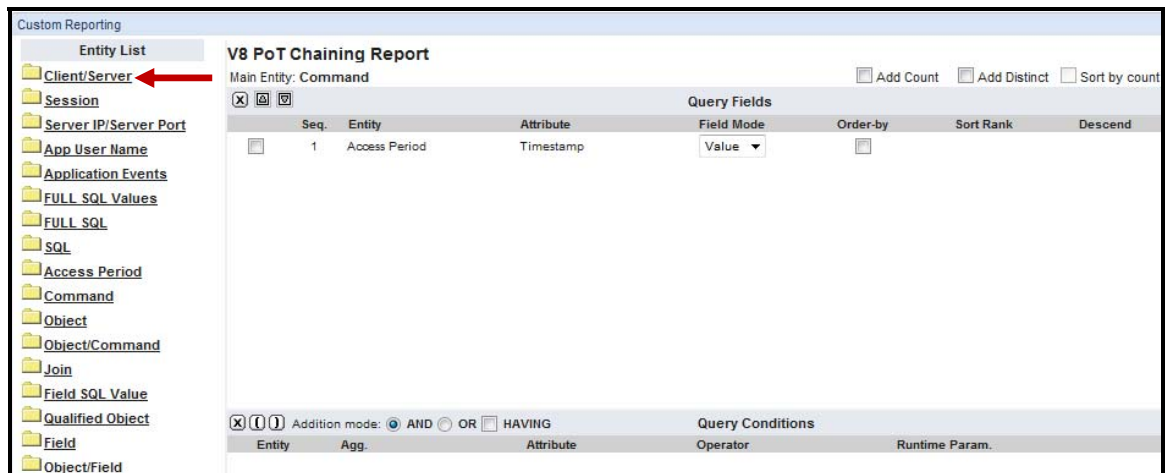
__3. The next few steps will add Custom *Query Fields* for the **V8 PoT Chaining Report**.

__a. Select the **Timestamp** attribute from *Access Period* entity and click **Add Field**. Then, select **Access Period** from the *Entity List* to collapse the **Access Period** folder.



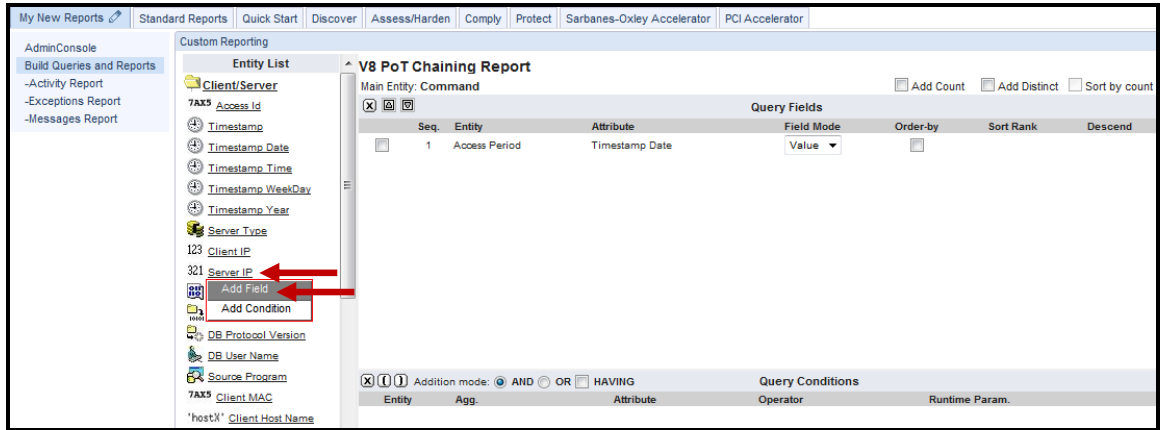
Note: The Timestamp attribute has now been added to the query window.

__b. Now select **Client/Server** from the *Entity List*.

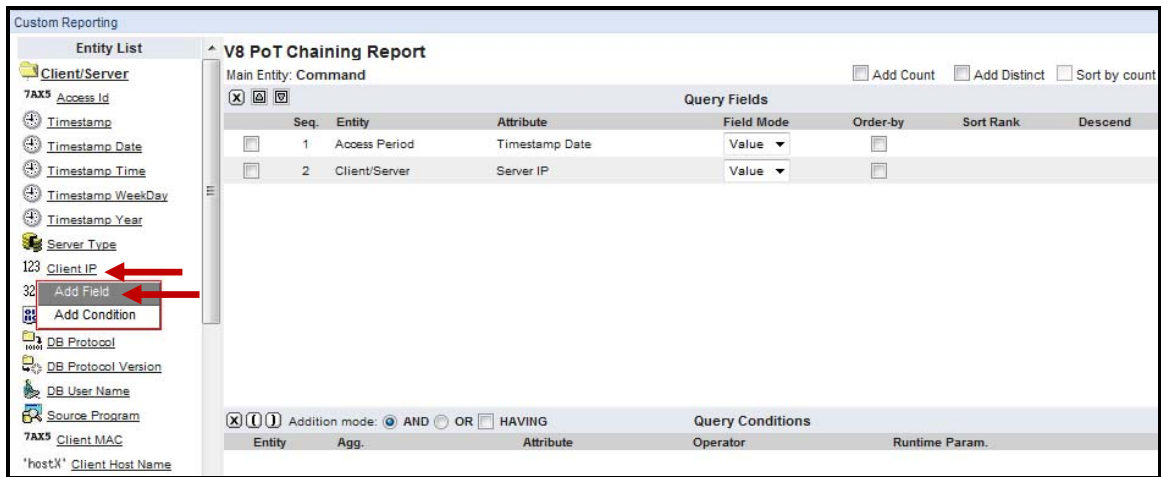


We will continue using the same procedure to add the remaining attributes.

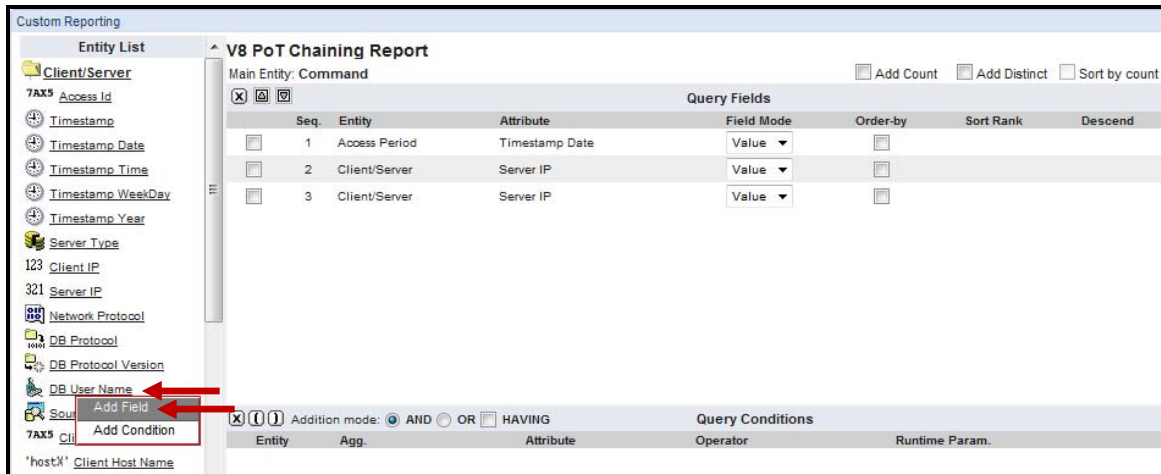
- c. Select the **Server IP** attribute from the *Client/Server* entity and click **Add Field**.



- d. Select the **Client IP** attribute from the *Client/Server* entity and click **Add Field**.



- e. Select the **DB User Name** attribute from the *Client/Server* entity and click **Add Field**.



- __f. Select the **Source Program** attribute from the *Client Server* entity and click **Add Field**. Then, select **Client/Server** from the *Entity List* to collapse the **Client/Server** folder.

Custom Reporting

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

7AX Source Program

7AX Add Field

7AX Add Condition

V8 PoT Chaining Report

Main Entity: Command

Add Count Add Distinct Sort by count

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Access Period	Timestamp Date	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Server IP	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	3	Client/Server	Server IP	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	4	Client/Server	DB User Name	Value	<input type="checkbox"/>	<input type="checkbox"/>

Query Fields

Entity Agg. Attribute Operator Runtime Param.

Additional mode: AND OR HAVING

- __g. Now select **Session** from the *Entity List*.

Custom Reporting

Entity List

Client/Server

Session

Server IP/Server Port

App User Name

Application Events

FULL SQL Values

FULL SQL

SQL

Access Period

Command

Object

Object/Command

Join

Field SQL Value

Qualified Object

Field

Object/Field

V8 PoT Chaining Report

Main Entity: Command

Add Count Add Distinct Sort by count

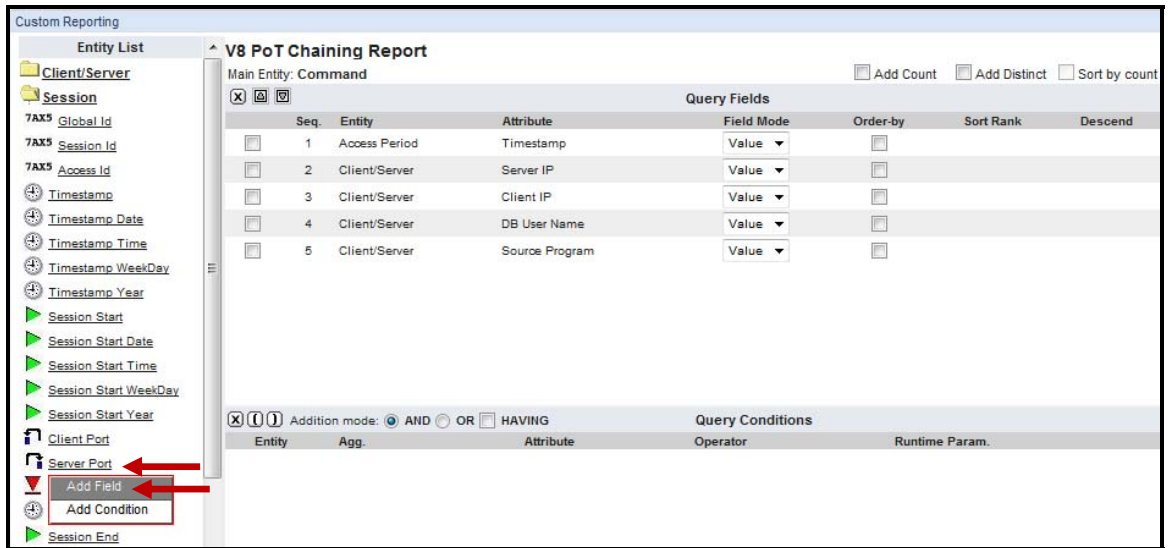
Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Access Period	Timestamp Date	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Server IP	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	3	Client/Server	Server IP	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	4	Client/Server	DB User Name	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	5	Client/Server	Source Program	Value	<input type="checkbox"/>	<input type="checkbox"/>

Query Fields

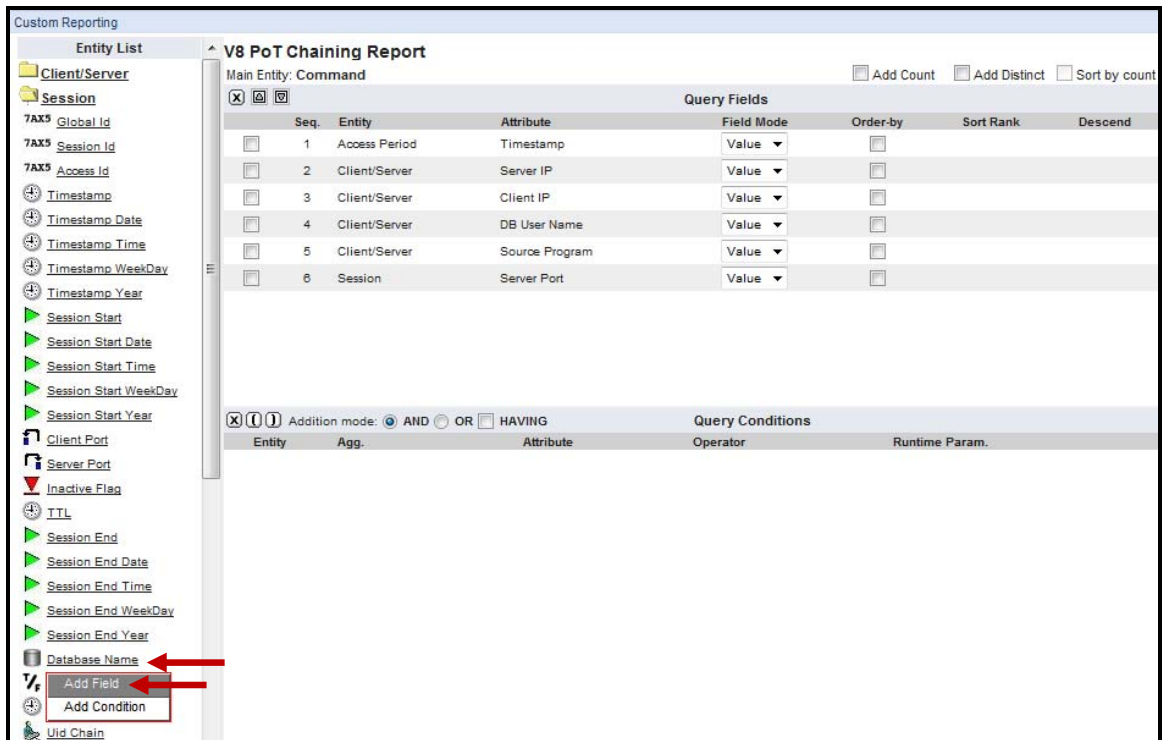
Entity Agg. Attribute Operator Runtime Param.

Additional mode: AND OR HAVING

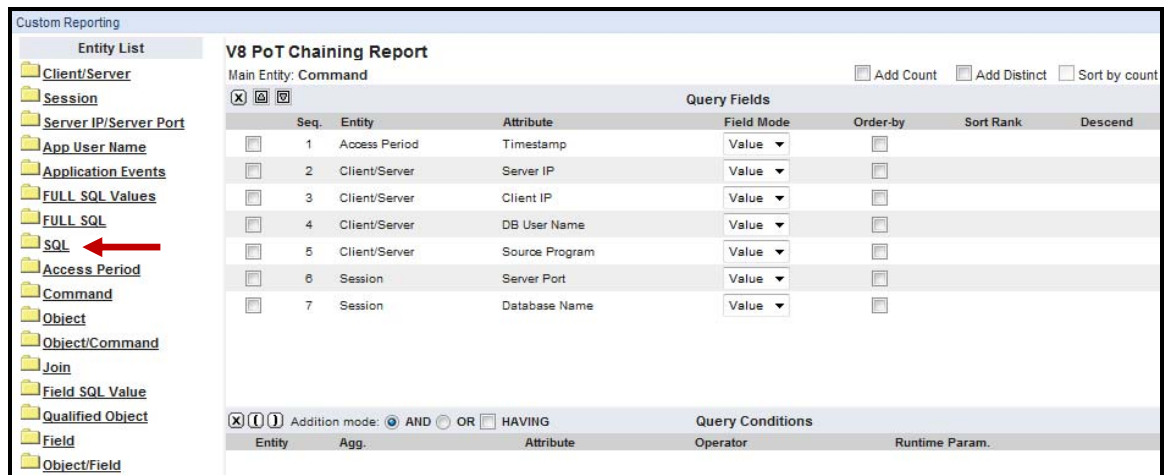
__h. Select the **Server Port** attribute from the *Session* entity and click **Add Field**.



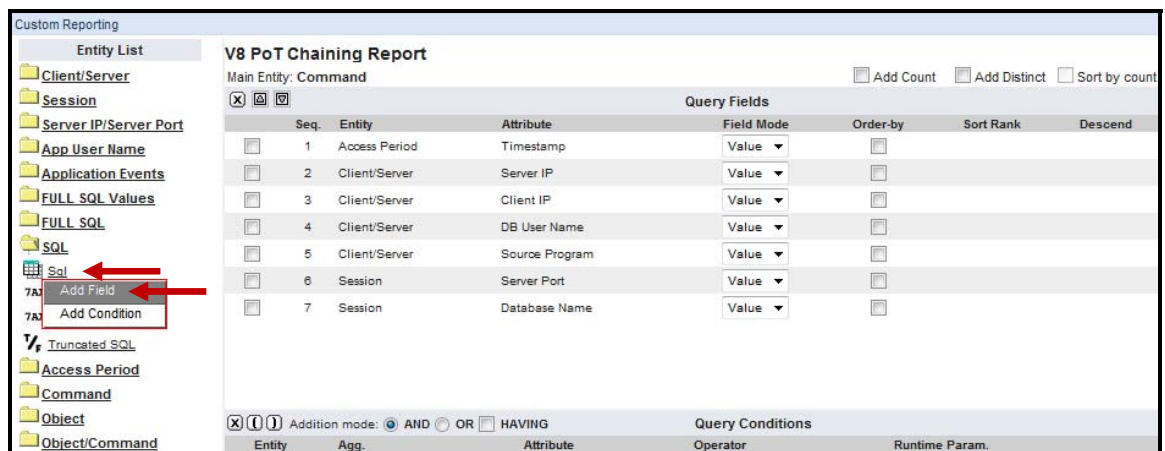
__i. Select the **Database Name** attribute from the *Session* entity and click **Add Field**. Then, select **Session** from the *Entity List* to collapse the **Session** folder.



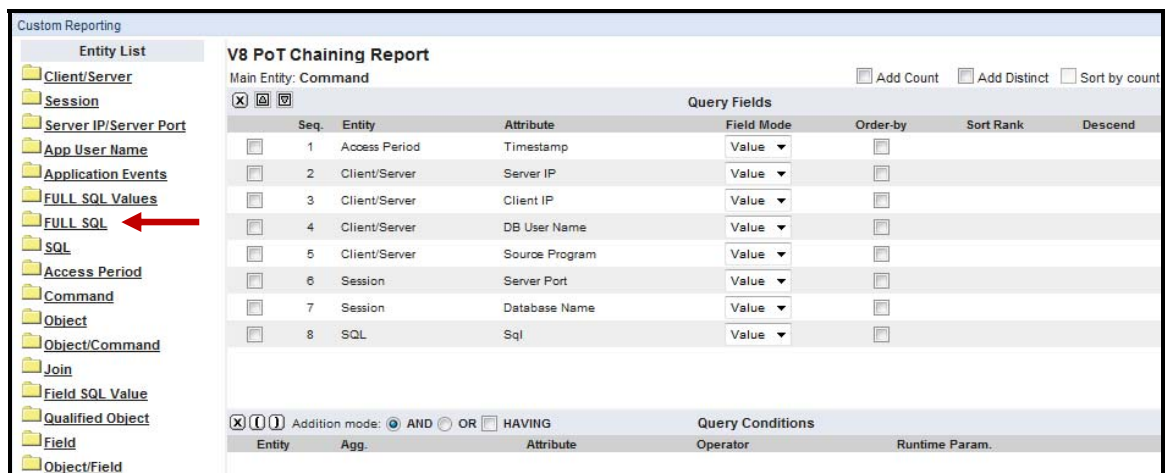
j. Now, select **SQL** from the *Entity List*.



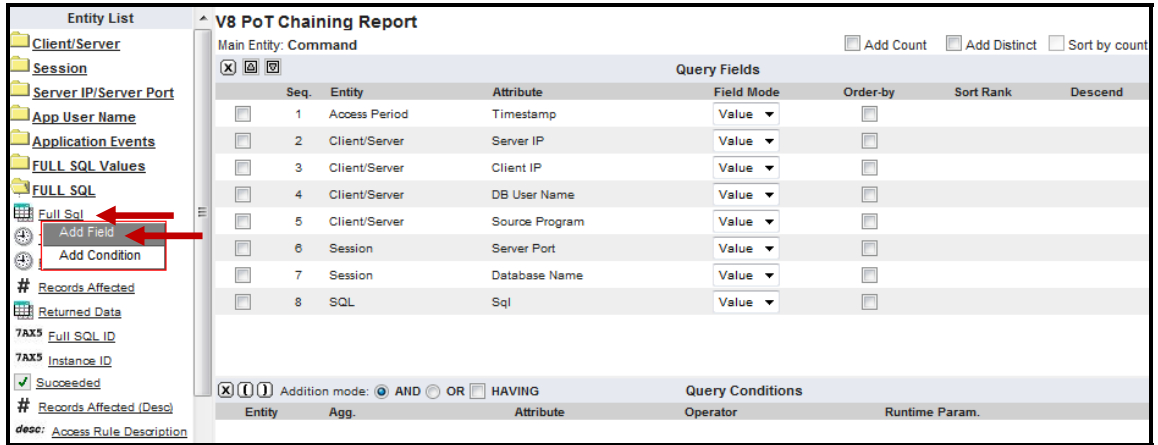
k. Select the **Sql** attribute from the *SQL* entity and click **Add Field**. Then, select **SQL** from the *Entity List* to collapse the **SQL** folder.



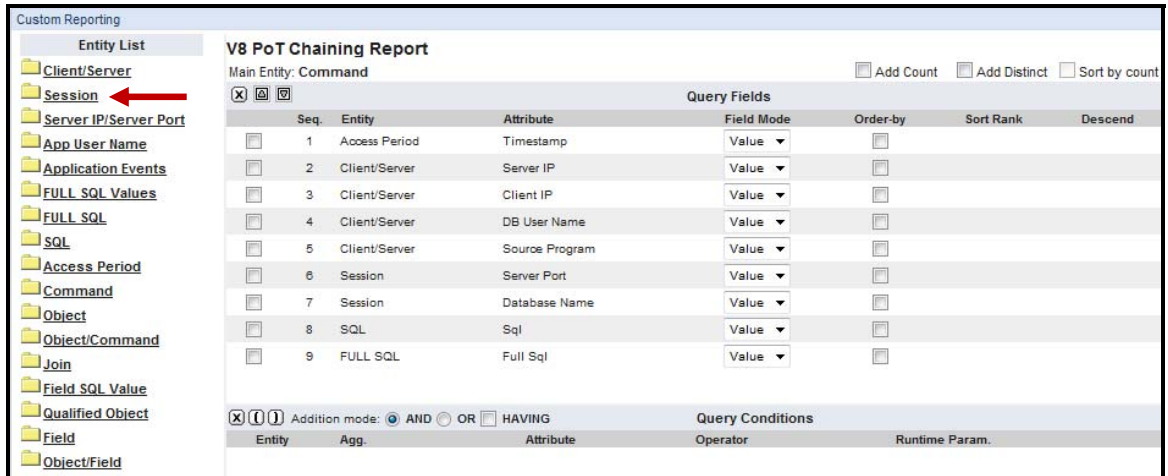
l. Now, select **FULL SQL** from the *Entity List*.



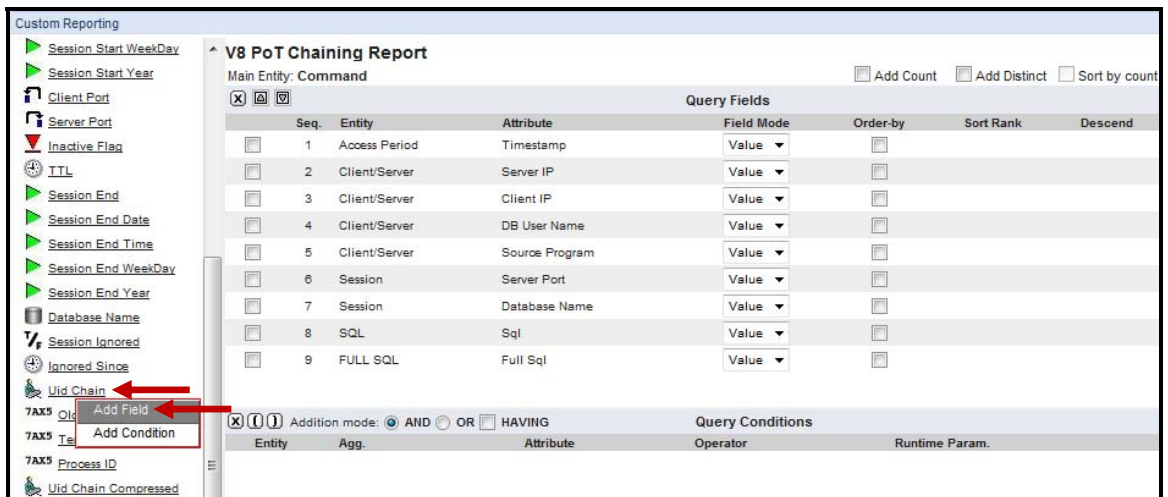
- m. Select the **Full Sql** attribute from the *FULL SQL* entity and click **Add Field**. Then, select **FULL SQL** from the *Entity List* to collapse the **FULL SQL** folder.



- n. Now, select **Session** from the *Entity List*.



- o. Select **UID Chain** attribute from the *Session* Entity List and Click **Add Field**.



Note: UID Chain will map all the IDs used by a specific user during each session.

- __p. Select the **UID Chain Compressed** attribute from the *Session* entity and click **Add Field**. Then, select **SESSION** from the *Entity List* to collapse the **SESSION** folder.

The screenshot displays the 'Custom Reporting' interface for a 'V8 PoT Chaining Report'. The main entity is 'Command'. The 'Query Fields' table is as follows:

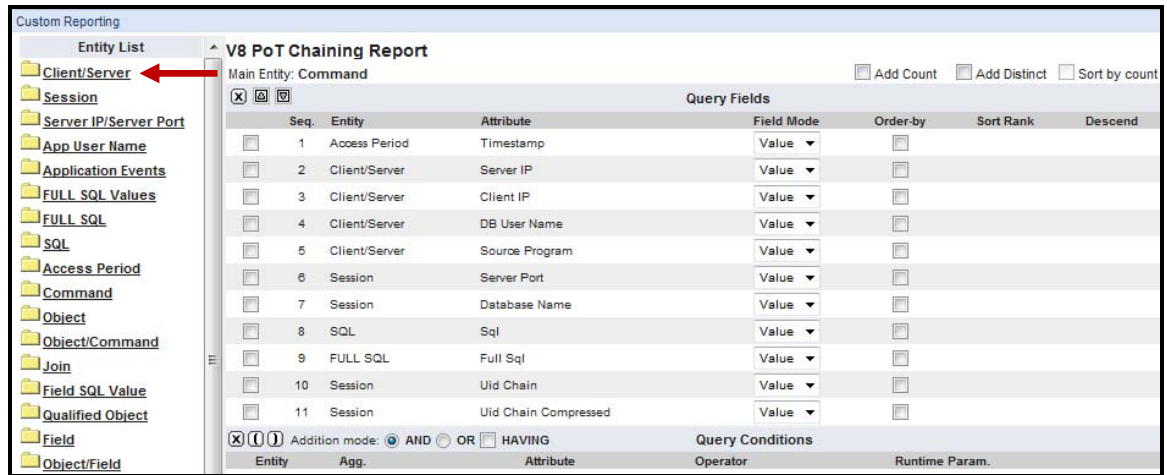
Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Access Period	Timestamp	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Server IP	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	3	Client/Server	Client IP	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	4	Client/Server	DB User Name	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	5	Client/Server	Source Program	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	6	Session	Server Port	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	7	Session	Database Name	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	8	SQL	Sql	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	9	FULL SQL	Full Sql	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	10	Session	Uid Chain	Value	<input type="checkbox"/>	<input type="checkbox"/>

Below the table, the 'Query Conditions' section shows 'Addition mode' set to 'AND'. The table below this section is currently empty.

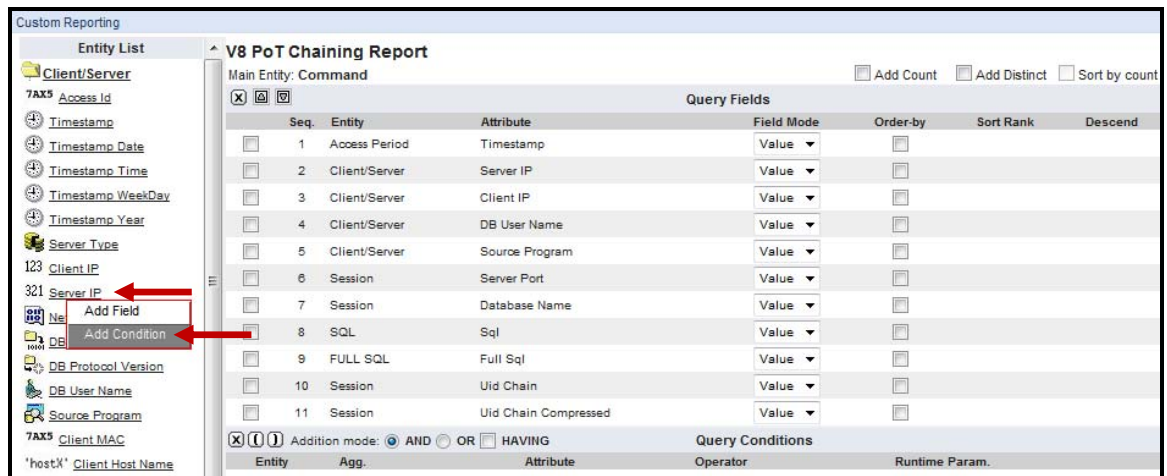
In the left sidebar, the 'UID Chain Compressed' attribute is highlighted with a red box, and the 'Add Field' button is also highlighted with a red box. A red arrow points from the 'Add Field' button to the 'UID Chain Compressed' attribute.

__4. The next few steps will add Custom *Conditions* for the **V8 PoT Chaining Report**.

__a. Now, select **Client/Server** from the *Entity List*.



__b. Select the **Server IP** attribute from the *Client/Server* entity and click **Add Condition**.



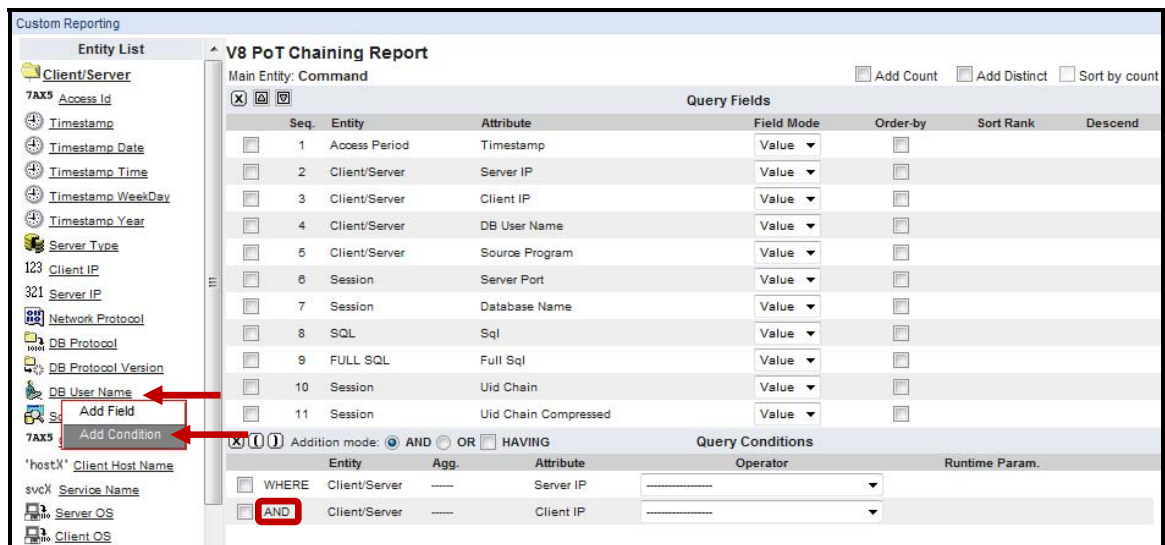
Note: The Query Condition Pane now has the *WHERE* clause with the *Server IP* attribute. We will be updating these clause parameters shortly.

- c. Select the **Client IP** attribute from the *Client/Server* entity and click **Add Condition**.



Note: The Query Condition Pane now has an 'AND' condition for the *Client IP* attribute.

- d. Select the **DB User Name** attribute from the *Client/Server* entity and click **Add Condition**. Then, select **Client/Server** from the *Entity List* to collapse the **Client/Server** folder.



__e. Now, select **Session** from the *Entity List*.

Custom Reporting

Entity List

- Client/Server
- Session** (selected)
- Server IP/Server Port
- App User Name
- Application Events
- FULL SQL Values
- FULL SQL
- SQL
- Access Period
- Command
- Object
- Object/Command
- Join
- Field SQL Value
- Qualified Object
- Field
- Object/Field

V8 PoT Chaining Report

Main Entity: Command Add Count Add Distinct Sort by count

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Access Period	Timestamp	Value		<input type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Server IP	Value		<input type="checkbox"/>
<input type="checkbox"/>	3	Client/Server	Client IP	Value		<input type="checkbox"/>
<input type="checkbox"/>	4	Client/Server	DB User Name	Value		<input type="checkbox"/>
<input type="checkbox"/>	5	Client/Server	Source Program	Value		<input type="checkbox"/>
<input type="checkbox"/>	6	Session	Server Port	Value		<input type="checkbox"/>
<input type="checkbox"/>	7	Session	Database Name	Value		<input type="checkbox"/>
<input type="checkbox"/>	8	SQL	Sql	Value		<input type="checkbox"/>
<input type="checkbox"/>	9	FULL SQL	Full Sql	Value		<input type="checkbox"/>
<input type="checkbox"/>	10	Session	Uid Chain	Value		<input type="checkbox"/>
<input type="checkbox"/>	11	Session	Uid Chain Compressed	Value		<input type="checkbox"/>

Addition mode: AND OR HAVING

Entity	Agg.	Attribute	Operator	Runtime Param.
WHERE	Client/Server	Server IP		
AND	Client/Server	Client IP		
AND	Client/Server	DB User Name		

__f. Select the **Server Port** attribute from the *Session* entity and click **Add Condition**. Then, select **Session** from the *Entity List* to collapse the **Session** folder.

Custom Reporting

Entity List

- Client/Server
- Session** (expanded)
 - 7AX5 Global Id
 - 7AX5 Session Id
 - 7AX5 Access Id
 - Timestamp
 - Timestamp Date
 - Timestamp Time
 - Timestamp WeekDay
 - Timestamp Year
 - Session Start
 - Session Start Date
 - Session Start Time
 - Session Start WeekDay
 - Session Start Year
 - Client Port
 - Server Port (selected)
 - Inet
 - TTI
 - Session End

V8 PoT Chaining Report

Main Entity: Command Add Count Add Distinct Sort by count

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Access Period	Timestamp	Value		<input type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Server IP	Value		<input type="checkbox"/>
<input type="checkbox"/>	3	Client/Server	Client IP	Value		<input type="checkbox"/>
<input type="checkbox"/>	4	Client/Server	DB User Name	Value		<input type="checkbox"/>
<input type="checkbox"/>	5	Client/Server	Source Program	Value		<input type="checkbox"/>
<input type="checkbox"/>	6	Session	Server Port	Value		<input type="checkbox"/>
<input type="checkbox"/>	7	Session	Database Name	Value		<input type="checkbox"/>
<input type="checkbox"/>	8	SQL	Sql	Value		<input type="checkbox"/>
<input type="checkbox"/>	9	FULL SQL	Full Sql	Value		<input type="checkbox"/>
<input type="checkbox"/>	10	Session	Uid Chain	Value		<input type="checkbox"/>
<input type="checkbox"/>	11	Session	Uid Chain Compressed	Value		<input type="checkbox"/>

Addition mode: AND OR HAVING

Entity	Agg.	Attribute	Operator	Runtime Param.
WHERE	Client/Server	Server IP		
AND	Client/Server	Client IP		
AND	Client/Server	DB User Name		

__g. Now, select **SQL** from the *Entity List*.

Custom Reporting

Entity List

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

V8 PoT Chaining Report

Main Entity: Command Add Count Add Distinct Sort by count

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Access Period	Timestamp	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Server IP	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	3	Client/Server	Client IP	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	4	Client/Server	DB User Name	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	5	Client/Server	Source Program	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	6	Session	Server Port	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	7	Session	Database Name	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	8	SQL	Sql	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	9	FULL SQL	Full Sql	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	10	Session	Uid Chain	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	11	Session	Uid Chain Compressed	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>

Addition mode: AND OR HAVING

Entity	Agg.	Attribute	Operator	Runtime Param.
WHERE	Client/Server	Server IP	-----	-----
AND	Client/Server	Client IP	-----	-----
AND	Client/Server	DB User Name	-----	-----
AND	Session	Server Port	-----	-----

__h. Select the **Sql** attribute from the *SQL entity* and click **Add Condition**. Then, select **SQL** from the *Entity List* to collapse the **SQL** folder.

Custom Reporting

Entity List

- Client/Server
- Session
- Server IP/Server Port
- App User Name
- Application Events
- FULL SQL Values
- FULL SQL
- SQL
 - Sql ←
 - Add Field
 - Add Condition ←
- Truncated SQL
- Access Period
- Command
- Object
- Object/Command
- Join
- Field SQL Value
- Qualified Object
- Field
- Object/Field

V8 PoT Chaining Report

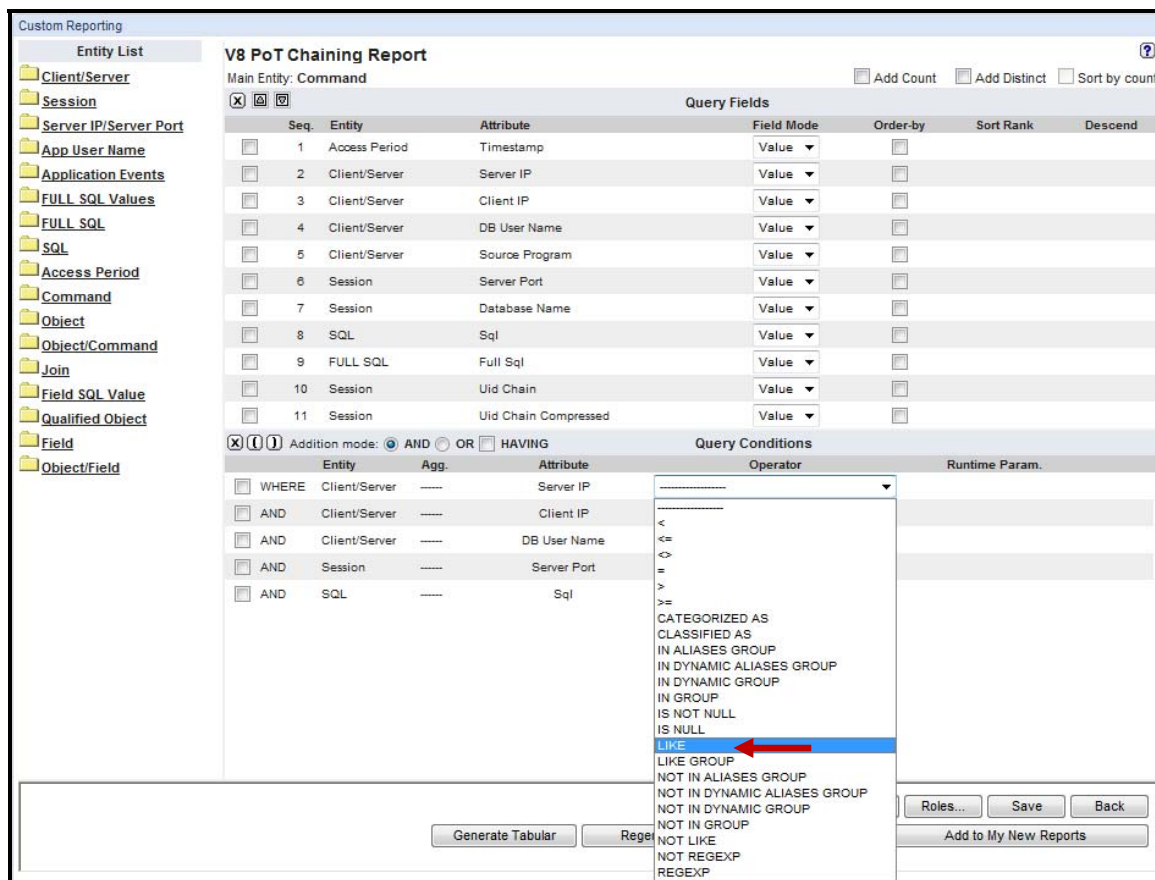
Main Entity: Command Add Count Add Distinct Sort by count

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Access Period	Timestamp	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Server IP	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	3	Client/Server	Client IP	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	4	Client/Server	DB User Name	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	5	Client/Server	Source Program	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	6	Session	Server Port	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	7	Session	Database Name	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	8	SQL	Sql	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	9	FULL SQL	Full Sql	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	10	Session	Uid Chain	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	11	Session	Uid Chain Compressed	Value ▼	<input type="checkbox"/>	<input type="checkbox"/>

Addition mode: AND OR HAVING

Entity	Agg.	Attribute	Operator	Runtime Param.
WHERE	Client/Server	Server IP	-----	-----
AND	Client/Server	Client IP	-----	-----
AND	Client/Server	DB User Name	-----	-----
AND	Session	Server Port	-----	-----

- __5. The next few steps will configure *Query Conditions Operators and Runtime Parameters* for the **V8 PoT Chaining Report**.
 - __a. Select **LIKE** from the *Query Conditions Operator* dropdown for each of the *Query Conditions*. You can also type 'L' to quickly select.



b. Make sure the **LIKE** operator is now reflected for each of the *Query Conditions*.

Custom Reporting

Entity List

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

V8 PoT Chaining Report

Main Entity: Command

Query Fields

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Access Period	Timestamp	Value		<input type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Server IP	Value		<input type="checkbox"/>
<input type="checkbox"/>	3	Client/Server	Client IP	Value		<input type="checkbox"/>
<input type="checkbox"/>	4	Client/Server	DB User Name	Value		<input type="checkbox"/>
<input type="checkbox"/>	5	Client/Server	Source Program	Value		<input type="checkbox"/>
<input type="checkbox"/>	6	Session	Server Port	Value		<input type="checkbox"/>
<input type="checkbox"/>	7	Session	Database Name	Value		<input type="checkbox"/>
<input type="checkbox"/>	8	SQL	Sql	Value		<input type="checkbox"/>
<input type="checkbox"/>	9	FULL SQL	Full Sql	Value		<input type="checkbox"/>
<input type="checkbox"/>	10	Session	Uid Chain	Value		<input type="checkbox"/>
<input type="checkbox"/>	11	Session	Uid Chain Compressed	Value		<input type="checkbox"/>

Query Conditions

Addition mode: AND OR HAVING

Entity	Agg.	Attribute	Operator	Runtime Param.
<input type="checkbox"/> WHERE	Client/Server	Server IP	LIKE	Value
<input type="checkbox"/> AND	Client/Server	Client IP	LIKE	Value
<input type="checkbox"/> AND	Client/Server	DB User Name	LIKE	Value
<input type="checkbox"/> AND	Session	Server Port	LIKE	Value
<input type="checkbox"/> AND	SQL	Sql	LIKE	Value

c. Now, select **Parameter** from the *Runtime Param.* dropdown for each of the *Query Conditions*. You can also type 'P' to quickly select.

Custom Reporting

Entity List

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

V8 PoT Chaining Report

Main Entity: Command

Query Fields

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Access Period	Timestamp	Value		<input type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Server IP	Value		<input type="checkbox"/>
<input type="checkbox"/>	3	Client/Server	Client IP	Value		<input type="checkbox"/>
<input type="checkbox"/>	4	Client/Server	DB User Name	Value		<input type="checkbox"/>
<input type="checkbox"/>	5	Client/Server	Source Program	Value		<input type="checkbox"/>
<input type="checkbox"/>	6	Session	Server Port	Value		<input type="checkbox"/>
<input type="checkbox"/>	7	Session	Database Name	Value		<input type="checkbox"/>
<input type="checkbox"/>	8	SQL	Sql	Value		<input type="checkbox"/>
<input type="checkbox"/>	9	FULL SQL	Full Sql	Value		<input type="checkbox"/>
<input type="checkbox"/>	10	Session	Uid Chain	Value		<input type="checkbox"/>
<input type="checkbox"/>	11	Session	Uid Chain Compressed	Value		<input type="checkbox"/>

Query Conditions

Addition mode: AND OR HAVING

Entity	Agg.	Attribute	Operator	Runtime Param.
<input type="checkbox"/> WHERE	Client/Server	Server IP	LIKE	Value
<input type="checkbox"/> AND	Client/Server	Client IP	LIKE	Value
<input type="checkbox"/> AND	Client/Server	DB User Name	LIKE	Parameter
<input type="checkbox"/> AND	Session	Server Port	LIKE	Value
<input type="checkbox"/> AND	SQL	Sql	LIKE	Value

___d. Verify that all Runtime Parameters are set to 'Parameter'.

Custom Reporting
V8 PoT Chaining Report
Main Entity: Command

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
1	Access Period	Timestamp	Value			
2	Client/Server	Server IP	Value			
3	Client/Server	Client IP	Value			
4	Client/Server	DB User Name	Value			
5	Client/Server	Source Program	Value			
6	Session	Server Port	Value			
7	Session	Database Name	Value			
8	SQL	Sql	Value			
9	FULL SQL	Full Sql	Value			
10	Session	Uid Chain	Value			
11	Session	Uid Chain Compressed	Value			

Entity	Agg.	Attribute	Operator	Runtime Param.
WHERE Client/Server	----	Server IP	LIKE	Parameter
AND Client/Server	----	Client IP	LIKE	Parameter
AND Client/Server	----	DB User Name	LIKE	Parameter
AND Session	----	Server Port	LIKE	Parameter
AND SQL	----	Sql	LIKE	Parameter

___e. Now, add a meaningful name for each **Runtime Parameter** using only alphanumeric characters and no spaces. The names are to the right of the *Runtime Param.* list.

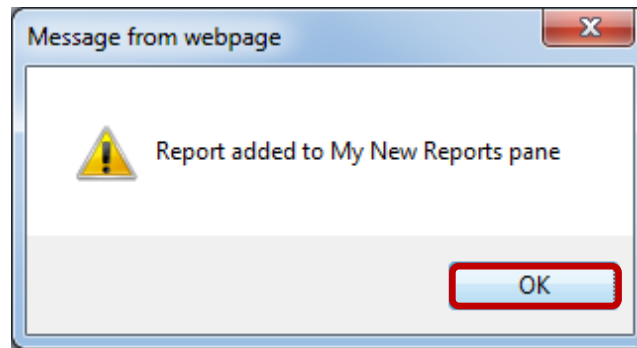
___f. Click **Save** and click **Add to My New Reports** to add it to the **My New Reports** pane.

Custom Reporting
V8 PoT Chaining Report
Main Entity: Command

Entity	Agg.	Attribute	Operator	Runtime Param.
WHERE Client/Server	----	Server IP	LIKE	Parameter
AND Client/Server	----	Client IP	LIKE	Parameter
AND Client/Server	----	DB User Name	LIKE	Parameter
AND Session	----	Server Port	LIKE	Parameter
AND SQL	----	Sql	LIKE	Parameter

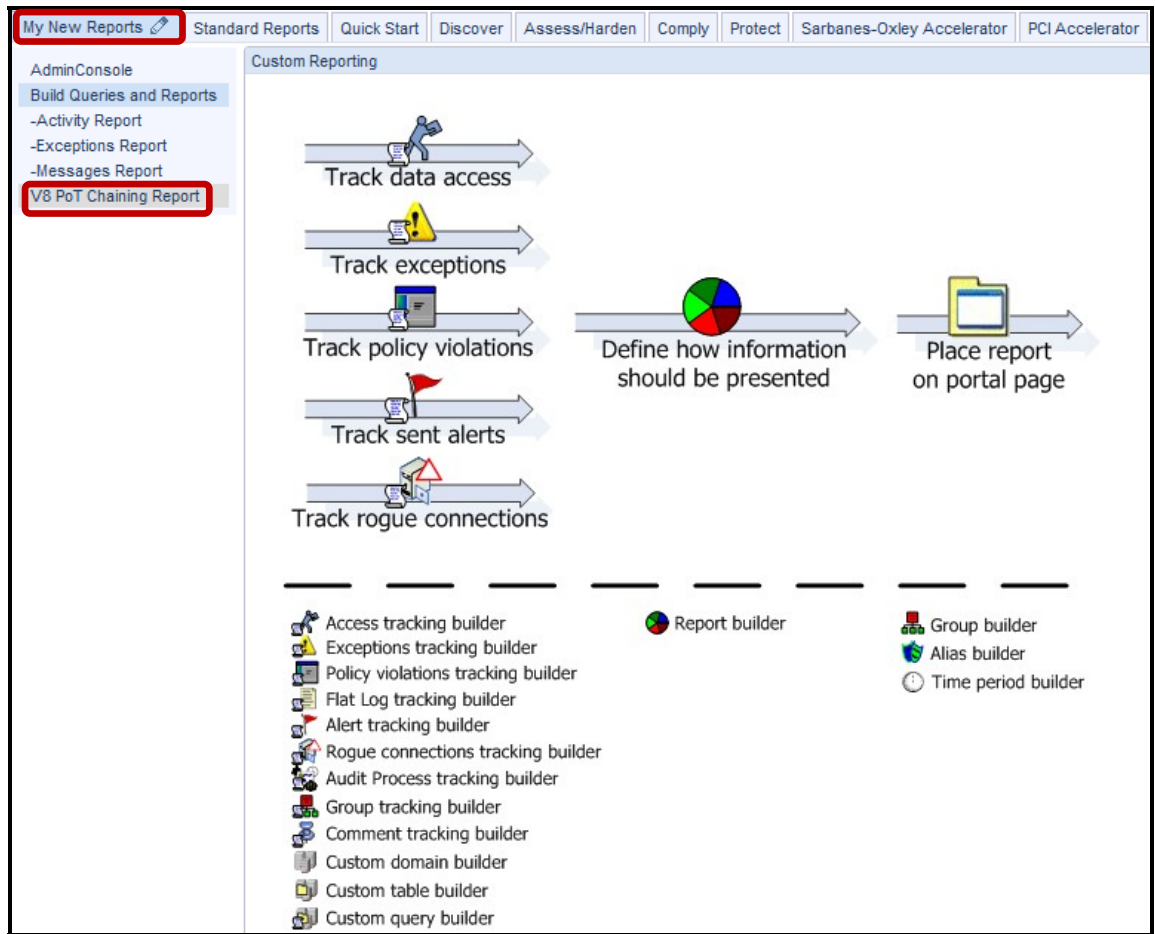
Buttons: Delete, Clone, Roles..., **Save**, Back
 Generate Tabular, Regenerate, Add to Pane..., **Add to My New Reports**

- __g. Click **OK** to acknowledge that the report has been added to the **My New Reports** pane.

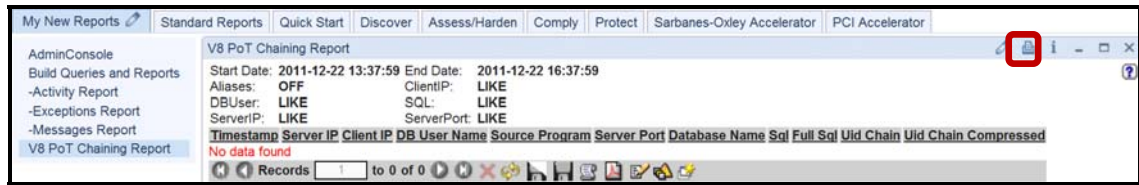


__6. Confirm that the Report has been created, and configure runtime parameters

__a. Click **My New Reports** tab, and then select the newly created **V8 PoT Chaining Report**.



__b. Click the **Pencil** icon to edit the report.



Note: The Parameter Names are reflected under Run Time Parameters.

__c. Type the '%' character (match all) in each 'LIKE' clause, enter '**Now -2 DAY**' for *QUERY_FROM_DATE*, '**Now +1 DAY**' for *QUERY_TO_DATE*, and click **Update**.

Customize Portlet

Report: **V8 PoT Chaining Report** Based on Query: **V8 PoT Chaining Report**

Title:

Run Time Parameters

ClientIP
 Enter Value for Client IP

DBUser
 Enter Value for DB User Name

QUERY_FROM_DATE
 Enter Period From

QUERY_TO_DATE
 Enter Period To

REMOTE_SOURCE
 Remote Data Source

ServerIP
 Enter Value for Server IP

ServerPort
 Enter Value for Server Port

SHOW_ALIASES On Off Default
 Show Aliases

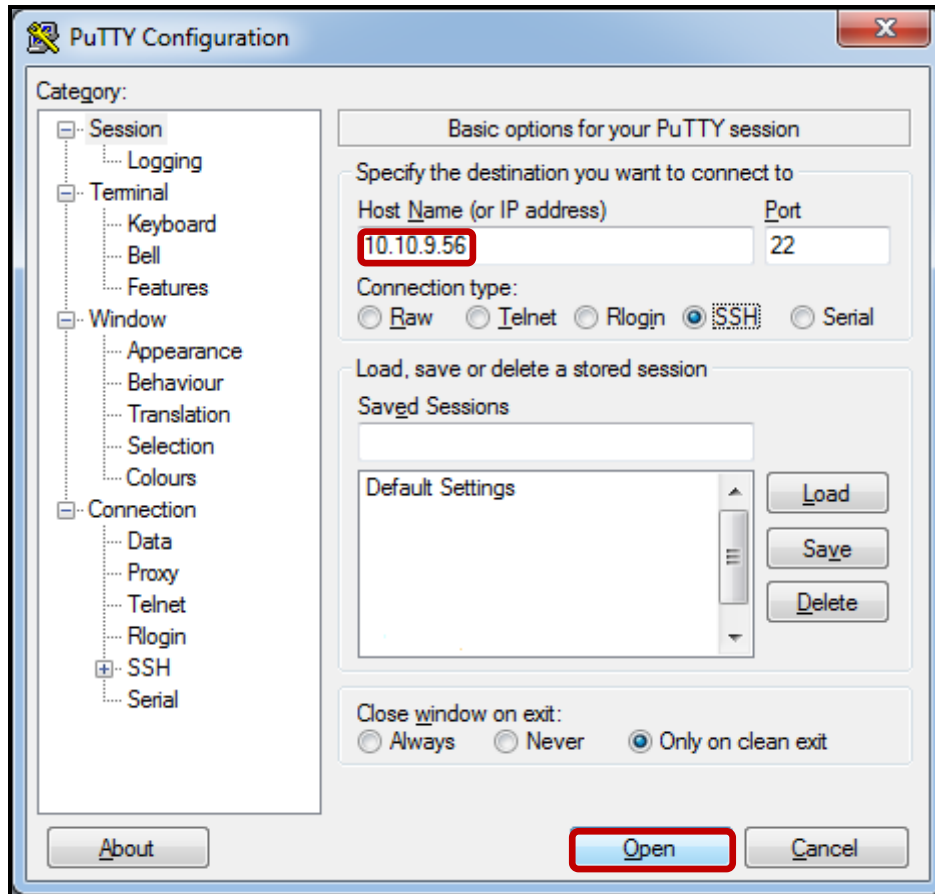
SQL
 Enter Value for Sql

Presentation Parameters

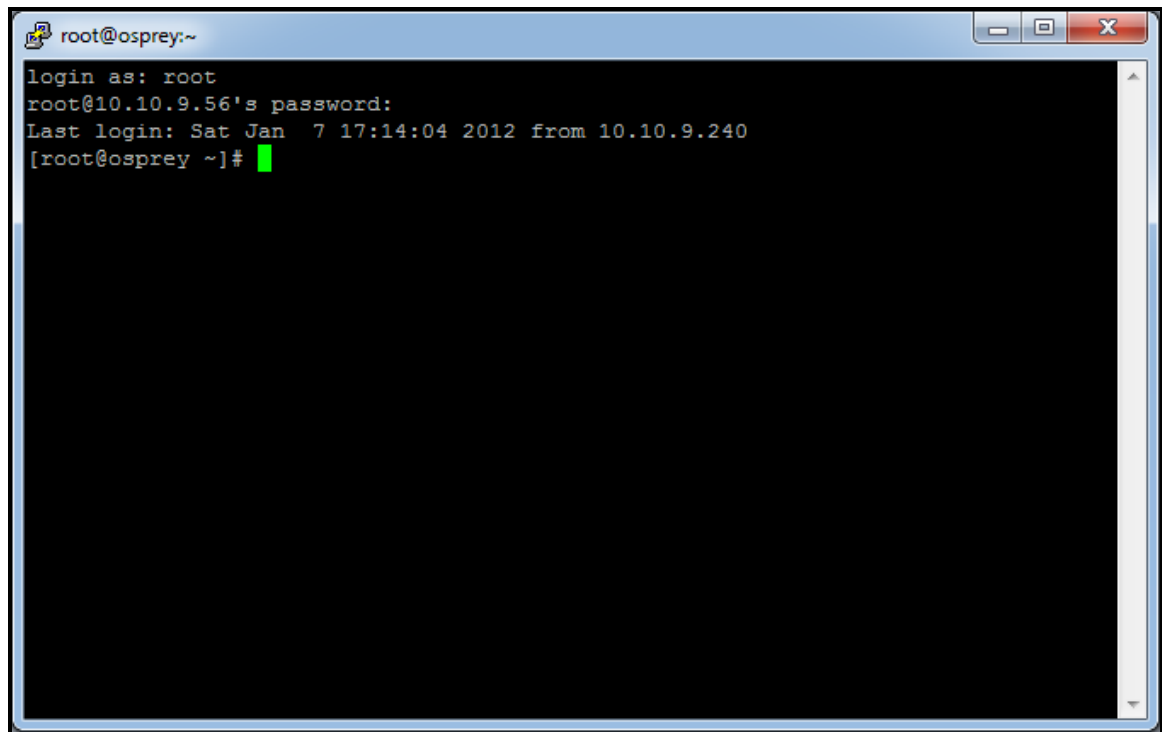
fetchSize
 Max. records per page

refreshRate
 Refresh rate (seconds)

- __7. Using a PuTTY SSH client, access the VM database server to demonstrate the ease with which the IBM InfoSphere Guardium solution can audit User ID chains.
 - __a. Start the PuTTY SSH client login.
 - __b. From your laptop, launch PuTTY, enter **10.10.9.56**, and click **Open**.

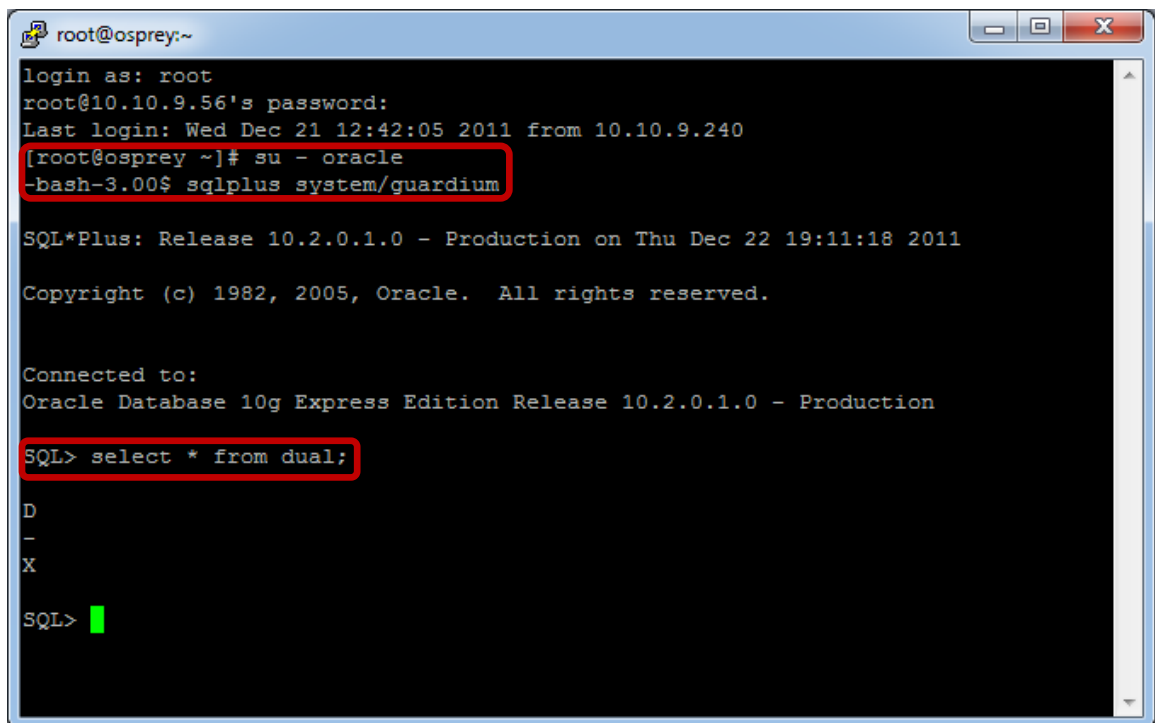


- __c. Login as **root** / **guardium**. After logging in, the following prompt will be displayed.



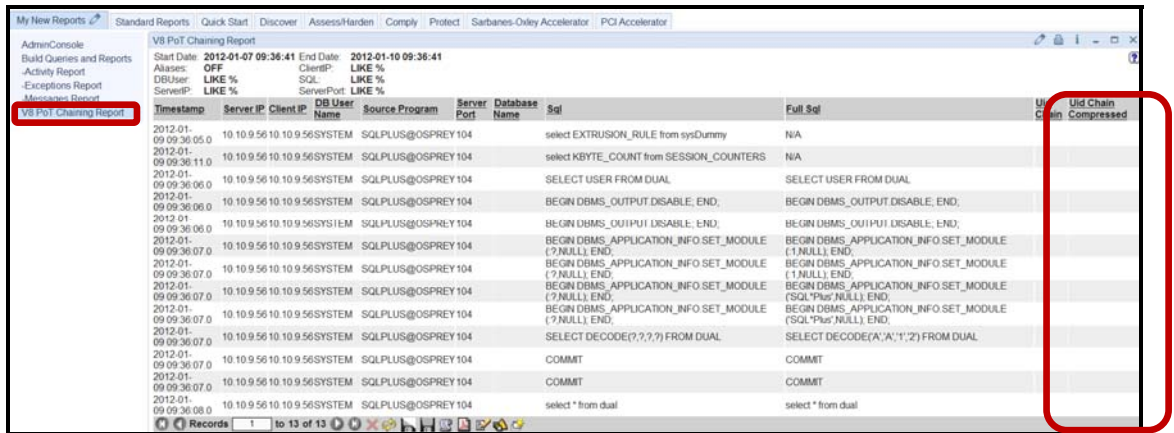
```
root@osprey:~  
login as: root  
root@10.10.9.56's password:  
Last login: Sat Jan 7 17:14:04 2012 from 10.10.9.240  
[root@osprey ~]#
```

- __d. Type **su - oracle**, type **sqlplus system/guardium**, and then type **select * from dual;** (Be sure to include semi-colon).



```
root@osprey:~  
login as: root  
root@10.10.9.56's password:  
Last login: Wed Dec 21 12:42:05 2011 from 10.10.9.240  
[root@osprey ~]# su - oracle  
-bash-3.00$ sqlplus system/guardium  
  
SQL*Plus: Release 10.2.0.1.0 - Production on Thu Dec 22 19:11:18 2011  
Copyright (c) 1982, 2005, Oracle. All rights reserved.  
  
Connected to:  
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production  
SQL> select * from dual;  
  
D  
-  
X  
  
SQL>
```

- __8. Return to the InfoSphere Guardium GUI to verify the report results.
- __a. Click the **V8 PoT Chaining Report** to refresh the report results.



- __b. Initially, there are no values for the **UID Chain** fields. It may take a few minutes for the **UID Chain** field to populate so just keep clicking on the **refresh** icon. Expect it to take two or three minutes to see the report populated with the UID Chain report. Look for the Full Sql select * from dual. The report indicates:

Original Login: *root*

su - to the os user: *oracle*

bequeath login (local sqlplus login) to: *oracle*

So we have tracked the database user who executed the select * from dual sql command, all the way back to the original OS user login.

Out of curiosity, you may want to try some longer chains.

Timestamp	Server IP	Client IP	DB User Name	Source Program	Server Port	Database Name	Sql	Full Sql	Uid Chain
2010-11-20 15:43:27.0	10.10.9.56	10.10.9.56	SYSTEM	SQLPLUS@OSPREY195	Customer		select * from dual	select * from dual	(1 root init [3])-> (2247 root,/usr /sbin/sshd)-> (4317 root,sshd: root@pts/0)->(4343, root,-bash)-> (4393,root,su - oracle)-> (4394,oracle,-bash)-> (4426,oracle,sqlplus)-> (4427,oracle,oracleXE (DESCRIPTION=(LOCAL=YES) (ADDRESS=(PROTOCOL=beq))))

Thank You

5.2 Using Computed Attributes (Optional)

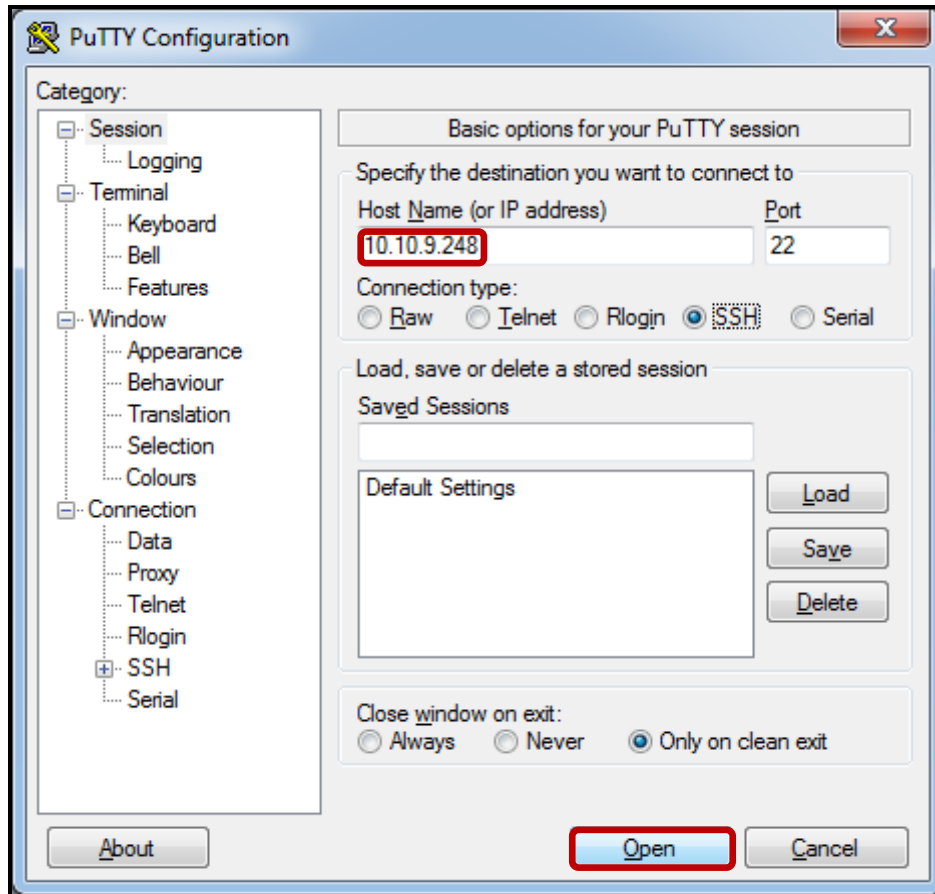
Overview

There may be situations where you desire only a subset of an output field. For example, a report may contain the Event Value Str attribute with a large mixture of data needing to be parsed to retrieve valuable application information. In the case of SAP, a string such as “APPLNAME=SE11” indicates the SAP Transaction Code that was issued by the application user. Suppose we wanted to create a new field containing just the SAP code (SE11 in this case). This lab will use Guardium Computed Attributes to demonstrate unique solutions for pulling valuable data from existing streams of mixed data.

Objectives

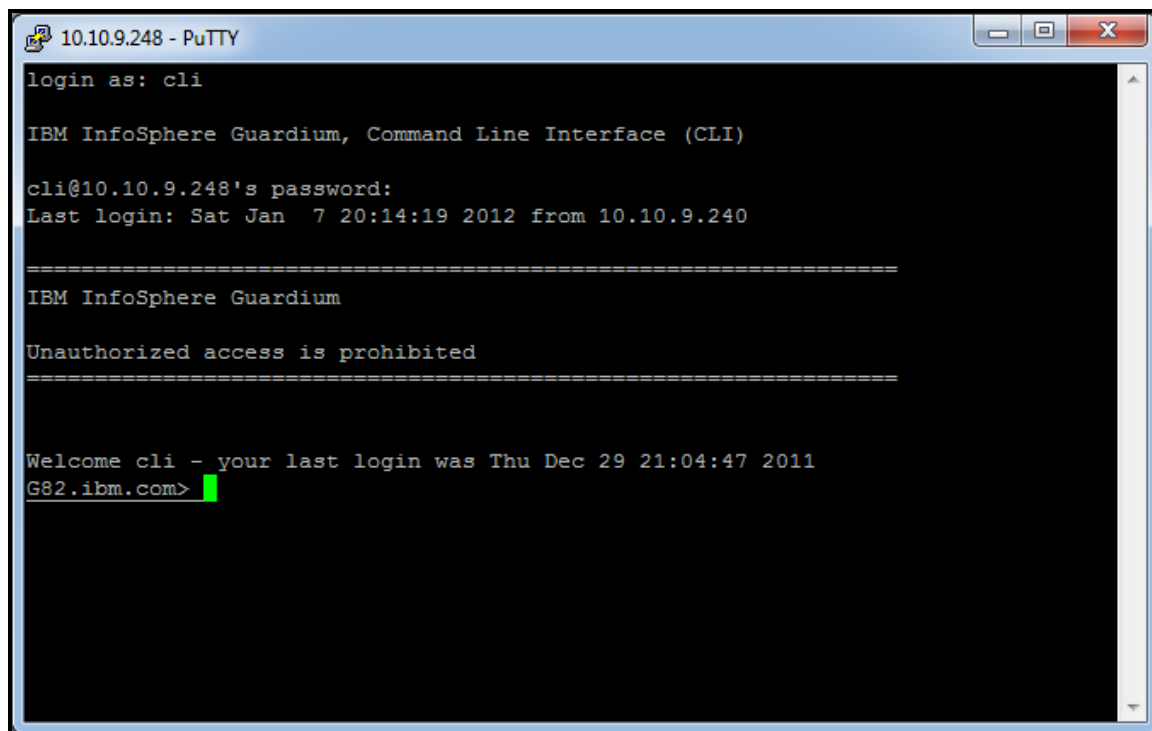
- __1. Open a PuTTY SSH client and log in to the IBM InfoSphere Guardium appliance.
- __2. Create a computed attribute to filter on SAP transaction report fields.
- __3. Open a browser window and log in to the IBM InfoSphere Guardium appliance.
- __4. Build a custom report to monitor SAP transactions, using the new computed attribute
- __5. Configure and view the report.

- __1. Using a PuTTY SSH client, access the VM Appliance to demonstrate the ease with which the IBM InfoSphere Guardium solution can configure computed attributes.
 - __a. Start the PuTTY SSH client login.
 - __b. From your laptop, launch PuTTY, enter **10.10.9.248**, and click **Open**.



__2. Create '**SAP-ID3**' Computed Attribute

__a. Login as **cli / guardium**. After logging in, the following prompt will be displayed.



```
10.10.9.248 - PuTTY
login as: cli

IBM InfoSphere Guardium, Command Line Interface (CLI)

cli@10.10.9.248's password:
Last login: Sat Jan  7 20:14:19 2012 from 10.10.9.240

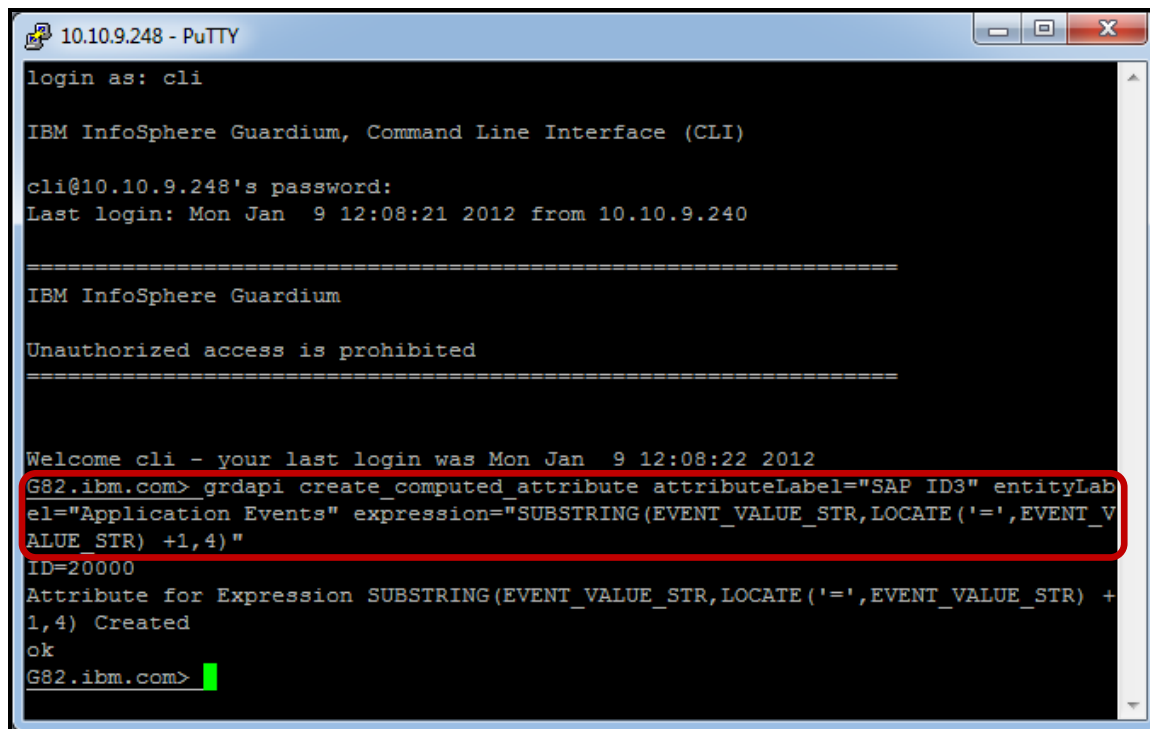
=====
IBM InfoSphere Guardium

Unauthorized access is prohibited
=====

Welcome cli - your last login was Thu Dec 29 21:04:47 2011
G82.ibm.com> █
```

- __b. Type (**Copy and Paste**) the following Guardium API command:

```
grdapi create_computed_attribute attributeLabel="SAP ID3" entityLabel="Application Events"
expression="SUBSTRING(EVENT_VALUE_STR,LOCATE('=',EVENT_VALUE_STR) +1,4)"
```



```
10.10.9.248 - PuTTY
login as: cli

IBM InfoSphere Guardium, Command Line Interface (CLI)

cli@10.10.9.248's password:
Last login: Mon Jan  9 12:08:21 2012 from 10.10.9.240

=====
IBM InfoSphere Guardium
Unauthorized access is prohibited
=====

Welcome cli - your last login was Mon Jan  9 12:08:22 2012
G82.ibm.com> grdapi create_computed_attribute attributeLabel="SAP ID3" entityLabel="Application Events" expression="SUBSTRING(EVENT_VALUE_STR,LOCATE('=',EVENT_VALUE_STR) +1,4)"
ID=20000
Attribute for Expression SUBSTRING(EVENT_VALUE_STR,LOCATE('=',EVENT_VALUE_STR) +1,4) Created
ok
G82.ibm.com>
```

Note: Here are details on the arguments used by the Guardium API command:

create_computed_attribute grdapi command to create a computed attribute.

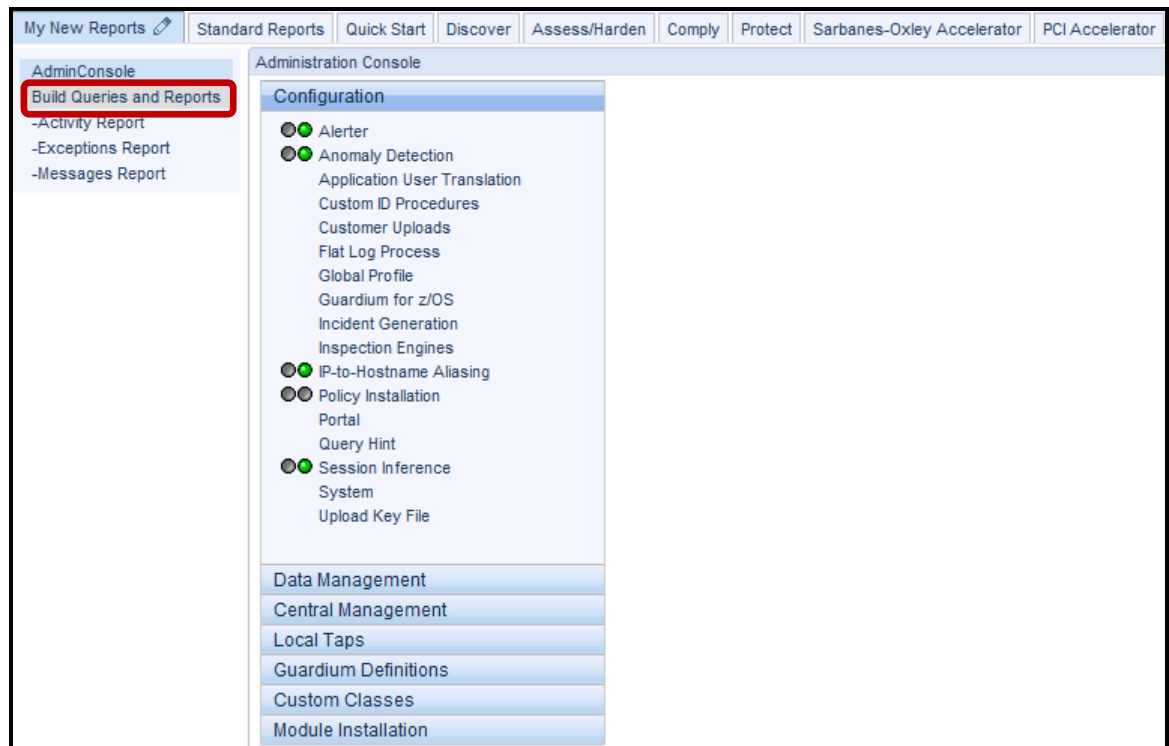
attributeLabel="SAP ID3" The name of the attribute being created.

entityLabel="Application Events" The entity domain for the newly created attribute.

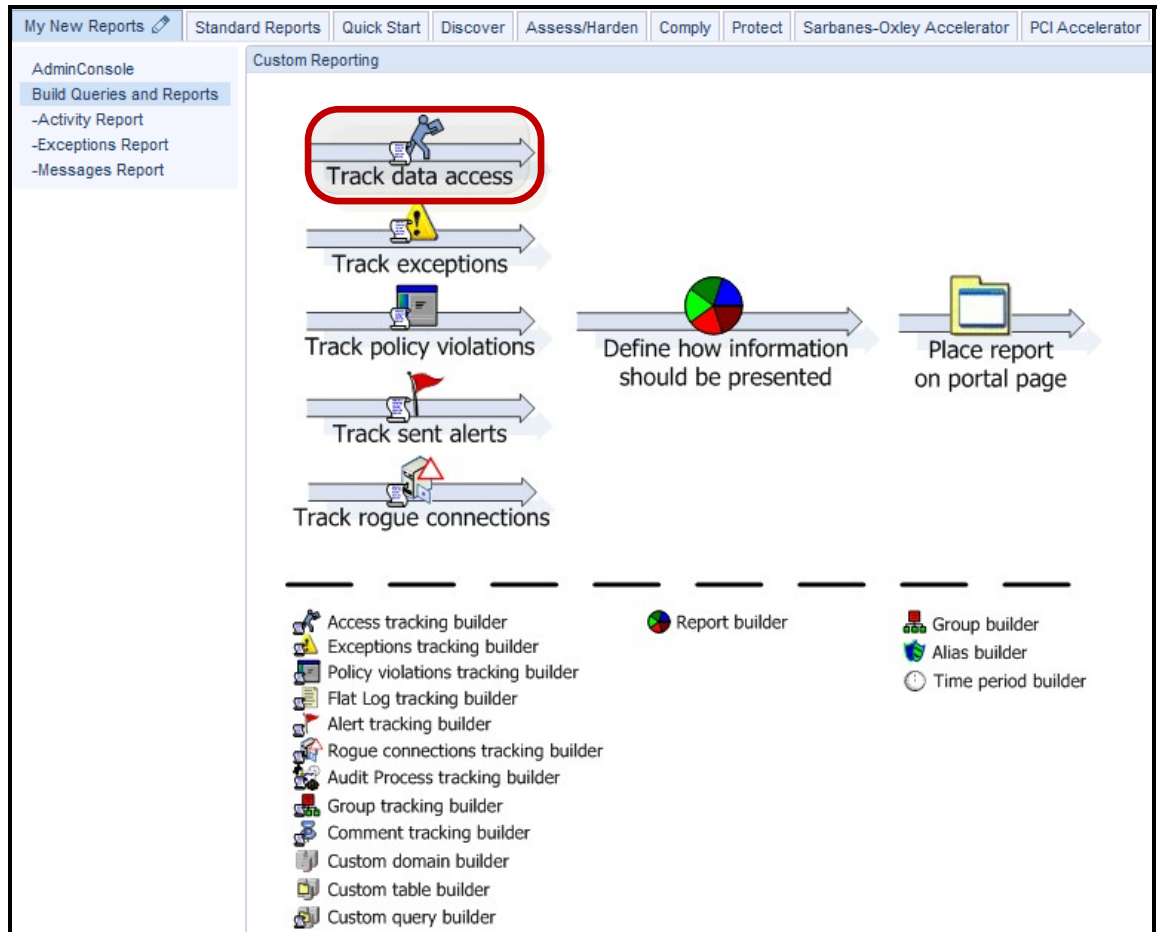
expression="SUBSTRING(EVENT_VALUE_STR,LOCATE('=',EVENT_VALUE_STR) +1,4)"

The expression is an SQL Query SUBSTRING function call on the EVENT_VALUE_STR attribute using the LOCATE function to detect the first '=' token. Once found, it extracts the next four characters from the first position immediately following the '='.

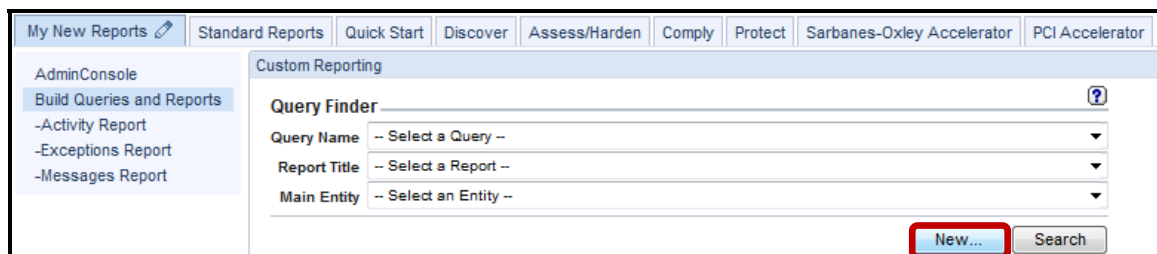
- __3. Use the IBM InfoSphere Guardium GUI to create a report to use our new computed attribute.
- __a. Click **Build Queries and Reports** under the **My New Reports** tab.



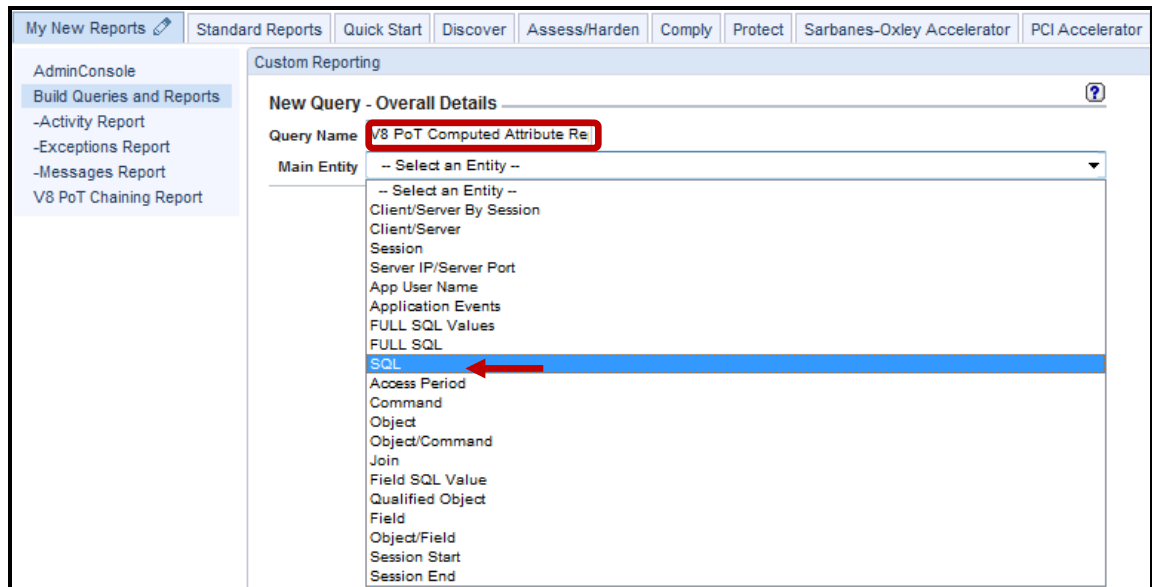
__b. Click **Track data access**.



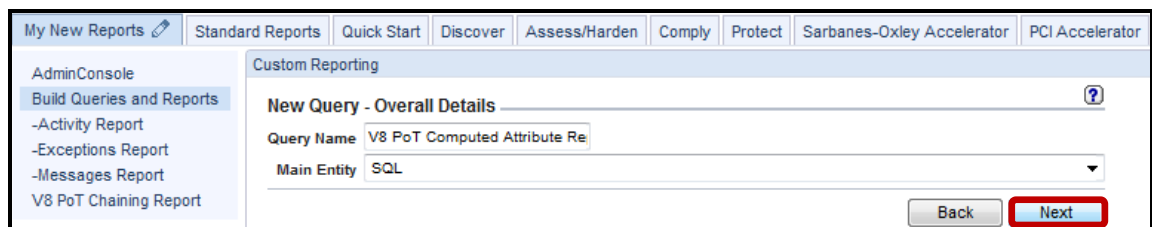
__c. Click **New**.



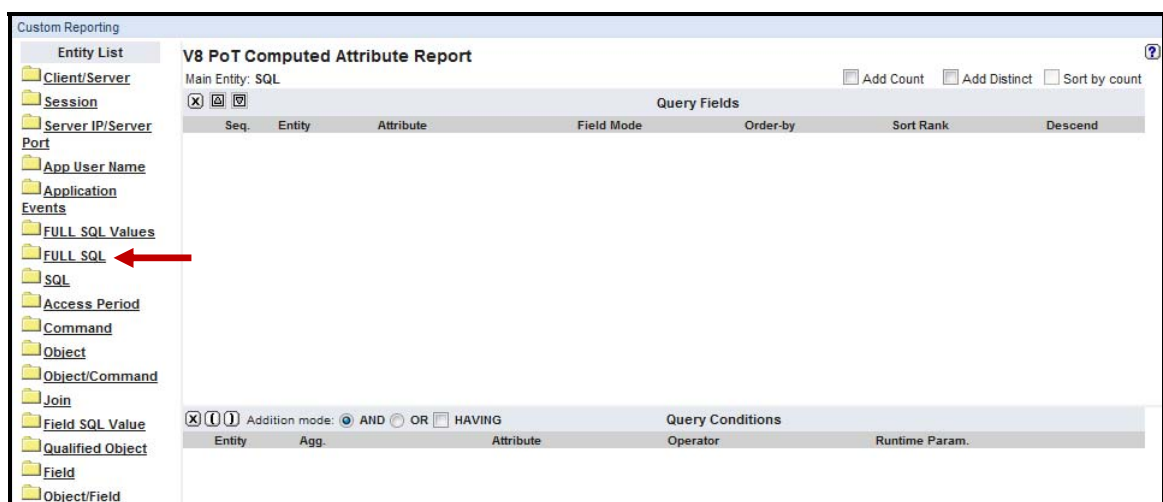
- d. Enter '**V8 PoT Computed Attribute Report**' for the *Query Name* and Select **SQL** from the *Main Entity* dropdown.



- e. Click **Next**.

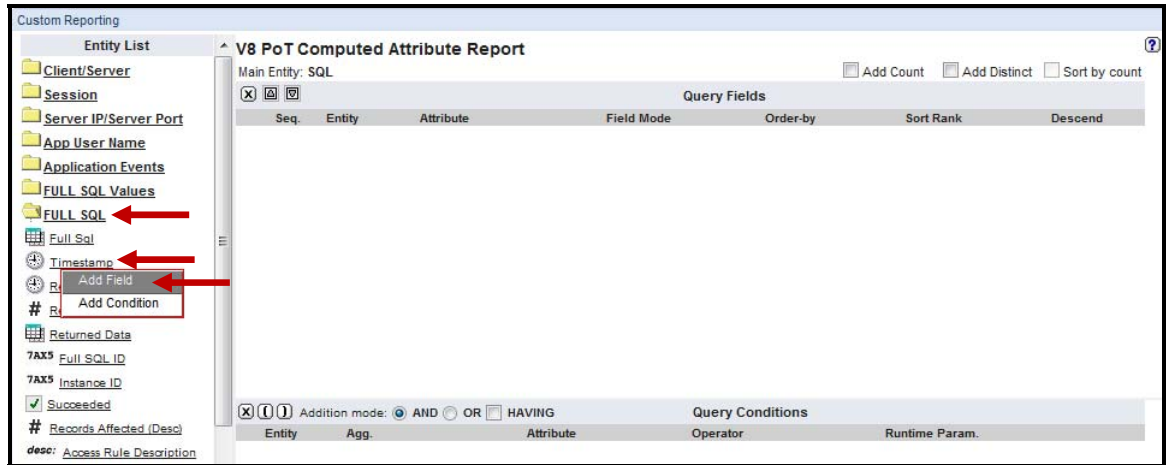


- f. Select **Full SQL** from *Entity List*.



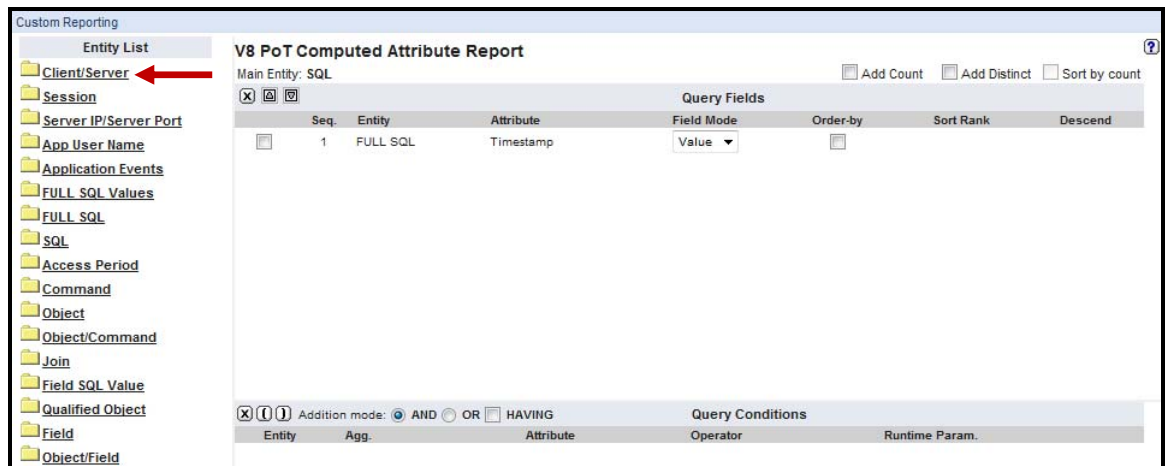
__4. The next few steps will add Custom *Query* Fields for the **V8 PoT Computed Attribute Report**.

- __a. Select the **Timestamp** attribute from *Full SQL* entity and click **Add Field**. Then, select **Full SQL** from the *Entity List* to collapse the **Full SQL** folder.



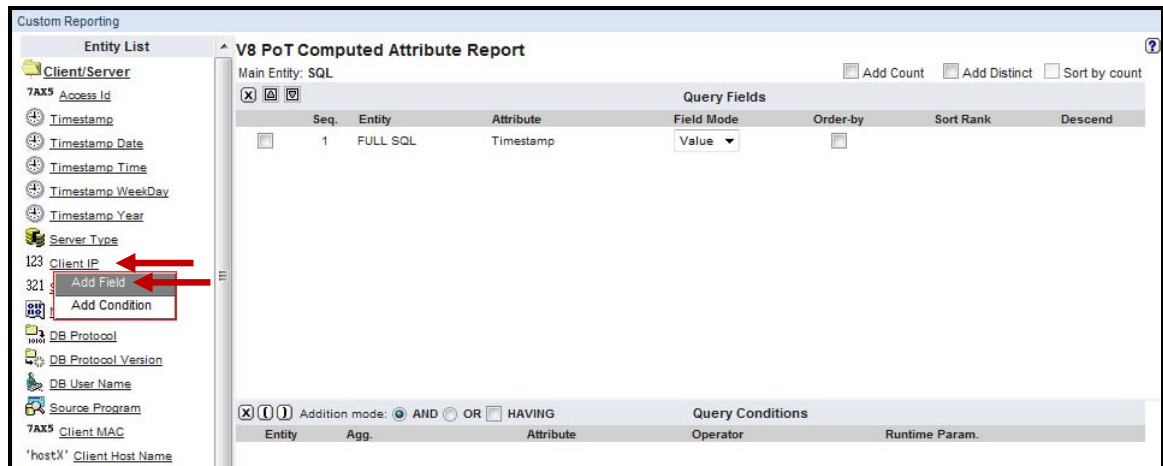
Note: The Timestamp attribute has now been added to the query window.

- __b. Now select **Client/Server** from the *Entity List*.

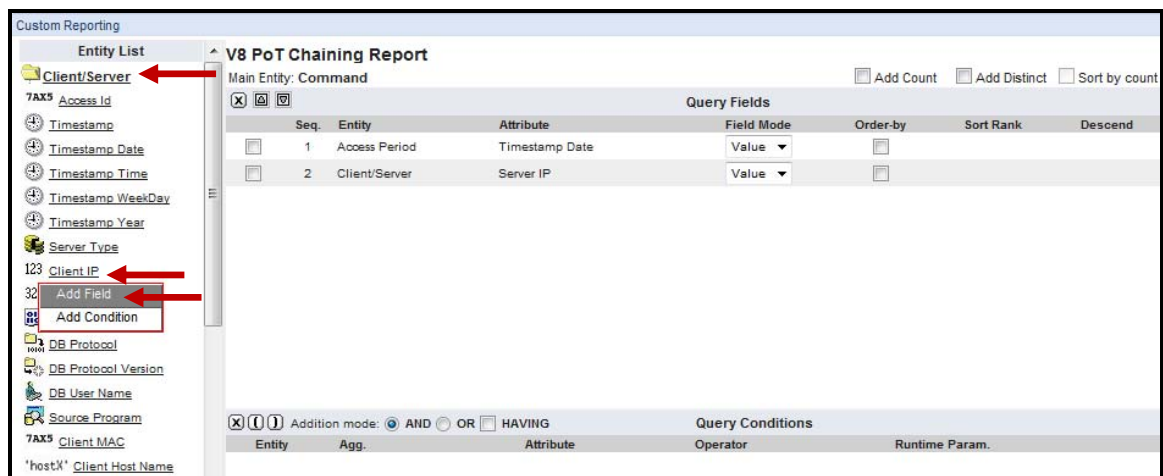


We will continue using the same procedure to add the remaining attributes.

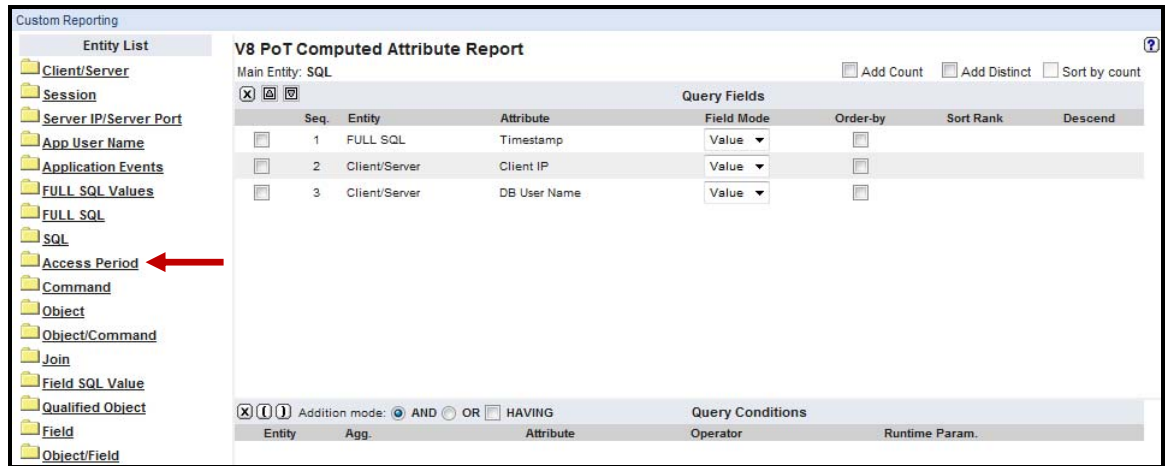
- __c. Select the **Client IP** attribute from the *Client/Server* entity and click **Add Field**.



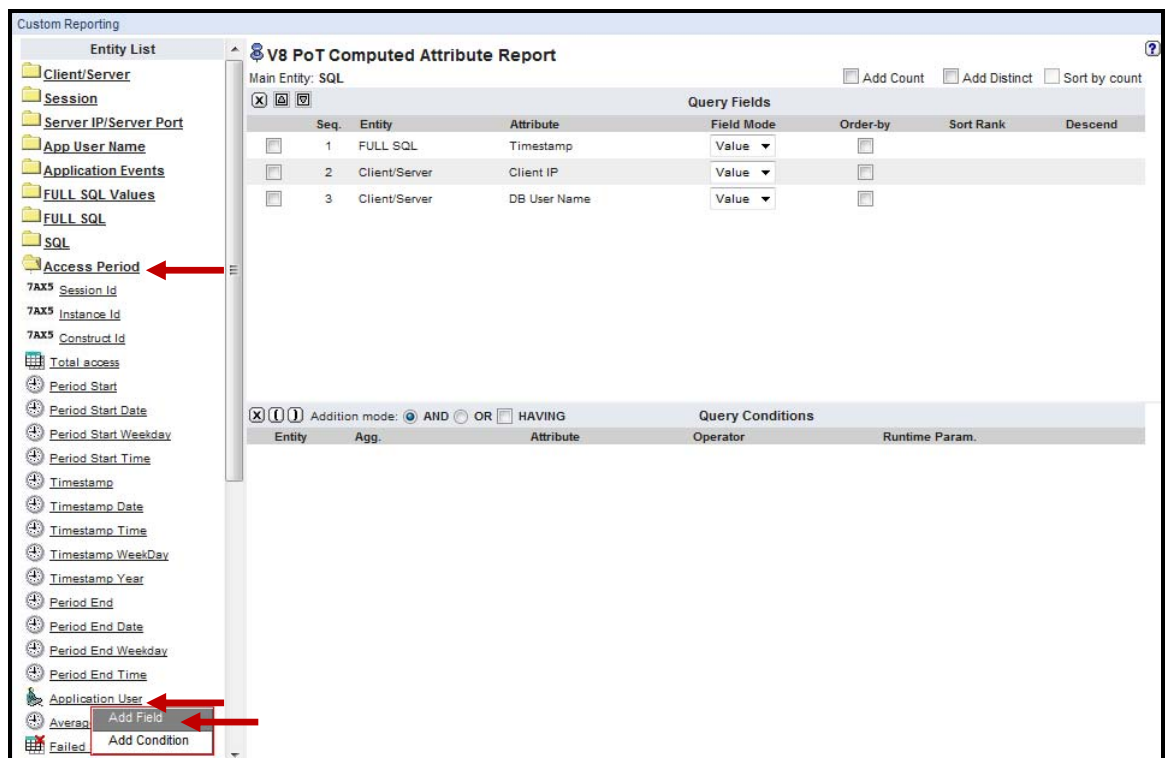
- __d. Select the **DB User Name** attribute from the *Client/Server* entity and click **Add Field**. Then select **Client/Server** from the *Entity List* to collapse the **Client/Server** folder.



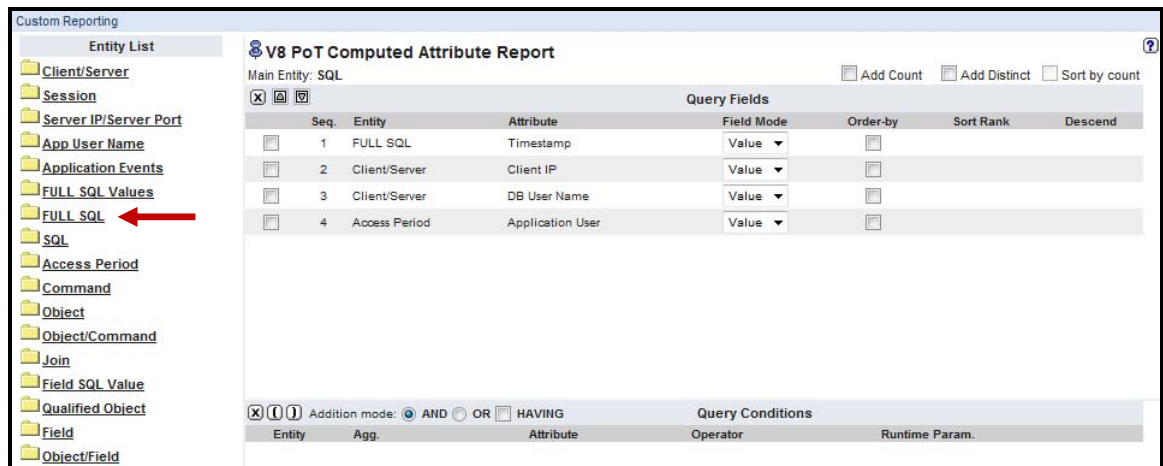
__e. Now select **Access Period** from the *Entity List*.



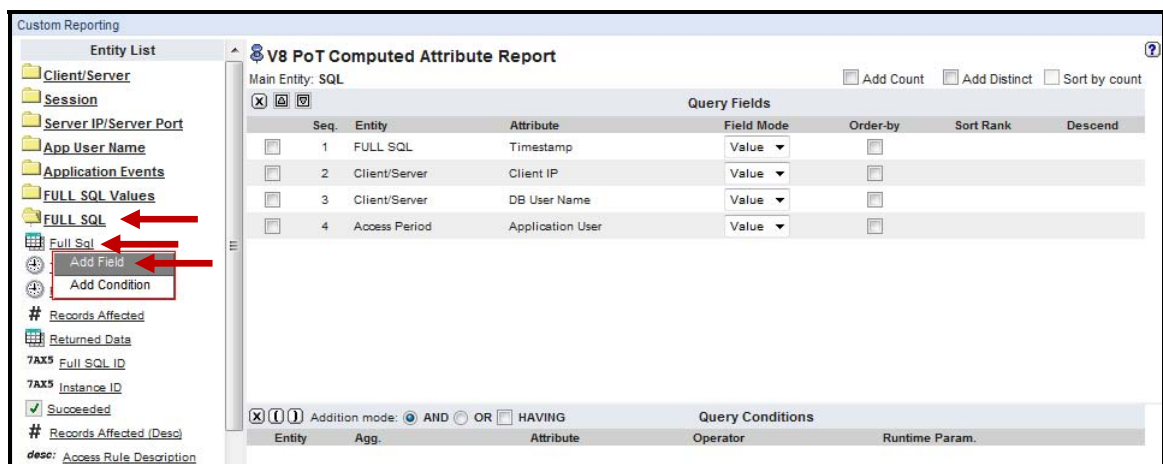
__f. Select the **Application User** attribute from the *Access Period* entity and click **Add Field**. Then, select **Access Period** from the *Entity List* to collapse the **Access Period** folder.



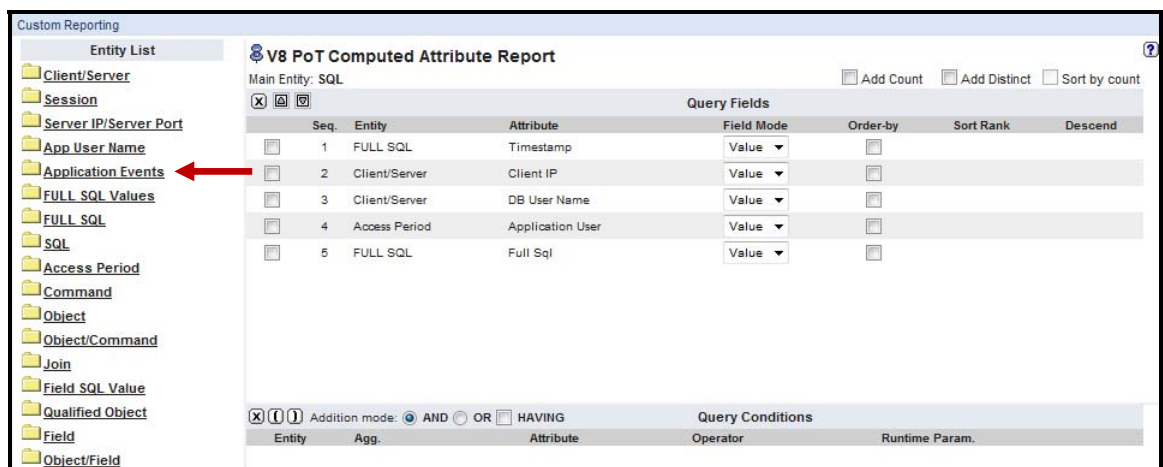
g. Now select **Full SQL** from the *Entity List*.



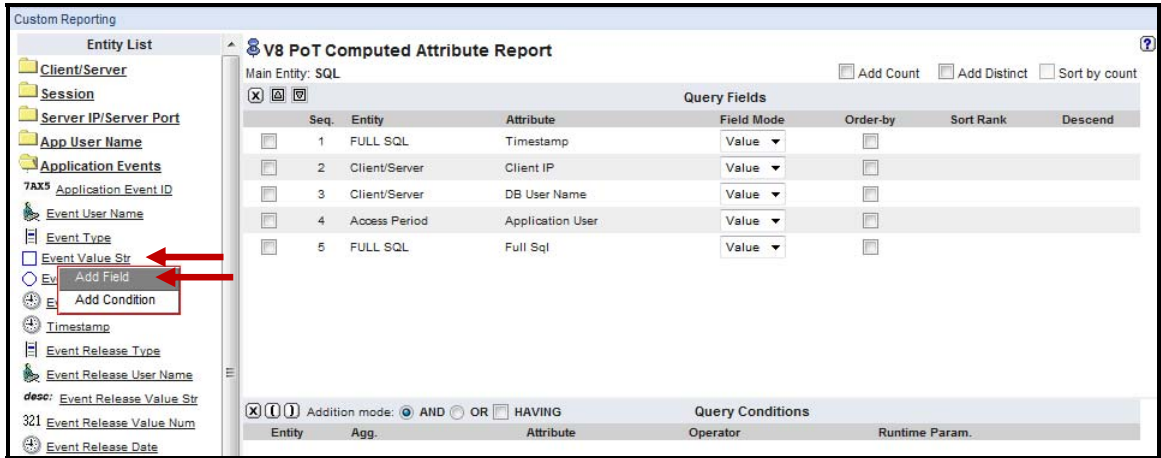
h. Select the **Full Sql** attribute from the *Full SQL* entity and click **Add Field**. Then, select **Full SQL** from the *Entity List* to collapse the **Full SQL** folder.



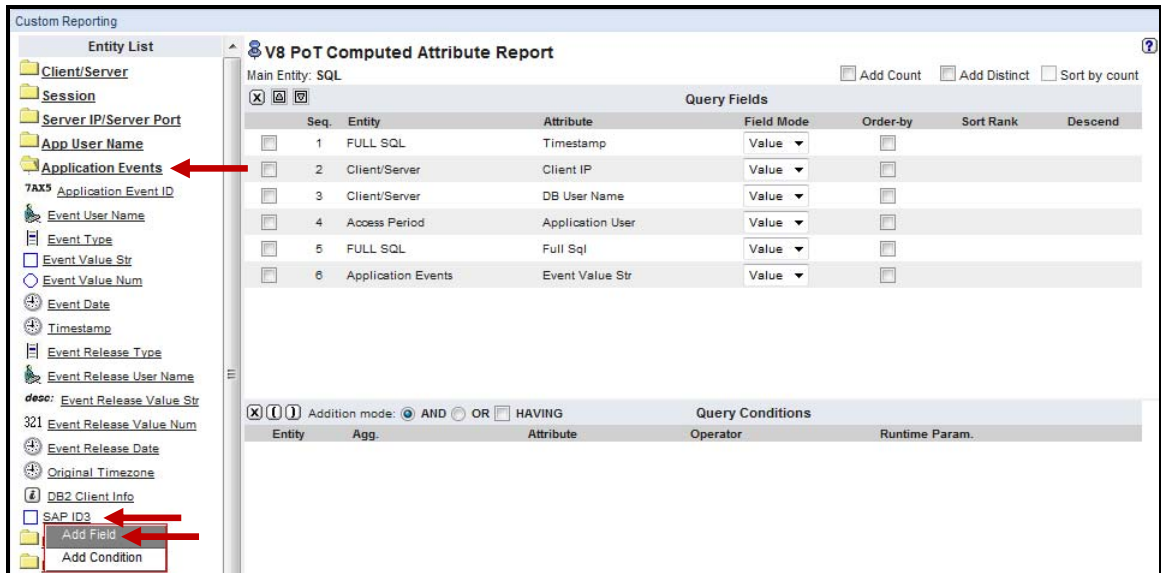
i. Now select **Application Events** from the *Entity List*.



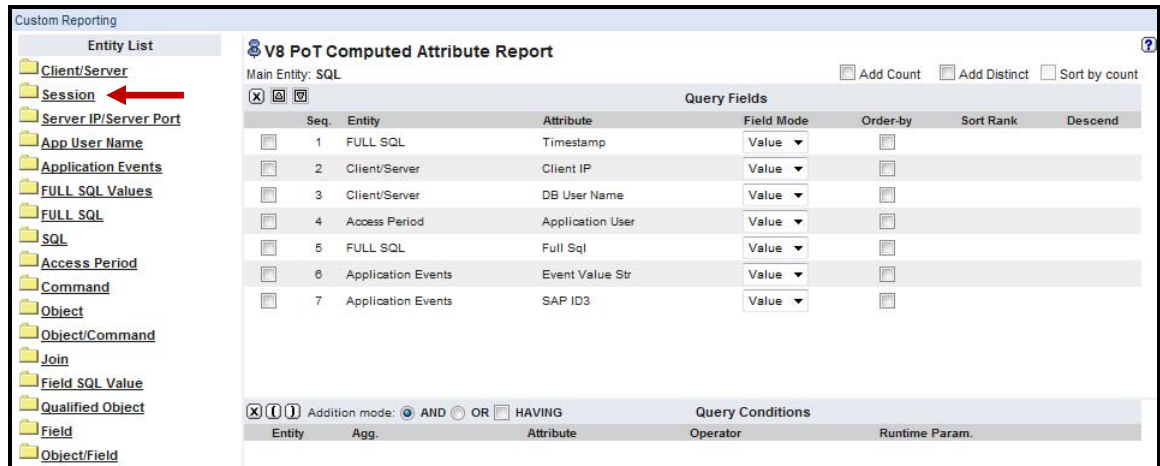
- ___j. Select the **Event Value Str** attribute from the *Application Events* entity and click **Add Field**.



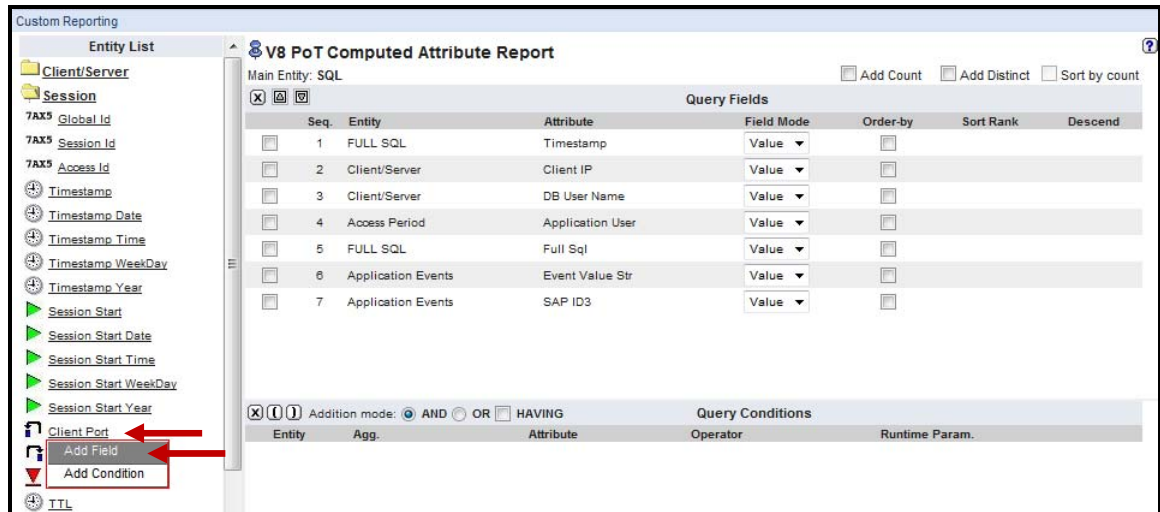
- ___k. Select the newly created **SAP ID3** computed attribute from the *Application Events* entity and click **Add Field**. Then, select **Application Events** from the *Entity List* to collapse the **Application Events** folder.



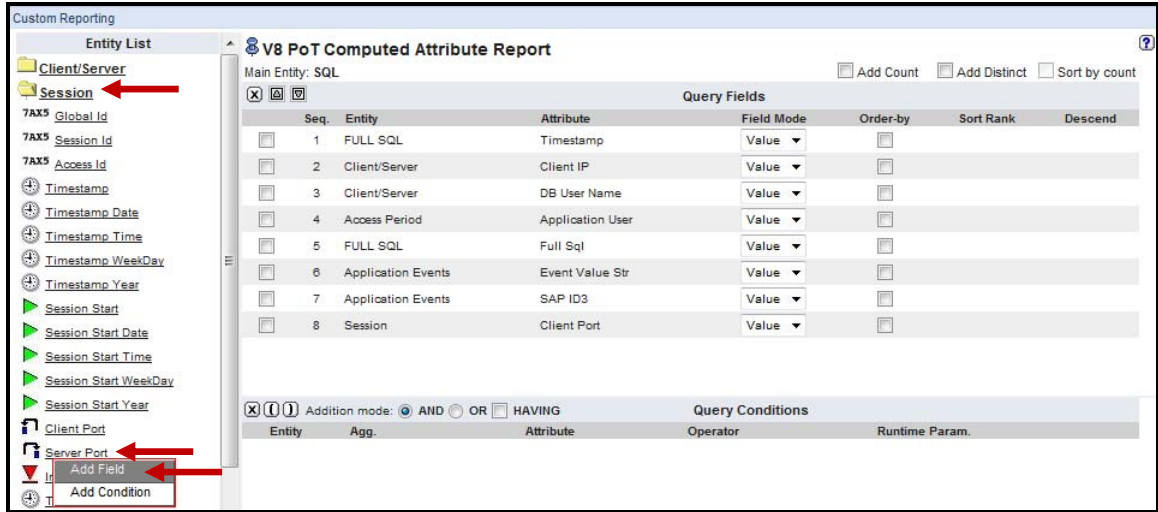
__l. Now, select **Session** from the *Entity List*.



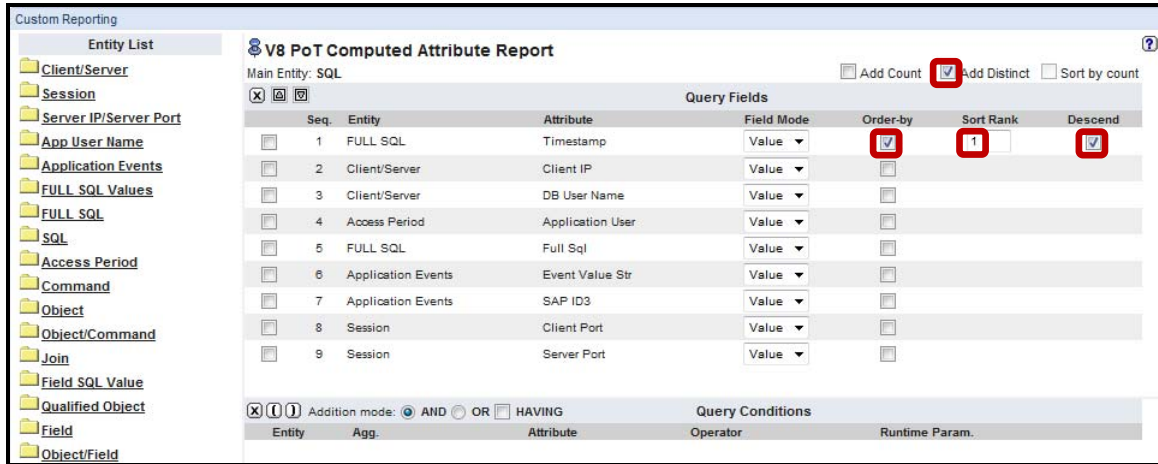
__m. Select the **Client Port** attribute from the *Session* entity and click **Add Field**.



- n. Select the **Server Port** attribute from the *Session* entity and click **Add Field**. Then, select **Session** from the *Entity List* to collapse the **Session** folder.

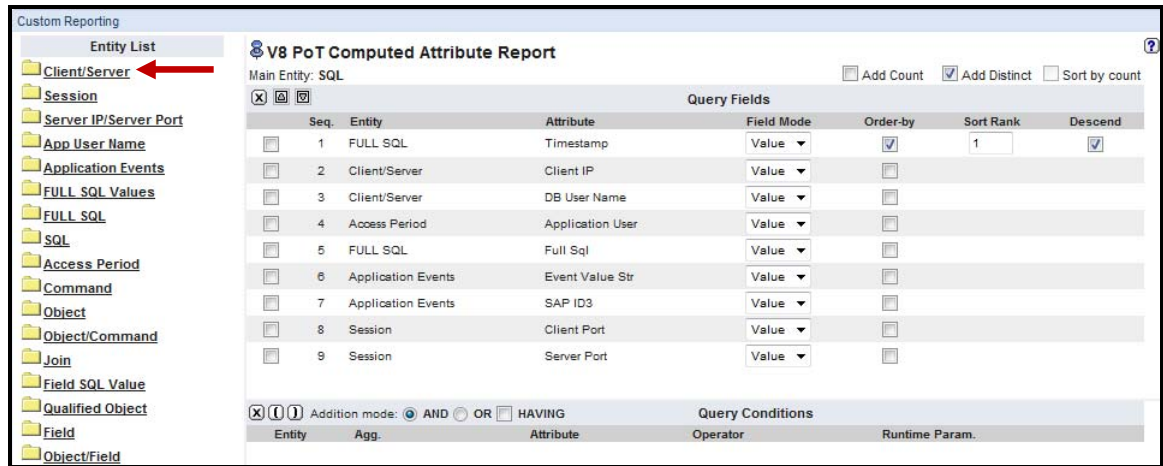


- o. Finally, check the **'Add Distinct'** checkbox at the top right of the screen, then alongside the **Timestamp** attribute, check the **'Order by'** checkbox, enter **'1'** in the *Sort Rank* dialog box, and then check the **'Descend'** checkbox on the far right.

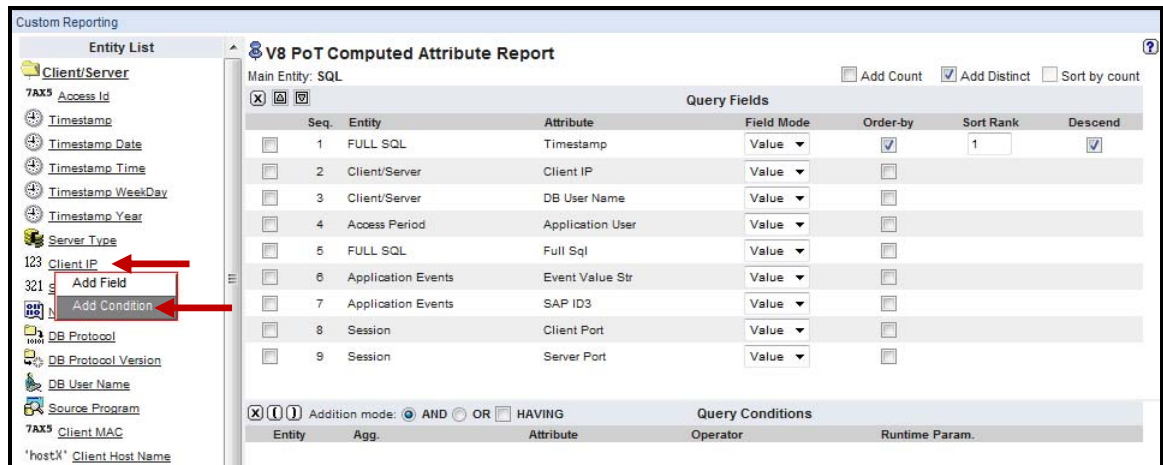


__5. The next few steps will add Custom *Conditions* for the **V8 PoT Computed Attribute Report**.

__a. Now, select **Client/Server** from the *Entity List*.

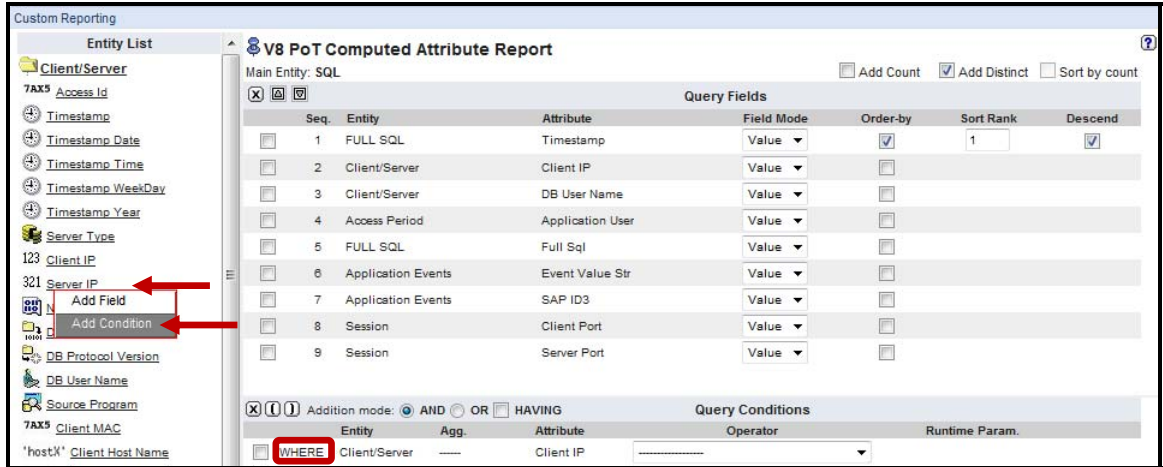


__b. Select the **Client IP** attribute from the *Client/Server* entity and click **Add Condition**.



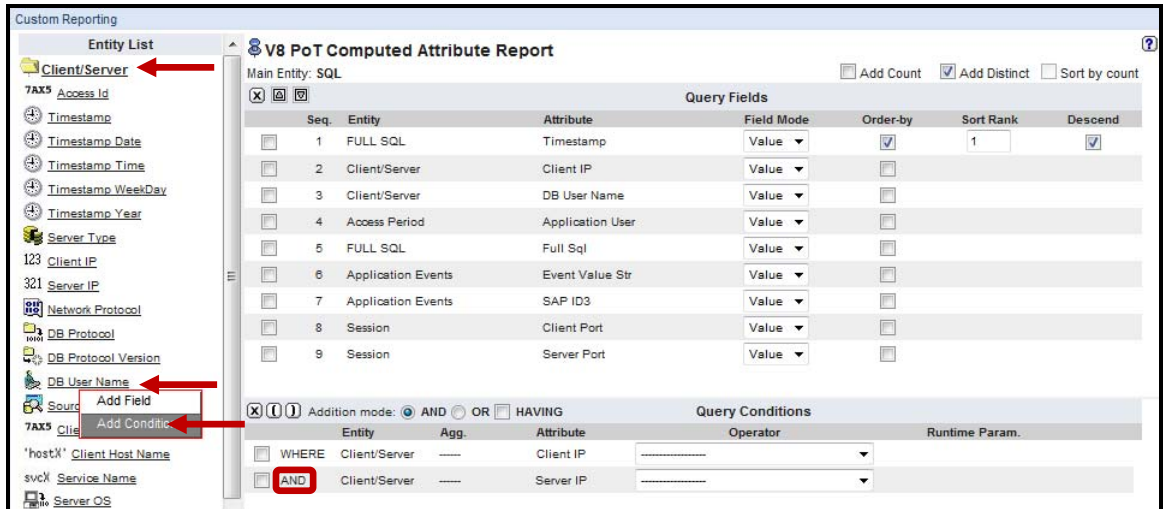
Note: The Query Condition Pane now has the *WHERE* clause with the *Client IP* attribute. We will be updating these clause parameters shortly.

- a. Select the **Server IP** attribute from the *Client/Server* entity and click **Add Condition**.



Note: The Query Condition Pane now has an 'AND' condition for the *Server IP* attribute.

- b. Select the **DB User Name** attribute from the *Client/Server* entity and click **Add Condition**. Then, select **Client/Server** from the *Entity List* to collapse the **Client/Server** folder.



c. Now, select **Access Period** from the *Entity List*.

Custom Reporting

Entity List

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

V8 PoT Computed Attribute Report

Main Entity: SQL

Query Fields

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
1	FULL SQL	Timestamp	Value	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>
2	Client/Server	Client IP	Value	<input type="checkbox"/>		
3	Client/Server	DB User Name	Value	<input type="checkbox"/>		
4	Access Period	Application User	Value	<input type="checkbox"/>		
5	FULL SQL	Full Sql	Value	<input type="checkbox"/>		
6	Application Events	Event Value Str	Value	<input type="checkbox"/>		
7	Application Events	SAP ID3	Value	<input type="checkbox"/>		
8	Session	Client Port	Value	<input type="checkbox"/>		
9	Session	Server Port	Value	<input type="checkbox"/>		

Query Conditions

Entity	Agg.	Attribute	Operator	Runtime Param.
WHERE Client/Server	----	Client IP	-----	
AND Client/Server	----	Server IP	-----	
AND Client/Server	----	DB User Name	-----	

d. Select the **Application User** attribute from the *Access Period* entity and click **Add Condition**. Then, select **Access Period** from the *Entity List* to collapse the **Access Period** folder.

Custom Reporting

Entity List

- Client/Server
- Session
- Server IP/Server Port
- App User Name
- Application Events
- FULL SQL Values
- FULL SQL
- SQL
- 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
 - Aver
 - Fail

V8 PoT Computed Attribute Report

Main Entity: SQL

Query Fields

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
1	FULL SQL	Timestamp	Value	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>
2	Client/Server	Client IP	Value	<input type="checkbox"/>		
3	Client/Server	DB User Name	Value	<input type="checkbox"/>		
4	Access Period	Application User	Value	<input type="checkbox"/>		
5	FULL SQL	Full Sql	Value	<input type="checkbox"/>		
6	Application Events	Event Value Str	Value	<input type="checkbox"/>		
7	Application Events	SAP ID3	Value	<input type="checkbox"/>		
8	Session	Client Port	Value	<input type="checkbox"/>		
9	Session	Server Port	Value	<input type="checkbox"/>		

Query Conditions

Entity	Agg.	Attribute	Operator	Runtime Param.
WHERE Client/Server	----	Client IP	-----	
AND Client/Server	----	Server IP	-----	
AND Client/Server	----	DB User Name	-----	

__e. Now, select **Full SQL** from the *Entity List*.

Custom Reporting
V8 PoT Computed Attribute Report
 Main Entity: SQL Add Count Add Distinct Sort by count

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	FULL SQL	Timestamp	Value <input type="checkbox"/>	<input checked="" type="checkbox"/>	1 <input type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Client IP	Value <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	3	Client/Server	DB User Name	Value <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	4	Access Period	Application User	Value <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	5	FULL SQL	Full Sql	Value <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	6	Application Events	Event Value Str	Value <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	7	Application Events	SAP ID3	Value <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	8	Session	Client Port	Value <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	9	Session	Server Port	Value <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Entity List (Left): Client/Server, Session, Server IP/Server Port, App User Name, Application Events, FULL SQL Values, **FULL SQL**, SQL, Access Period, Command, Object, Object/Command, Join, Field SQL Value, Qualified Object, Field, Object/Field.

Query Conditions (Bottom):
 Addition mode: AND OR HAVING
 WHERE Client/Server Client IP
 AND Client/Server Server IP
 AND Client/Server DB User Name
 AND Access Period Application User

__f. Select the **Full Sql** attribute from the *Full SQL* entity and click **Add Condition**. Then, select **Full SQL** from the *Entity List* to collapse the **Full SQL** folder.

Custom Reporting
V8 PoT Computed Attribute Report
 Main Entity: SQL Add Count Add Distinct Sort by count

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	FULL SQL	Timestamp	Value <input type="checkbox"/>	<input checked="" type="checkbox"/>	1 <input type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Client IP	Value <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	3	Client/Server	DB User Name	Value <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	4	Access Period	Application User	Value <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	5	FULL SQL	Full Sql	Value <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	6	Application Events	Event Value Str	Value <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	7	Application Events	SAP ID3	Value <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	8	Session	Client Port	Value <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	9	Session	Server Port	Value <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Entity List (Left): Client/Server, Session, Server IP/Server Port, App User Name, Application Events, FULL SQL Values, **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.

Query Conditions (Bottom):
 Addition mode: AND OR HAVING
 WHERE Client/Server Client IP
 AND Client/Server Server IP
 AND Client/Server DB User Name
 AND Access Period Application User

g. Now, select **Application Events** from the *Entity List*.

The screenshot shows the 'Custom Reporting' interface for a report titled 'V8 PoT Computed Attribute Report'. On the left, the 'Entity List' is expanded to show 'Application Events', which is highlighted with a red arrow. The main area displays a table of 'Query Fields' with columns for Seq., Entity, Attribute, Field Mode, Order-by, Sort Rank, and Descend. The table contains 9 rows of fields. Below the table, there are options for 'Addition mode' (AND, OR, HAVING) and a 'Query Conditions' section with a table for adding conditions.

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
1	FULL SQL	Timestamp	Value	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>
2	Client/Server	Client IP	Value	<input type="checkbox"/>		
3	Client/Server	DB User Name	Value	<input type="checkbox"/>		
4	Access Period	Application User	Value	<input type="checkbox"/>		
5	FULL SQL	Full Sql	Value	<input type="checkbox"/>		
6	Application Events	Event Value Str	Value	<input type="checkbox"/>		
7	Application Events	SAP ID3	Value	<input type="checkbox"/>		
8	Session	Client Port	Value	<input type="checkbox"/>		
9	Session	Server Port	Value	<input type="checkbox"/>		

h. Select the **Event Value Str** attribute from the *Application Events* entity and click **Add Condition**. Then, select **Application Events** from the *Entity List* to collapse the **Application Events** folder.

The screenshot shows the 'Custom Reporting' interface after selecting the 'Event Value Str' attribute. The 'Entity List' on the left is expanded to show 'Application Events' and its sub-items, with 'Event Value Str' selected and highlighted by a red arrow. The 'Add Condition' button is also highlighted with a red arrow. The 'Query Fields' table remains the same as in the previous screenshot.

__6. The next few steps will configure *Query Conditions Operators and Runtime Parameters* for the **V8 PoT Computed Attribute Report**.

__a. Select **LIKE** from the *Query Conditions Operator* dropdown for each of the *Query Conditions*. You can also type 'L' to quickly select.

The screenshot shows the 'Custom Reporting' interface for the 'V8 PoT Computed Attribute Report'. On the left is an 'Entity List' tree. The main area is divided into 'Query Fields' and 'Query Conditions' sections.

Query Fields Table:

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	FULL SQL	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	Client/Server	DB User Name	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	4	Access Period	Application User	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	5	FULL SQL	Full Sql	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	6	Application Events	Event Value Str	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	7	Application Events	SAP ID3	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	8	Session	Client Port	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	9	Session	Server Port	Value	<input type="checkbox"/>	<input type="checkbox"/>

Query Conditions Table:

Entity	Agg.	Attribute	Operator	Runtime Param.
<input type="checkbox"/>	WHERE	Client/Server	-----	Client IP
<input type="checkbox"/>	AND	Client/Server	-----	Server IP
<input type="checkbox"/>	AND	Client/Server	-----	DB User Name
<input type="checkbox"/>	AND	Access Period	-----	Application User
<input type="checkbox"/>	AND	FULL SQL	-----	Full Sql
<input type="checkbox"/>	AND	Application Events	-----	Event Value Str

The 'Operator' dropdown menu is open, showing a list of operators. 'LIKE' is highlighted with a blue bar and a red arrow points to it. Other operators include '<', '<=', '<>', '=', '>', '>=', 'CATEGORIZED AS', 'CLASSIFIED AS', 'IN ALIASES GROUP', 'IN DYNAMIC ALIASES GROUP', 'IN DYNAMIC GROUP', 'IN GROUP', 'IS NOT NULL', 'IS NULL', 'LIKE GROUP', 'NOT IN ALIASES GROUP', 'NOT IN DYNAMIC ALIASES GROUP', 'NOT IN DYNAMIC GROUP', 'NOT IN GROUP', 'NOT LIKE', 'NOT REGEXP', and 'REGEXP'.

b. Make sure the **LIKE** operator is now reflected for each of the *Query Conditions*.

Custom Reporting

Entity List

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

V8 PoT Computed Attribute Report

Main Entity: SQL Add Count Add Distinct Sort by count

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	FULL SQL	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	Client/Server	DB User Name	Value	<input type="checkbox"/>	
<input type="checkbox"/>	4	Access Period	Application User	Value	<input type="checkbox"/>	
<input type="checkbox"/>	5	FULL SQL	Full Sql	Value	<input type="checkbox"/>	
<input type="checkbox"/>	6	Application Events	Event Value Str	Value	<input type="checkbox"/>	
<input type="checkbox"/>	7	Application Events	SAP ID3	Value	<input type="checkbox"/>	
<input type="checkbox"/>	8	Session	Client Port	Value	<input type="checkbox"/>	
<input type="checkbox"/>	9	Session	Server Port	Value	<input type="checkbox"/>	

Addition mode: AND OR HAVING

Entity	Agg.	Attribute	Operator	Runtime Param.
<input type="checkbox"/> WHERE	Client/Server	Client IP	LIKE	Value
<input type="checkbox"/> AND	Client/Server	Server IP	LIKE	Value
<input type="checkbox"/> AND	Client/Server	DB User Name	LIKE	Value
<input type="checkbox"/> AND	Access Period	Application User	LIKE	Value
<input type="checkbox"/> AND	FULL SQL	Full Sql	LIKE	Value
<input type="checkbox"/> AND	Application Events	Event Value Str	LIKE	Value

c. Now, select **Parameter** from the *Runtime Param.* dropdown for each of the *Query Conditions*. You can also type 'P' to quickly select.

Custom Reporting

Entity List

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

V8 PoT Computed Attribute Report

Main Entity: SQL Add Count Add Distinct Sort by count

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	FULL SQL	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	Client/Server	DB User Name	Value	<input type="checkbox"/>	
<input type="checkbox"/>	4	Access Period	Application User	Value	<input type="checkbox"/>	
<input type="checkbox"/>	5	FULL SQL	Full Sql	Value	<input type="checkbox"/>	
<input type="checkbox"/>	6	Application Events	Event Value Str	Value	<input type="checkbox"/>	
<input type="checkbox"/>	7	Application Events	SAP ID3	Value	<input type="checkbox"/>	
<input type="checkbox"/>	8	Session	Client Port	Value	<input type="checkbox"/>	
<input type="checkbox"/>	9	Session	Server Port	Value	<input type="checkbox"/>	

Addition mode: AND OR HAVING

Entity	Agg.	Attribute	Operator	Runtime Param.
<input type="checkbox"/> WHERE	Client/Server	Client IP	LIKE	Value
<input type="checkbox"/> AND	Client/Server	Server IP	LIKE	Parameter
<input type="checkbox"/> AND	Client/Server	DB User Name	LIKE	Attribute
<input type="checkbox"/> AND	Access Period	Application User	LIKE	Value
<input type="checkbox"/> AND	FULL SQL	Full Sql	LIKE	Value
<input type="checkbox"/> AND	Application Events	Event Value Str	LIKE	Value

__d. Verify that all Runtime Parameters are set to 'Parameter'.

Custom Reporting

Entity List

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

V8 PoT Computed Attribute Report

Main Entity: SQL Add Count Add Distinct Sort by count

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	FULL SQL	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	Client/Server	DB User Name	Value	<input type="checkbox"/>	
<input type="checkbox"/>	4	Access Period	Application User	Value	<input type="checkbox"/>	
<input type="checkbox"/>	5	FULL SQL	Full Sql	Value	<input type="checkbox"/>	
<input type="checkbox"/>	6	Application Events	Event Value Str	Value	<input type="checkbox"/>	
<input type="checkbox"/>	7	Application Events	SAP ID3	Value	<input type="checkbox"/>	
<input type="checkbox"/>	8	Session	Client Port	Value	<input type="checkbox"/>	
<input type="checkbox"/>	9	Session	Server Port	Value	<input type="checkbox"/>	

Query Conditions

Entity Agg. Attribute Operator Runtime Param.

<input type="checkbox"/>	WHERE	Client/Server	Client IP	LIKE	Parameter	
<input type="checkbox"/>	AND	Client/Server	Server IP	LIKE	Parameter	
<input type="checkbox"/>	AND	Client/Server	DB User Name	LIKE	Parameter	
<input type="checkbox"/>	AND	Access Period	Application User	LIKE	Parameter	
<input type="checkbox"/>	AND	FULL SQL	Full Sql	LIKE	Parameter	
<input type="checkbox"/>	AND	Application Events	Event Value Str	LIKE	Parameter	

__e. Now, add a meaningful name for each **Runtime Parameter** using only alphanumeric characters and no spaces. The names are to the right of the *Runtime Param.* list.

__f. Click **Save** and click **Add to My New Reports** to add it to the **My New Reports** pane.

Custom Reporting

Entity List

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

V8 PoT Computed Attribute Report

Main Entity: SQL Add Count Add Distinct Sort by count

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	FULL SQL	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	Client/Server	DB User Name	Value	<input type="checkbox"/>	
<input type="checkbox"/>	4	Access Period	Application User	Value	<input type="checkbox"/>	
<input type="checkbox"/>	5	FULL SQL	Full Sql	Value	<input type="checkbox"/>	
<input type="checkbox"/>	6	Application Events	Event Value Str	Value	<input type="checkbox"/>	
<input type="checkbox"/>	7	Application Events	SAP ID3	Value	<input type="checkbox"/>	
<input type="checkbox"/>	8	Session	Client Port	Value	<input type="checkbox"/>	
<input type="checkbox"/>	9	Session	Server Port	Value	<input type="checkbox"/>	

Query Conditions

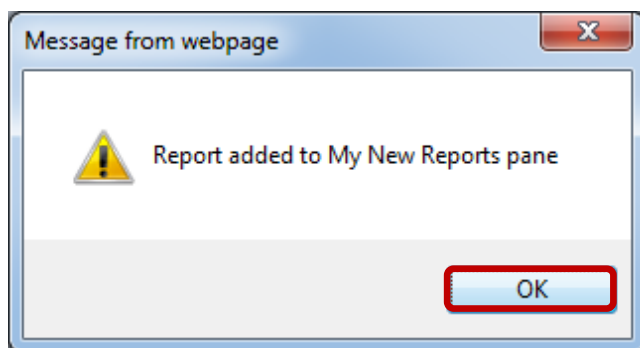
Entity Agg. Attribute Operator Runtime Param.

<input type="checkbox"/>	WHERE	Client/Server	Client IP	LIKE	Parameter	ClientIP
<input type="checkbox"/>	AND	Client/Server	Server IP	LIKE	Parameter	ServerIP
<input type="checkbox"/>	AND	Client/Server	DB User Name	LIKE	Parameter	DBUser
<input type="checkbox"/>	AND	Access Period	Application User	LIKE	Parameter	AppUser
<input type="checkbox"/>	AND	FULL SQL	Full Sql	LIKE	Parameter	FullSql
<input type="checkbox"/>	AND	Application Events	Event Value Str	LIKE	Parameter	EventValStr

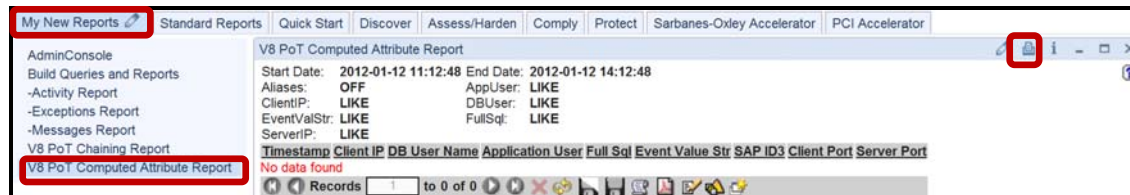
Buttons: Delete, Clone, Roles..., **Save**, Back

Buttons: Generate Tabular, Regenerate, Add to Pane..., **Add to My New Reports**

- __g. Click **OK** to acknowledge the report has been added to the **My New Reports** pane.



- __h. Click **My New Reports** tab, and then select the newly created **V8 PoT Computed Attribute Report**.
- __i. Click the **Pencil** icon to edit the report.



Note: The Parameter Names are reflected under Run Time Parameters.

- j. Type the '%' character (match all) in each 'LIKE' clause, enter 'Now -2 DAY' for QUERY_FROM_DATE, 'NOW +1 DAY' for QUERY_TO_DATE, and click **Update**.

Customize Portlet

Report: **V8 PoT Computed Attribute Report** Based on Query: **V8 PoT Computed Attribute Report**

Title:

Run Time Parameters

AppUser
 Enter value for Application User

ClientIP
 Enter value for Client IP

DBUser
 Enter value for DB User Name

EventValStr
 Enter value for Event Value Str

FullSql
 Enter value for Full Sql

QUERY_FROM_DATE
 Enter Period From

QUERY_TO_DATE
 Enter Period To

REMOTE_SOURCE
 Remote Data Source

ServerIP
 Enter value for Server IP

SHOW_ALIASES On Off Default
 Show Aliases

Presentation Parameters

fetchSize
 Max. records per page

refreshRate
 Refresh rate (seconds)

__7. Compare the results with and without a computed attribute.

Note: The following reports reference historical data to demonstrate the benefits of making use of computed attributes.

The GrdAPI Computed Attribute feature creates a new attribute generally designed to contain a subset of an existing attribute within a specified Entity.

The new report includes the **SAP ID3** computed attribute in the Application Events Entity.

Timestamp	Client IP	Server IP	DB User Name	Application User	Full Sql	Event Value Str	SAP ID3
2011-05-11 10:38:39.0	9.70.147.1069	70.147.106	SAPE6A	LARRY	SELECT * FROM "SBAON_CCHK" WHERE "MANDT" = ? AND "MANDT" = '1970-01-01-00.00.000000' WITH UR -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLSR11 , 788) -- SYSTEM(E6A , SAPE6A)	APPLNAME=SE54; ACCTNG=SQL09010NT SE54 LARRY ,X'08', SAPLSD41	SE54
2011-05-11 10:37:59.0	9.70.147.1069	70.147.106	SAPE6A	LARRY	SET CLIENT ACCTNG 'SQL09010NT SE54 LARRY ,X'08',SAPLSD41'	APPLNAME=SE54; ACCTNG=SQL09010NT SE54 LARRY ,X'08', SAPLSD41	SE54

Records 1 to 2 of 285

The **SAP Transaction Code (SE54)** is embedded in the **Event_Value_Str** attribute in any reports not using the computed attribute.

Timestamp	Client IP	Server IP	DB User Name	Application User	Full Sql	Event Value Str
2011-05-11 10:38:39.0	9.70.147.1069	70.147.106	SAPE6A	LARRY	SELECT * FROM "SBAON_CCHK" WHERE "MANDT" = ? AND "MANDT" = '1970-01-01-00.00.000000' WITH UR -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLSR11 , 788) -- SYSTEM(E6A , SAPE6A)	APPLNAME=SE54; ACCTNG=SQL09010NT SE54 LARRY ,X'08', SAPLSD41
2011-05-11 10:37:59.0	9.70.147.1069	70.147.106	SAPE6A	LARRY	SET CLIENT ACCTNG 'SQL09010NT SE54 LARRY ,X'08',SAPLSD41'	APPLNAME=SE54; ACCTNG=SQL09010NT SE54 LARRY ,X'08', SAPLSD41

Records 1 to 2 of 285

This lab demonstrates how the use of computed attributes can harness the power of InfoSphere Guardium custom reporting enable you to mine additional intelligence from your existing audit data.

Thank You

Custom Reports review

- __1. A handy way to build custom reports is to:
 - __a. Put a dash at the front of the name so it will show up at the top of the list of reports
 - __b. Sort by the timestamp descending, so the most recent record appears at the top
 - __c. Use runtime parameters to allow filtering when viewing the report
 - __d. All of the above

- __2. For query conditions, the "LIKE" and "=" do the same thing. (**True** or **False**).

- __3. The UID Chain is captured in real-time with the audit data. (**True** or **False**).

- __4. When defining a query, the Entity selected controls:
 - __a. Which entity most of the fields will come from
 - __b. Which entity the background SQL will be built to include
 - __c. Which entity the report will be sorted on

- __5. The "Client/Server" entity includes the following attributes:
 - __a. Client IP and Server IP
 - __b. UID Chain
 - __c. Full SQL
 - __d. Session Start Timestamp

Custom Reports review (Answers)

__1. A handy way to build custom reports is to:

D – All of the above.

__2. For query conditions, the "LIKE" and "=" do the same thing.
(True or False).

False. The "Like" operator allows use of a wildcard (%).

__3. The UID Chain is captured in real-time with the audit data.
(True or False).

False. It will take about one or two minutes to be populated.

__4. When defining a query, the Entity selected controls:

B – Which entity the background SQL will be built to include.

__5. The "Client/Server" entity includes the following attributes:

A – Client IP and Server IP.

Lab 6 Policy Builder

6.1 Configuring Alert Policy

Overview

IBM InfoSphere® Guardium® provides real-time controls for responding to unauthorized or anomalous behaviors before they can do significant harm. Policy-based actions can include real-time security alerts (SMTP, SNMP, Syslog); software blocking; full logging; user quarantines; and custom actions such as shutting down VPN ports and coordinating with perimeter IDS/IPS systems.

Objectives

This section will illustrate how we can create a new policy with a rule that will trigger if a privileged user attempts to access a sensitive object.

1. Create a policy.
2. Add an Access Rule to the policy.
3. Specify an Alert action when the rule is triggered.
4. Select a SYSLOG Notification Method.
5. Install the policy.
6. Test the policy.

- __1. Using the InfoSphere Guardium GUI, demonstrate the ease of use within the InfoSphere Guardium solution. Start the InfoSphere Guardium appliance and login.
 - __a. From your laptop, go to to <https://10.10.9.248:8443>
 - __b. Log in as **pot/guardium**.

Login

Please enter your information

User name:

Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

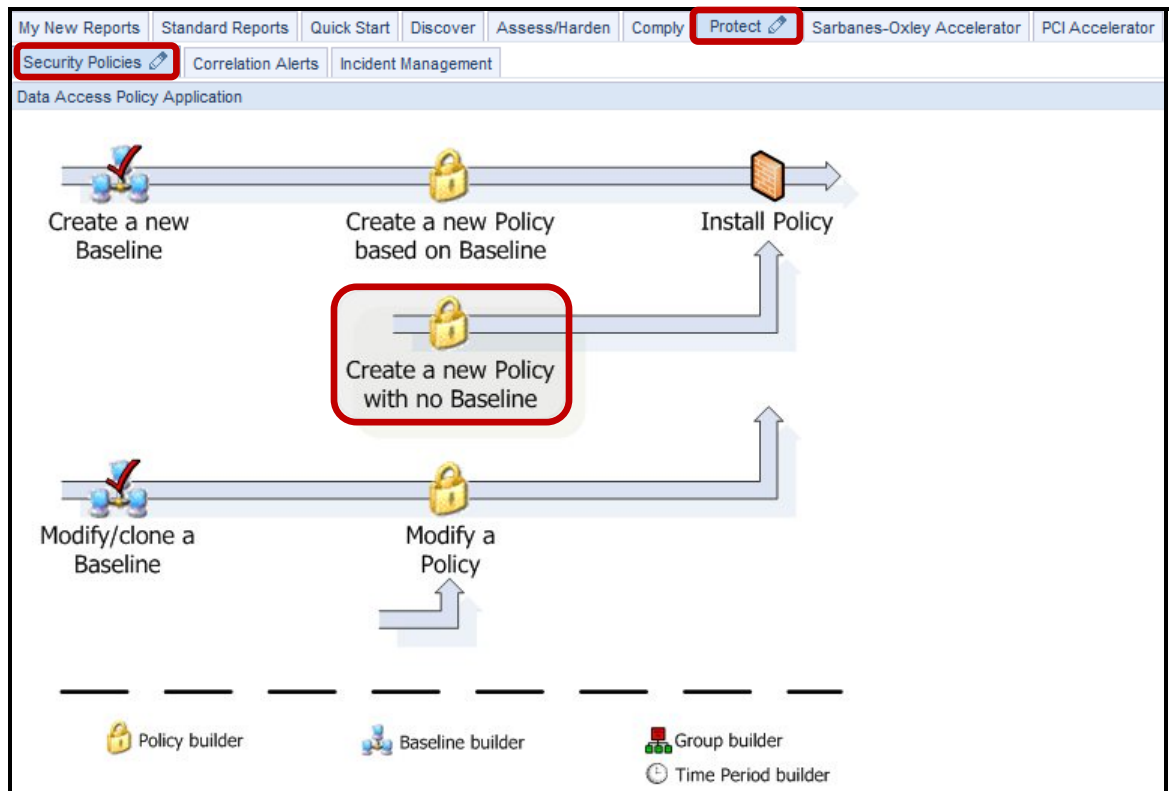
Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistrykey © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

__2. Create a new alert policy to trigger on privileged user access to credit card data.

__a. Click **Security Policies** under the **Protect** tab.

__b. Click **Create a new Policy with no Baseline**.



__c. Enter '**V8 PoT Alert Policy**' for Policy description and click **Apply**.

The screenshot shows the 'Data Access Policy Application' interface. The 'Policy Definition' section is visible, with the 'Policy description' field containing 'V8 PoT Alert Policy'. Other fields include 'Policy category', 'Log flat', 'Rules on flat', 'Selective audit trail', and 'Audit pattern'. The 'Roles' section shows 'No roles have been assigned to this policy' with a 'Roles...' button. At the bottom, there are 'Back', 'Edit Rules...', and 'Apply' buttons, with the 'Apply' button highlighted in red.

__d. Click **Edit Rules**.

The screenshot shows the 'Data Access Policy Application' interface. At the top, there are navigation tabs: 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect' (selected), 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below these are sub-tabs: 'Security Policies' (selected), 'Correlation Alerts', and 'Incident Management'. The main content area is titled 'Data Access Policy Application' and contains a 'Policy Definition' section for 'V8 PoT Alert Policy'. This section includes fields for 'Policy description', 'Policy category', and 'Audit pattern', along with checkboxes for 'Log flat', 'Rules on flat', and 'Selective audit trail'. Below the definition is a 'Roles' section with a message 'No roles have been assigned to this policy' and a 'Roles...' button. At the bottom of the form, there are four buttons: 'Back', 'Add Comments', 'Edit Rules...' (highlighted with a red box), and 'Apply'.

__e. Click **Add Access Rule** to add a rule to the policy.

The first rule will alert when a privileged user attempts to access a sensitive data object containing a 'creditcard' token.

The screenshot shows the 'Data Access Policy Application' interface, now displaying the 'Policy Rules' section for the 'V8 PoT Alert Policy'. The top navigation and sub-tabs are the same as in the previous screenshot. The main content area is titled 'Policy Rules' and shows the policy name 'V8 PoT Alert Policy' with a 'Filter:' dropdown. Below the policy name are several action buttons: 'Expand All', 'Collapse All', 'Select All', 'Unselect All', 'Delete Selected', and 'Copy Rules ...'. The main area is currently empty. At the bottom, there are three buttons for adding rules: 'Add Access Rule...' (highlighted with a red box), 'Add Exception Rule...', and 'Add Extrusion Rule...'. To the right, there is a 'Rule Suggestion' section with a 'Suggest from DB' button and two input fields for 'Rule min. ct.' (set to 0) and 'Object Group min. ct.' (set to 1), with a 'Suggest Rules' button. At the very bottom, there are 'Back' and 'Policy Simulator' buttons.

- f. Enter 'Alert on CreditCard Access' for the Policy Rule Description and select **(Public) Admin Users** from the *DB User Group* drop-down list. This group contains a list of the privileged users we want to audit for this policy.

The screenshot displays the 'Access Rule Definition' configuration page in the IBM InfoSphere Guardium V8.2 interface. The page title is 'Data Access Policy Application'. The rule is identified as 'Rule #1 of policy V8 PoT Alert Policy'. The 'Description' field is filled with 'Alert on CreditCard Access'. The 'Severity' is set to 'INFO'. Below this, there are several configuration sections with checkboxes and input fields: 'Server IP', 'Client IP', 'Client MAC', 'Net Prtcl.', 'DB Type', 'Svc. Name', 'DB Name', 'DB User', 'App. User', 'OS User', 'Src App.', 'Field', 'Object', 'Command', 'Object/Cmd. Group', 'Object/Field Group', 'Pattern', and 'XML Pattern'. The 'DB User' dropdown menu is open, showing a list of user groups. The group '(Public) Admin Users' is selected and highlighted with a blue background and a red arrow pointing to it. Other groups in the list include Functional Users, Privilege Users, Production Users, (Public) Active Users, (Public) Application Schema Users, (Public) Authorized Users, (Public) BASEL Recognized Users, (Public) Data Privacy - Sensitive Data Authorized Admin Users, (Public) Data Privacy - Sensitive Data Authorized Users, (Public) DB Predefined Users, (Public) Oracle Predefined Users, (Public) PCI Admin Users, (Public) PCI Limited Access Users, (Public) SOX Recognized Users, (Public) Suspicious Users, and (Public) Terminated DB Users. At the bottom, there are fields for 'App Event Exists', 'Event Type', 'Event User Name', 'App Event Values' (Text, Numeric, Date), and 'Masking Pattern' (RE, Replacement Character).

- g. Scroll down, enter ‘%creditcard’ in the *Object* field, and then click **Add Action**.

Note: The ‘%’ is a wildcard character. This rule will trigger whenever an object whose name ends with ‘creditcard’ is referenced by a member of the *Admin Users* group.

The screenshot displays the 'Data Access Policy Application' configuration window. The interface includes a top navigation bar with tabs for 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below this, there are sub-tabs for 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main configuration area is divided into several sections:

- Client Information:** Fields for Client MAC, Net Prtcl., DB Type, Svc. Name, DB Name, DB User, and Client IP/Src App./DB User/Server IP/Svc. Name.
- User and Application Information:** Fields for App. User, OS User, Src App., Field, Object, and Command.
- Object/Field Group:** Fields for Object/Field Group, Pattern, and XML Pattern.
- Event Configuration:** Fields for App Event Exists, Event Type, Event User Name, App Event Values (Text, Numeric, Date), Masking Pattern, and Replacement Character.
- Time and Quota Settings:** Fields for Time Period, Minimum Count, Reset Interval, Quarantine for, and Records Affected Threshold.
- Actions:** A section at the bottom with an 'Add Action' button highlighted in red, and 'Back' and 'Save' buttons.

__h. Select **ALERT PER MATCH** from the *ACTION* drop-down list.

The screenshot displays the 'Data Access Policy Application' configuration page. At the top, there are navigation tabs: 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below these are sub-tabs: 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main area is titled 'Data Access Policy Application' and contains various configuration fields. A dropdown menu is open over the 'Action' field, listing several options. The option 'ALERT PER MATCH' is highlighted with a blue background and a red arrow pointing to it. Other options in the menu include 'ALERT DAILY', 'ALERT ONCE PER SESSION', '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', 'QUARANTINE', 'QUICK PARSE', 'RECORD VALUES SEPARATELY', 'S-GATE ATTACH', 'S-GATE DETACH', 'S-GATE TERMINATE', 'S-TAP TERMINATE', and 'SKIP LOGGING'. The 'Action' field itself is currently empty. At the bottom of the page, there are buttons for 'Add Action', 'Back', and 'Save'.

i. Select **SYSLOG** from the *Notification Type* drop-down list, and click **Add**.

The screenshot displays the IBM Security Policy Builder interface. At the top, there are navigation tabs: My New Reports, Standard Reports, Quick Start, Discover, Assess/Harden, Comply, Protect, Sarbanes-Oxley Accelerator, and PCI Accelerator. Below these are sub-tabs: Security Policies, Correlation Alerts, and Incident Management. The main area is titled 'Data Access Policy Application' and contains various configuration fields for defining a policy rule, such as Src App, Field, Object, Command, and various patterns. An 'Add New Action' dialog box is open in the foreground, showing the configuration for an 'ALERT PER MATCH' action. The 'Message Template' is set to 'Default'. The 'Notification Type' dropdown menu is open, showing options: MAIL, SNMP, CUSTM, and SYSLOG. A red arrow points to the 'SYSLOG' option. There are 'Add' and 'Apply' buttons in the dialog, and 'Add Action', 'Back', and 'Save' buttons at the bottom of the main interface.

j. Click **Apply** and then click **Save**.

The screenshot displays the IBM InfoSphere Guardium configuration interface for a Data Access Policy Application. The top navigation bar includes tabs for 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below this, there are sub-tabs for 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main configuration area is titled 'Data Access Policy Application' and contains several sections:

- Object/Command Configuration:** Fields for 'Object' (with a dropdown menu), 'Command', 'Object/Cmd. Group', and 'Object/Field Group'.
- Pattern Configuration:** Fields for 'Pattern' and 'XML Pattern', each with a 'RE' (Regular Expression) icon.
- Event Configuration:** Fields for 'App Event Exists', 'Event Type', 'Event User Name', 'App Event Values' (Text, Numeric, Date), and 'Masking Pattern'.
- Time and Count Configuration:** Fields for 'Time Period', 'Minimum Count', 'Reset Interval', 'Quarantine for', and 'Records Affected Threshold'.
- Actions Section:** A section titled 'Actions' containing a modal window titled 'ALERT PER MATCH'. This modal window has fields for 'Action' (set to 'ALERT PER MATCH'), 'Message Template' (set to 'Default'), and a 'Notification' section with a checked 'Notification Type' of 'SYSLOG' and 'Alert Receiver' of 'SYSLOG'. There is an 'Add' button and an 'Apply' button (highlighted with a red box) in the modal.

At the bottom right of the main configuration area, there are three buttons: 'Add Action', 'Back', and 'Save' (highlighted with a red box).

- __k. Click **Back** to return to the Policy Definition screen.

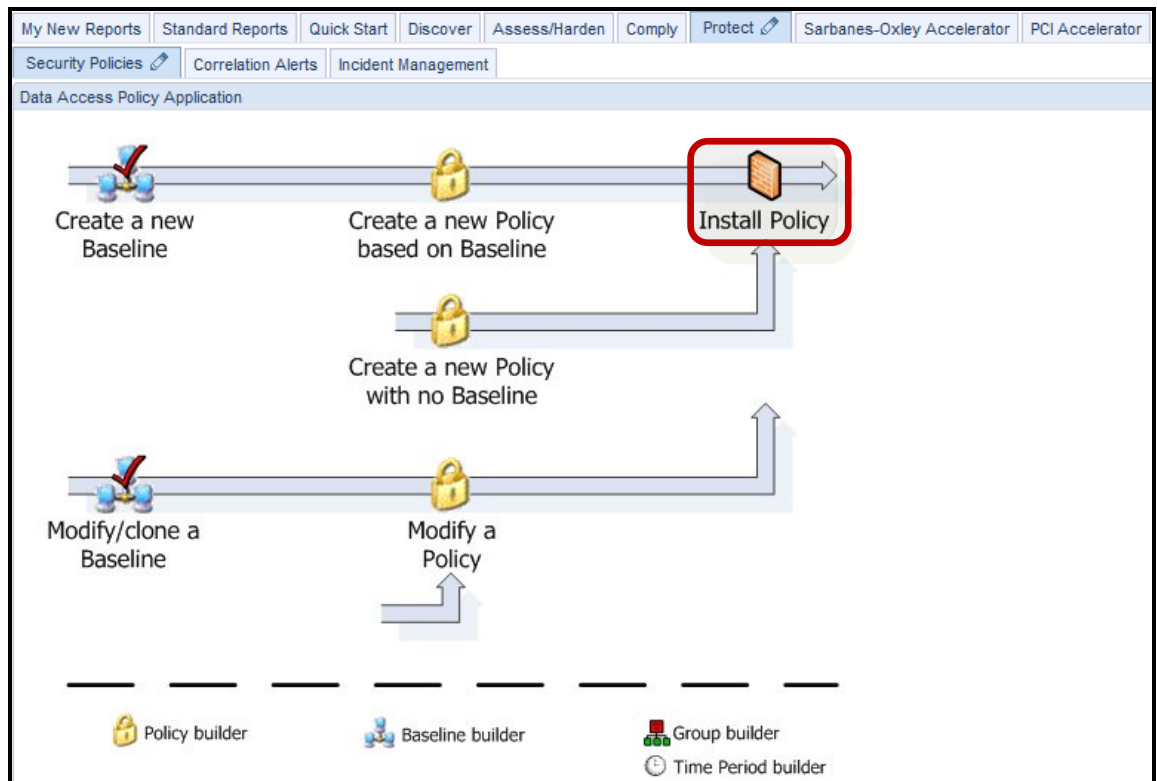
The screenshot shows the 'Data Access Policy Application' interface. At the top, there are navigation tabs: 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below these are sub-tabs: 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main area is titled 'Policy Rules' and displays 'V8 PoT Alert Policy'. A filter dropdown is set to '-----'. Action buttons include 'Expand All', 'Collapse All', 'Select All', 'Unselect All', 'Delete Selected', and 'Copy Rules...'. A list of rules is shown, with one rule: '1 Access Rule: Alert on CreditCard Access'. At the bottom, there are buttons for 'Add Access Rule...', 'Add Exception Rule...', and 'Add Extrusion Rule...'. A 'Rule Suggestion' section includes 'Suggest from DB' and 'Suggest Rules' buttons, with input fields for 'Rule min. ct.' (0) and 'Object Group min. ct.' (1). A 'Back' button is highlighted with a red box, and a 'Policy Simulator' button is visible to its right.

- __l. Click **Back** once more to return to the main **Security Policies** tab screen.

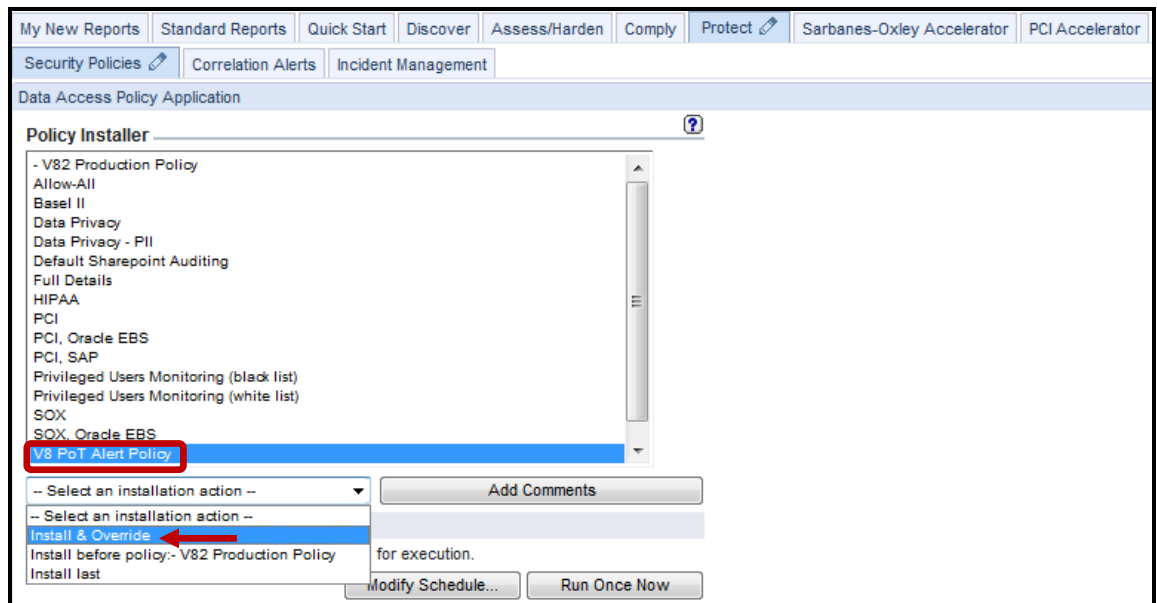
The screenshot shows the 'Data Access Policy Application' interface. At the top, there are navigation tabs: 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below these are sub-tabs: 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main area is titled 'Policy Definition' and displays 'V8 PoT Alert Policy'. The 'Policy description' is 'V8 PoT Alert Policy'. The 'Policy category' is an empty text field. There are checkboxes for 'Log flat', 'Rules on flat', and 'Selective audit trail'. The 'Audit pattern' is an empty text field. Below this is a 'Roles' section with the text 'No roles have been assigned to this policy' and a 'Roles...' button. At the bottom, there are buttons for 'Back', 'Add Comments', 'Edit Rules...', and 'Apply'. The 'Back' button is highlighted with a red box.

__3. Install the V8 PoT Alert Policy.

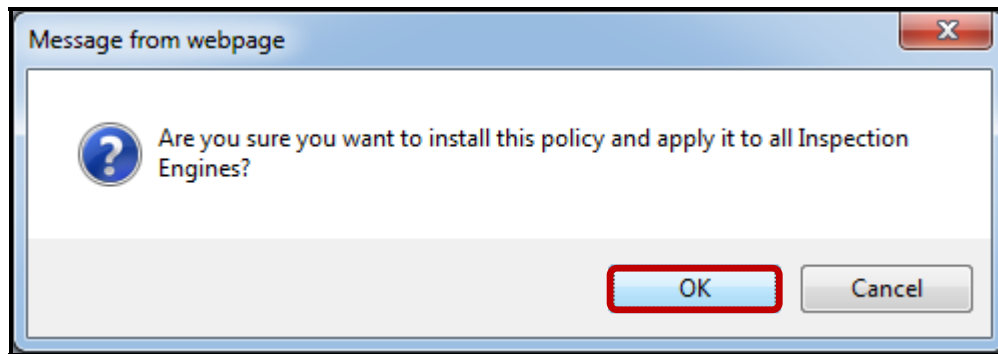
__a. Click **Install Policy**.



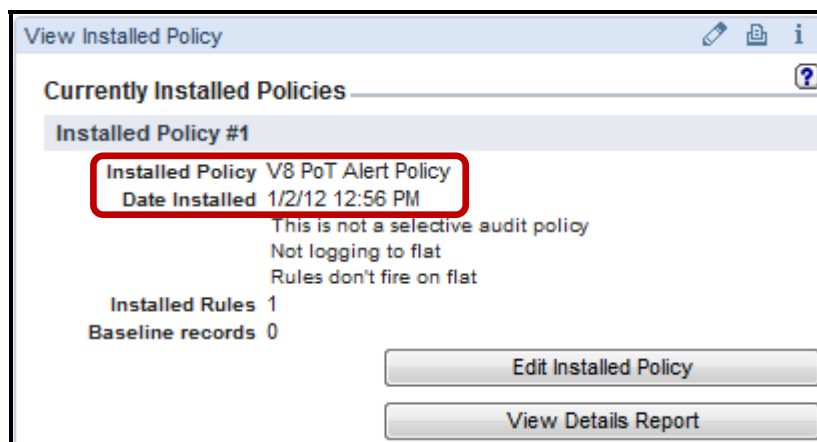
__b. Select '**V8 PoT Alert Policy**' from the *Policy Installer* list, and then select **Install & Override** from the *Select an installation action* drop-down list.



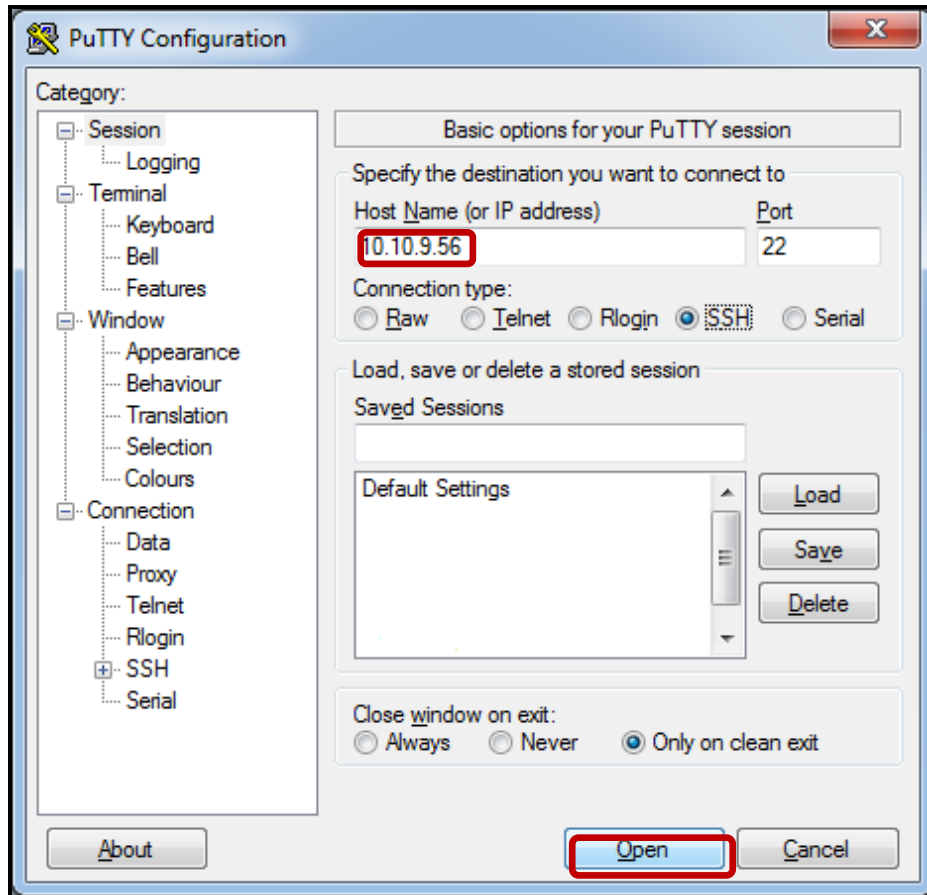
- __c. Click **OK** to acknowledge.



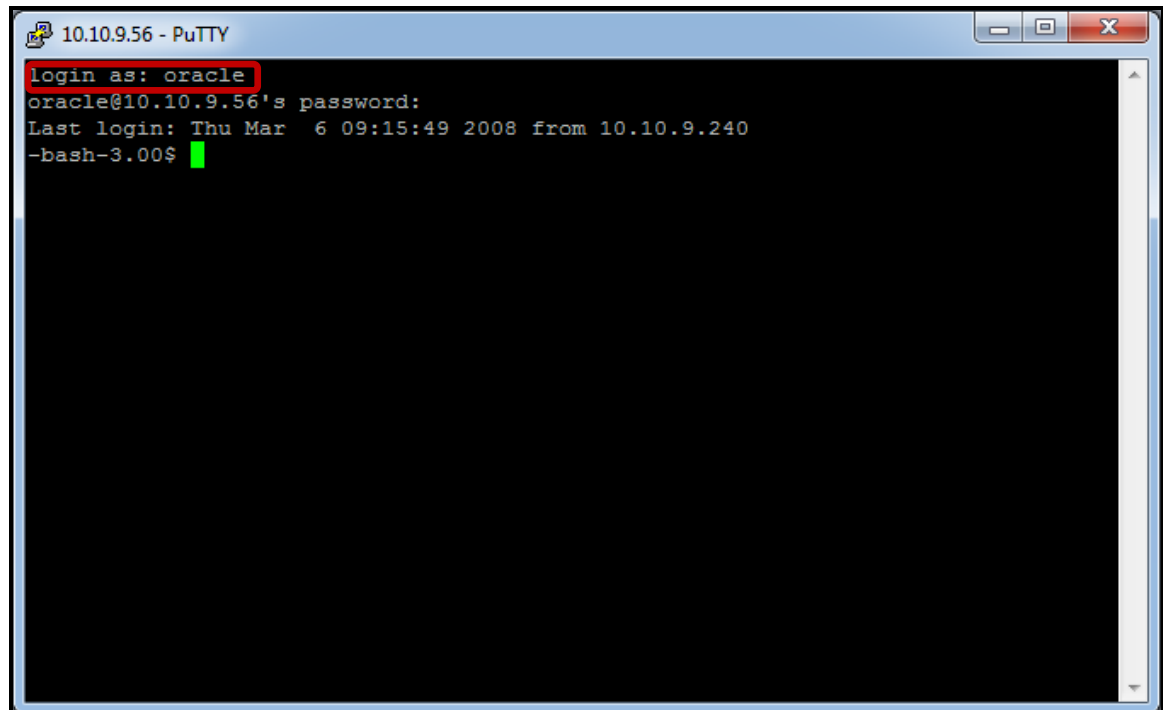
- __d. Check under the *View Installed Policy* section to the upper right of the screen to verify that the **V8 PoT Alert Policy** has been successfully installed.



- __4. Test the V8 PoT Alert Policy.
 - __a. Using a PuTTY SSH client, access the VM database server to demonstrate the InfoSphere Guardium policy capability.
 - __b. Start the PuTTY SSH client login.
 - __c. From your laptop, launch PuTTY, enter **10.10.9.56**, and click **Open**.

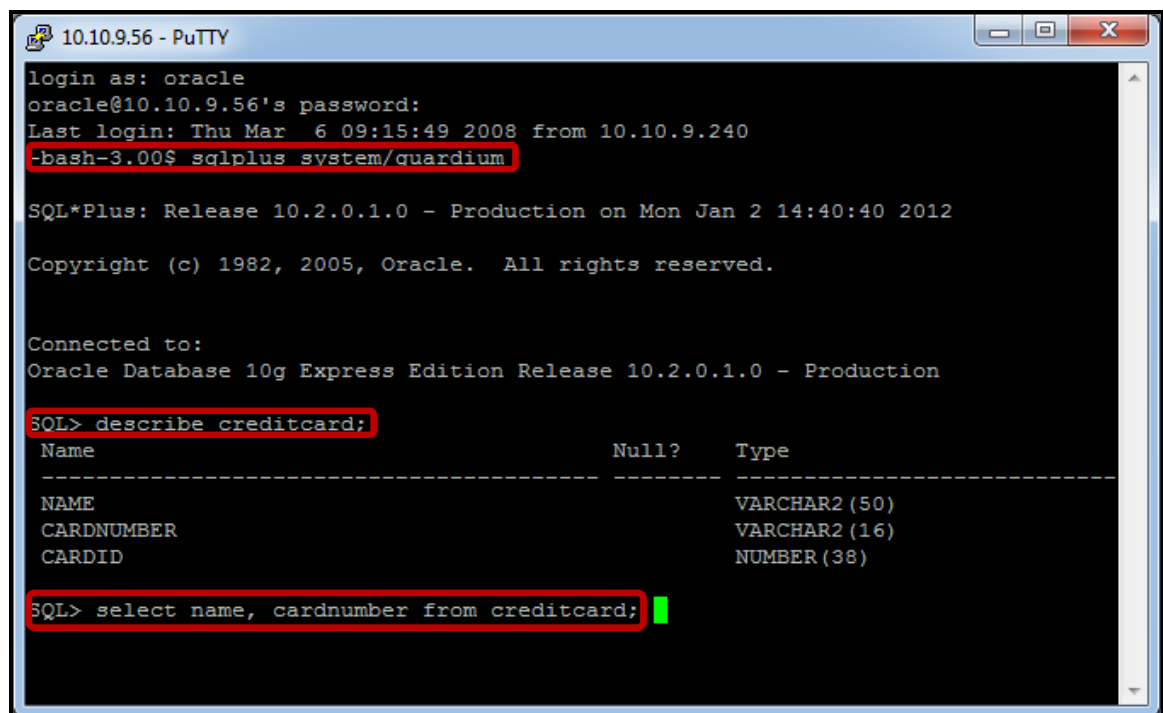


- ___d. Login as **oracle** / **guardium** (Oracle DBA Account). After logging in, the following prompt will be displayed.



```
10.10.9.56 - PuTTY
login as: oracle
oracle@10.10.9.56's password:
Last login: Thu Mar  6 09:15:49 2008 from 10.10.9.240
-bash-3.00$
```

- ___e. Login to Oracle as an admin user by typing: **'sqlplus system/guardium.'**
- ___f. Type **'describe creditcard;'**, then type **'select name, cardnumber from creditcard;'**



```
10.10.9.56 - PuTTY
login as: oracle
oracle@10.10.9.56's password:
Last login: Thu Mar  6 09:15:49 2008 from 10.10.9.240
-bash-3.00$ sqlplus system/guardium

SQL*Plus: Release 10.2.0.1.0 - Production on Mon Jan 2 14:40:40 2012

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

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

SQL> describe creditcard;
Name                               Null?    Type
-----
NAME                                VARCHAR2(50)
CARDNUMBER                          VARCHAR2(16)
CARDID                              NUMBER(38)

SQL> select name, cardnumber from creditcard;
```

- __g. After receiving the result set, type **exit** to exit Oracle sqlplus, and then type **exit** to logout.

```

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

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

SQL> describe creditcard;
Name                                Null?    Type
-----
NAME                                VARCHAR2(50)
CARDNUMBER                          VARCHAR2(16)
CARDID                              NUMBER(38)

SQL> select name, cardnumber from creditcard;

NAME                                CARDNUMBER
-----
Joe D                                1234567890123456
Harry S                              2345678901234567

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

- __h. From the GUI click **Incident Management** under the **Protect** tab to view the *Policy Violations / Incident Management Report* and verify that the alert was actually recorded.

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 Violation
16	2012-01-02 14:43:20.0	Alert on CreditCard Access	10.10.9.56:10.10.9.56:SYSTEM	select name, cardnumber from creditcard	INFO	0	1				
15	2012-01-02 14:41:41.0	Alert on CreditCard Access	10.10.9.56:10.10.9.56:SYSTEM	check_object(creditcard)	INFO	0	1				

We see 2 alerts. One for the **describe** command and the other for the **select** command.

Note: It is possible to associate a color with the severity of the triggered rule. This can be very useful to quickly identify and prioritize critical alerts.

Thank You

Configuring Alert Policy review

- __1. Guardium send the syslog alert message to:
- __a. Database server configuration file
 - __b. Guardium message file
 - __c. S-TAP log file
 - __d. Windows event log file
- __2. Remote syslog is an option to send alert message to:
- __a. SIEM product
 - __b. Guardium message file
 - __c. Windows event log file
 - __d. a and c
- __3. Correlation alerts can send messages to syslog.
(**True** or **False**)
- __4. What is the maximum syslog message size?
- __a. 1,000
 - __b. 2,000
 - __c. 10,000
 - __d. Unlimited
- __5. The Central Manager can view each managed unit's syslog.
(**True** or **False**)

Configuring Alert Policy review (Answers)

__1. Guardium send the syslog alert message to:

B – Guardium message file.

__2. Remote syslog is an option to send alert message to:

D – A (SIEM product) and C (Windows Event Log file).

__3. Correlation alerts can send messages to syslog.
(**True** or **False**)

True.

__4. What is the maximum syslog message size?

B – 2,000.

__5. The Central Manager can view each managed unit's syslog.
(**True** or **False**)

True.

6.2 Configuring Terminate Policy with S-GATE

Overview

The InfoSphere Guardium Data-Level Access Control module simplifies enterprise security with a single set of granular policies for enforcing separation of duties spanning multiple DBMS platforms, without disrupting application access or changing database configurations. It's the only cross-DBMS technology that blocks privileged users, such as DBAs, developers, outsourced personnel and other superusers, from viewing or changing sensitive data. The InfoSphere Guardium Data-Level Access Control module monitors all database connections, including local access by privileged users, by way of non-TCP connections such as Oracle BEQ, SHM, TLI, IPC and others.

Implemented as a lightweight, host-based software agent with fine-grained security policies, the InfoSphere Guardium Data-Level Access Control module provides automated, real-time controls that prevent privileged users from performing unauthorized actions, such as:

- Executing queries on sensitive tables
- Changing sensitive data values
- Adding or deleting critical tables (schema changes) outside change windows
- Creating new user accounts and modifying privileges

The InfoSphere Guardium Data-Level Access Control module is completely non-intrusive, and does not require add-on functionality inside the database. As a result, it is implemented quickly without disrupting business-critical applications such as Oracle E-Business Suite, PeopleSoft, Siebel, SAP, Business Objects and in-house applications.

Objectives

This section of Lab 6 will demonstrate how to build an S-GATE policy with various rules for logging transactions and blocking privileged users (for example, System) from accessing sensitive information like creditcard info. The following steps will guide us through the lab:

- __1. Build a new policy.
- __2. Add a logging rule to the policy.
- __3. Add S-GATE TERMINATE rule to prevent unauthorized access to sensitive PCI objects.
- __4. Install the policy.
- __5. Test S-GATE blocking.

- __1. Start the InfoSphere Guardium appliance and login (if necessary, otherwise skip ahead).
 - __a. From your laptop, go to to <https://10.10.9.248:8443>
 - __b. Login as **pot / guardium**.

Login

Please enter your information

User name:

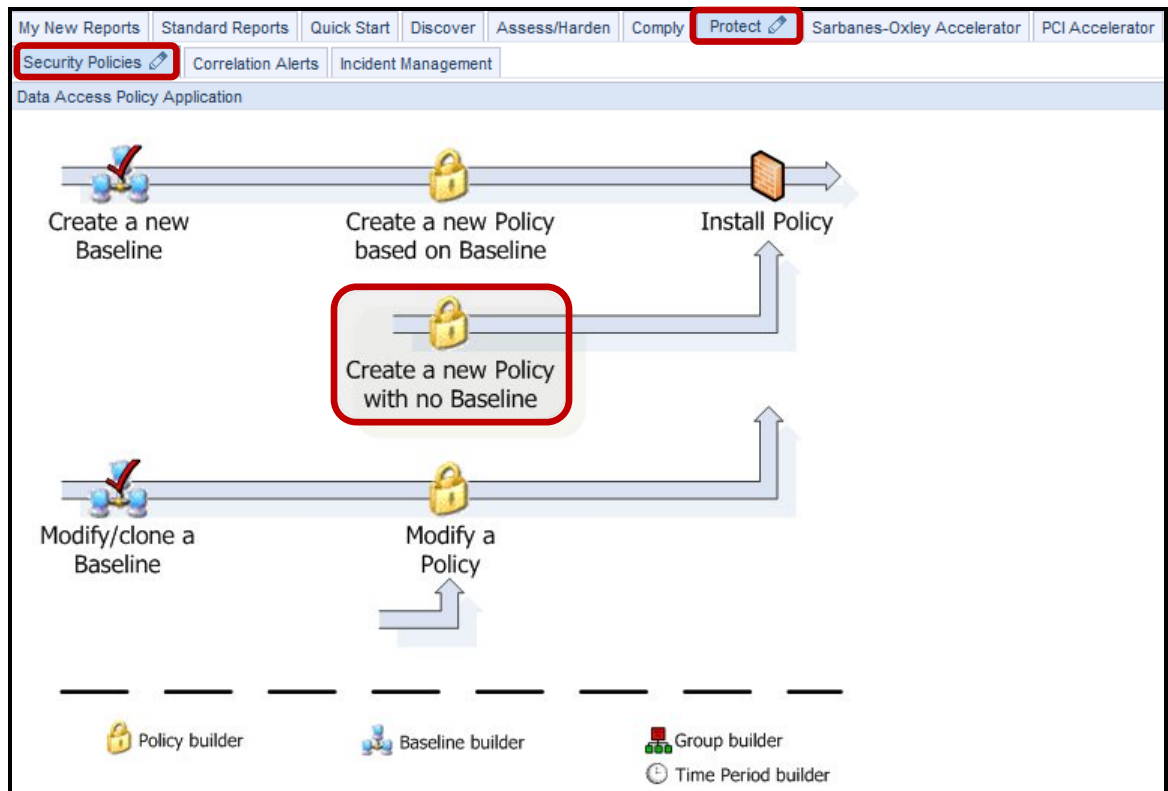
Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

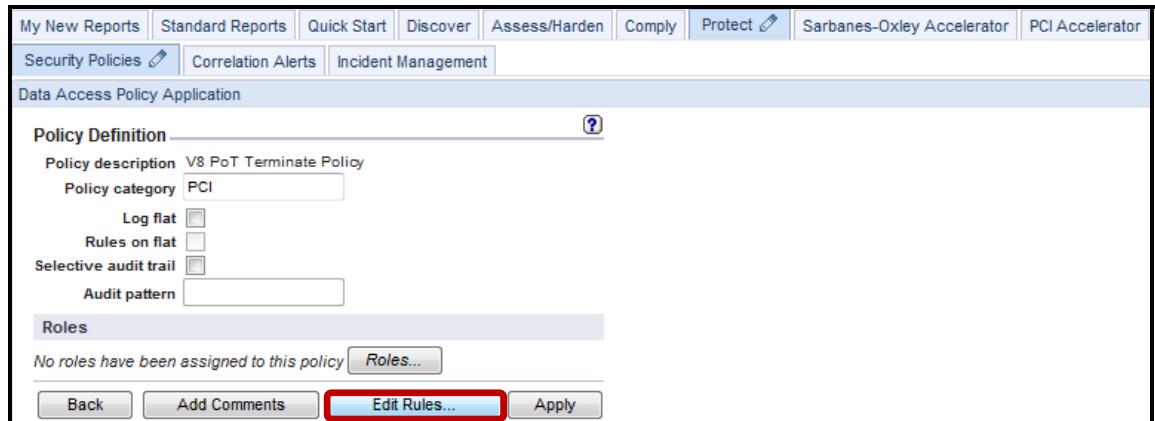
CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistry/key © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com, Zthread © Copyright 2000-2003, Eric Crahen.

- __2. Create a new terminate policy to trigger on.
 - __a. Click **Security Policies** under the **Protect** tab.
 - __b. Click **Create a new Policy with no Baseline**.

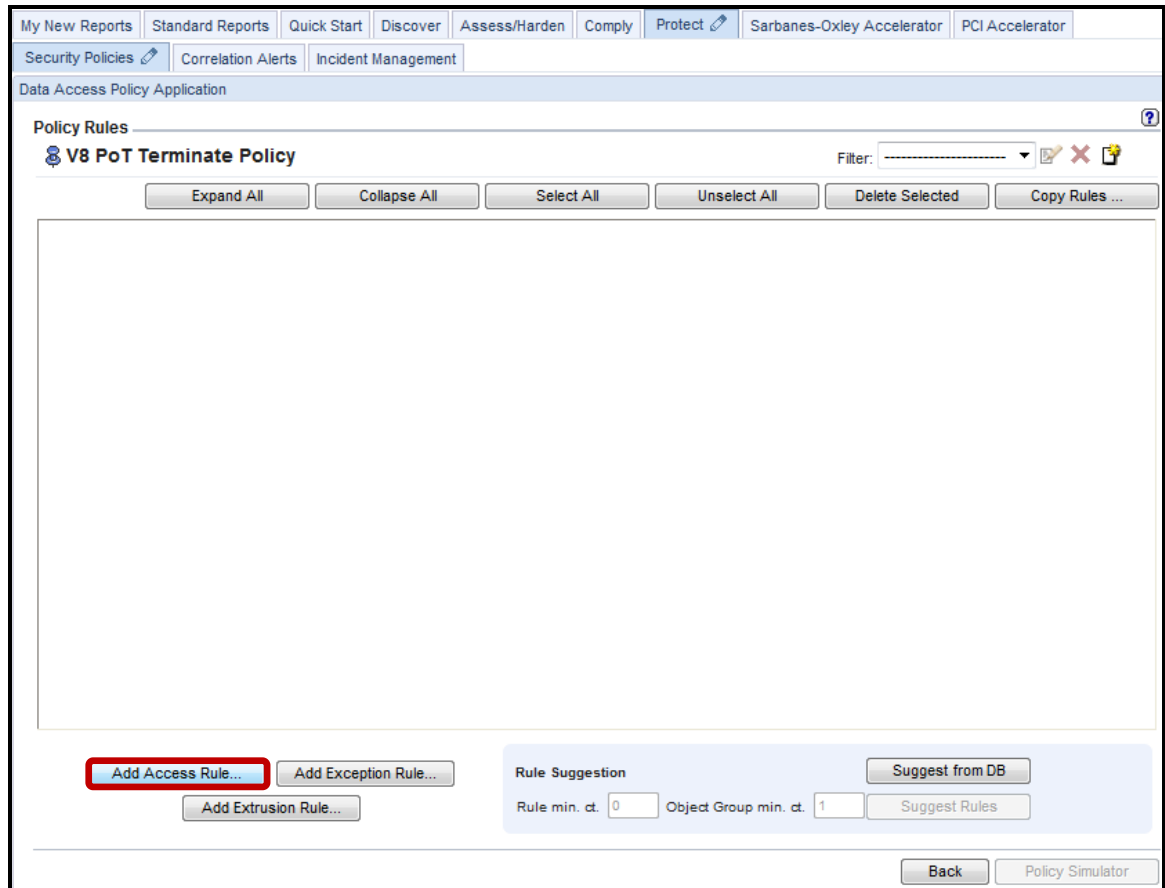


- __c. Enter **'V8 PoT Terminate Policy'** for *Policy description*, **'PCI'** for *Policy category*, and then click **Apply**.

__d. Click **Edit Rules** to add a rule to the policy.



__e. Click **Add Access Rule**.



f. Enter **Log Full Details** for *Rule #1 Description*.

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

Security Policies | Correlation Alerts | Incident Management

Data Access Policy Application

Access Rule Definition ?

Rule #1 of policy V8 PoT Terminate Policy

Description **Log Full Details**

Category Classification Severity INFO

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 and/or Group

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

Not Object and/or Group

Not Command and/or Group

Object/Cmd. Group

Object/Field Group

Pattern (RE)

XML Pattern (RE)

App Event Exists Event Type Event User Name

App Event Values Text and/or Group

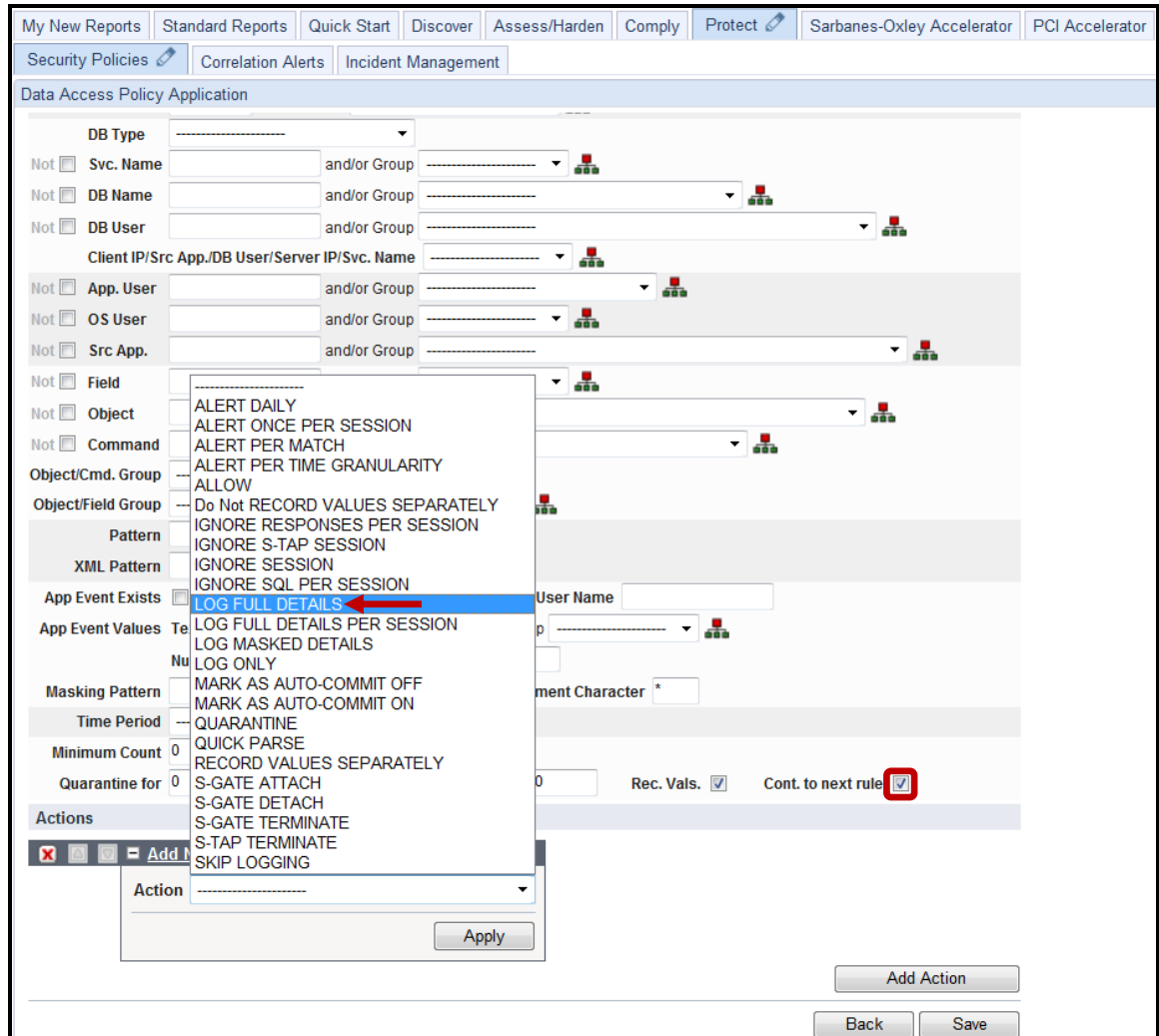
Numeric Date

Masking Pattern (RE) Replacement Character

__g. Scroll down and click **Add Action**.

The screenshot displays the 'Data Access Policy Application' configuration interface. At the top, there is a navigation bar with tabs for 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below this, there are sub-tabs for 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main content area is titled 'Data Access Policy Application' and contains a list of search criteria, each with a 'Not' checkbox and a search field. The criteria include: Client MAC, Net Prtcl., DB Type, Svc. Name, DB Name, DB User, Client IP/Src App./DB User/Server IP/Svc. Name, App. User, OS User, Src App., Field, Object, Command, Object/Cmd. Group, and Object/Field Group. Below these are fields for Pattern and XML Pattern (both with 'RE' icons), App Event Exists (checkbox), Event Type, Event User Name, App Event Values (Text, Numeric, Date), Masking Pattern (with 'RE' icon), Replacement Character, Time Period, Minimum Count, Reset Interval (minutes), Quarantine for (minutes), Records Affected Threshold, Rec. Vals. (checkbox), and Cont. to next rule (checkbox). At the bottom right of the configuration area, the 'Add Action' button is highlighted with a red box. Below the configuration area are 'Back' and 'Save' buttons.

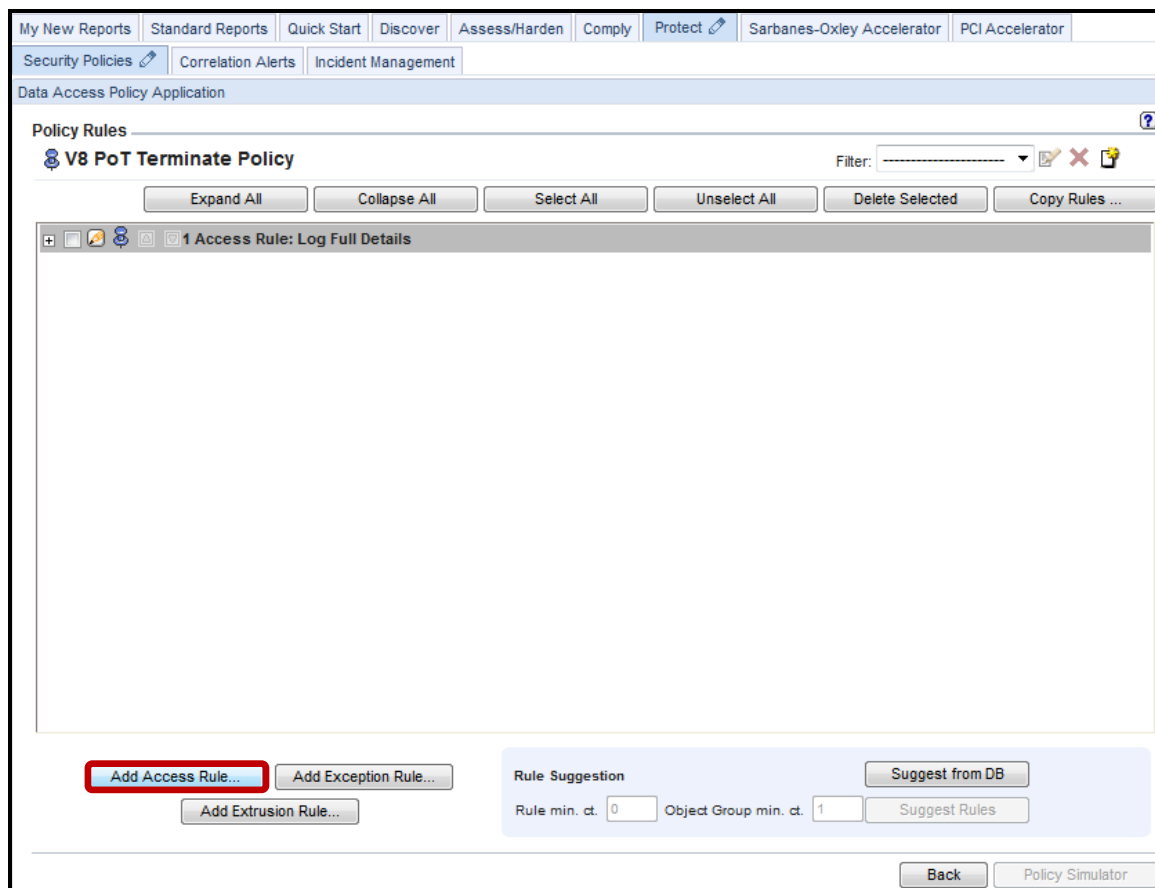
- __h. **Critical Step** – Check the **Cont. to next rule** checkbox. If this is not checked, none of the subsequent rules will be processed. This must be repeated for all dependent rules.
- __i. Select **LOG FULL DETAILS** from the **ACTION** drop-down list.



j. Click **Apply** and then click **Save**.

The screenshot displays the 'Data Access Policy Application' configuration interface. The top navigation bar includes tabs for 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below this, there are sub-tabs for 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main configuration area is titled 'Data Access Policy Application' and contains several sections of search criteria, each with a 'Not' checkbox and a search field followed by 'and/or Group' and a dropdown menu. The criteria include: DB Name, DB User, Client IP/Src App./DB User/Server IP/Svc. Name, App. User, OS User, Src App., Field, Object, Command, Object/Cmd. Group, Object/Field Group, Pattern, XML Pattern, App Event Exists (with Event Type and Event User Name), App Event Values (with Text, Numeric, and Date options), Masking Pattern, Time Period, Minimum Count, Reset Interval, Quarantine for, Records Affected Threshold, Rec. Vals., and Cont. to next rule. At the bottom, there is an 'Actions' section with an 'Add New Action' dialog box. This dialog box has a dropdown menu showing 'LOG FULL DETAILS' and an 'Apply' button. To the right of the dialog box is an 'Add Action' button. At the very bottom right of the page are 'Back' and 'Save' buttons.

__k. Click **Add Access Rule** to add the next rule.



- 1. Enter 'Attach Privileged Users' in the *Rule #2 description* field, and enter 'system' in the *DB User* field.

The screenshot shows the 'Access Rule Definition' interface for 'Rule #2 of policy V8 PoT Terminate Policy'. The 'Description' field contains the text 'Attach Privileged Users'. The 'DB User' field contains the text 'system'. The interface includes several sections for defining search criteria:

- Server/Client Information:** Fields for Server IP, Client IP, Client MAC, and Net Prtcl. with 'and/or Group' dropdowns.
- Database Information:** Fields for DB Type, Svc. Name, DB Name, and DB User (set to 'system').
- Application/OS Information:** Fields for App. User, OS User, Src App., Field, Object, and Command.
- Advanced Search:** Fields for Object/Cmd. Group, Object/Field Group, Pattern, and XML Pattern.
- Event Configuration:** Fields for App Event Exists, Event Type, Event User Name, App Event Values (Text, Numeric, Date), and Masking Pattern.

__m. Scroll down and click **Add Action**.

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

Security Policies | Correlation Alerts | Incident Management

Data Access Policy Application

Not Client MAC and/or Group

Net Prtcl. and/or Group

DB Type

Not Svc. Name and/or Group

Not DB Name and/or Group

Not DB User system and/or Group

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

Not Object and/or Group

Not Command and/or Group

Object/Cmd. Group

Object/Field Group

Pattern

XML Pattern

App Event Exists Event Type Event User Name

App Event Values Text and/or Group

Numeric Date

Masking Pattern Replacement Character

Time Period

Minimum Count 0 Reset Interval 0 minutes

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

Actions

Add Action

Back Save

- __n. **Critical Step** – Check the **Cont. to next rule** checkbox. If this is not checked, none of the subsequent rules will be processed. This must be repeated for all dependent rules.
- __o. Select **S-GATE ATTACH** from the **ACTION** drop-down list.

The screenshot displays the 'Data Access Policy Application' configuration window. At the top, there are navigation tabs: 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below these are sub-tabs: 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main area is titled 'Data Access Policy Application' and contains a list of policy rules. Each rule has several fields for defining the policy, such as 'DB Type', 'Svc. Name', 'DB Name', 'DB User', 'Client IP/Src App./DB User/Server IP/Svc. Name', 'App. User', 'OS User', 'Src App.', 'Field', 'Object', 'Command', 'Object/Cmd. Group', 'Object/Field Group', 'Pattern', 'XML Pattern', 'App Event Exists', 'App Event Values', 'Masking Pattern', 'Time Period', 'Minimum Count', and 'Quarantine for'. A dropdown menu is open over the 'Action' field, showing a list of actions: 'ALERT DAILY', 'ALERT ONCE PER SESSION', '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', 'QUARANTINE', 'QUICK PARSE', 'RECORD VALUES SEPARATELY', 'S-GATE ATTACH', 'S-GATE DETACH', 'S-GATE TERMINATE', 'S-TAP TERMINATE', and 'SKIP LOGGING'. The 'S-GATE ATTACH' action is highlighted with a red arrow. To the right of the 'Action' dropdown, there is a 'Cont. to next rule' checkbox, which is checked and highlighted with a red box. At the bottom of the window, there are buttons for 'Apply', 'Add Action', 'Back', and 'Save'.

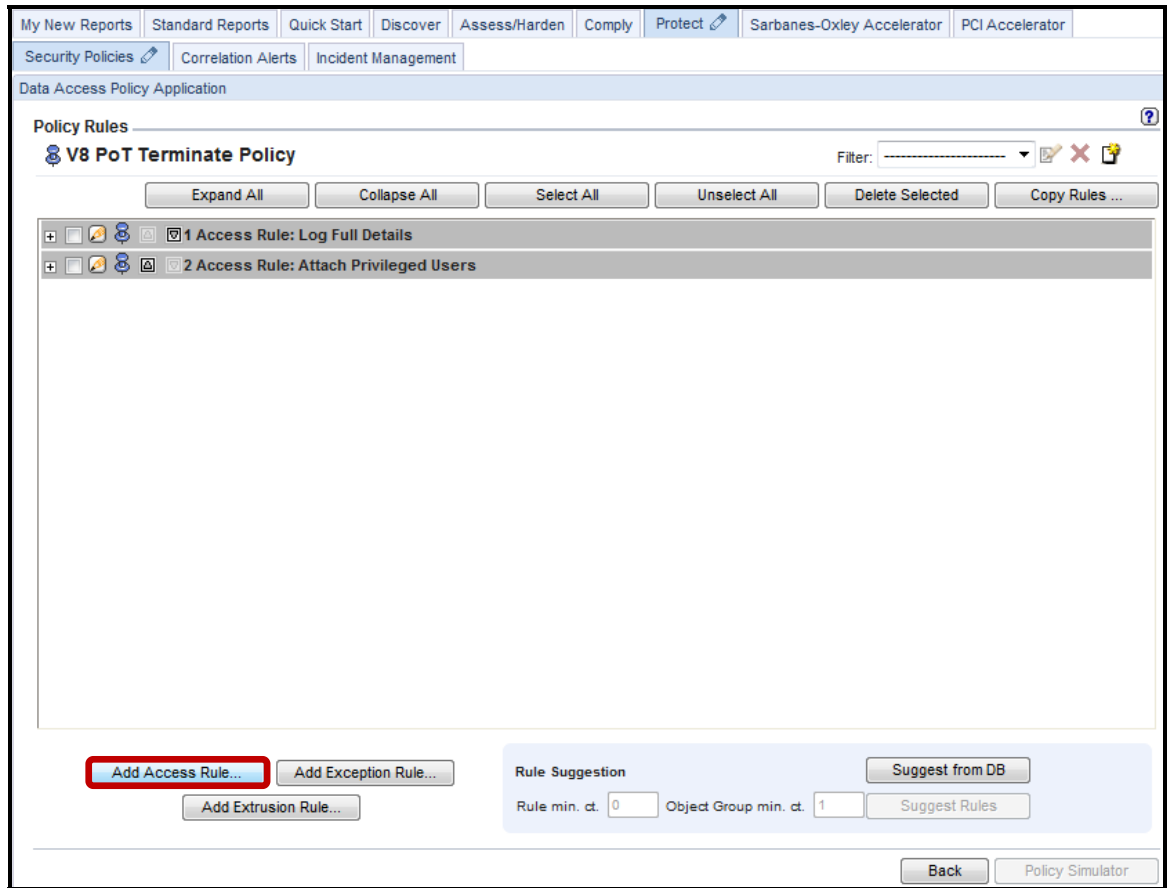
__p. Click **Apply** and then click **Save**.

The screenshot displays the 'Data Access Policy Application' configuration page in the IBM Security Policy Builder. The top navigation bar includes tabs for 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below this, there are sub-tabs for 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main configuration area is divided into several sections:

- Criteria Section:** Contains multiple rows of criteria, each with a 'Not' checkbox, a text input field, and a dropdown menu for 'and/or Group'. Criteria include DB Name, DB User (pre-filled with 'system'), Client IP/Src App./DB User/Server IP/Svc. Name, App. User, OS User, Src App., Field, Object, and Command.
- Advanced Criteria:** Includes 'Object/Cmd. Group', 'Object/Field Group', 'Pattern' (with a regex icon), and 'XML Pattern' (with a regex icon).
- Event Configuration:** Includes 'App Event Exists' (checkbox), 'Event Type', 'Event User Name', and 'App Event Values' (Text, Numeric, Date).
- Masking and Time:** Includes 'Masking Pattern' (with a regex icon), 'Replacement Character', 'Time Period' (dropdown), 'Minimum Count', and 'Reset Interval' (minutes).
- Thresholds:** Includes 'Quarantine for' (minutes), 'Records Affected Threshold', 'Rec. Vals.' (checkbox), and 'Cont. to next rule' (checkbox).
- Actions Section:** A pop-up window titled 'Add New Action' is open, showing a dropdown menu with 'S-GATE ATTACH' selected and an 'Apply' button highlighted with a red box.

At the bottom right of the main configuration area, there are three buttons: 'Add Action', 'Back', and 'Save'. The 'Save' button is highlighted with a red box.

__q. Click **Add Access Rule** to add the final rule.



- __r. Enter **Terminate Privileged User Credit Card Access** in the *Description* field, and select **HIGH** from the *Severity* drop-down list.

Note: **HIGH** severity policy violations will automatically appear highlighted in **RED** in the incident management report.

The screenshot displays the 'Access Rule Definition' configuration page in the IBM Security Policy Builder. The interface includes a navigation bar at the top with tabs for 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below this, there are sub-tabs for 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main content area is titled 'Data Access Policy Application' and 'Access Rule Definition'. The rule is identified as 'Rule #3 of policy V8 PoT Terminate Policy'. The 'Description' field contains the text 'Terminate Privileged User Credit Card Access'. The 'Severity' dropdown menu is open, showing options: INFO, LOW, NONE, MED, and HIGH. A red arrow points to the 'HIGH' option. The form also includes various fields for defining the rule's scope, such as 'Server IP', 'Client IP', 'Client MAC', 'DB Type', 'Svc. Name', 'DB Name', 'DB User', 'App. User', 'OS User', 'Src App.', 'Field', 'Object', 'Command', 'Object/Cmd. Group', 'Object/Field Group', 'Pattern', 'XML Pattern', 'App Event Exists', 'Event Type', 'Event User Name', 'App Event Values', 'Masking Pattern', and 'Replacement Character'.

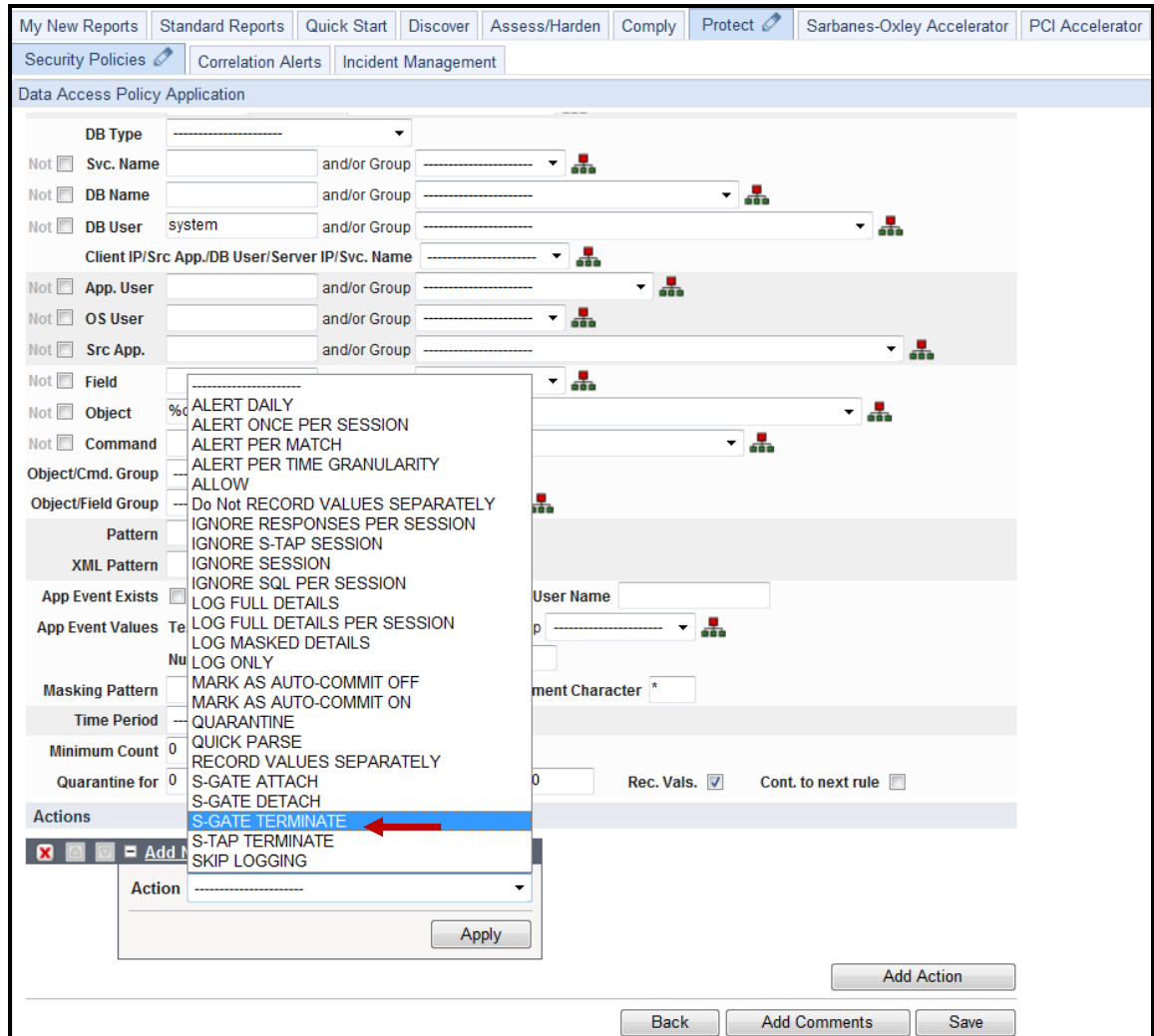
- __s. Scroll down, enter 'system' in the *DB User* field, and then enter '%creditcard' in the *Object* field.
- __t. Click **Add Action**.

The screenshot displays the 'Data Access Policy Application' configuration interface. At the top, there are navigation tabs: 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below these are sub-tabs: 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main configuration area includes several sections:

- Client Information:** Fields for Client MAC, Net Prtol., DB Type, Svc. Name, DB Name, DB User (set to 'system'), and Client IP/Src App./DB User/Server IP/Svc. Name.
- User and Application Information:** Fields for App. User, OS User, Src App., Field, Object (set to '%creditcard'), and Command.
- Object/Field Group:** Fields for Object/Cmd. Group and Object/Field Group.
- Pattern Fields:** Fields for Pattern and XML Pattern, both with 'RE' icons.
- Event Configuration:** Fields for App Event Exists, Event Type, Event User Name, App Event Values (Text, Numeric, Date), Masking Pattern, and Replacement Character.
- Time and Count Settings:** Fields for Time Period, Minimum Count, Reset Interval, Quarantine for, and Records Affected Threshold.
- Options:** Checkboxes for 'Rec. Vals.' and 'Cont. to next rule'.
- Actions:** A section at the bottom with a prominent 'Add Action' button highlighted in red, and 'Back', 'Add Comments', and 'Save' buttons below it.

__u. Select **S-GATE TERMINATE** from the *ACTION* drop-down list.

Note: There is no need to check the 'Cont. to next rule' checkbox since this is the last rule, and there are no more dependent rules.



__v. Click **Apply** and then click **Save**.

This policy rule will prevent the 'system' user from accessing the *credit card* table.

The screenshot displays the 'Data Access Policy Application' configuration window. The interface includes a top navigation bar with tabs for 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below this, there are sub-tabs for 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main configuration area is divided into several sections: 'Data Access Policy Application' with various input fields for 'DB Name', 'DB User' (set to 'system'), 'App. User', 'OS User', 'Src App.', 'Field', 'Object' (set to '%creditcard'), 'Command', 'Object/Cmd. Group', and 'Object/Field Group'; 'Pattern' and 'XML Pattern' fields with 'RE' icons; 'App Event Exists' and 'Event Type' fields; 'App Event Values' with 'Text', 'Numeric', and 'Date' options; 'Masking Pattern' and 'Replacement Character' fields; 'Time Period' with a calendar icon; 'Minimum Count' (0), 'Reset Interval' (0 minutes), and 'Quarantine for' (0 minutes) fields; and 'Records Affected Threshold' (0), 'Rec. Vals.' (checked), and 'Cont. to next rule' (unchecked) options. At the bottom, there is an 'Actions' section with an 'Add New Action' dialog box showing 'S-GATE TERMINATE' as the selected action and an 'Apply' button. Other buttons at the bottom include 'Back', 'Add Comments', and 'Save'.

___w. Click **Back** to return to the Policy Definition screen.

The screenshot shows the 'Data Access Policy Application' interface. The main heading is 'Policy Rules' for the 'V8 PoT Terminate Policy'. Below the heading are buttons for 'Expand All', 'Collapse All', 'Select All', 'Unselect All', 'Delete Selected', and 'Copy Rules...'. A list of three access rules is displayed:

- 1 Access Rule: Log Full Details
- 2 Access Rule: Attach Privileged Users
- 3 Access Rule: Terminate Privileged User Credit Card Access

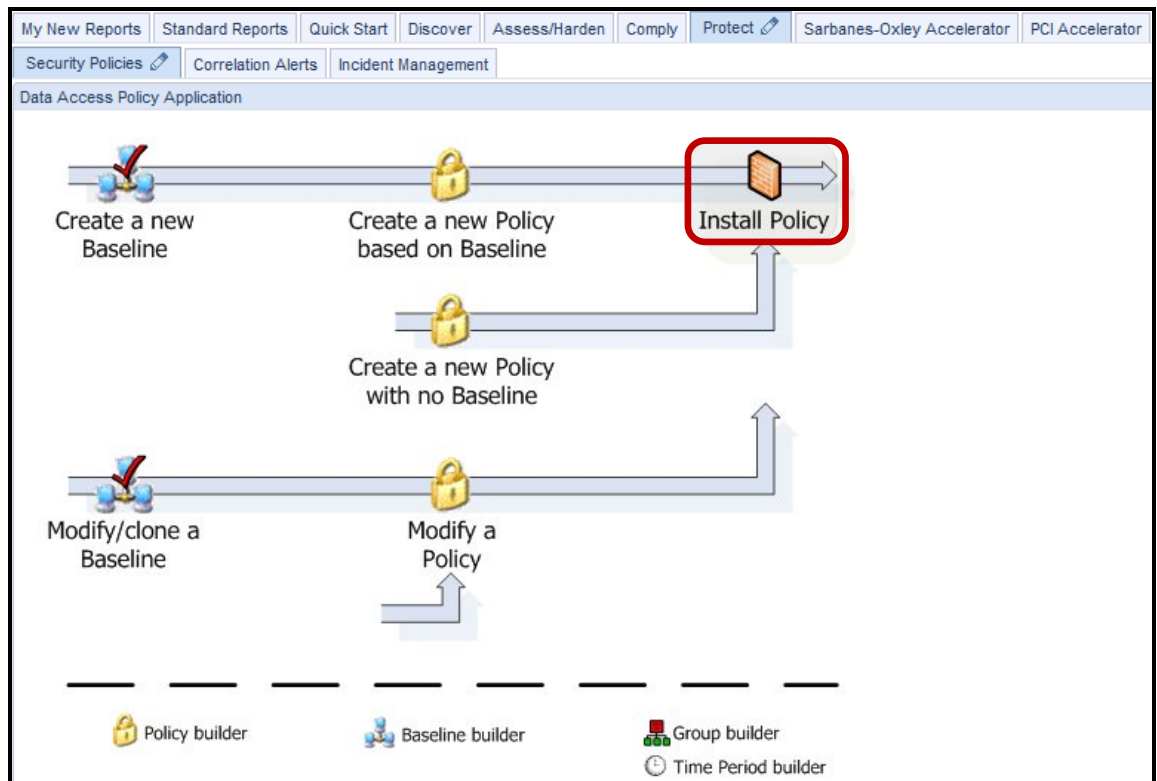
At the bottom of the screen, there are buttons for 'Add Access Rule...', 'Add Exception Rule...', and 'Add Exclusion Rule...'. A 'Rule Suggestion' section includes 'Suggest from DB' and 'Suggest Rules' buttons, along with input fields for 'Rule min. ct.' (0) and 'Object Group min. ct.' (1). A 'Back' button is highlighted with a red box at the bottom right, next to a 'Policy Simulator' link.

___x. Click **Back** once more to return to the main **Security Policies** tab screen.

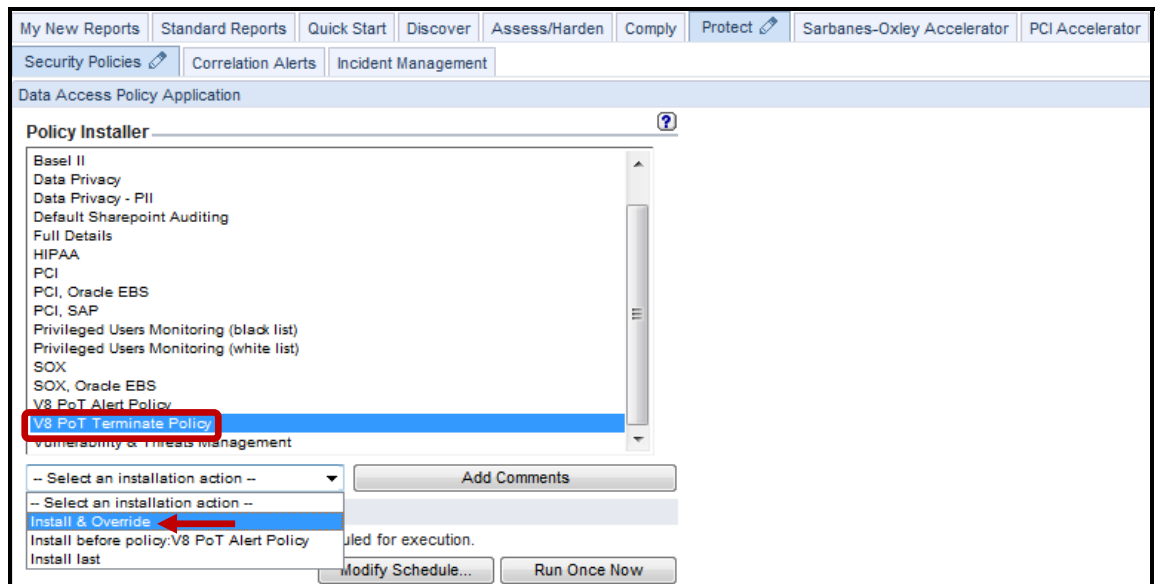
The screenshot shows the 'Policy Definition' screen for the 'V8 PoT Terminate Policy'. The 'Policy description' is 'V8 PoT Terminate Policy' and the 'Policy category' is 'PCI'. There are checkboxes for 'Log flat', 'Rules on flat', and 'Selective audit trail', all of which are currently unchecked. An 'Audit pattern' field is present but empty. Below these fields is a 'Roles' section with the text 'No roles have been assigned to this policy' and a 'Roles...' button. At the bottom left, a 'Back' button is highlighted with a red box. Other buttons at the bottom include 'Add Comments', 'Edit Rules...', and 'Apply'.

__3. Install the V8 PoT Terminate Policy.

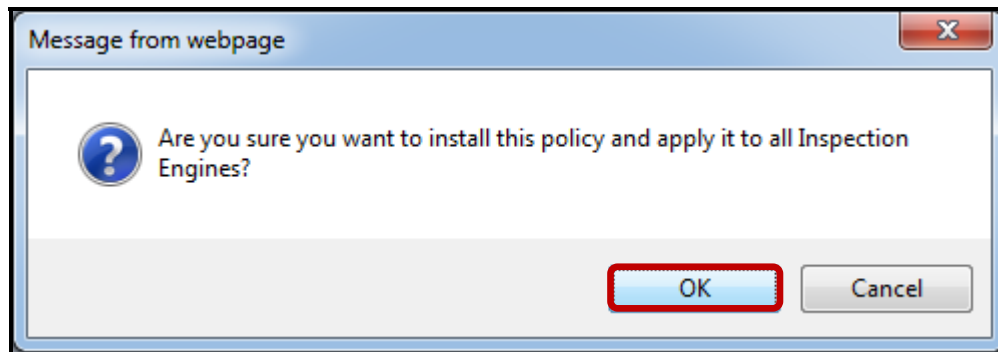
__a. Click **Install Policy**.



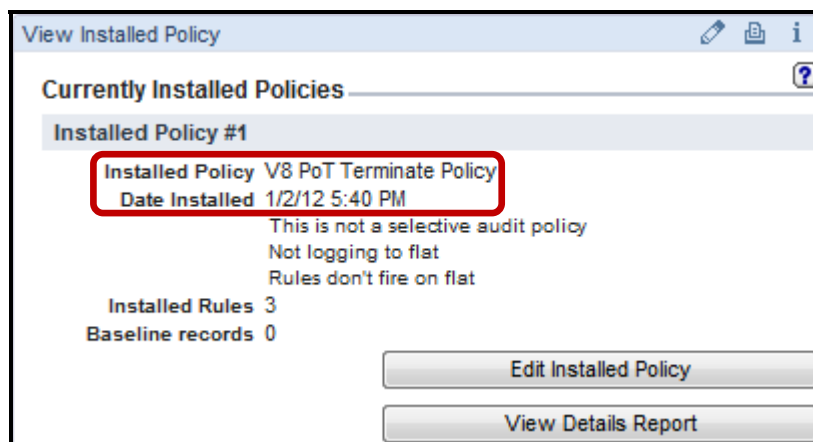
__b. Scroll down, select **V8 Terminate Policy** from the *Policy installer* list, and then select **Install & Override** from the *Select an installation action* drop-down list.



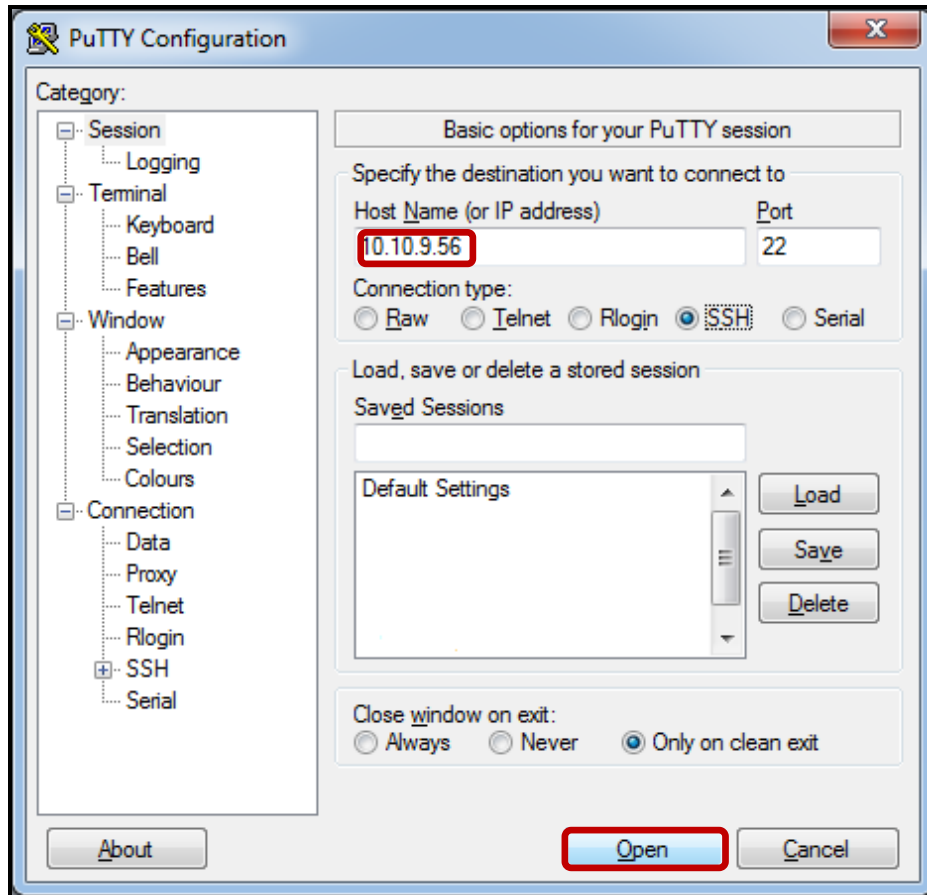
- __c. Click **OK** to acknowledge.



- __d. Verify that the **V8 PoT Terminate Policy** has been successfully installed. Check under the *View Installed Policy* section to the upper right of the screen.



- __4. Test the V8 PoT Terminate Policy.
 - __a. Using a PuTTY SSH client, access the VM database server to demonstrate the InfoSphere Guardium policy capability.
 - __b. Start the PuTTY SSH client login.
 - __c. From your laptop, launch PuTTY, enter **10.10.9.56**, and click **Open**.



- __d. Login as **oracle** / **guardium**. After logging in, the following prompt will be displayed.

```

10.10.9.56 - PuTTY
login as: oracle
oracle@10.10.9.56's password:
Last login: Thu Mar  6 09:15:49 2008 from 10.10.9.240
-bash-3.00$ █

```

- __e. Login to Oracle as user *joe* by typing: **sqlplus joe/guardium**.
- __f. Type '**select cardid, lastname from joe.creditcard where cardid >= 203 and cardid < 208 order by cardid;**'

```

10.10.9.56 - PuTTY
oracle@10.10.9.56's password:
Last login: Mon Jan  2 18:00:05 2012 from 10.10.9.240
-bash-3.00$ sqlplus joe/guardium

SQL*Plus: Release 10.2.0.1.0 - Production on Mon Jan 2 18:55:45 2012
Copyright (c) 1982, 2005, Oracle. All rights reserved.

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

SQL> select cardid, lastname from joe.creditcard where cardid >= 203 and cardid < 208 order by cardid;

CARDID LASTNAME
-----
203 Dole
204 Dunn
205 OLeary
206 OTool
207 Peterson

SQL> █

```

- __g. Now, login to Oracle as privileged user *system* by typing: '**connect system/guardium.**'

```

10.10.9.56 - PuTTY
-bash-3.00$ sqlplus joe/guardium

SQL*Plus: Release 10.2.0.1.0 - Production on Mon Jan 2 18:55:45 2012

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

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

SQL> select cardid, lastname from joe.creditcard where cardid >= 203 and cardid
< 208 order by cardid;

   CARDID LASTNAME
-----
      203 Dole
      204 Dunn
      205 OLeary
      206 OTool
      207 Peterson

SQL> connect system/guardium
Connected.
SQL>

```

- __h. Once more, type '**select cardid, lastname from joe.creditcard where cardid >= 203 and cardid < 208 order by cardid;**'

The policy immediately terminates the privileged user accessing creditcard information.

```

10.10.9.56 - PuTTY

SQL> select cardid, lastname from joe.creditcard where cardid >= 203 and cardid
< 208 order by cardid;

   CARDID LASTNAME
-----
      203 Dole
      204 Dunn
      205 OLeary
      206 OTool
      207 Peterson

SQL> connect system/guardium
Connected.
SQL> select cardid, lastname from joe.creditcard where cardid >= 203 and cardid
< 208 order by cardid;
select cardid, lastname from joe.creditcard where cardid >= 203 and cardid < 208
order by cardid
*
ERROR at line 1:
ORA-03113: end-of-file on communication channel

SQL>

```

- __5. Validate that the Policy has successfully triggered a Policy Violation.
- __a. From the GUI click **Incident Management** under the **Protect** tab to view the *Policy Violations / Incident Management* Report and verify that the alert was actually recorded.

Violation Log Id	Timestamp	Category	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description	Incident Number	Policy Rule Violations
17	2012-01-02 18:59:49.0	PCI	Terminate Privileged User Credit Card Access	10.10.9.56	10.10.9.56	SYSTEM	select cardid, lastname from joe.creditcard where cardid >= 203 and cardid < 208 order by cardid, then type select name, cardnumber from creditcard	HIGH	0	1
16	2012-01-02 14:43:20.0		Alert on CreditCard Access	10.10.9.56	10.10.9.56	SYSTEM	select name, cardnumber from creditcard	INFO	0	1
15	2012-01-02 14:41:41.0		Alert on CreditCard Access	10.10.9.56	10.10.9.56	SYSTEM	check_object(creditcard)	INFO	0	1

We see the blocked user (system) with a high severity level.

Thank You

Configuring Terminate Policy with S-GATE review

- __1. Where does the S-GATE termination occur?
- __a. Database server
 - __b. Guardium appliance
 - __c. S-TAP
 - __d. TCP/IP Reset
- __2. S-GATE blocking is an optional component enabled by product key. (True or False).
- __3. The terminate action can work given the following guard_tap.ini file settings. (True or False)
- firewall_installed=0
- firewall_fail_close=0
- firewall_default_state=0
- __4. The terminate action can work given the following guard_tap.ini file settings. (True or False)
- firewall_installed=1
- firewall_fail_close=0
- firewall_default_state=0
- __5. If firewall_installed=1, what policy rule must be defined for a terminate action to work?
- __a. A rule with an S-GATE DETACH action
 - __b. No rule is required
 - __c. A rule with an S-GATE ATTACH action
 - __d. A rule with an ALERT action
- __6. An S-GATE TERMINATE action will increase database access time due to latency. (True or False)

Configuring Terminate Policy with S-GATE review (Answers)

__1. Where does the S-GATE termination occur?

S-TAP.

__2. S-GATE blocking is an optional component enabled by product key.
(**True** or **False**).

True.

__3. The terminate action can work given the following guard_tap.ini file settings.
(**True** or **False**)

firewall_installed=0

firewall_fail_close=0

firewall_default_state=0

False.

__4. The terminate action can work given the following guard_tap.ini file settings.
(**True** or **False**)

firewall_installed=1

firewall_fail_close=0

firewall_default_state=0

True.

__5. If firewall_installed=1, what policy rule must be defined for a terminate action to work?

C – A rule with an S-GATE ATTACH action.

__6. An S-GATE TERMINATE action will increase database access time due to latency.
(**True** or **False**)

True.

6.3 Configuring Quarantine Policy

Overview

The InfoSphere Guardium platform supports granular, deterministic policies to positively identify violations (rather than relying on heuristics). Rules are based on specific session properties such as client IP address, MAC address, source application, DB user, OS user, application user, time-of-day, SQL command and table names, which are typically defined by way of pre-defined groups to simplify ongoing management. A broad range of policy actions can be invoked for policy violations, such as real-time alerts (SMTP, SNMP, Syslog, CEF), user quarantine and terminate connection.

In addition to examining SQL, the InfoSphere Guardium Data-Level Access Control module also examines query results. For example, a connection from an anomalous script or application that is suddenly seen to be extracting Personally Identifiable Information (PII) from the database can be terminated or quarantined while being investigated, although a valid application that extracts the same PII data will be allowed.

Quarantine is available for access, exception and extrusion rules and can prevent the same user from logging into the same server for a certain period of time. There is one validation item: you cannot have a rule with a QUARANTINE action without having filled in a value for amount of time that the user is quarantined. Each element has, in addition to the timestamp, a server IP, server type, a DB user name, a service name and a flag saying whether this was a watched session or not.

Objectives

In this section, we will demonstrate how InfoSphere Guardium can quarantine a suspicious user for a specified period of time and send out alerts. During this time period, the user will not be allowed to log onto the server from the same IP address with the same user ID. This will allow the alerted administrators to secure against possible further intrusions. The quarantine can be lifted by an administrator if the situation was deemed to be a harmless mistake. The following objectives will be discussed:

- __1. Build a new policy.
- __2. Add a logging rule to the policy.
- __3. Add Quarantine rule to prevent unauthorized access to sensitive objects
- __4. Install the policy.
- __5. Test Quarantine features.

- __1. Start the InfoSphere Guardium appliance and login (if necessary, otherwise skip ahead).
 - __a. From your laptop, go to to <https://10.10.9.248:8443>
 - __b. Login as **pot / guardium**

Login

Please enter your information

User name:

Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

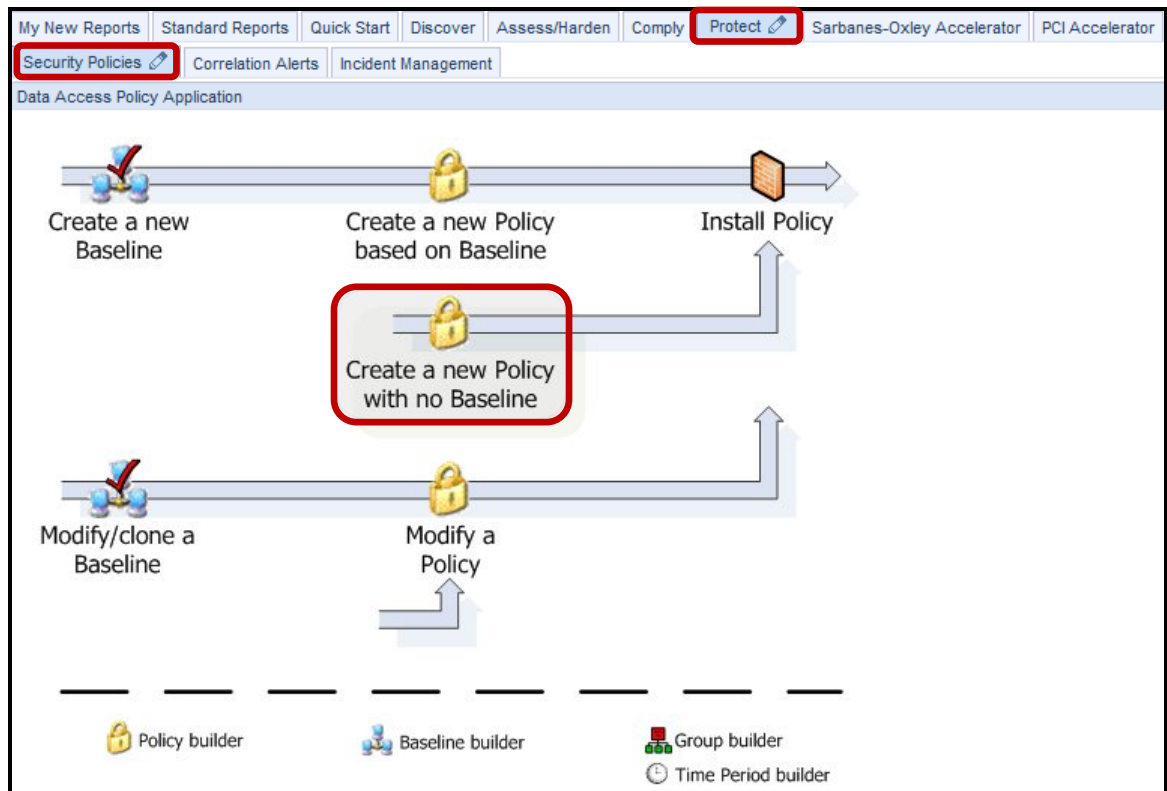
Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistry/key © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com, Zthread © Copyright 2000-2003, Eric Crahen.

__2. Use the InfoSphere Guardium GUI to create a new policy.

__a. Click **Security Policies** under the **Protect** tab.

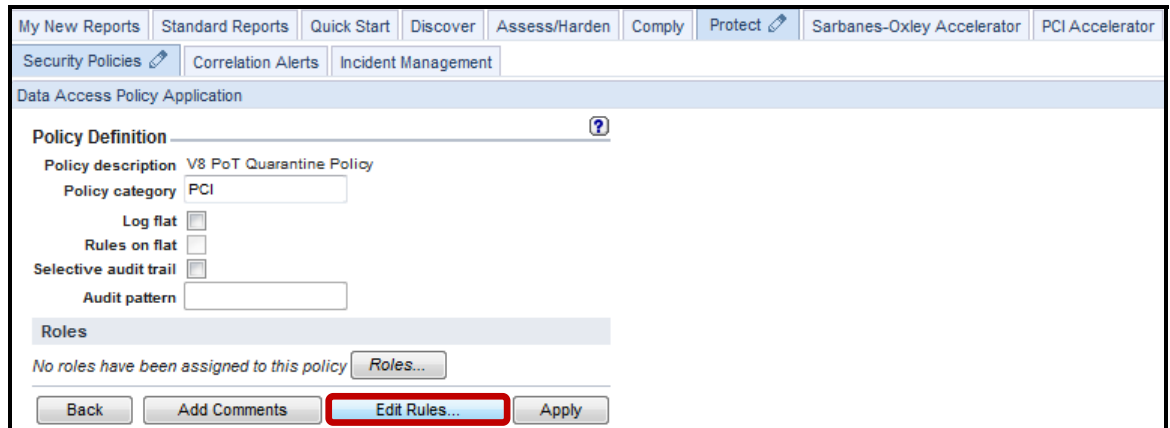
__b. Click **Create a new Policy with no Baseline**.



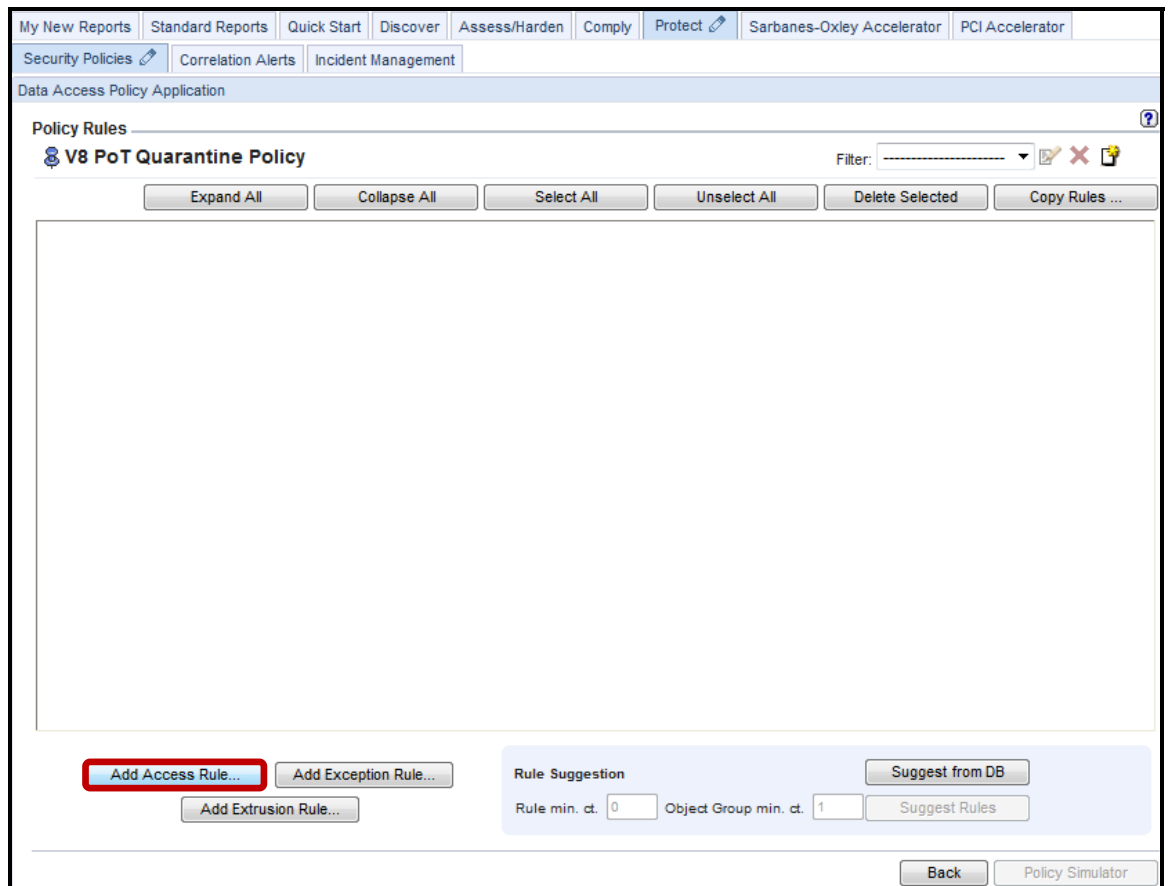
__c. Enter '**V8 PoT Quarantine Policy**' for *Policy description*, '**PCI**' for *Policy category*, and then click **Apply**.

The screenshot shows the 'Policy Definition' form in the InfoSphere Guardium GUI. The 'Policy description' field contains 'V8 PoT Quarantine Policy' and the 'Policy category' field contains 'PCI'. The 'Apply' button is highlighted with a red box.

__d. Click **Edit Rules** to add a rule to the policy.



__e. Click **Add Access Rule** to add first rule.



f. Enter 'Log Full Details' for Description.

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

Security Policies | Correlation Alerts | Incident Management

Data Access Policy Application

Access Rule Definition ?

Rule #1 of policy V8 PoT Quarantine Policy

Description **Log Full Details**

Category Classification Severity **INFO**

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 and/or Group

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

Not Object and/or Group

Not Command and/or Group

Object/Cmd. Group

Object/Field Group

Pattern (RE)

XML Pattern (RE)

App Event Exists Event Type Event User Name

App Event Values Text and/or Group

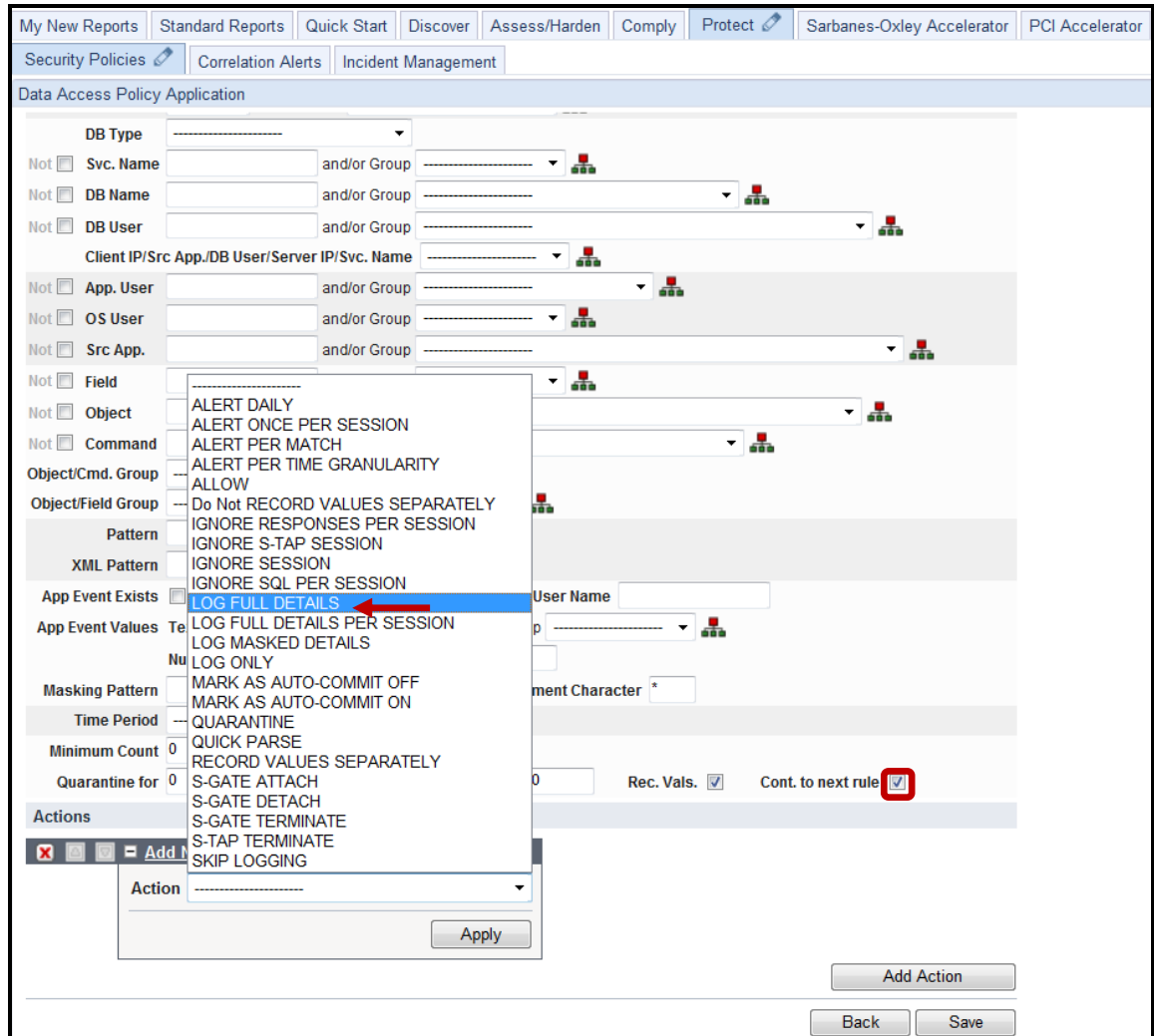
Numeric Date

Masking Pattern (RE) Replacement Character

g. Scroll down and click **Add Action**.

The screenshot displays the 'Data Access Policy Application' configuration page. The top navigation bar includes tabs for 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below this, there are sub-tabs for 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main content area is titled 'Data Access Policy Application' and contains a series of search criteria fields, each with a 'Not' checkbox and an 'and/or Group' dropdown menu. The fields include: Client MAC, Net Prtcl., DB Type, Svc. Name, DB Name, DB User, Client IP/Src App./DB User/Server IP/Svc. Name, App. User, OS User, Src App., Field, Object, Command, Object/Cmd. Group, Object/Field Group, Pattern, XML Pattern, App Event Exists, Event Type, Event User Name, App Event Values (Text, Numeric, Date), Masking Pattern, Replacement Character, Time Period, Minimum Count, Reset Interval, Quarantine for, Records Affected Threshold, Rec. Vals., and Cont. to next rule. At the bottom right, there is a red-bordered 'Add Action' button, and below it are 'Back' and 'Save' buttons.

- __h. **Critical Step** – Check the **Cont. to next rule** checkbox. If this is not checked, none of the subsequent rules will be processed. This must be repeated for all dependent rules.
- __i. Select **LOG FULL DETAILS** from the **ACTION** drop-down list.



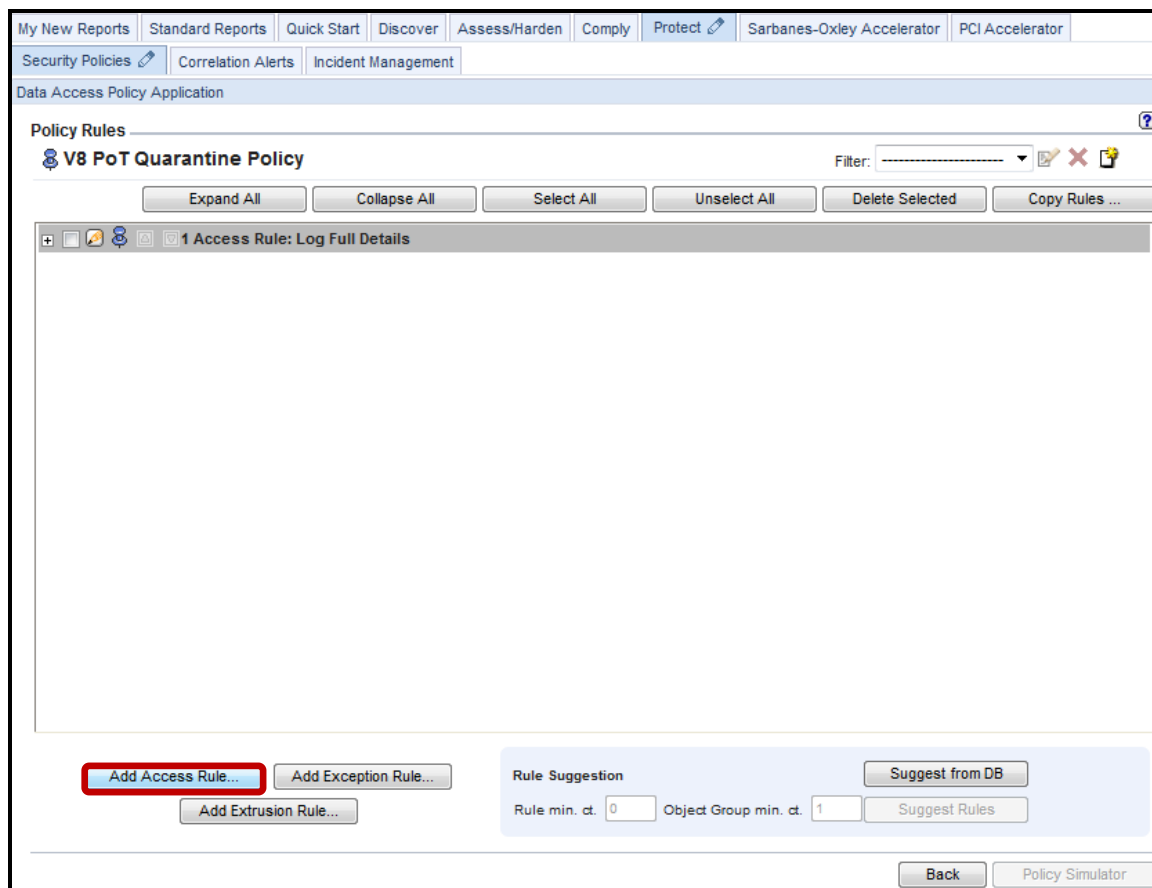
j. Click **Apply** and then click **Save**.

The screenshot displays the 'Data Access Policy Application' configuration page. At the top, there is a navigation bar with tabs: 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below this, there are sub-tabs for 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main configuration area includes several sections:

- Not** checkboxes for: DB Name, DB User, App. User, OS User, Src App., Field, Object, and Command. Each has an associated text input and a dropdown menu for 'and/or Group'.
- Client IP/Src App./DB User/Server IP/Svc. Name dropdown.
- Object/Cmd. Group dropdown.
- Object/Field Group dropdown.
- Pattern and XML Pattern text inputs, each with a 'RE' icon.
- App Event Exists checkbox, Event Type text input, and Event User Name text input.
- App Event Values section with Text, Numeric, and Date options, each with a text input and 'and/or Group' dropdown.
- Masking Pattern text input with a 'RE' icon and a Replacement Character text input.
- Time Period dropdown.
- Minimum Count (0) and Reset Interval (0) minutes.
- Quarantine for (0) minutes, Records Affected Threshold (0), Rec. Vals. (checked), and Cont. to next rule (checked).

The **Actions** section at the bottom features an 'Add New Action' dialog box with a dropdown menu set to 'LOG FULL DETAILS' and an 'Apply' button. Below the dialog are 'Add Action', 'Back', and 'Save' buttons. The 'Save' button is highlighted with a red box.

__k. Click **Add Access Rule** to add the final rule.



- 1. Enter 'Quarantine PCI Objects' in the *Description* field, and select **MED** from the *Severity* drop-down list.

Note: MED severity policy violations will automatically appear highlighted in **ORANGE** in the incident management report.

The screenshot shows the 'Access Rule Definition' page in the IBM InfoSphere Guardium V8.2 interface. The page title is 'Data Access Policy Application'. The current rule is 'Rule #2 of policy V8 PoT Quarantine Policy'. The 'Description' field contains 'Quarantine PCI Objects'. The 'Severity' dropdown menu is open, and 'MED' is selected, indicated by a red arrow. The interface includes various fields for defining access rules, such as 'Server IP', 'Client IP', 'Client MAC', 'Net Prtol.', 'DB Type', 'Svc. Name', 'DB Name', 'DB User', 'App. User', 'OS User', 'Src App.', 'Field', 'Object', 'Command', 'Object/Cmd. Group', 'Object/Field Group', 'Pattern', 'XML Pattern', 'App Event Exists', 'Event Type', 'Event User Name', 'App Event Values', 'Numeric', 'Date', 'Masking Pattern', and 'Replacement Character'.

__m. Enter 'cardnumber' in the *Field* field and enter 'creditcard' in the *Object* field.

The screenshot displays the 'Access Rule Definition' configuration page in the IBM Security Policy Builder. The page title is 'Data Access Policy Application' and the specific rule is 'Rule #2 of policy V8 PoT Quarantine Policy'. The description is 'Quarantine PCI Objects' and the severity is set to 'MED'. The configuration includes various fields for defining the rule's scope, such as Server IP, Client IP, Client MAC, Net Prtol, DB Type, Svc. Name, DB Name, DB User, App. User, OS User, Src App., Field, Object, Command, Object/Cmd. Group, Object/Field Group, Pattern, XML Pattern, App Event Exists, Event Type, Event User Name, App Event Values, Numeric, Date, Masking Pattern, and Replacement Character. The 'Field' and 'Object' fields are highlighted with red boxes and contain the text 'cardnumber' and 'creditcard' respectively.

__n. Select **ORACLE** from the *DB Type* drop-down list.

The screenshot shows the 'Access Rule Definition' window for 'Rule #2 of policy V8 PoT Quarantine Policy'. The 'Description' is 'Quarantine PCI Objects' and the 'Severity' is 'INFO'. The 'DB Type' dropdown menu is open, displaying a list of database types: CIFS, DB2, DB2 COLLECTION PROFILE, FTP, IBM INFORMIX (DRDA), IBM ISERIES, IMS, INFORMIX, MS SQL SERVER, MYSQL, NETEZZA, **ORACLE** (highlighted with a red arrow), POSTGRESQL, SYBASE, TERADATA, VSAM, and VSAM COLLECTION PROFILE. Other fields include 'Server IP', 'Client IP', 'Client MAC', 'Net Prtol.', 'Svc. Name', 'DB Name', 'DB User', 'App. User', 'OS User', 'Src App.', 'Field', 'Object', 'Command', 'Object/Cmd. Group', 'Object/Field Group', 'Pattern', 'XML Pattern', 'App Event Exists', 'Event Type', 'Event User Name', 'App Event Values', 'Masking Pattern', and 'Replacement Character'.

__o. Scroll down and click **Add Action**.

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

Security Policies | Correlation Alerts | Incident Management

Data Access Policy Application

Not Client MAC and/or Group

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

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

Not Object and/or Group

Not Command and/or Group

Object/Cmd. Group

Object/Field Group

Pattern

XML Pattern

App Event Exists Event Type Event User Name

App Event Values Text and/or Group

Numeric Date

Masking Pattern Replacement Character

Time Period

Minimum Count Reset Interval minutes

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

Actions

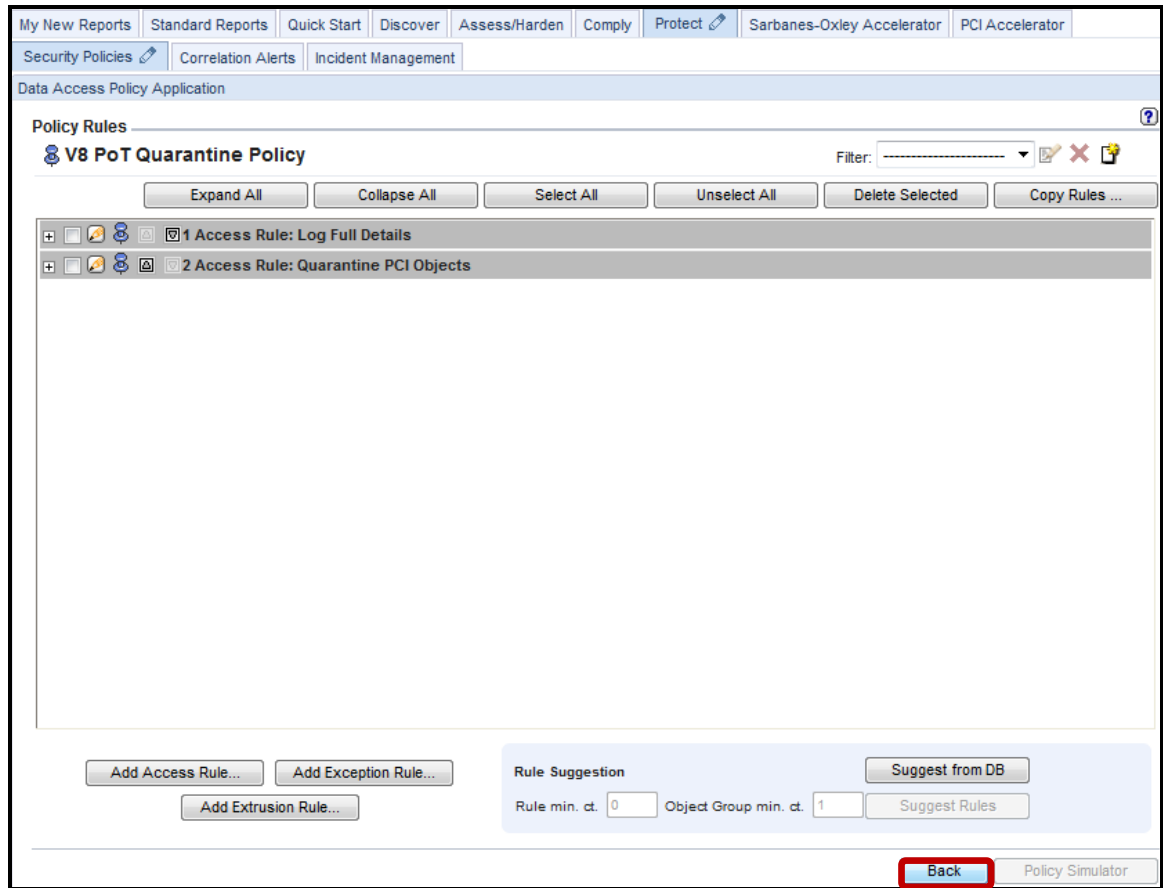
Add Action

Back Save

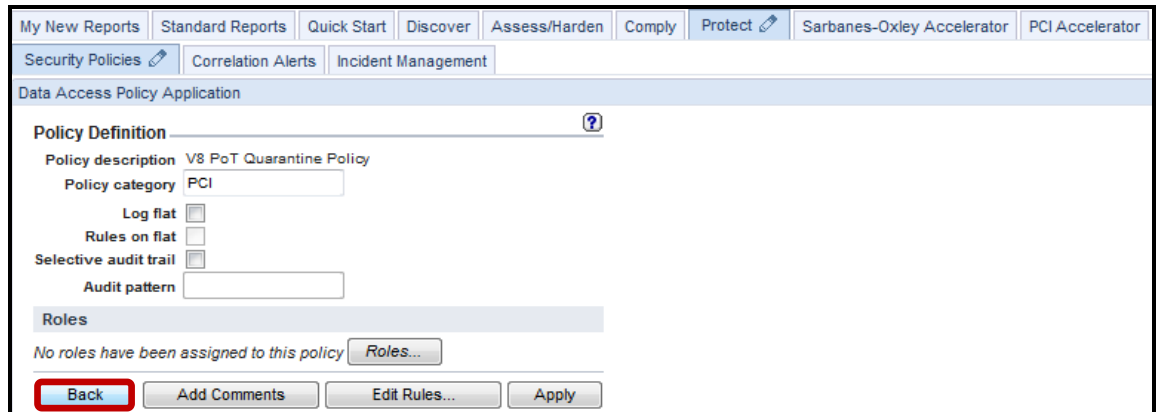
- __q. Enter '15' in the *Quarantine for _ minutes* field (to set quarantine time to 15 minutes).
- __r. Click **Apply** and then click **Save**.

The screenshot displays the 'Data Access Policy Application' configuration page. The interface includes a navigation bar at the top with tabs for 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below this, there are sub-tabs for 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main configuration area is titled 'Data Access Policy Application' and contains various fields for defining policy rules, such as 'DB Name', 'DB User', 'App. User', 'OS User', 'Src App.', 'Field', 'Object', 'Command', 'Object/Cmd. Group', 'Object/Field Group', 'Pattern', 'XML Pattern', 'App Event Exists', 'Event Type', 'Event User Name', 'App Event Values', 'Masking Pattern', 'Replacement Character', 'Time Period', 'Minimum Count', 'Reset Interval', 'Quarantine for', 'Records Affected Threshold', 'Rec. Vals.', and 'Cont. to next rule'. The 'Quarantine for' field is highlighted with a red box and contains the value '15'. Below the main configuration area, there is an 'Actions' section with a sub-window titled 'Add New Action'. In this sub-window, the 'Action' dropdown menu is set to 'QUARANTINE', and the 'Apply' button is highlighted with a red box. At the bottom right of the main configuration area, there are buttons for 'Add Action', 'Back', and 'Save', with the 'Save' button also highlighted with a red box.

__s. Click **Back** to return to the Policy Definition screen.

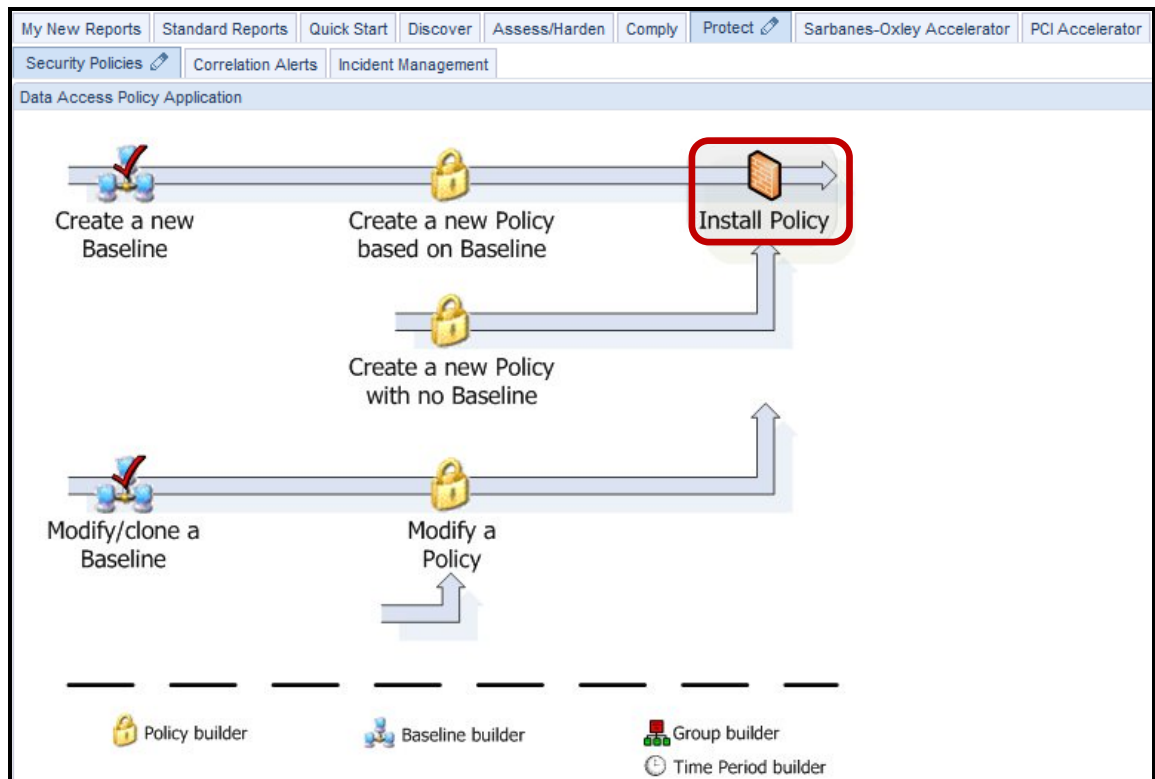


__t. Click **Back** once more to return to the main **Security Policies** tab screen.

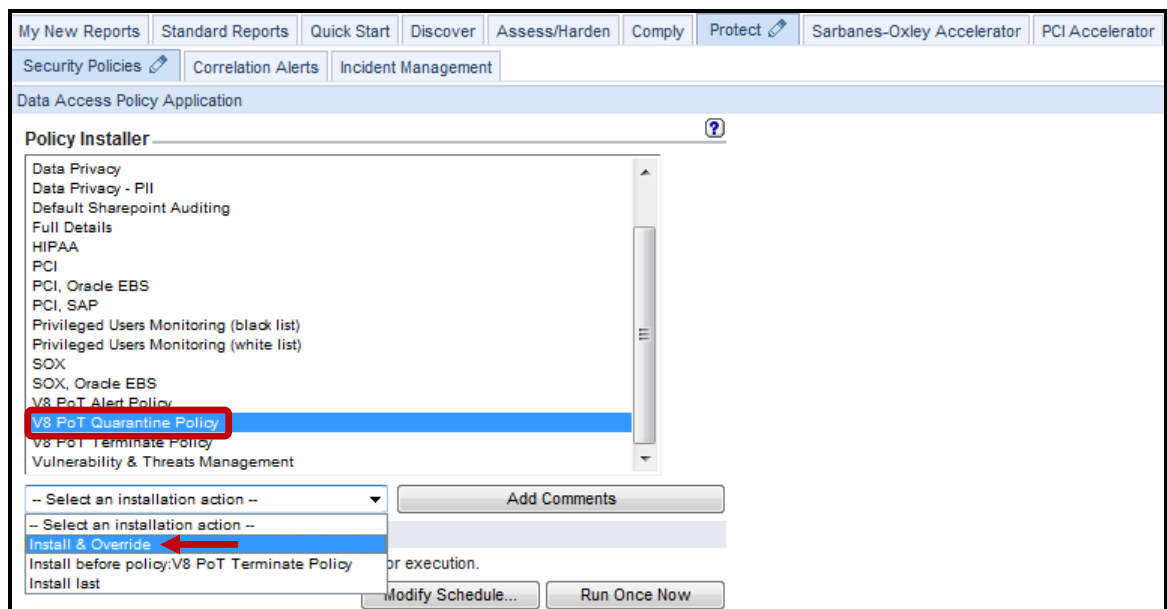


__3. Install the V8 PoT Quarantine Policy.

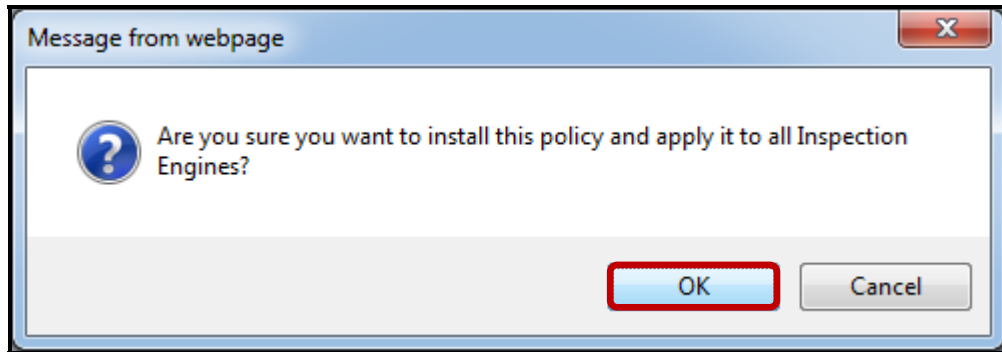
__a. Click **Install Policy**.



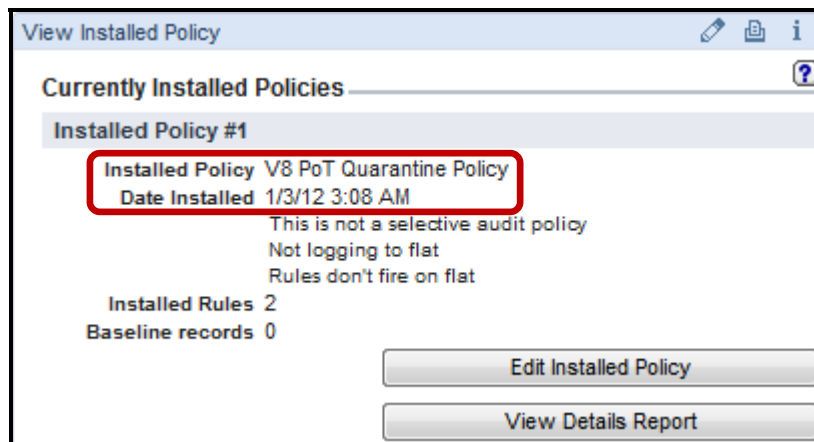
__b. Scroll down, select **V8 Quarantine Policy** from the *Policy installer* list, and then select **Install & Override** from the *Select an installation action* drop-down list.



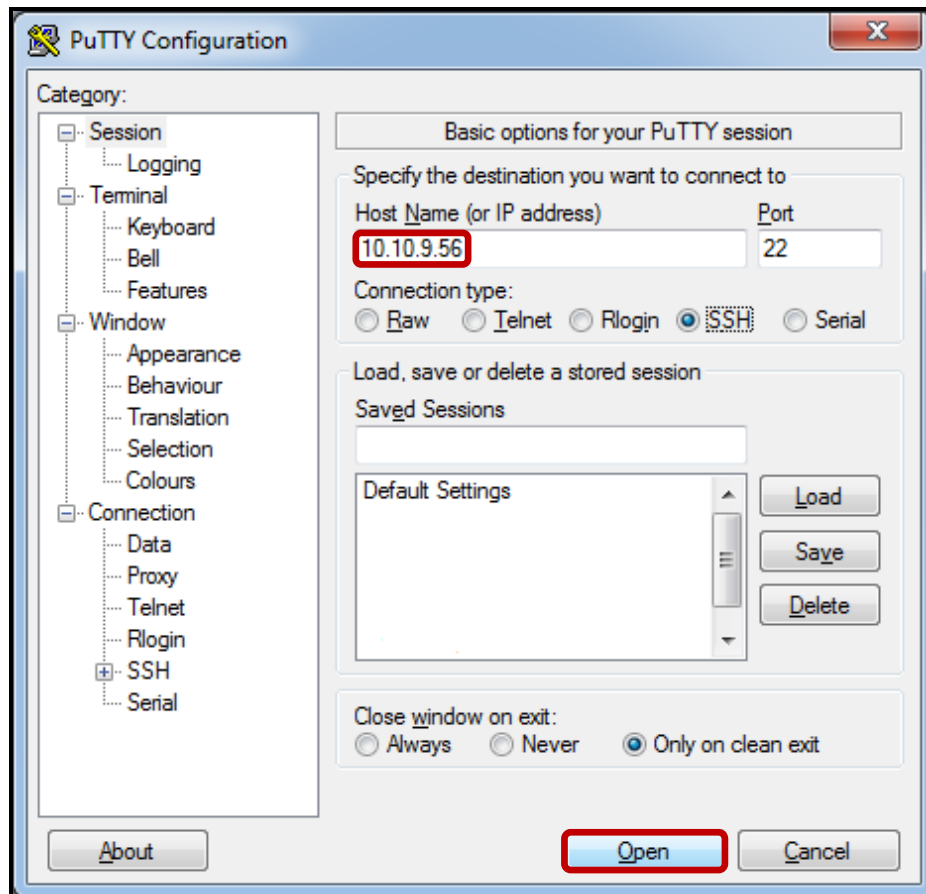
__c. Click **OK** to acknowledge.



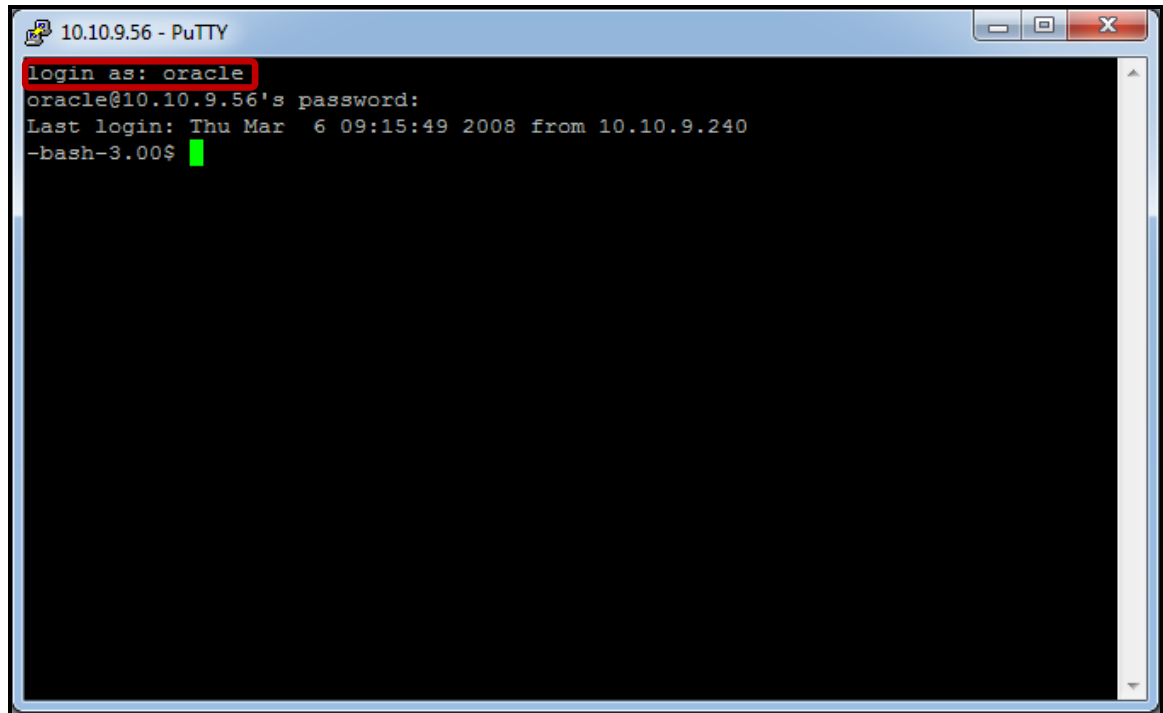
__d. Verify that the **V8 PoT Quarantine Policy** has been successfully installed. Check under the *View Installed Policy* section to the upper right of the screen.



- __4. Test the V8 PoT Quarantine Policy.
- __a. Using a PuTTY SSH client, access the VM database server to demonstrate the InfoSphere Guardium policy capability.
 - __b. Start the PuTTY SSH client login.
 - __c. From your laptop, launch PuTTY, enter **10.10.9.56**, and click **Open**.

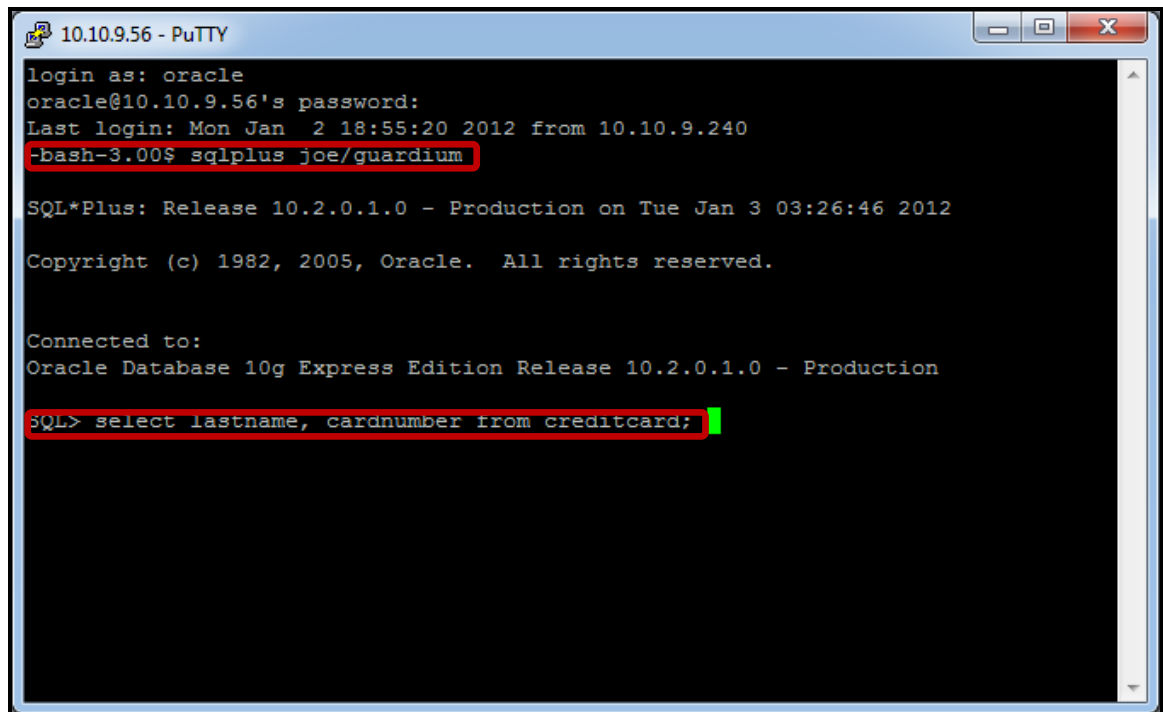


- __d. Login as **oracle** / **guardium**. After logging in, the following prompt will be displayed.



```
10.10.9.56 - PuTTY
login as: oracle
oracle@10.10.9.56's password:
Last login: Thu Mar  6 09:15:49 2008 from 10.10.9.240
-bash-3.00$ █
```

- __e. Login to Oracle as user *joe* by typing: **sqlplus joe/guardium**.
- __f. Type '**select lastname, cardnumber from creditcard;**'



```
10.10.9.56 - PuTTY
login as: oracle
oracle@10.10.9.56's password:
Last login: Mon Jan  2 18:55:20 2012 from 10.10.9.240
-bash-3.00$ sqlplus joe/guardium

SQL*Plus: Release 10.2.0.1.0 - Production on Tue Jan 3 03:26:46 2012

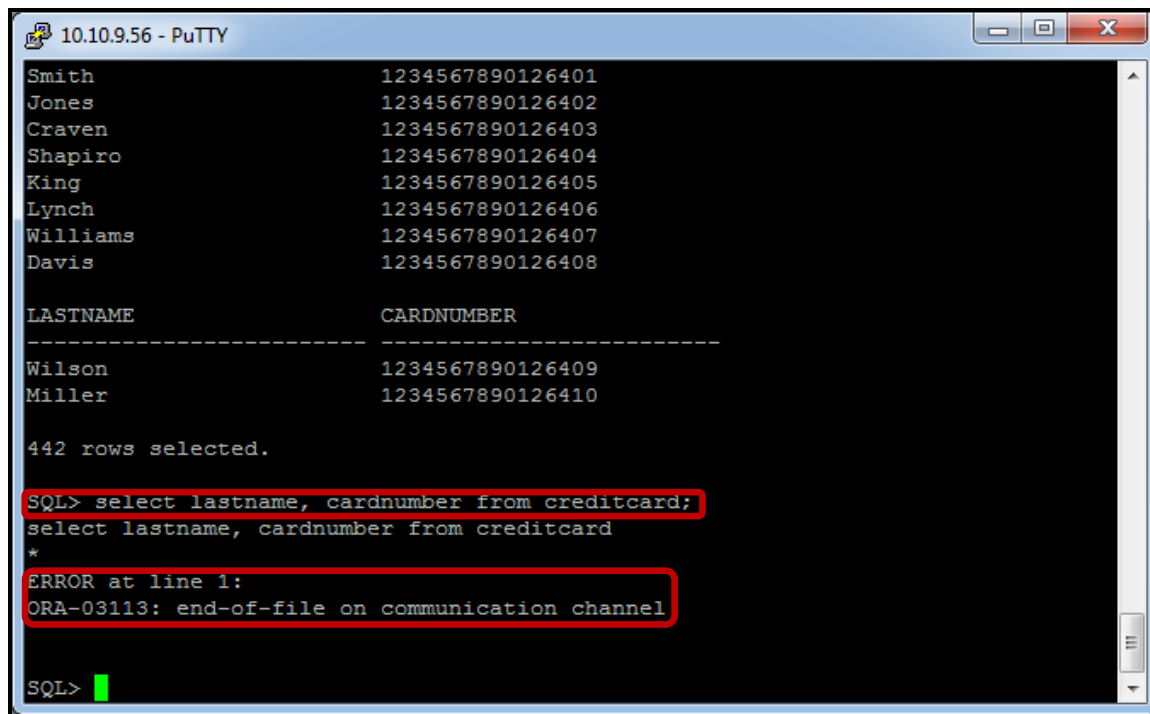
Copyright (c) 1982, 2005, Oracle. All rights reserved.

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

SQL> select lastname, cardnumber from creditcard; █
```

- __g. Type **'select lastname, cardnumber from creditcard;'** one more time.

Note: The initial select is successful with 442 rows selected, but the subsequent select is unsuccessful. The session is dropped and the user *joe* is quarantined.



```
10.10.9.56 - PuTTY
Smith          1234567890126401
Jones          1234567890126402
Craven         1234567890126403
Shapiro        1234567890126404
King           1234567890126405
Lynch          1234567890126406
Williams       1234567890126407
Davis          1234567890126408

LASTNAME      CARDNUMBER
-----
Wilson        1234567890126409
Miller        1234567890126410

442 rows selected.

SQL> select lastname, cardnumber from creditcard;
select lastname, cardnumber from creditcard
*
ERROR at line 1:
ORA-03113: end-of-file on communication channel

SQL>
```

- __5. Validate that the Policy has successfully triggered a Policy Violation.
 - __a. From the GUI click **Incident Management** under the **Protect** tab to view the *Policy Violations / Incident Management Report* and verify that the alert was actually recorded.

Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description	Incident Number	Policy Rule Violations
19	2012-01-03 04:43:54.0	PCI	Quarantine PCI Objects	10.10.9.56	10.10.9.56	JOE	select lastname, cardnumber from creditcard	MED	0	1
18	2012-01-03 04:43:50.0	PCI	Quarantine PCI Objects	10.10.9.56	10.10.9.56	JOE	select lastname, cardnumber from creditcard	MED	0	1
17	2012-01-03 04:42:03.0	PCI	Terminate Privileged User Credit Card Access	10.10.9.56	10.10.9.56	SYSTEM	by cardid	HIGH	0	1
16	2012-01-03 04:39:34.0		Alert on CreditCard Access	10.10.9.56	10.10.9.56	SYSTEM	select name, cardnumber from creditcard	INFO	0	1
15	2012-01-03 04:39:20.0		Alert on CreditCard Access	10.10.9.56	10.10.9.56	SYSTEM	check_object(creditcard)	INFO	0	1

We see the quarantined user (joe) with a medium severity level.

- __b. Logout as user **pot** and log back in as **admin/guardium**.

Login

Please enter your information

User name:

Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM. 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org, JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl, Jregistrykey © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com, Zthread © Copyright 2000-2003, Eric Crahen.

__c. Click **Connections Quarantined** under the **Daily Monitor** tab.

User Joe is quarantined for the time period (15 minutes) as specified by the policy rule.

The screenshot shows the IBM Security Guardium console interface. The 'Daily Monitor' tab is selected. In the left-hand navigation pane, 'Connections Quarantined' is highlighted. The main content area displays a table of quarantined connections. The table has the following columns: Server IP, Service Name, DB User, Access Code, TimeStamp, Quarantined Until, and Allowed Until. One record is shown, indicating a connection from 10.10.9.56 to ORACLEXE for user JOE, which was quarantined on 2012-01-03 at 04:43:54.0 and will be allowed until 2012-01-03 at 04:58:54.0. The record count at the bottom shows 1 record out of 1 total.

Server IP	Service Name	DB User	Access Code	TimeStamp	Quarantined Until	Allowed Until
10.10.9.56	ORACLEXE	JOE	0	2012-01-03 04:43:54.0	2012-01-03 04:58:54.0	

Thank You

Configuring Quarantine Policy review

- __1. A Quarantine action is valid for which policy rule type(s):
- __a. Access rule
 - __b. Exception rule
 - __c. Extrusion rule
 - __d. All above
- __2. Which policy rule attribute is required by a Quarantine action?
- __a. Records Affected Threshold
 - __b. Quarantine for ___ minutes
 - __c. Masking Pattern
 - __d. Time Period
- __3. What is the `gdapi` command to invoke a new quarantine?
- __a. `create_api_parameter_mapping`
 - __b. `update_rule`
 - __c. `create_group`
 - __d. `create_quarantine_allowed_until`
- __4. Quarantine actions can be automatically triggered as the result of query lines.
(**True** or **False**)

Configuring Quarantine Policy review (Answers)

__1. A Quarantine action is valid for which policy rule type(s):

D – All of the above.

__2. Which policy rule attribute is required by a Quarantine action?

B – Quarantine for ___ minutes.

__3. What is the grdapi command to invoke a new quarantine?

D – create_quarantine_allowed_until.

__4. Quarantine actions can be automatically triggered as the result of query lines.
(**True** or **False**)

True.

6.4 Configuring Redact (Data Masking) Policy

Overview

This InfoSphere Guardium feature allows a customer to mask portions of database query output (for example, credit card numbers) in reports for certain users. The selection Replacement Character in the Data Pattern/SQL Pattern section of the extrusion rule menu choices defines the masking character. Should the output produced by the extrusion rule match the regular expression of the Data Pattern, the portions that match sub-expressions between parenthesis "(" and ")" will be replaced by the masking character. Predefined regular expressions (fast regexp) can also be used.

InfoSphere Guardium provides the following built-in Redaction (SCRUB) functions to mask common sensitive data patterns necessary to adhere to compliance standards such as PCI-DSS and/or SOX:

- SCRUB_SSN_ANSI
- SCRUB_SSN_UNICODE
- SCRUB_CC_SPACES_ANSI
- SCRUB_CC_SPACES_UNICODE
- SCRUB_CC_SOLID_ANSI
- SCRUB_CC_SOLID_UNICODE
- SCRUB_AMEX_SOLID_ANSI
- SCRUB_AMEX_SOLID_UNICODE

Note: Redaction (Scrub) rules should only be set on the session level (that is, trigger rules on session attributes like IPs, Users, and so on), rather than the SQL level / attributes (such as - OBJECT_NAME or VERB). If the scrub rules are set on the SQL that needs to be scrubbed, it probably will take a few milliseconds for the scrub instructions to make it to the S-TAP where some results may go through unmasked.

Note: To guarantee all SQL is scrubbed, set the S-TAP (S-GATE) default mode to "attach" for all sessions (in guard_tap.ini). This will guarantee that no command goes through without being inspected by the rules engine and holding each request and waiting for the policy's verdict on the request. This deployment will introduce some latency but this is the way to ensure 100-percent scrubbed data.

Objectives

In this section, we will demonstrate how InfoSphere Guardium can mask sensitive data. This is critical when it comes to ensuring 'Need to Know' compliance requirements. The following objectives will be discussed:

- __1. Build a new policy.
- __2. Add a logging rule to the policy.
- __3. Add Redact (Scrub) rule to prevent unauthorized access to sensitive HIPAA objects.
- __4. Install the policy.
- __5. Test Redact features.

- __1. Start the InfoSphere Guardium appliance and login (if necessary, otherwise skip ahead).
 - __a. From your laptop, go to to <https://10.10.9.248:8443>
 - __b. Login as **pot / guardium**

Login

Please enter your information

User name:

Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

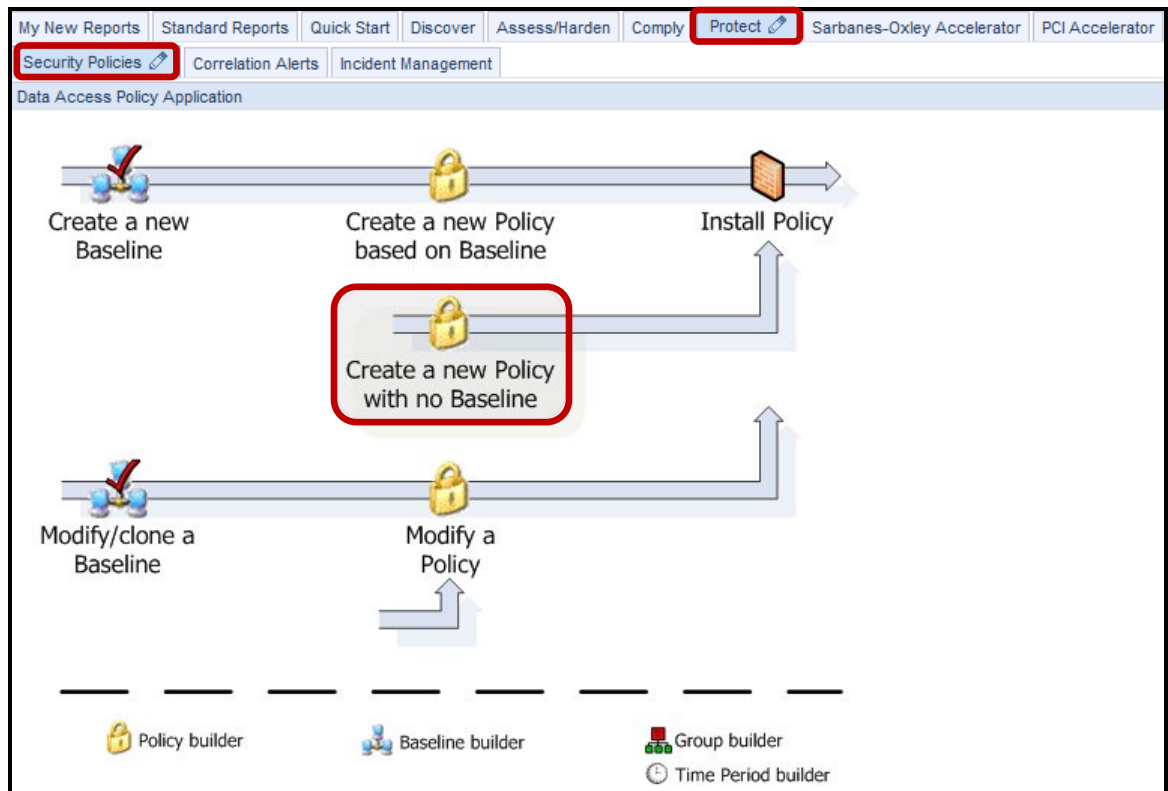
Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistry/key © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com, Zthread © Copyright 2000-2003, Eric Crahen.

__2. Use the InfoSphere Guardium GUI to create a new policy.

__a. Click **Security Policies** under the **Protect** tab.

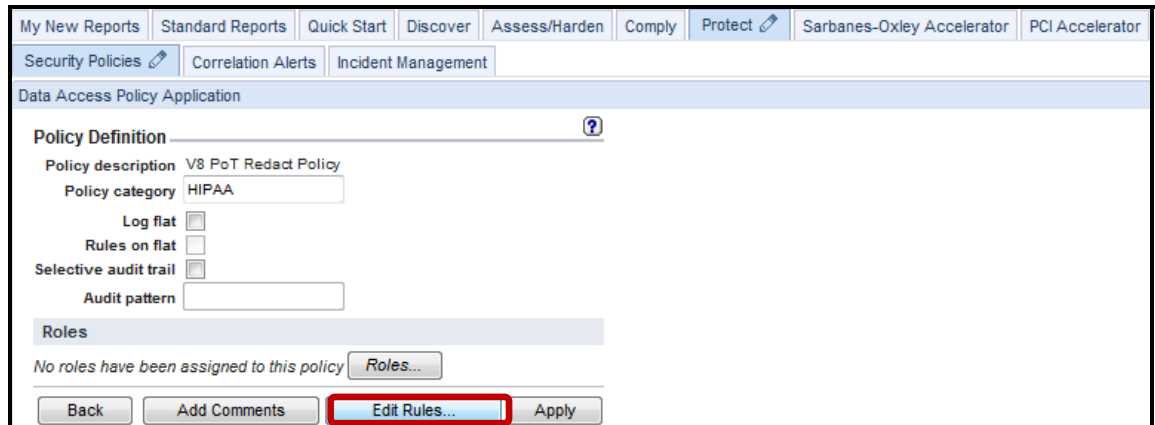
__b. Click **Create a new Policy with no Baseline**.



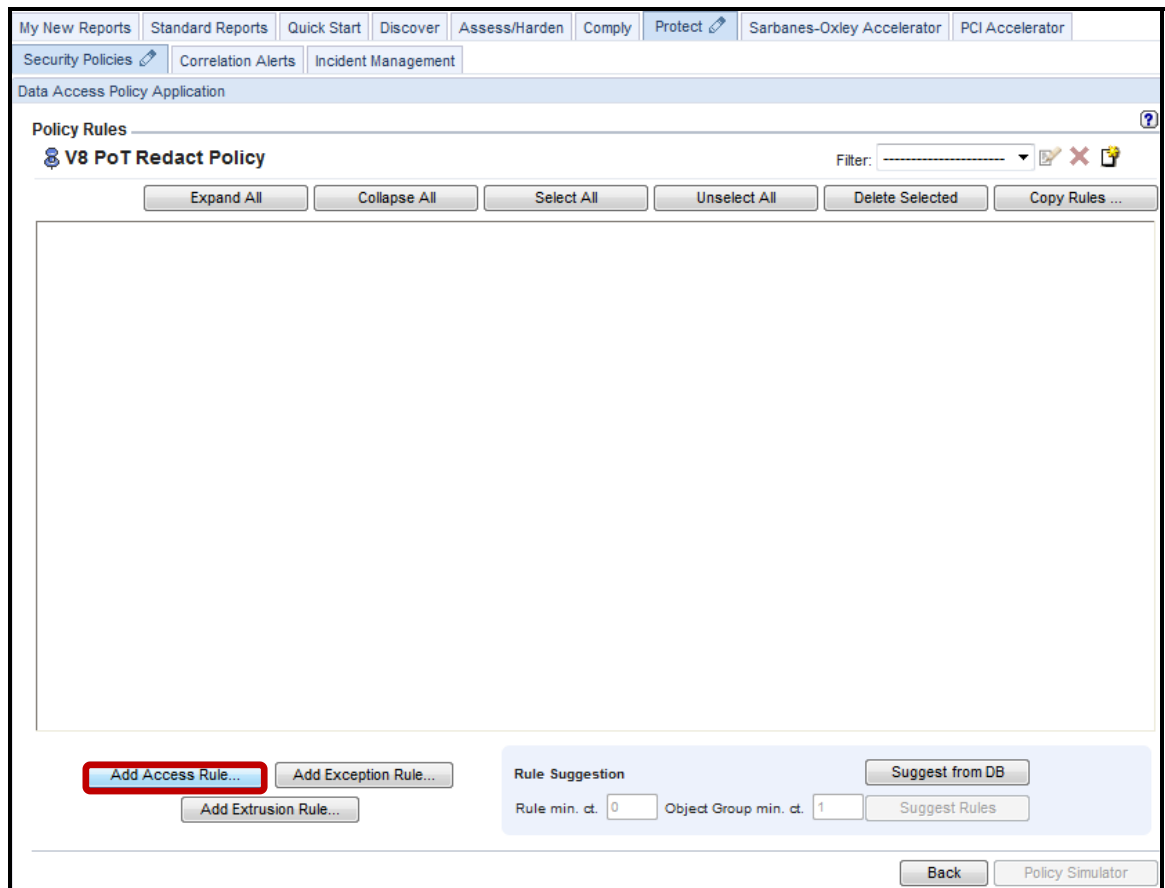
__c. Enter '**V8 PoT Redact Policy**' for *Policy description*, '**HIPAA**' for *Policy category*, and then click **Apply**.

The screenshot shows the 'Policy Definition' form in the InfoSphere Guardium GUI. The 'Policy description' field contains 'V8 PoT Redact Policy' and the 'Policy category' field contains 'HIPAA'. The 'Apply' button is highlighted with a red box.

__d. Click **Edit Rules** to add a rule to the policy.



__e. Click **Add Access Rule** to add first rule.



__f. Enter 'Log Full Details' for Description.

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

Security Policies | Correlation Alerts | Incident Management

Data Access Policy Application

Access Rule Definition ?

Rule #1 of policy V8 PoT Redact Policy

Description **Log Full Details**

Category Classification Severity INFO

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 and/or Group

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

Not Object and/or Group

Not Command and/or Group

Object/Cmd. Group

Object/Field Group

Pattern (RE)

XML Pattern (RE)

App Event Exists Event Type Event User Name

App Event Values Text and/or Group

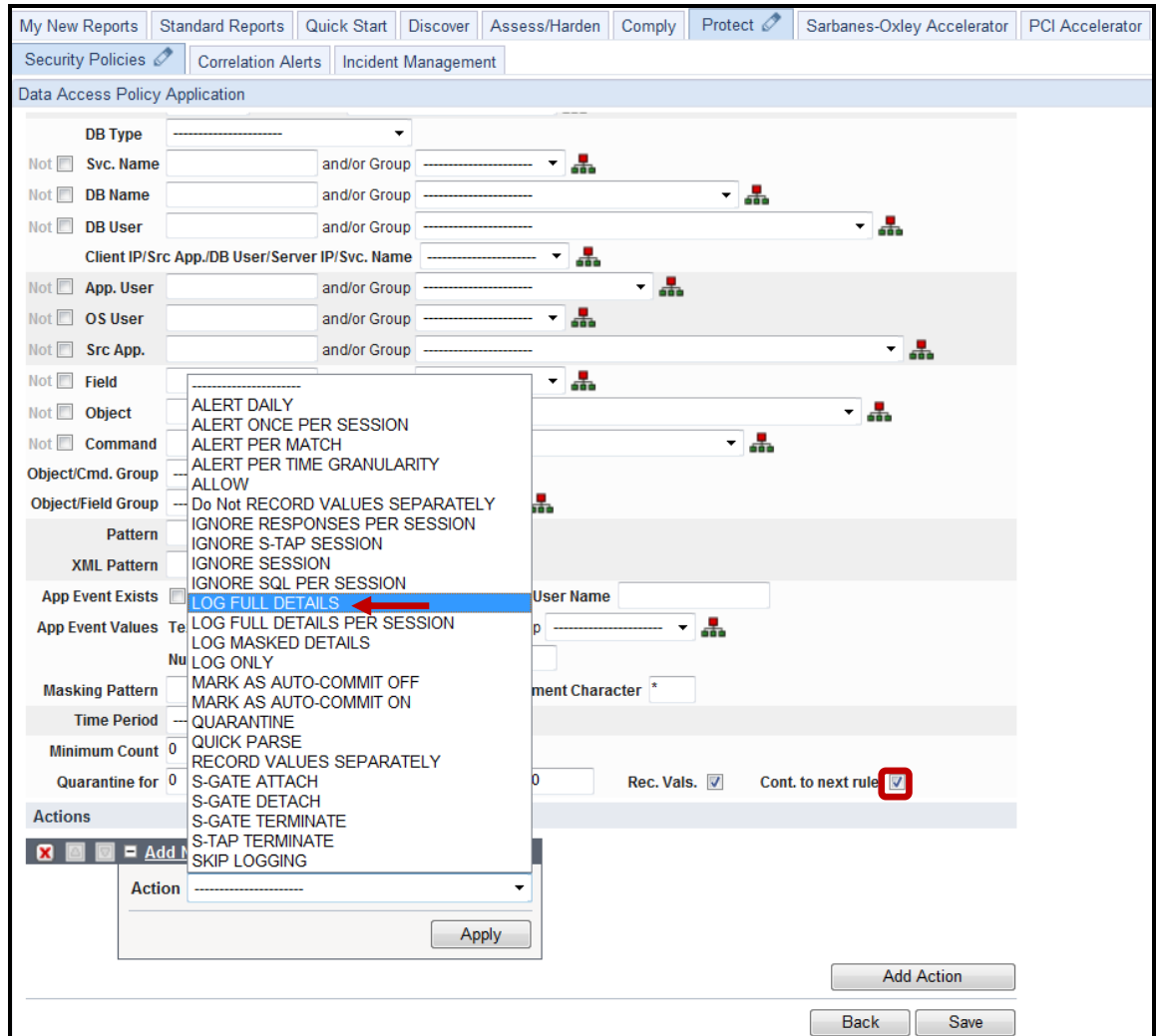
Numeric Date

Masking Pattern (RE) Replacement Character

g. Scroll down and click **Add Action**.

The screenshot displays the 'Data Access Policy Application' configuration page. The top navigation bar includes tabs for 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below this, there are sub-tabs for 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main content area is titled 'Data Access Policy Application' and contains a series of search criteria sections. Each section starts with a 'Not' checkbox and a text input field, followed by an 'and/or Group' dropdown menu and a small red icon with three vertical bars. The criteria include: Client MAC, Net Prtcl., DB Type, Svc. Name, DB Name, DB User, Client IP/Src App./DB User/Server IP/Svc. Name, App. User, OS User, Src App., Field, Object, Command, Object/Cmd. Group, Object/Field Group, Pattern, XML Pattern, App Event Exists, Event Type, Event User Name, App Event Values (Text, Numeric, Date), Masking Pattern, Replacement Character, Time Period, Minimum Count, Reset Interval, Quarantine for, Records Affected Threshold, Rec. Vals., and Cont. to next rule. At the bottom right, there is a red-bordered 'Add Action' button, a 'Back' button, and a 'Save' button.

- __h. **Critical Step** – Check the **Cont. to next rule** checkbox. If this is not checked, none of the subsequent rules will be processed. This must be repeated for all dependent rules.
- __i. Select **LOG FULL DETAILS** from the **ACTION** drop-down list.



j. Click **Apply** and then click **Save**.

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

Security Policies | Correlation Alerts | Incident Management

Data Access Policy Application

Not DB Name and/or Group

Not DB User and/or Group

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

Not Object and/or Group

Not Command and/or Group

Object/Cmd. Group

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

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

Actions

Add New Action

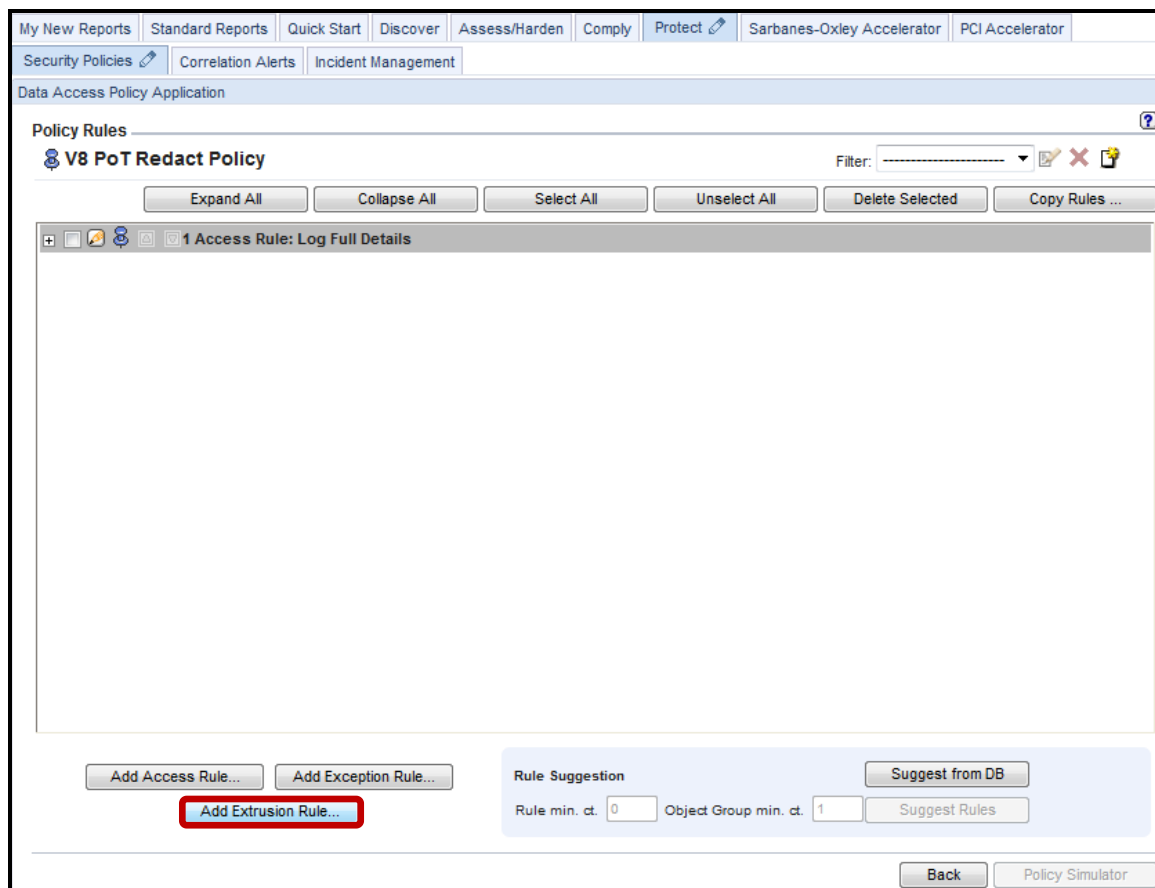
Action LOG FULL DETAILS

Apply

Add Action

Back Save

__k. Click **Add Extrusion Rule** to add the final rule.



- 1. Enter 'Mask Sensitive HIPAA Objects' in the *Description* field, 'joed' in the *DB User* field, 'SCRUB_SSN_ANSI' in the *Data Pattern* field, and then click **Add Action**.

The screenshot displays the 'Data Access Policy Application' interface for defining an 'Extrusion Rule'. The rule is identified as 'Rule #2 of policy V8 PoT Redact Policy'. The configuration fields are as follows:

- Description:** Mask Sensitive HIPAA Objects
- Category:** (Empty)
- Classification:** (Empty)
- Severity:** INFO
- DB User:** joed
- Data Pattern:** SCRUB_SSN_ANSI
- Replacement Character:** *
- Sql Pattern:** (Empty)
- Time Period:** (Empty)
- Minimum Count:** 0
- Reset Interval:** 0 minutes
- Quarantine for:** 0 minutes
- Matched Returned Data Threshold:** 0
- Rec. Vals.:**
- Revoke:**

The 'Add Action' button is highlighted with a red box, indicating the next step in the configuration process.

__m. Select **REDACT** from the *ACTION* drop-down list.

The screenshot displays the 'Extrusion Rule Definition' window for 'Rule #2 of policy V8 PoT Redact Policy'. The 'Description' field contains 'Mask Sensitive HIPAA Objects'. The 'Severity' is set to 'INFO'. A dropdown menu for 'Actions' is open, showing options like 'ALERT DAILY', 'LOG FULL DETAILS', and 'REDACT', with 'REDACT' highlighted by a red arrow. The 'Actions' list also includes 'S-TAP TERMINATE' and 'SET CHARACTER SET'. Other visible fields include 'Client IP', 'DB User' (set to 'joed'), and 'Replacement Character' (set to '*'). Buttons for 'Add Action', 'Back', and 'Save' are visible at the bottom.

__n. Click **Apply** and then click **Save**.

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

Security Policies | Correlation Alerts | Incident Management

Data Access Policy Application

Description: Mask Sensitive HIPAA Objects

Category: [] Classification: [] Severity: INFO

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: joed and/or Group []

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 []

Data Pattern: SCRUB_SSN_ANSI [RE] Replacement Character: *

Sql Pattern: [] [RE]

Time Period: []

Minimum Count: 0 Reset Interval: 0 minutes

Quarantine for: 0 minutes Matched Returned Data Threshold: 0 Rec. Vals. [x] Revoke []

Actions

[-] Add New Action

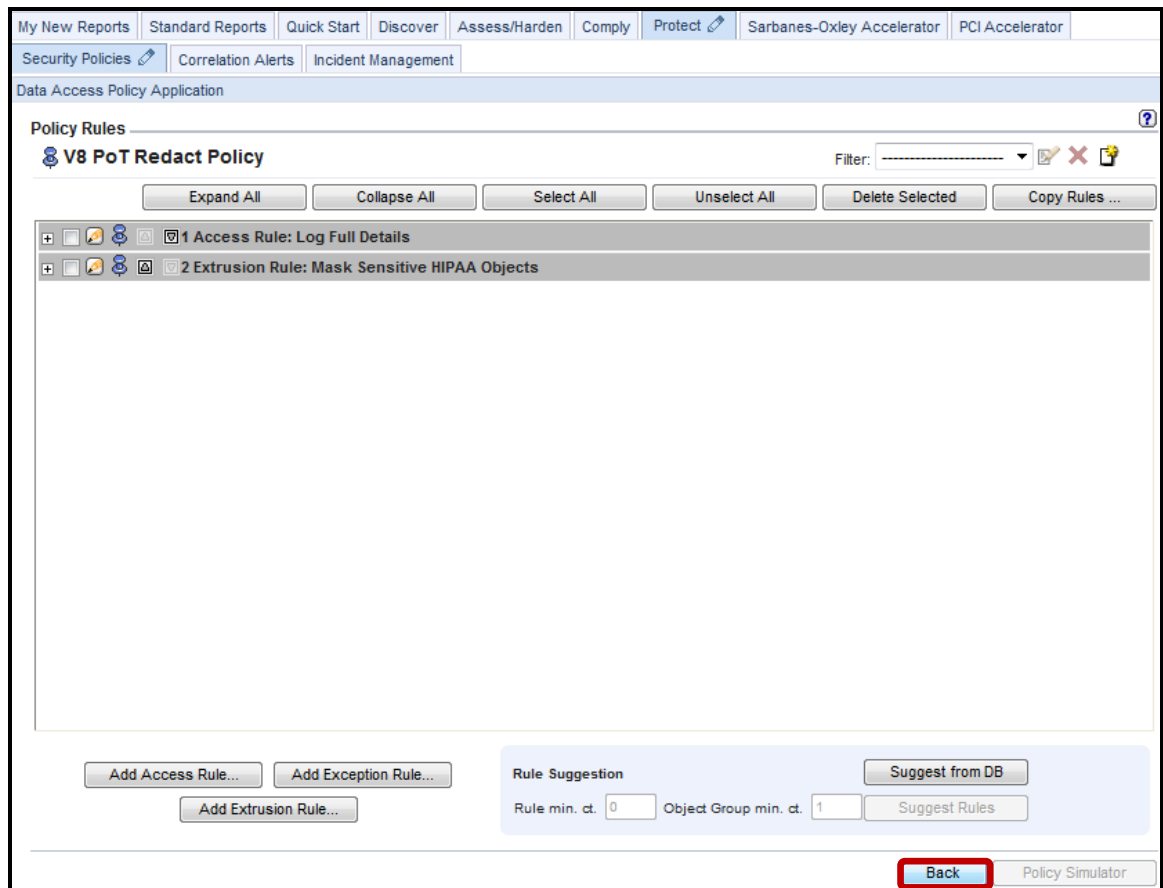
Action: REDACT

Apply

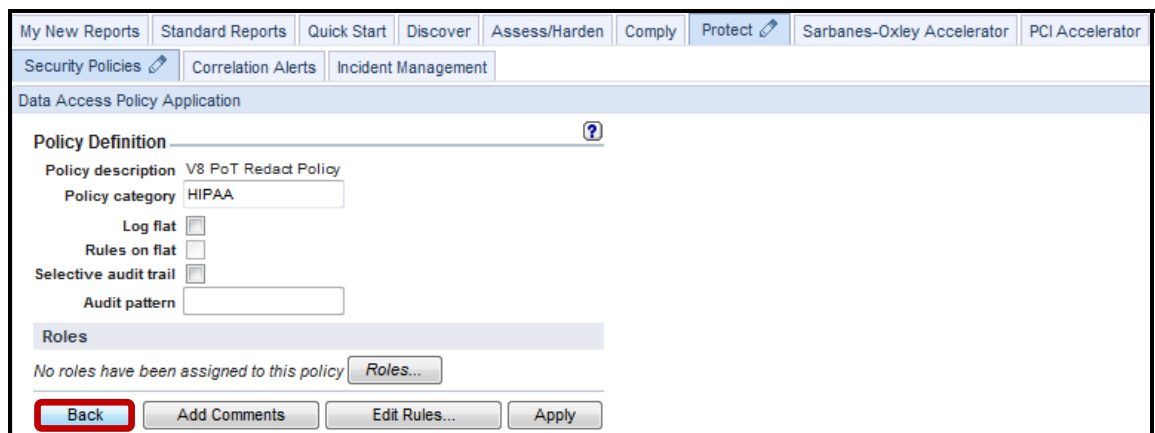
Add Action

Back Save

__o. Click **Back** to return to the Policy Definition screen.

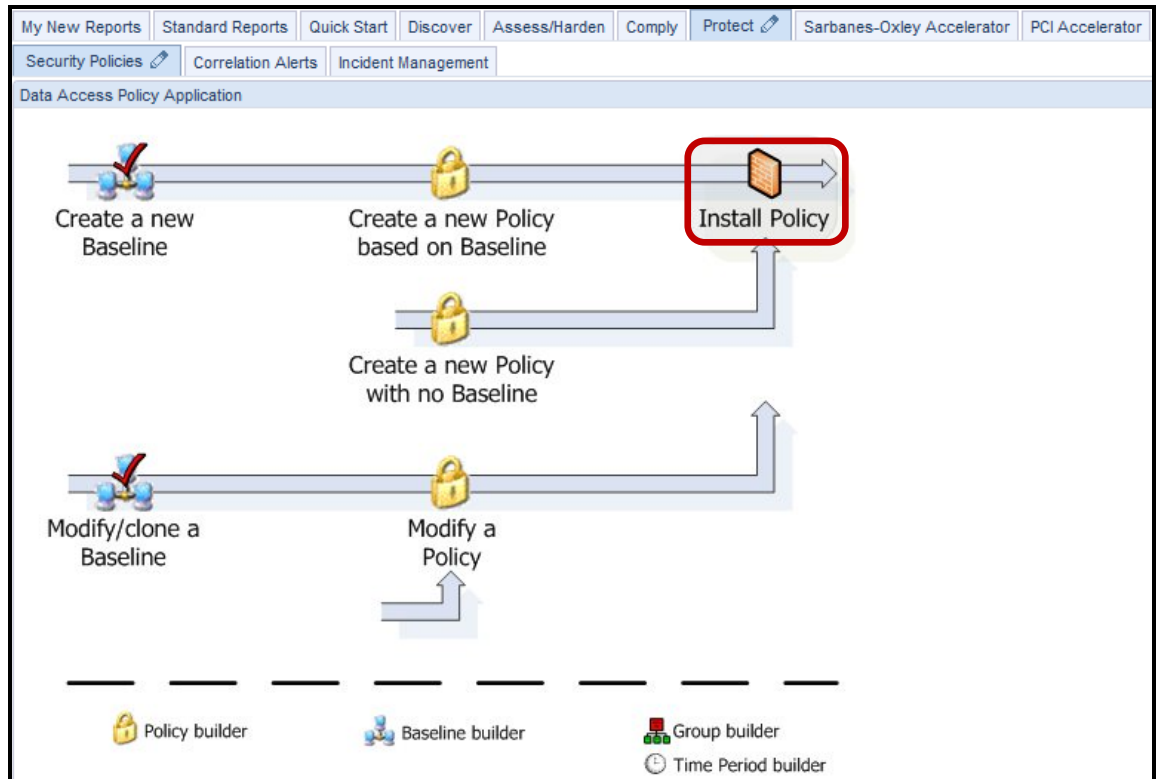


__p. Click **Back** once more to return to the main **Security Policies** tab screen.

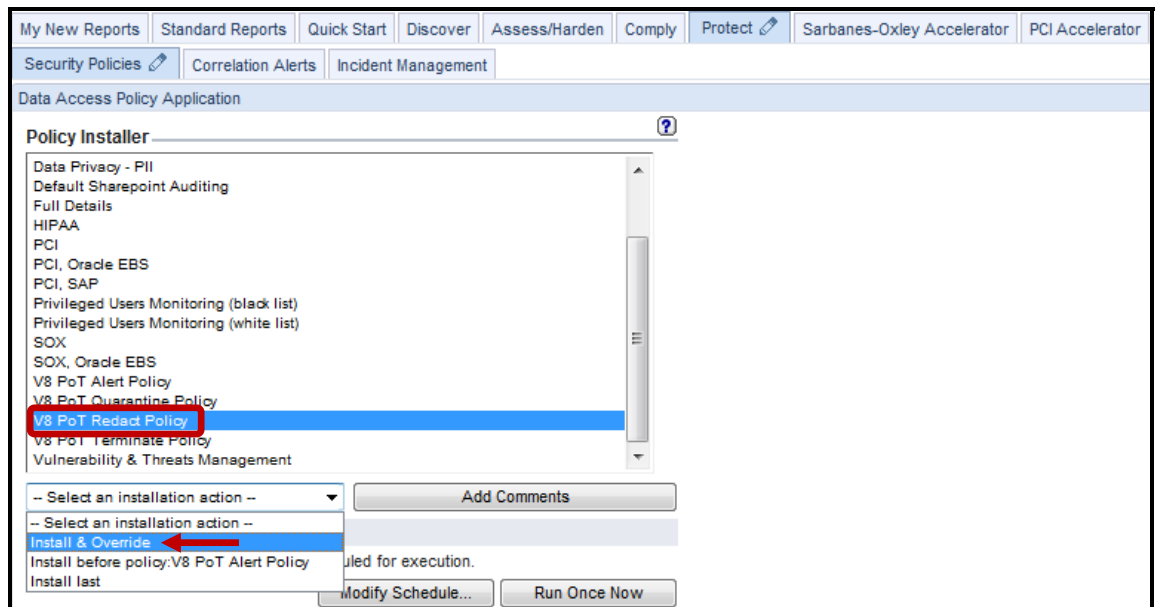


__3. Install the V8 PoT Redact Policy.

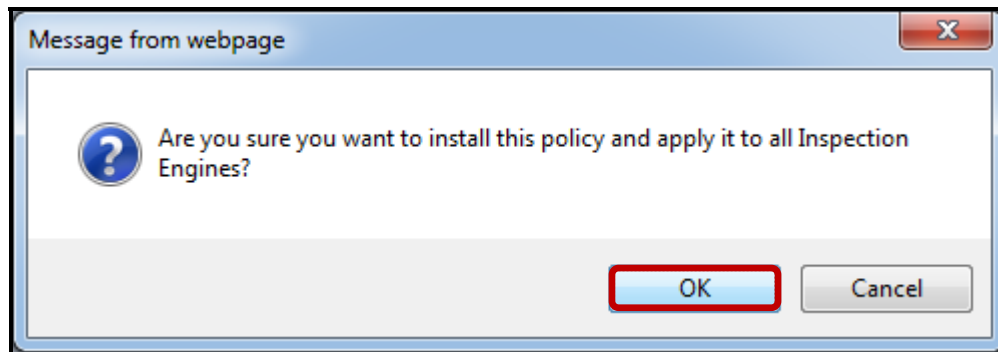
__a. Click **Install Policy**.



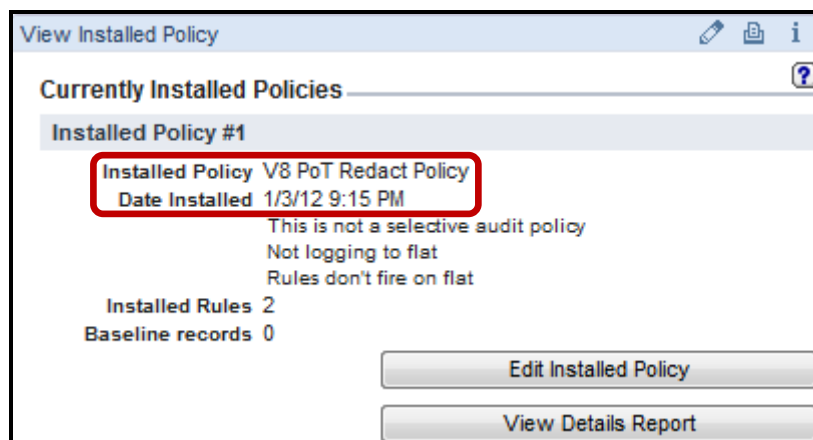
__b. Scroll down, select **V8 Redact Policy** from the *Policy installer* list, and then select **Install & Override** from the *Select an installation action* drop-down list.



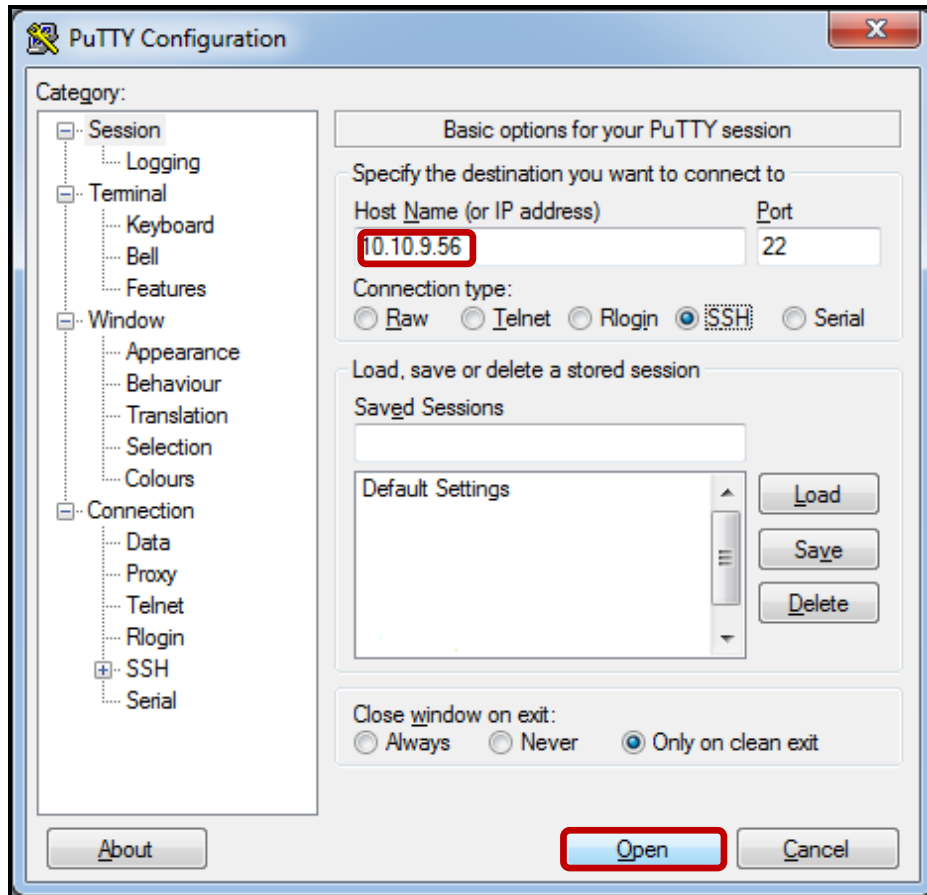
- __c. Click **OK** to acknowledge.



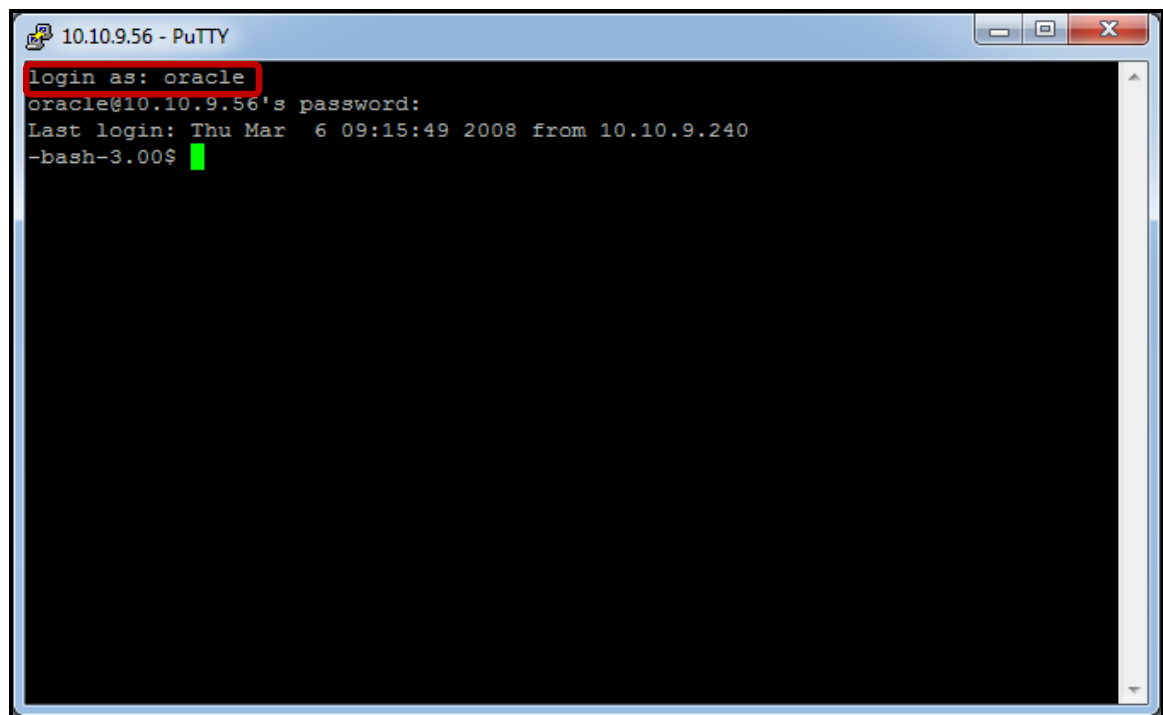
- __d. Verify that the **V8 PoT Redact Policy** has been successfully installed. Check under the *View Installed Policy* section to the upper right of the screen.



- __4. Test the V8 PoT Redact Policy.
 - __a. Using a PuTTY SSH client, access the VM database server to demonstrate the InfoSphere Guardium policy capability.
 - __b. Start the PuTTY SSH client login.
 - __c. From your laptop, launch PuTTY, enter **10.10.9.56**, and click **Open**.

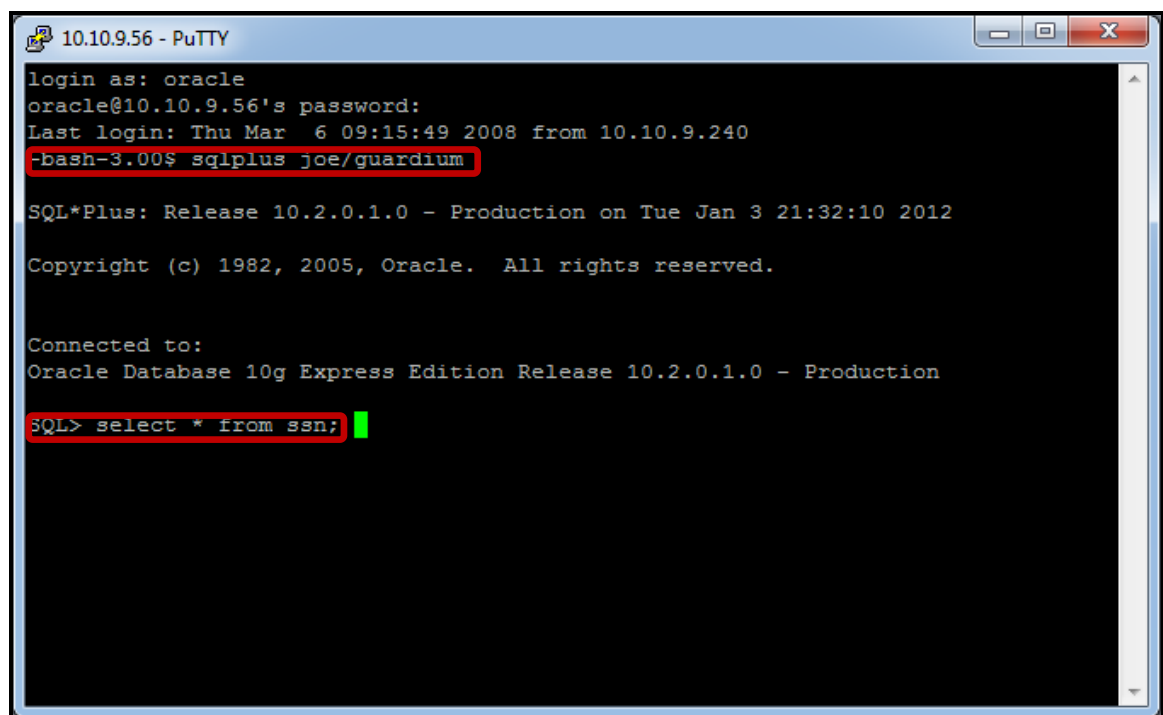


- __d. Login as **oracle** / **guardium**. After logging in, the following prompt will be displayed.



```
10.10.9.56 - PuTTY
login as: oracle
oracle@10.10.9.56's password:
Last login: Thu Mar  6 09:15:49 2008 from 10.10.9.240
-bash-3.00$ █
```

- __e. Login to Oracle as user *joe* by typing: **sqlplus joe/guardium**, then type **'select * from ssn;'**



```
10.10.9.56 - PuTTY
login as: oracle
oracle@10.10.9.56's password:
Last login: Thu Mar  6 09:15:49 2008 from 10.10.9.240
-bash-3.00$ sqlplus joe/guardium

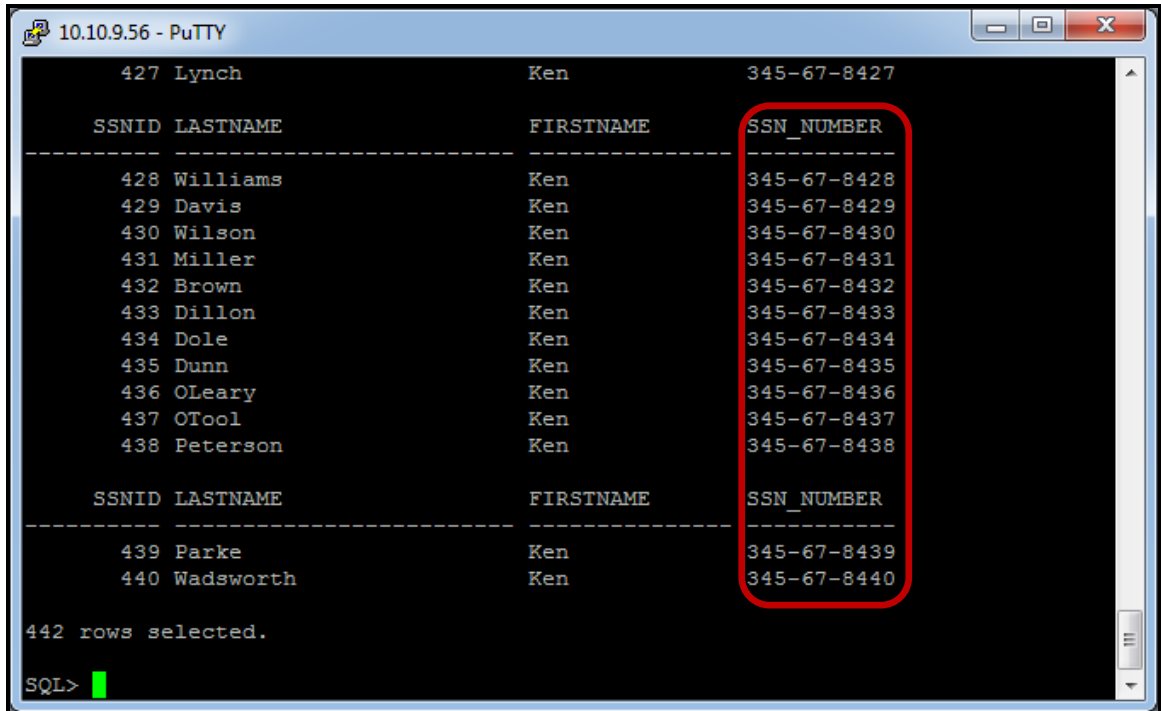
SQL*Plus: Release 10.2.0.1.0 - Production on Tue Jan 3 21:32:10 2012

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

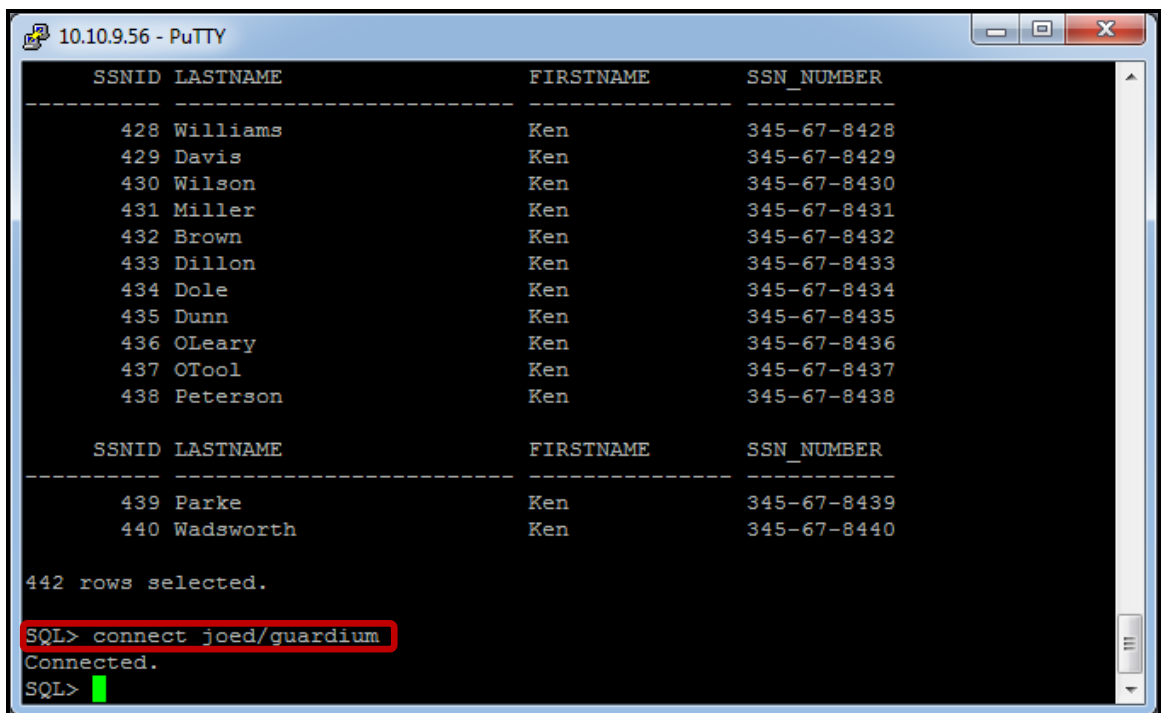
Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

SQL> select * from ssn; █
```

Note: Joe is authorized to view *unmasked*, sensitive data, as a function of his job role because he has a 'Need to Know.'

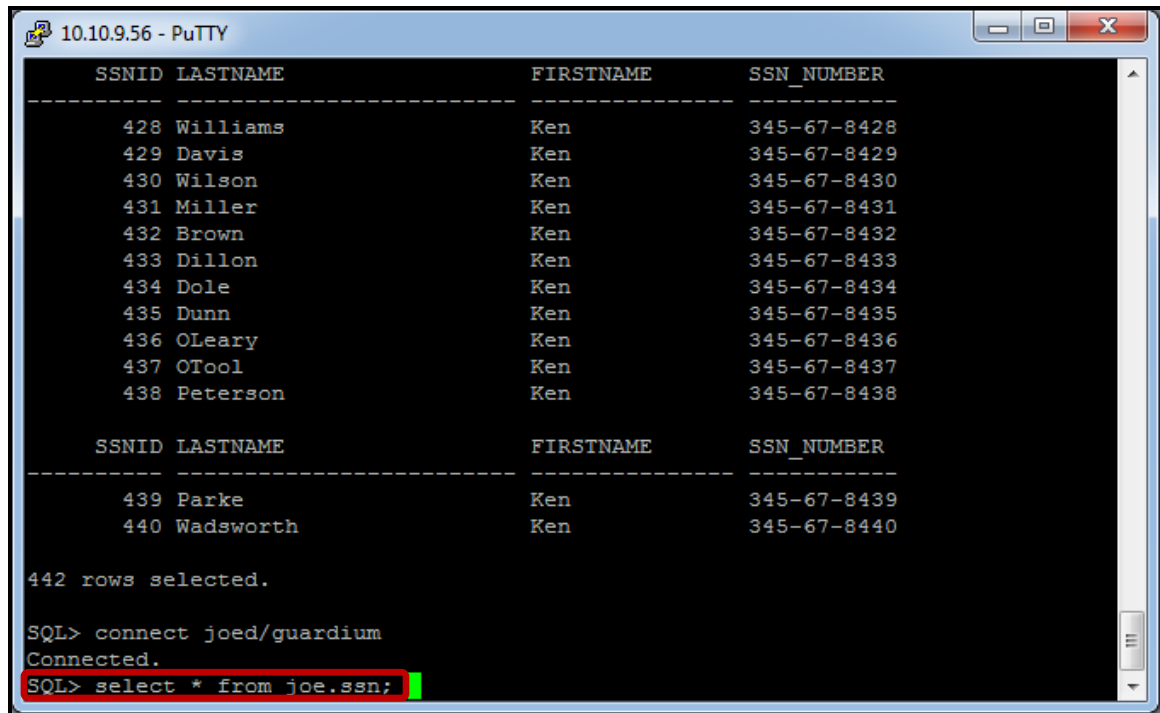


__f. Now, login to Oracle as user *joed* by typing: 'connect joed/guardium.'



__g. Type 'select * from joe.ssn;'

Note: JoeD is not authorized to view sensitive data, and has no 'Need to Know' the actual contents of the data.



```

10.10.9.56 - PuTTY
-----
SSNID LASTNAME                FIRSTNAME  SSN_NUMBER
-----
428 Williams                Ken        345-67-8428
429 Davis                   Ken        345-67-8429
430 Wilson                  Ken        345-67-8430
431 Miller                  Ken        345-67-8431
432 Brown                   Ken        345-67-8432
433 Dillon                  Ken        345-67-8433
434 Dole                     Ken        345-67-8434
435 Dunn                     Ken        345-67-8435
436 OLeary                  Ken        345-67-8436
437 OTool                   Ken        345-67-8437
438 Peterson                Ken        345-67-8438

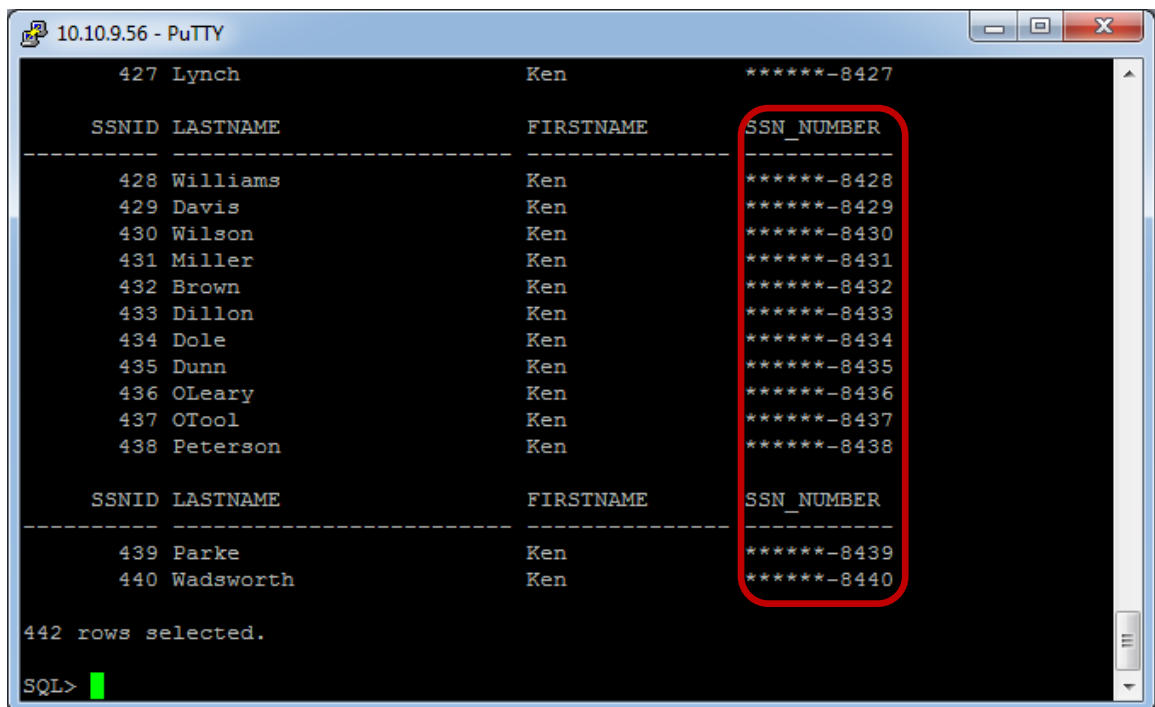
-----
SSNID LASTNAME                FIRSTNAME  SSN_NUMBER
-----
439 Parke                    Ken        345-67-8439
440 Wadsworth                Ken        345-67-8440

442 rows selected.

SQL> connect joed/guardium
Connected.
SQL> select * from joe.ssn;

```

As we can see, the Redact Policy triggers to mask all sensitive data returned to JoeD.



```

10.10.9.56 - PuTTY
-----
427 Lynch                    Ken        *****-8427

-----
SSNID LASTNAME                FIRSTNAME  SSN_NUMBER
-----
428 Williams                Ken        *****-8428
429 Davis                   Ken        *****-8429
430 Wilson                  Ken        *****-8430
431 Miller                  Ken        *****-8431
432 Brown                   Ken        *****-8432
433 Dillon                  Ken        *****-8433
434 Dole                     Ken        *****-8434
435 Dunn                     Ken        *****-8435
436 OLeary                  Ken        *****-8436
437 OTool                   Ken        *****-8437
438 Peterson                Ken        *****-8438

-----
SSNID LASTNAME                FIRSTNAME  SSN_NUMBER
-----
439 Parke                    Ken        *****-8439
440 Wadsworth                Ken        *****-8440

442 rows selected.

SQL>

```

Thank You

Configuring Redact (Data Masking) Policy review

- __1. For which platform(s) does InfoSphere Guardium provide Data Redaction support?
- __a. Unix
 - __b. Windows
 - __c. Linux
 - __d. A and B
 - __e. B and C
 - __f. All OS
- __1. How do you define the data targeted for redaction?
- __a. Create a query, and add a condition based upon a pattern
 - __b. Create a policy rule, and use Regex to define the Masking pattern
 - __c. Configure redact settings in the Admin Console.
 - __d. Setup a correlation alert with two conditions; one for alert, and one for redact
- __2. InfoSphere Guardium Data Redaction is granular enough to redact a single table column. **(True or False)**.
- __3. Data redaction SCRUB functions only support ANSI character sets. **(True or False)**.

Configuring Redact (Data Masking) Policy review (Answers)

__1. For which platform(s) does InfoSphere Guardium provide Data Redaction support?

D – A (Unix) and B (Windows).

__2. How do you define the data targeted for redaction?

B – Create a policy rule, and use Regular Expression to define the Masking pattern.

__3. InfoSphere Guardium Data Redaction is granular enough to redact a single table column.
(**True** or **False**).

False.

__4. Data redaction SCRUB functions only support ANSI character sets.
(**True** or **False**).

True.

Lab 7 Vulnerability Assessment

7.1 Exploring Vulnerability Assessment

Overview

One of the best ways to secure database infrastructures, and comply with regulations and pass your audits, is to perform security assessments of your database environment regularly.

Security assessments evaluate the security strength of your database environment and compare it with industry best practices. These in-depth evaluations examine patch levels and database configurations to highlight vulnerabilities in your environment, so you can quickly remediate problems and safeguard your critical enterprise data from internal and external threats.

The IBM® InfoSphere® Guardium® Database Vulnerability Assessment (VA) module scans your database infrastructure for vulnerabilities and provides an ongoing evaluation of your security posture, using both real-time and historical data. This capability includes a comprehensive library of preconfigured tests based on industry-best practices such as the Computer Internet Security (CIS) benchmarks and the Database Security Technical Implementation Guide (STIG) created by the Department of Defense (DoD). These tests check for common vulnerabilities, such as missing patches, weak passwords, misconfigured privileges and default accounts, as well as unique vulnerabilities for each DBMS platform.

Tests are updated on a quarterly basis by way of the InfoSphere Guardium Knowledgebase service. You can also define custom tests and schedule automated audit tasks incorporating scans, distribution of reports, electronic sign-offs and escalations.

In addition to producing detailed reports with drill-down capabilities, the assessment module recommends concrete action plans, for each vulnerability, to help you strengthen security. For example, if there are privilege-related issues, the system will tell you exactly which privileges need to be revoked in order to comply with best practices. Test results also include references to related external resources, such as Common Vulnerabilities and Exposures (CVE) identifiers.

Objectives

This Lab will illustrate how we can create a new Vulnerability Assessment using the InfoSphere Guardium GUI. The following objectives will be targeted:

- __1. Start a new Vulnerability Assessment.
- __2. Select (create) a target datasource.
- __3. Identify the preconfigured tests for the assessment.
- __4. Run the Assessment.
- __5. View the Results.

- __1. Using the InfoSphere Guardium GUI, demonstrate the ease of use within the InfoSphere Guardium solution. Start the InfoSphere Guardium appliance and login.
- __a. From your laptop, go to to <https://10.10.9.248:8443>.
- __b. Login as **pot / guardium**.

Login

Please enter your information

User name:

Password:

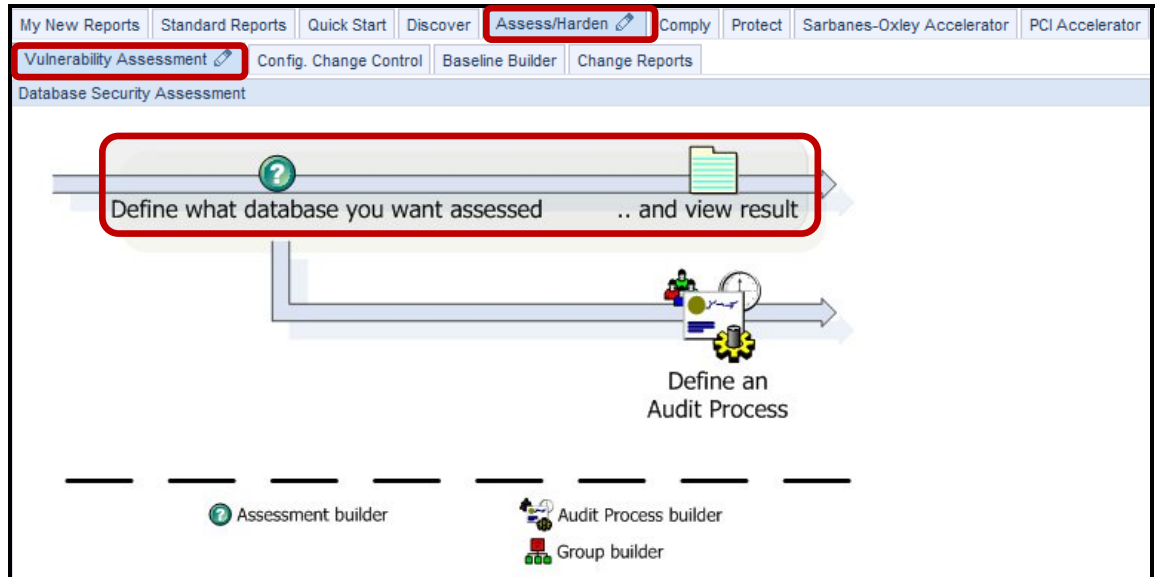
Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

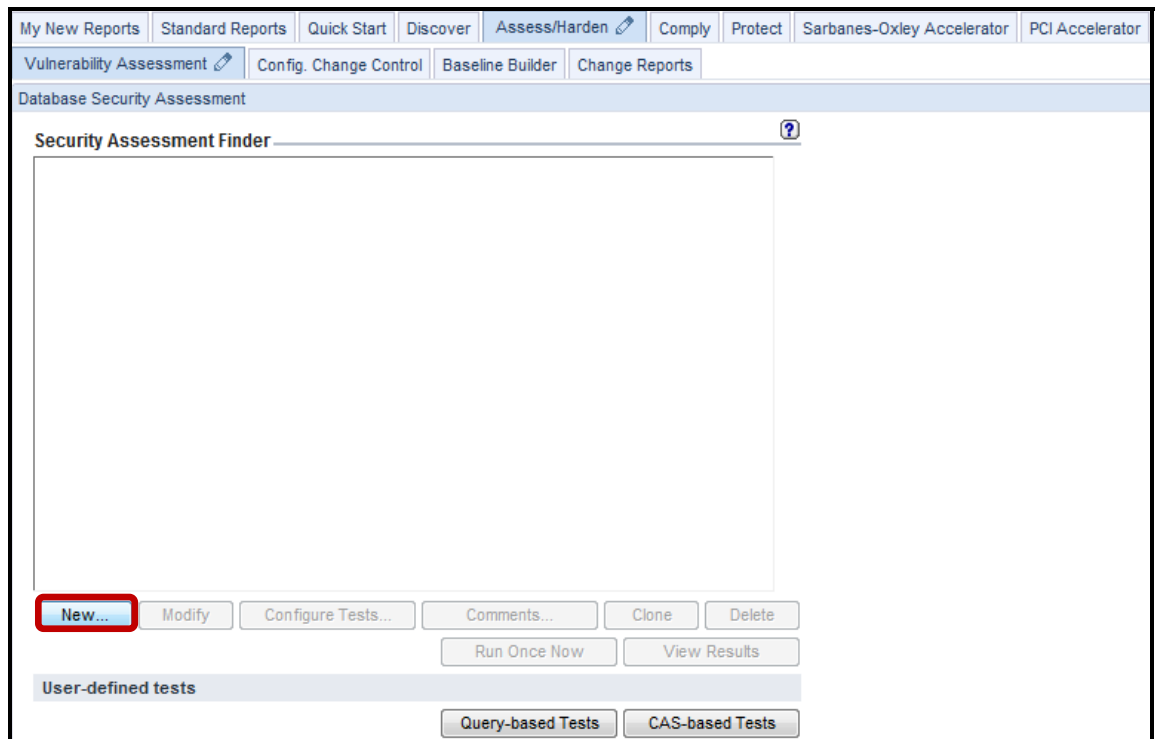
CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistrykey © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

__2. Create a new Vulnerability Assessment.

__a. Click the **Vulnerability Assessment** tab under the **Assess/Harden** tab, and then click 'Define what database you want assessed .. and view result'.



__b. Click **New**.



- __c. Enter 'V8 PoT Oracle VA' for *Description* and click **Add Datasource**.

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

Vulnerability Assessment | Config. Change Control | Baseline Builder | Change Reports

Database Security Assessment

Security Assessment Builder

Description: **V8 PoT Oracle VA**

Observed Test Parameters:

Period From: NOW -1 DAY

To: NOW

Client IP or IP subnet: (optional)

Server IP or IP subnet: (optional)

Datasources

Name	Type	Host	UserName
No datasource has been added to this item			

Add Datasource...

Roles

No Roles have been assigned to this Security Assessment Roles...

Revert | Apply | Configure Tests... | CAS Support... | Back

- __d. Select **osprey_system_ORACLE(Classifier)** from the *Datasource Finder* list, and click **Add**.

Datasource Finder

osprey_admin_MYSQL(Classifier)

osprey_db2inst2_DB2(Classifier)

osprey_postgres_POSTGRESQL(Classifier)

osprey_sa_SYBASE(Classifier)

osprey_system_ORACLE(Classifier)

Select multiple items using Shift- or Ctrl-click

New | Clone | Modify | Delete | **Add** | Back

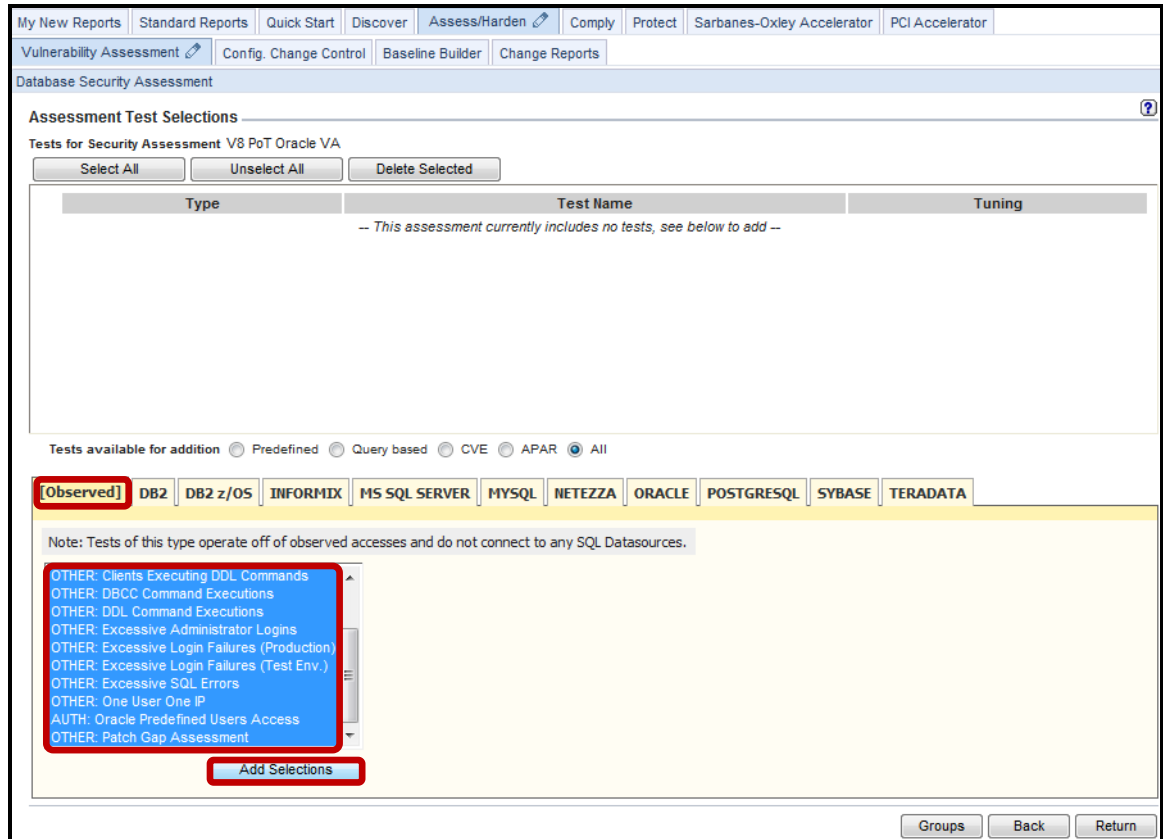
__e. Click **Apply**.

The screenshot shows the 'Security Assessment Builder' interface. At the top, there is a navigation bar with tabs: 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden' (active), 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below this is a sub-navigation bar with 'Vulnerability Assessment' (active), 'Config. Change Control', 'Baseline Builder', and 'Change Reports'. The main content area is titled 'Database Security Assessment' and contains the 'Security Assessment Builder' form. The form includes a 'Description' field with the value 'V8 PoT Oracle VA'. Under 'Observed Test Parameters', there are 'Period From' (NOW -1 DAY) and 'To' (NOW) fields, each with a calendar icon. There are also optional fields for 'Client IP or IP subnet' and 'Server IP or IP subnet'. Below these is a 'Datasources' table with one entry: 'osprey_system_ORACLE(Classifier)' of type 'ORACLE' on host '10.10.9.56' with user 'system'. A 'Roles' section below the table shows 'No Roles have been assigned to this Security Assessment' with a 'Roles...' button. At the bottom, there are buttons for 'Revert', 'Apply' (highlighted in red), 'Configure Tests...', 'CAS Support...', and 'Back'.

__f. Click **Configure Tests**.

This screenshot is identical to the one above, showing the 'Security Assessment Builder' interface. The only difference is that the 'Configure Tests...' button at the bottom of the form is highlighted in red, indicating the next step in the process.

- __g. Select all of the **[Observed]** tests either by clicking and dragging to the end of the list or by clicking the first test, scrolling down to the bottom, and pressing Shift and click on the last test.
- __h. Click **Add Selections** to add all of the selecting test conditions.



i. Click the **ORACLE** tab, select all of the Oracle tests, and click **Add Selections**.

The screenshot shows the 'Assessment Test Selections' window in the IBM InfoSphere Guardium V8.2 interface. The window title is 'Assessment Test Selections' and it is for 'Tests for Security Assessment V8 PoT Oracle VA'. The 'ORACLE' tab is selected among other database types like DB2, Informix, etc. A list of tests is shown with columns for Type, Test Name, and Tuning. A red box highlights the 'Add Selections' button at the bottom of the test list.

Type	Test Name	Tuning
<input type="checkbox"/>	Access Rule Violations	OTHER Major 10: Maximum Number of Policy violations allowed per day (after factoring the assessed period)
<input type="checkbox"/>	Admin Command Executions	OTHER Informational 30: Maximum Number of administration commands allowed per day (after factoring the assessed period)
<input type="checkbox"/>	After Hours Logins	OTHER Minor 5: Maximum number of after-hours logins allowed
<input type="checkbox"/>	Clients Executing Admin Commands	OTHER Minor 3: Maximum Number of clients executing administration commands allowed
<input type="checkbox"/>	Clients Executing DDL Commands	OTHER Minor 2: Maximum Number of clients executing DDL commands allowed
<input type="checkbox"/>	DBCC Command Executions	OTHER Informational 5: Maximum Number of DBCC commands allowed per day (after factoring the assessed period)

Tests available for addition: Predefined Query based CVE APAR All

Database tabs: [Observed] | DB2 | DB2 z/OS | INFORMIX | MS SQL SERVER | MYSQL | NETEZZA | **ORACLE** | POSTGRESQL | SYBASE | TERADATA

Tests marks with an asterisk (*) require specific CAS monitoring running on the Datasource(s) tested

- CONF: SQL92_SECURITY is true
- CONF: SQLNET.EXPIRE_TIME within limit *
- CONF: SQLNET.INBOUND_CONNECT_TIMEOUT within limit *
- AUTH: SYS And SYSTEM Account Status Is Not Open.
- CONF: TCP.EXCLUDED_NODES is set *
- CONF: TCP.INVITED_NODES is set *
- CONF: TCP.VALIDNODE_CHECKING set to Yes *
- CONF: UTL_FILE_DIR Should Not Point To Sensitive Directories
- VER: Version: Oracle
- AUTH: Weak Passwords Are Screened

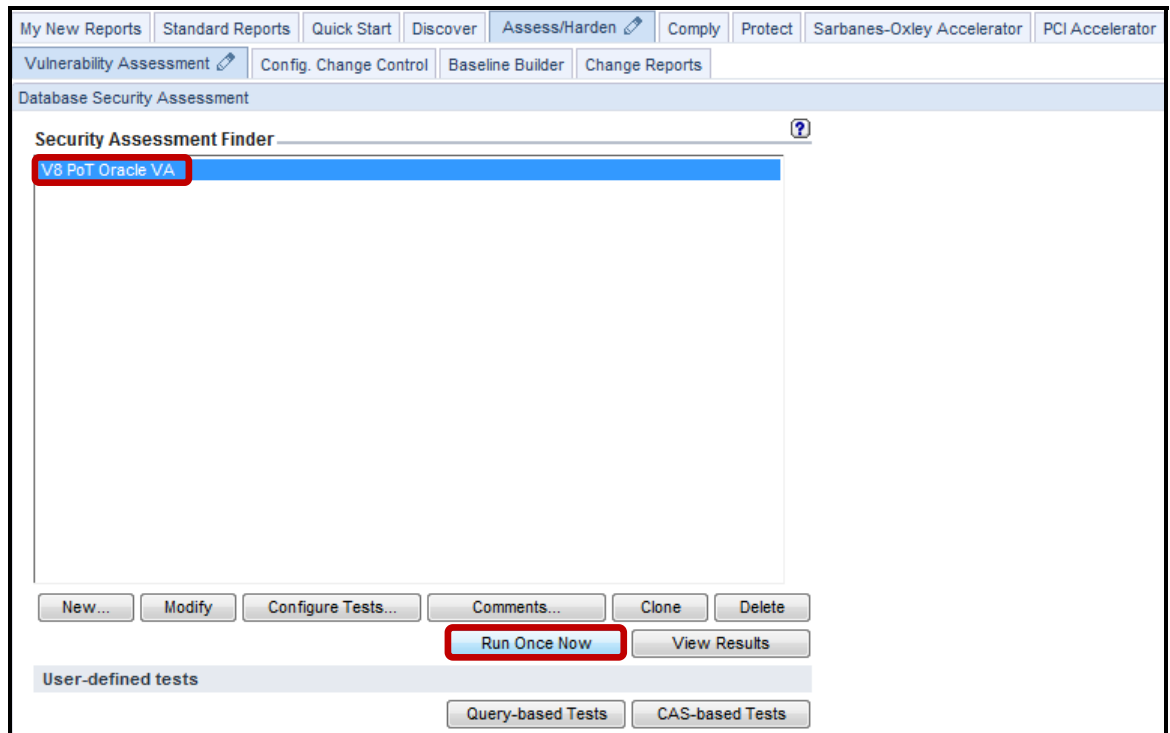
Add Selections

j. Click **Return** to save the assessment and return to the initial screen.

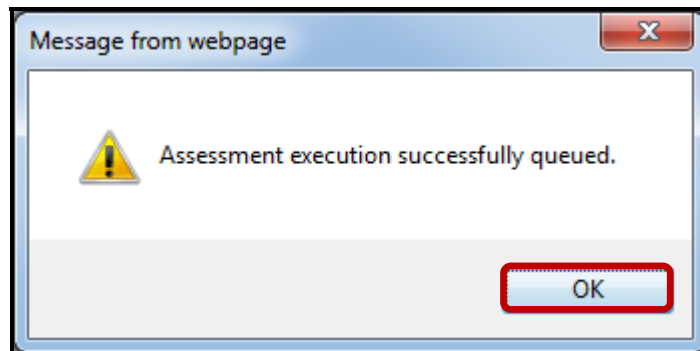
The screenshot displays the 'Database Security Assessment' interface. At the top, there are navigation tabs: 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below these are sub-tabs: 'Vulnerability Assessment', 'Config. Change Control', 'Baseline Builder', and 'Change Reports'. The main section is titled 'Database Security Assessment' and contains 'Assessment Test Selections' for 'Tests for Security Assessment V8 PoT Oracle VA'. There are buttons for 'Select All', 'Unselect All', and 'Delete Selected'. A table lists various tests with columns for 'Type', 'Test Name', and 'Tuning'. The 'Tuning' column contains details for tests like 'OTHER Major 10', 'OTHER Informational 30', 'OTHER Minor 5', 'OTHER Minor 3', 'OTHER Minor 2', and 'OTHER Informational 5'. Below the table, there are radio buttons for 'Tests available for addition' with options: 'Predefined', 'Query based', 'CVE', 'APAR', and 'All'. A database type selector shows 'ORACLE' selected among others like 'DB2', 'INFORMIX', 'MS SQL SERVER', 'MYSQL', 'NETEZZA', 'POSTGRESQL', 'SYBASE', and 'TERADATA'. A note states: 'Tests marks with an asterisk (*) require specific CAS monitoring running on the Datasource(s) tested'. Below this is a text area containing '-- no more tests of this type found / available --' and an 'Add Selections' button. At the bottom right, there are 'Groups', 'Back', and 'Return' buttons, with the 'Return' button highlighted by a red box.

__3. Run the V8 PoT Oracle VA Vulnerability Assessment.

__a. Select **V8 PoT Oracle VA** that was just created and click **Run Once Now**.



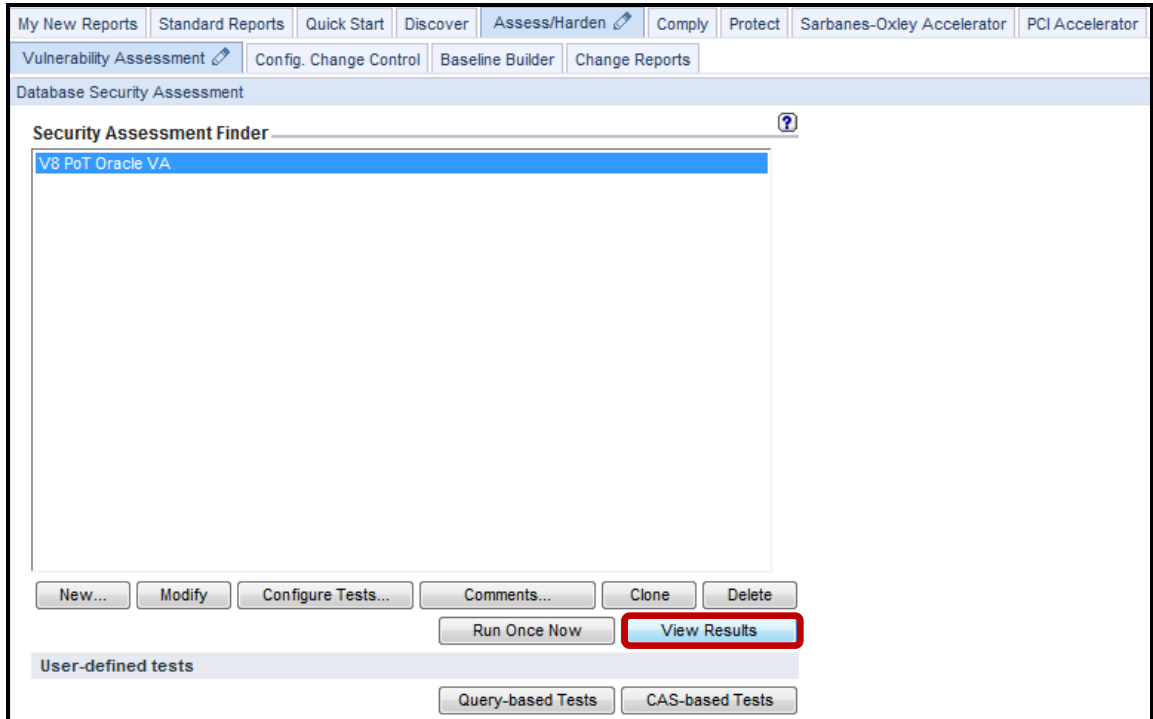
__b. Click **OK** to acknowledge.



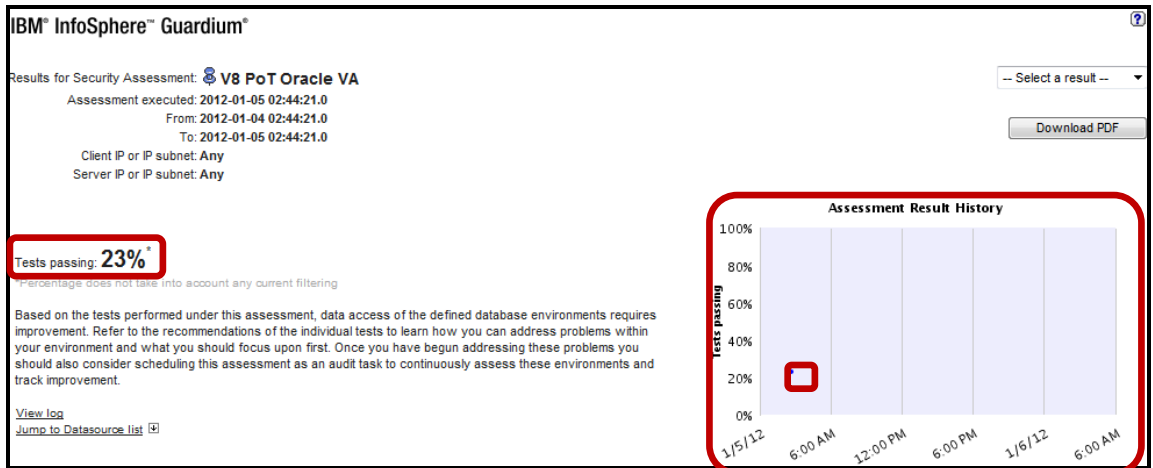
__4. View the Vulnerability Assessment Results.

__a. Click **View Results**.

Note: When *View Results* is launched before the Vulnerability Assessment job has completed, only partial results will be available. Use the **F5** key to refresh the results.



The upper portion of the output shows the percent of the tests passed. By looking at the History graph, we can see how many times the assessment has run. In this case, it has only been run once, so we see a single dot in the lower left corner.



The 'Result Summary' box provides a summary of passed and failed tests by category and by criticality. Each test is listed with a Pass/Fail as well as the explanation and Recommendation for addressing 'failed' tests.

Result Summary Showing 396 of 396 results (0 filtered)

	Critical	Major	Minor	Caution	Info
Privilege	6p 16f	2p 5f	-- 1f	-- --	-- --
Authentication	2p 4f	1p 1f	-- 1f	-- --	-- --
Configuration	2p 4f 1e	11p 90f 215e	3p 1f 4e	-- 6f 1e	-- --
Version	-- --	-- 2f	-- --	-- --	-- --
Other	1p	-- 4p 1f	-- 3p -- 1e	-- --	4p -- 3e

Current filtering applied:

Test Severities: - Show All -

Datasource Severities: - Show All -

Scores: - Show All -

Types: - Show All -

[Reset Filtering](#) [Filter / Sort Controls](#)

Assessment Test Results Showing 396 of 396 results (0 filtered)

Test / Datasource	Result
<p>DBA Profile FAILED_LOGIN_ATTEMPTS Are Limited</p> <p>Test category: Conf. Severity: Critical</p> <p>This test checks the value of the FAILED_LOGIN_ATTEMPTS parameter for each account. The FAILED_LOGIN_ATTEMPTS value limits the number of failed login attempts allowed before an account is locked. Setting this value limits the ability of unauthorized users to guess passwords and alerts the DBA when password guessing has occurred (i.e., such accounts display as LOCKED).</p> <p>Ext. Reference: STIG D03537 CIS Oracle v2.01 Item # 8.01</p> <p>osprey_system</p> <p>Datasource type: ORACLE Severity: None</p>	<p>Fail User profile [DEFAULT] setup parameter FAILED_LOGIN_ATTEMPTS found out of defined threshold value</p> <p><i>Recommendation: The FAILED_LOGIN_ATTEMPTS parameter is not set. A high number of failed login attempts can indicate that an unauthorized user is trying to gain unauthorized access to your data. We recommend that you set this parameter in order to limit the number of failed login attempts before locking the user's account.</i></p>
<p>DBA Profile PASSWORD_GRACE_TIME Is Limited</p> <p>Test category: Conf. Severity: Critical</p> <p>This test checks the value of the PASSWORD_GRACE_TIME parameter. The PASSWORD_GRACE_TIME value serves as a limit to the number of days after password expiration before the user's account is disabled. Setting this value ensures that users change their passwords at prescribed intervals. PASSWORD_GRACE_TIME can be set to any of the following: A.) A specific number of days; B.) UNLIMITED, meaning never require an account to change the password; C.) DEFAULT, which uses the value set in the DEFAULT profile. Leaving this value as UNLIMITED allows users to use the same passwords indefinitely. You should set PASSWORD_GRACE_TIME to a value <= 7. This parameter is set for profiles; accounts must then be associated with these profiles.</p> <p>Ext. Reference: Guardium, Test ID 2203</p> <p>osprey_system</p> <p>Datasource type: ORACLE Severity: None</p>	<p>Fail PASSWORD_GRACE_TIME is not set, or is set to an unacceptable value</p> <p><i>Recommendation: Set PASSWORD_GRACE_TIME to a value <= 7</i></p>
<p>DBA Profile PASSWORD_LIFE_TIME Is Limited</p> <p>Test category: Conf. Severity: Critical</p> <p>This test checks the value of the PASSWORD_LIFE_TIME parameter. The PASSWORD_LIFE_TIME value serves as a limit to the number of days until a password expires. Setting this value ensures that users are change their passwords at specified intervals. PASSWORD_LIFE_TIME can be set to any of the following: A specific number of days; UNLIMITED, meaning never require an account to change the password; or to DEFAULT, which uses the value indicated in the DEFAULT profile. Leaving this value on UNLIMITED allows users to use the same passwords indefinitely. This parameter is set for profiles; accounts must then be associated with these profiles.</p> <p>Ext. Reference: STIG D03485 CIS Oracle v2.01 Item # 8.02</p> <p>osprey_system</p> <p>Datasource type: ORACLE Severity: None</p>	<p>Fail User profile [DEFAULT] setup parameter PASSWORD_LIFE_TIME found out of defined threshold value</p> <p><i>Recommendation: The PASSWORD_LIFE_TIME parameter is not set, allowing users to retain the same password indefinitely. Passwords that have been in use for long periods of time ar likely to become known to unauthorized users. We recommend that you set this parameter in order to limit the lifetime of users' passwords.</i></p>

b. Scroll to the bottom of the report, and click the '+' icon next to **Datasource Details**.

Datasource Details +

[Close this window.](#)

This section of the Vulnerability Assessment provides details on database server patch levels, and other information that can be utilized to reveal present vulnerabilities.

Datasource Details Showing 1 of 1 datasources (0 filtered)

Type	Name	Sev.	Desc.	Host	Port	Service	User	DB	Version	Patch Level	Full Ver. Info
ORACLE	osprey_system	None		10.10.9.56	0	xe	system		10.2.0.1.0	NO Patch	10.2.0.1.0

Page 352

IBM InfoSphere Guardium V8.2

Thank You

7.2 Configuring Query-Based Tests (Optional)

Overview

Query-based tests are user-defined tests that can be quickly and easily created by defining or modifying a SQL query to be run against a database datasource. The results of the query are then compared to a predefined test value, enabling the user to check items such as database internals, structures, parameters, and even application data.

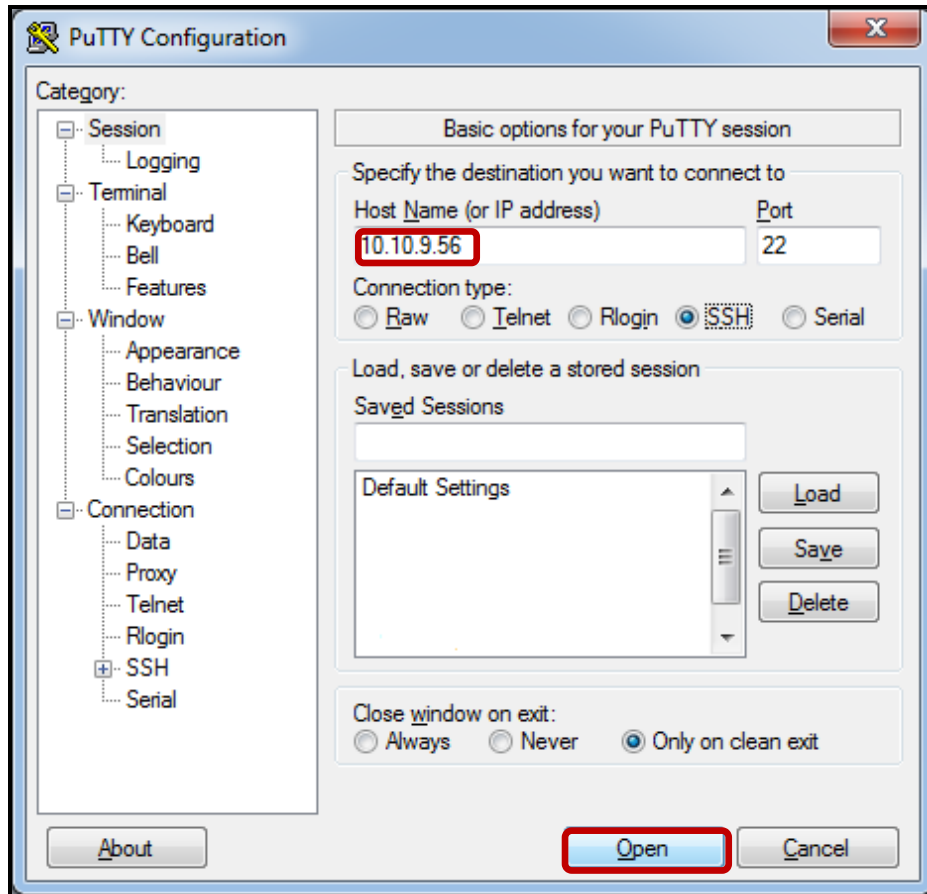
There are likely to be situations where a more specific or additional test may be required within the scope of a Vulnerability Assessment instance. InfoSphere Guardium offers the ability to create a Query-based Test in order to meet these unique requirements.

Objectives

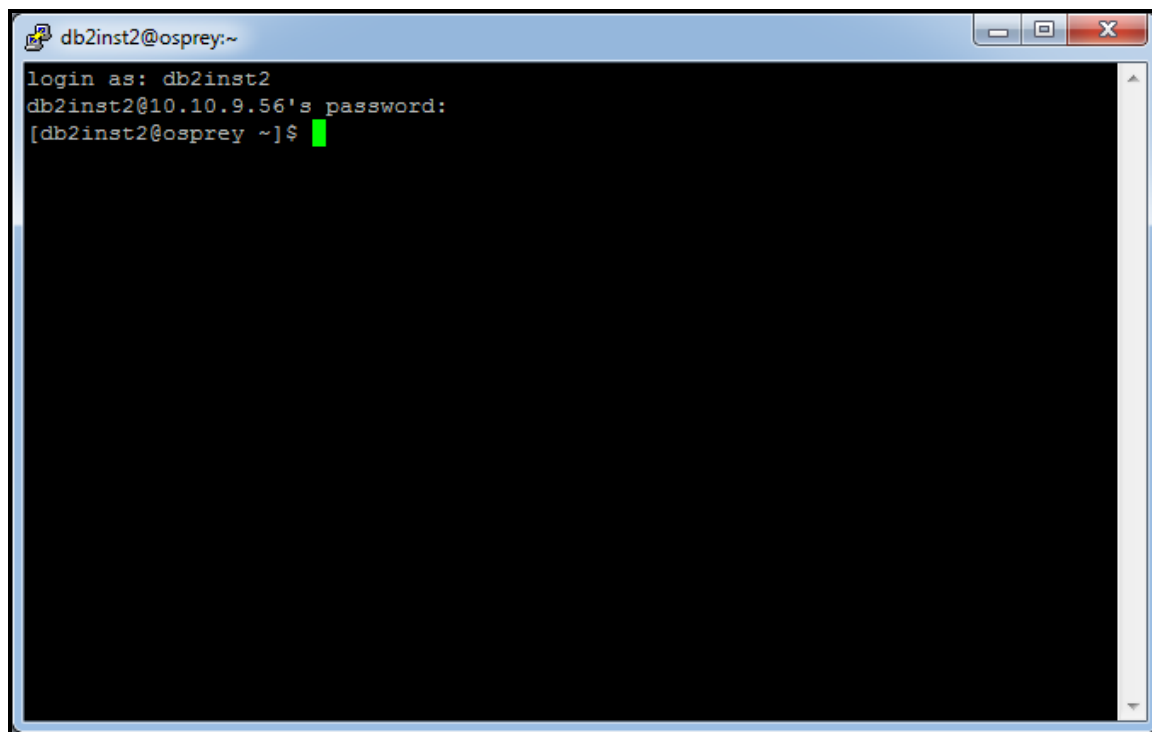
This Lab will illustrate how we can create a new Query-based test using the InfoSphere Guardium GUI. The following objectives will be targeted:

- __1. Accessing Query-based Test Builder.
- __2. Build a Query-based test.
- __3. Include the new test in a Test Configuration.
- __4. Run a Vulnerability Assessment with a newly defined test.
- __5. Verify a Successful Test Result.

- __1. Using a PuTTY SSH client, access the VM database server to ensure that the IBM DB2® database server is currently running and available to perform a Vulnerability Assessment upon.
 - __a. Start the PuTTY SSH client login.
 - __b. From your laptop, launch PuTTY, enter **10.10.9.56**, and click **Open**.

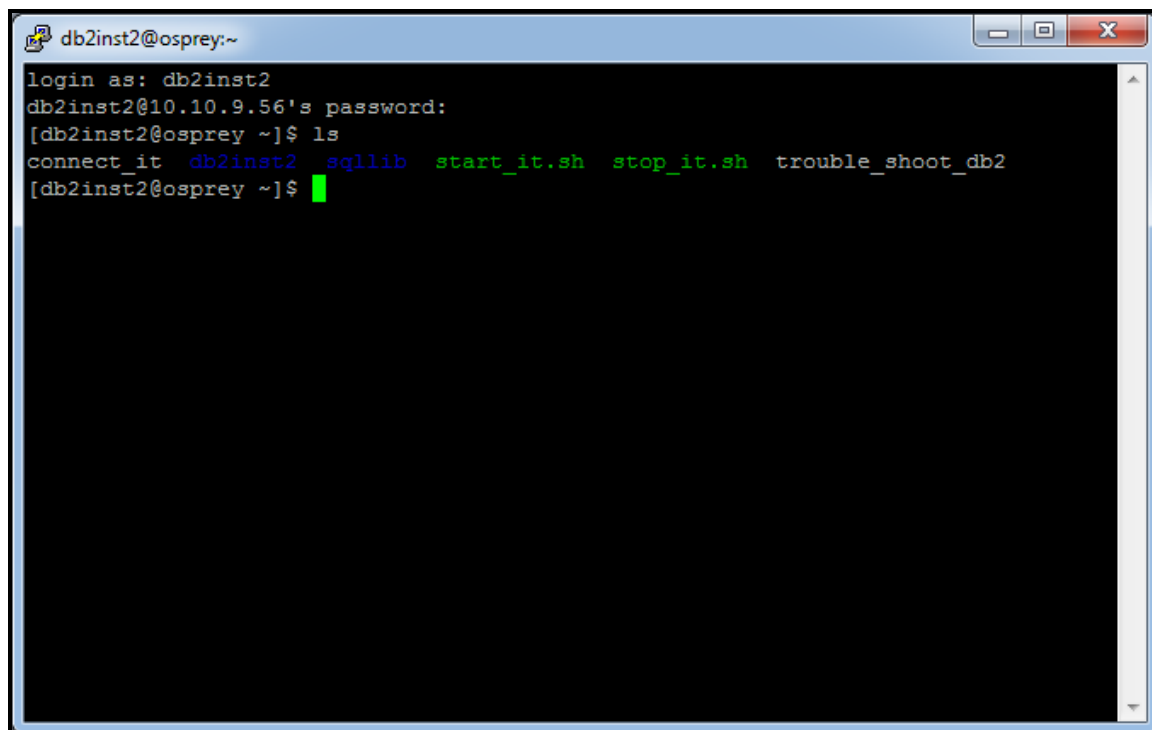


- __c. Login as **db2inst2** / **guardium**. After logging in, the following prompt will be displayed:

A terminal window titled 'db2inst2@osprey:~' with standard window controls. The text inside shows a successful login for the user 'db2inst2' on host '10.10.9.56'. The prompt is '[db2inst2@osprey ~]\$' with a green cursor.

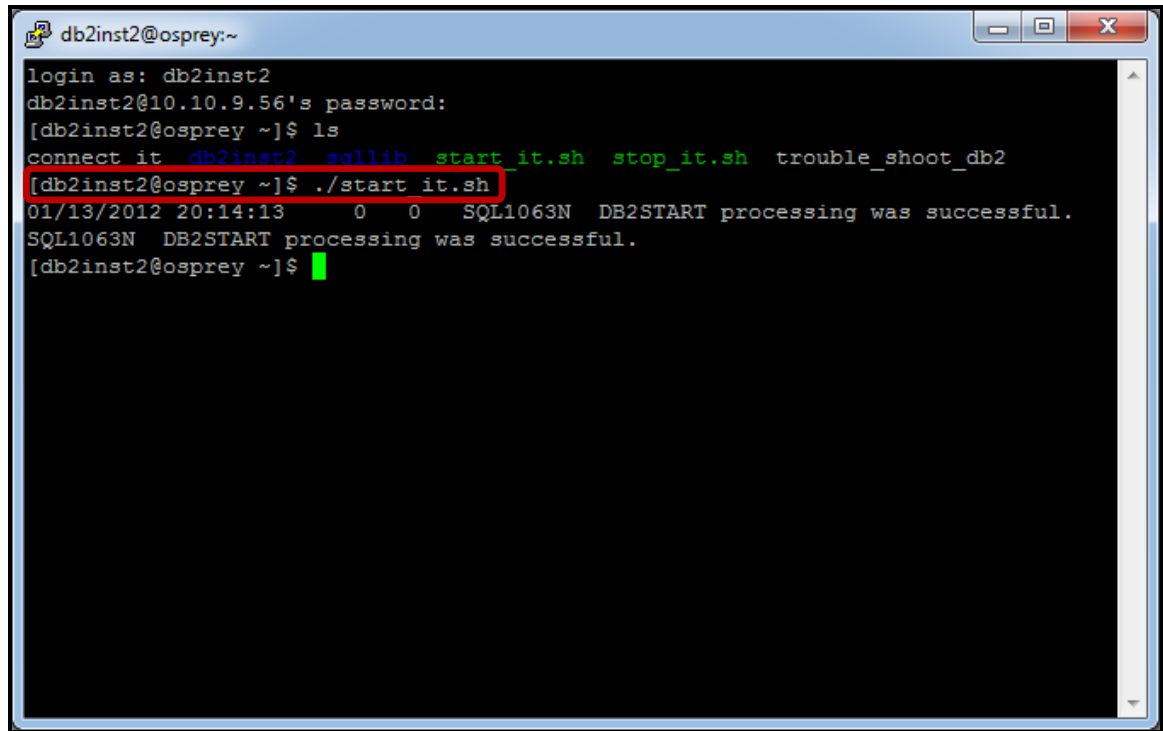
```
db2inst2@osprey:~  
login as: db2inst2  
db2inst2@10.10.9.56's password:  
[db2inst2@osprey ~]$
```

- __d. Type **ls** to get a list of available files.

A terminal window titled 'db2inst2@osprey:~' with standard window controls. The text shows the 'ls' command being executed, resulting in a list of files: 'connect_it', 'db2inst2', 'sqllib', 'start_it.sh', 'stop_it.sh', and 'trouble_shoot_db2'. The prompt is '[db2inst2@osprey ~]\$' with a green cursor.

```
db2inst2@osprey:~  
login as: db2inst2  
db2inst2@10.10.9.56's password:  
[db2inst2@osprey ~]$ ls  
connect_it  db2inst2  sqllib  start_it.sh  stop_it.sh  trouble_shoot_db2  
[db2inst2@osprey ~]$
```

- __e. **Critical Step** – Start the db2 database server by executing the following script:
./start_it.sh.



```
db2inst2@osprey:~  
login as: db2inst2  
db2inst2@10.10.9.56's password:  
[db2inst2@osprey ~]$ ls  
connect it db2inst2 sqllib start_it.sh stop_it.sh trouble_shoot_db2  
[db2inst2@osprey ~]$ ./start_it.sh  
01/13/2012 20:14:13      0  0  SQL1063N  DB2START processing was successful.  
SQL1063N  DB2START processing was successful.  
[db2inst2@osprey ~]$ █
```

Note: A database server must be running to perform a Vulnerability Assessment upon it.

The contents of the **start_it.sh** script:

```
#!/bin/sh  
db2start
```

- __f. Type **exit** to exit the PuTTY SSH client.

- __2. Now, launch the InfoSphere Guardium GUI to demonstrate the ease with which the InfoSphere Guardium solution can perform automated Vulnerability Assessments.
- __a. From your laptop, go to to <https://10.10.9.248:8443>.
- __b. Login as **pot / guardium**.

Login

Please enter your information

User name:

Password:

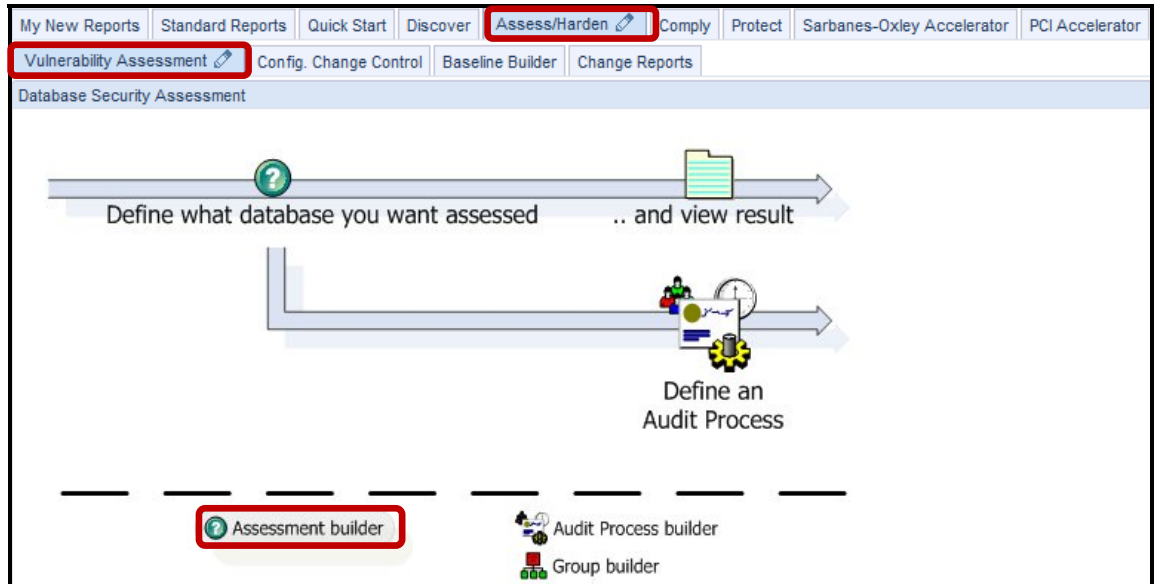
Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

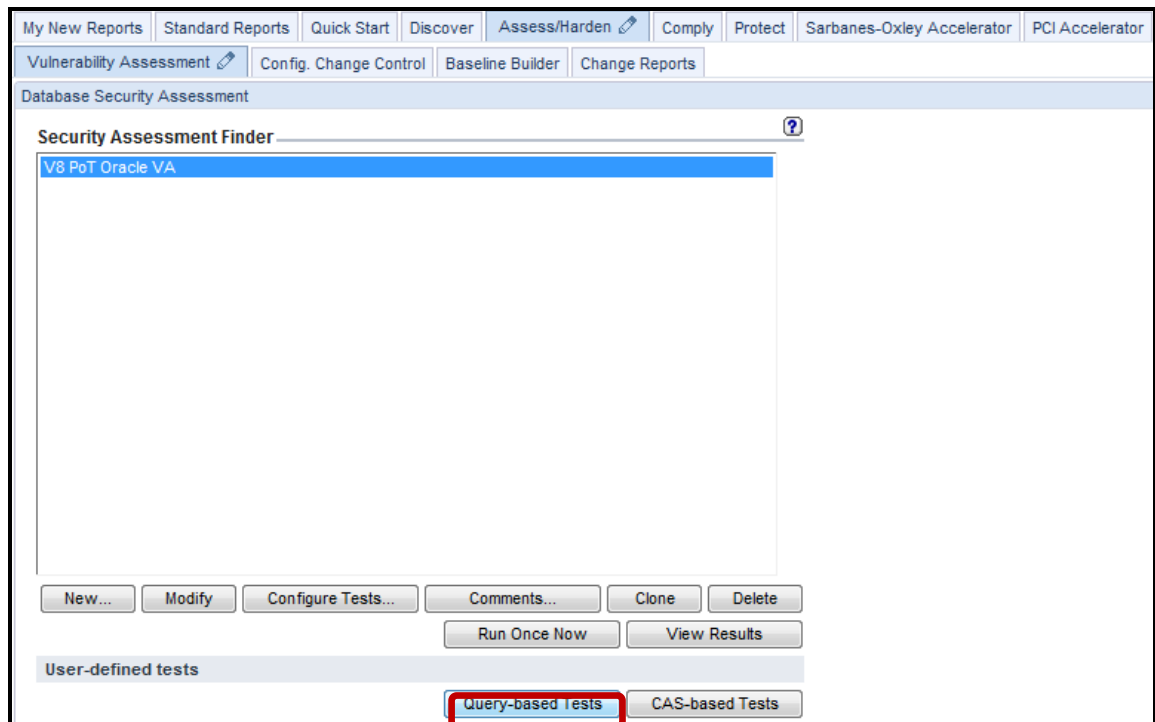
CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistrykey © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

__3. Create a new Query-based Test.

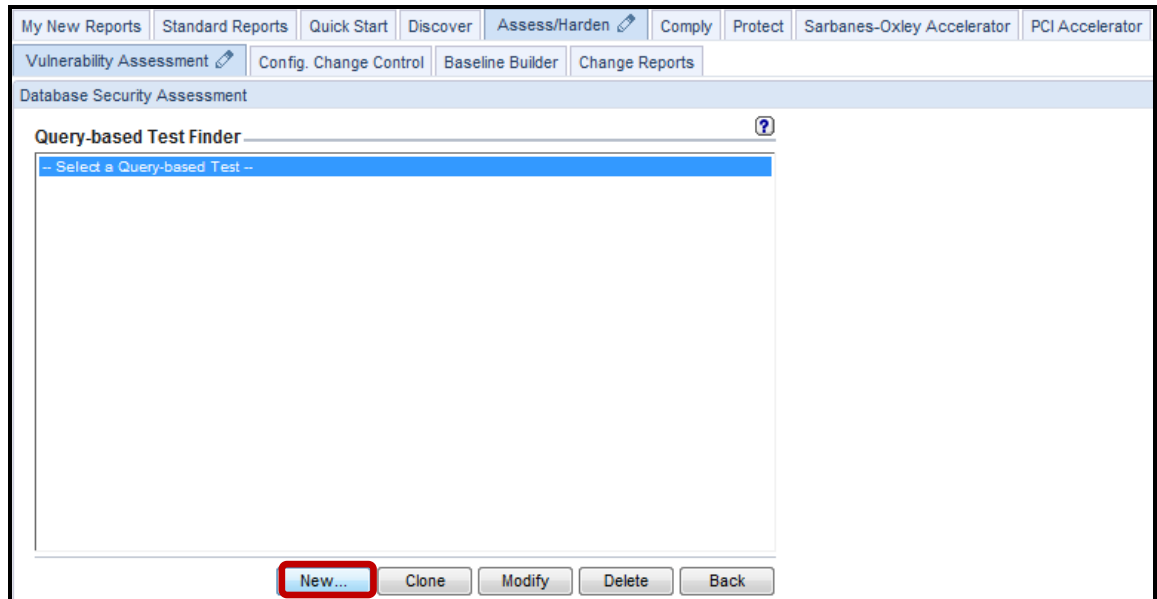
__a. Click **Vulnerability Assessment** under the **Assess/Harden** tab, and then click **Assessment builder**.



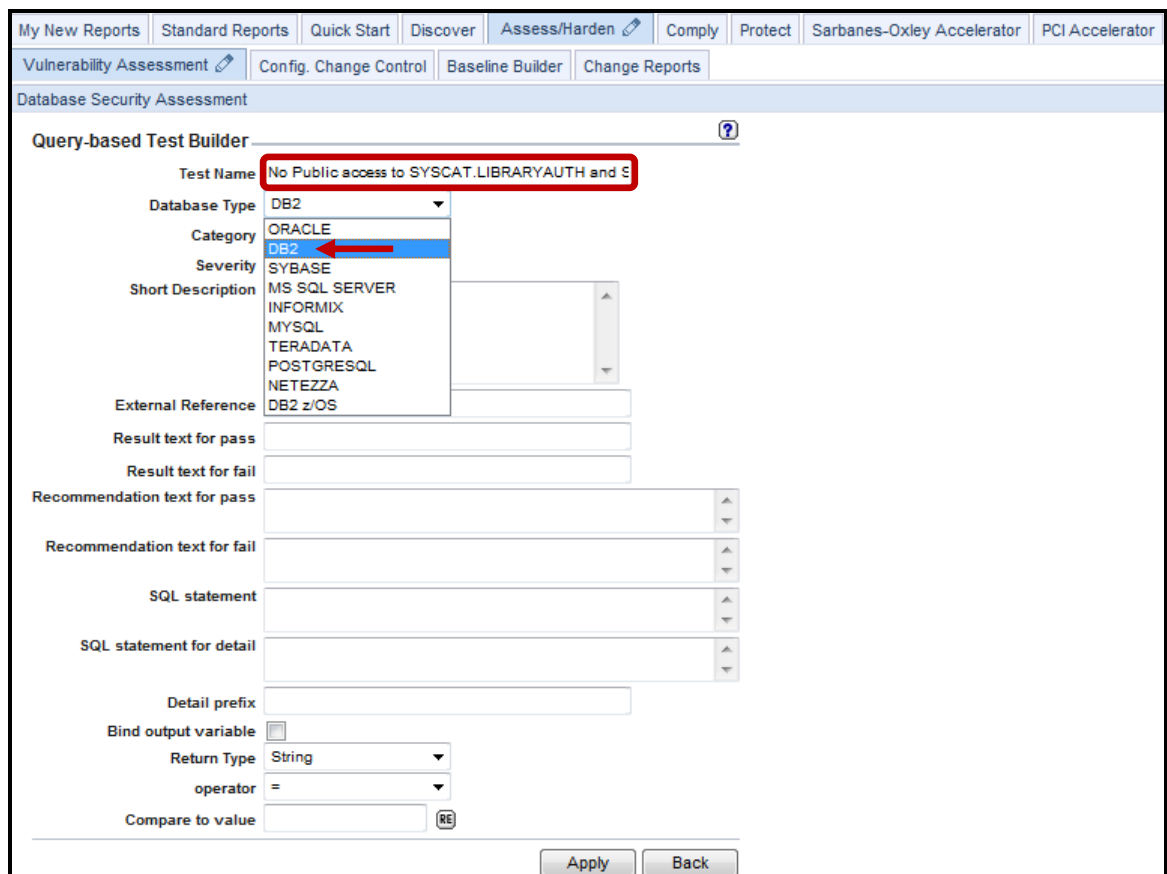
__b. Click **Query-based Tests**.



___c. Click **New**.



___d. The *Test Name* is the name that appears in the Configuration Tests list. Enter '**No PUBLIC access to SYSCAT.LIBRARYAUTH and SYSIBM.SYSLIBRARYAUTH**' for *Test Name*, and select **DB2** from the *Database Type* drop-down list.



- ___e. Enter (Copy and Paste) **'The SYSCAT_LIBRARYAUTH view and SYSIBM.SYSLIBRARYAUTH table contain the column privileges granted to a user or group of users. It is recommended that the PUBLIC role be restricted from accessing these views'** for the *Short Description* field.
- ___f. Enter **'CIS IBM_DB2 v1.1 item #6.0.4'** for the optional *External Reference* field which refers to the CIS record for the test. The example here is just to show the format
- ___g. Enter **'The SYSCAT.LIBRARYAUTH view and SYSIBM.SYSLIBRARYAUTH table are not granted to PUBLIC'** for the *Result text the pass* field. This is the text that will be displayed in the results output if the test has passes. Actually, you can type any meaningful text.

The screenshot displays the 'Query-based Test Builder' window. The 'Test Name' is 'No Public access to SYSCAT.LIBRARYAUTH and S'. The 'Database Type' is set to 'DB2', 'Category' to 'Privilege', and 'Severity' to 'Informational'. The 'Short Description' field is highlighted with a red box and contains the text: 'The SYSCAT_LIBRARYAUTH view and SYSIBM.SYSLIBRARYAUTH table contain the column privileges granted to a user or group of users. It is recommended that the PUBLIC role be restricted from accessing these views'. The 'External Reference' field is also highlighted with a red box and contains 'CIS IBM_DB2 v1.1 item #6.0.4'. The 'Result text for pass' field is highlighted with a red box and contains 'The SYSCAT.LIBRARYAUTH view and SYSIBM.SYSLIBRARYAUTH table are not granted to PUBLIC'. The 'Test Name' field is also highlighted with a red box. The interface includes navigation buttons like 'Apply' and 'Back'.

- ___h. Enter **'The SYSCAT.LIBRARYAUTH view and SYSIBM.SYSLIBRARYAUTH table are granted to PUBLIC'** for the *Result text for fail* field. Once again, this will show up in the results output if the test fails. You can type your own replacement text, as well.
- ___i. Enter **'No Action Required'** for the *Recommendation text for pass* field.
- ___j. Enter (Copy and Paste) **'We recommend you revoke SYSCAT.LIBRARYAUTH view and SYSIBM.SYSLIBRARYAUTH table privilege from PUBLIC. You can use this command to revoke: REVOKE ALL ON SYSCAT.LIBRARYAUTH FROM PUBLIC. REVOKE ALL ON SYSIBM.SYSLIBRARYAUTH FROM PUBLIC'** in the *Recommendation text for fail* field.

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

Vulnerability Assessment | Config. Change Control | Baseline Builder | Change Reports

Database Security Assessment

Query-based Test Builder

Test Name: No Public access to SYSCAT.LIBRARYAUTH and SYSIBM.SYSLIBRARYAUTH

Database Type: DB2

Category: Privilege

Severity: Informational

Short Description: The SYSCAT.LIBRARYAUTH view and SYSIBM.SYSLIBRARYAUTH table contain the column privileges granted to a user or group of users. It is recommended that the PUBLIC role be restricted from accessing

External Reference: CIS IBM_DB2 v1.1 item #6.0.4

Result text for pass: The SYSCAT.LIBRARYAUTH view and SYSIBM.SYSLIBRARYAUTH table contain the column privileges granted to a user or group of users. It is recommended that the PUBLIC role be restricted from accessing

Result text for fail: The SYSCAT.LIBRARYAUTH view and SYSIBM.SYSLIBRARYAUTH table contain the column privileges granted to a user or group of users. It is recommended that the PUBLIC role be restricted from accessing

Recommendation text for pass: No Action Required

Recommendation text for fail: We recommend you revoke SYSCAT.LIBRARYAUTH view and SYSIBM.SYSLIBRARYAUTH table privilege from PUBLIC. You can use this command to revoke: REVOKE ALL ON SYSCAT.LIBRARYAUTH FROM PUBLIC. REVOKE ALL ON SYSIBM.SYSLIBRARYAUTH FROM PUBLIC

SQL statement:

SQL statement for detail:

Detail prefix:

Bind output variable:

Return Type: String

operator: =

Compare to value:

Apply Back

Note: The *SQL statement* and *SQL statement for detail* fields contain the actual SQL for the test.

__k. Enter (Copy and Paste) the following SQL Query for the **SQL statement** field:

```
select sum(counter) from (select count(*) as counter from syscat.tabauth where tabschema = 'SYSCAT' and tabname = 'LIBRARY' and grantee = 'PUBLIC' union all select count(*) as counter from syscat.tabauth where tabschema = 'SYSIBM' and tabname = 'SYSLIBRARYAUTH' and grantee = 'PUBLIC') as cis_test
```

__l. Enter (Copy and Paste) the following SQL Query for the **SQL Statement for Detail** field:

```
select 'VIEW: ' || rtrim(tabschema) || '.' || rtrim(tabname) from syscat.tabauth where tabschema = 'SYSCAT' and tabname = 'LIBRARYAUTH' and grantee = 'PUBLIC' union all select 'TABLE: ' || rtrim(tabschema) || '.' || rtrim(tabname) from syscat.tabauth where tabschema = 'SYSIBM' and tabname = 'SYSLIBRARYAUTH' and grantee = 'PUBLIC'
```

__m. Select **Integer** from the *Return Type* drop-down list.

The screenshot displays the 'Query-based Test Builder' window. The 'Test Name' is 'No Public access to SYSCAT.LIBRARYAUTH and S'. The 'Database Type' is 'DB2', 'Category' is 'Privilege', and 'Severity' is 'Informational'. The 'Short Description' states that SYSCAT.LIBRARYAUTH view and SYSIBM.SYSLIBRARYAUTH table contain column privileges for the PUBLIC role. The 'SQL statement' field contains the query for summing counters, and the 'SQL statement for detail' field contains the query for listing views and tables. The 'Return Type' dropdown is set to 'Integer', indicated by a red arrow.

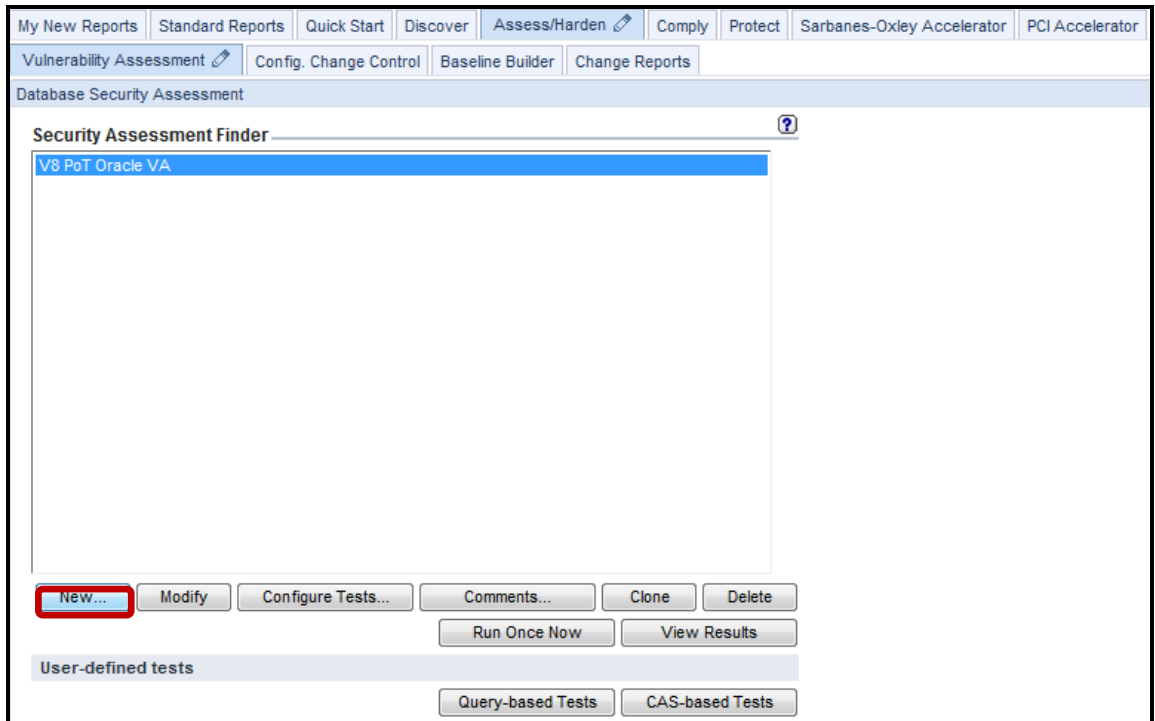
__n. Enter '0' for the *Compare to value* field, click **Apply**, and then click **Back**.

The screenshot shows the 'Query-based Test Builder' window in the Database Security Assessment tool. The 'Test Name' is 'No Public access to SYSCAT.LIBRARYAUTH and SYSIBM.SYSLIBRARYAUTH'. The 'Database Type' is 'DB2', 'Category' is 'Privilege', and 'Severity' is 'Informational'. The 'Short Description' and 'SQL statement' fields contain detailed information about the test. The 'Compare to value' field is set to '0'. The 'Apply' and 'Back' buttons are highlighted with red boxes.

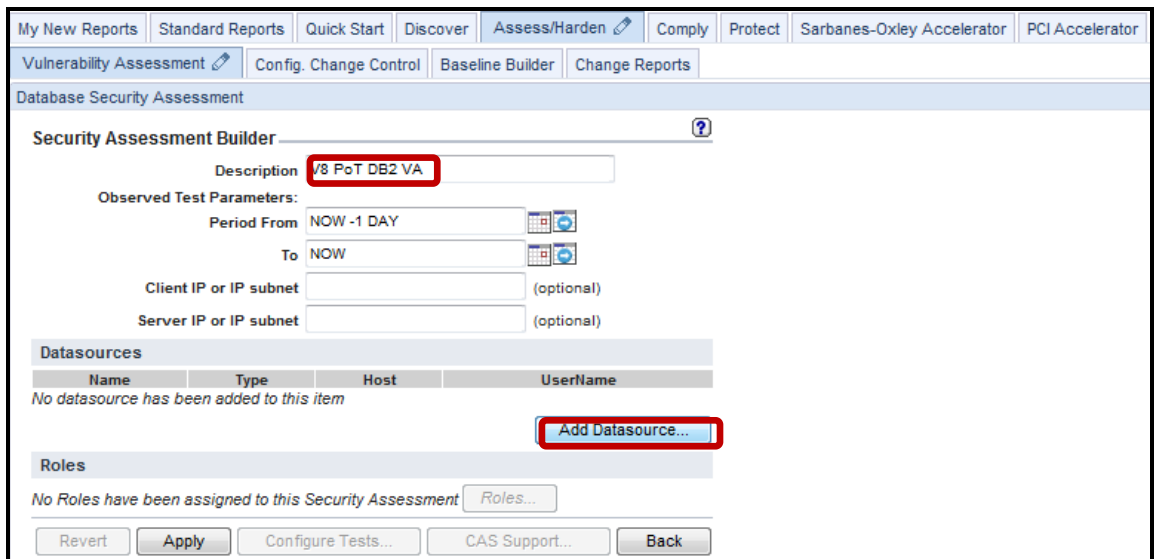
__o. Verify that the Query-based Test you created is listed in the **Query-based Test Finder** box and click **Back**.

The screenshot shows the 'Query-based Test Finder' window. A list of tests is displayed, with the test 'DB2: No Public access to SYSCAT.LIBRARYAUTH and SYSIBM.SYSLIBRARYAUTH' highlighted in blue and red. The 'Back' button is highlighted with a red box.

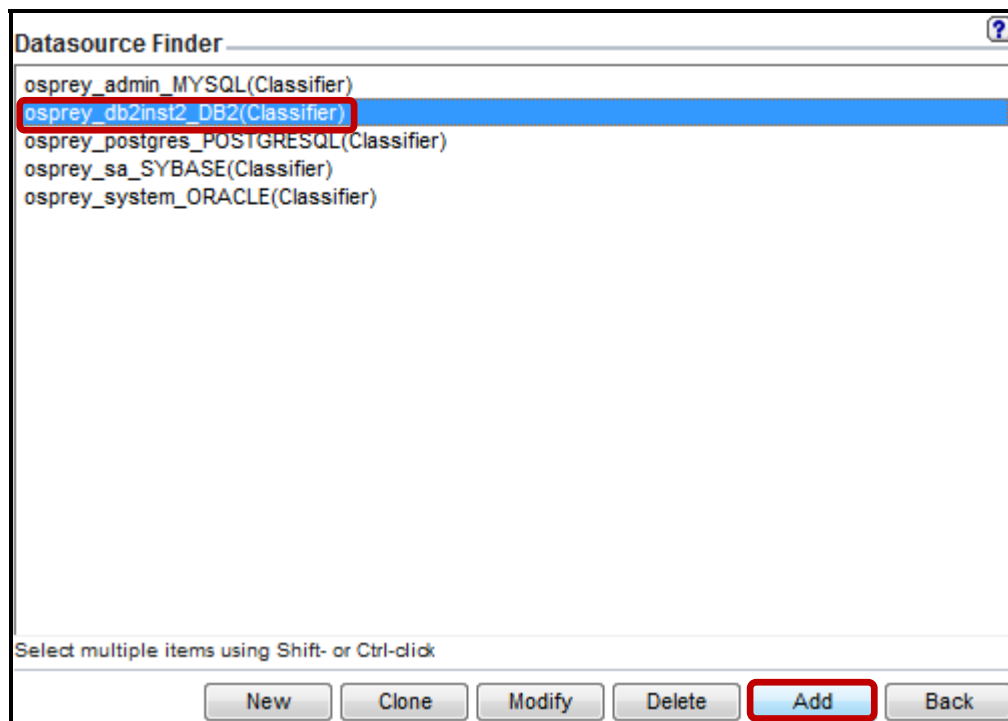
__p. Click **New**.



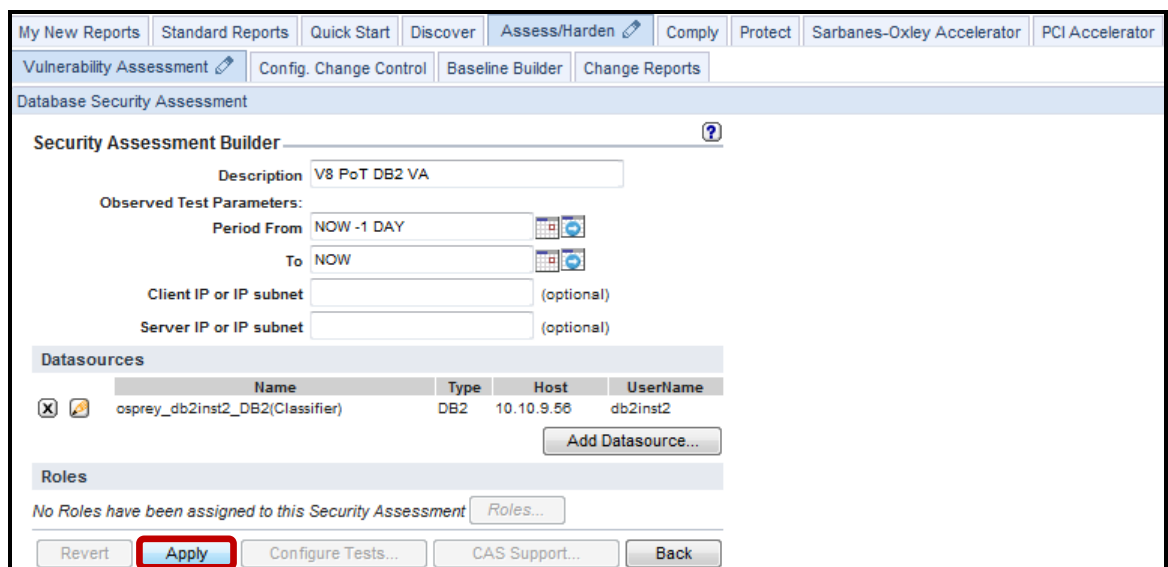
__q. Enter **V8 PoT DB2 VA** in the *Description* field and click **Add Datasource**.



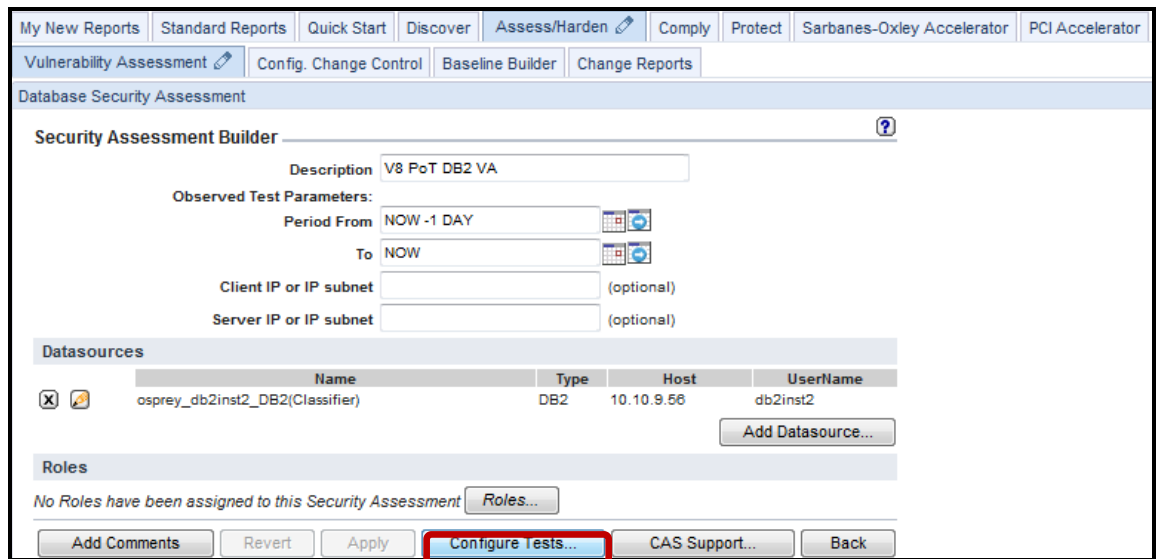
- __r. Select **osprey_db2inst2_DB2(Classifier)** from the *Datasource finder* list, and click **Add**.



- __s. Click **Apply**.

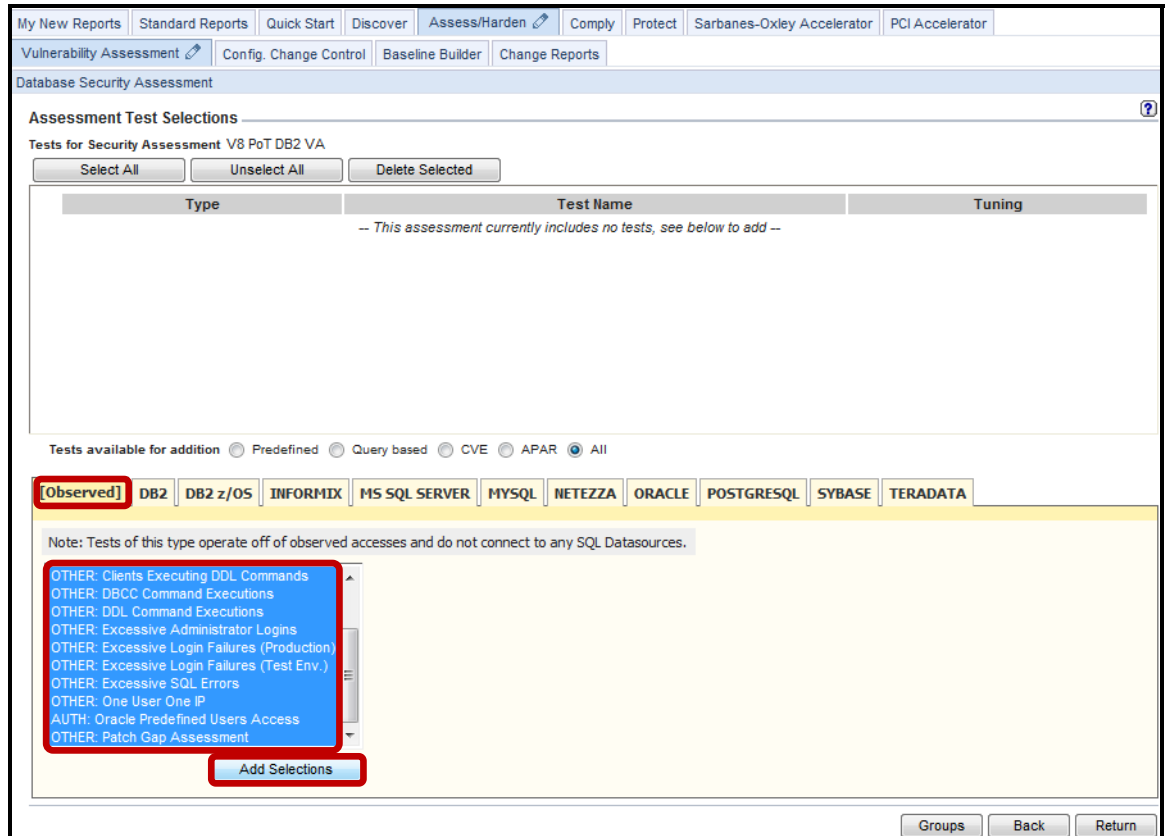


__t. Click **Configure Tests**.



__u. Select all of the **[Observed]** tests either by clicking and dragging to the end of the list or by clicking the first test, scrolling down to the bottom, and pressing Shift and clicking on the last test.

__v. Click **Add Selections** to add all of the selecting test conditions.



- ___w. Click the **DB2** tab, select the **Query based** radio button, select the new *Query-based Test*, and click **Add Selections**.

The screenshot shows the 'Assessment Test Selections' window for a Security Assessment V8 PoT DB2 VA. The interface includes a navigation bar at the top with tabs like 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below this is a sub-menu with 'Vulnerability Assessment', 'Config. Change Control', 'Baseline Builder', and 'Change Reports'. The main section is titled 'Database Security Assessment' and 'Assessment Test Selections'. It features a table of tests with columns for 'Type', 'Test Name', and 'Tuning'. The 'Query based' radio button is selected under 'Tests available for addition'. The 'DB2' tab is highlighted in the database type selection bar. A specific test, 'PRIV: No PUBLIC access to SYSCATLIBRARYAUTH and SYSEM.SYSLIBRARYAUTH', is highlighted in blue. The 'Add Selections' button is also highlighted.

Type	Test Name	Tuning
<input type="checkbox"/>	Access Rule Violations	OTHER Major 10: Maximum Number of Policy violations allowed per day (after factoring the assessed period)
<input type="checkbox"/>	Admin Command Executions	OTHER Informational 30: Maximum Number of administration commands allowed per day (after factoring the assessed period)
<input type="checkbox"/>	After Hours Logins	OTHER Minor 5: Maximum number of after-hours logins allowed
<input type="checkbox"/>	Clients Executing Admin Commands	OTHER Minor 3: Maximum Number of clients executing administration commands allowed
<input type="checkbox"/>	Clients Executing DDL Commands	OTHER Minor 2: Maximum Number of clients executing DDL commands allowed
<input type="checkbox"/>	DBCC Command Executions	OTHER Informational 5: Maximum Number of DBCC commands allowed per day (after factoring the assessed period)

Tests available for addition: Predefined Query based CVE APAR All

[Observed] **DB2** DB2 z/OS INFORMIX MS SQL SERVER MYSQL NETEZZA ORACLE POSTGRESQL SYBASE TERADATA

Tests marks with an asterisk (*) require specific CAS monitoring running on the Datasource(s) tested

PRIV: No PUBLIC access to SYSCATLIBRARYAUTH and SYSEM.SYSLIBRARYAUTH

Add Selections

Groups Back Return

__x. Now, select the **All radio button**, select all of the remaining DB2 tests, and click **Add Selections**.

The screenshot displays the 'Assessment Test Selections' window in the IBM InfoSphere Guardium V8.2 interface. At the top, there are navigation tabs including 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below these are sub-tabs for 'Vulnerability Assessment', 'Config. Change Control', 'Baseline Builder', and 'Change Reports'. The main title is 'Database Security Assessment'.

The 'Assessment Test Selections' section is titled 'Tests for Security Assessment V8 PoT DB2 VA'. It includes three buttons: 'Select All', 'Unselect All', and 'Delete Selected'. A table lists various tests with columns for 'Type', 'Test Name', and 'Tuning'. The tests listed are:

Type	Test Name	Tuning
<input type="checkbox"/>	Access Rule Violations	OTHER Major 10: Maximum Number of Policy violations allowed per day (after factoring the assessed period)
<input type="checkbox"/>	Admin Command Executions	OTHER Informational 30: Maximum Number of administration commands allowed per day (after factoring the assessed period)
<input type="checkbox"/>	After Hours Logins	OTHER Minor 5: Maximum number of after-hours logins allowed
<input type="checkbox"/>	Clients Executing Admin Commands	OTHER Minor 3: Maximum Number of clients executing administration commands allowed
<input type="checkbox"/>	Clients Executing DDL Commands	OTHER Minor 2: Maximum Number of clients executing DDL commands allowed
<input type="checkbox"/>	DBCC Command Executions	OTHER Informational 5: Maximum Number of DBCC commands allowed per day (after factoring the assessed period)

Below the table, there are radio buttons for 'Tests available for addition': 'Predefined', 'Query based', 'CVE', 'APAR', and 'All' (which is selected). A database type filter is shown with tabs for '[Observed]', 'DB2', 'DB2 z/OS', 'INFORMIX', 'MS SQL SERVER', 'MYSQL', 'NETEZZA', 'ORACLE', 'POSTGRESQL', 'SYBASE', and 'TERADATA'. The 'DB2' tab is highlighted with a red box.

A text box below the filter contains the following text:

```

Tests marks with an asterisk (*) require specific CAS monitoring running on the Datasource(s) tested
CONF: Set failed archive retry delay *
CONF: SNA_AUTH Is No *
CONF: SPM_LOG_PATH Owned by a SYS Group *
CONF: SYSADM_GROUP Is Set *
CONF: SYSTRM_GROUP Is Set *
CONF: SYSMANT_GROUP Is Set *
CONF: SYSMON_GROUP Is Set *
CONF: TRUST_ALLCLNTS To No *
PRV: User objects in System Tablespaces
VER: Version: DB2
    
```

The 'Add Selections' button at the bottom right of this text box is highlighted with a red box. At the very bottom of the window, there are 'Groups', 'Back', and 'Return' buttons.

___y. Click **Return** to save the assessment and return to the initial screen.

The screenshot displays the 'Database Security Assessment' interface. At the top, there is a navigation bar with tabs: 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below this is a sub-navigation bar with 'Vulnerability Assessment', 'Config. Change Control', 'Baseline Builder', and 'Change Reports'. The main header is 'Database Security Assessment'.

The section is titled 'Assessment Test Selections' and shows 'Tests for Security Assessment V8 PoT DB2 VA'. There are three buttons: 'Select All', 'Unselect All', and 'Delete Selected'. Below is a table with columns 'Type', 'Test Name', and 'Tuning'. The table lists several test types with their corresponding tuning parameters:

Type	Test Name	Tuning
<input type="checkbox"/>	Access Rule Violations	OTHER Major 10: Maximum Number of Policy violations allowed per day (after factoring the assessed period)
<input type="checkbox"/>	Admin Command Executions	OTHER Informational 30: Maximum Number of administration commands allowed per day (after factoring the assessed period)
<input type="checkbox"/>	After Hours Logins	OTHER Minor 5: Maximum number of after-hours logins allowed
<input type="checkbox"/>	Clients Executing Admin Commands	OTHER Minor 3: Maximum Number of clients executing administration commands allowed
<input type="checkbox"/>	Clients Executing DDL Commands	OTHER Minor 2: Maximum Number of clients executing DDL commands allowed

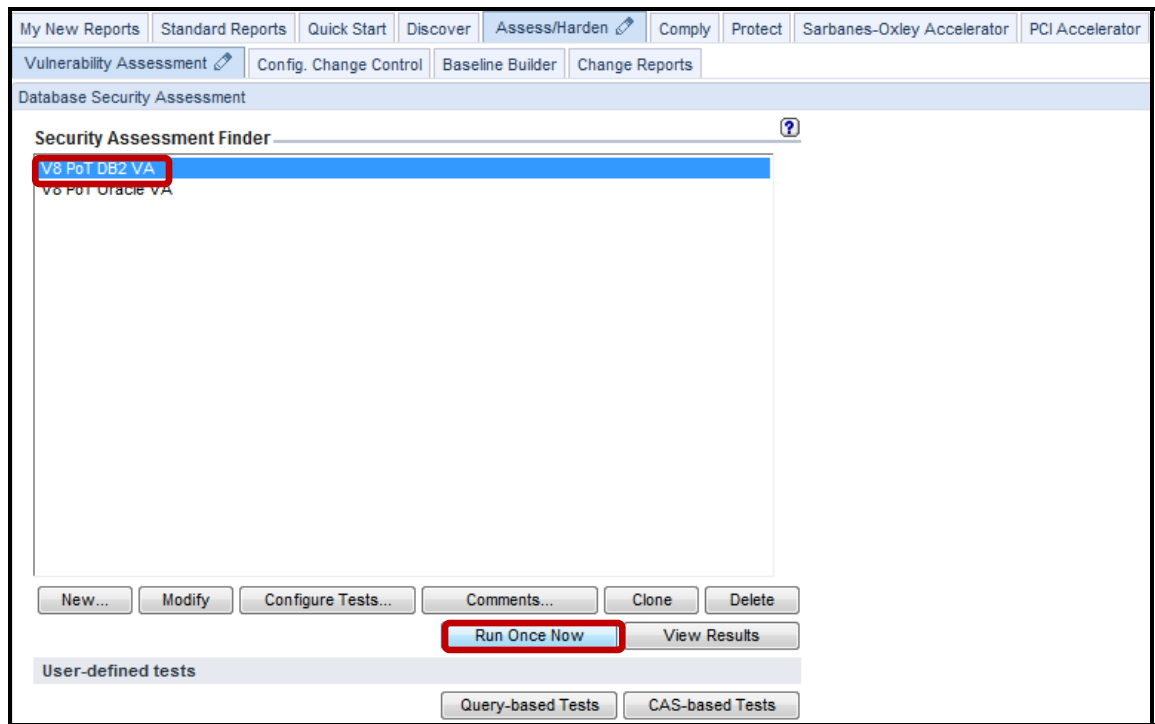
Below the table, there are radio buttons for 'Tests available for addition': 'Predefined', 'Query based', 'CVE', 'APAR', and 'All' (selected).

At the bottom of the table area, there are tabs for database types: '[Observed]', 'DB2', 'DB2 z/OS', 'INFORMIX', 'MS SQL SERVER', 'MYSQL', 'NETEZZA', 'ORACLE', 'POSTGRESQL', 'SYBASE', and 'TERADATA'. The 'DB2' tab is selected.

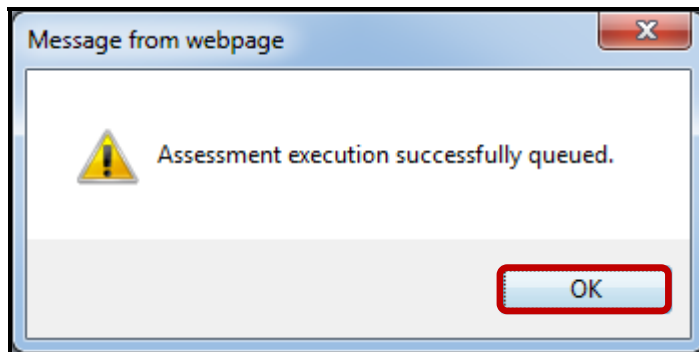
A text box below the tabs contains the message: 'Tests marks with an asterisk (*) require specific CAS monitoring running on the Datasource(s) tested'. Below this is a large empty text area with the text '-- no more tests of this type found / available --' and an 'Add Selections' button.

At the bottom right of the interface, there are three buttons: 'Groups', 'Back', and 'Return' (highlighted in red).

- __4. Verify the new Query-based Test.
 - __a. Select **V8 PoT DB2 VA**, and click **Run Once Now**.

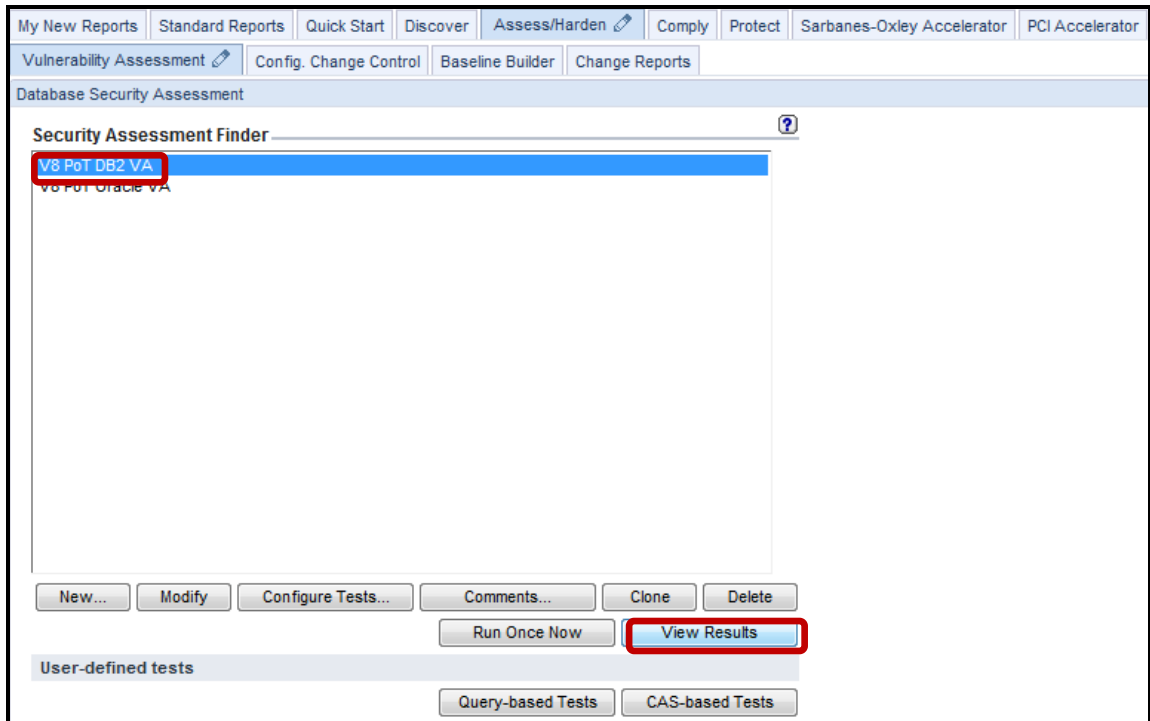


- __b. Click **OK** to acknowledge.

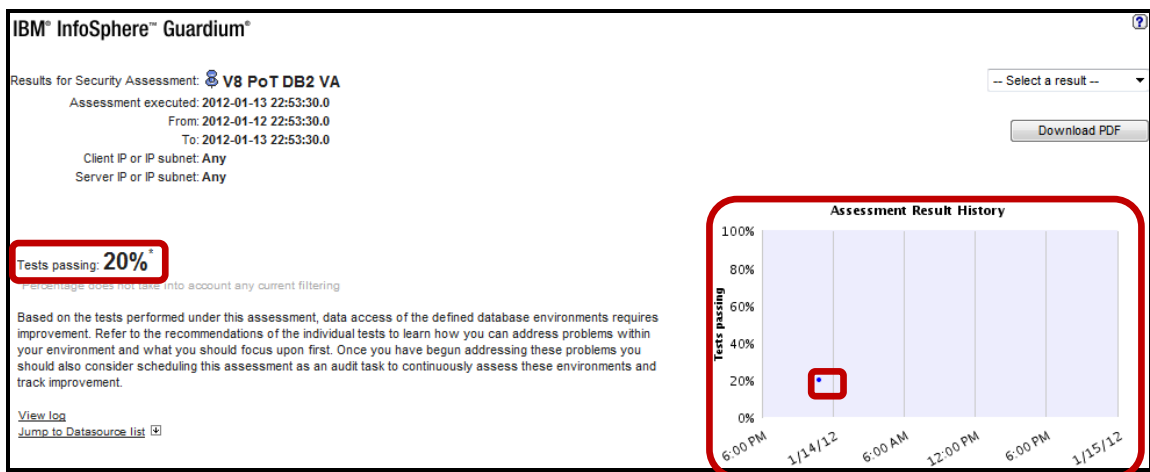


- __5. View the Vulnerability Assessment Results.
 - __a. Select **V8 PoT DB2 VA** and click **View Results**.

Note: When *View Results* is launched before the Vulnerability Assessment job has completed, only partial results will be available. Use the **F5** key to refresh the results.



The upper portion of the output shows the percent of the tests passed. By looking at the History graph, we can see how many times the assessment has been run. In this case, it has only been run once, so we see a single dot in the lower left corner.



The 'Result Summary' box provides a summary of passed and failed tests by category and by criticality. Each test is listed with a Pass/Fail as well as the explanation and Recommendation for addressing 'failed' tests.

Note: Our Query-based Test has successfully identified a new Vulnerability in DB2 that would have otherwise gone undetected. We have demonstrated the power of augmenting the existing set of predefined tests with additional custom tests. This also offers the capability to quickly determine the risk associated with a newly discovered vulnerability throughout the organization without having to wait for a new test to be discovered and documented by the main organizations such as DoD, STIG or the CIS.

Result Summary Showing 234 of 234 results (0 filtered)

	Critical	Major	Minor	Caution	Info
Privilege	12p 35f 5e	1p 2f	-- --	1p 1f	-- 1f
Authentication	-- --	-- --	1p	-- --	-- --
Configuration	-- --	66f 87e	-- 3e	-- 1e	-- --
Version	-- --	1p 1f	-- --	-- --	-- --
Other	1p	3p	2e 3p	-- --	4p 3e

Current filtering applied:

Test Severities: - Show All -

Datasource Severities: - Show All -

Scores: - Show All -

Types: - Show All -

Reset Filtering Filter / Sort Controls

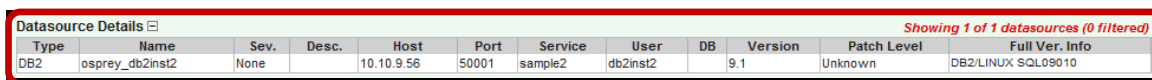
Assessment Test Results Compare with other results Showing 234 of 234 results (0 filtered)

Test / Datasource	Result
<p>Delete Unused Schemas</p> <p>Test category: Priv. Severity: Critical</p> <p>A schema is a logical grouping of database objects. It is recommended that unused schemas be removed from the database. Unused schemas can be left unmonitored and may be subjected to abuse and therefore should be removed.</p> <p>Ext. Reference: CIS IBM_DB2 v1.1.0 Item #8.0.3</p> <p>osprey_db2inst2</p> <p>Datasource type: DB2 Severity: None</p>	<p>Fail Unused schema are present in your database</p> <p>Recommendation: We recommend you drop all schemas that are not required by your database. You can use this command to drop schema: <code>drop schema <schema name> restrict</code>. To exclude schemas that are required by your database, you can create a group, then populate it with valid schemas name and link your group to this test. Before dropping any schemas, please make sure to consult with your database and application administrator. Dropping schemas that are required by your application or database can cause serious negative implication.</p>
<p>No PUBLIC access to SYSCAT.COLAUTH and SYSIBM.SYSCOLAUTH</p> <p>Test category: Priv. Severity: Critical</p> <p>The SYSCAT.COLAUTH view and SYSIBM.SYSCOLAUTH table contains the column privileges granted to the user or a group of users. It is recommended that the PUBLIC role be restricted from accessing this view.</p> <p>Ext. Reference: CIS IBM_DB2 v1.1.0 Item #6.0.4</p> <p>osprey_db2inst2</p> <p>Datasource type: DB2 Severity: None</p>	<p>Fail The SYSCAT.COLAUTH view and SYSIBM.SYSCOLAUTH table are granted to PUBLIC.</p> <p>Recommendation: We recommend you revoke SYSCAT.COLAUTH view and SYSIBM.SYSCOLAUTH table privilege from PUBLIC. You can use this command to revoke: <code>REVOKE ALL ON SYSCAT.COLAUTH FROM PUBLIC. REVOKE ALL ON SYSIBM.SYSCOLAUTH FROM PUBLIC.</code></p>
<p>No PUBLIC access to SYSCAT.DBAUTH and SYSIBM.SYSDBAUTH</p> <p>Test category: Priv. Severity: Critical</p> <p>The SYSCAT.DBAUTH view and SYSIBM.SYSDBAUTH table contains information on authorities granted to users or group of users. It is recommended that the PUBLIC role be restricted from accessing this view.</p> <p>Ext. Reference: CIS IBM_DB2 v1.1.0 Item #6.0.3</p> <p>osprey_db2inst2</p> <p>Datasource type: DB2 Severity: None</p>	<p>Fail The SYSCAT.DBAUTH view and SYSIBM.SYSDBAUTH table are granted to PUBLIC.</p> <p>Recommendation: We recommend you revoke SYSCAT.DBAUTH view and SYSIBM.SYSDBAUTH table privilege from PUBLIC. You can use this command to revoke: <code>REVOKE ALL ON SYSCAT.DBAUTH FROM PUBLIC. REVOKE ALL ON SYSIBM.SYSDBAUTH FROM PUBLIC.</code></p>
<p>No PUBLIC access to SYSCAT.EVENTS and SYSIBM.SYSEVENTS</p> <p>Test category: Priv. Severity: Critical</p> <p>The SYSCAT.EVENTS view and SYSIBM.SYSEVENTS table contains all events that the database is currently monitoring. It is recommended that the PUBLIC role be restricted from accessing this view.</p> <p>Ext. Reference: CIS IBM_DB2 v1.1.0 Item #6.0.5</p> <p>osprey_db2inst2</p> <p>Datasource type: DB2 Severity: None</p>	<p>Fail The SYSCAT.EVENTS view and SYSIBM.SYSEVENTS table are granted to PUBLIC.</p> <p>Recommendation: We recommend you revoke SYSCAT.EVENTS view and SYSIBM.SYSEVENTS table privilege from PUBLIC. You can use this command to revoke: <code>REVOKE ALL ON SYSCAT.EVENTS FROM PUBLIC. REVOKE ALL ON SYSIBM.SYSEVENTS FROM PUBLIC.</code></p>
<p>No PUBLIC access to SYSCAT.EVENTTABLES and SYSIBM.SYSEVENTTABLES</p> <p>Test category: Priv. Severity: Critical</p> <p>The SYSCAT.EVENTTABLES view and SYSIBM.SYSEVENTTABLES table contains the name of the destination table that will receive the monitoring events. It is recommended that the PUBLIC role be restricted from accessing this view.</p> <p>Ext. Reference: CIS IBM_DB2 v1.1.0 Item #6.0.6</p> <p>osprey_db2inst2</p> <p>Datasource type: DB2 Severity: None</p>	<p>Fail The SYSCAT.EVENTTABLES view and SYSIBM.SYSEVENTTABLES table are granted to PUBLIC.</p> <p>Recommendation: We recommend you revoke SYSCAT.EVENTTABLES view and SYSIBM.SYSEVENTTABLES table privilege from PUBLIC. You can use this command to revoke: <code>REVOKE ALL ON SYSCAT.EVENTTABLES FROM PUBLIC. REVOKE ALL ON SYSIBM.SYSEVENTTABLES FROM PUBLIC.</code></p>
<p>No PUBLIC access to SYSCAT.INDEXAUTH and SYSIBM.SYSINDEXAUTH</p> <p>Test category: Priv. Severity: Critical</p> <p>The SYSCAT.INDEXAUTH view and SYSIBM.SYSINDEXAUTH table contains a list of user or group that has CONTROL access on an index. It is recommended that the PUBLIC role be restricted from accessing this view.</p> <p>Ext. Reference: CIS IBM_DB2 v1.1.0 Item #6.0.8</p> <p>osprey_db2inst2</p> <p>Datasource type: DB2 Severity: None</p>	<p>Fail The SYSCAT.INDEXAUTH view and SYSIBM.SYSINDEXAUTH table are granted to PUBLIC.</p> <p>Recommendation: We recommend you revoke SYSCAT.INDEXAUTH view and SYSIBM.SYSINDEXAUTH table privilege from PUBLIC. You can use this command to revoke: <code>REVOKE ALL ON SYSCAT.INDEXAUTH FROM PUBLIC. REVOKE ALL ON SYSIBM.SYSINDEXAUTH FROM PUBLIC.</code></p>

- b. Scroll to the bottom of the report, and click the '+' icon next to **Datasource Details**.



This section of the Vulnerability Assessment provides details on database server patch levels, and other information that can be utilized to reveal present vulnerabilities.

A screenshot of a table titled "Datasource Details" with a red border. The table has 12 columns: Type, Name, Sev., Desc., Host, Port, Service, User, DB, Version, Patch Level, and Full Ver. Info. There is one data row. Above the table, it says "Showing 1 of 1 datasources (0 filtered)".

Type	Name	Sev.	Desc.	Host	Port	Service	User	DB	Version	Patch Level	Full Ver. Info
DB2	osprey_db2inst2	None		10.10.9.56	50001	sample2	db2inst2		9.1	Unknown	DB2/LINUX SQL09010

Thank You

7.3 Configuring Exception Tests (Optional)

Overview

There are likely to be situations where a more flexible test criterion is desired. InfoSphere Guardium offers the ability to create a VA Exception Tests in order to meet these unique requirements.

For example: a test ID that requires DB2 dbadm may get flagged and cause the test to fail despite the administrator's knowledge and acceptance. In such a case, the administrator may add an exception to the test criteria so that the flagging will be ignored instead of causing the test to fail.

Objectives

This optional portion of the lab will take you through the necessary steps for creating a new VA Test Exception:

- __1. Accessing Test Exception Builder
- __2. Build a new VA Test Exception
- __3. Implement a Test Exception
- __4. Test the new Test Exception

- __1. Using the InfoSphere Guardium GUI, demonstrate the ease of use within the InfoSphere Guardium solution. Start the InfoSphere Guardium appliance and login.
 - __a. From your laptop, go to to <https://10.10.9.248:8443>.
 - __b. Login as **pot / guardium**.

Login

Please enter your information

User name:

Password:

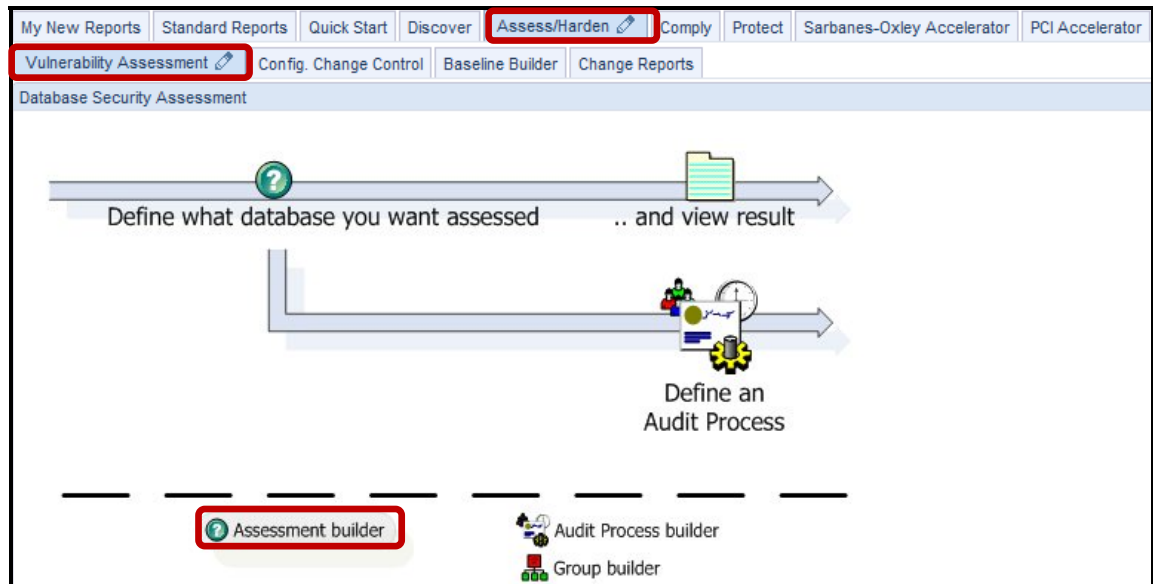
Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistrykey © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

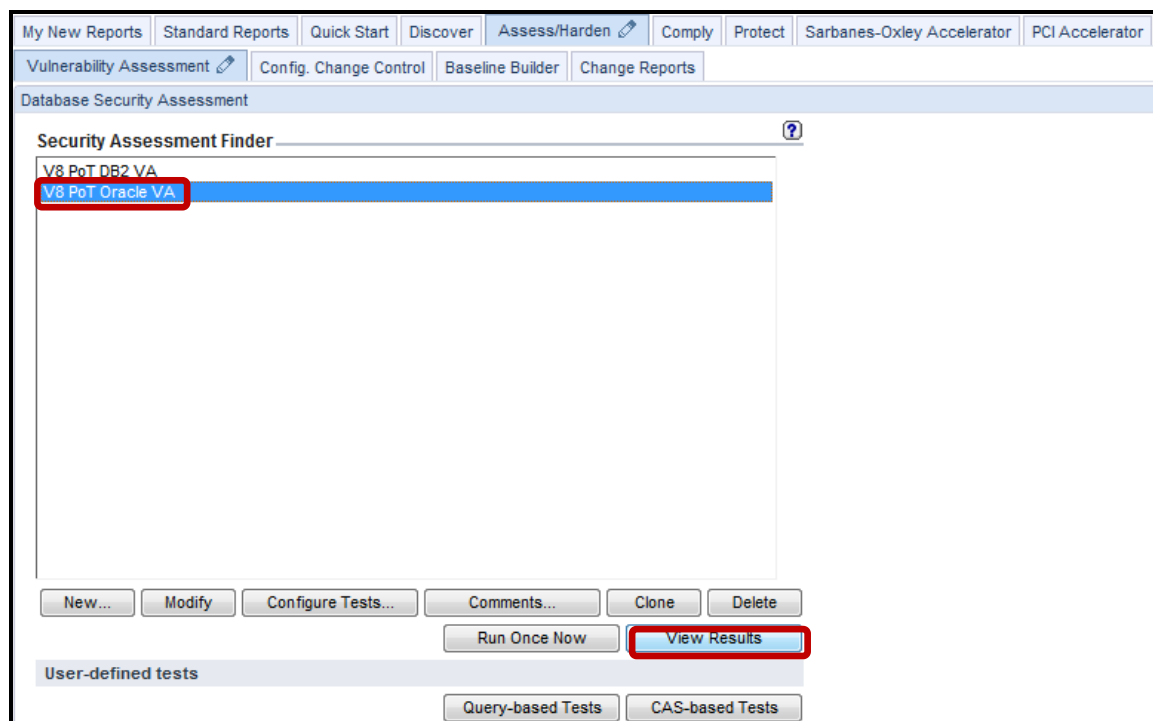
__2. Identify a Vulnerability Assessment test failure for which to create a *Test Exception*.

__a. Click **Vulnerability Assessment** under the **Assess/Harden** tab, and then click **Assessment builder**.



__b. Select **V8 PoT Oracle VA** and click **View Results**.

Note: When *View Results* is launched before the Vulnerability Assessment job has completed, only partial results will be available. Use the **F5** key to refresh the results.



c. Search for 'No Roles' to locate the 'No Roles With The Admin Option' failed test.

Result Summary										Showing 396 of 396 results (0 filtered)	
	Critical	Major	Minor	Caution	Info						
Privilege	6p	16f	--	2p	5f	--	--	1f	--	--	--
Authentication	2p	4f	--	1p	1f	--	--	1f	--	--	--
Configuration	2p	4f	1e	11p	90f	215e	3p	1f	4e	--	6f
Version	--	--	--	--	2f	--	--	--	--	--	--
Other	1p	--	--	4p	1f	--	3p	--	1e	--	4p

Current filtering applied:
 Test Severities: - Show All -
 Datasource Severities: - Show All -
 Scores: - Show All -
 Types: - Show All -

[Reset Filtering](#) [Filter / Sort Controls](#)

Assessment Test Results		Showing 396 of 396 results (0 filtered)
Test / Datasource	Result	
<p><u>DBA Profile FAILED_LOGIN_ATTEMPTS Are Limited</u> Test category: Conf. Severity: Critical This test checks the value of the FAILED_LOGIN_ATTEMPTS parameter for each account. The FAILED_LOGIN_ATTEMPTS value limits the number of failed login attempts allowed before an account is locked. Setting this value limits the ability of unauthorized users to guess passwords and alerts the DBA when password guessing has occurred (i.e., such accounts display as LOCKED). Ext. Reference: STIG D03537 CIS Oracle v2.01 Item # 8.01</p> <p>osprey_system Datasource type: ORACLE Severity: None</p>	<p>Fail User profile [DEFAULT] setup parameter FAILED_LOGIN_ATTEMPTS found out of defined threshold value <i>Recommendation: The FAILED_LOGIN_ATTEMPTS parameter is not set. A high number of failed login attempts can indicate that an unauthorized user is trying to gain unauthorized access to your data. We recommend that you set this parameter in order to limit the number of failed login attempts before locking the user's account.</i></p>	
<p><u>DBA Profile PASSWORD_GRACE_TIME Is Limited</u> Test category: Conf. Severity: Critical This test checks the value of the PASSWORD_GRACE_TIME parameter. The PASSWORD_GRACE_TIME value serves as a limit to the number of days after password expiration before the user's account is disabled. Setting this value ensures that users change their passwords at prescribed intervals. PASSWORD_GRACE_TIME can be set to any of the following: A.) A specific number of days; B.) UNLIMITED, meaning never require an account to change the password; C.) DEFAULT, which uses the value set in the DEFAULT profile. Leaving this value as UNLIMITED allows users to use the same passwords indefinitely. You should set PASSWORD_GRACE_TIME to a value <= 7. This parameter is set for profiles; accounts must then be associated with these profiles. Ext. Reference: Guardium, Test ID 2203</p> <p>osprey_system Datasource type: ORACLE Severity: None</p>	<p>Fail PASSWORD_GRACE_TIME is not set, or is set to an unacceptable value <i>Recommendation: Set PASSWORD_GRACE_TIME to a value <= 7</i></p>	
<p><u>DBA Profile PASSWORD_LIFE_TIME Is Limited</u> Test category: Conf. Severity: Critical This test checks the value of the PASSWORD_LIFE_TIME parameter. The PASSWORD_LIFE_TIME value serves as a limit to the number of days until a password expires. Setting this value ensures that users are change their passwords at specified intervals. PASSWORD_LIFE_TIME can be set to any of the following: A specific number of days; UNLIMITED, meaning never require an account to change the password; or to DEFAULT, which uses the value indicated in the DEFAULT profile. Leaving this value as UNLIMITED allows users to use the same passwords indefinitely. This parameter is set for profiles; accounts must then be associated with these profiles. Ext. Reference: STIG D03485 CIS Oracle v2.01 Item # 8.02</p> <p>osprey_system Datasource type: ORACLE Severity: None</p>	<p>Fail User profile [DEFAULT] setup parameter PASSWORD_LIFE_TIME found out of defined threshold value <i>Recommendation: The PASSWORD_LIFE_TIME parameter is not set, allowing users to retain the same password indefinitely. Passwords that have been in use for long periods of time ar likely to become known to unauthorized users. We recommend that you set this parameter in order to limit the lifetime of users' passwords.</i></p>	

d. Click the 'No Roles With The Admin Option' heading for details on the failed test.

<p><u>No Roles With The Admin Option</u> Test category: Priv. Severity: Major This test checks whether Oracle privileges have been granted with the ADMIN option to users with no DBA role, which allows the grantee to make grants to other users. The ADMIN option reduces administrative control and creates an unwarranted vulnerability. Ext. Reference: CIS Oracle v2.01 Item # 9.30</p> <p>osprey_system Datasource type: ORACLE Severity: None</p>	<p>Fail Found roles granted WITH ADMIN option <i>Recommendation: Roles have been granted with the admin option to roles or users other than users with role DBA. When a role is grantable, a user can grant that role to other users. Since granting roles should be restricted, we recommend that you not grant roles with the GRANT option</i></p>
---	--

- __e. Locate the role(s) with the admin option as detailed in the lower right corner, and click the **Close this window** link when finished.

Note: The **No Roles With The Admin Option** test failed because a role was granted with the "WITH ADMIN" option, but we will now create an exception test for this role.

IBM® InfoSphere™ Guardium®

Results for Security Assessment: **V8 PoT Oracle VA**

Assessment executed: 2012-01-13 22:51:30.0
 From: 2012-01-12 22:51:30.0
 To: 2012-01-13 22:51:30.0
 Client IP or IP subnet: Any
 Server IP or IP subnet: Any

Test Result History

Time	Result
6:00 PM 1/14/12	FAIL
6:00 AM 1/15/12	PASS
12:00 PM 1/15/12	PASS
6:00 PM 1/15/12	PASS

No Roles With The Admin Option
 Test category: Priv. Test severity: Major

osprey_system
 Datasource type: ORACLE Datasource severity: None

Fail

Found roles granted WITH ADMIN option

Short Description: This test checks whether Oracle privileges have been granted with the ADMIN option to users with no DBA role, which allows the grantee to make grants to other users. The ADMIN option reduces administrative control and creates an unwarranted vulnerability.

External Reference: CIS Oracle v2.01 Item # 9.30

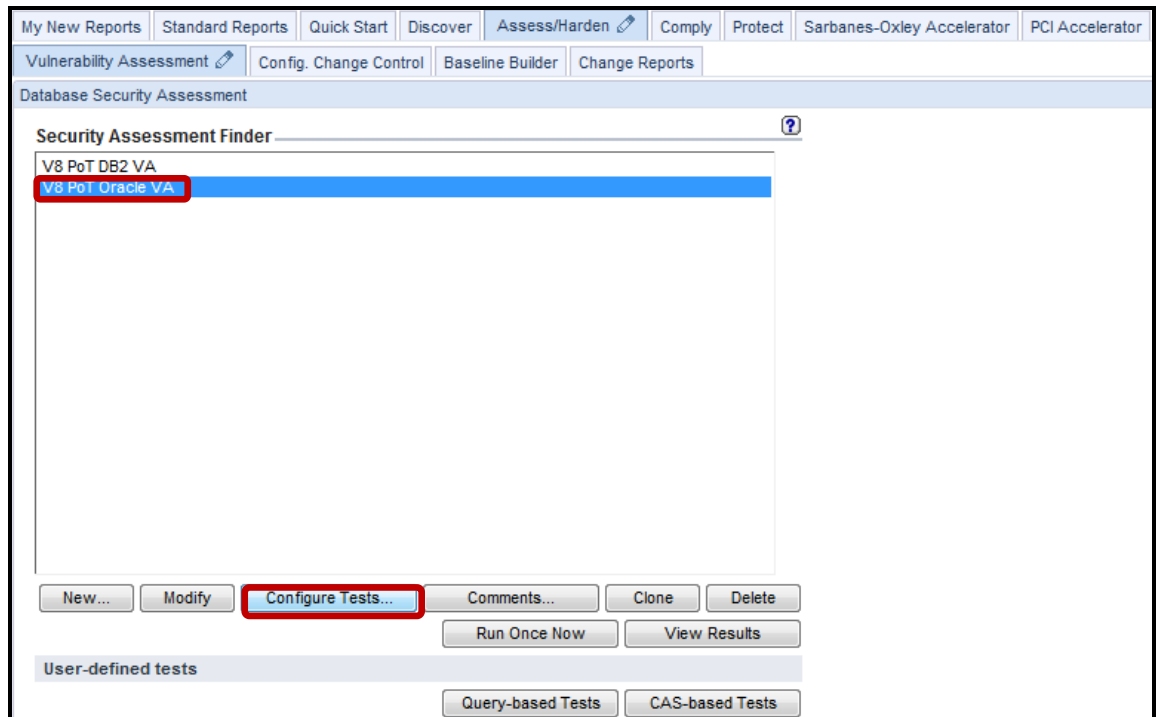
Recommendation: Roles have been granted with the admin option to roles or users other than users with role DBA. When a role is grantable, a user can grant that role to other users. Since granting roles should be restricted, we recommend that you not grant roles with the GRANT option

Details:
 Following Roles with admin option found:
 CTXSYS

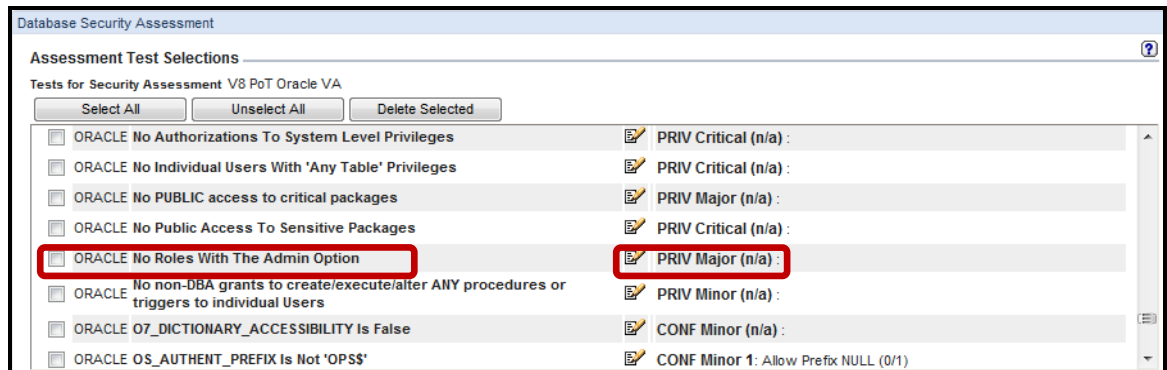
[Close this window](#)


Note: The detailed view identifies the **CTXSYS** role as the cause of the test failure.

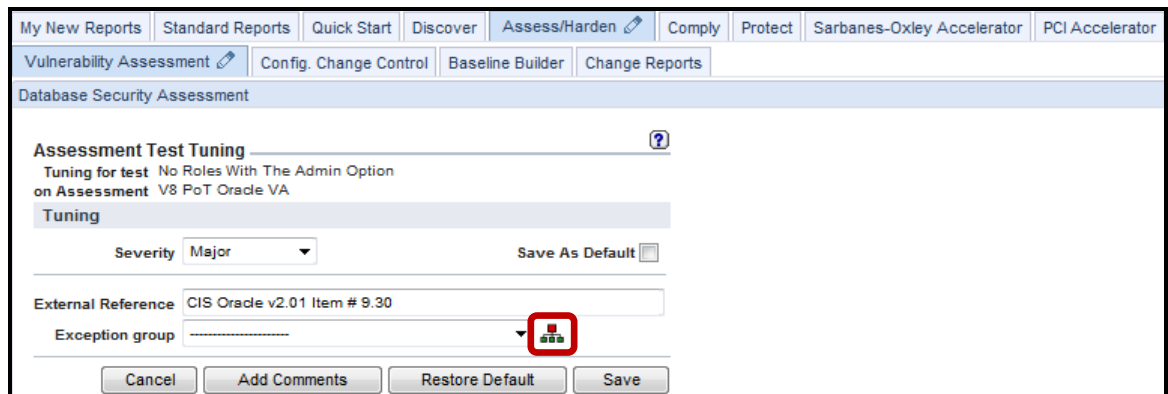
- ___3. Create a new Test Exception for the desired Vulnerability Assessment test failure.
 - ___a. Click **Configure Tests** for the **V8 PoT Oracle VA Vulnerability Assessment**.



- ___b. Scroll down to locate the **No Roles With The Admin Option** test definition (definitions are in alphabetical order) and click on the **pencil icon** to '*Adjust this test's tuning*'.



___c. Click the  (Group) icon on the lower right of the screen.



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

Vulnerability Assessment | Config. Change Control | Baseline Builder | Change Reports

Database Security Assessment


Assessment Test Tuning ?

Tuning for test No Roles With The Admin Option
on Assessment V8 PoT Oracle VA

Tuning

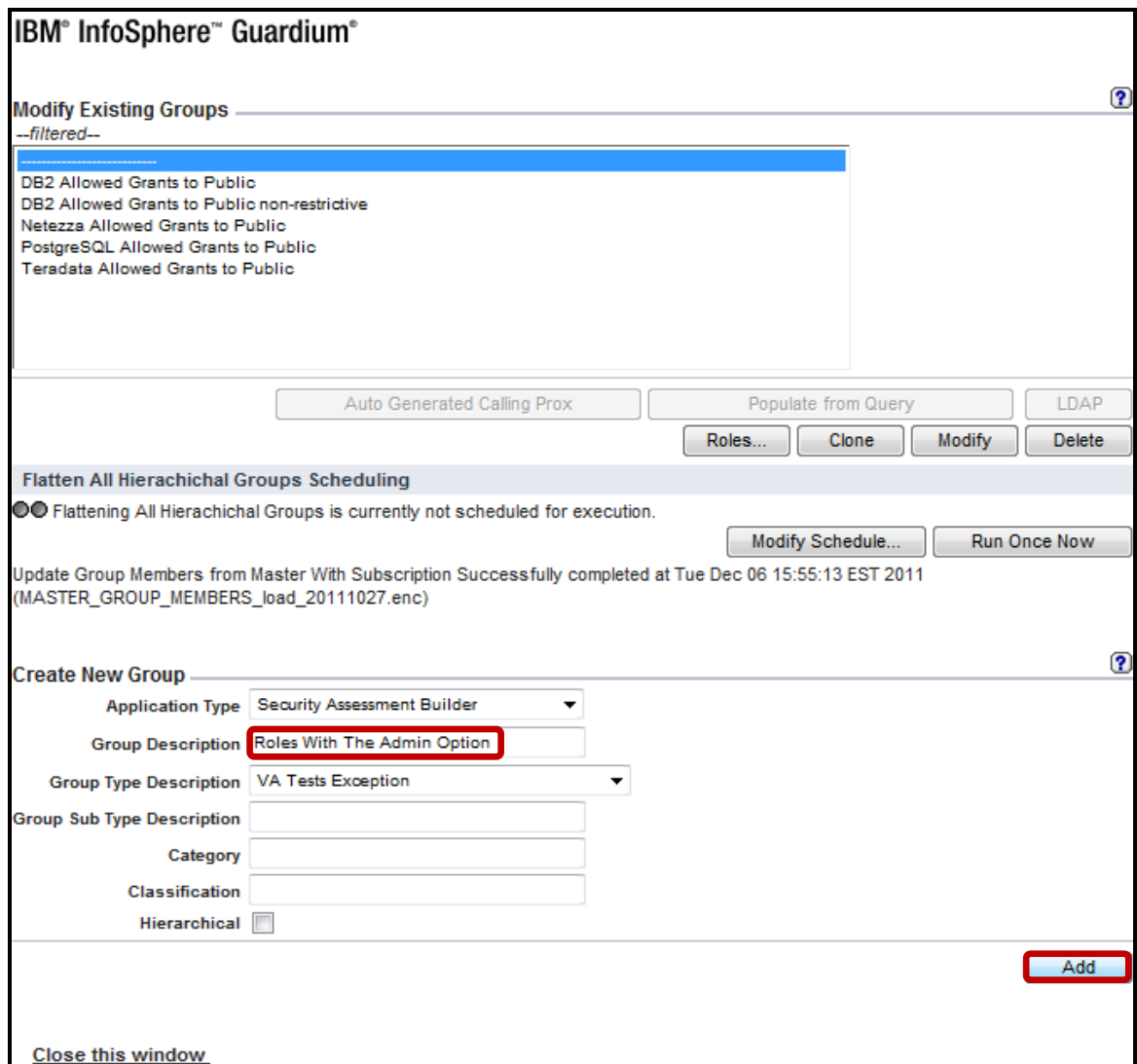
Severity Major Save As Default

External Reference CIS Oracle v2.01 Item # 9.30

Exception group 

Cancel Add Comments Restore Default Save

___d. Enter 'Roles With The Admin Option Granted' for *Group Description*, then scroll down and click **Add**.



IBM® InfoSphere™ Guardium®

Modify Existing Groups ?

--filtered--

- DB2 Allowed Grants to Public
- DB2 Allowed Grants to Public non-restrictive
- Netezza Allowed Grants to Public
- PostgreSQL Allowed Grants to Public
- Teradata Allowed Grants to Public

Auto Generated Calling Prox Populate from Query LDAP

Roles... Clone Modify Delete

Flatten All Hierarchical Groups Scheduling

Flattening All Hierarchical Groups is currently not scheduled for execution. Modify Schedule... Run Once Now

Update Group Members from Master With Subscription Successfully completed at Tue Dec 06 15:55:13 EST 2011
(MASTER_GROUP_MEMBERS_load_20111027.enc)

Create New Group ?

Application Type Security Assessment Builder

Group Description Roles With The Admin Option

Group Type Description VA Tests Exception

Group Sub Type Description

Category

Classification

Hierarchical

Add

[Close this window.](#)

- __e. Enter the **CTXSYS** role in the *Create & add a new Member named* field.
- __f. Click **Add** and then **Back**.

IBM® InfoSphere™ Guardium®

Manage Members for Selected Group ?

Group Name Roles With The Admin Option

Group Type VA Tests Exception Modify Group Type

Category Modify Category

Group Members Filter ➡ ✎

Please select one of the following options

Create & add a new Member named Add

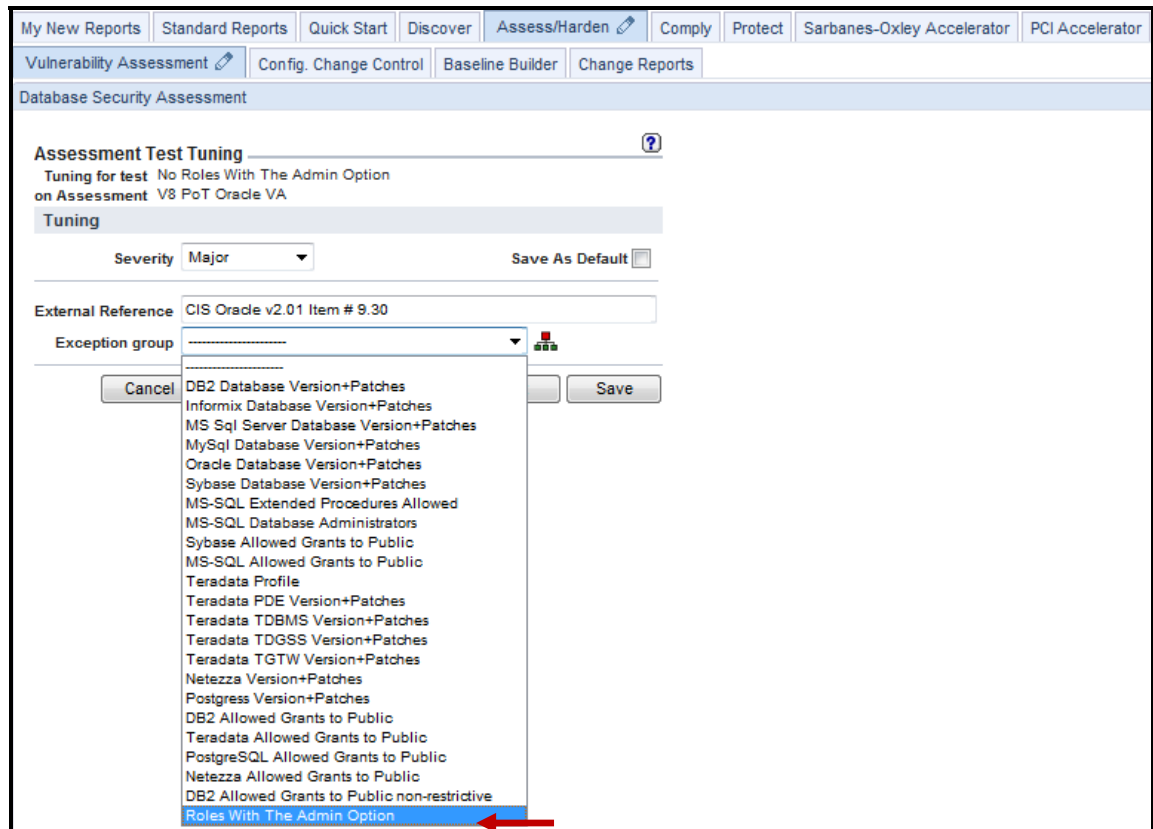
Rename selected Member to Update

Delete selected Member Delete

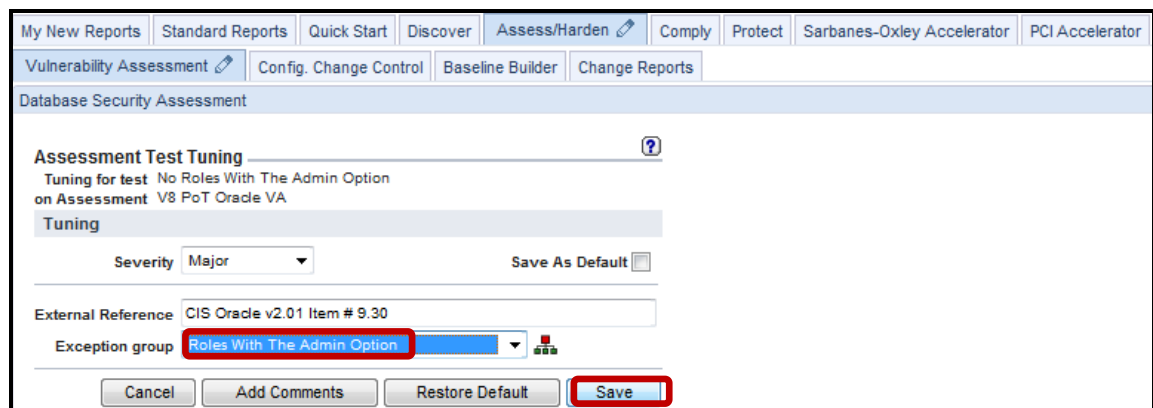
Add Comments Aliases... LDAP Back

[Close this window](#)

- g. Select the newly created **Roles With The Admin Option Granted** *Exception Group* from the drop-down list to add it.

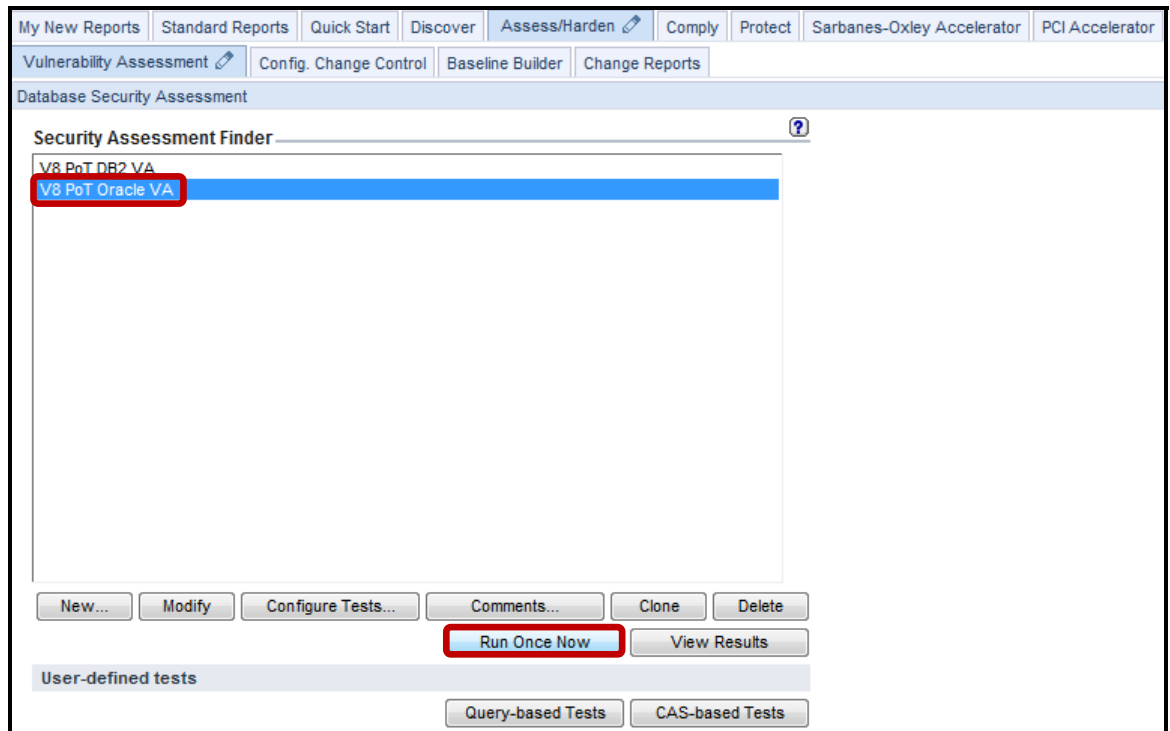


- h. Click **Save** and then click **Return** on the next screen to return to the initial *Security Assessment Finder* screen.

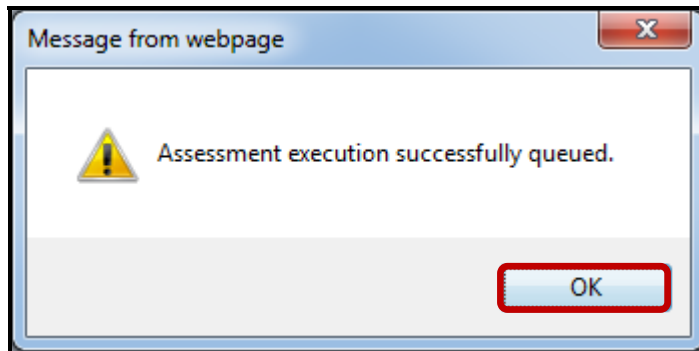


__4. Verify the new Test Exception Group.

__a. Select the **V8 PoT Oracle VA** Vulnerability Assessment and click **Run Once Now**.



__b. Click **OK** to acknowledge.



__c. Check the Guardium Job Queue until the Vulnerability Assessment has completed.

Process Run Id	Process Type	Status	Process Id	Report Result	Guardium Job Description	Task Description	Queue Time	Start Time	End Time	Datasources
5	ASSESSMENT	COMPLETED	20000	3	V8 PoT Oracle VA		2012-01-14 19:23:39.0	2012-01-14 19:24:16.0	2012-01-14 19:25:30.0	ORACLE osprey_system
4	ASSESSMENT	COMPLETED	20001	2	V8 PoT DB2 VA		2012-01-14 19:20:21.0	2012-01-14 19:20:56.0	2012-01-14 19:21:23.0	DB2 osprey_db2inst2
3	ASSESSMENT	COMPLETED	20000	1	V8 PoT Oracle VA		2012-01-14 19:17:52.0	2012-01-14 19:18:16.0	2012-01-14 19:19:33.0	ORACLE osprey_system
2	CLASSIFICATION	COMPLETED	20001	2	V8 PoT Fire only with Marker		2012-01-14 17:12:52.0	2012-01-14 17:13:32.0	2012-01-14 17:14:10.0	ORACLE osprey_system
1	CLASSIFICATION	COMPLETED	20000	1	V8 PoT PCI Classification Process		2012-01-14 16:47:00.0	2012-01-14 16:47:31.0	2012-01-14 16:47:50.0	ORACLE osprey_system

__d. Verify that the test has passed after adding the new **Test Exception**.

<p>No 'Catalog' Role Assignments Test category: Priv. Severity: Major This test checks whether Oracle privileges containing the word 'CATALOG'. These roles permit users to perform operations on other roles and across the entire database, and are inconsistent with good administration practices. Ext. Reference: STIG D00170 CIS Oracle v2.01 Item # 9.23</p> <p>osprey_system Datasource type: ORACLE Severity: None</p>	<p>Pass Predefined catalog roles are only granted to other predefined dba or roles. Recommendation: Data Dictionary and Catalog roles, 'SELECT_CATALOG_ROLE', 'OLAP_DBA', 'EXECUTE_CATALOG_ROLE', 'DELETE_CATALOG_ROLE', and 'RECOVERY_CATALOG_OWNER' are restricted to predefined roles, as recommended.</p>
<p>No Roles With The Admin Option Test category: Priv. Severity: Major This test checks whether Oracle privileges have been granted with the ADMIN option to users with no DBA role, which allows the grantee to make grants to other users. The ADMIN option reduces administrative control and creates an unwarranted vulnerability. Ext. Reference: CIS Oracle v2.01 Item # 9.30</p> <p>osprey_system Datasource type: ORACLE Severity: None</p>	<p>Pass roles granted WITH ADMIN option not found Recommendation: Roles are granted without the admin option except to users with ROLE DBA as recommended</p>
<p>OS_ROLES is False Test category: Conf. Severity: Major This test checks the value of the OS_ROLES parameter. The OS_ROLES configuration parameter, when enabled, allows permissions to be granted by OS group membership, which is controlled outside of the database access controls. Ext. Reference: CIS Oracle v2.01 Item # 4.09</p> <p>osprey_system Datasource type: ORACLE Severity: None</p>	<p>Pass Parameter: 'OS_ROLES' is 'FALSE'. Recommendation: The OS_ROLES parameter is set to false, as recommended.</p>

Note: The Test Exception has successfully filtered out a test failure that may have been deemed to be unnecessary under current compliance standards. Perhaps, these represent known vulnerabilities that will soon be resolved with a patch that is awaiting the proper maintenance window before it can be applied.

The Test Exception feature can be useful to cut down on the “noise” of test failures across the enterprise. This lab has shown how easy, and flexible this capability can be.

Thank You

Vulnerability Assessment review

- __1. Vulnerability Assessment runs on:
 - __a. The InfoSphere Guardium Collector
 - __b. The database server
 - __c. The client PC
 - __d. Part of S-TAP

- __2. Guardium Vulnerability Assessments requires access to the databases (**True** or **False**)

- __3. Where does Guardium store the Vulnerability Assessment results?
 - __a. Custom domain
 - __b. Access domain
 - __c. Database server
 - __d. Vulnerability Access domain

- __4. Guardium allows adding custom VA test. (**True** or **False**)

- __5. Virtual patching is a component of:
 - __a. S-TAP
 - __b. Vulnerability Assessment
 - __c. Database Auto-Discovery
 - __d. CAS

Vulnerability Assessment review (Answers)

__1. Vulnerability Assessment runs on:

A – The InfoSphere Guardium Collector

__2. Guardium Vulnerability Assessments requires access to the databases
(**True** or **False**)

True.

__3. Where does Guardium store the Vulnerability Assessment results?

D – Vulnerability Assessment domain.

__4. Guardium allows adding custom VA test.
(**True** or **False**)

True.

__5. Virtual patching is a component of:

B – Vulnerability Assessment.

Lab 8 Compliance Workflow Automation

8.1 Exploring Compliance Workflow Automation

Overview

The IBM InfoSphere® Guardium® Compliance Workflow Automation application streamlines the entire compliance workflow process, helping automate audit report generation, distribution to key stakeholders, electronic sign-off and escalations. Workflow processes are completely user customizable; specific audit items can be individually routed and tracked through sign-off.

An Audit Workflow enables you to bundle a set of reports, classifier jobs or Vulnerability Assessment runs and schedule their delivery to specified recipients. In addition, InfoSphere Guardium manages the distribution status automatically by keeping track of which recipients have reviewed or signed off.

Objectives

This Lab will illustrate how we can create a simple audit workflow using the InfoSphere Guardium GUI in the following steps:

- __1. Add users who will manage the audit process
- __2. Create a workflow process with notification recipients.
- __3. Bundle a set of reports.
- __4. Schedule/run the workflow process.
- __5. Verify the distribution process.

- __1. **Critical Step** – We will require four additional InfoSphere Guardium user accounts to manage the audit processes for the Compliance Workflow Automation labs. The following steps will take you through the process to create these users.
- __a. From your laptop, go to <https://10.10.9.248:8443>
- __b. Login as **accessmgr / guardium**. User accessmgr is used to create and manage IDs.

Login

Please enter your information

User name:

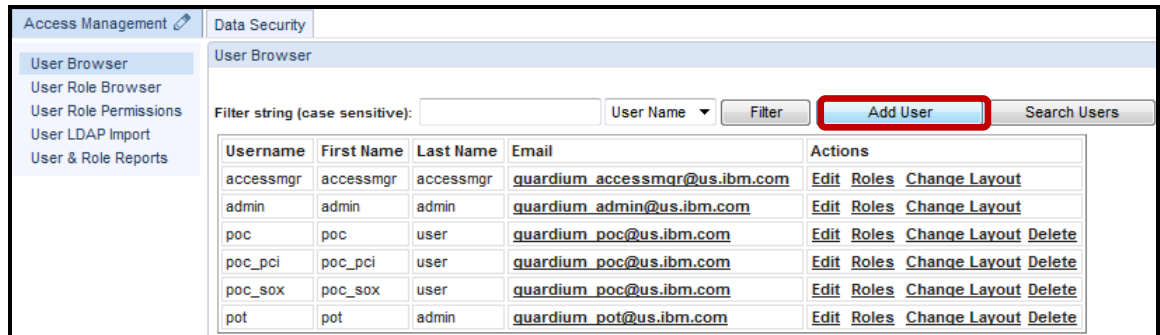
Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIF5 Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistrykey © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

- c. Click **Add User** from the *Access Management* window to add a Database Admin user.



- d. Enter 'joe' for the *Username* field, 'guardium' for the *password* field, and 'guardium' for the *password confirm* field.
- e. Enter 'joe' for the *First Name* field, 'dba' for the *Last Name* field, uncheck the **Disabled** checkbox, and then click **Add User**.
- f. Enter 'guardium_pot@us.ibm.com' for the *Email* field.

Note: If the **Disabled** checkbox is left checked, the user will remain locked out of the system. This is used for new users and in cases of too many failed login attempts.



- __g. Click **Add User** from the *Access Management* window to add an Info Security user.

The screenshot shows the 'User Browser' section of the 'Data Security' interface. A table lists existing users with columns for Username, First Name, Last Name, Email, and Actions. The 'Add User' button is highlighted with a red box.

Username	First Name	Last Name	Email	Actions
accessmgr	accessmgr	accessmgr	guardium_accessmgr@us.ibm.com	Edit Roles Change Layout
admin	admin	admin	guardium_admin@us.ibm.com	Edit Roles Change Layout
joe	joe	dba	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
poc	poc	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
poc_pci	poc_pci	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
poc_sox	poc_sox	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
pot	pot	admin	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete

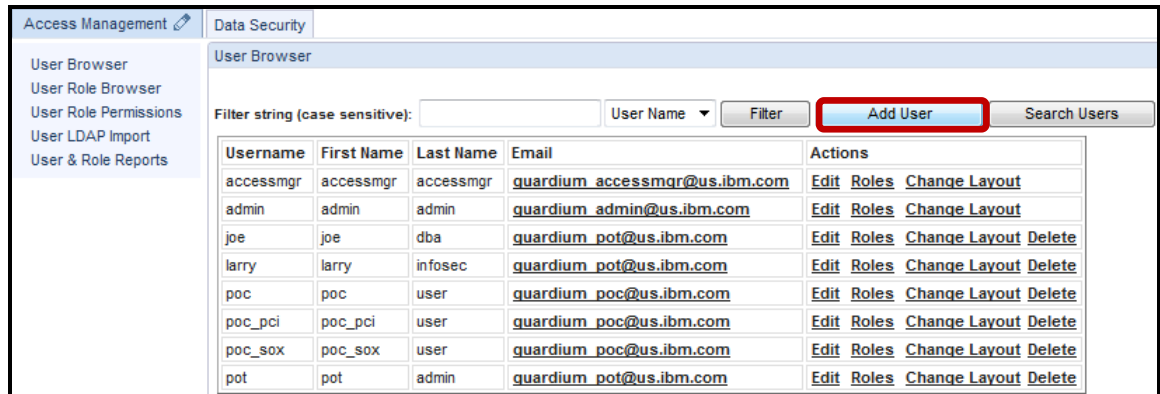
- __h. Enter '**larry**' for the *Username* field, '**guardium**' for the *password* field, and '**guardium**' for the *password confirm* field.
- __i. Enter '**larry**' for the *First Name* field, '**infosec**' for the *Last Name* field, uncheck the **Disabled** checkbox, and then click **Add User**.
- __j. Enter '**guardium_pot@us.ibm.com**' for the *Email* field.

Note: If the **Disabled** checkbox is left checked, the user will remain locked out of the system. This is used for new users, and in cases of too many failed login attempts.

The screenshot shows the 'User Form' section of the 'Data Security' interface. The form fields are filled with the following values: Username: larry, Password: [masked], Password (confirm): [masked], First Name: larry, Last Name: infosec, Email: guardium_pot@us.ibm.com. The 'Disabled' checkbox is unchecked. The 'Add User' button is highlighted with a red box.

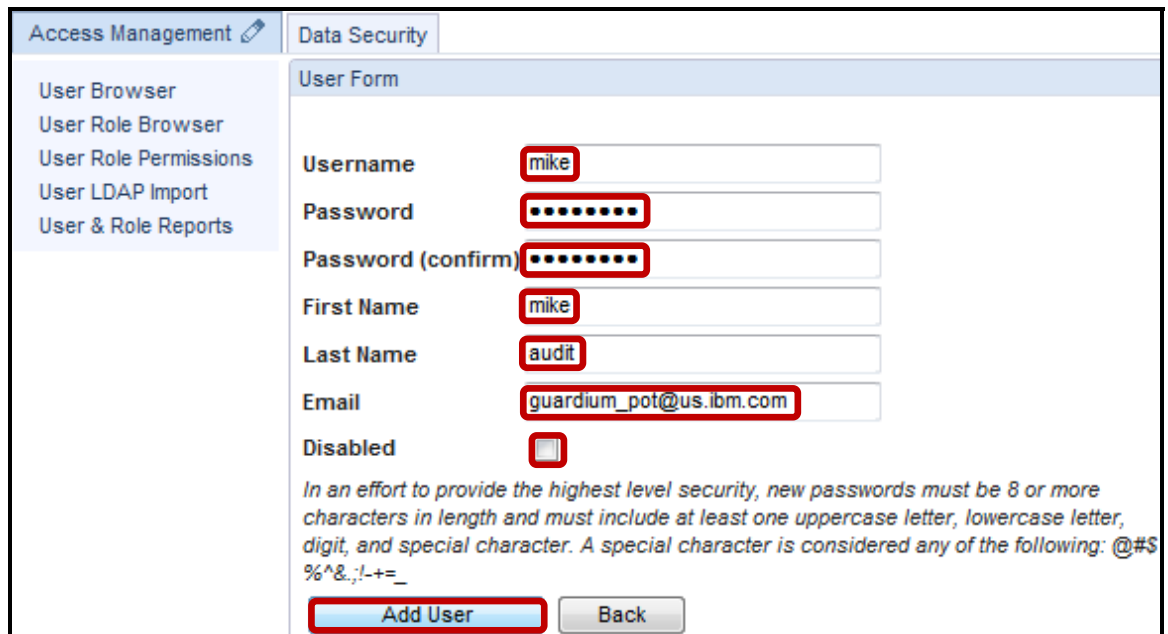
In an effort to provide the highest level security, new passwords must be 8 or more characters in length and must include at least one uppercase letter, lowercase letter, digit, and special character. A special character is considered any of the following: @#\$%^&.,!-+=_

- __k. Click **Add User** from the *Access Management* window to add an Auditor user.



- __l. Enter 'mike' for the *Username* field, 'guardium' for the *password* field, and 'guardium' for the *password confirm* field.
- __m. Enter 'mike' for the *First Name* field, 'audit' for the *Last Name* field, uncheck the **Disabled** checkbox, and then click **Add User**.
- __n. Enter 'guardium_pot@us.ibm.com' for the *Email* field.

Note: If the **Disabled** checkbox is left checked, the user will remain locked out of the system. This is used for new users, and in cases of too many failed login attempts.



- ___o. Click **Add User** from the *Access Management* window to add a PCI Compliance user.

The screenshot shows the 'User Browser' window in the 'Access Management' application. The 'Add User' button is highlighted with a red box. Below the button is a table of existing users.

Username	First Name	Last Name	Email	Actions
accessmgr	accessmgr	accessmgr	guardium_accessmgr@us.ibm.com	Edit Roles Change Layout
admin	admin	admin	guardium_admin@us.ibm.com	Edit Roles Change Layout
joe	joe	dba	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
larry	larry	infosec	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
mike	mike	audit	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
poc	poc	user	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
poc_pci	poc_pci	user	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
poc_sox	poc_sox	user	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
pot	pot	admin	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete

- ___p. Enter **'peter'** for the *Username* field, **'guardium'** for the *password* field, and **'guardium'** for the *password confirm* field.
- ___q. Enter **'peter'** for the *First Name* field, **'pci'** for the *Last Name* field, uncheck the **Disabled** checkbox, and then click **Add User**.
- ___r. Enter **'guardium_pot@us.ibm.com'** for the *Email* field.

Note: If the **Disabled** checkbox is left checked, the user will remain locked out of the system. This is used for new users, and in cases of too many failed login attempts.

The screenshot shows the 'User Form' window in the 'Access Management' application. The 'Add User' button is highlighted with a red box. The form fields are filled with the following values:

- Username: peter
- Password: [Redacted]
- Password (confirm): [Redacted]
- First Name: peter
- Last Name: pci
- Email: guardium_pot@us.ibm.com
- Disabled:

Below the form, there is a note: "In an effort to provide the highest level security, new passwords must be 8 or more characters in length and must include at least one uppercase letter, lowercase letter, digit, and special character. A special character is considered any of the following: @#\$%^&.~!+=_%^&.~!+=_"

__2. Assign Roles to newly created users.

__a. Click **Roles** alongside *user joe* to add the **dba** role to user *joe*.

The screenshot shows the 'User Browser' interface. At the top, there are tabs for 'Access Management' and 'Data Security'. Below the tabs is a navigation menu with options like 'User Browser', 'User Role Browser', etc. The main area contains a table of users with columns for Username, First Name, Last Name, Email, and Actions. The 'Actions' column for user 'joe' has a 'Roles' link highlighted with a red box.

Username	First Name	Last Name	Email	Actions
accessmgr	accessmgr	accessmgr	guardium_accessmgr@us.ibm.com	Edit Roles Change Layout
admin	admin	admin	guardium_admin@us.ibm.com	Edit Roles Change Layout
joe	joe	dba	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
larry	larry	infosec	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
mike	mike	audit	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
peter	peter	pci	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
poc	poc	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
poc_pci	poc_pci	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
poc_sox	poc_sox	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
pot	pot	admin	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete

__b. Check the **dba** box and click **Save** to add the *dba* role to user *joe*.

Note: The *user* role is given by default.

The screenshot shows the 'User Role Form' for user 'joe'. The title is 'Roles for joe dba'. Below the title is a table with two columns: 'Role Name' and 'Assign'. The 'dba' role has its checkbox checked and highlighted with a red box. The 'user' role at the bottom also has its checkbox checked.

Role Name	Assign
accessmgr	<input type="checkbox"/>
admin	<input type="checkbox"/>
appdev	<input type="checkbox"/>
audit	<input type="checkbox"/>
Basell	<input type="checkbox"/>
cas	<input type="checkbox"/>
cli	<input type="checkbox"/>
DataPrivacy	<input type="checkbox"/>
datasec-exempt	<input type="checkbox"/>
dba	<input checked="" type="checkbox"/>
diag	<input type="checkbox"/>
infosec	<input type="checkbox"/>
inv	<input type="checkbox"/>
netadm	<input type="checkbox"/>
pci	<input type="checkbox"/>
review-only	<input type="checkbox"/>
sox	<input type="checkbox"/>
user	<input checked="" type="checkbox"/>

At the bottom of the form are 'Save' and 'Back' buttons.

- __c. Click **Roles** alongside *user larry* to add the **infosec** role to user **larry**.

The screenshot shows the 'User Browser' interface. On the left is a navigation menu with options: User Browser, User Role Browser, User Role Permissions, User LDAP Import, and User & Role Reports. The main area is titled 'User Browser' and contains a search filter and a table of users. The table has columns for Username, First Name, Last Name, Email, and Actions. The user 'larry' is highlighted, and the 'Roles' link in the Actions column is circled in red.

Username	First Name	Last Name	Email	Actions
accessmgr	accessmgr	accessmgr	guardium_accessmgr@us.ibm.com	Edit Roles Change Layout
admin	admin	admin	guardium_admin@us.ibm.com	Edit Roles Change Layout
joe	joe	dba	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
larry	larry	infosec	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
mike	mike	audit	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
peter	peter	pci	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
poc	poc	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
poc_pci	poc_pci	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
poc_sox	poc_sox	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
pot	pot	admin	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete

- __d. Check the **infosec** box and click **Save** to add the *infosec* role to user **larry**.

Note: The *user* role is given by default.

The screenshot shows the 'User Role Form' interface. On the left is a navigation menu with options: User Browser, User Role Browser, User Role Permissions, User LDAP Import, and User & Role Reports. The main area is titled 'User Role Form' and contains a section 'Roles for larry infosec'. Below this is a table with columns for Role Name and Assign. The 'infosec' role is checked, and the checkbox is highlighted with a red box. At the bottom are 'Save' and 'Back' buttons.

Role Name	Assign
accessmgr	<input type="checkbox"/>
admin	<input type="checkbox"/>
appdev	<input type="checkbox"/>
audit	<input type="checkbox"/>
Basell	<input type="checkbox"/>
cas	<input type="checkbox"/>
cli	<input type="checkbox"/>
DataPrivacy	<input type="checkbox"/>
datasec-exempt	<input type="checkbox"/>
dba	<input type="checkbox"/>
diag	<input type="checkbox"/>
infosec	<input checked="" type="checkbox"/>
inv	<input type="checkbox"/>
netadm	<input type="checkbox"/>
pci	<input type="checkbox"/>
review-only	<input type="checkbox"/>
sox	<input type="checkbox"/>
user	<input checked="" type="checkbox"/>

__e. Click **Roles** alongside *user mike* to add the **audit** role to user **mike**.

The screenshot shows the 'User Browser' interface. At the top, there are tabs for 'Access Management' and 'Data Security'. Below the tabs is a navigation menu with options like 'User Browser', 'User Role Browser', etc. The main area contains a table of users with columns for Username, First Name, Last Name, Email, and Actions. The 'Actions' column for user 'mike' has a 'Roles' link highlighted with a red box.

Username	First Name	Last Name	Email	Actions
accessmgr	accessmgr	accessmgr	guardium_accessmgr@us.ibm.com	Edit Roles Change Layout
admin	admin	admin	guardium_admin@us.ibm.com	Edit Roles Change Layout
joe	joe	dba	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
larry	larry	infosec	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
mike	mike	audit	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
peter	peter	pci	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
poc	poc	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
poc_pci	poc_pci	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
poc_sox	poc_sox	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
pot	pot	admin	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete

__f. Check the **audit** box and click **Save** to add the *audit* role to user **mike**.

Note: The *user* role is given by default.

The screenshot shows the 'User Role Form' interface. It has a navigation menu on the left and a main area titled 'Roles for mike audit'. Below the title is a table with columns for 'Role Name' and 'Assign'. The 'audit' role has its checkbox checked and highlighted with a red box. At the bottom, there are 'Save' and 'Back' buttons.

Role Name	Assign
accessmgr	<input type="checkbox"/>
admin	<input type="checkbox"/>
appdev	<input type="checkbox"/>
audit	<input checked="" type="checkbox"/>
Basell	<input type="checkbox"/>
cas	<input type="checkbox"/>
cli	<input type="checkbox"/>
DataPrivacy	<input type="checkbox"/>
datasec-exempt	<input type="checkbox"/>
dba	<input type="checkbox"/>
diag	<input type="checkbox"/>
infosec	<input type="checkbox"/>
inv	<input type="checkbox"/>
netadm	<input type="checkbox"/>
pci	<input type="checkbox"/>
review-only	<input type="checkbox"/>
sox	<input type="checkbox"/>
user	<input checked="" type="checkbox"/>

- g. Click **Roles** alongside *user peter* to add the **pci** role to user **peter**.

The screenshot shows the 'User Browser' interface. At the top, there are tabs for 'Access Management' and 'Data Security'. Below the tabs is a navigation menu with options like 'User Browser', 'User Role Browser', etc. The main area contains a search bar and a table of users. The table has columns for Username, First Name, Last Name, Email, and Actions. The 'Roles' link for the user 'peter' is highlighted with a red box.

Username	First Name	Last Name	Email	Actions
accessmgr	accessmgr	accessmgr	guardium_accessmgr@us.ibm.com	Edit Roles Change Layout
admin	admin	admin	guardium_admin@us.ibm.com	Edit Roles Change Layout
joe	joe	dba	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
larry	larry	infosec	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
mike	mike	audit	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
peter	peter	pci	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete
poc	poc	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
poc_pci	poc_pci	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
poc_sox	poc_sox	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
pot	pot	admin	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete

- h. Check the **pci** box and click **Save** to add the *pci* role to user **peter**.
- i. Logout of the InfoSphere Guardium GUI as user **accessmgr**.

Note: The *user* role is given by default.

The screenshot shows the 'User Role Form' for user 'peter pci'. It displays a list of roles with checkboxes next to them. The 'pci' role checkbox is checked and highlighted with a red box. At the bottom, there are 'Save' and 'Back' buttons.

Role Name	Assign
accessmgr	<input type="checkbox"/>
admin	<input type="checkbox"/>
appdev	<input type="checkbox"/>
audit	<input type="checkbox"/>
Basell	<input type="checkbox"/>
cas	<input type="checkbox"/>
cli	<input type="checkbox"/>
DataPrivacy	<input type="checkbox"/>
datasec-exempt	<input type="checkbox"/>
dba	<input type="checkbox"/>
diag	<input type="checkbox"/>
infosec	<input type="checkbox"/>
inv	<input type="checkbox"/>
netadm	<input type="checkbox"/>
pci	<input checked="" type="checkbox"/>
review-only	<input type="checkbox"/>
sox	<input type="checkbox"/>
user	<input checked="" type="checkbox"/>

- __3. Use the InfoSphere Guardium GUI to create a new Compliance Audit Process.
 - __a. From your laptop, go to <https://10.10.9.248:8443>
 - __b. Login as **pot / guardium**.

Login

Please enter your information

User name:

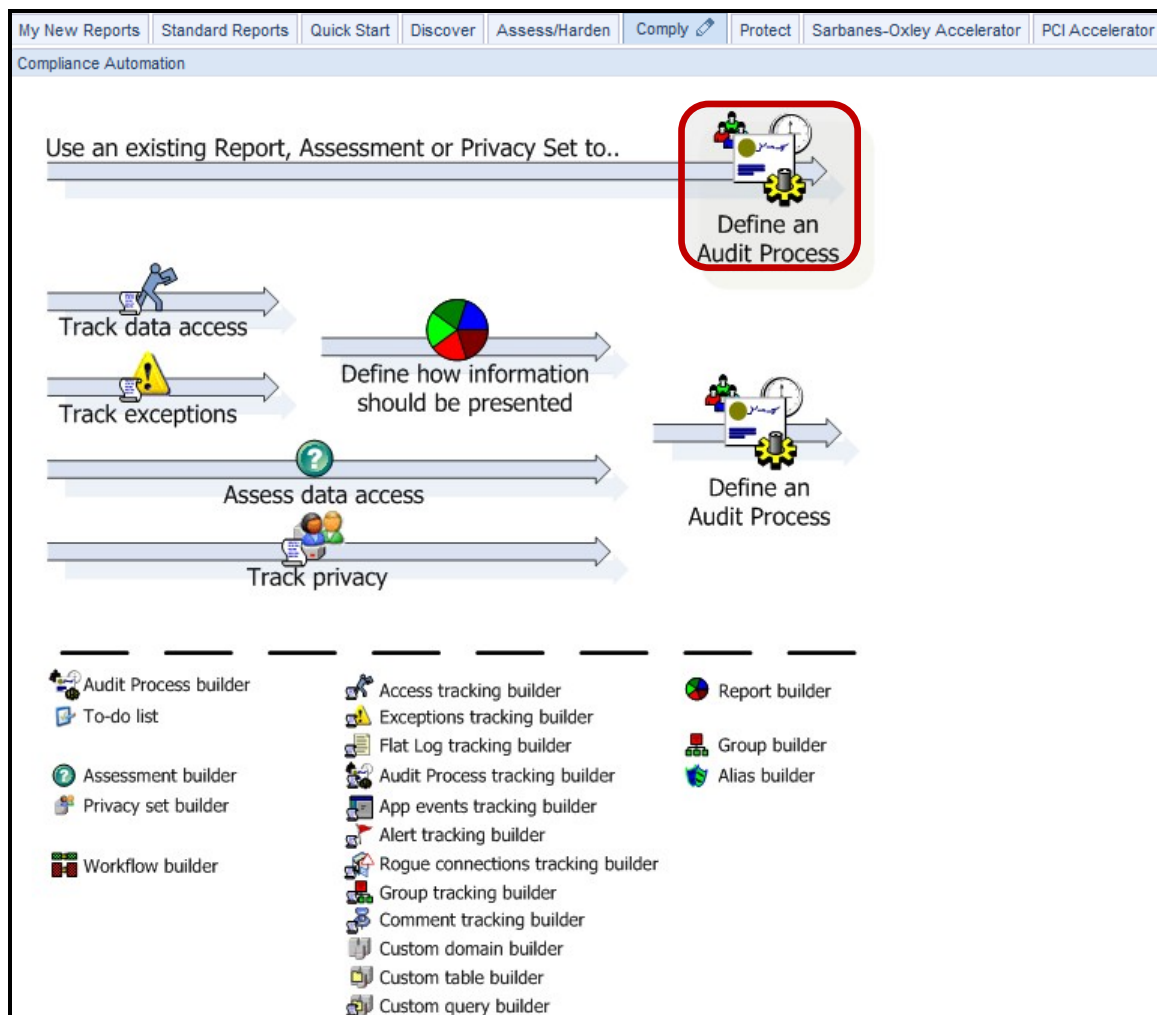
Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

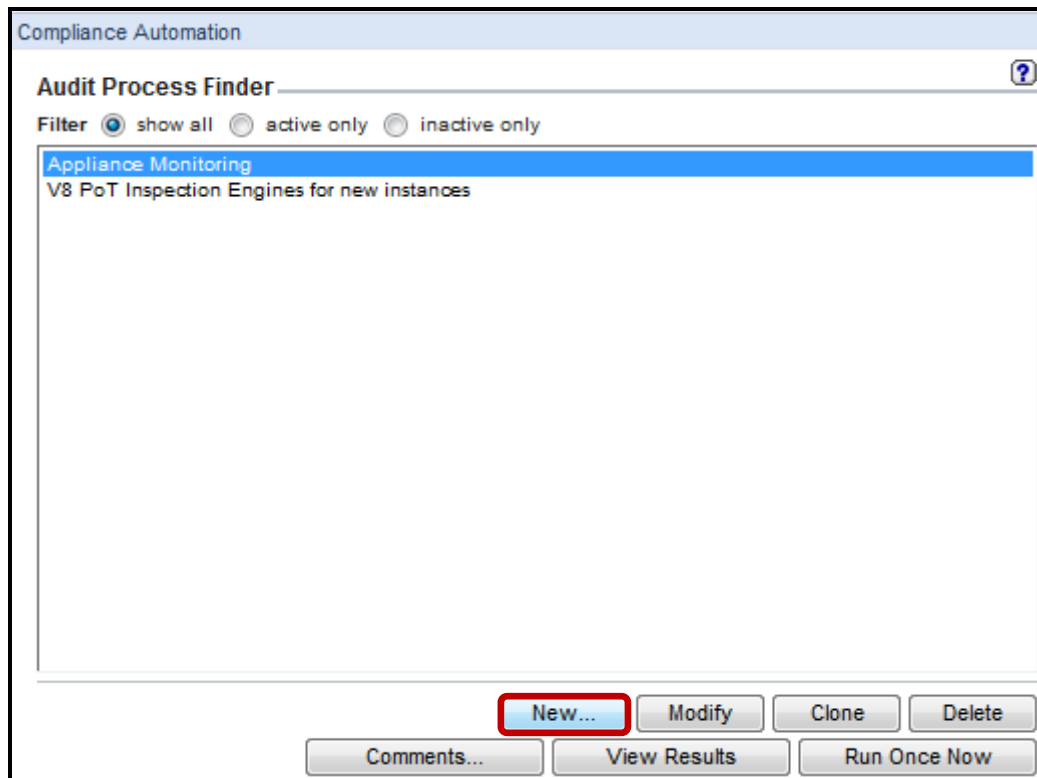
Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistry/key © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

c. Click **Define an Audit Process** under the **Comply** tab.



__d. Click **New**.



- e. Enter 'V8 PoT PCI Audit Process' for the *Description* field, select **mike(mike audit)** from the *Receiver name* drop-down list, and click **Add**.

Compliance Automation

Audit Process Definition ?

Description

Active There is no schedule associated with this process

Archive Results

Keep for a minimum of days or runs

CSV/CEF File Label Zip CSV for mail

Email Subject:

View Run Once Now Modify Schedule...

Receiver	Action Req.	To-Do List	Email Notif.	Cont.	Appv. if Empty
Add Receiver					
Receiver name	mike(mike audit) <input type="button" value="Search users"/>				
Action Required	-----				
To-Do List	email:				
Email Notification	role: accessmgr				
	role: admin				
Continuous	role: audit				
Approve if Empty	role: cas				
	role: dba				
	role: infosec				
	role: pci				
	role: sox				
	role: user				
	accessmgr(accessmgr accessmgr)				
	admin(admin admin)				
	joe(joe dba)				
	larry(larry infosec)				
	mike(mike audit) ←				
	peter(peter pci)				
	poc(poc user)				
	poc_pci(poc_pci user)				
	poc_sox(poc_sox user)				
	pot(pot admin)				
Roles	No roles have been assigned to this Process				
	<input type="button" value="Roles..."/>				
	<input type="button" value="Delete"/> <input type="button" value="Clone"/> <input type="button" value="Refresh"/> <input type="button" value="Apply"/> <input type="button" value="Back"/>				

- f. Select the **Full Results** radio button for the *Email Notification* type, check the **PDF** checkbox, select **peter(peter pci)** from the *Receiver name* drop-down list, and click **Add**.

The screenshot displays the 'Compliance Automation' interface for configuring an 'Audit Process Definition'. The process is named 'V8 PoT PCI Audit Process'. Under the 'Receiver Table', a receiver named 'mike' is listed with the following settings: Action Required (Review), To-Do List (checked), Email Notification (Full Results selected, PDF checked, CSV unchecked), Continuous (checked), and Approve if Empty (unchecked). The 'Add Receiver' dropdown menu is open, showing a list of roles including 'peter(peter pci)', which is highlighted with a red arrow. The 'Add' button is also highlighted with a red box. The 'Roles' section at the bottom indicates that no roles have been assigned to this process.

- g. Select the **Sign** radio button for the *Action Required*, select the **Full Results** radio button for the *Email Notification* type, check the **PDF** checkbox, enter '**V8 PoT PCI Oracle VA**' for the *Description* field, and then select the **Security Assessment** radio button.

Compliance Automation

Audit Process Definition

Description: V8 PoT PCI Audit Process

Active: There is no schedule associated with this process

Archive Results:

Keep for a minimum of 0 days or 5 runs

CSV/CEF File Label: V8_PoT_PCI_Audit_P Zip CSV for mail

Email Subject:

View Run Once Now Modify Schedule...

Receiver Table

Receiver	Action Req.	To-Do List	Email Notif.	Cont.	Appv. if Empty
<input checked="" type="checkbox"/> mike <input type="checkbox"/> (mike audit)	<input checked="" type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input type="radio"/> No <input type="radio"/> Link <input checked="" type="radio"/> Full Results <input checked="" type="checkbox"/> PDF <input type="checkbox"/> CSV	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> peter <input type="checkbox"/> (peter pci)	<input type="radio"/> Review <input checked="" type="radio"/> Sign	<input checked="" type="checkbox"/>	<input type="radio"/> No <input type="radio"/> Link <input checked="" type="radio"/> Full Results <input checked="" type="checkbox"/> PDF <input type="checkbox"/> CSV	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add Receiver

Receiver name: Search users

Action Required: Review Sign

To-Do List: Add

Email Notification: None Link Only Full Results

Continuous:

Approve if Empty: Yes

Add

Audit Tasks

Add New Task

Description: V8 PoT PCI Oracle VA

Task Type: Report Security Assessment Entity Audit Trail Privacy Set Classification Process

Apply

Add Audit Task

Roles

No roles have been assigned to this Process

Roles...

Delete Clone

Refresh Apply Back

- h. Select **V8 PoT Oracle VA** (created during the Vulnerability Assessment lab) from the *Security Assessment* drop-down list, click **Apply**, and then click **Add Audit Task**.

Note: The workflow process can include any existing reports, Vulnerability Assessments or classifications.

The screenshot displays the 'Compliance Automation' interface. The 'Audit Process Definition' section includes fields for Description ('V8 PoT PCI Audit Process'), Active status, Archive Results, and scheduling options (Keep for a minimum of 0 days or 5 runs). The CSV/CEF File Label is 'V8_PoT_PCI_Audit_P' with 'Zip CSV for mail' checked. The Email Subject field is empty. Buttons for 'View', 'Run Once Now', and 'Modify Schedule...' are present.

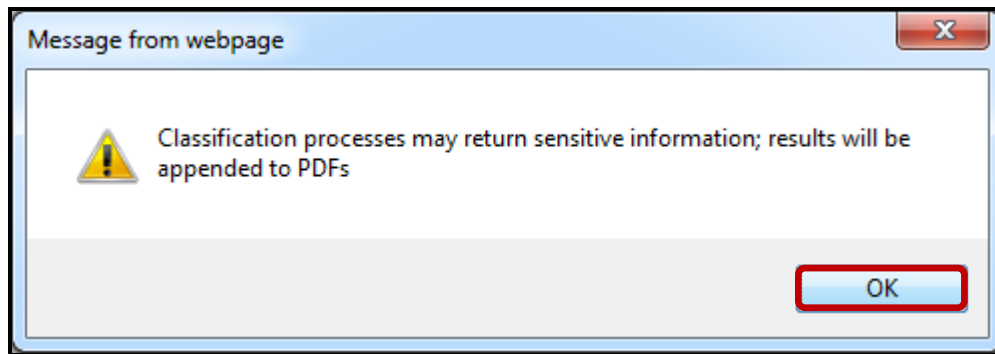
The 'Receiver Table' section contains a table with columns: Receiver, Action Req., To-Do List, Email Notif., Cont., and Appv. if Empty. Two receivers are listed: 'mike' (Action Req. Review, To-Do List checked, Email Notif. Full Results, PDF checked) and 'peter' (Action Req. Sign, To-Do List checked, Email Notif. Full Results, PDF checked).

The 'Add Receiver' section includes a 'Receiver name' dropdown, a 'Search users' button, and radio buttons for 'Action Required' (Review selected), 'To-Do List' (Add checked), 'Email Notification' (None selected), 'Continuous' (checked), and 'Approve if Empty' (Yes unchecked). An 'Add' button is at the bottom right.

The 'Audit Tasks' section shows an 'Add New Task' dialog box. The 'Description' is 'V8 PoT PCI Oracle VA'. The 'Task Type' is 'Security Assessment'. The 'Security Assessment' dropdown is open, showing 'V8 PoT DB2 VA' and 'V8 PoT Oracle VA' (highlighted with a red arrow). The 'PDF Content' dropdown is set to 'Report and Diff'. An 'Apply' button is highlighted with a red box. Below the dialog, an 'Add Audit Task' button is also highlighted with a red box.

The 'Roles' section shows 'No roles have been assigned to this Process' and a 'Roles...' button. At the bottom right, there are buttons for 'Refresh', 'Apply', 'Back', 'Delete', and 'Clone'.

- j. Click **OK** to acknowledge.



- __k. Select **V8 PoT Demo Find CC Objects** from the *Classification Process* drop-down list, click **Apply** (for the task), and then scroll down to the bottom and click **Apply** once more.

Compliance Automation

Audit Process Definition

Description: V8 PoT PCI Audit Process

Active: There is no schedule associated with this process

Archive Results:

Keep for a minimum of 0 days or 5 runs

CSV/CEF File Label: V8_PoT_PCI_Audit_P Zip CSV for mail

Email Subject:

View Run Once Now Modify Schedule...

Receiver Table

Receiver	Action Req.	To-Do List	Email Notif.	Cont.	Appv. if Empty
<input checked="" type="checkbox"/> mike <input checked="" type="checkbox"/> (mike audit)	<input checked="" type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input type="radio"/> No <input type="radio"/> Link <input checked="" type="radio"/> Full Results <input checked="" type="checkbox"/> PDF <input type="checkbox"/> CSV	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> peter <input checked="" type="checkbox"/> (peter pci)	<input type="radio"/> Review <input checked="" type="radio"/> Sign	<input checked="" type="checkbox"/>	<input type="radio"/> No <input type="radio"/> Link <input checked="" type="radio"/> Full Results <input checked="" type="checkbox"/> PDF <input type="checkbox"/> CSV	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add Receiver

Receiver name: Search users

Action Required: Review Sign

To-Do List: Add

Email Notification: None Link Only Full Results

Continuous:

Approve if Empty: Yes

Add

Audit Tasks

Security Assessment: V8 PoT PCI Oracle VA [V8 PoT Oracle VA]

Add New Task

Description: V8 PoT PCI Classification

Task Type: Report Security Assessment Entity Audit Trail Privacy Set Classification Process

Classification Process:

V8 PoT Fire only with Marker
V8 PoT PCI Classification Process

Apply

Add Audit Task

Roles

No roles have been assigned to this Process

Roles...

Delete Clone Refresh **Apply** Back

__4. Execute the new Audit Process.

__a. Click **Run Once Now**.

Compliance Automation

Audit Process Definition

Description: V8 PoT PCI Audit Process

Active: There is no schedule associated with this process

Archive Results:

Keep for a minimum of 0 days or 5 runs

CSV/CEF File Label: V8_PoT_PCI_Audit_P Zip CSV for mail

Email Subject: _____

View **Run Once Now** Modify Schedule...

Receiver Table

Receiver	Action Req.	To-Do List	Email Notif.	Cont.	Appv. if Empty
<input checked="" type="checkbox"/> mike <input checked="" type="checkbox"/> (mike audit)	<input checked="" type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input type="radio"/> No <input type="radio"/> Link <input checked="" type="radio"/> Full Results <input checked="" type="checkbox"/> PDF <input type="checkbox"/> CSV	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> peter <input checked="" type="checkbox"/> (peter pci)	<input type="radio"/> Review <input checked="" type="radio"/> Sign	<input checked="" type="checkbox"/>	<input type="radio"/> No <input type="radio"/> Link <input checked="" type="radio"/> Full Results <input checked="" type="checkbox"/> PDF <input type="checkbox"/> CSV	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add Receiver

Receiver name: _____ Search users

Action Required: Review Sign

To-Do List: Add

Email Notification: None Link Only Full Results

Continuous:

Approve if Empty: Yes

Add

Audit Tasks

- Security Assessment: V8 PoT PCI Oracle VA [V8 PoT Oracle VA]
- Classification Process: V8 PoT PCI Classification [V8 PoT PCI Classification Process]

Description: V8 PoT PCI Classification

Task Type: Report Security Assessment Entity Audit Trail Privacy Set Classification Process

Classification Process: V8 PoT PCI Classification Process

Event and Additional Columns Apply

Add Audit Task

Roles

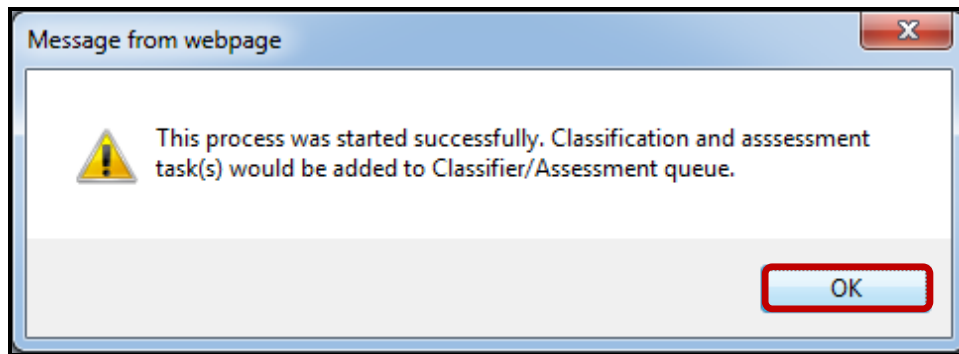
No roles have been assigned to this Process

Roles...

Delete Clone Add Comments

Refresh Apply Back

__b. Click **OK** to Acknowledge.



__c. Click **Guardium Job Queue** under the **Discover** tab to check status.

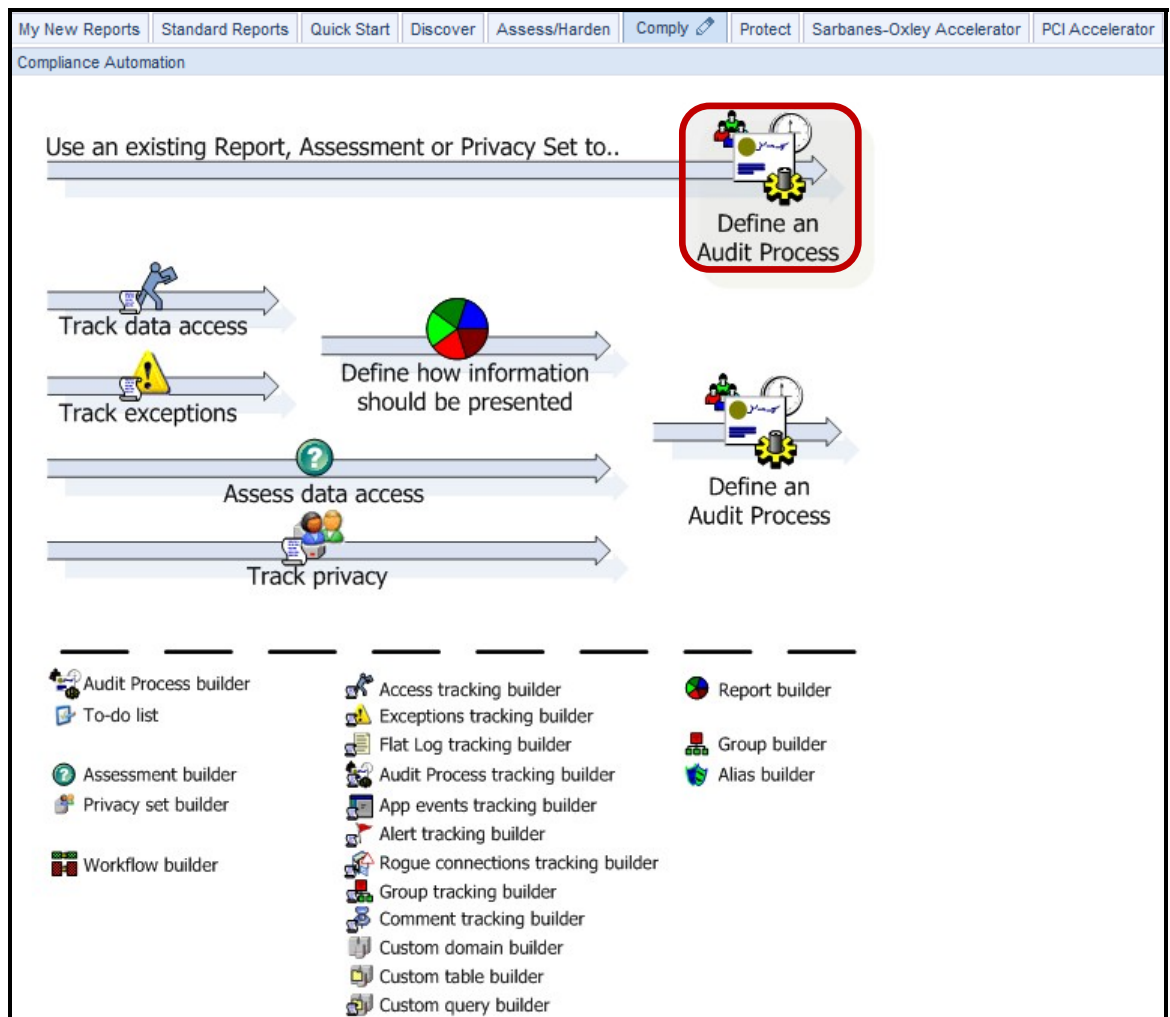
Note: The **Guardium Job Queue** will list present and previous Assessment and Classification processes.

Process Run Id	Process Type	Status	Process Id	Report Result Id	Guardium Job Description	Task Description	Queue Time	Start Time	End Time	Datasources
6	ASSESSMENT	COMPLETED	20000	4	V8 PoT Oracle VA	V8 PoT PCI Oracle VA	2012-01-14 19:34:54.0	2012-01-14 19:34:57.0	2012-01-14 19:36:28.0	ORACLE osprey_system
7	CLASSIFICATION	COMPLETED	20000	50	V8 PoT PCI Classification Process	V8 PoT PCI Classification	2012-01-14 19:34:54.0	2012-01-14 19:34:57.0	2012-01-14 19:35:27.0	ORACLE osprey_system
5	ASSESSMENT	COMPLETED	20000	3	V8 PoT Oracle VA		2012-01-14 19:23:39.0	2012-01-14 19:24:16.0	2012-01-14 19:25:30.0	ORACLE osprey_system
4	ASSESSMENT	COMPLETED	20001	2	V8 PoT DB2 VA		2012-01-14 19:20:21.0	2012-01-14 19:20:58.0	2012-01-14 19:21:23.0	DB2 osprey_db2inst2
3	ASSESSMENT	COMPLETED	20000	1	V8 PoT Oracle VA		2012-01-14 19:17:52.0	2012-01-14 19:18:16.0	2012-01-14 19:19:33.0	ORACLE osprey_system
2	CLASSIFICATION	COMPLETED	20001	2	V8 PoT Fire only with Marker		2012-01-14 17:12:52.0	2012-01-14 17:13:32.0	2012-01-14 17:14:10.0	ORACLE osprey_system
1	CLASSIFICATION	COMPLETED	20000	1	V8 PoT PCI Classification Process		2012-01-14 16:47:00.0	2012-01-14 16:47:31.0	2012-01-14 16:47:50.0	ORACLE osprey_system

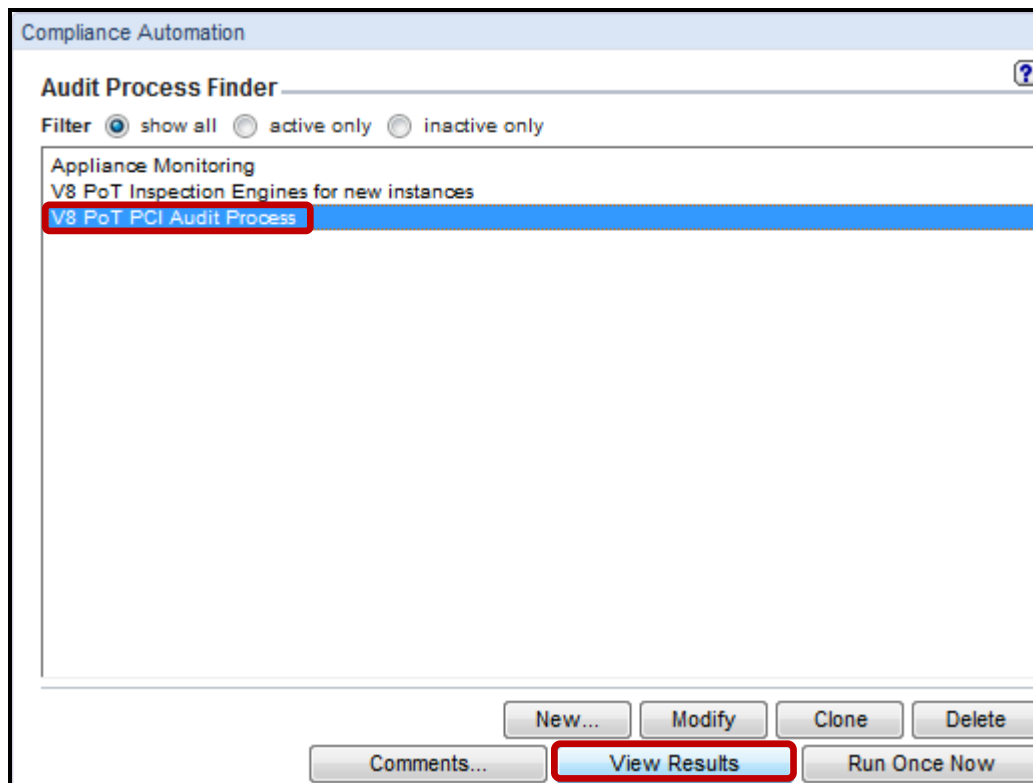
Ensure that both processes have completed before proceeding to the next step.

__5. View the results of the Audit Process

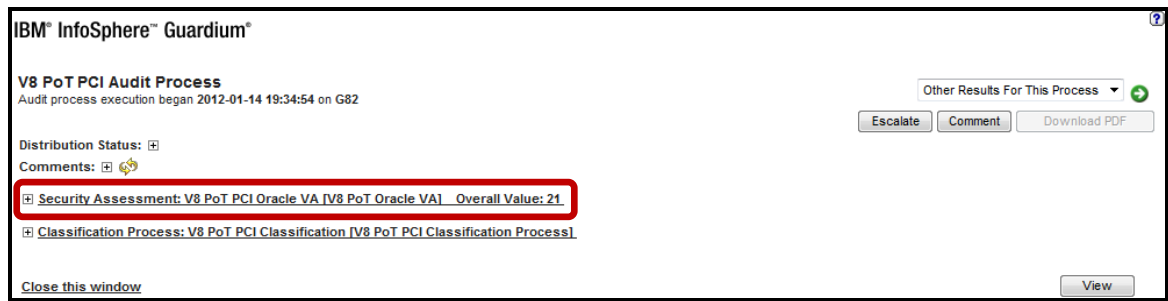
__a. Click **Define an Audit Process** under the **Comply** tab.



- __b. Select **V8 PoT PCI Audit Process** from the *Audit Process Finder* drop-down list and then click **View Results**.

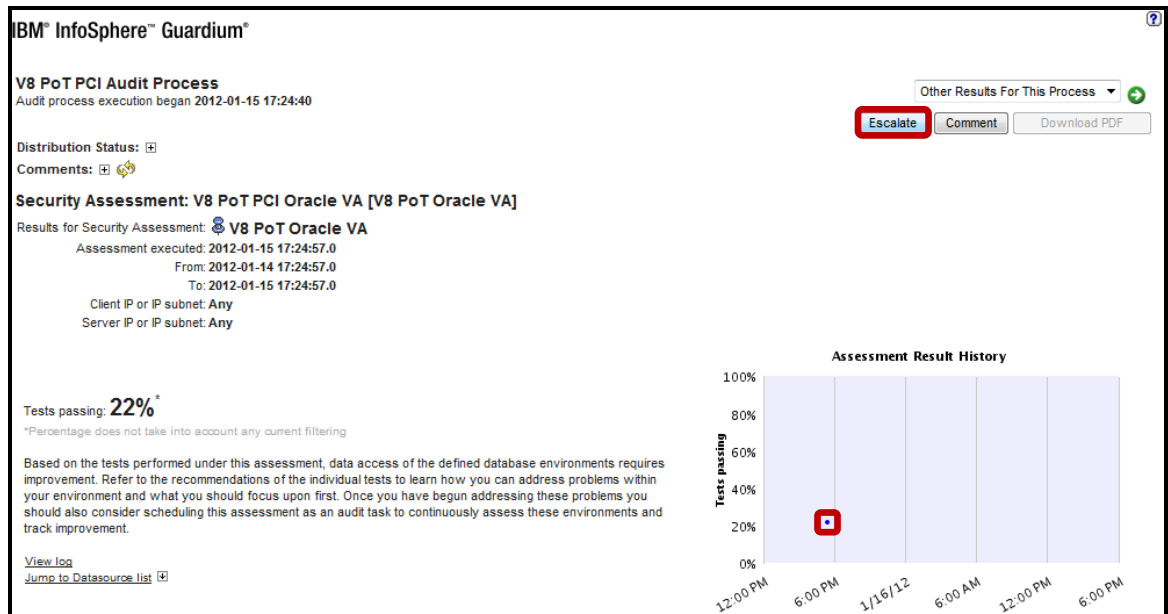


__c. Click the '+' icon to expand and view the Security Assessment report.

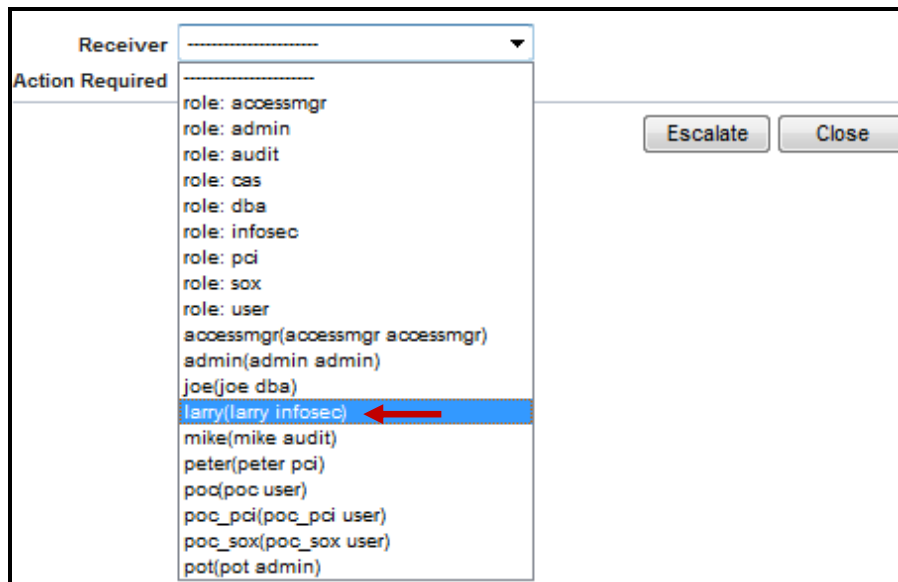


__d. Click **Escalate**.

Note: The Vulnerability Assessment results show that only 22 percent of the tests were passed. The graph shows progress over the time based on subsequent executions. Since this Audit Process is being run for the first time, we only see a dot rather than a line graph.



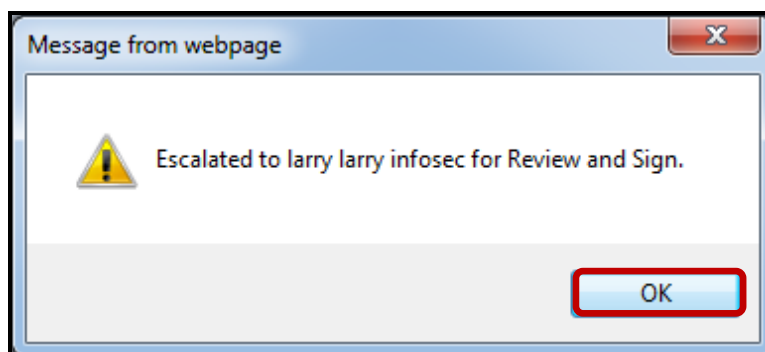
__e. Select **larry(larry infosec)** from the *Receiver* drop-down list.



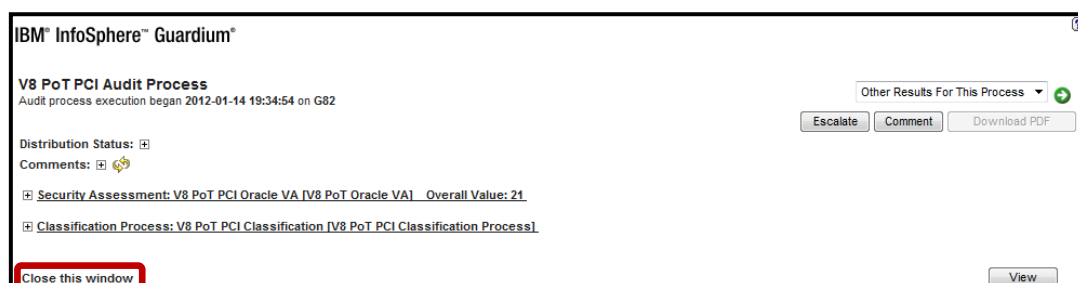
__f. Select the **Review and Sign** radio button and click **Escalate**.



__g. Click **OK** to acknowledge.

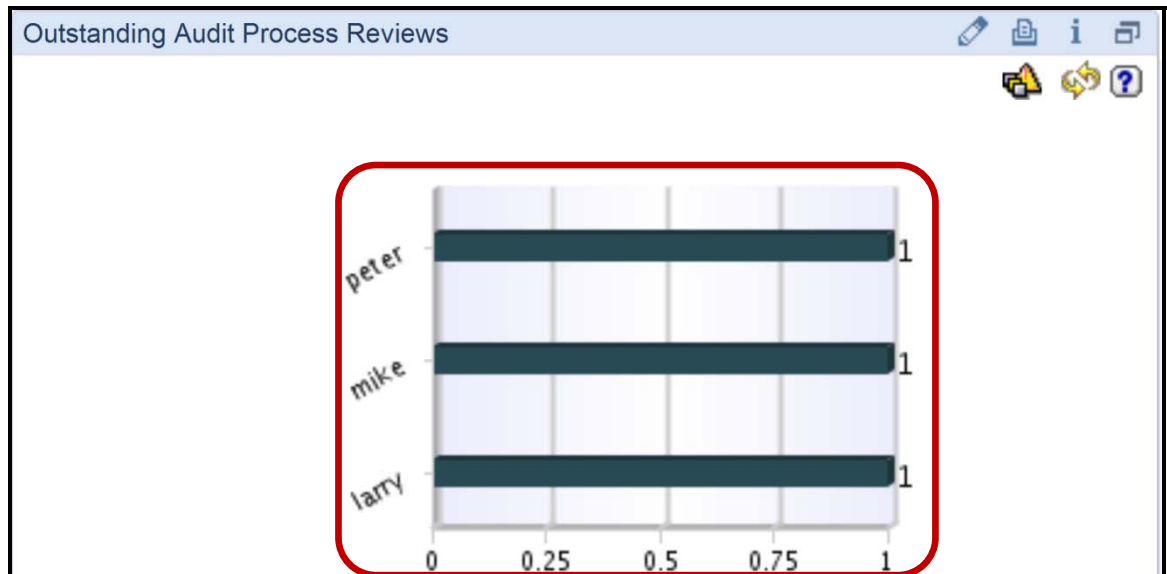


__h. Click the **Close this window** link in the lower left of the screen to close the results view.

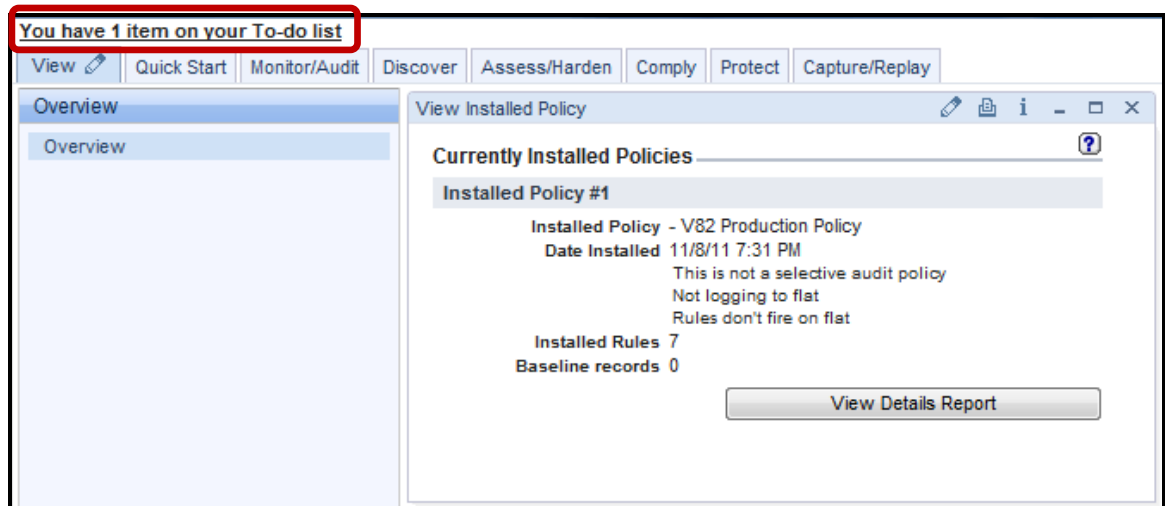


- __i. Click the **Comply** tab to view the Outstanding Audit Process Reviews, and then **Logout**.

Note: Outstanding processes for the **Audit**, **PCI Compliance**, and **Info Security** users.



- __6. Simulate the Audit Management Process.
- __a. Login to InfoSphere Guardium as **larry./guardium**.
- __b. Click the **You have 1 item on your To-do list** link at top left of the screen.



- __c. Click **View** for the **V8 PoT PCI Audit Process**.

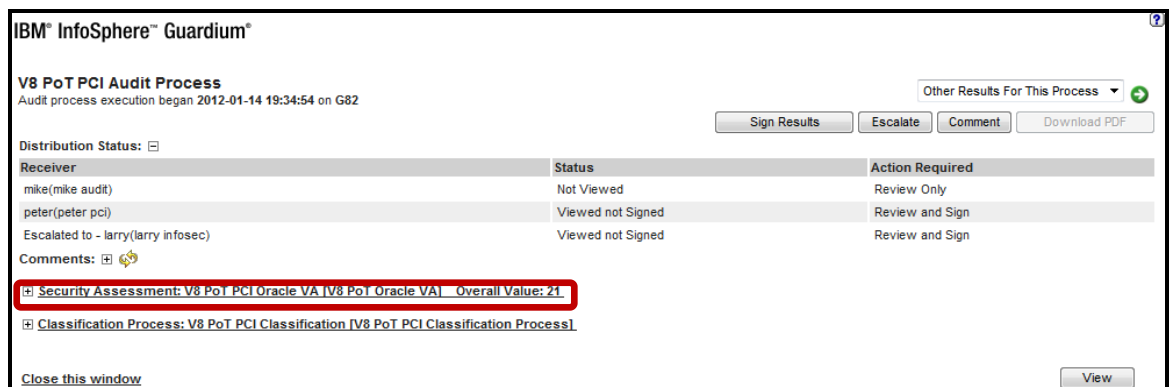
Note: **larry** currently has one pending *Review and Sign* action.



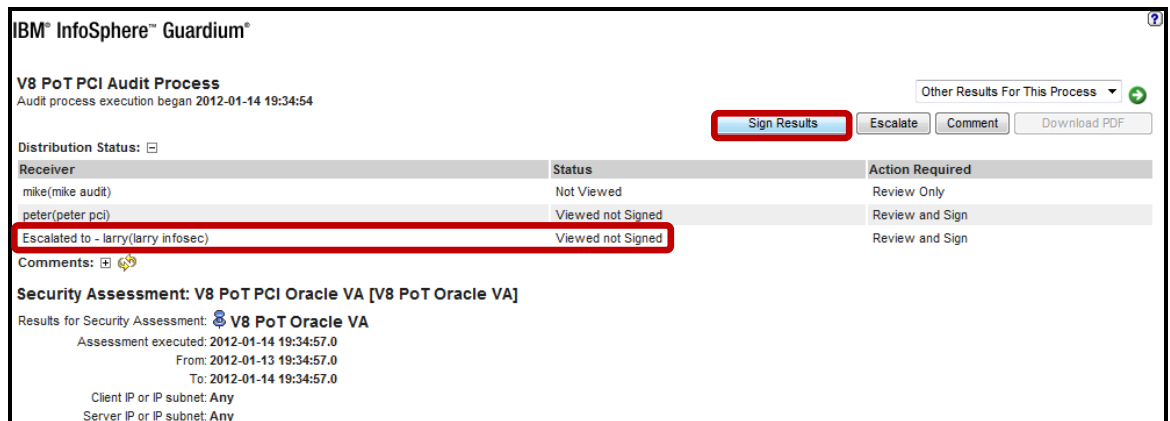
__d. Click the '+' icon to expand the **Distribution Status** details.



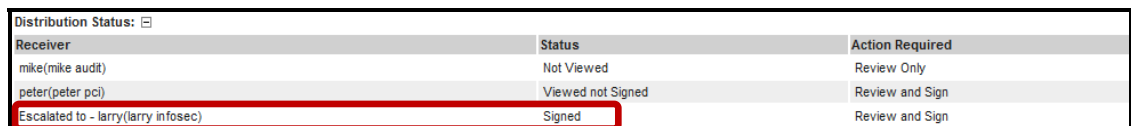
__e. Click the '+' icon to expand and view the **V8 PoT PCI Oracle VA** report.



__f. Click **Sign Results**.



Note The Status has changed from **Viewed not Signed** to **Signed** for the admin user.



__g. Click the **Close this window** link in the lower left of the screen of each of the dialogs, and then **Logout** of the InfoSphere Guardium GUI.

Thank You

Exploring Compliance Workflow Automation review

- __1. Multiple Audit processes can be created, each with its own schedule.
(**True** or **False**).
- __2. If a Compliance Workflow is sent to a role (instead of a user), and sign-off is required, then:
 - __a. Each user in that role must sign-off.
 - __b. Any one user in that role must sign-off.
 - __c. No user in the role is required to sign-off.
- __3. Compliance Workflow Automation can run not only reports, but also Vulnerability Assessments and Classifier.
(**True** or **False**).
- __4. A report can be added to a Compliance Workflow multiple times, and run with different parameters (for example, for different Server IPs)
(**True** or **False**).
- __5. InfoSphere Guardium can monitor the status of a Compliance Workflow using:
 - __a. The “Scheduled Job” report as the ‘pot’ user.
 - __b. The “Guardium Job Queue” report as the ‘admin’ user.
 - __c. None – there is no way to track these jobs.
- __6. When viewing a Compliance Workflow report, users can sign-off on the report:
 - __a. At any time.
 - __b. Not until they have at least viewed the report (or it has been delivered to them).
 - __c. Only after the approved sign-off time window.

Exploring Compliance Workflow Automation review (Answers)

__1. Multiple Audit processes can be created, each with its own schedule.
(True or False).

True.

__2. If a Compliance Workflow is sent to a role (instead of a user), and sign-off is required, then:

B – Any one user in that role must sign-off.

__3. Compliance Workflow Automation can run not only reports, but also Vulnerability Assessments and Classifier.
(True or False).

True.

__4. A report can be added to a Compliance Workflow multiple times, and run with different parameters (for example, for different Server IPs)
(True or False).

True.

__5. InfoSphere Guardium can monitor the status of a Compliance Workflow using:

B – The “Guardium Job Queue” report as the ‘admin’ user

__6. When viewing a Compliance Workflow report, users can sign-off on the report:

B – Not until they have at least viewed the report (or it has been delivered to them).

8.2 Custom Workflow Builder

Overview

The Workflow Builder is an optional component used to define customized workflows (steps, transitions and actions) to be used in the Audit Process.

Relevant Terms for this feature:

Event Type – Custom workflow.

Event Status – State/status of the workflow.

Event Action – Action/Transition.

Objectives

This Lab will illustrate how to create a Workflow Builder process by performing the following steps in the InfoSphere Guardium GUI:

- __1. Define the workflow steps (Event Status).
- __2. Define the flow of transit from one step to another (Actions).
- __3. Define which actions require sign-off.
- __4. Assign roles to each status, to define the users permitted to view each status.

- __1. Using the InfoSphere Guardium GUI, demonstrate the ease of use within the Guardium solution. Start the InfoSphere Guardium appliance and login.
 - __a. From your laptop, go to <https://10.10.9.248:8443>
 - __b. Login as **pot / guardium**.

Login

Please enter your information

User name:

Password:

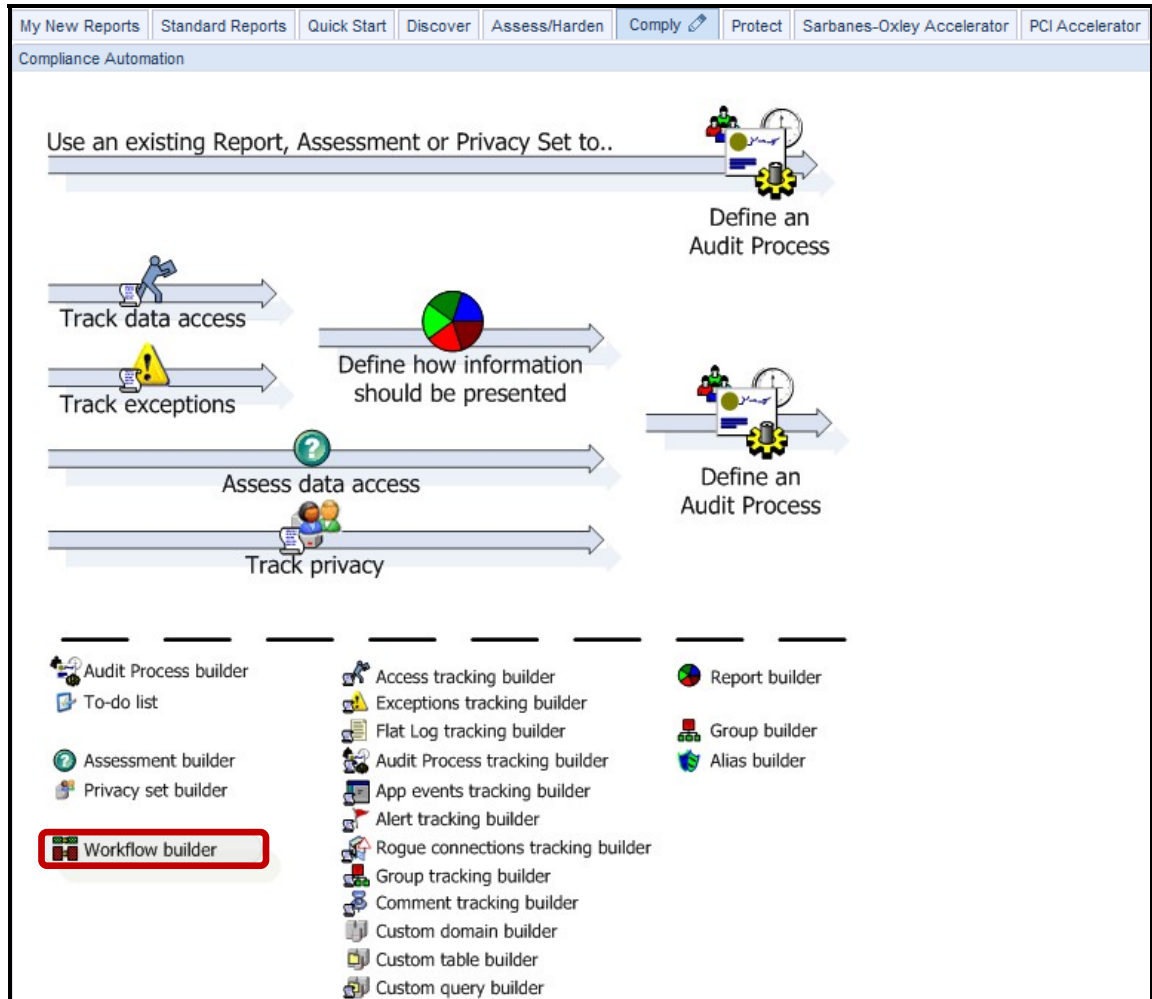
Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

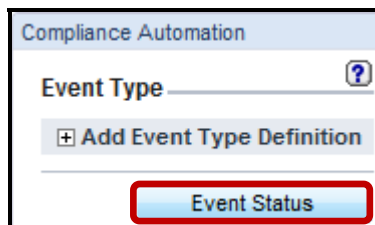
CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistrykey © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

__2. Use the InfoSphere Guardium GUI to create three *Event Statuses* (**Open**, **Under Review** and **Closed**) to support our custom workflow.

__a. Click **Workflow builder** on the bottom left of the screen under the **Comply** tab.



__b. Click **Event Status** on the *Event Type* screen to go to the Event Status configuration.



- __c. Enter 'Open' as the first workflow state in the *Status* field and click **Apply**.

The screenshot shows the 'Compliance Automation' dialog box. At the top, there is a title bar and a 'Event Status' label with a help icon. Below this is an 'Add Event Status' button. A table with two columns, 'Status' and 'Is Final', is displayed. The 'Status' column contains the text 'Open' and the 'Is Final' column contains an unchecked checkbox. To the right of the table are 'Cancel' and 'Apply' buttons. At the bottom of the dialog is an 'Event Type' button.

- __d. Enter 'Under Review' in the Status box and click **Apply**.

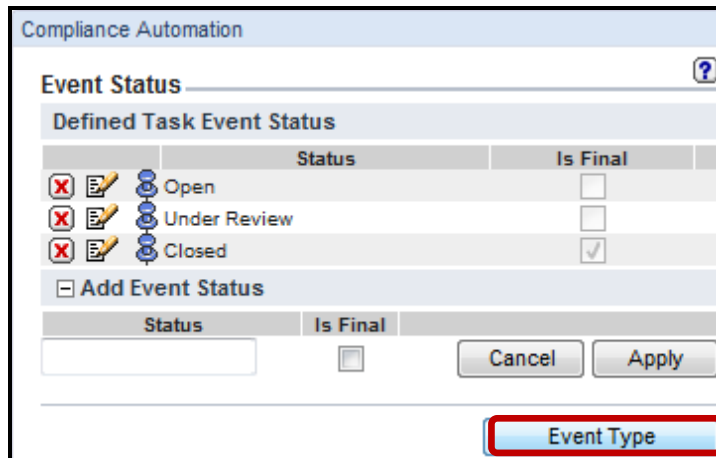
The screenshot shows the 'Compliance Automation' dialog box. It includes a 'Defined Task Event Status' section with a table. The table has two columns: 'Status' and 'Is Final'. The 'Status' column contains 'Open' and the 'Is Final' column contains an unchecked checkbox. Below this table is an 'Add Event Status' button. The main table below has 'Status' and 'Is Final' columns. The 'Status' field now contains 'Under Review' and the 'Is Final' checkbox is still unchecked. The 'Apply' button is highlighted.

- __e. Enter 'Closed' in the *Status* box, check the **Is Final** checkbox, and click **Apply**.

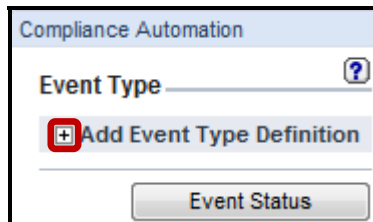
The screenshot shows the 'Compliance Automation' dialog box. The 'Defined Task Event Status' table now lists two entries: 'Open' and 'Under Review'. The main table below has 'Status' and 'Is Final' columns. The 'Status' field now contains 'Closed' and the 'Is Final' checkbox is checked. The 'Apply' button is highlighted.

__3. Create an Event Type and Populate with Allowed Workflow States.

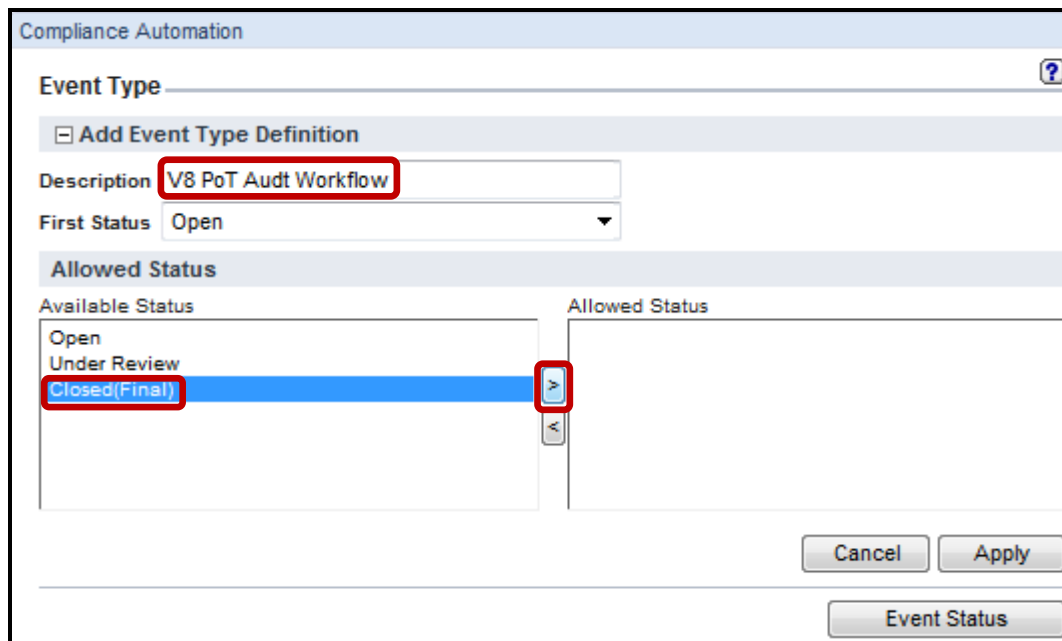
__a. Click **Event Type**.



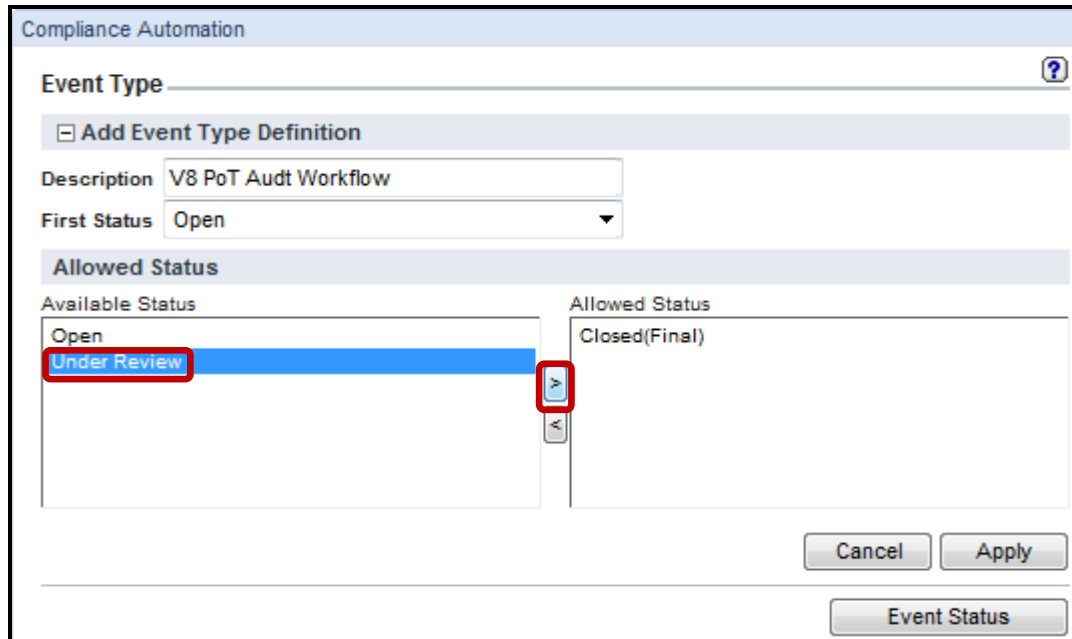
__b. Click on the '+' icon to expand the **Add Event Type Definition** drop-down list.



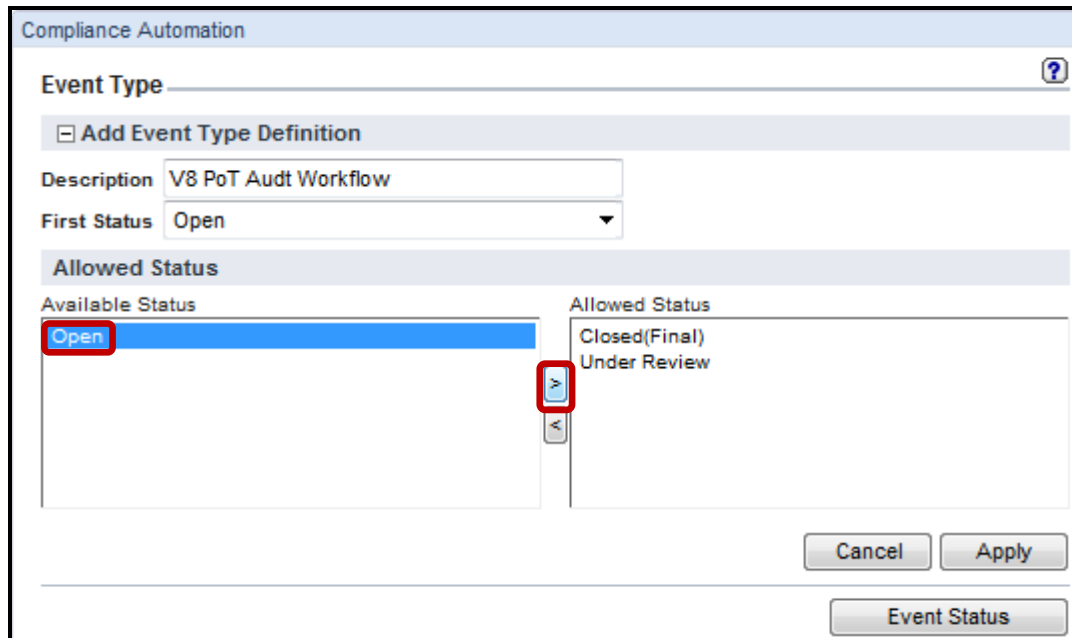
__c. Enter '**V8 PoT Audit Workflow**' for the *Description* field, select **Closed (Final)** from the *Available Status* list box, and click the '>' button to move to the *Allowed Status*.



- ___d. Select **Under Review** from the *Available Status* list box and click the “>” button to move to the *Allowed Status*.



- ___e. Select **Open** from the *Available Status* box and click the “>” button to move to the *Allowed Status*.



__f. Click **Apply**.

The screenshot shows a dialog box titled "Compliance Automation" with a sub-header "Add Event Type Definition". The "Event Type" field is empty. Below it, the "Description" is set to "V8 PoT Audt Workflow" and the "First Status" is set to "Open". A section titled "Allowed Status" contains two lists: "Available Status" (which is empty) and "Allowed Status" (which contains "Closed(Final)", "Open", and "Under Review"). At the bottom right, there are "Cancel" and "Apply" buttons, with the "Apply" button highlighted by a red rectangle. An "Event Status" button is located at the very bottom of the dialog.

__4. Define Event Actions to Details Valid State Transitions.

__a. In the *Defined Event Actions* section, click **New** to define the first event action.

The screenshot displays the 'Event Type' configuration interface in the Compliance Automation tool. At the top, the title bar reads 'Compliance Automation'. Below it, the 'Event Type' section shows a search icon and a help icon. The main area is divided into several sections:

- Existing Task Event Types:** A table with columns 'Event Type', 'First Status', and 'Allowed Status'. The first row is '*V8 PoT Audt Workflow' with 'Open' as the first status and 'Closed, Open, Under Review' as allowed statuses.
- Edit Event Type Definition V8 PoT Audt Workflow:** A sub-section with a 'Description' field containing 'V8 PoT Audt Workflow' and a 'First Status' dropdown menu set to 'Open'.
- Allowed Status:** A section with two panes: 'Available Status' (empty) and 'Allowed Status' (containing 'Closed(Final)', 'Open', and 'Under Review').
- Defined Event Actions:** A section containing a 'New...' button, which is highlighted with a red rectangle.
- Roles:** A section with three entries: 'No roles have been assigned to this event type with status Open', 'No roles have been assigned to this event type with status Under Review', and 'No roles have been assigned to this event type with status Closed'. Each entry has a 'Roles...' button next to it.

At the bottom of the window, there are 'Cancel' and 'Apply' buttons. Below the main window frame, there are two additional buttons: 'New Event Type' and 'Event Status'.

- b. Enter **'Submit for Review'** for the *Event Action Description* field and select **Open** from *Prior Status* drop-down list.

Compliance Automation

Event Type ?

Existing Task Event Types

Event Type	First Status	Allowed Status
*V8 PoT Audt Workflow	Open	Closed, Open, Under Review

Edit Event Type Definition V8 PoT Audt Workflow

Description: V8 PoT Audt Workflow

First Status: Open

Allowed Status

Available Status

Allowed Status

Closed(Final)
 Open
 Under Review

Defined Event Actions

Event Action Description	Prior Status	Next Status	Sign-off
Submit for Review	Open		<input type="checkbox"/>

Roles

No roles have been assigned to this event type with status Open Roles...

No roles have been assigned to this event type with status Under Review Roles...

No roles have been assigned to this event type with status Closed Roles...

Cancel Apply

New Event Type Event Status

__c. Select **Under Review** from the *Next Status* drop-down list, and click **Apply**.

The screenshot shows the 'Event Type' configuration interface in Compliance Automation. The main window title is 'Compliance Automation'. Below the title bar, there's a search field for 'Event Type'. The 'Existing Task Event Types' section contains a table with columns 'Event Type', 'First Status', and 'Allowed Status'. The first row is '* V8 PoT Audt Workflow' with 'Open' as the first status and 'Closed, Open, Under Review' as allowed statuses. Below this is the 'Edit Event Type Definition' section for 'V8 PoT Audt Workflow', with fields for 'Description' (V8 PoT Audt Workflow) and 'First Status' (Open). The 'Allowed Status' section shows a list of available statuses (Closed(Final), Open, Under Review) and a list of allowed statuses (Closed(Final), Open, Under Review). The 'Defined Event Actions' section has a table with columns 'Event Action Description', 'Prior Status', 'Next Status', and 'Sign-off'. The first row is 'Submit for Review' with 'Open' as the prior status and a dropdown for 'Next Status'. The 'Next Status' dropdown is open, showing 'Closed(Final)', 'Open', and 'Under Review' (highlighted with a red arrow). The 'Apply' button is highlighted with a red box. The 'Roles' section shows three rows of text: 'No roles have been assigned to this event type with status Under Review', 'No roles have been assigned to this event type with status Under Review', and 'No roles have been assigned to this event type with status Closed'. There are 'Roles...' buttons next to each row. At the bottom, there are 'New Event Type' and 'Event Status' buttons.

__d. Click **New** to define the next *Event Action*.

Compliance Automation

Event Type ?

Existing Task Event Types

Event Type	First Status	Allowed Status
* V8 PoT Audt Workflow	Open	Closed, Open, Under Review

Edit Event Type Definition V8 PoT Audt Workflow

Description: V8 PoT Audt Workflow

First Status: Open

Allowed Status

Available Status:

Allowed Status: Closed(Final), Open, Under Review

Defined Event Actions

Event Action Description	Prior Status	Next Status	Sign-off
Submit for Review	Open	Under Review	<input type="checkbox"/>

New...

Roles

No roles have been assigned to this event type with status **Open** Roles...

No roles have been assigned to this event type with status **Under Review** Roles...

No roles have been assigned to this event type with status **Closed** Roles...

Cancel Apply

New Event Type Event Status

- e. Enter **'Reject'** for the *Event Action Description* field and select **Under Review** from *Prior Status* drop-down list.

Compliance Automation

Event Type ?

Existing Task Event Types

Event Type	First Status	Allowed Status
* V8 PoT Audt Workflow	Open	Closed, Open, Under Review

Edit Event Type Definition V8 PoT Audt Workflow

Description: V8 PoT Audt Workflow

First Status: Open

Allowed Status

Available Status:

Allowed Status: Closed(Final), Open, Under Review

Defined Event Actions

Event Action Description	Prior Status	Next Status	Sign-off
Submit for Review	Open	Under Review	<input type="checkbox"/>
Reject	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Roles

No roles have been assigned to this event type with status **Open** Roles...

No roles have been assigned to this event type with status **Under Review** Roles...

No roles have been assigned to this event type with status **Closed** Roles...

Cancel Apply

New Event Type Event Status

__f. Select **Open** from the *Next Status* drop-down list, and click **Apply**.

Compliance Automation

Event Type ?

Existing Task Event Types

Event Type	First Status	Allowed Status
* V8 PoT Audt Workflow	Open	Closed, Open, Under Review

Edit Event Type Definition V8 PoT Audt Workflow

Description: V8 PoT Audt Workflow

First Status: Open

Allowed Status

Available Status:

Allowed Status: Closed(Final), Open, Under Review

Defined Event Actions

Event Action Description	Prior Status	Next Status	Sign-off
Submit for Review	Open	Under Review	<input type="checkbox"/>
Reject	Under Review	<input type="text"/>	<input type="checkbox"/>

Cancel **Apply**

Roles

No roles have been assigned to this event type with status **Open** ←

No roles have been assigned to this event type with status Under Review

No roles have been assigned to this event type with status Closed

Roles... Roles... Roles...

Cancel Apply

New Event Type Event Status

__g. Click **New** to define the final *Event Action*.

Compliance Automation

Event Type ?

Existing Task Event Types

Event Type	First Status	Allowed Status
* V8 PoT Audt Workflow	Open	Closed, Open, Under Review

Edit Event Type Definition V8 PoT Audt Workflow

Description: V8 PoT Audt Workflow

First Status: Open

Allowed Status

Available Status:

Allowed Status: Closed(Final), Open, Under Review

Defined Event Actions

Event Action Description	Prior Status	Next Status	Sign-off
Submit for Review	Open	Under Review	<input type="checkbox"/>
Reject	Under Review	Open	<input type="checkbox"/>

New...

Roles

No roles have been assigned to this event type with status **Open** Roles...

No roles have been assigned to this event type with status **Under Review** Roles...

No roles have been assigned to this event type with status **Closed** Roles...

Cancel Apply

New Event Type Event Status

- h. Enter 'Approve' for the *Event Action Description* field and select **Under Review** from the *Prior Status* drop-down list.

Compliance Automation

Event Type ?

Existing Task Event Types

Event Type	First Status	Allowed Status
* V8 PoT Audt Workflow	Open	Closed, Open, Under Review

Edit Event Type Definition V8 PoT Audt Workflow

Description: V8 PoT Audt Workflow

First Status: Open

Allowed Status

Available Status:

Allowed Status: Closed(Final), Open, Under Review

Defined Event Actions

Event Action Description	Prior Status	Next Status	Sign-off
Submit for Review	Open	Under Review	<input type="checkbox"/>
Reject	Under Review	Open	<input type="checkbox"/>
Approve	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Roles

No roles have been assigned to this event type with status Open Roles...

No roles have been assigned to this event type with status Under Review Roles...

No roles have been assigned to this event type with status Closed Roles...

Cancel Apply

New Event Type Event Status

- i. Select **Closed (Final)** from the *Next Status* drop-down list, and click **Apply**.

Compliance Automation

Event Type ?

Existing Task Event Types

Event Type	First Status	Allowed Status
* V8 PoT Audt Workflow	Open	Closed, Open, Under Review

Edit Event Type Definition V8 PoT Audt Workflow

Description: V8 PoT Audt Workflow

First Status: Open

Allowed Status

Available Status:

Allowed Status: Closed(Final), Open, Under Review

Defined Event Actions

Event Action Description	Prior Status	Next Status	Sign-off
Submit for Review	Open	Under Review	<input type="checkbox"/>
Reject	Under Review	Open	<input type="checkbox"/>
Approve	Under Review	<input type="text"/>	<input type="checkbox"/>

Roles

No roles have been assigned to this event type with status Open

No roles have been assigned to this event type with status Under Review

No roles have been assigned to this event type with status Closed

Buttons: Cancel, Apply, Roles..., Roles..., Roles..., Cancel, Apply, New Event Type, Event Status

- __5. Assign roles to each event type.
 - __a. Click the first **Roles** button to assign roles for the *Open* status.

Compliance Automation

Event Type ?

Existing Task Event Types

Event Type	First Status	Allowed Status
* V8 PoT Audt Workflow	Open	Closed, Open, Under Review

Edit Event Type Definition V8 PoT Audt Workflow

Description: V8 PoT Audt Workflow

First Status: Open

Allowed Status

Available Status:

Allowed Status: Closed(Final), Open, Under Review

Defined Event Actions

Event Action Description	Prior Status	Next Status	Sign-off
Submit for Review	Open	Under Review	<input type="checkbox"/>
Reject	Under Review	Open	<input type="checkbox"/>
Approve	Under Review	Closed	<input type="checkbox"/>

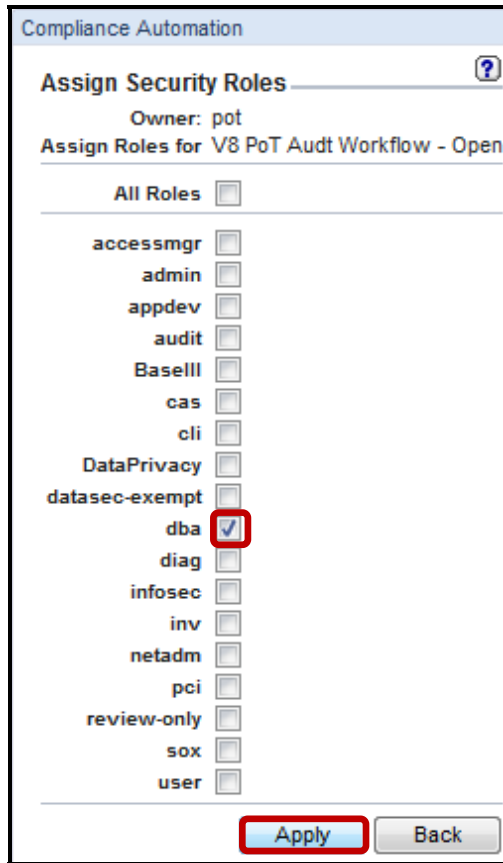
Roles

No roles have been assigned to this event type with status **Open**

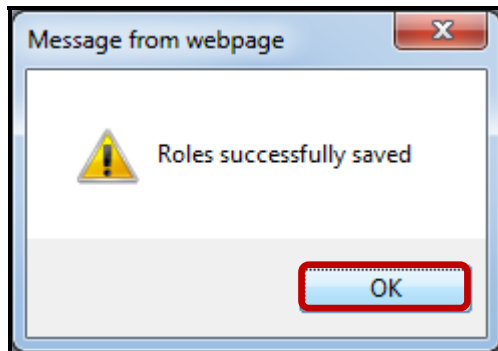
No roles have been assigned to this event type with status **Under Review**

No roles have been assigned to this event type with status **Closed**

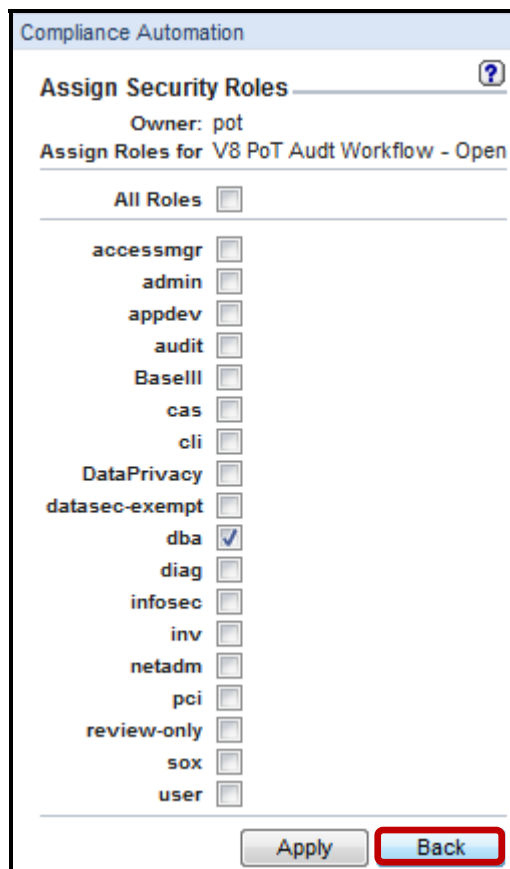
- __b. Check the **dba** checkbox to assign the 'dba' role to the *Open* status, and click **Apply**.



- __c. Click **OK** to acknowledge.



- __d. Click **Back** to return and assign the next role.



Compliance Automation

Assign Security Roles ?

Owner: pot

Assign Roles for V8 PoT Audt Workflow - Open

All Roles

accessmgr

admin

appdev

audit

Baselll

cas

cli

DataPrivacy

datasec-exempt

dba

diag

infosec

inv

netadm

pci

review-only

sox

user

- __e. Now click the middle **Roles** checkbox to assign a role for the *Under Review* status.

Compliance Automation

Event Type ?

Existing Task Event Types

Event Type	First Status	Allowed Status
* V8 PoT Audt Workflow	Open	Closed, Open, Under Review

Edit Event Type Definition V8 PoT Audt Workflow

Description: V8 PoT Audt Workflow

First Status: Open

Allowed Status

Available Status:

Allowed Status: Closed(Final), Open, Under Review

Defined Event Actions

Event Action Description	Prior Status	Next Status	Sign-off
Submit for Review	Open	Under Review	<input type="checkbox"/>
Reject	Under Review	Open	<input type="checkbox"/>
Approve	Under Review	Closed	<input type="checkbox"/>

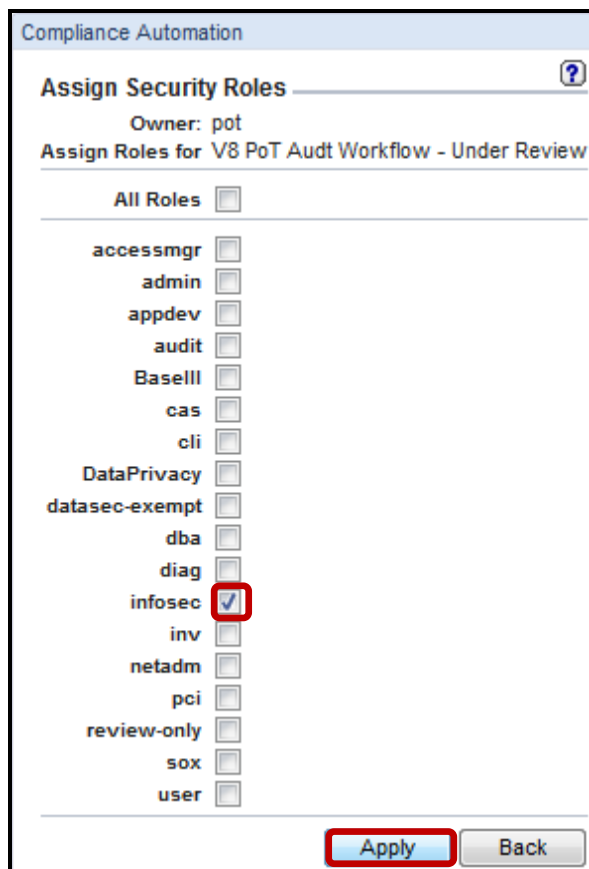
Roles

Roles have been assigned to this event type with status **Open**

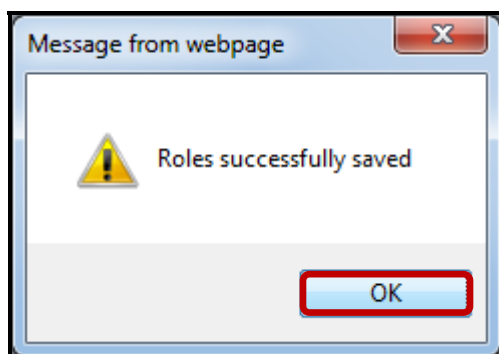
No roles have been assigned to this event type with status **Under Review**

No roles have been assigned to this event type with status **Closed**

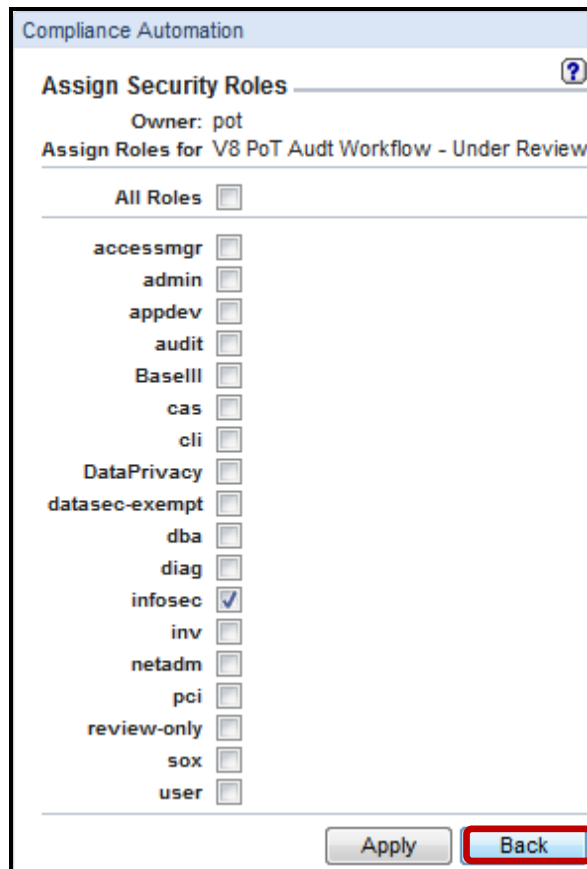
- ___f. Check the **infosec** checkbox to assign the *infosec* role to the 'Under Review' status, and click **Apply**.



- ___g. Click **OK** to acknowledge.



__h. Click **Back** to return and assign the next role.



- __i. Click the lower **Roles** checkbox to assign role to the 'Closed' status.

Compliance Automation

Event Type ?

Existing Task Event Types

Event Type	First Status	Allowed Status
* V8 PoT Audt Workflow	Open	Closed, Open, Under Review

Edit Event Type Definition V8 PoT Audt Workflow

Description: V8 PoT Audt Workflow

First Status: Open

Allowed Status

Available Status:

Allowed Status: Closed(Final), Open, Under Review

Defined Event Actions

Event Action Description	Prior Status	Next Status	Sign-off
Submit for Review	Open	Under Review	<input type="checkbox"/>
Reject	Under Review	Open	<input type="checkbox"/>
Approve	Under Review	Closed	<input type="checkbox"/>

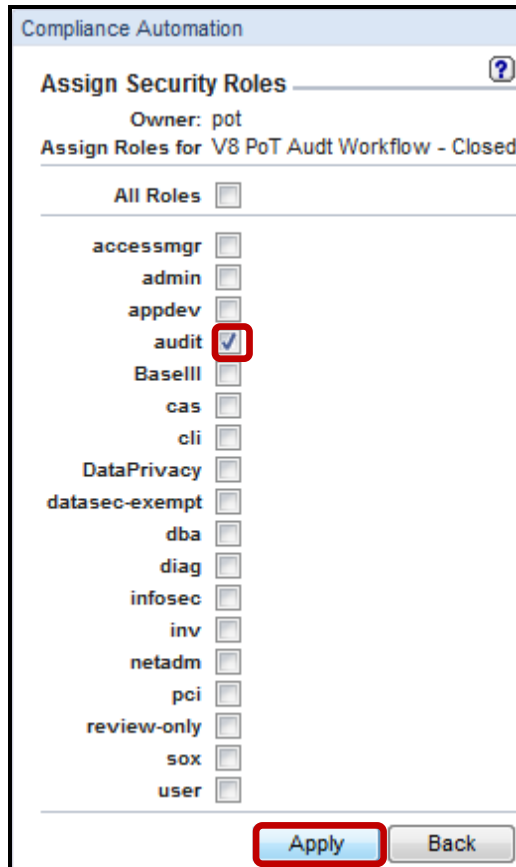
Roles

Roles have been assigned to this event type with status **Open**

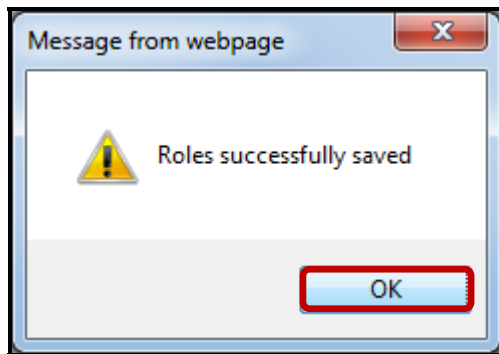
Roles have been assigned to this event type with status **Under Review**

No roles have been assigned to this event type with status **Closed**

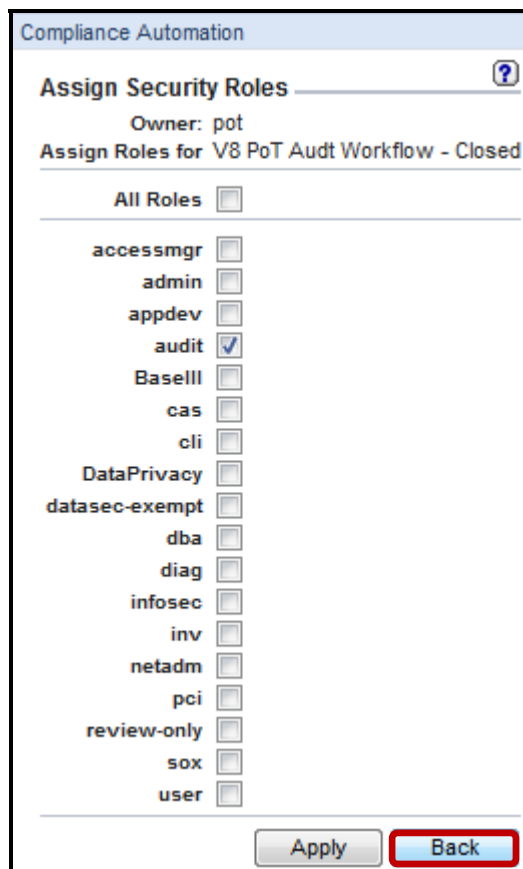
- __j. Check the **audit** checkbox to assign the *audit* role to the *Closed* status, and click **Apply**.



- __k. Click **OK** to acknowledge.



__I. Click **Back** to return.



Compliance Automation

Assign Security Roles ?

Owner: pot

Assign Roles for V8 PoT Audt Workflow - Closed

All Roles

accessmgr

admin

appdev

audit

Baselll

cas

cli

DataPrivacy

datasec-exempt

dba

diag

infosec

inv

netadm

pci

review-only

sox

user

This completes this section of the lab. Continue to the next section to learn how to implement the Audit Workflow that we have just created.

Thank You

Custom Workflow Builder review

- __1. The report “Number of Active Audit Processes” will only show Compliance Workflow processes that have not been set to a status marked as:
 - __a. Is Final
 - __b. Is Complete
 - __c. Is Done
 - __d. Is Finished

- __2. The Workflow Builder:
 - __a. Allows roles to be defined and assigned to statuses.
 - __b. Allows statuses to be defined and assigned to roles.
 - __c. Allows roles and statuses to be defined.

- __3. Multiple roles can be assigned to a status
(**True** or **False**)

- __4. The Workflow Builder is part of the Optional Advanced Compliance Workflow component.
(**True** or **False**)

Custom Workflow Builder review (Answers)

__1. The report “Number of Active Audit Processes” will only show Compliance Workflow processes that have not been set to a status marked as:

A – Is Final.

__2. The Workflow Builder:

B – Allows statuses to be defined and assigned to roles.

__3. Multiple roles can be assigned to a status
(**True** or **False**)

True.

__4. The Workflow Builder is part of the Optional Advanced Compliance Workflow component.
(**True** or **False**)

True.

8.3 Advanced Compliance Workflow (Optional)

Overview

The InfoSphere Guardium Advanced Compliance Workflow Automation module automates the entire security and compliance workflow process, eliminating manual tasks and ensuring timely completion of oversight activities. An easy-to-use graphical user interface allows a wide variety of processes to be created to match the unique needs of the tasks and individuals involved. New processes can be created with a few simple steps:

1. Create a custom workflow composed of individual event states and actions.
2. Assign one or more individuals or roles to actions to be performed. Actions can optionally require electronic sign-off. Parallel actions are allowed, supporting processes where actions are segmented by various criteria (for instance, the review of exceptions generated by different database management systems (DBMSs) may be signed off by different parties).
3. Create and schedule an audit process to execute the workflow automatically on a regular basis.
4. Add any combination of tasks to each audit process. For example, several reports that are to be executed and reviewed on a weekly basis using the same workflow can be assigned to the same audit task. A wide variety of audit tasks are supported, including reviewing the results of automatically generated vulnerability assessments, asset discovery, data classification, configuration auditing and database-activity monitoring reports.

The InfoSphere Guardium Advanced Compliance Workflow Automation module enables users to easily create workflows that are customized to each of their own unique processes by specifying the appropriate combination of actions, event states and roles through a simple graphical user interface.

Objectives

This Lab will illustrate how we can create an Advanced Workflow application incorporating the features of the Custom Workflow Process created in the previous lab. The following objectives will be featured:

- __1. Creating users for the lab exercise.
- __2. Create an advanced workflow process with notification recipients.
- __3. Bundle a set of reports.
- __4. Incorporate a Custom Workflow process.
- __5. Schedule and run the advanced workflow process.
- __6. Verify the distribution process.

- __1. Start the InfoSphere Guardium appliance and login.
 - __a. From your laptop, go to <https://10.10.9.248:8443>
 - __b. Login as **pot / guardium**.

Login

Please enter your information

User name:

Password:

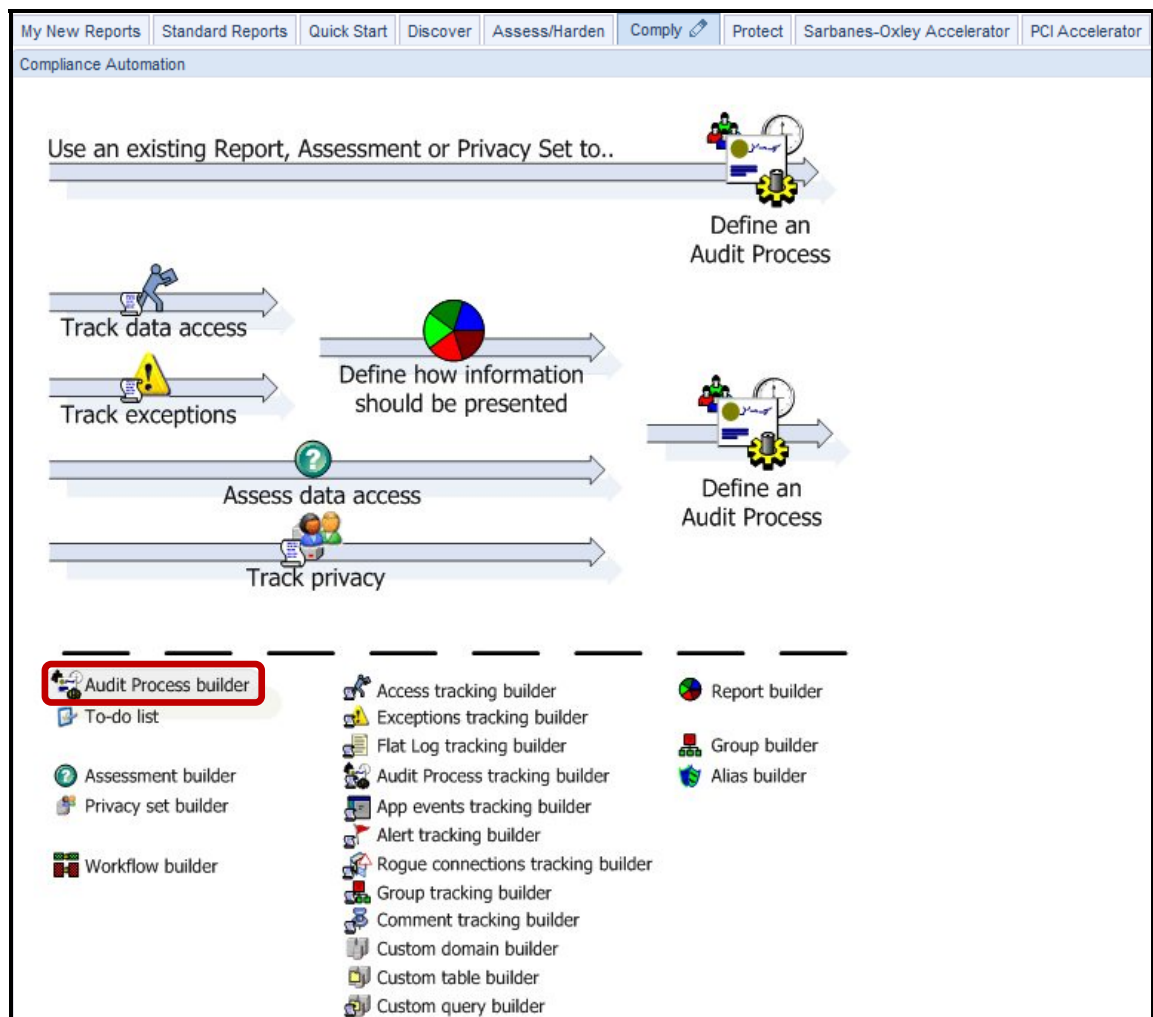
Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

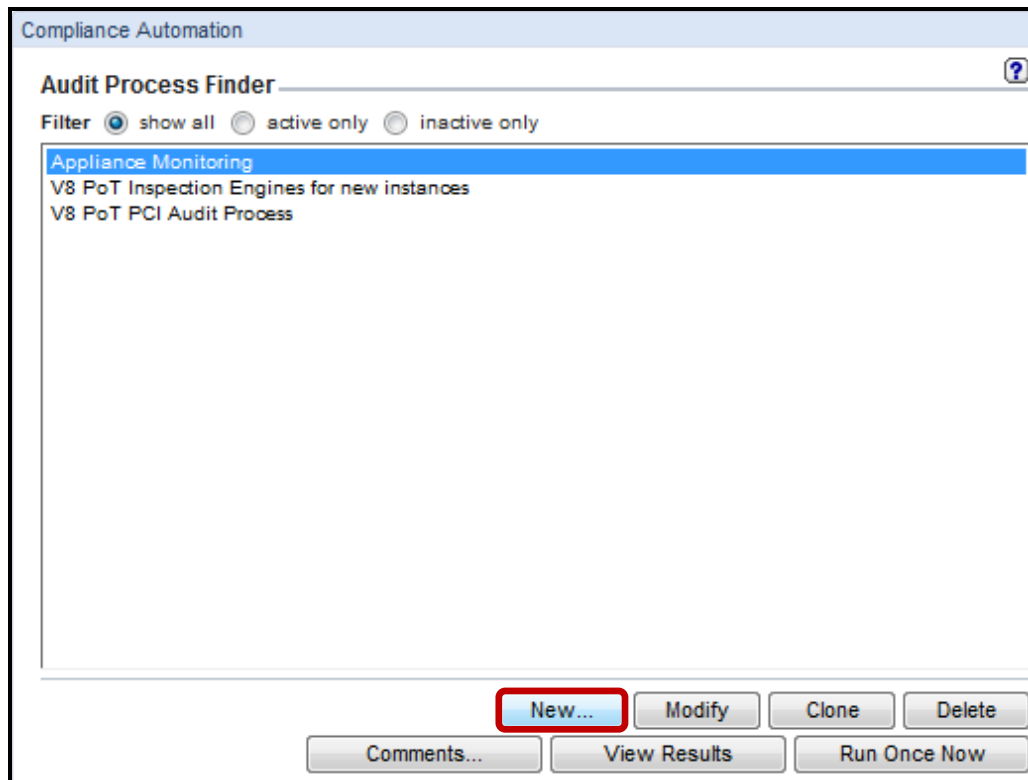
CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistry/key © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com, Zthread © Copyright 2000-2003, Eric Crahen.

__2. Use the InfoSphere Guardium GUI to create a new Custom Workflow.

__a. Click **Audit Process builder** under the **Comply** tab.



__b. Click **New**.



- c. Enter 'V8 PoT Audit Workflow Process' for *Description*, select **role: dba** from the *Receiver name* drop-down list, and then click **Add** to add the first receiver.

Compliance Automation

Audit Process Definition

Description:

Active: There is no schedule associated with this process

Archive Results:

Keep for a minimum of days or runs

CSV/CEF File Label: Zip CSV for mail

Email Subject:

Receiver	Action Req.	To-Do List	Email Notif.	Cont.	Appv. if Empty
Add Receiver					
Receiver name	<input type="text"/> Search users				
Action Required	<input type="text"/>				
To-Do List	email:				
Email Notification	role: accessmgr				
	role: admin				
Continuous	role: audit				
Approve if Empty	role: cas				
	role: dba				
	role: infosec				
	role: pci				
	role: sox				
	role: user				
Audit Tasks	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>				
	accessmgr(accessmgr accessmgr)				
	admin(admin admin)				
	joe(joe dba)				
	larry(larry infosec)				
	mike(mike audit)				
	peter(peter pci)				
	poc(poc user)				
	poc_pci(poc_pci user)				
	poc_sox(poc_sox user)				
	pot(pot admin)				
Roles	No roles have been assigned to this Process				
	<input style="float: right;" type="button" value="Roles..."/>				
	<input type="button" value="Add"/>				
	<input type="button" value="Apply"/>				
	<input type="button" value="Add Audit Task"/>				
	<input type="button" value="Delete"/> <input type="button" value="Clone"/>				
	<input type="button" value="Refresh"/> <input type="button" value="Apply"/> <input type="button" value="Back"/>				

- d. Select **role: infosec** from *Receiver name* drop-down list, and click **Add** to add the second receiver.

Compliance Automation

Audit Process Definition ?

Description: V8 PoT Audit Workflow Process

Active: There is no schedule associated with this process

Archive Results:

Keep for a minimum of 0 days or 5 runs

CSV/CEF File Label: V8_PoT_Audit_Workfl Zip CSV for mail

Email Subject:

View Run Once Now Modify Schedule...

Receiver	Action Req.	To-Do List	Email Notif.	Cont.	Appv. if Empty
<input checked="" type="checkbox"/> role: dba	<input checked="" type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> No <input type="radio"/> Link <input type="radio"/> Full Results	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add Receiver

Receiver name: Search users

Action Required:

To-Do List: email:

Email Notification: role: accessmgr

Continuous: role: admin

Approve if Empty: role: audit

role: cas

role: infosec ←

role: pci

role: sox

role: user

accessmgr(accessmgr accessmgr)

admin(admin admin)

joe(joe dba)

larry(larry infosec)

mike(mike audit)

peter(peter pci)

poc(poc user)

poc_pci(poc_pci user)

poc_sox(poc_sox user)

pot(pot admin)

Add

Audit Tasks

assessment Entity Audit Trail Privacy Set Classification Process

Apply

Add Audit Task

Roles

No roles have been assigned to this Process

Roles...

Delete Clone Refresh Apply Back

- e. Select **role: audit** from *Receiver name* drop-down list, and click **Add** to add the third and final receiver.

Compliance Automation

Audit Process Definition

Description: V8 PoT Audit Workflow Process

Active: There is no schedule associated with this process

Archive Results:

Keep for a minimum of 0 days or 5 runs

CSV/CEF File Label: V8_PoT_Audit_Workfl Zip CSV for mail

Email Subject:

View Run Once Now Modify Schedule...

Receiver	Action Req.	To-Do List	Email Notif.	Cont.	Appv. if Empty
<input checked="" type="checkbox"/> role: dba	<input checked="" type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> No <input type="radio"/> Link <input type="radio"/> Full Results	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> role: infosec	<input checked="" type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> No <input type="radio"/> Link <input type="radio"/> Full Results	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add Receiver

Receiver name: Search users

Action Required:

To-Do List:

Email Notification:

Continuous:

Approve if Empty:

role: audit ←

role: cas
role: pci
role: sox
role: user

Audit Tasks

- accessmgr(accessmgr accessmgr)
- admin(admin admin)
- joe(joe dba)
- D larry(larry infosec)
- mike(mike audit)
- peter(peter pci)
- poc(poc user)
- poc_pci(poc_pci user)
- poc_sox(poc_sox user)
- pot(pot admin)

assessment Entity Audit Trail Privacy Set Classification Process

Apply

Add Audit Task

Roles

No roles have been assigned to this Process

Roles...

Delete Clone

Refresh Apply Back

__f. Select the **Report** radio button in the *Add New Task* box.

Compliance Automation

Audit Process Definition

Description: V8 PoT Audit Workflow Process

Active: There is no schedule associated with this process

Archive Results:

Keep for a minimum of 0 days or 5 runs

CSV/CEF File Label: V8_PoT_Audit_Workfl Zip CSV for mail

Email Subject:

View Run Once Now Modify Schedule...

Receiver Table

Receiver	Action Req.	To-Do List	Email Notif.	Cont.	Appv. if Empty
<input checked="" type="checkbox"/> role: dba	<input checked="" type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> No <input type="radio"/> Link <input type="radio"/> Full Results	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> role: infosec	<input checked="" type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> No <input type="radio"/> Link <input type="radio"/> Full Results	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> role: audit	<input checked="" type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> No <input type="radio"/> Link <input type="radio"/> Full Results	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add Receiver

Receiver name: Search users

Action Required: Review Sign

To-Do List: Add

Email Notification: None Link Only Full Results

Continuous:

Approve if Empty: Yes

Add

Audit Tasks

Add New Task

Description:

Task Type: Report Security Assessment Entity Audit Trail Privacy Set Classification Process

Apply

Add Audit Task

Roles

No roles have been assigned to this Process

Roles...

Delete Clone

Refresh Apply Back

- g. Enter 'V8 PoT Audit Failed Logins' for the Audit Tasks *Description* field, and Select **Failed User Login Attempts** from the *Report* drop-down list.

The screenshot displays the 'Compliance Automation' interface. The top section is 'Audit Process Definition' with the following details:

- Description: V8 PoT Audit Workflow Process
- Active: There is no schedule associated with this process
- Archive Results:
- Keep for a minimum of: 0 days or 5 runs
- CSV/CEF File Label: V8_PoT_Audit_Workfl. Zip CSV for mail
- Email Subject: [Empty field]

Buttons: View, Run Once Now, Modify Schedule...

The 'Receiver Table' section contains the following data:

Receiver	Action Req.	To-Do List	Email Notif.	Cont.	Appv. if Empty
<input checked="" type="checkbox"/> role: dba	<input checked="" type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> No <input type="radio"/> Link <input type="radio"/> Full Results	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> role: infosec	<input checked="" type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> No <input type="radio"/> Link <input type="radio"/> Full Results	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> role: audit	<input checked="" type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> No <input type="radio"/> Link <input type="radio"/> Full Results	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The 'Add Receiver' section includes:

- Receiver name: [Dropdown]
- Action Required: Review Sign
- To-Do List: Add
- Email Notification: None Link Only Full Results
- Continuous:
- Approve if Empty: Yes

The 'Audit Tasks' section is expanded to show the 'Add New Task' form:

- Description: **V8 PoT Audit Failed Logins** (highlighted with a red box)
- Task Type: Report Security Assessment Entity Audit Trail Privacy Set Classification Process
- Report dropdown menu is open, showing a list of report types. 'Failed User Login Attempts' is highlighted with a blue bar and a red arrow.

Other visible elements include 'Roles' (No roles have been assigned to this Proc...) and a 'Compress PDF Content' checkbox.

- __h. Enter 'NOW -12 MONTH' in the *Enter Period From* input field, enter 'NOW' in the *Enter Period To* input field, and then click **Apply**.

Audit Tasks

Report: V8 PoT Audit Failed Logins [Failed User Login Attempts]

Description V8 PoT Audit Failed Logins

Task Type Report Security Assessment Entity Audit Trail Privacy Set Classification Process

Report

Report Failed User Login Attempts

CSV/CEF File Label V8_PoT_Audit_Failed_Logins

Export CSV file

Export CEF file

Export PDF file

Write to Syslog

Compress

PDF Content Report Diff Report and Diff

Task Parameters

* On aggregators, only reports not exceeding the maximum merge period will be executed.

Enter Period From NOW -12 MONTH

Enter Period To NOW

Show Aliases On Off Default

Remote Data Source -- none --

Apply

Add Audit Task

- __i. Scroll down and click **Apply** in the lower right portion of the screen.

Roles

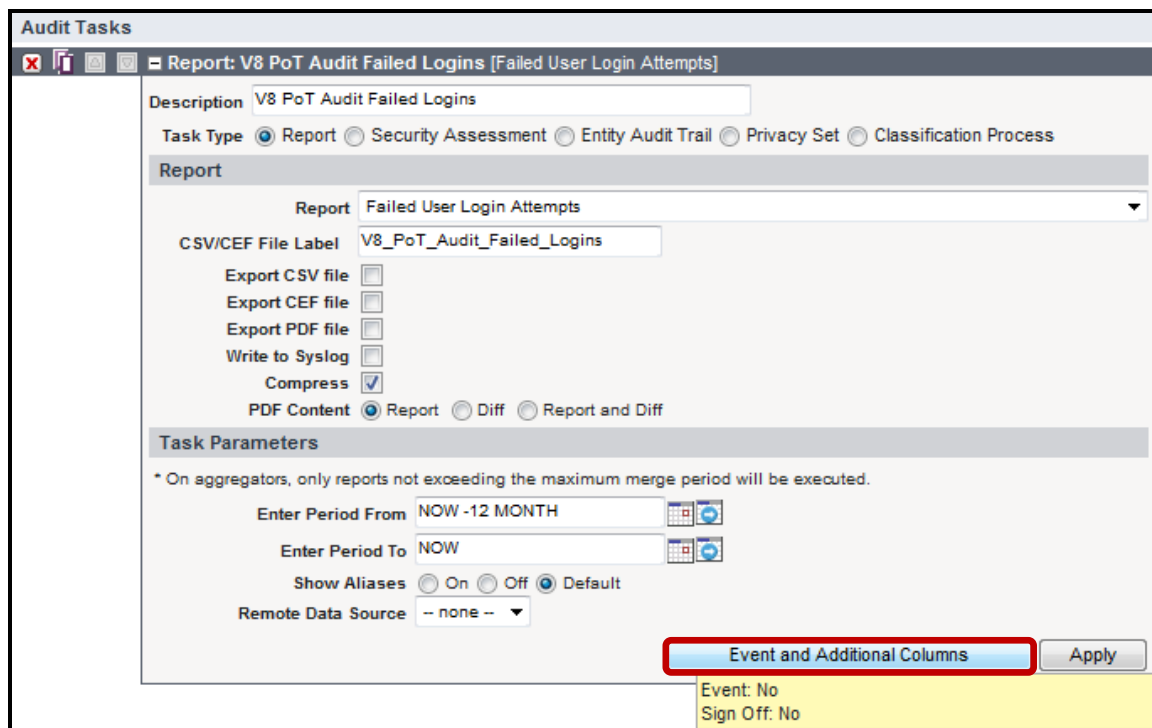
No roles have been assigned to this Process

Roles...

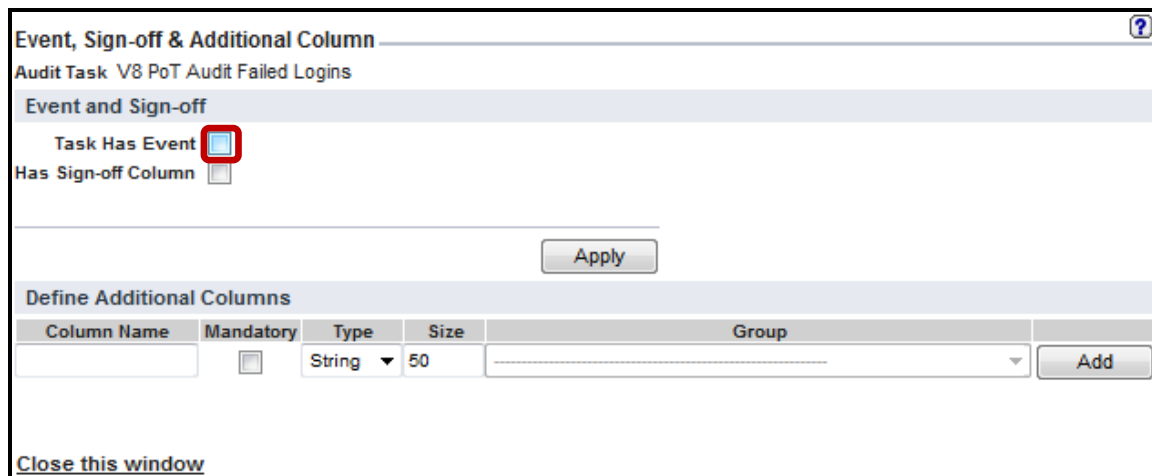
Delete Clone

Refresh Apply Back

__j. Click **Event and Additional Columns** in the *Audit Tasks* section.



__k. Check the **Task Has Event** checkbox in the *Event and Sign-off* section.



- __l. Select **V8 PoT Audit Workflow** from the *Default Event Type* drop-down list.

Event, Sign-off & Additional Column

Audit Task V8 PoT Audit Failed Logins

Event and Sign-off

Task Has Event

Has Sign-off Column

Default Event Type V8 PoT Audit Workflow

Define Additional Columns

Column Name	Mandatory	Type	Size	Group	
	<input type="checkbox"/>	String	50		Add

[Close this window](#)

- __m. Click **Apply** and click the **Close this window** link to close the window.

Event, Sign-off & Additional Column

Audit Task V8 PoT Audit Failed Logins

Event and Sign-off

Task Has Event

Has Sign-off Column

Default Event Type V8 PoT Audit Workflow

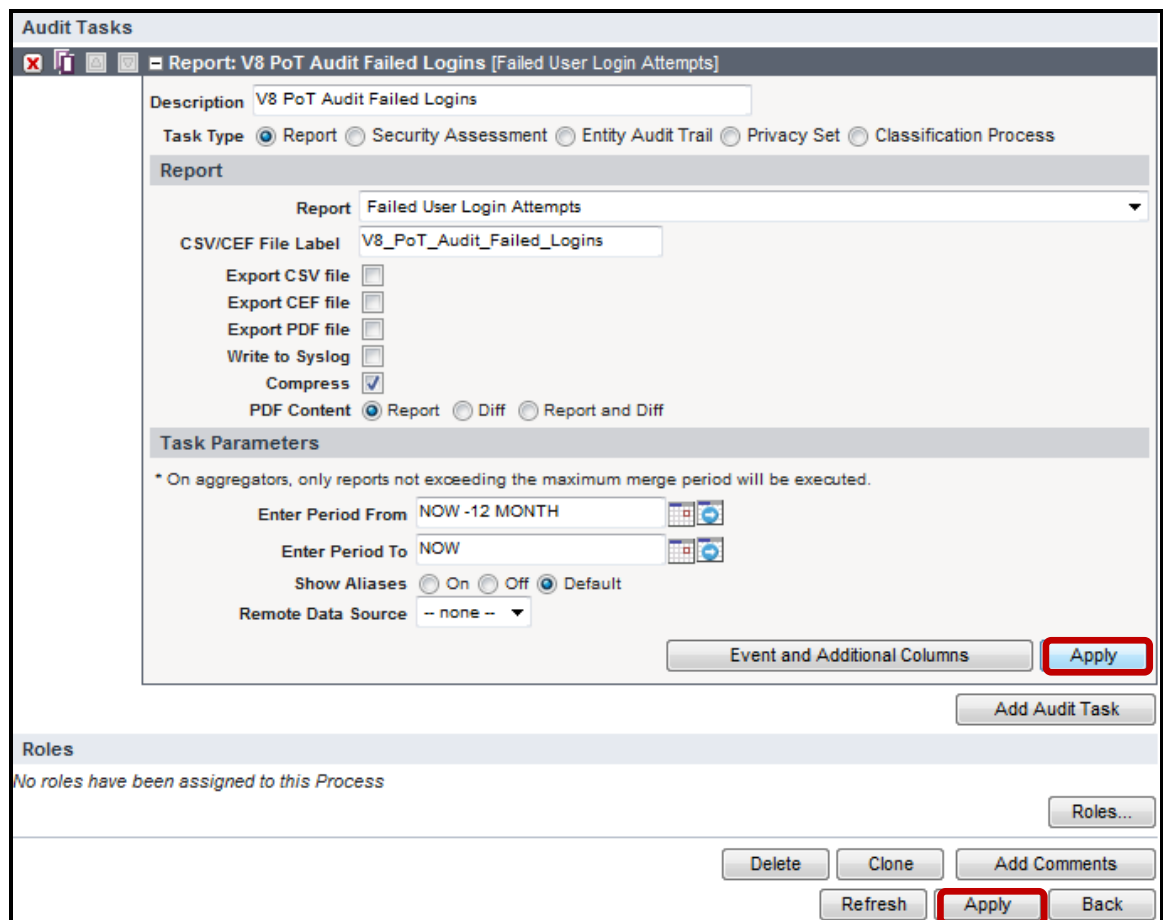
Apply

Define Additional Columns

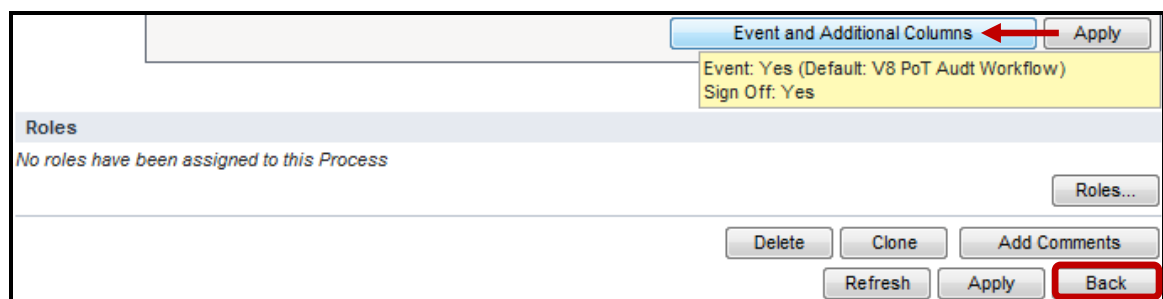
Column Name	Mandatory	Type	Size	Group	
	<input type="checkbox"/>	String	50		Add

[Close this window](#)

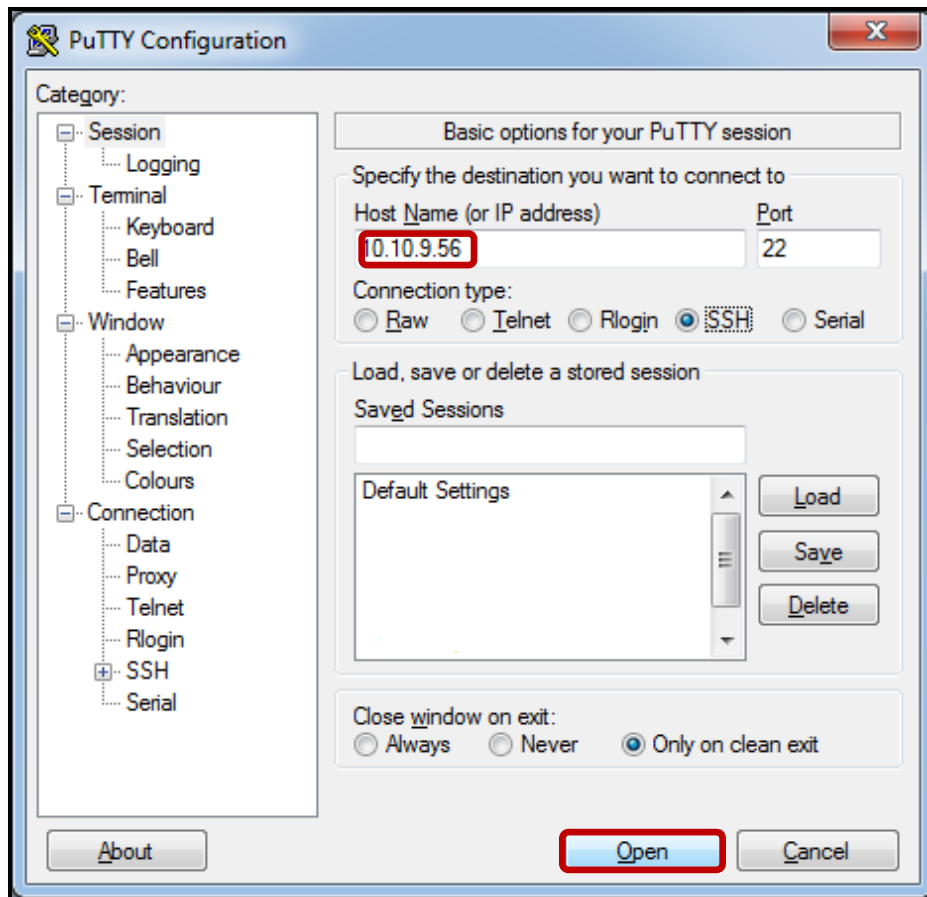
- __n. Click **Apply** in the *Audit Task* panel, and then click **Apply** at the bottom of the screen.



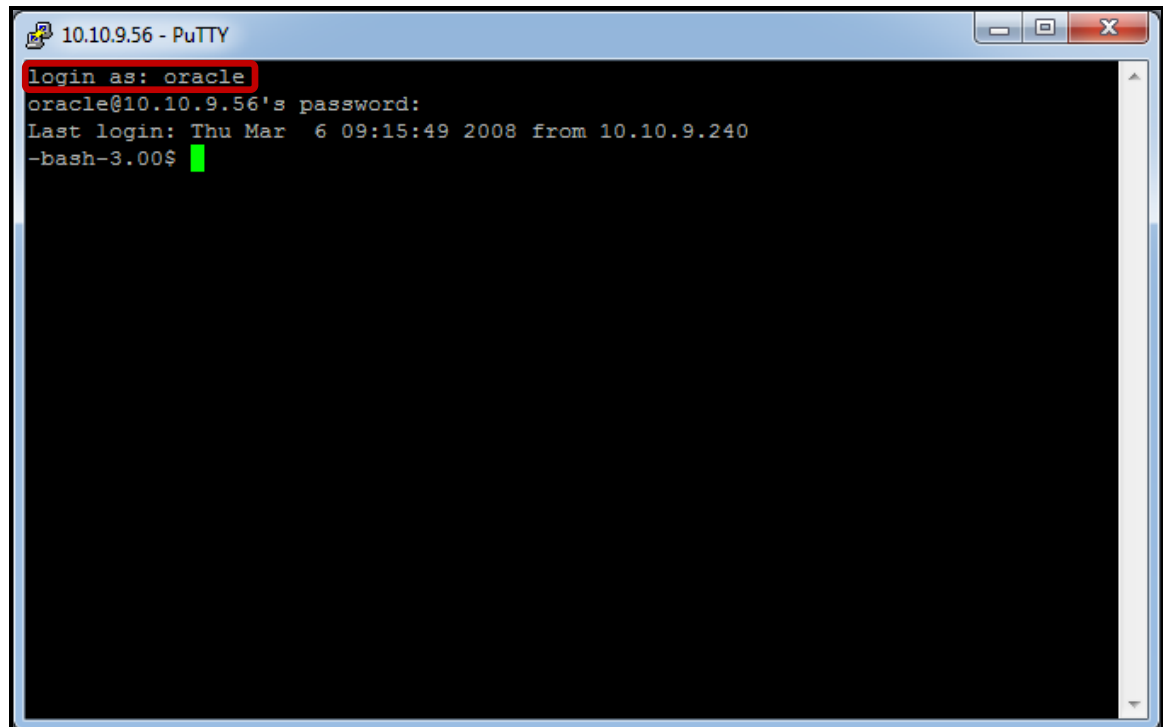
- __o. Hover over **Event and Additional Columns** to confirm that the event is now reflected - **Event: Yes (Default: V8 PoT Audit Workflow)**, and then click **Back**.



- __3. Generate Failed Logins for Report.
 - __a. Using a PuTTY SSH client, access the VM database server to generate data for the Failed User Login Attempts report.
 - __b. Start the PuTTY SSH client login.
 - __c. From your laptop, launch PuTTY, enter **10.10.9.56**, and click **Open**.

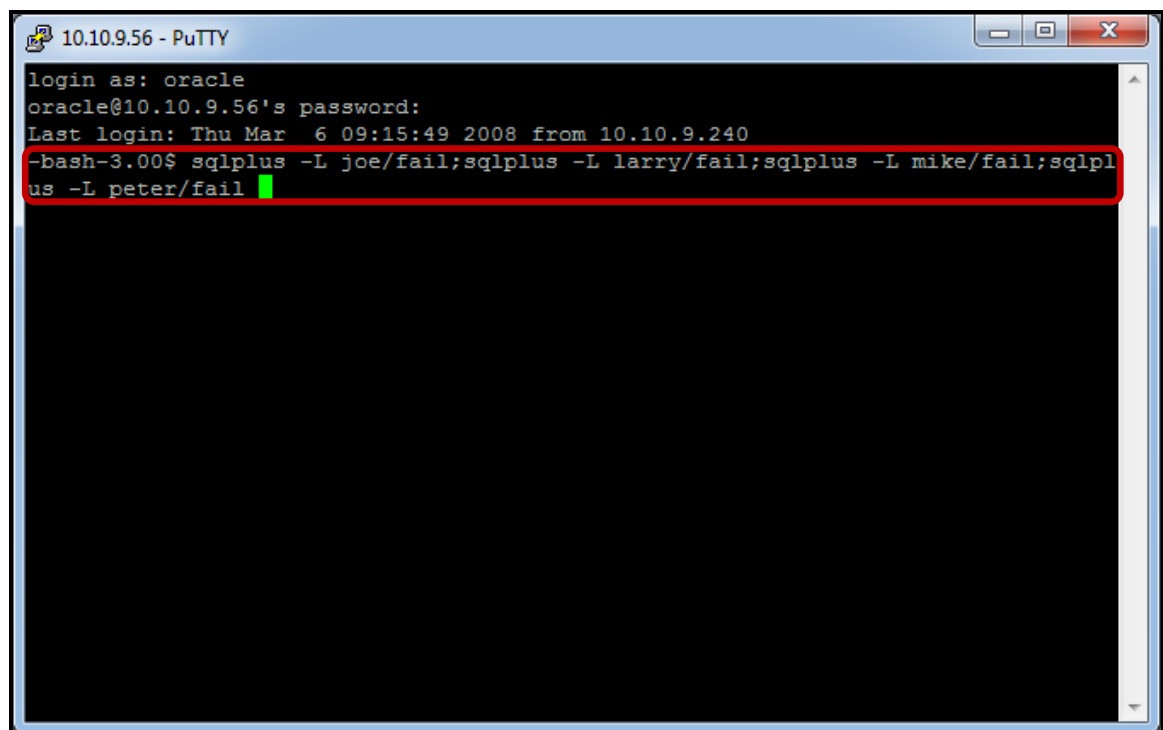


- ___d. Login as **oracle** / **guardium** (Oracle DBA Account). After logging in, the following prompt will be displayed:



```
10.10.9.56 - PuTTY
login as: oracle
oracle@10.10.9.56's password:
Last login: Thu Mar  6 09:15:49 2008 from 10.10.9.240
-bash-3.00$
```

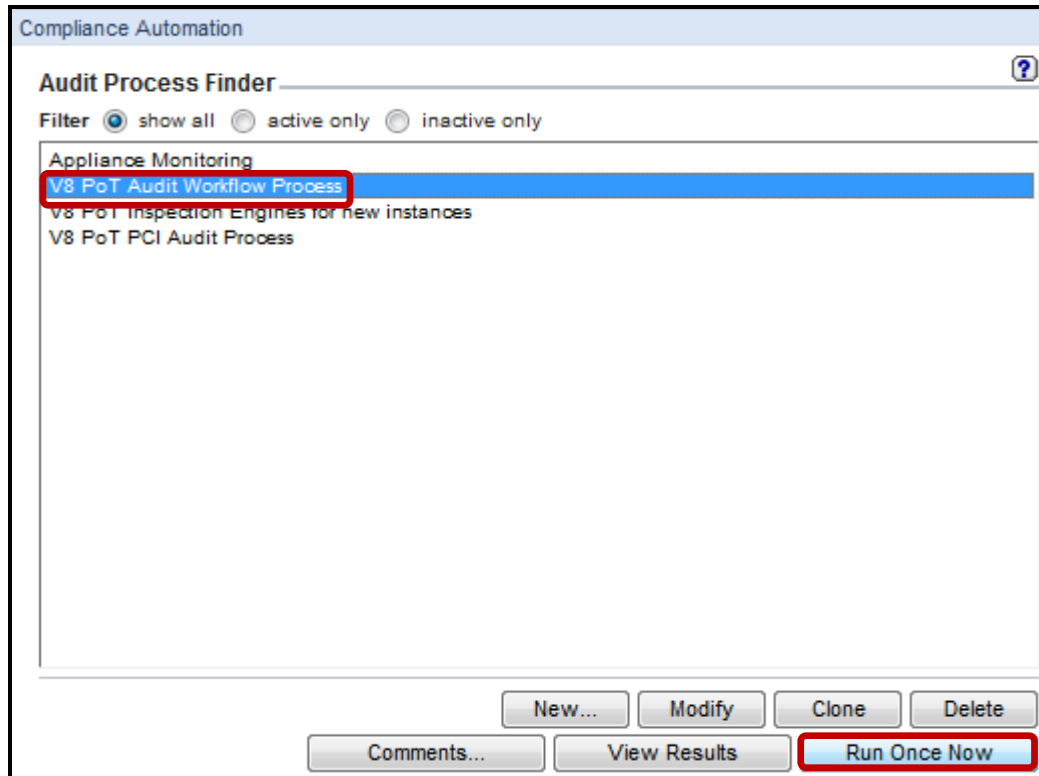
- ___e. Type '**sqlplus -L joe/fail;sqlplus -L larry/fail;sqlplus -L mike/fail;sqlplus -L peter/fail**' to generate a failed login attempt for each of the four named users.



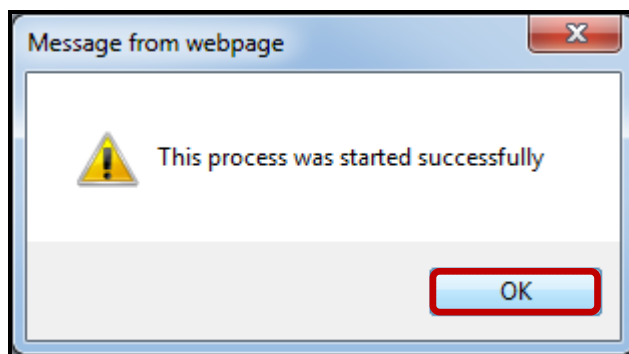
```
10.10.9.56 - PuTTY
login as: oracle
oracle@10.10.9.56's password:
Last login: Thu Mar  6 09:15:49 2008 from 10.10.9.240
-bash-3.00$ sqlplus -L joe/fail;sqlplus -L larry/fail;sqlplus -L mike/fail;sqlpl
us -L peter/fail
```

__4. Execute the Audit Workflow Process.

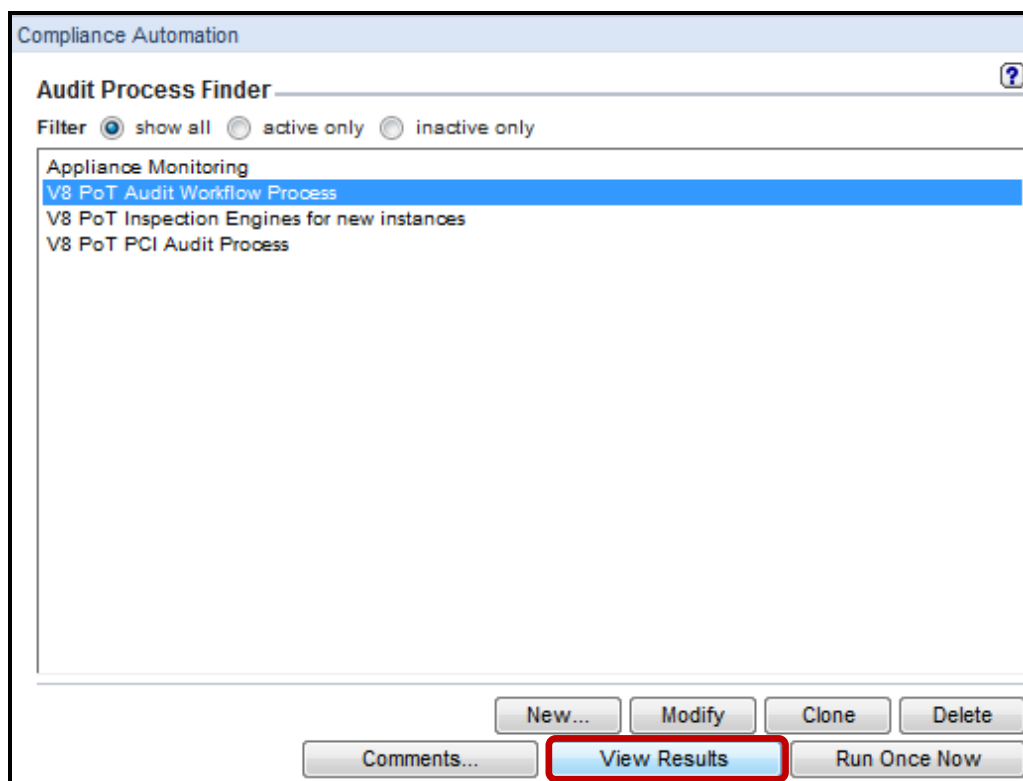
__a. Select **V8 PoT Audit Workflow Process** from the *Audit Process Finder* drop-down list, and click **Run Once Now**.



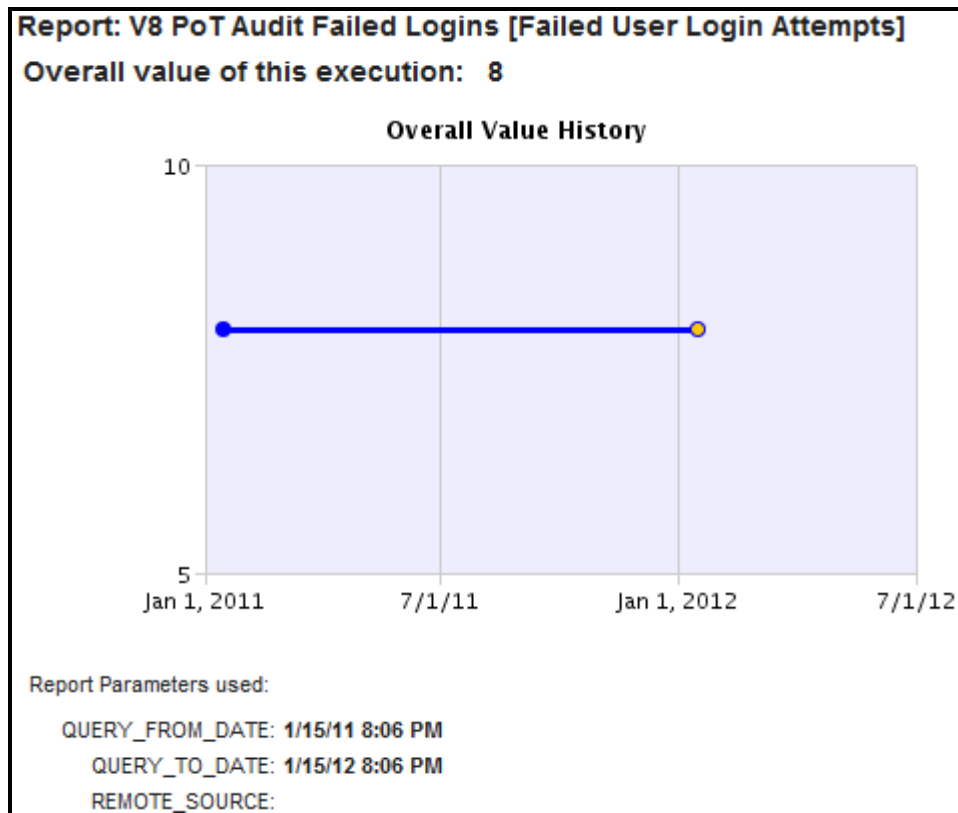
__b. Click **OK** to acknowledge.



- __5. Examine the results of the Audit Workflow Process.
- __a. Click **View Results** to browse output.



- __b. Examine the *upper* portion of output which shows an **Overall Value History** graph.



- __c. Now examine the *lower* portion of output which displays all **failed logins**.
- __d. Click the **Close this window** link to close the results, and logout as user **pot**.

Events and Custom Fields Filter Display Event: Status: Filter

For selected rows, add or update:

New Event: Action: Sign Apply

Report details: Compare with other results Show original values Use Aliases

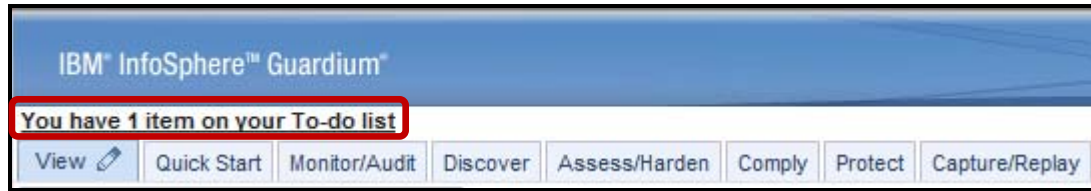
DB User Name	Client IP	Server IP	Server Type	Exception Timestamp	Count of Exceptions	Event/Status	Sign	By
<input type="checkbox"/> JOE	10.10.9.56	10.10.9.56	ORACLE	2012-02-21 02:41:39	1	V8 PoT Audit Workflow/Open		Default Event 2012-02-21 02:54:08
<input type="checkbox"/> LARRY	10.10.9.56	10.10.9.56	ORACLE	2012-02-21 02:41:39	1	V8 PoT Audit Workflow/Open		Default Event 2012-02-21 02:54:08
<input type="checkbox"/> MIKE	10.10.9.56	10.10.9.56	ORACLE	2012-02-21 02:41:39	1	V8 PoT Audit Workflow/Open		Default Event 2012-02-21 02:54:08
<input type="checkbox"/> PETER	10.10.9.56	10.10.9.56	ORACLE	2012-02-21 02:41:39	1	V8 PoT Audit Workflow/Open		Default Event 2012-02-21 02:54:08

Records: 1 To 4 Of 4

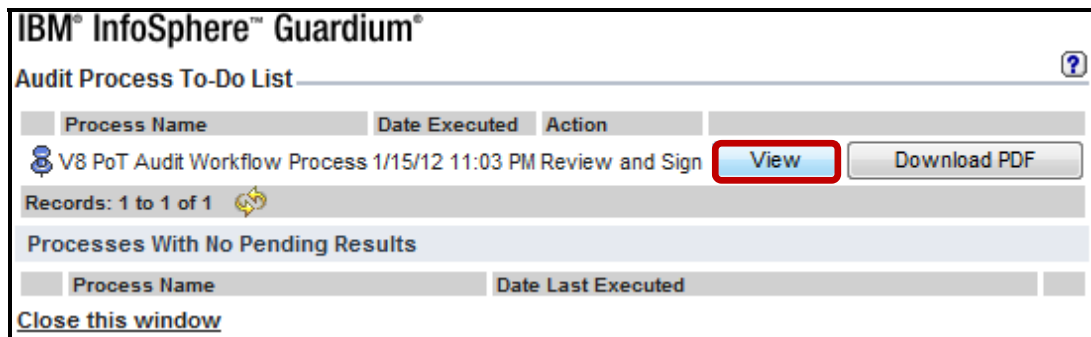
[Close this window](#)

__6. DBA Role Views Results and Transitions from Open to Under Review.

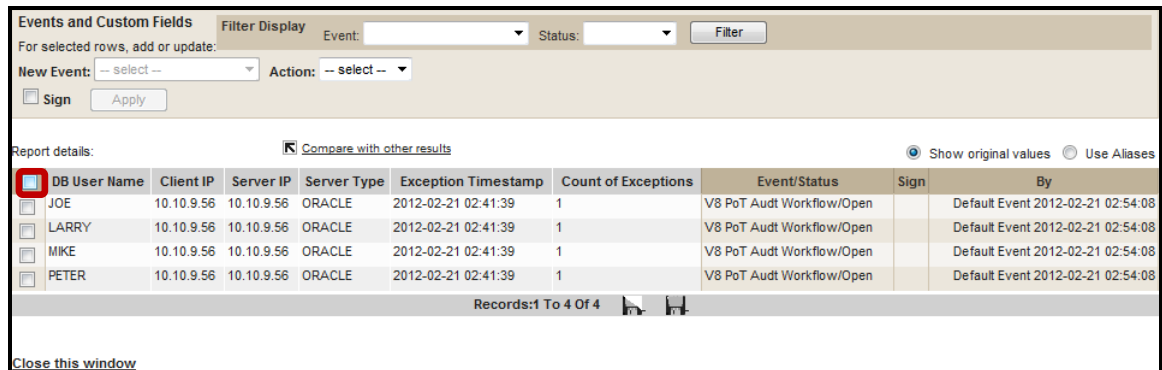
- __a. Login to InfoSphere Guardium as user **joe / guardium**, and click the link at the upper left of the screen – **You have 1 item on your To-do list**.



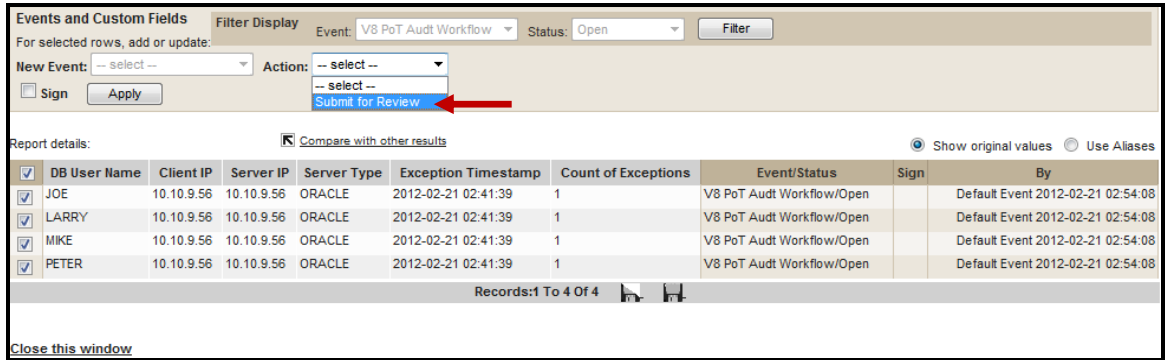
- __b. Click **View** to view the **V8 PoT Audit Workflow Process**.



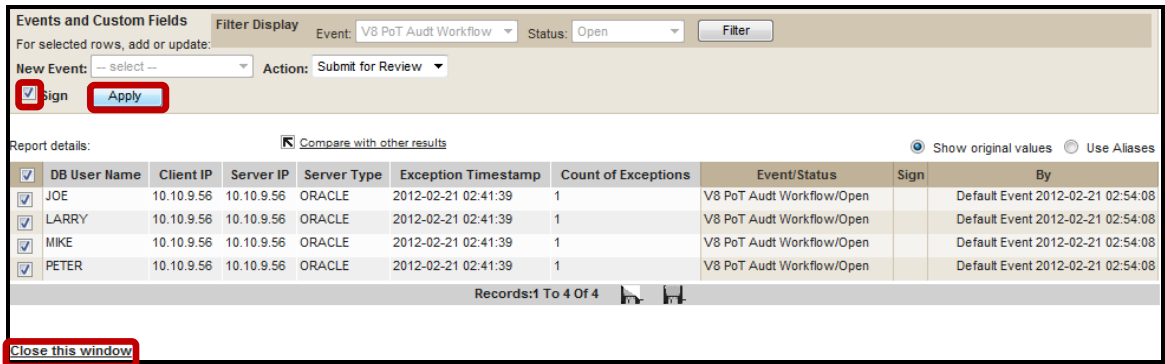
- __c. Check the **DB User Name** checkbox to select all listed users.



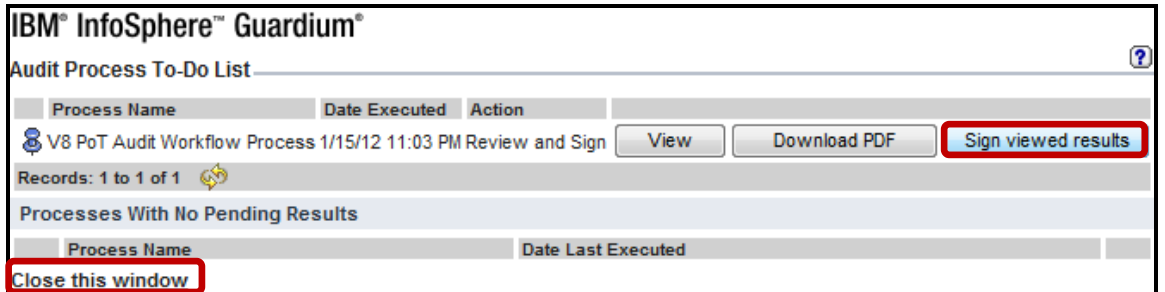
__d. Select **Submit for Review** from the *Action* drop-down list.



__e. Check the **Sign** checkbox, click **Apply**, and then click the **Close this window** link to close this window.

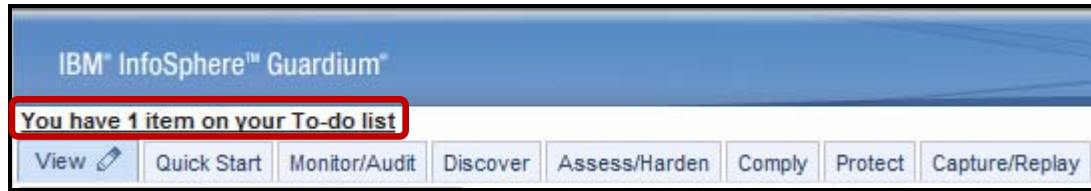


__f. Click **Sign viewed results** on the previous window to complete the To-Do List task item, click the **Close this window** link to close the window, and then logout as user **joe**.

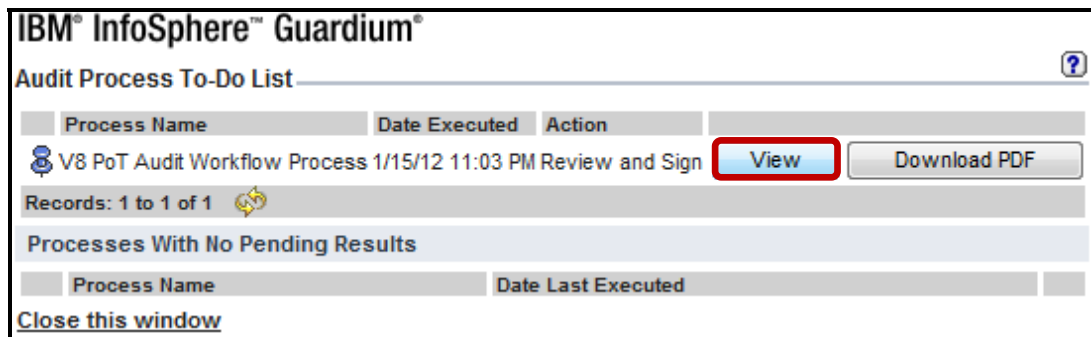


__7. Information Security Role Views Results and Transitions from Under Review to Approve.

- __a. Login to InfoSphere Guardium as user **larry / guardium**, and click the link at the upper left of the screen – **You have 1 item on your To-do list**.

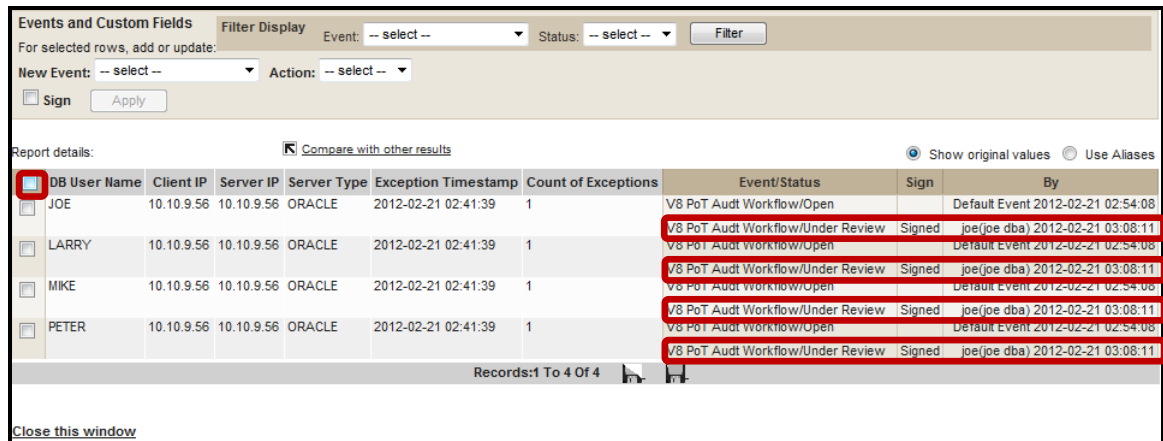


- __b. Click **View** to view the **V8 PoT Audit Workflow Process**.



- __c. Check the **DB User Name** checkbox to select all listed users.

Note: Joe’s previous signing is now reflected in the *Sign* column.



__d. Select **Approve** from the *Action* drop-down list.

The screenshot shows the 'Events and Custom Fields' window. At the top, there are filters for 'Event: V8 PoT Audt Workflow' and 'Status: Under Review'. Below the filters, there are dropdown menus for 'New Event' and 'Action'. The 'Action' dropdown menu is open, showing options: '-- select --', 'Reject', and 'Approve'. A red arrow points to the 'Approve' option. Below the dropdowns are 'Sign' and 'Apply' buttons. The main area contains a table with columns: DB User Name, Client IP, Server IP, Server Type, Exception Timestamp, Count of Exceptions, Event/Status, Sign, and By. The table lists four users: JOE, LARRY, MIKE, and PETER. At the bottom, there is a 'Close this window' link.

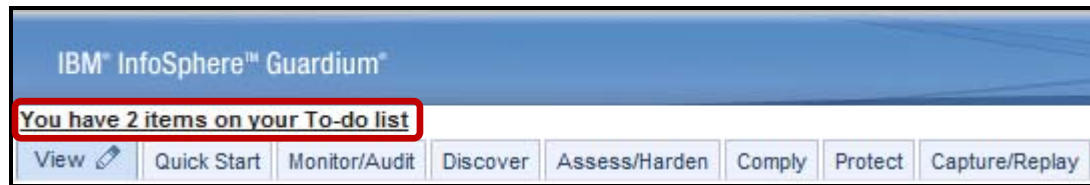
__e. Check the **Sign** checkbox, click **Apply**, and then click the **Close this window** link to close this window.

This screenshot is similar to the previous one, but the 'Sign' checkbox is now checked. The 'Apply' button is highlighted with a red box. The 'Action' dropdown menu is now set to 'Approve'. The 'Close this window' link at the bottom is also highlighted with a red box.

__f. Click **Sign viewed results** on the previous window to complete the To-Do List task item, click the **Close this window** link to close the window, and then logout as user larry.

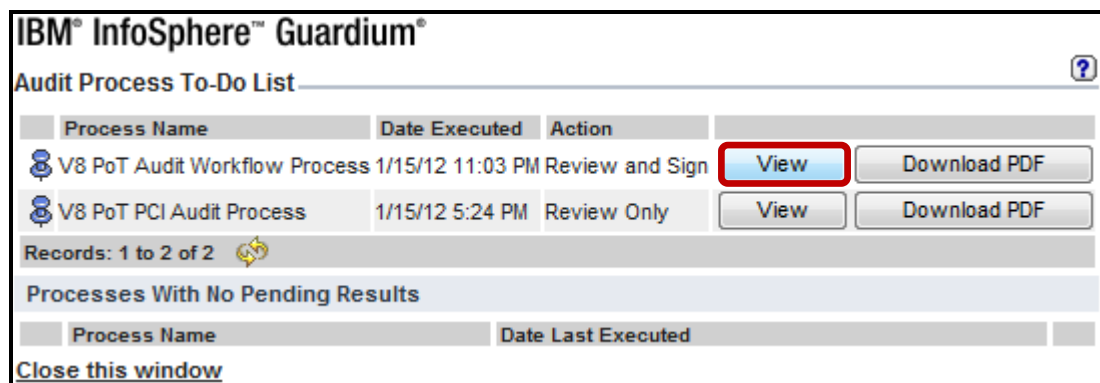
The screenshot shows the 'Audit Process To-Do List' window. It has a header 'IBM InfoSphere Guardium' and a sub-header 'Audit Process To-Do List'. Below the header is a table with columns: Process Name, Date Executed, and Action. The table contains one row: 'V8 PoT Audit Workflow Process 1/15/12 11:03 PM Review and Sign'. To the right of this row are three buttons: 'View', 'Download PDF', and 'Sign viewed results'. The 'Sign viewed results' button is highlighted with a red box. Below the table, there is a section 'Processes With No Pending Results' with a sub-table. At the bottom left, there is a 'Close this window' link highlighted with a red box.

- __8. Auditor Role Views Results and Sign-offs on Approved Tasks.
- __a. Login to InfoSphere Guardium as user **mike / guardium**, and click the link at the upper left of the screen – **You have 2 items on your To-do list.**



- __b. Click **View** to view the **V8 PoT Audit Workflow Process**.

Note: The second item is from the previously run **V8 PoT PCI Audit Process**.



__c. Check the **DB User Name** checkbox to select all listed users.

Note: Larry's previous signing is also reflected in the *Sign* column.

Events and Custom Fields Filter Display Event: [] Status: [] Filter

For selected rows, add or update: New Event: [] Action: []

Sign Apply

Report details: Compare with other results Show original values Use Aliases

<input type="checkbox"/> DB User Name	Client IP	Server IP	Server Type	Exception Timestamp	Count of Exceptions	Event/Status	Sign	By
<input type="checkbox"/> JOE	10.10.9.56	10.10.9.56	ORACLE	2012-02-21 02:41:39	1	V8 PoT Audit Workflow/Open		Default Event 2012-02-21 02:54:08
<input type="checkbox"/> LARRY	10.10.9.56	10.10.9.56	ORACLE	2012-02-21 02:41:39	1	V8 PoT Audit Workflow/Under Review	Signed	ip(ice dba) 2012-02-21 03:08:11
<input type="checkbox"/> MIKE	10.10.9.56	10.10.9.56	ORACLE	2012-02-21 02:41:39	1	V8 PoT Audit Workflow/Closed(Final)	Signed	larry(larry infosec) 2012-02-21 03:16:18
<input type="checkbox"/> PETER	10.10.9.56	10.10.9.56	ORACLE	2012-02-21 02:41:39	1	V8 PoT Audit Workflow/Open		Default Event 2012-02-21 02:54:08
						V8 PoT Audit Workflow/Under Review	Signed	ip(ice dba) 2012-02-21 03:08:11
						V8 PoT Audit Workflow/Closed(Final)	Signed	larry(larry infosec) 2012-02-21 03:16:18
						V8 PoT Audit Workflow/Open		Default Event 2012-02-21 02:54:08
						V8 PoT Audit Workflow/Under Review	Signed	ip(ice dba) 2012-02-21 03:08:11
						V8 PoT Audit Workflow/Closed(Final)	Signed	larry(larry infosec) 2012-02-21 03:16:18
						V8 PoT Audit Workflow/Open		Default Event 2012-02-21 02:54:08
						V8 PoT Audit Workflow/Under Review	Signed	ip(ice dba) 2012-02-21 03:08:11
						V8 PoT Audit Workflow/Closed(Final)	Signed	larry(larry infosec) 2012-02-21 03:16:18

Records: 1 To 4 Of 4

Close this window

- d. Check the **Sign** checkbox, click **Apply**, and then click the **Close this window** link to close this window.

Note: The **V8 PoT Audit Workflow Process** has been reviewed and signed by each of Joe (DBA), Larry (Information Security) and Mike (Audit).

Events and Custom Fields Filter Display Event: V8 PoT Audit Workflow Status: Closed Filter

For selected rows, add or update: New Event: -- select -- Action: -- select --

Sign **Apply**

Report details: Compare with other results Show original values Use Aliases

DB User Name	Client IP	Server IP	Server Type	Exception Timestamp	Count of Exceptions	Event/Status	Sign	By
<input checked="" type="checkbox"/> JOE	10.10.9.56	10.10.9.56	ORACLE	2012-02-21 02:41:39	1	V8 PoT Audit Workflow/Open		Default Event 2012-02-21 02:54:08
						V8 PoT Audit Workflow/Under Review	Signed	joe(joe dba) 2012-02-21 03:08:11
						V8 PoT Audit Workflow/Closed(Final)	Signed	larry(larry infosec) 2012-02-21 03:16:18
<input checked="" type="checkbox"/> LARRY	10.10.9.56	10.10.9.56	ORACLE	2012-02-21 02:41:39	1	V8 PoT Audit Workflow/Open		Default Event 2012-02-21 02:54:08
						V8 PoT Audit Workflow/Under Review	Signed	joe(joe dba) 2012-02-21 03:08:11
						V8 PoT Audit Workflow/Closed(Final)	Signed	larry(larry infosec) 2012-02-21 03:16:18
<input checked="" type="checkbox"/> MIKE	10.10.9.56	10.10.9.56	ORACLE	2012-02-21 02:41:39	1	V8 PoT Audit Workflow/Open		Default Event 2012-02-21 02:54:08
						V8 PoT Audit Workflow/Under Review	Signed	joe(joe dba) 2012-02-21 03:08:11
						V8 PoT Audit Workflow/Closed(Final)	Signed	larry(larry infosec) 2012-02-21 03:16:18
<input checked="" type="checkbox"/> PETER	10.10.9.56	10.10.9.56	ORACLE	2012-02-21 02:41:39	1	V8 PoT Audit Workflow/Open		Default Event 2012-02-21 02:54:08
						V8 PoT Audit Workflow/Under Review	Signed	joe(joe dba) 2012-02-21 03:08:11
						V8 PoT Audit Workflow/Closed(Final)	Signed	larry(larry infosec) 2012-02-21 03:16:18

Records: 1 To 4 Of 4

Close this window

- e. Click **Sign viewed results** on the previous window to complete this To-Do List task item, click the **Close this window** link to close the window, and then logout as user **mike**.

IBM® InfoSphere™ Guardium®

Audit Process To-Do List

Process Name	Date Executed	Action
V8 PoT Audit Workflow Process	1/15/12 11:03 PM	Review and Sign View Download PDF Sign viewed results
V8 PoT PCI Audit Process	1/15/12 5:24 PM	Review Only View Download PDF

Records: 1 to 2 of 2

Processes With No Pending Results

Process Name	Date Last Executed
--------------	--------------------

Close this window

Thank You

Advanced Compliance Workflow (Optional) review

- __1. Advanced Compliance Workflow gives you the ability to:
 - __a. Generate and distribute reports.
 - __b. Use Custom workflows.
 - __c. Add additional columns for report details.
 - __d. All of the above.
 - __e. b and c.

- __2. With Advanced Compliance Workflow, you can sign-off reports at the line-item level. **(True or False)**.

- __3. Each Compliance Workflow can use multiple Custom Workflows. **(True or False)**.

- __4. Reports can be exported into the following formats:
 - __a. CSV, PDF, CEF, and HTML.
 - __b. CSV, PDF, and TXT.
 - __c. CSV, PDF, HTML, and TXT.
 - __d. CSV, PDF, and CEF.

- __5. Multiple columns can be added for sign-off (e.g. Explanation, Project, and Review Status). **(True or False)**.

Advanced Compliance Workflow (Optional) review (Answers)

__1. Advanced Compliance Workflow gives you the ability to:

E – B (Use Custom workflows) and C (Add additional columns for report details).

__2. With Advanced Compliance Workflow, you can sign-off reports at the line-item level.
(**True** or **False**).

True.

__3. Each Compliance Workflow can use multiple Custom Workflows.
(**True** or **False**).

False.

__4. Reports can be exported into the following formats:

D – CSV, PDF and CEF.

__5. Multiple columns can be added for sign-off (e.g. Explanation, Project, and Review Status).
(**True** or **False**).

True.

Lab 9 Configuration Audit System (CAS)

9.1 Exploring CAS

Overview

A database is a program that is installed at the operating system level and makes use of operating system services. There are many configuration elements that reside within operating system constructs rather than within the database itself.

Examples include files, registry values and environment variables. Many of these files and values control some of the most important aspects of database security. A good example is the authentication method of the database. In almost all database platforms, an administrator can change the way that a database authenticates users by changing such a value, either in addition to or instead of using SQL.

The IBM InfoSphere® Guardium® Configuration Audit System (CAS) tracks all changes made to the database at various levels, and reports on these changes to a centralized web-based console. Using the CAS module, database security administrators can know that no changes that may affect security have been made in ways that bypass the database's SQL engine.

Objectives

This Lab will illustrate how we can check to make sure CAS is installed and configured on both the appliance and database server, describe and create a template and utilize CAS to distinguish changes made on the operating system that may affect database performance, using the following steps:

- __1. Validate that CAS is installed on the database server.
- __2. Ensure that CAS is running.
- __3. Discuss and create and utilize a template for mapping changes.
- __4. Create changes on operating system and view CAS results.
- __5. Automate CAS report for future usage.

- __1. Using the InfoSphere Guardium GUI, demonstrate the ease of use within the InfoSphere Guardium solution. Start the InfoSphere Guardium appliance and login.
 - __a. From your laptop, go to <https://10.10.9.248:8443>
 - __b. Login as **pot / guardium**.

Login

Please enter your information

User name:

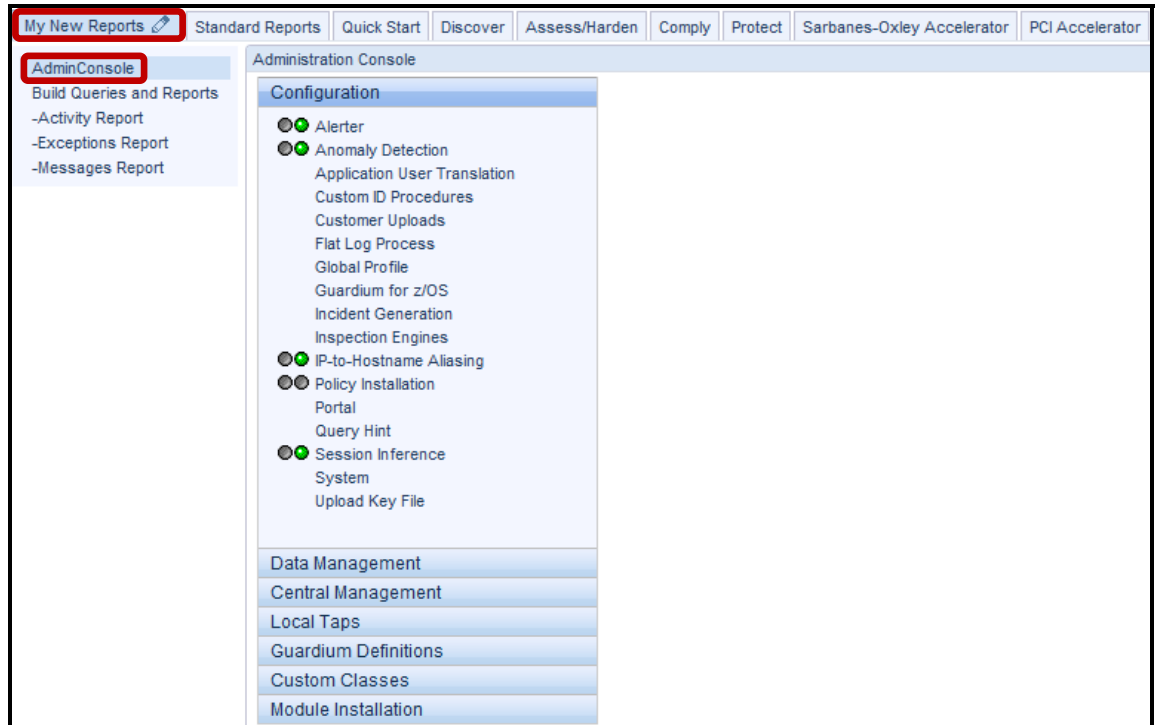
Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

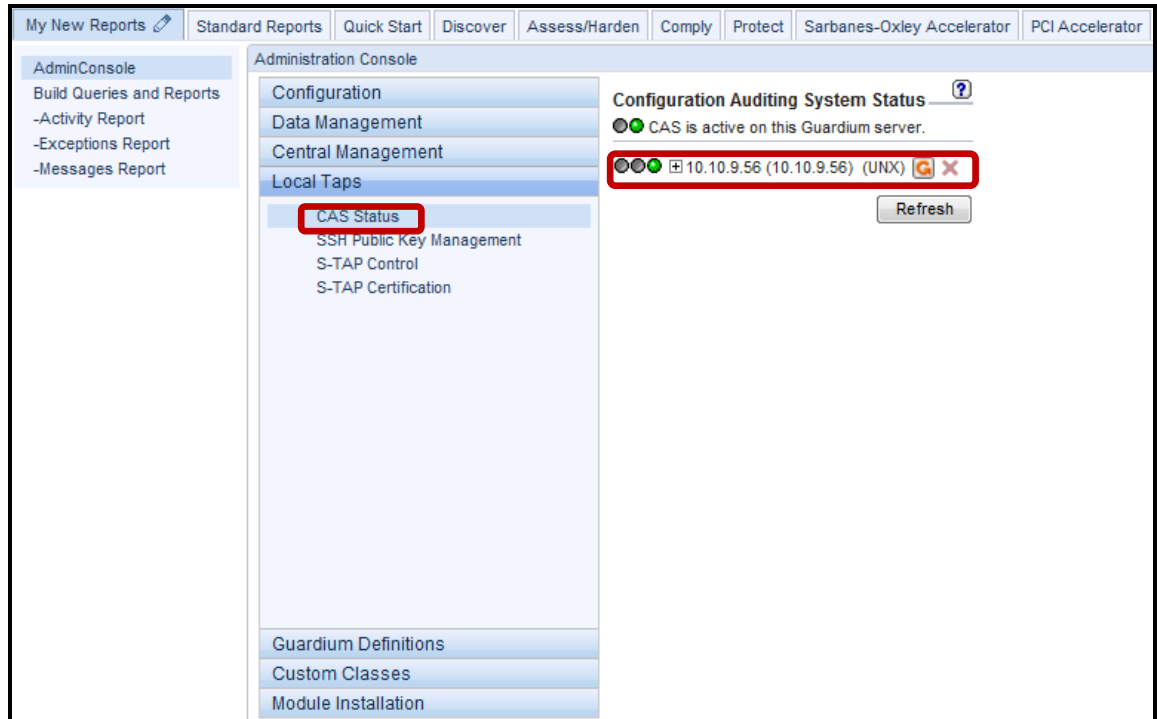
CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistrykey © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

- c. Click on **AdminConsole** under the **My New Reports Tab**. The InfoSphere Guardium console will be displayed.

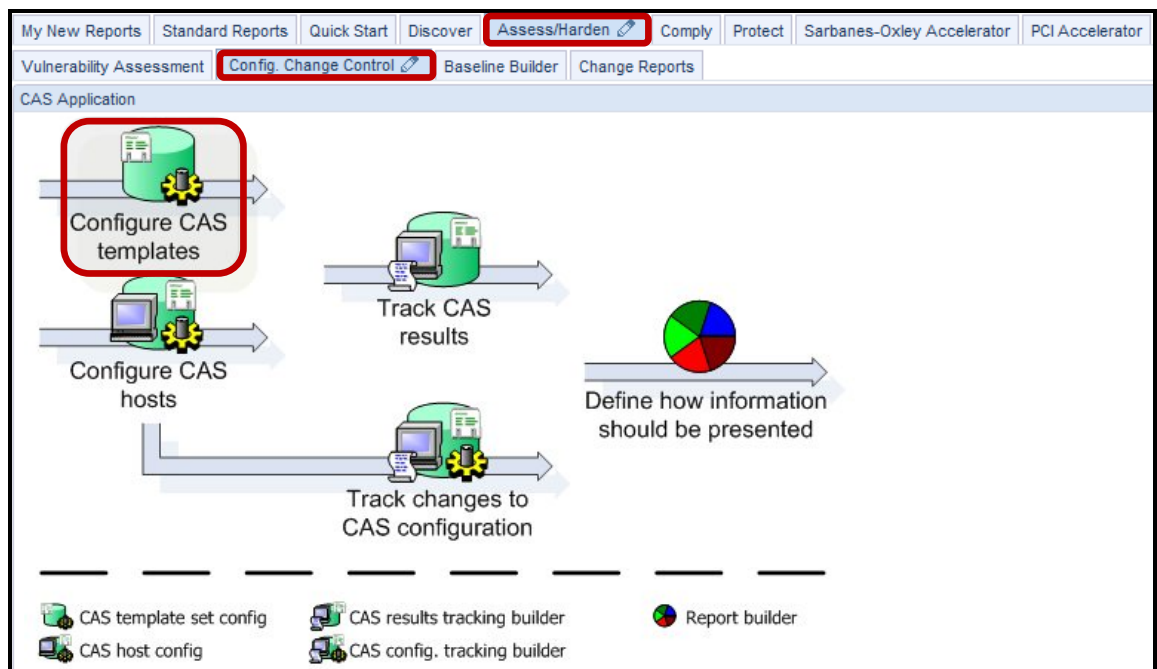


__2. Create a new CAS template to monitor a sensitive UNIX operating system file.

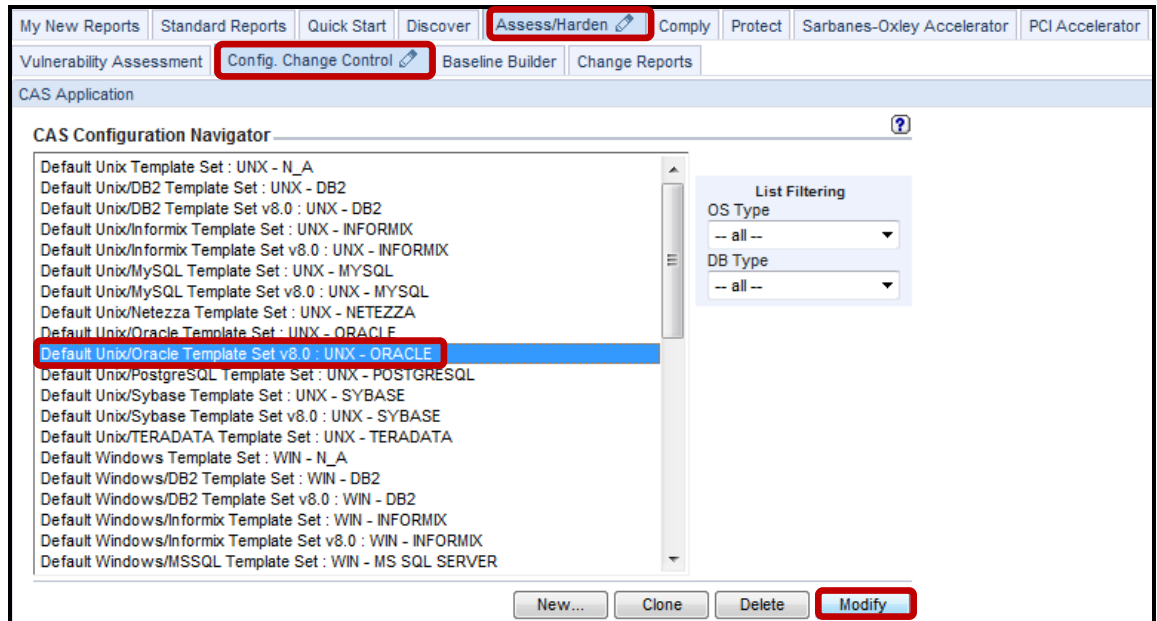
__a. Click **CAS Status** under the **Local Taps** tab to confirm that CAS is currently active on the Database server (Indicated by Green).



__b. Click **Configure CAS templates** under the **Assess/Harden->Config. Change Control** tabs, and select **Configure CAS templates**.



c. Select **Default Unix/Oracle Template Set v8.0 : UNIX – ORACLE** and click **Modify**.



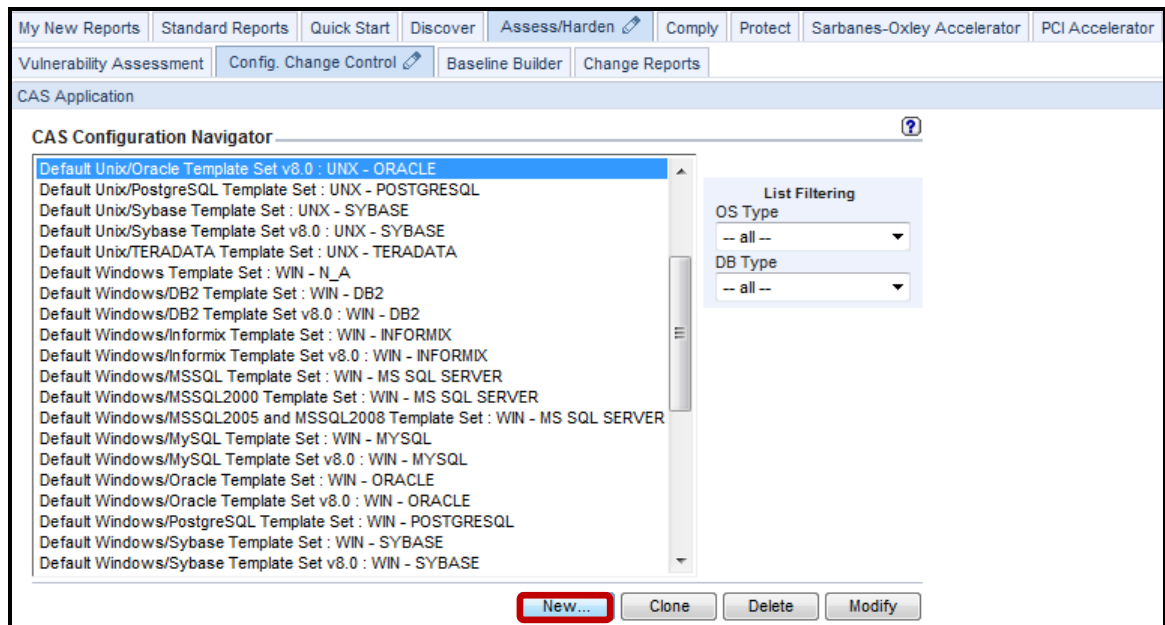
__d. View contents for reference and click **Back**

Monitored Item Template Definitions ?

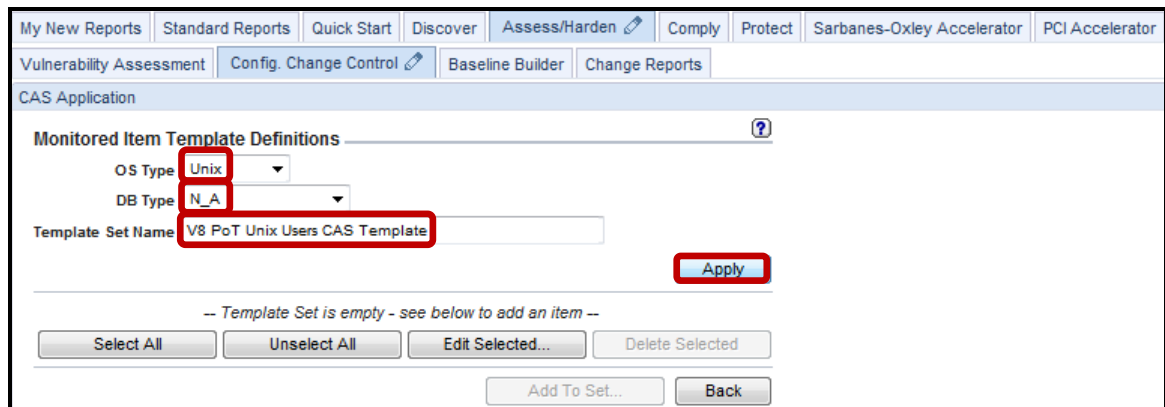
OS Type UNX
DB Type ORACLE
Template Set Name Default Unix/Oracle Template Set v8.0

Item	Type	Period	Use MD5	Keep Data
<input type="checkbox"/> \$ORACLE_HOME/dbs/*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/inventory/Templates/bin/*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/jdk/jre/bin/*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/jre/*bin/*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/network/admin/*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/oui/bin/./.*so	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/Oracle/Oracle/bin/*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/Oracle/Oracle/fcgi-bin/*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/Oracle/Jsdk/bin/servletrunner	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/Oracle/open_ssl/bin/openssl*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/assistants/dbma/mep.cfg	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/ds/bin/*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/javavm/admin/*so	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/jdk/bin/*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/ocommon/nls/lbuilder/lbuilder	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/olap/ov*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/soap/bin/*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/syndication/bin/*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/sysman/admin/OMSRepositoryConstraints.properties	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/sysman/config/*properties	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$ORACLE_HOME/xdk/admin/xml.properties	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> ORACLE_BASE	Environment Variable	10m	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> ORACLE_HOME	Environment Variable	10m	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> ORACLE_SID	Environment Variable	10m	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> TNS_ADMIN	Environment Variable	10m	<input type="checkbox"/>	<input type="checkbox"/>

__e. Click **New** to define new template for this lab



__f. Enter '**V8 PoT Unix Users CAS Template**' for *Template Set Name*, select **Unix** from the *OS Type* drop-down list, **N_A** from *DB Type* drop-down list, and then click **Apply**.



__g. Click **Add To Set**.

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

Vulnerability Assessment | Config. Change Control | Baseline Builder | Change Reports

CAS Application

Monitored Item Template Definitions ?

OS Type: Unix
DB Type: N_A
Template Set Name: V8 PoT Unix Users CAS Template

Apply

-- Template Set is empty - see below to add an item --

Select All | Unselect All | Edit Selected... | Delete Selected

Add To Set... | Add Comments | Back

__h. Enter **V8 PoT /etc/passwd** for the *Description* field, enter **/etc/passwd** for the *File name* field, enter **root** for both the *File Owner* and *File Group* fields, select **Minutes** from the *Period* drop-down list, check the **Keep data** checkbox, and then click **Apply**.

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

Vulnerability Assessment | Config. Change Control | Baseline Builder | Change Reports

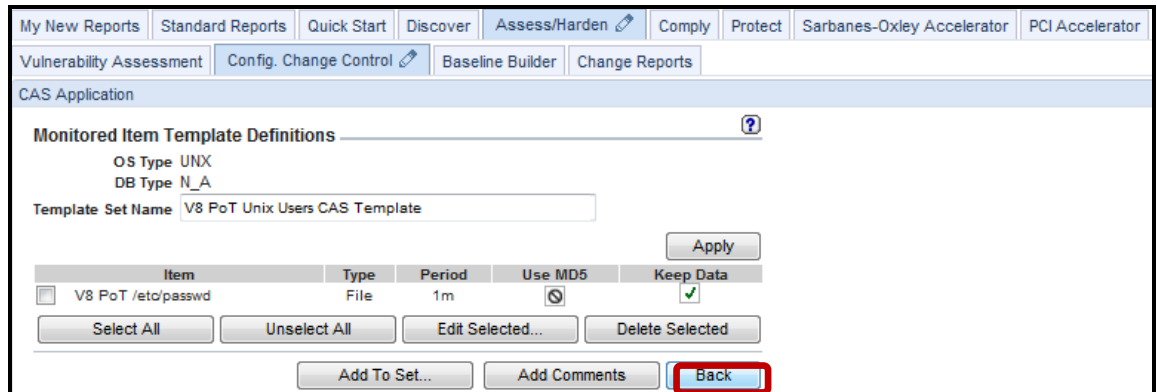
CAS Application

Monitored Item Template Definition ?

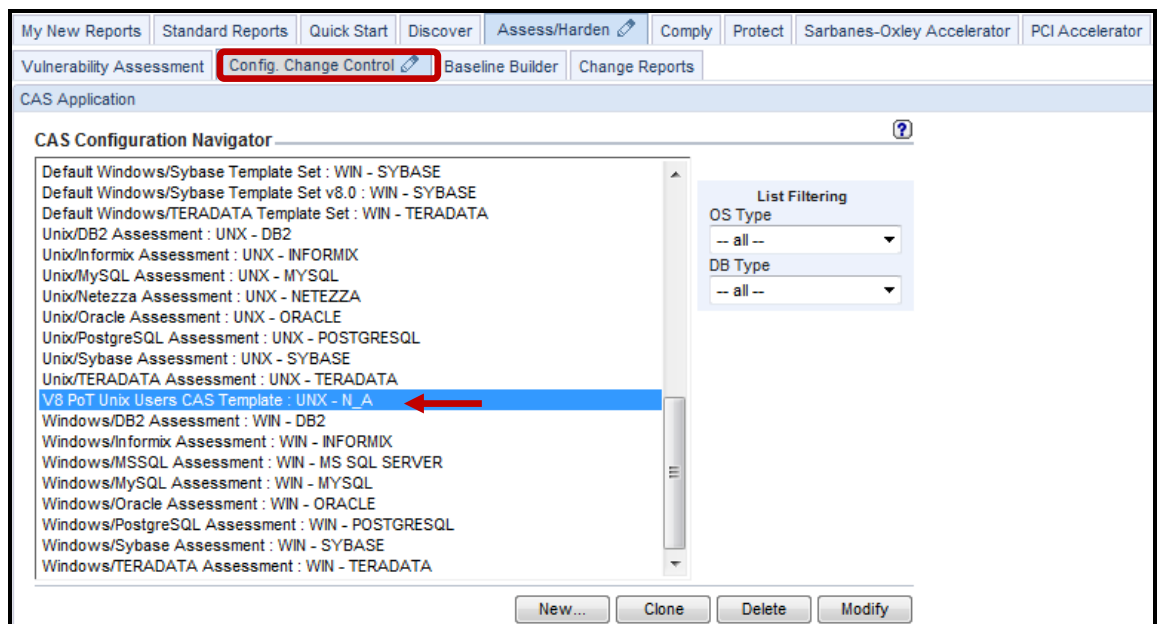
OS Type: UNX
DB Type: N_A
Description: V8 PoT /etc/passwd
Type: File
File name: /etc/passwd
Permissions limit:
File Owner: root
File Group: root
Period: 1 Minute(s)
* Period will: Minute(s) (selected)
Keep data:
Use MD5:
Enabled:

Delete | **Apply** | Back

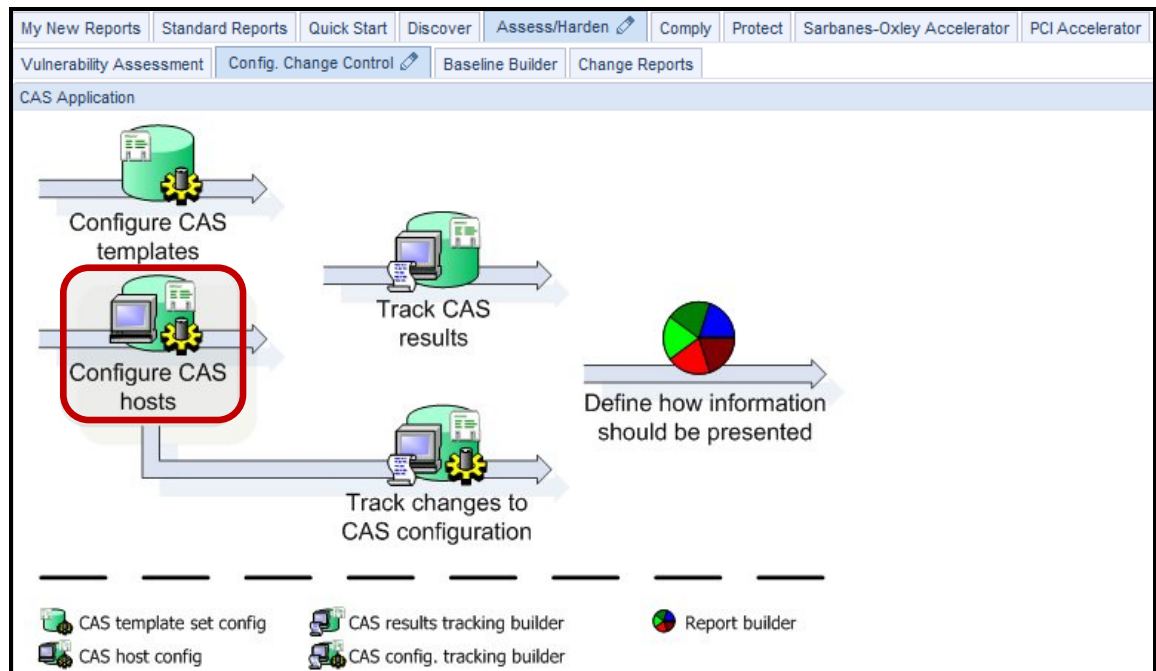
__i. Click **Back**.



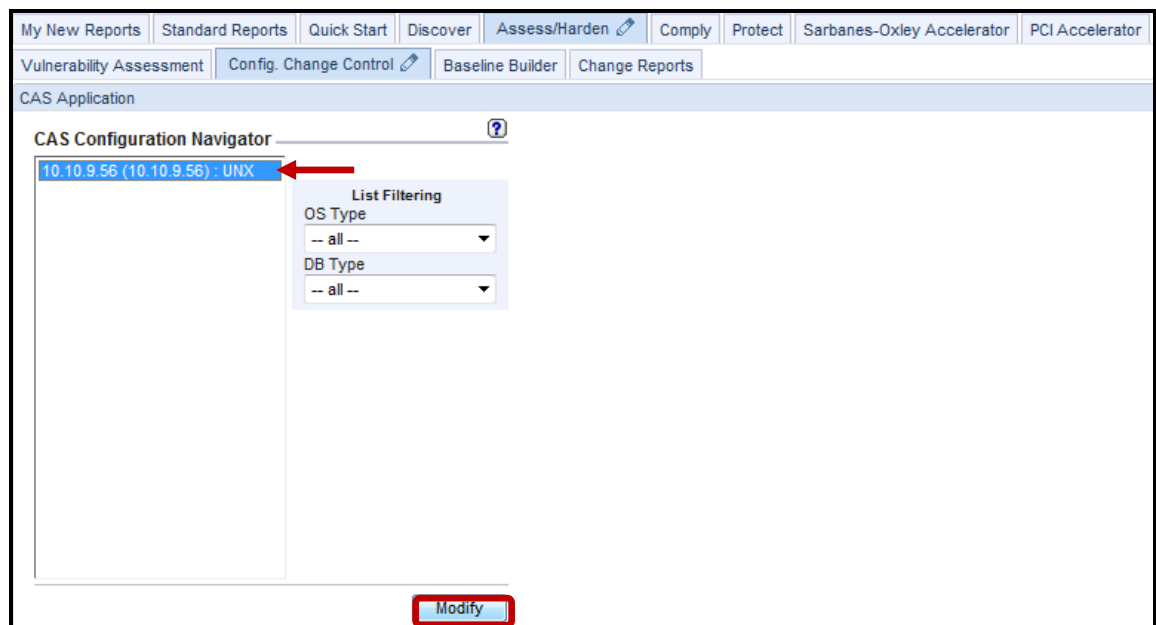
__j. Verify the Template was properly added, and then click the **Config. Change Control** tab.



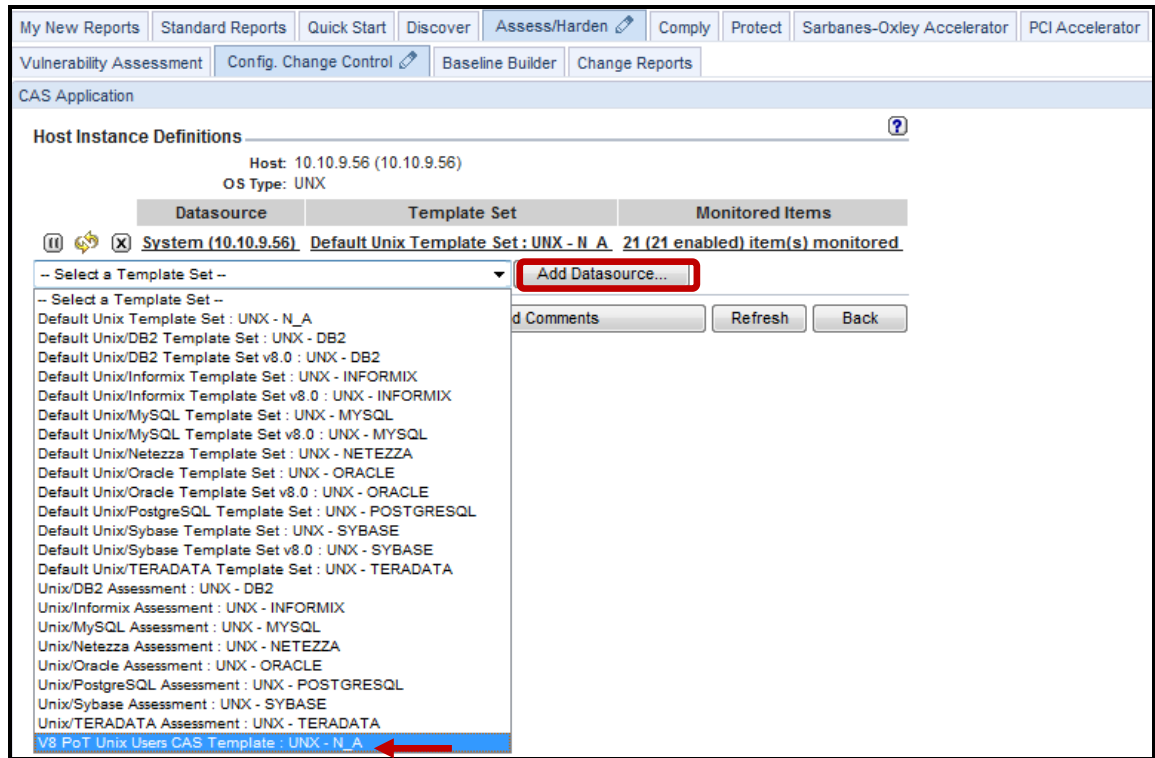
__k. Select **Configure CAS hosts**.



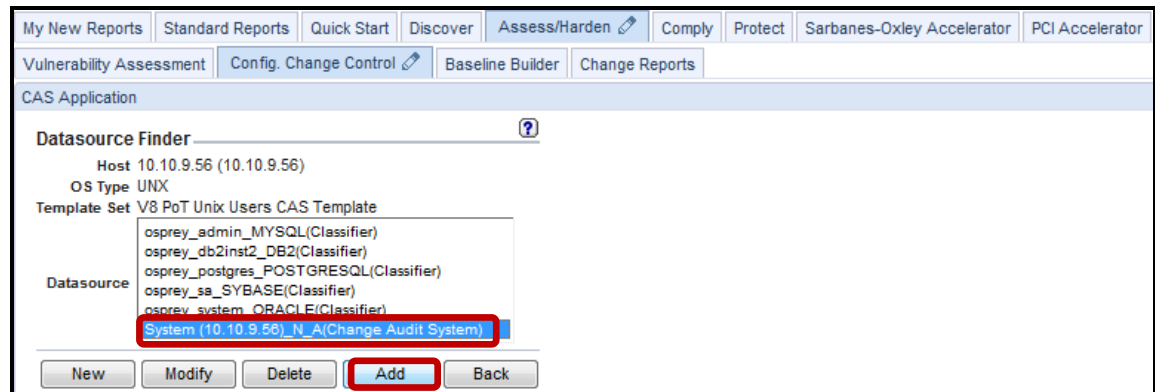
__l. Select **10.10.9.56 (10.10.9.56): UNX** and click **Modify**.



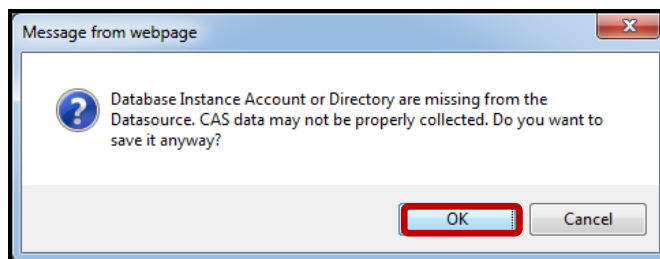
- m. Select the **V8 PoT Unix Users CAS Template** that was previously created, and click **Add Datasource**.



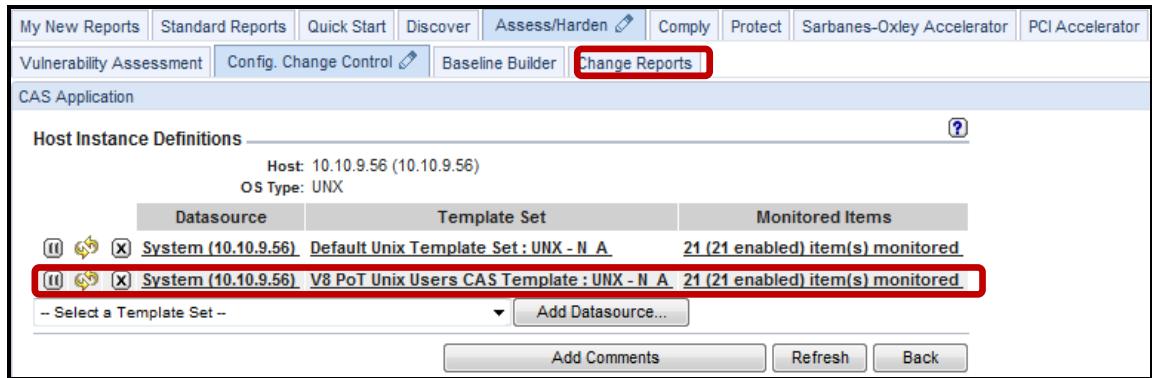
- n. Select **System (10.10.9.56) N A(Change Audit System)**.



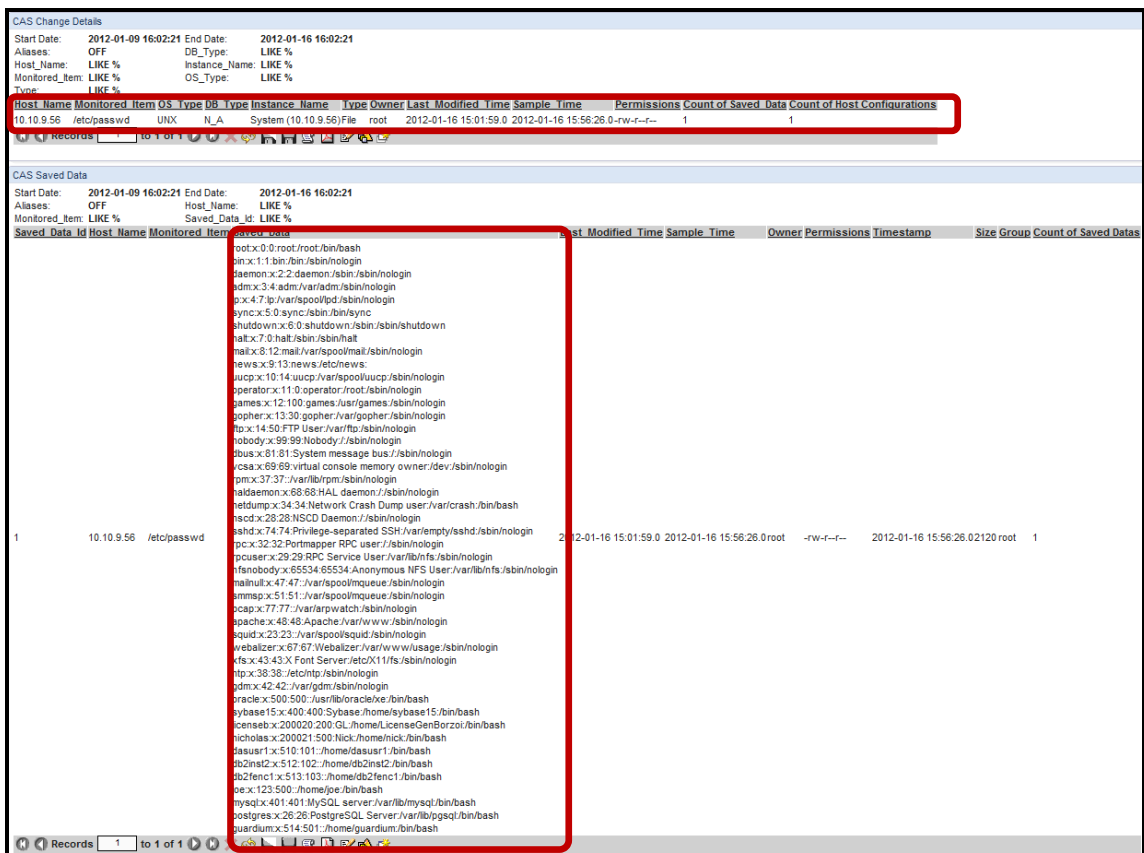
- o. Click **OK** to ignore the warning since a datasource is not required to access a file.



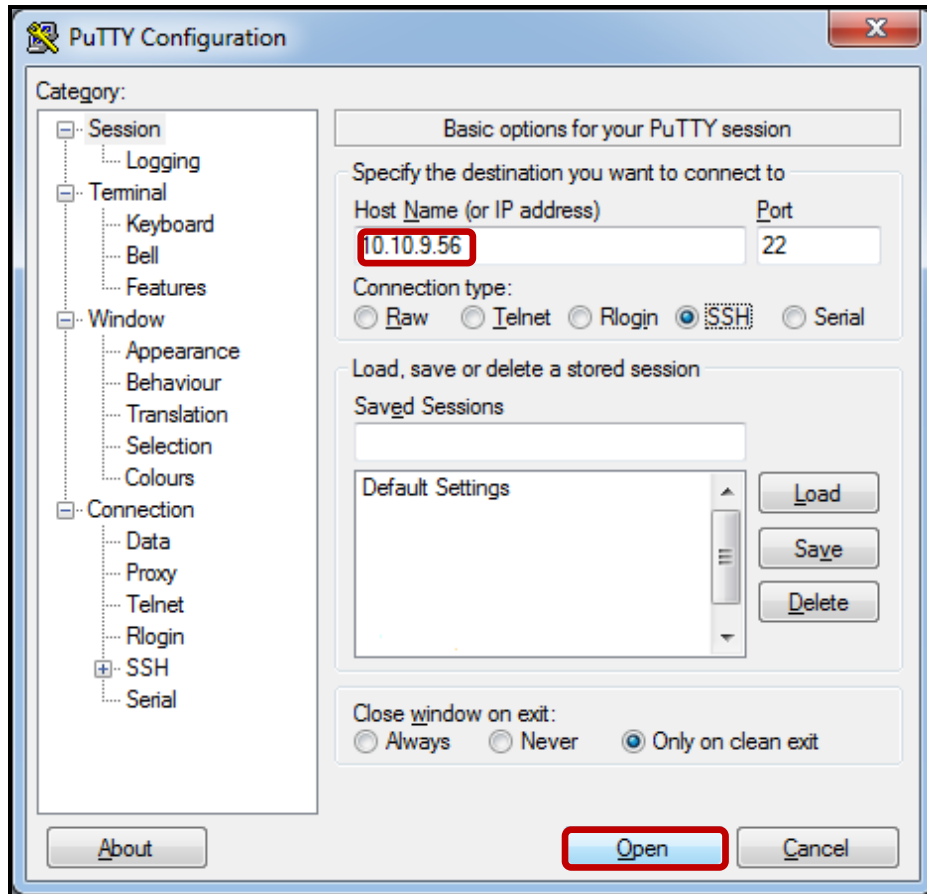
__p. Verify the following screen appears, and then click the **Change Reports** tab.



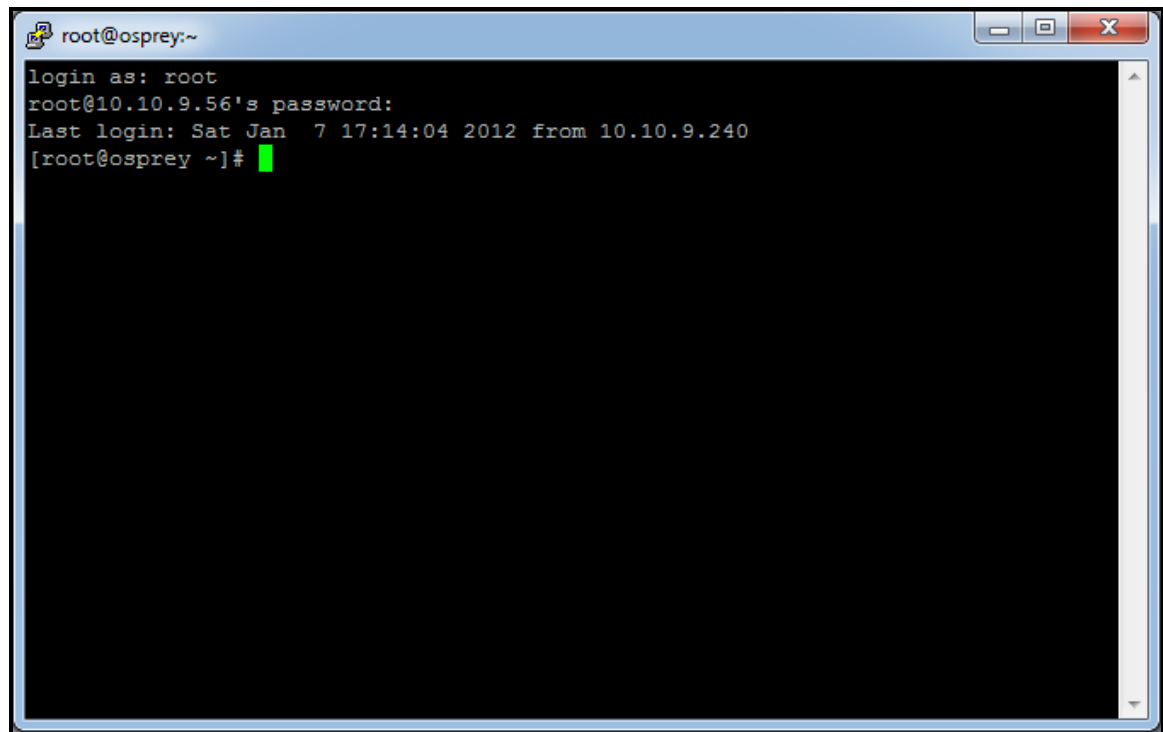
The **Changes** report displays two reports containing the monitored file (/etc/passwd) along with the current contents of the /etc/passwd file.



- __3. Simulate suspicious changes made to the monitored UNIX operating system file using a PuTTY SSH client to access the VM database server.
 - __a. Start the PuTTY SSH client login.
 - __b. From your laptop, launch PuTTY, enter **10.10.9.56**, and click **Open**

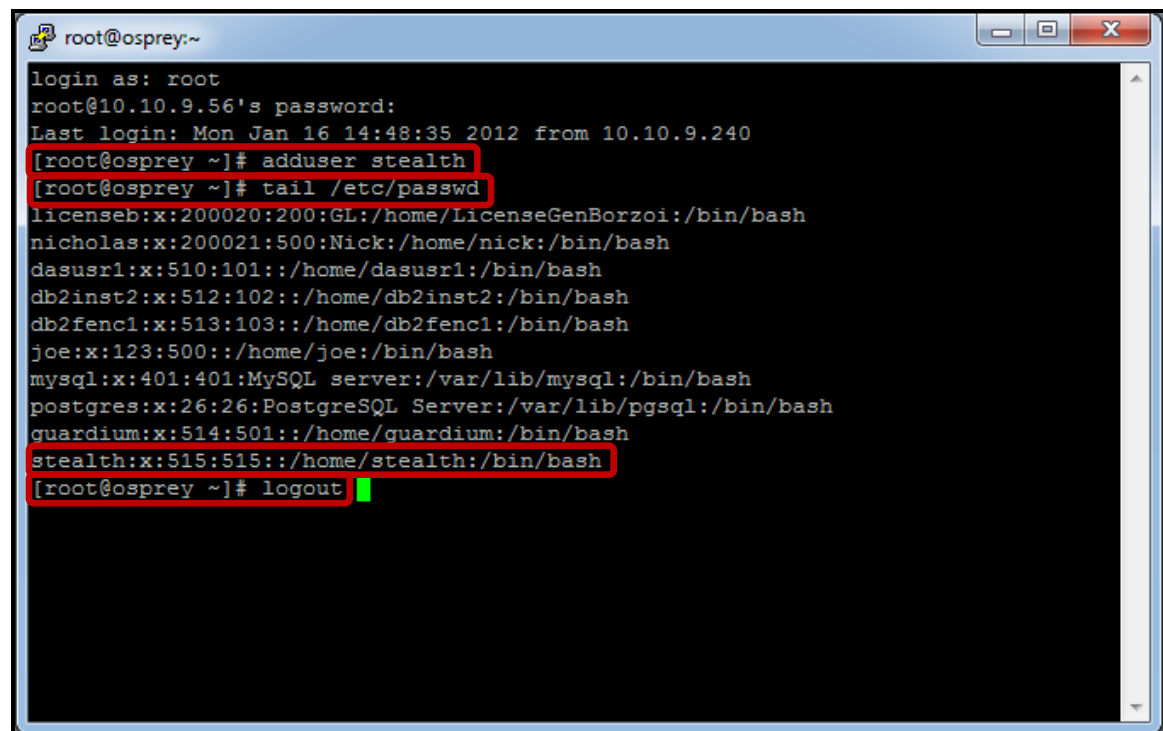


- __c. Login as **root / guardium**. After logging in, the following prompt will be displayed:



```
root@osprey:~  
login as: root  
root@10.10.9.56's password:  
Last login: Sat Jan 7 17:14:04 2012 from 10.10.9.240  
[root@osprey ~]#
```

- __d. Type **adduser stealth**, type **tail /etc/passwd** to confirm the new entry, and then type **logout** to exit.



```
root@osprey:~  
login as: root  
root@10.10.9.56's password:  
Last login: Mon Jan 16 14:48:35 2012 from 10.10.9.240  
[root@osprey ~]# adduser stealth  
[root@osprey ~]# tail /etc/passwd  
licenseb:x:200020:200:GL:/home/LicenseGenBorzoi:/bin/bash  
nicholas:x:200021:500:Nick:/home/nick:/bin/bash  
dasusr1:x:510:101:./home/dasusr1:/bin/bash  
db2inst2:x:512:102:./home/db2inst2:/bin/bash  
db2fenc1:x:513:103:./home/db2fenc1:/bin/bash  
joe:x:123:500:./home/joe:/bin/bash  
mysql:x:401:401:MySQL server:/var/lib/mysql:/bin/bash  
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash  
guardium:x:514:501:./home/guardium:/bin/bash  
stealth:x:515:515:./home/stealth:/bin/bash  
[root@osprey ~]# logout
```

4. Examine Reports to Demonstrate CAS Capabilities.

a. Click the **Change Reports** tab again to run the report. Results may take a minute or so.

CAS Change Details

Start Date: 2012-01-09 16:41:30 End Date: 2012-01-16 16:41:30
 Aliases: OFF DB_Type: LIKE %
 Host_Name: LIKE % Instance_Name: LIKE %
 Monitored_Item: LIKE % OS_Type: LIKE %
 Type: LIKE %

Host Name	Monitored Item	OS Type	DB Type	Instance Name	Type	Owner	Last Modified Time	Sample Time	Permissions	Count of Saved Data	Count of Host Configurations
10.10.9.56	/etc/passwd	UNIX	N_A	System (10.10.9.56)	File	root	2012-01-16 15:01:59.0	2012-01-16 15:56:26.0	-rw-r--	1	1
10.10.9.56	/etc/passwd	UNIX	N_A	System (10.10.9.56)	File	root	2012-01-16 16:37:37.0	2012-01-16 16:38:27.0	-rw-r--	1	1

Records 1 to 2 of 2

CAS Saved Data

Start Date: 2012-01-09 16:41:30 End Date: 2012-01-16 16:41:30
 Aliases: OFF Host_Name: LIKE %
 Monitored_Item: LIKE % Saved_Data_Id: LIKE %

Saved Data Id	Host Name	Monitored Item	Saved Data	Last Modified Time	Sample Time	Owner	Permissions	Timestamp	Size Group	Count of Saved Data	
2	10.10.9.56	/etc/passwd	root:x:0:root:/root:/bin/bash bin:x:1:bin:/bin:/sbin/nologin daemon:x:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/sbin/nologin dbus:x:81:81:System message bus:/sbin/nologin vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin rpm:x:37:37:/var/lib/rpm:/sbin/nologin haldaemon:x:68:68:HAL daemon:/sbin/nologin netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash nsd:x:28:28:NSCD Daemon:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin rpc:x:32:32:Portmapper RPC user:/sbin/nologin rpouser:x:29:29:RPC Service User:/var/lib/rfs:/sbin/nologin nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin mailnull:x:47:47:/var/spool/mqueue:/sbin/nologin smmsp:x:51:51:/var/spool/mqueue:/sbin/nologin pcap:x:77:77:/var/arpwatch:/sbin/nologin apache:x:48:48:Apache:/var/www:/sbin/nologin squid:x:23:23:/var/spool/squid:/sbin/nologin webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin ntp:x:38:38:/etc/ntp:/sbin/nologin gdm:x:42:42:/var/gdm:/sbin/nologin oracle:x:500:500:/usr/lib/oracle/ie:/bin/bash s/ibase15:x:400:400:S/ibase.home/s/ibase15:/bin/bash licenseb:x:200020:200:GL:/home/LicenseGenBorzo:/bin/bash nicholas:x:200021:500:Nick:/home/nick:/bin/bash dasusr1:x:510:101:/home/dasusr1:/bin/bash db2inst2:x:512:102:/home/db2inst2:/bin/bash db2fenc1:x:513:103:/home/db2fenc1:/bin/bash joe:x:123:500:/home/joe:/bin/bash mysql:x:401:401:MySQL server:/var/lib/mysql:/bin/bash postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash guardium:x:514:501:/home/guardium:/bin/bash s/health:x:515:515:/home/s/health:/bin/bash root:x:0:root:/root:/bin/bash bin:x:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/sbin/nologin dbus:x:81:81:System message bus:/sbin/nologin vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin rpm:x:37:37:/var/lib/rpm:/sbin/nologin haldaemon:x:68:68:HAL daemon:/sbin/nologin netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash nsd:x:28:28:NSCD Daemon:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin rpc:x:32:32:Portmapper RPC user:/sbin/nologin rpouser:x:29:29:RPC Service User:/var/lib/rfs:/sbin/nologin nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin mailnull:x:47:47:/var/spool/mqueue:/sbin/nologin smmsp:x:51:51:/var/spool/mqueue:/sbin/nologin pcap:x:77:77:/var/arpwatch:/sbin/nologin apache:x:48:48:Apache:/var/www:/sbin/nologin squid:x:23:23:/var/spool/squid:/sbin/nologin webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin ntp:x:38:38:/etc/ntp:/sbin/nologin gdm:x:42:42:/var/gdm:/sbin/nologin oracle:x:500:500:/usr/lib/oracle/ie:/bin/bash s/ibase15:x:400:400:S/ibase.home/s/ibase15:/bin/bash licenseb:x:200020:200:GL:/home/LicenseGenBorzo:/bin/bash nicholas:x:200021:500:Nick:/home/nick:/bin/bash dasusr1:x:510:101:/home/dasusr1:/bin/bash db2inst2:x:512:102:/home/db2inst2:/bin/bash db2fenc1:x:513:103:/home/db2fenc1:/bin/bash joe:x:123:500:/home/joe:/bin/bash mysql:x:401:401:MySQL server:/var/lib/mysql:/bin/bash postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash guardium:x:514:501:/home/guardium:/bin/bash	2012-01-16 16:37:37.0	2012-01-16 16:38:27.0	root	-rw-r--	2012-01-16 16:38:26.0	2163	root	1
1	10.10.9.56	/etc/passwd	root:x:0:root:/root:/bin/bash bin:x:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/sbin/nologin dbus:x:81:81:System message bus:/sbin/nologin vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin rpm:x:37:37:/var/lib/rpm:/sbin/nologin haldaemon:x:68:68:HAL daemon:/sbin/nologin netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash nsd:x:28:28:NSCD Daemon:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin rpc:x:32:32:Portmapper RPC user:/sbin/nologin rpouser:x:29:29:RPC Service User:/var/lib/rfs:/sbin/nologin nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin mailnull:x:47:47:/var/spool/mqueue:/sbin/nologin smmsp:x:51:51:/var/spool/mqueue:/sbin/nologin pcap:x:77:77:/var/arpwatch:/sbin/nologin apache:x:48:48:Apache:/var/www:/sbin/nologin squid:x:23:23:/var/spool/squid:/sbin/nologin webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin ntp:x:38:38:/etc/ntp:/sbin/nologin gdm:x:42:42:/var/gdm:/sbin/nologin oracle:x:500:500:/usr/lib/oracle/ie:/bin/bash s/ibase15:x:400:400:S/ibase.home/s/ibase15:/bin/bash licenseb:x:200020:200:GL:/home/LicenseGenBorzo:/bin/bash nicholas:x:200021:500:Nick:/home/nick:/bin/bash dasusr1:x:510:101:/home/dasusr1:/bin/bash db2inst2:x:512:102:/home/db2inst2:/bin/bash db2fenc1:x:513:103:/home/db2fenc1:/bin/bash joe:x:123:500:/home/joe:/bin/bash mysql:x:401:401:MySQL server:/var/lib/mysql:/bin/bash postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash guardium:x:514:501:/home/guardium:/bin/bash	2012-01-16 15:01:59.0	2012-01-16 15:56:26.0	root	-rw-r--	2012-01-16 15:56:26.0	2120	root	1

Records 1 to 2 of 2

b. Double-click on the report, and click **View Differences** to inspect changes.

CAS Change Details
 Start Date: 2012-01-09 16:41:30 End Date: 2012-01-16 16:41:30
 Aliases: OFF DB_Type: LIKE %
 Host_Name: LIKE % Instance_Name: LIKE %
 Monitored_Item: LIKE % OS_Type: LIKE %
 Type: LIKE %

Host Name	Monitored_Item	OS_Type	DB_Type	Instance_Name	Type	Owner	Last_Modified_Time	Sample_Time	Permissions	Count of Saved_Data	Count of Host Configurations
10.10.9.56	/etc/passwd	UNIX	N/A	System (10.10.9.56)File	root		2012-01-16 15:01:59.0	2012-01-16 15:56:26.0	-rw-r--r--	1	1
10.10.9.56	/etc/passwd	UNIX	N/A	System (10.10.9.56)File	root		2012-01-16 16:37:37.0	2012-01-16 16:38:27.0	-rw-r--r--	1	1

Records 1 to 2 of 2

CAS Saved Data
 Start Date: 2012-01-09 16:41:30 End Date: 2012-01-16 16:41:30
 Aliases: OFF Host_Name: LIKE %
 Monitored_Item: LIKE % Saved_Data_Id: LIKE %

Saved_Data_Id	Host Name	Monitored_Item	Saved_Data	Last_Modified_Time	Sample_Time	Owner	Permissions	Timestamp	Size Group	Count of Saved Data
			/sbin/nologin			adm:x:3:4:adm:/var/adm:/sbin/nologin				
			/sbin/nologin			lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin				
			/sbin/nologin			sync:x:5:0:sync:/sbin:/bin/sync				
			/sbin/shutdown			shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown				
			/sbin/halt			halt:x:7:0:halt:/sbin:/sbin/halt				
			/sbin/nologin			mail:x:8:12:mail:/var/spool/mail:/sbin/nologin				
			/etc/news			news:x:9:13:news:/etc/news				
			/sbin/nologin			uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin				

View Difference

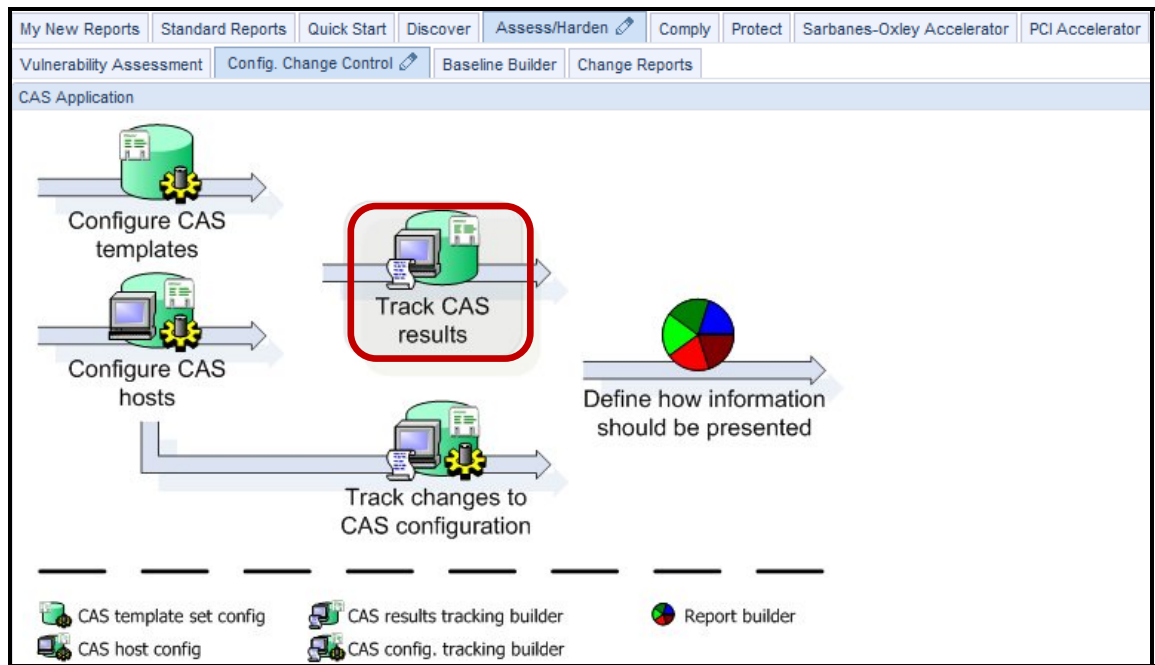
Verify the differences. In this case, a new entry was added on line 47.

c. When finished reviewing the results, cancel the window.

Selected Record Differences		Newer record	Earlier record	Changed
	Newer record 1/16/12 4:38 PM		Earlier record 1/16/12 3:56 PM	
	Line 42		Line 42	
42	db2fenc1:x:513:103::/home/db2fenc1:/bin/bash		42 db2fenc1:x:513:103::/home/db2fenc1:/bin/bash	
43	joe:x:123:500::/home/joe:/bin/bash		43 joe:x:123:500::/home/joe:/bin/bash	
44	mysql:x:401:401:MySQL server:/var/lib/mysql:/bin/bash		44 mysql:x:401:401:MySQL server:/var/lib/mysql:/bin/bash	
45	postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash		45 postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash	
46	guardium:x:514:501::/home/guardium:/bin/bash		46 guardium:x:514:501::/home/guardium:/bin/bash	
47	stealth:x:515:515::/home/stealth:/bin/bash			

__5. Create a Custom Report to Alert of New Changes Based upon the CAS Template.

__a. Click **Track CAS results** under the **Config. Change Control** tab.



__b. Click **New**.

__c. Enter '**V8 PoT CAS Alert Query**' for the *Query Name* field, select **Host Configuration** from the *Main Entity* drop-down list, and then click **Next**.

- __d. Enter the fields from the links on the left (in the same order) and add a condition for the host-name as shown.

Note – Recall from the Custom Reports lab that when you click an attribute, a context menu appears with two selections: one to add the attribute to the Query Fields and the other to add the attribute to the Query Conditions.

- __e. Click **Save**, click **Add to My New reports** and then click **OK** to acknowledge the popup.

The screenshot shows the 'CAS Application' interface. On the left is an 'Entity List' with folders for 'Monitored Changes', 'Host Configuration', and 'Saved Data'. The main area is titled 'V8 PoT CAS Alert Query' and shows a 'Main Entity: Host Configuration'. Below this is a 'Query Fields' table with columns for Seq., Entity, Attribute, Field Mode, Order-by, Sort Rank, and Descend. The table contains six rows of field selections. Below the table is a 'Query Conditions' section with an 'Addition mode' dropdown set to 'AND' and a 'WHERE' clause: 'Host Configuration --- Host_Name = Value 10.10.9.56'. At the bottom right, there are buttons for 'Delete', 'Clone', 'Roles...', 'Save', and 'Back'. The 'Save' button is highlighted with a red box. Below these buttons are 'Generate Tabular', 'Regenerate', 'Add to Pane...', and 'Add to My New Reports' buttons, with the last one also highlighted with a red box.

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Monitored Changes	Owner	Value	<input type="checkbox"/>	
<input type="checkbox"/>	2	Host Configuration	Host_Name	Value	<input type="checkbox"/>	
<input type="checkbox"/>	3	Host Configuration	Monitored_Item	Value	<input type="checkbox"/>	
<input type="checkbox"/>	4	Monitored Changes	Owner	Value	<input type="checkbox"/>	
<input type="checkbox"/>	5	Monitored Changes	Permissions	Value	<input type="checkbox"/>	
<input type="checkbox"/>	6	Saved Data	Timestamp	Value	<input type="checkbox"/>	

The screenshot shows a 'Message from webpage' dialog box with a yellow warning icon. The text inside the box reads 'Report added to My New Reports pane'. At the bottom right of the dialog is an 'OK' button, which is highlighted with a red box.

f. Click the **V8 PoT CAS Alert Query** report under the **My New Reports** tab.

The results from the most recent run will be displayed

The screenshot displays the IBM InfoSphere Guardium V8.2 interface. At the top, there is a navigation bar with tabs: My New Reports (selected), Standard Reports, Quick Start, Discover, Assess/Harden, Comply, Protect, Sarbanes-Oxley Accelerator, and PCI Accelerator. On the left side, there is a sidebar menu with options: AdminConsole, Build Queries and Reports, -Activity Report, -Exceptions Report, -Messages Report, and V8 PoT CAS Alert Query (selected). The main content area shows the details of the V8 PoT CAS Alert Query report. It includes the Start Date: 2012-01-16 14:25:14 and End Date: 2012-01-16 17:25:14, and Aliases: OFF. Below this is a table with the following data:

Owner	Host Name	Monitored Item	Owner	Permissions	Timestamp
root	10.10.9.56	/etc/passwd	root	-rw-r--r--	2012-01-16 15:56:26.0
root	10.10.9.56	/etc/passwd	root	-rw-r--r--	2012-01-16 16:38:26.0

At the bottom of the table, there is a pagination control showing "Records 1 to 2 of 2" and various icons for navigation and actions.

Thank You

Configuration Audit System (CAS) review

- __1. The CAS process runs on:
- __a. The InfoSphere Guardium Collector.
 - __b. The database server.
 - __c. The client PC.
 - __d. A network switch.
- __2. CAS can detect and alert on changes as they happen.
(**True** or **False**).
- __3. CAS would NOT be useful for monitoring which of the following:
- __a. OS Script results.
 - __b. Specific files.
 - __c. All files matching a pattern.
 - __d. Database script results.
 - __e. Network activity.
- __4. CAS can add a substantial load to the database system.
(**True** or **False**).
- __5. Multiple CAS templates can be assigned to a host.
(**True** or **False**).
- __6. CAS cannot monitor files at which level:
- __a. MD5.
 - __b. Owner/group, date modified, size.
 - __c. Zip.
 - __d. File text contents.

Configuration Audit System (CAS) review (Answers)

__1. The CAS process runs on:

B – The database server.

__2. CAS can detect and alert on changes as they happen.
(**True** or **False**).

False.

__3. CAS would NOT be useful for monitoring which of the following:

E – Network activity (since it may change frequently).

__4. CAS can add a substantial load to the database system.
(**True** or **False**).

False.

__5. Multiple CAS templates can be assigned to a host.
(**True** or **False**).

True.

__6. CAS cannot monitor files at which level:

C – ZIP.

Lab 10 Correlation Alerts

10.1 Exploring Correlation Alerts

Overview

The Alerter subsystem transmits messages that have been queued by other components: for example, correlation alerts that have been queued by the Anomaly Detection subsystem, or run-time alerts that have been generated by security policies. The Alerter subsystem can be configured to send messages to both SMTP and SNMP servers. Alerts can also be sent to syslog or custom alerting classes, but no special configuration is required for those two options beyond starting the Alerter. There are four types of Alerter commands.

An alert is a message indicating that an exception or policy rule violation was detected. Alerts are triggered in two ways:

- A **Correlation Alert** is triggered by a query that looks back over a specified time period to determine if an alert threshold has been met. The IBM InfoSphere® Guardium® Anomaly Detection Engine runs correlation queries on a scheduled basis. By default, correlation alerts do not log Policy violations, but they can be configured to do so.
- A **Real-Time** alert is triggered by a security policy rule. The InfoSphere Guardium Inspection Engine component runs the security policy as it collects and analyzes database traffic in real time.

Objectives

This Lab will illustrate how we can create Correlation Alert using the InfoSphere Guardium GUI. The following objectives will be targeted:

- __1. Create a report to detail those instances where records affected ≥ 100 .
- __2. Define thresholds to alert upon.
- __3. Issue SQL statements to trigger alert.
- __4. View report to verify there was a policy violation.
- __5. Verify Incident Management report logged the incident.

- __1. Using the InfoSphere Guardium GUI, demonstrate the ease of use within the InfoSphere Guardium solution. Start the InfoSphere Guardium appliance and login.
 - __a. From your laptop, go to <https://10.10.9.248:8443>
 - __b. Login as **pot / guardium**.

Login

Please enter your information

User name:

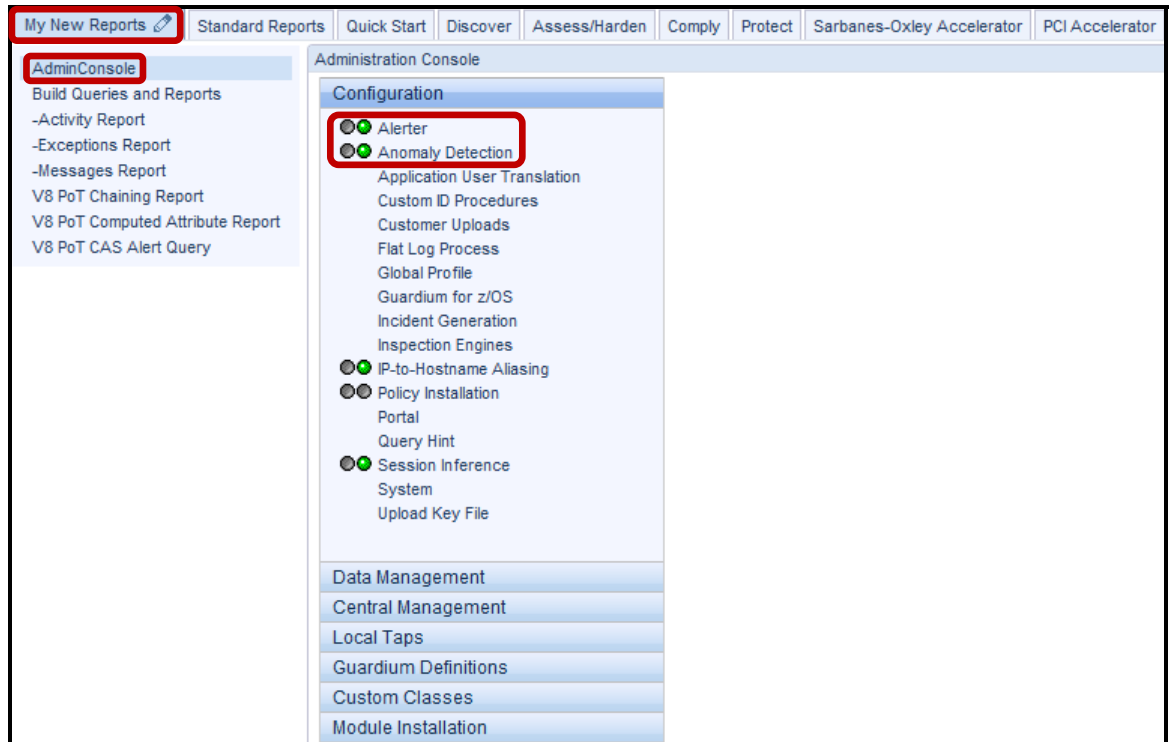
Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

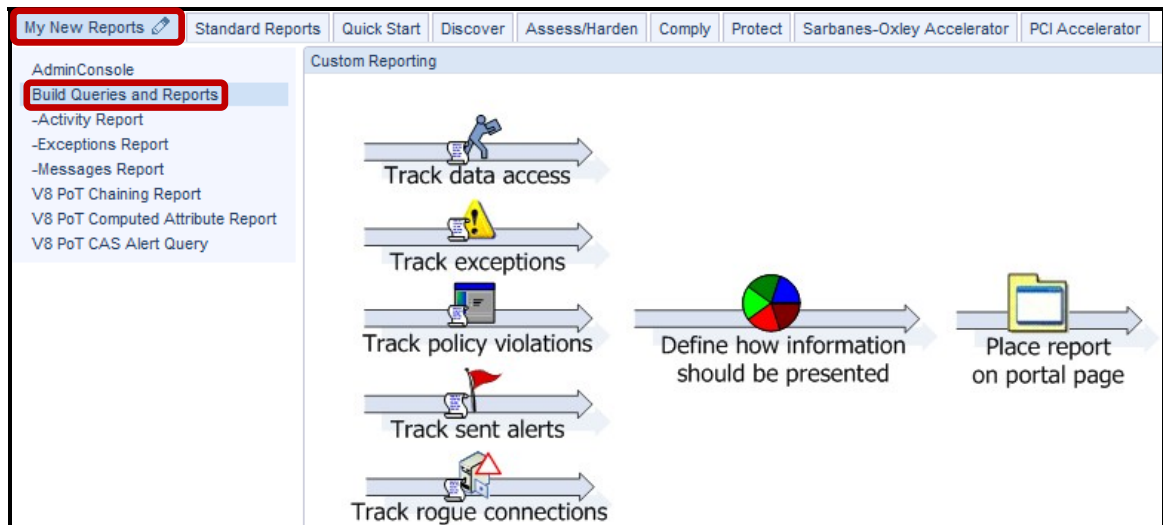
CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistrykey © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

- c. Click **AdminConsole** under the **My New Reports** tab to confirm that the **Alerter** and **Anomaly Detection** are both active and running (indicated by green).

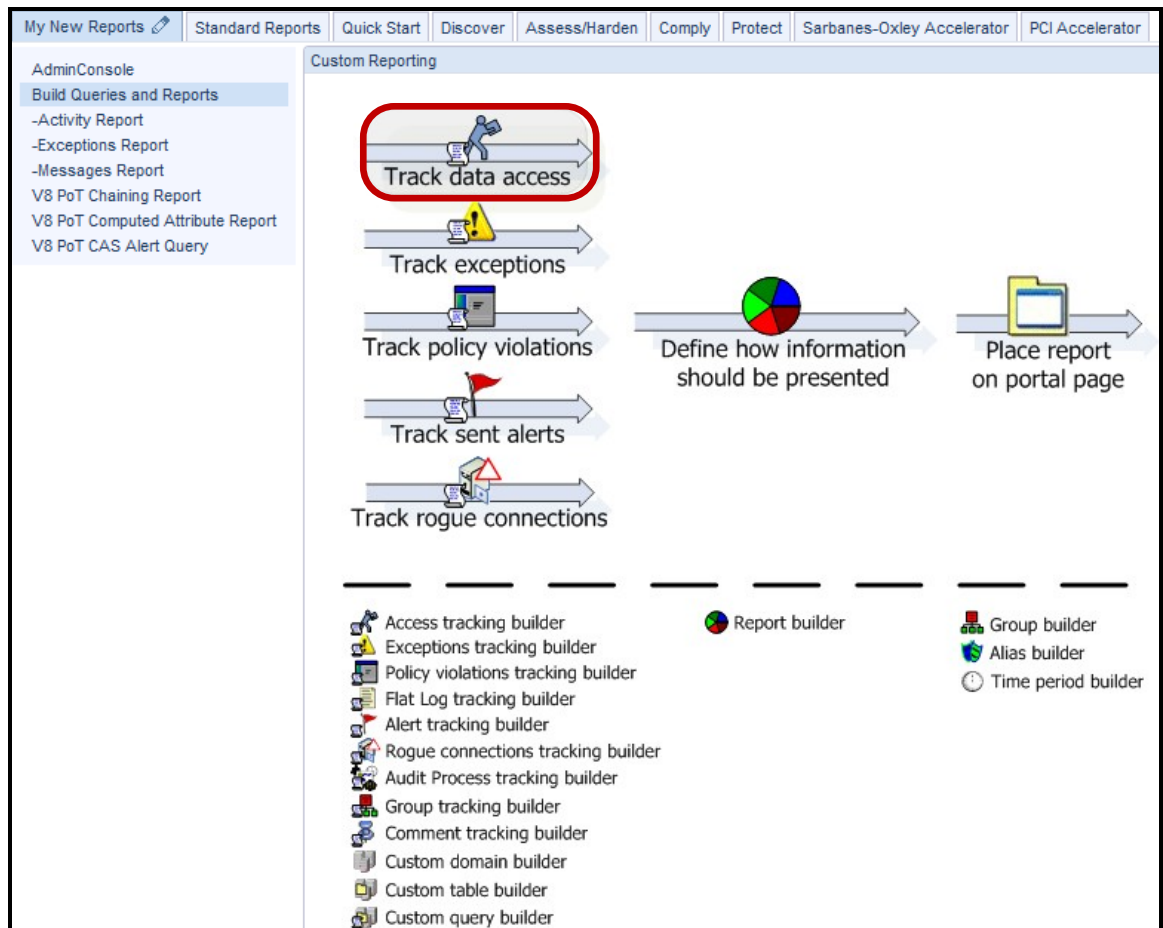


__2. Create a report to monitor result sets containing an excessive amount of SQL records.

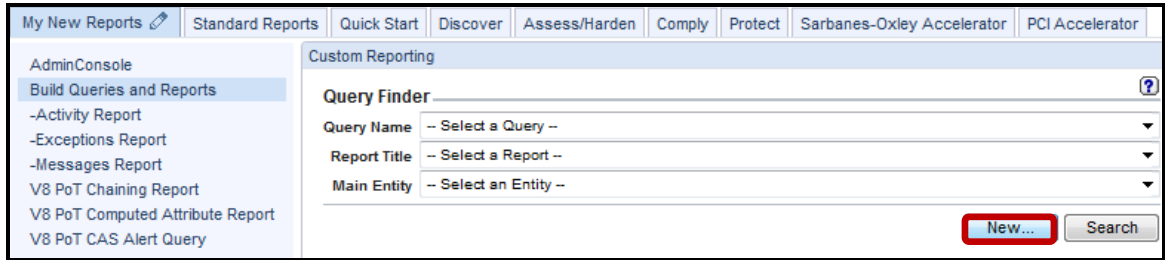
__a. Click **Build Queries and Reports** under the **My New Reports** tab.



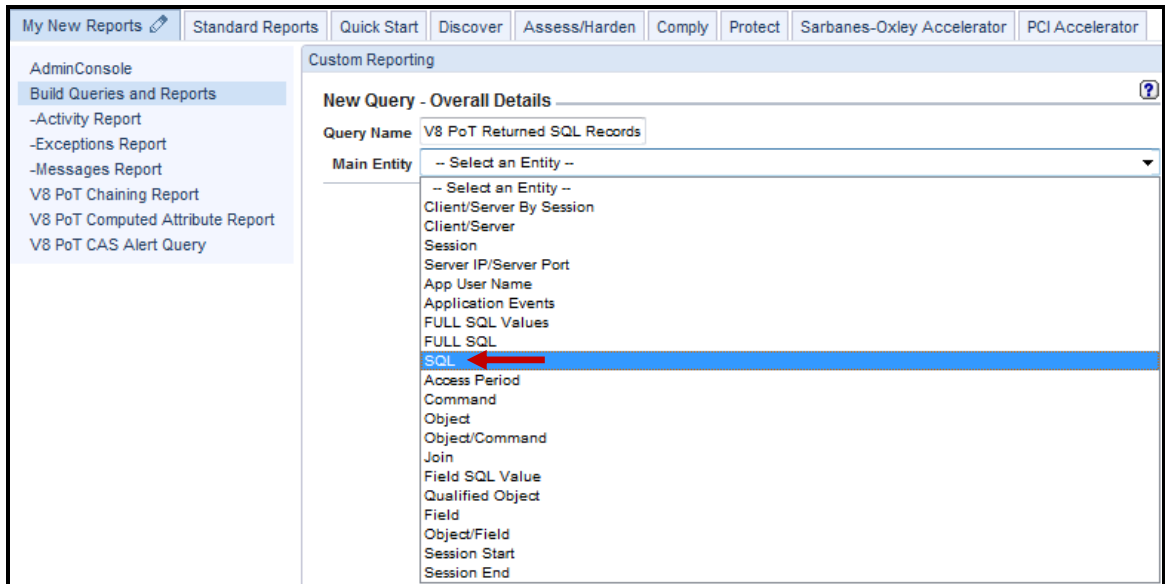
__b. Click **Track data access**.



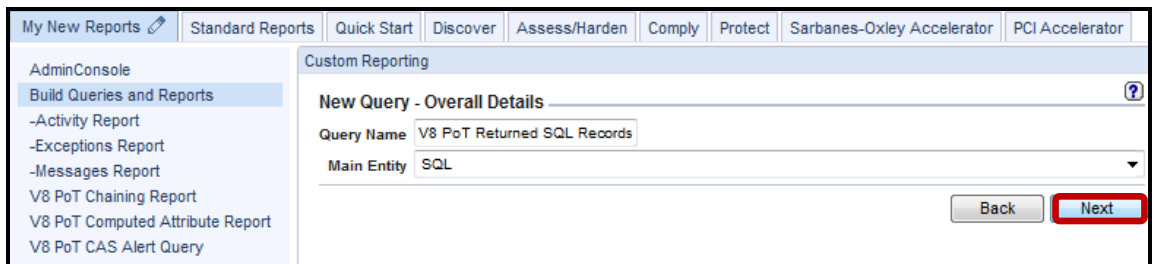
__c. Click **New**.



__d. Enter 'V8 PoT Returned SQL Records' for the *Query Name* and Select **SQL** from the *Main Entity* drop-down list.

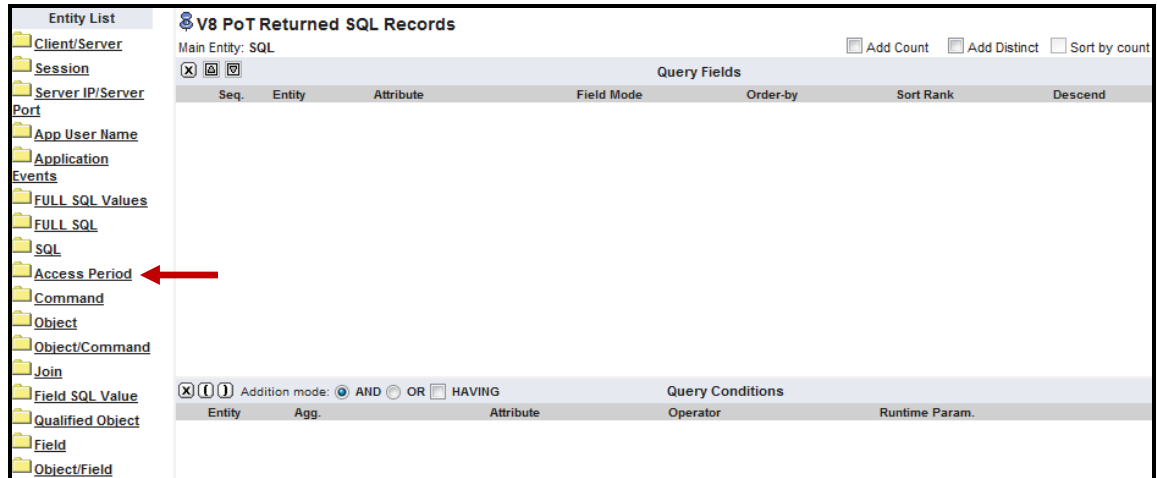


__e. Click **Next**.

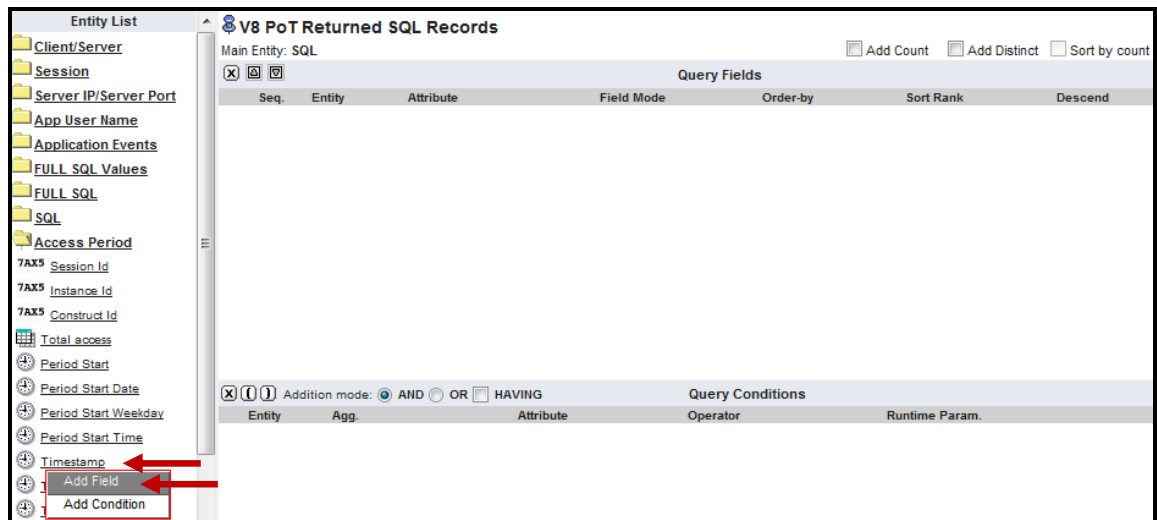


__3. The next few steps will add Custom *Query Fields* for the **V8 PoT Returned SQL Records** report.

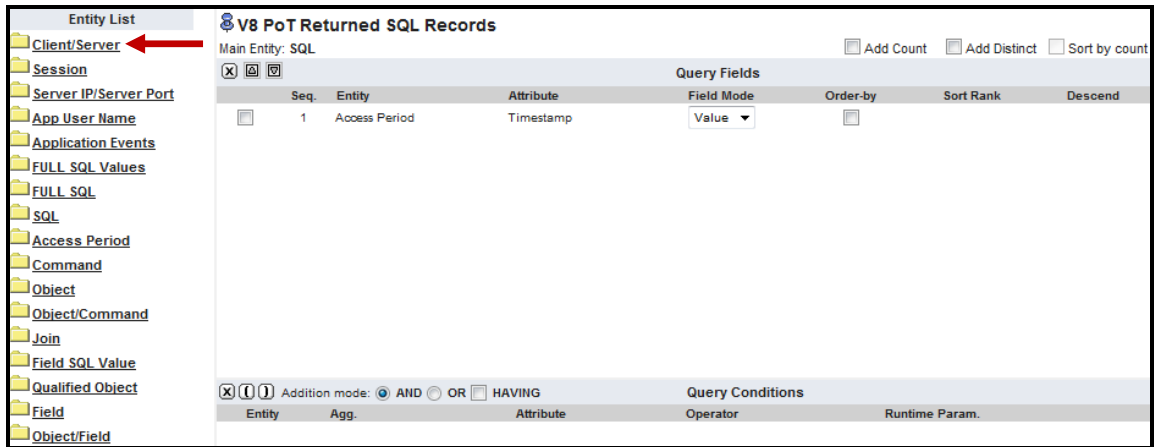
__a. Select **Access Period** from *Entity List*.



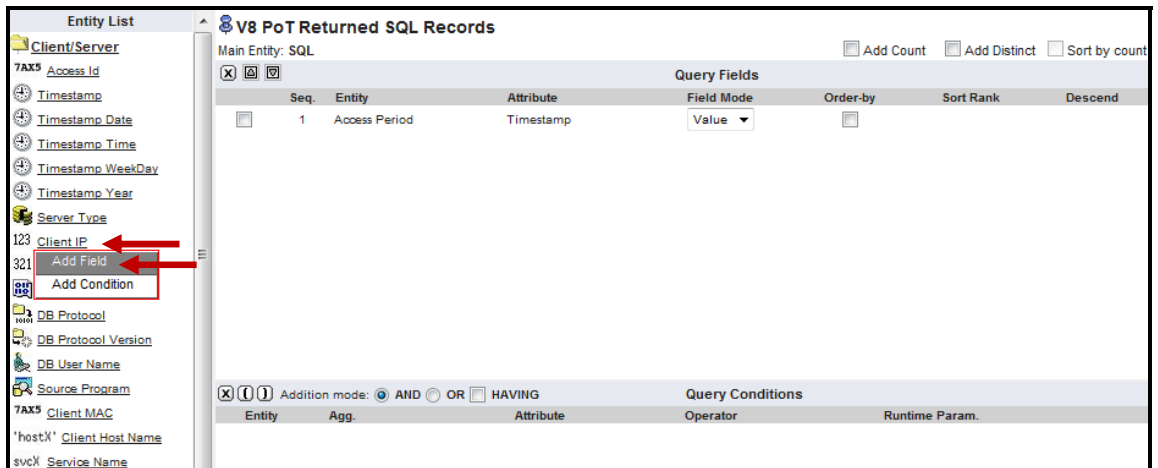
__b. Select the **Timestamp** attribute from *Access Period* entity and click **Add Field**. Then, select **Access Period** from the *Entity List* to collapse the **Access Period** folder.



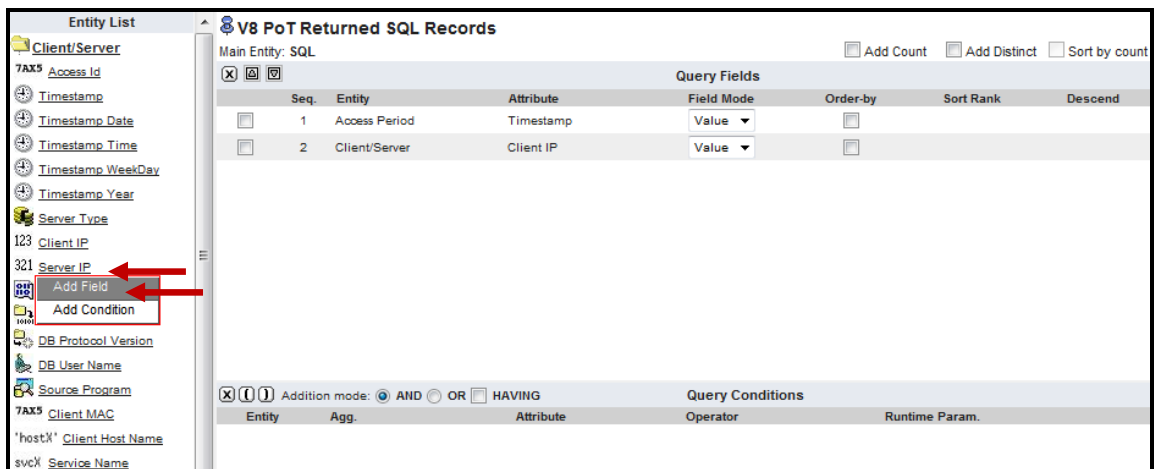
c. Now select **Client Server** from *Entity List*.



d. Select the **Client IP** attribute from the *Client/Server* entity and click **Add Field**.



e. Select the **Server IP** attribute from the *Client/Server* entity and click **Add Field**. Then, select **Client/Server** from the *Entity List* to collapse the **Client/Server** folder.



__f. Now select **FULL SQL** from *Entity List*.

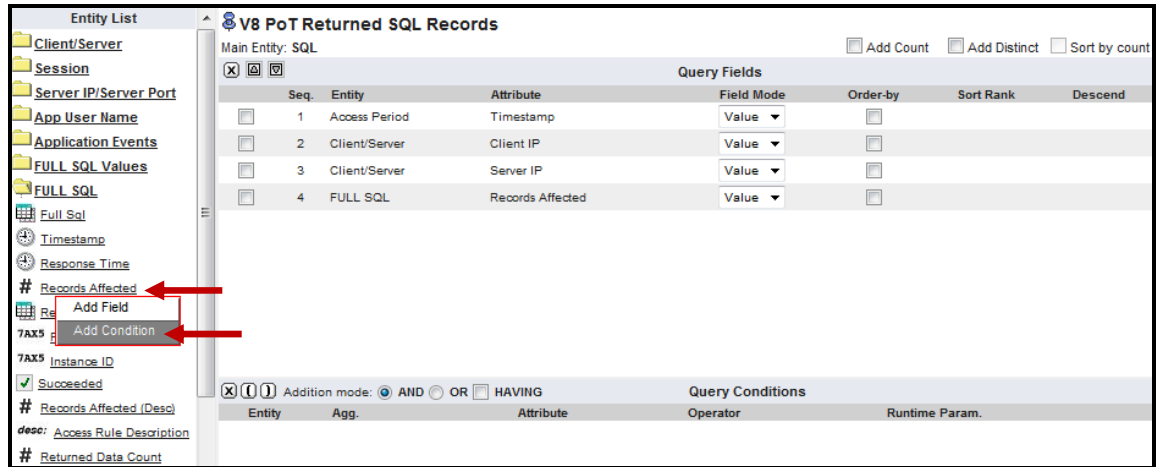
The screenshot shows the 'V8 PoT Returned SQL Records' interface. On the left, the 'Entity List' is expanded to show 'FULL SQL' with a red arrow pointing to it. The main area displays a table with the following data:

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
1	Access Period	Timestamp	Value			
2	Client/Server	Client IP	Value			
3	Client/Server	Server IP	Value			

__g. Select the **Records Affected** attribute from the *FULL SQL* entity and click **Add Field**.

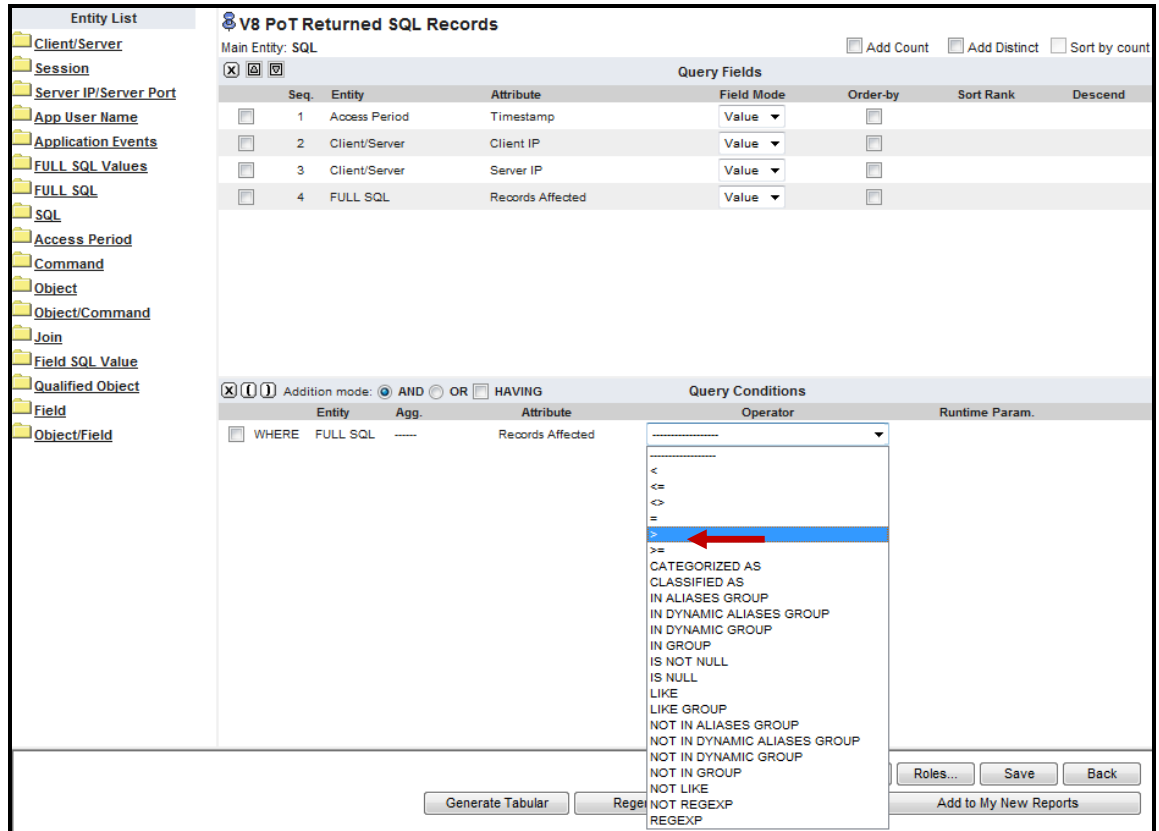
The screenshot shows the 'V8 PoT Returned SQL Records' interface. In the 'Entity List' on the left, 'Records Affected' is selected with a red arrow. Below it, the 'Add Field' button is highlighted with a red box and a red arrow. The main table remains the same as in the previous screenshot.

- ___4. The next few steps will add Custom *Conditions* for the **V8 PoT Returned SQL Records** report.
 - ___a. Now, select the **Records Affected** attribute from the *FULL SQL* entity and click **Add Condition**. Then, select **FULL SQL** from the *Entity List* to collapse the **FULL SQL** folder.

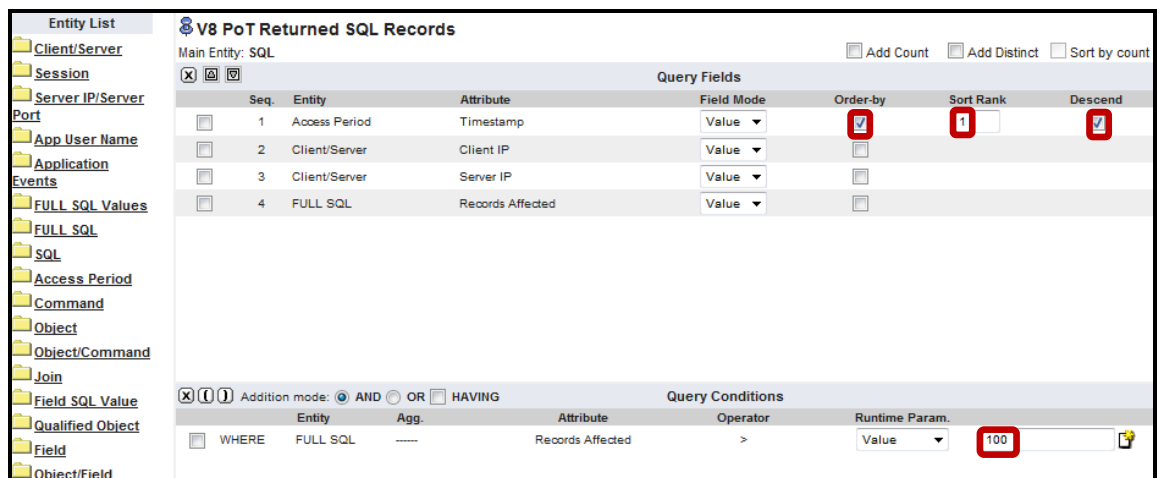


__5. The next few steps will configure *Query Conditions Operators and Runtime Parameters* for the **V8 PoT Returned SQL Records** report.

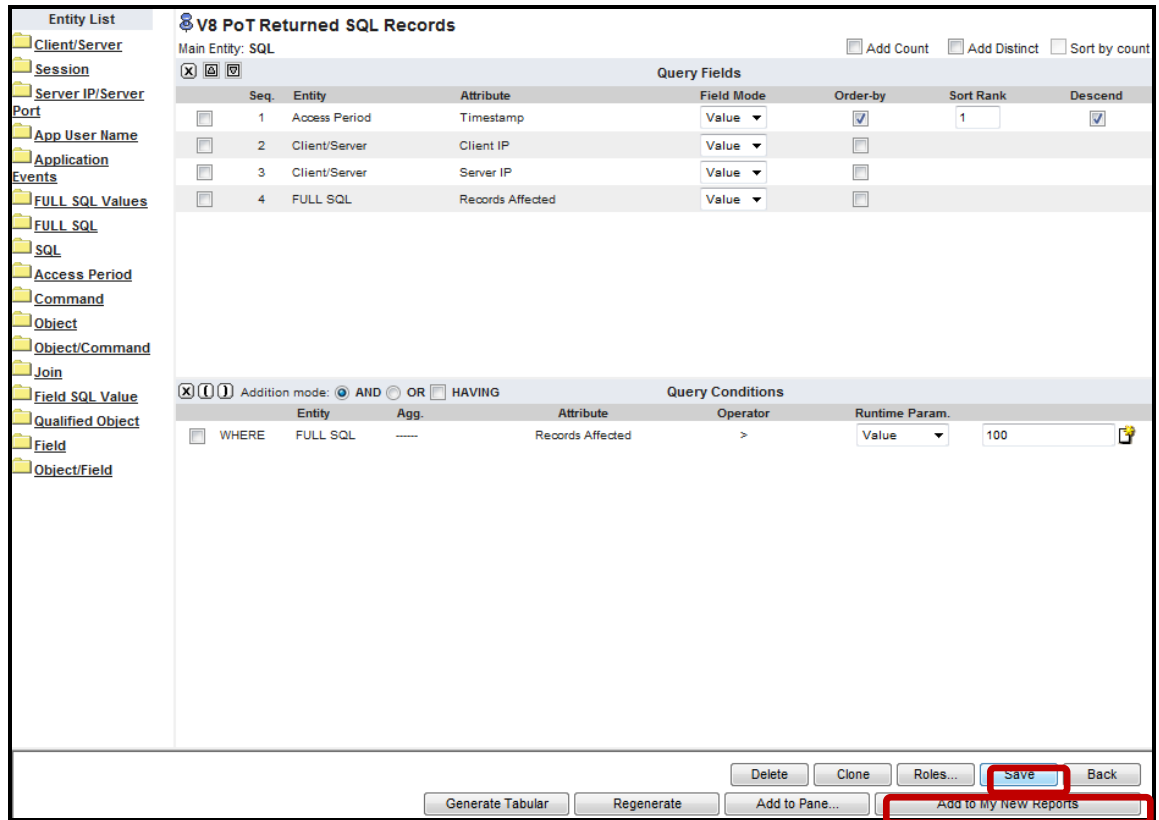
__a. Select '>' from the *Query Conditions Operator* drop-down list for the *Records Affected* attribute. You can also type '>' to quickly select.



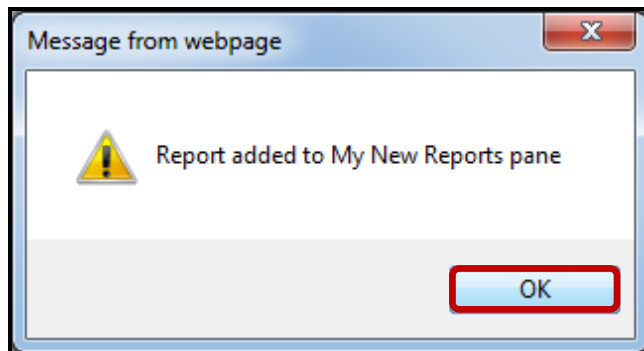
__b. Now, add a value of '100' to report only upon result sets of more than 100 records. Then, check the *Order-by* checkbox, enter '1' in the *Sort Rank* box, and check the *Descend* checkbox.




__c. Click **Save** and click **Add to My New Reports** to add it to the **My New Reports** pane.

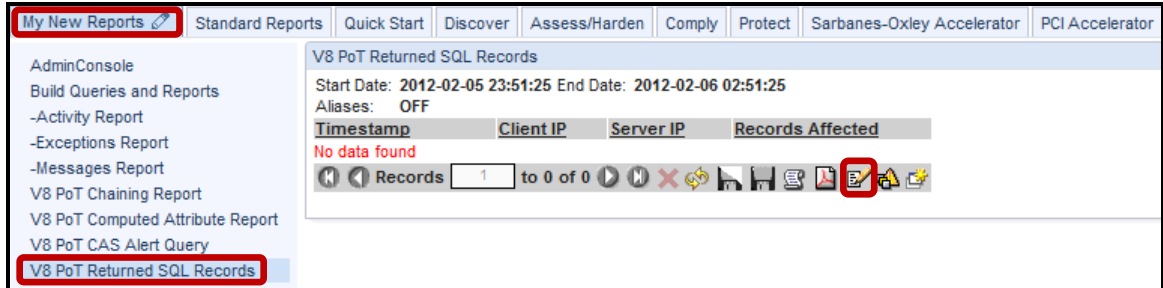


__d. Click **OK** to acknowledge the report has been added to the **My New Reports** pane.

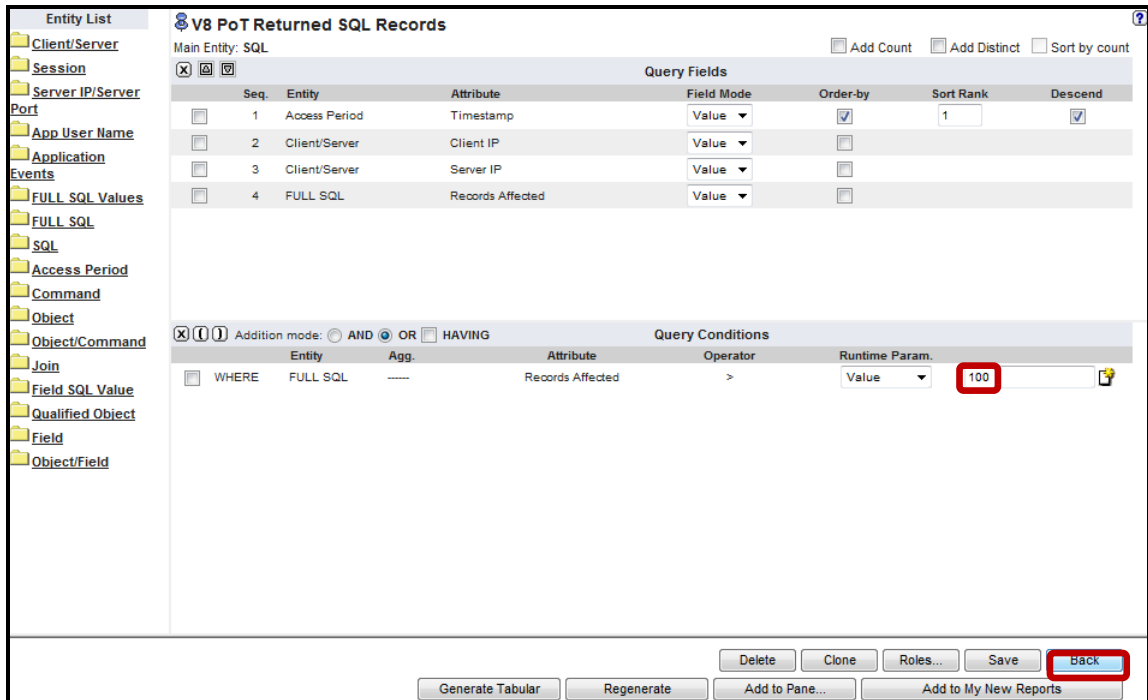


__6. Configure the **V8 PoT Returned SQL Records** report.

- __a. Click **V8 PoT Returned SQL Records** under the **My New Reports** tab, and then click the  icon to edit the query definition.



- __b. The alert Threshold **can be edited if desired**. It is currently set to 100 Records. You can enter a new value and click **Save** to change the current number. Click **Back** to return.



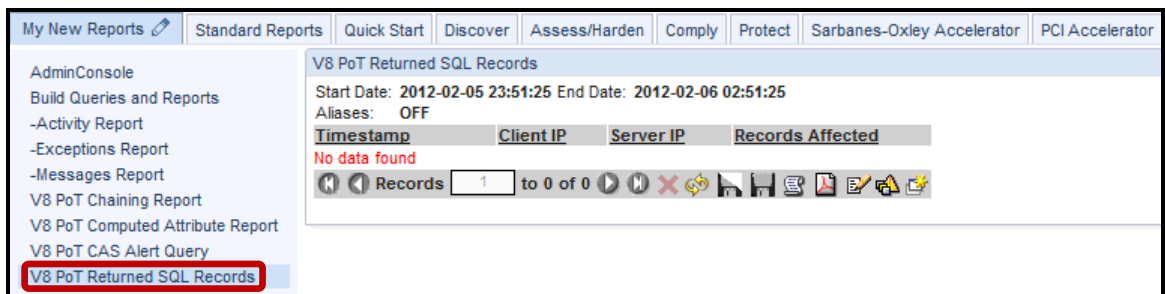
c. Next, click the  icon at on the upper right.



d. The *QUERY_FROM_DATE* is set to **NOW -3 HOUR** and the *QUERY_TO_DATE* is set to **NOW**. To edit, select new ranges and click **Update**. Otherwise, click **Cancel** to return.

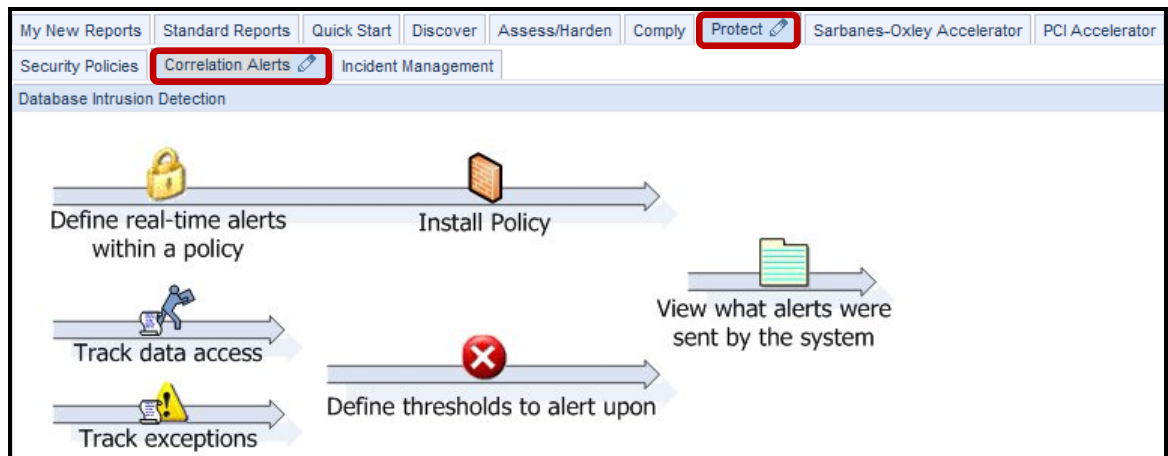


e. Click **SQL Records Returned** to manually run report. The report will be empty since the alert has yet to be triggered.

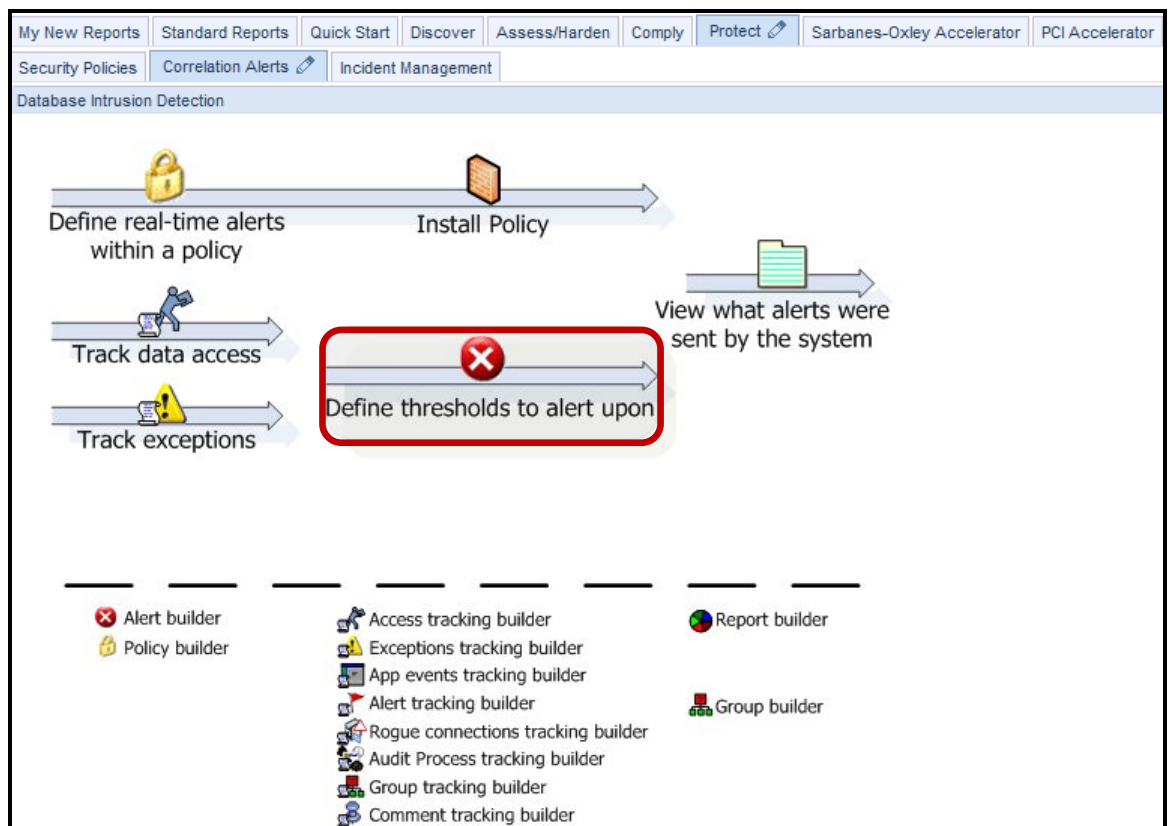


__7. Create a new Correlation Alert.

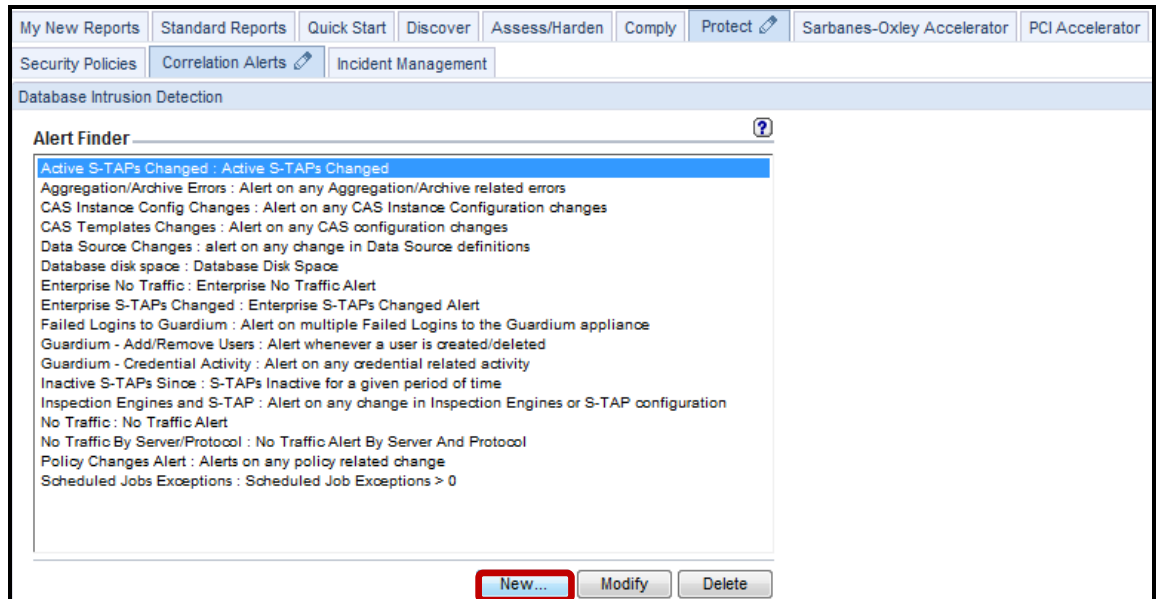
__a. Click **Correlation Alerts** under the **Protect** tab.



__b. Click **Define thresholds to alert upon**.



__c. Click **New** to configure the alert settings.



- d. Enter **V8 PoT Returned Records** for the *Name* field and **Alert on Excess Records** for the *Description* field, **SOX** for the *Category* field **Threshold Alert** for the *Classification* field, and then select **HIGH** from the *Severity* drop-down list.

Note: For an email alert, a **HIGH** Severity results in the email being flagged as urgent.

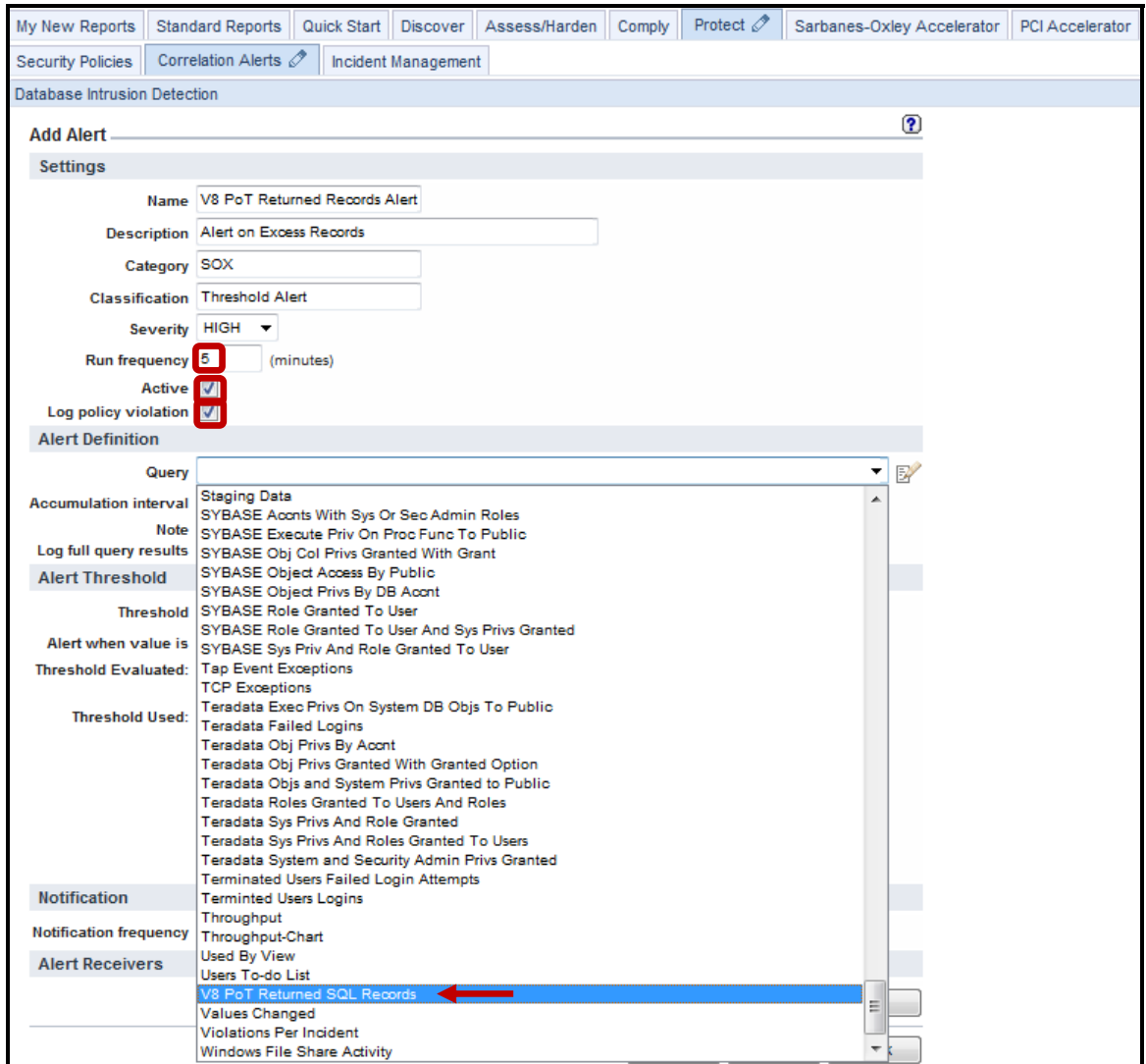
The screenshot displays the 'Add Alert' configuration interface within the 'Database Intrusion Detection' section. The 'Settings' tab is active, showing the following configuration details:

- Name:** V8 PoT Returned Records Alert
- Description:** Alert on Excess Records
- Category:** SOX
- Classification:** Threshold Alert
- Severity:** HIGH (selected from a dropdown menu)
- Run frequency:** INFO (minutes)
- Active:** NONE
- Log policy violation:** MED
- Alert Definition:** HIGH
- Query:** (empty field)
- Accumulation interval:** (empty field) (minutes)
- Note:** Alerts run on aggregators will be based only on data within the defined merge period
- Log full query results:**
- Alert Threshold:**
 - Threshold:** (empty field)
 - Alert when value is:** threshold
 - Threshold Evaluated:** per report, per line
 - Threshold Used:** As absolute limit, As percentage change within period:
 - From:** (empty field)
 - To:** (empty field)
 - As percentage change for the same "Accumulation Period" on a relative time:
 - Ending at:** (empty field)
- Notification:**
 - Notification frequency:** (empty field) (minutes)
- Alert Receivers:** (empty list)

Buttons at the bottom include 'Add Receiver...', 'Roles...', 'Apply', and 'Back'.

- e. Enter **5** (minutes) for the **Run frequency** field, check the **Active** checkbox, check the **Log policy violation** checkbox, and then select **V8 PoT Returned SQL Records** from the *Query* drop-down list.

Note: Run Frequency is the number of minutes between executions of the query.



- ___f. Enter **10** (minutes) for the *Accumulation interval* field, enter **0** for the Threshold field, and then select '>' from the **Alert when value is** drop-down list.

Note: The **Accumulation Interval** is the span of time over which the query should evaluate the query results, counting back from the current time.

The screenshot displays the 'Add Alert' configuration page in the IBM Security Center for Protection. The interface includes a navigation bar at the top with options like 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below this, there are tabs for 'Security Policies', 'Correlation Alerts', and 'Incident Management'. The main content area is titled 'Database Intrusion Detection' and contains the following sections:

- Settings:**
 - Name: V8 PoT Returned Records Alert
 - Description: Alert on Excess Records
 - Category: SOX
 - Classification: Threshold Alert
 - Severity: HIGH
 - Run frequency: 5 (minutes)
 - Active:
 - Log policy violation:
- Alert Definition:**
 - Query: V8 PoT Returned SQL Records
 - Accumulation interval: 10 (minutes)
 - Note: Alerts run on aggregators will be based only on data within the defined merge period
 - Log full query results:
 - Column: (optional)
- Alert Threshold:**
 - Threshold: 0
 - Alert when value is: >
 - Threshold Evaluated: <, <=, >, >=
 - Threshold Used: >
 - As percentage change within period:
 - Ending at: (calendar icon)
- Notification:**
 - Notification frequency: (minutes)
- Alert Receivers:**
 - Add Receiver..

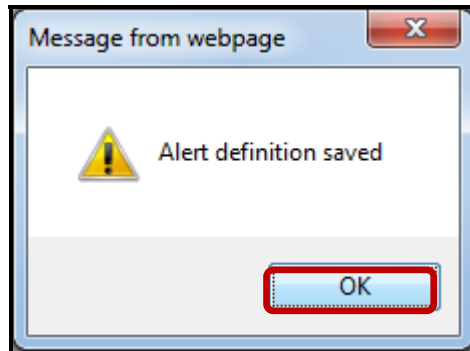
At the bottom of the page, there are buttons for 'Roles...', 'Apply', and 'Back'.

__g. Enter **10** (minutes) for the *Notification Frequency* field, and click **Apply**.

Note: The **Notification Frequency** determines how often the Alert Receivers should be notified when the alert condition has been satisfied.

The screenshot shows the 'Add Alert' configuration interface for Database Intrusion Detection. The 'Settings' section includes fields for Name, Description, Category, Classification, Severity, Run frequency (5 minutes), Active, and Log policy violation. The 'Alert Definition' section includes a Query dropdown, Accumulation interval (10 minutes), a Note, Log full query results checkbox, and a Column dropdown. The 'Alert Threshold' section includes a Threshold field (0), Alert when value is dropdown (> threshold), Threshold Evaluated radio buttons (per report, per line), Threshold Used radio buttons (As absolute limit, As percentage change within period), and From/To date pickers. The 'Notification' section includes a Notification frequency field (10 minutes) highlighted with a red box. The 'Alert Receivers' section has an 'Add Receiver..' button. At the bottom right, there are 'Roles...', 'Apply' (highlighted with a red box), and 'Back' buttons.

__h. Click **OK** to acknowledge.



__i. Click **Add Receiver**.

__j. Select **SYSLOG** from the *Notification Type* drop-down list.

__k. Click **Save**.

__l. Click **Apply**.

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

Security Policies | Correlation Alerts | Incident Management

Database Intrusion Detection

Modify Alert ?

Settings

Name: V8 PoT Returned Records Alert
Description: Alert on Excess Records
Category: SOX
Classification: Threshold Alert
Severity: HIGH
Run frequency: 5 (minutes)
Active:
Log policy violation:

Alert Definition

Query: V8 PoT Returned SQL Records
Accumulation interval: 10 (minutes)
Note: Alerts run on aggregators will be based only on data within the defined merge period
Log full query results:
Column: (optional)

Alert Threshold

Threshold: 0
Alert when value is: > threshold
Threshold Evaluated: per report
 per line
Threshold Used: As absolute limit
 As percentage change within period:
From: To:
 As percentage change for the same "Accumulation Period" on a relative time:
Ending at:

Notification

Notification frequency: 10 (minutes)

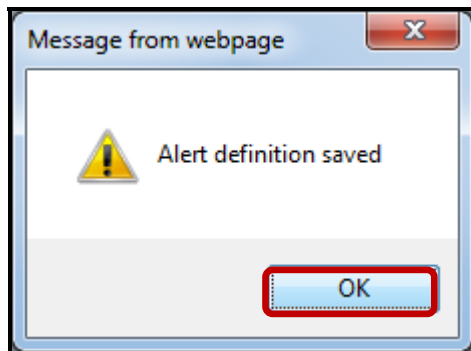
Alert Receivers

SYSLOG [Delete](#)

[Add Receiver..](#)

[Add Comments](#) [Roles...](#) **Apply** [Back](#)

__m. Click **OK** to acknowledge.



__n. Click **Back** to exit.

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

Security Policies | Correlation Alerts | Incident Management

Database Intrusion Detection

Modify Alert ?

Settings

Name: V8 PoT Returned Records Alert

Description: Alert on Excess Records

Category: SOX

Classification: Threshold Alert

Severity: HIGH

Run frequency: 5 (minutes)

Active:

Log policy violation:

Alert Definition

Query: V8 PoT Returned SQL Records

Accumulation interval: 10 (minutes)

Note: Alerts run on aggregators will be based only on data within the defined merge period

Log full query results:

Column: (optional)

Alert Threshold

Threshold: 0

Alert when value is: > threshold

Threshold Evaluated: per report
 per line

Threshold Used: As absolute limit
 As percentage change within period:
 From:
 To:

As percentage change for the same "Accumulation Period" on a relative time:
 Ending at:

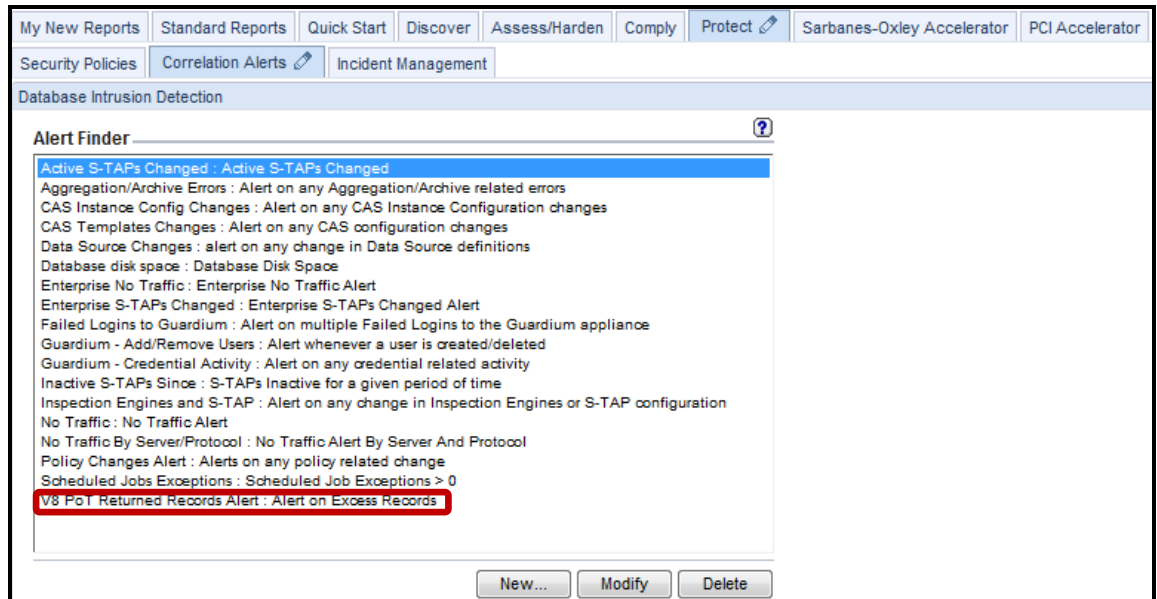
Notification

Notification frequency: 10 (minutes)

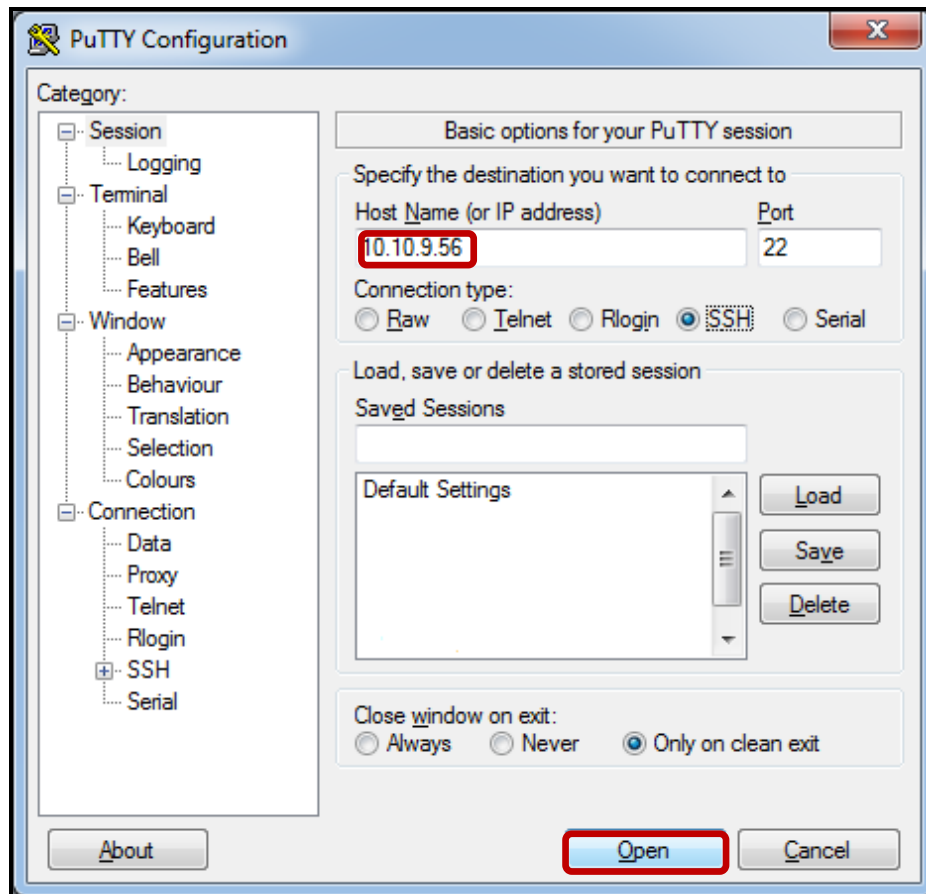
Alert Receivers

SYSLOG [Delete](#)

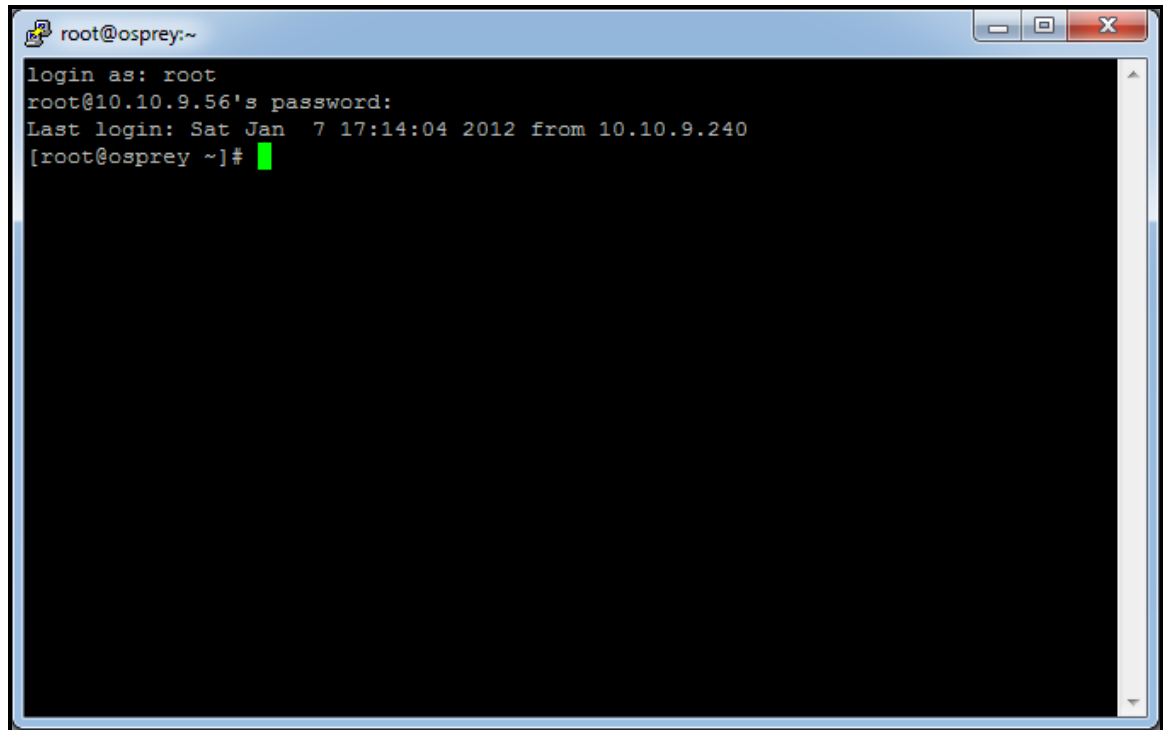
__o. Note that **SQL Records Returned** is now in the *Alert Finder* section.



- __8. Using a PuTTY SSH client, access the VM database server to demonstrate the ease with which the InfoSphere Guardium solution can audit Returned SQL Records.
- __a. Start the PuTTY SSH client login.
 - __b. From your laptop, launch PuTTY, enter **10.10.9.56**, and click **Open**.

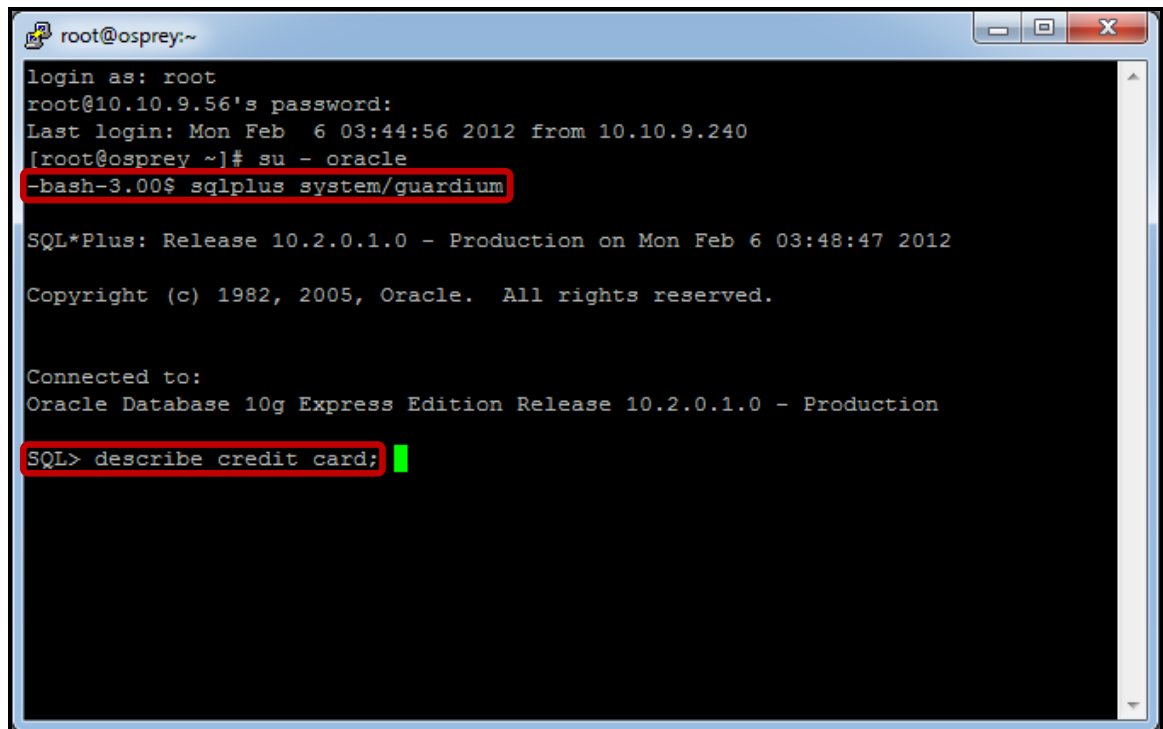


- __c. Login as **root / guardium**. After logging in, the following prompt will be displayed:

A terminal window titled 'root@osprey:~' with standard window controls. The text inside shows a successful login for the 'root' user. The prompt is '[root@osprey ~]#'.

```
root@osprey:~  
login as: root  
root@10.10.9.56's password:  
Last login: Sat Jan 7 17:14:04 2012 from 10.10.9.240  
[root@osprey ~]#
```

- __d. Login as the Oracle DBA account (**su – oracle**). Then, login to Oracle by typing: **sqlplus system/guardium** and then type the SQL Query '**describe credit_card;**'.

A terminal window titled 'root@osprey:~' showing the process of switching to the 'oracle' user and logging into the Oracle database. The 'su - oracle' and 'sqlplus system/guardium' commands are highlighted with red boxes. The Oracle prompt is 'SQL>'.

```
root@osprey:~  
login as: root  
root@10.10.9.56's password:  
Last login: Mon Feb 6 03:44:56 2012 from 10.10.9.240  
[root@osprey ~]# su - oracle  
-bash-3.00$ sqlplus system/guardium  
  
SQL*Plus: Release 10.2.0.1.0 - Production on Mon Feb 6 03:48:47 2012  
Copyright (c) 1982, 2005, Oracle. All rights reserved.  
  
Connected to:  
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production  
SQL> describe credit card;
```

- __e. Type the SQL Query 'select cardid, lastname, cardnumber from credit_card;'.

```

root@osprey:~
[root@osprey ~]# su - oracle
-bash-3.00$ sqlplus system/guardium

SQL*Plus: Release 10.2.0.1.0 - Production on Mon Feb 6 04:39:13 2012

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

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

SQL> describe credit_card;
Name                                                    Null?    Type
-----
CARDID                                                    NOT NULL NUMBER(10)
FIRSTNAME                                                VARCHAR2(15)
LASTNAME                                                 VARCHAR2(15)
CARDNUMBER                                               VARCHAR2(25)
PIN                                                       VARCHAR2(5)
EXP                                                       VARCHAR2(4)
TYPE                                                      VARCHAR2(12)
TRACK1_DATA                                              VARCHAR2(100)

SQL> select cardid, lastname, cardnumber from credit_card;

```

- __f. The select statement returns 1,000 rows. After receiving the result set, type **exit** to exit Oracle sqlplus, and then type **exit** to return to the root user account shell.

```

root@osprey:~
989 Metaxotos      4556490772823202
990 Meyer          5186222524375776

CARDID LASTNAME      CARDNUMBER
-----
991 Meyer          4539972143859389
992 Almonds       4916670600860030
993 Wilson        4556566779998350
994 Wise          5274927648418830
995 Gibson        4539237947998878
996 Harrold       5318879460787990
997 Briggs        5176611227224608
998 Day           4539753697157085
999 Day           5393480349018042
1000 Almonds      5119517756418695

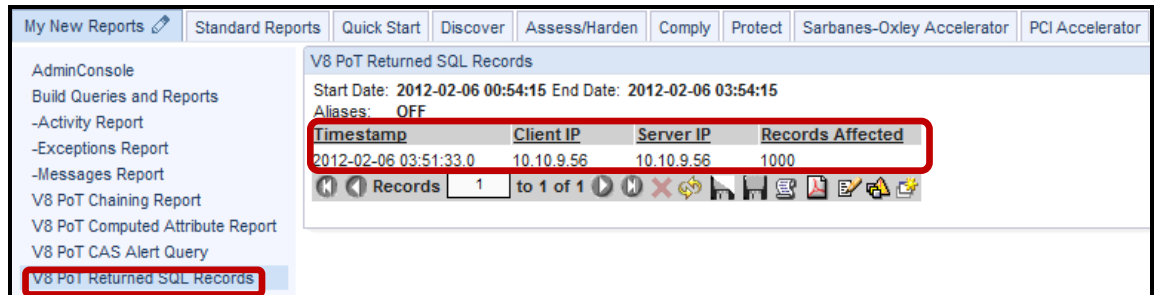
1000 rows selected.

SQL> exit
Disconnected from Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production
-bash-3.00$ exit
logout
[root@osprey ~]#

```

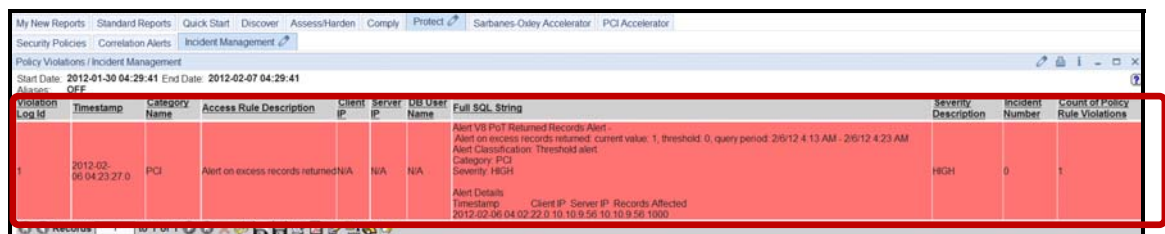
__9. Validate results from the **V8 PoT Returned SQL Records** correlation alert.

__a. Click the **V8 PoT Returned SQL Records** report once again to see the updated results.



__b. Click **Incident Management** under the **Protect** Tab to verify that the incident was logged. Keep clicking **Incident Management** to refresh the report until the policy violation appears.

Note: Since the accumulation period of the correlation alert is 10 minutes, it may take up to 10 minutes to appear as a policy violation.



Thank You

Correlation Alerts review

- __1. A correlation alert is triggered by:
- __a. a policy rule with an action.
 - __b. a query that looks back over a specified time period.
 - __c. a privacy set with a Boolean condition.
 - __d. a report that looks back over a specified time period.
- __2. The correlation alert threshold is based on a:
- __a. Specific query column.
 - __b. Query counter.
 - __c. Query condition.
 - __d. Correlation alert time period.
 - __e. a and b.
- __3. How is the correlation alert frequency configured?
- __a. Configuring the correlation alert schedule.
 - __b. Configuring the alerter in admin console.
 - __c. Configuring the run frequency parameter.
 - __d. Automatic, no configuration required.
- __4. Where is the correlation alert receiver configured?
- __a. Admin console.
 - __b. Anomaly detection setup.
 - __c. Correlation alert definition.
 - __d. As part of a rule definition.

- __5. What is the condition for “Query” to appear in the Alert definition query list?
- __a. One of the query columns is related to time/date data.
 - __b. All queries show in the alert definition query list.
 - __c. One of the query columns is related to counter.
 - __d. a and c.

Correlation Alerts review (Answers)

__1. A correlation alert is triggered by:

B – A query that looks back over a specified time period.

__2. The correlation alert threshold is based on a:

E – A (Specific query column) and B (Query counter).

__3. How is the correlation alert frequency configured?

C - Configuring the run frequency parameter.

__4. Where is the correlation alert receiver configured?

C – Correlation alert definition.

__5. What is the condition for “Query” to appear in the Alert definition query list?

D – A (One of the query columns is related to time/date data) and C (One of the query columns is related to counter).

Lab 11 Standard Reports

11.1 Exploring Standard Reports

Overview

The IBM InfoSphere® Guardium® solution includes more than 150 preconfigured policies and reports based on best practices and our experience working with Global 1000 companies, major auditors and assessors around the world. These reports help address regulatory requirements such as SOX, PCI DSS and data privacy laws, and they help streamline data governance and data privacy initiatives.

In addition to prepackaged report templates, InfoSphere Guardium provides a graphical drag-and-drop interface for easily building new reports or modifying existing reports. Reports can be automatically sent to users in PDF format (as email attachments) or as links to HTML pages. They can also be viewed online in the web console or exported to SIEM and other systems in standard formats.

Growing volumes of data, often physically distributed throughout an enterprise, are making it increasingly difficult for organizations to capture and analyze the detailed audit trails required for validating compliance.

InfoSphere Guardium creates a continuous, fine-grained trail of database activities that is contextually analyzed and filtered in real time to implement controls and produce the specific information required by auditors.

The resulting reports demonstrate compliance by making it possible to view database activities in detail, such as login failures, escalation of privileges, schema changes, access during off-hours or from unauthorized applications and access to sensitive tables.

Objectives

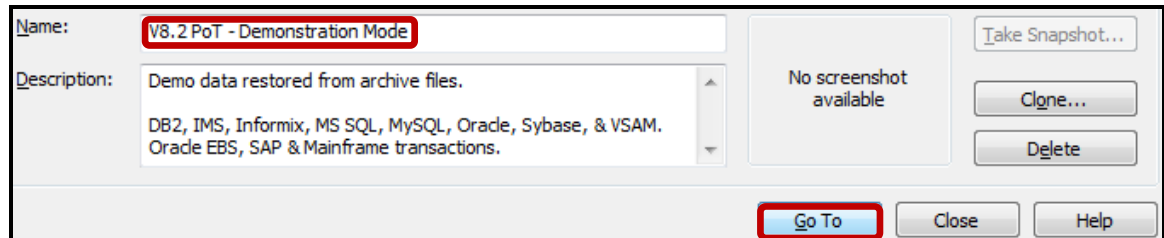
Lab 11 will demonstrate the ease of use with Standard Reports. The report set has grown over time as world-class customers such as you have guided the growth of this report set. This lab will focus on how the InfoSphere Guardium solution can accelerate report creation for you.

The following steps will guide us through the lab:

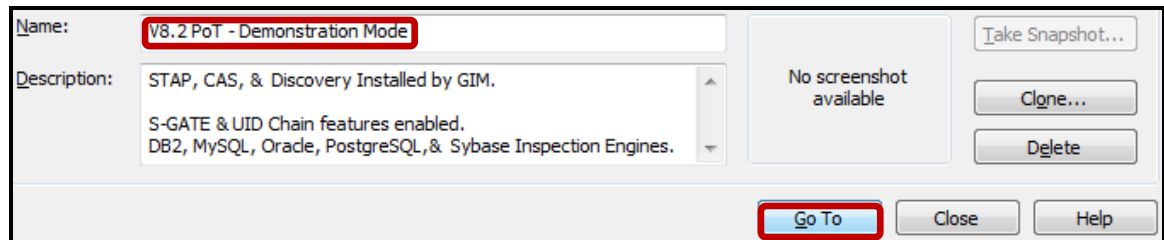
- __1. Explore the Standard Reports.
- __2. Find IBM DB2® Entitlements (Column-level privileges to object of creditcard between).
- __3. Find Oracle Entitlements (users with BECOME USER privilege).
- __4. Find Grant & Revoke (DB Administration).
 - __a. Grant Commands.
- __5. Find SQL Errors (Exceptions) – Identify which table does not exist for Bill (1st occurrence).

- ___1. **Critical Step** – Before beginning this lab, ensure that both the Appliance and Database Server VMs are set to the “**V8.2 PoT – Demonstration Mode**” snapshot. This is a critical step since only this snapshot contains all of the report data required by this lab. **Only start the Appliance VM. The Database Server VM is not required for this lab.**

- ___a. Set the Appliance VM to ‘**V8.2 PoT – Demonstration Mode**’, and restart the VM.



- ___b. **Critical Step** – The Database Server VM is not required for this lab. Set the Database Server VM to ‘**V8.2 PoT – Demonstration Mode**’ to shut it down. **Do Not Restart** the VM.



- __2. Using the InfoSphere Guardium GUI, demonstrate the ease of use within the InfoSphere Guardium solution using the Standard Reports. Start the InfoSphere Guardium Appliance VM and login.

Note: Lab Section 11.2 – Standard Reports Layout contains an outline of all of the InfoSphere Guardium standard reports.

- __a. From your laptop, go to <https://10.10.9.248:8443>
- __b. Login as **pot / guardium**.

Login

Please enter your information

User name:

Password:

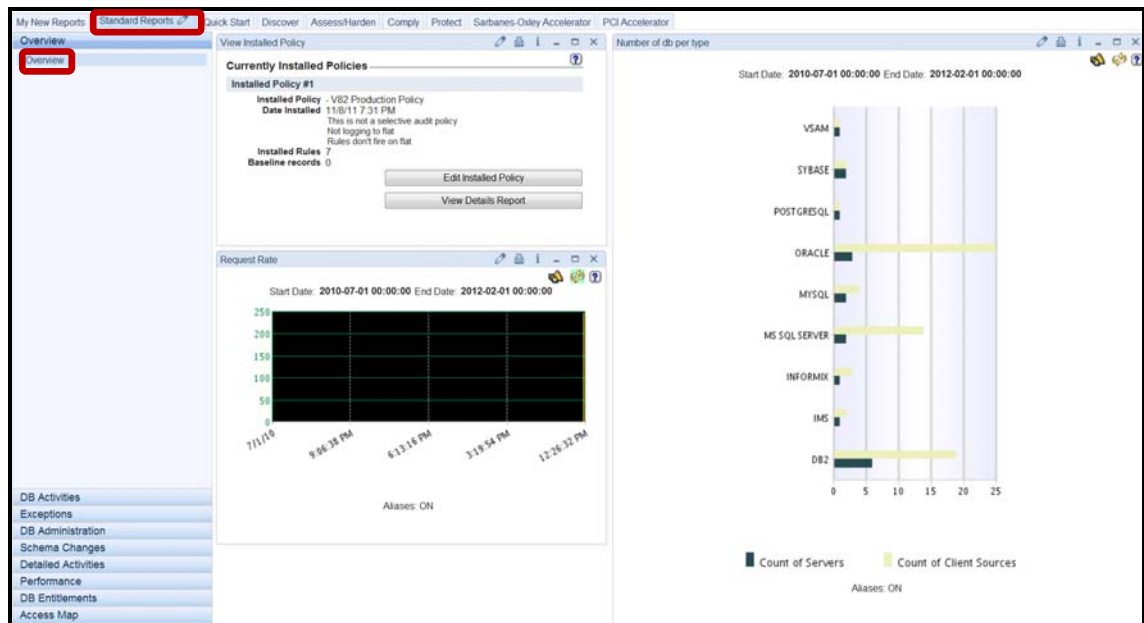
Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

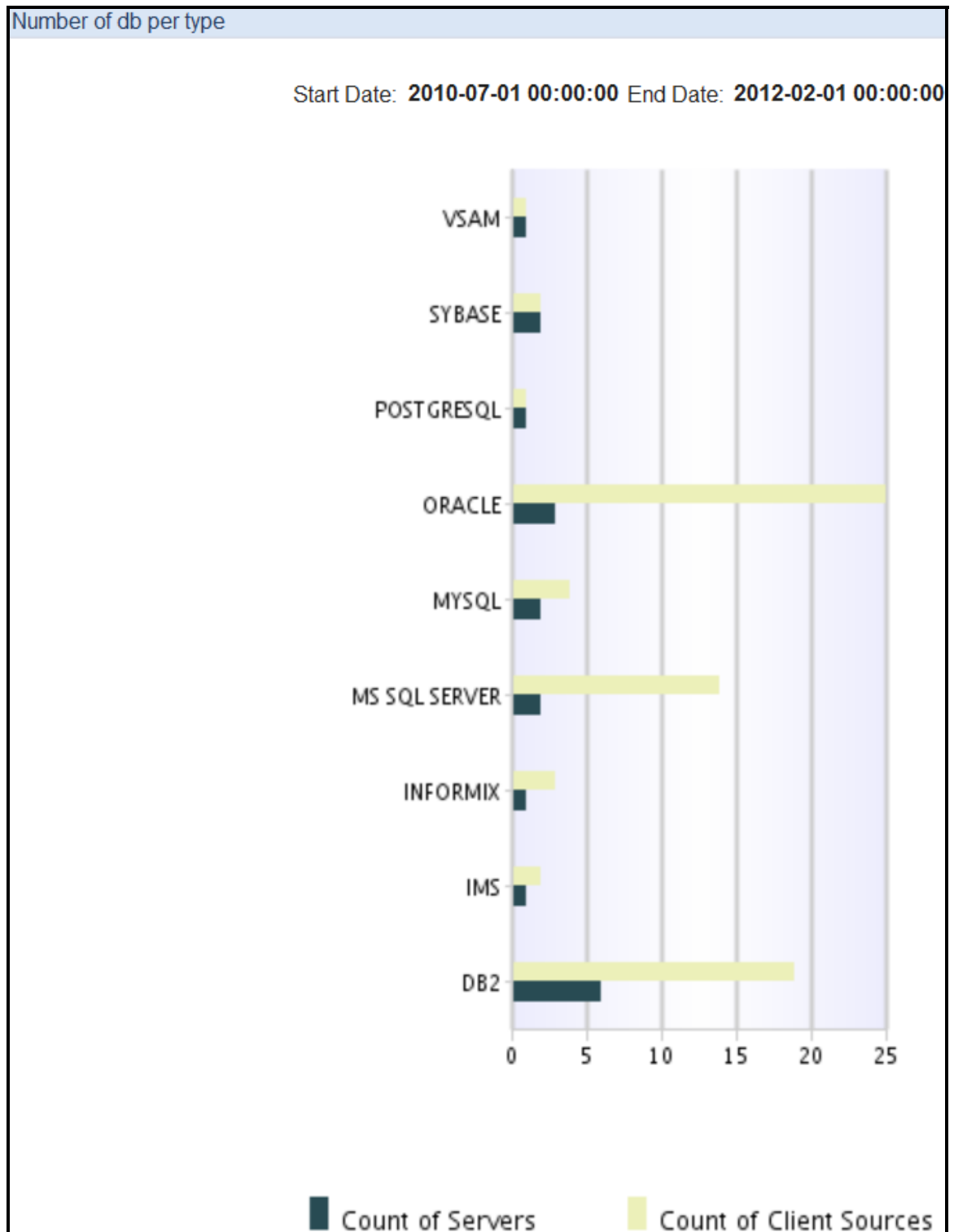
CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistrykey © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

__3. **Standard Reports – Overview.**

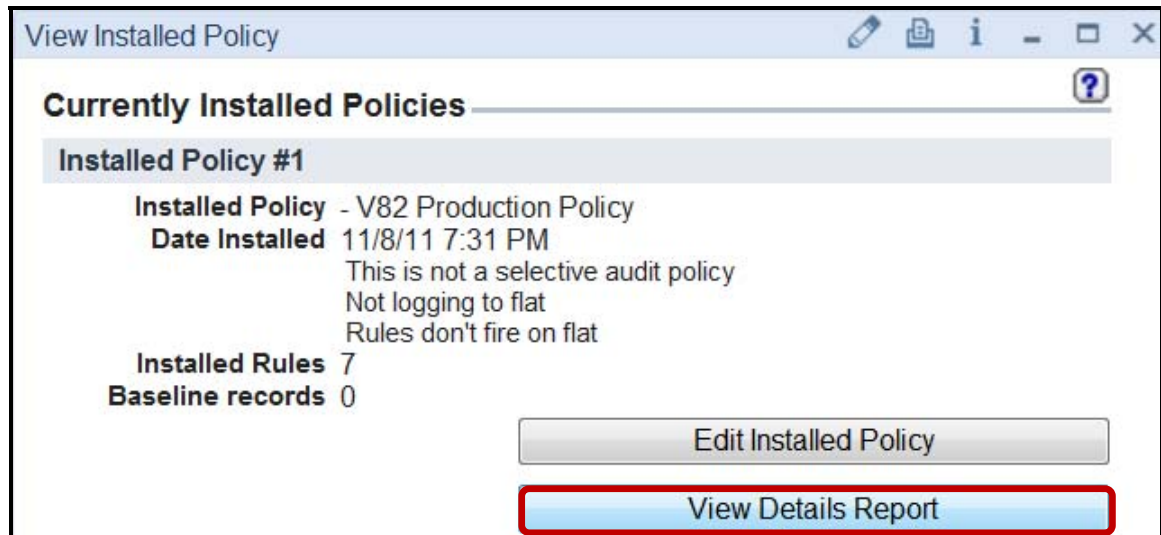
__a. Click **Overview** under the **Standard Reports->Overview** tab.



At a glance, the **'Number of DB per Type'** report provides a graphical view of the count of client sources broken down by database server type. Here, we see nine database types.



- b. The **'View Installed Policy'** report lists the currently installed policy, and provides access to edit the policy, or view policy details. Click the **View Details Report** button.



The **'Installed Policy Details Report'** lists each rule, and associated rule parameters.

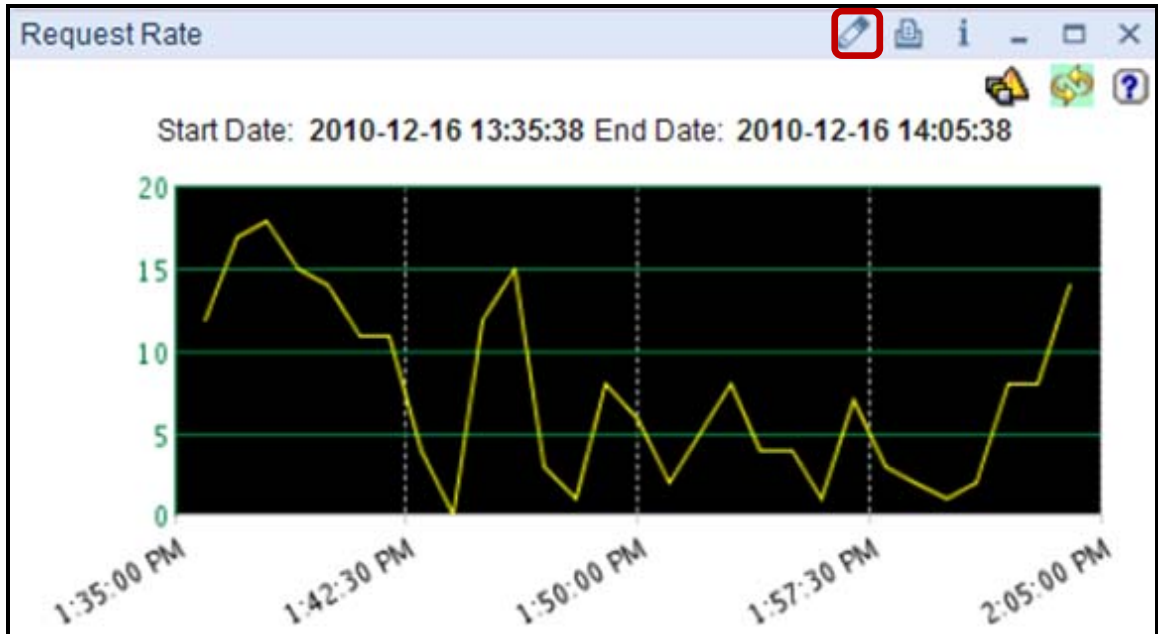
IBM® InfoSphere™ Guardium®
 Start Date: 2003-08-31 12:09:56 End Date: 2011-12-31 12:09:56
 Aliases: OFF

Rule Position	Rule Type	Policy Description	Rule Description	Client IP / Group	Server IP / Group	Client MAC	Net Protocol / Group	Field Name / Group	Object Name / Group	Command / Group
1	Extrusion	V82 Production Policy	Mask HIPAA Patient Information	/ - / -			-	-		
1	Extrusion	V82 Production Policy	Mask HIPAA Patient Information	/ - / -			-	-		
2	Access	V82 Production Policy	Log Full Details	/ - / -			-	-		-
3	Exception	V82 Production Policy	Alert on failed logins and quarantine	/ - / -			-	-		
3	Exception	V82 Production Policy	Alert on failed logins and quarantine	/ - / -			-	-		
4	Access	V82 Production Policy	Monitor Privilege Users	/ - / -			-	-		-
5	Access	V82 Production Policy	Block Unauthorized Access to Sensitive Tables/	/ - / -	Sensitive Database Servers		-	-	Cardholder Objects	-
5	Access	V82 Production Policy	Block Unauthorized Access to Sensitive Tables/	/ - / -	Sensitive Database Servers		-	-	Cardholder Objects	-
6	Access	V82 Production Policy	Monitor HIPAA Patient Information	/ - / -			-	-	- PHI Objects	Select Command
7	Exception	V82 Production Policy	Alert on SQL Errors	/ - / -			-	-		


Records 1 to 10 of 10






The **'Request Rate'** report is a Graphical report. By default, it displays the request rate for the last two hours. It is intended to display recent activity only. If you alter the run-time parameters to include a larger timeframe, you may receive a message indicating that there is too much data. In this case, use a tabular report to display data over a longer reporting period.

Note: If you hover over the Request Rate Graph, an information line will advise you to Double-click for drill-down. You can double click on the graphic report for a tabular version of the Graphic Data shown.



Note: The Request Rate report in this lab will not initially contain any data since setting the Appliance to **'Demonstration Mode'** removes all recent activity.

- ___c. To view or modify the query timeframe, click the  icon on the Request Rate ribbon (See above). The default Request Rate report setting is from **'NOW -2 HOUR'** to **'NOW.'** Then, scroll to the bottom, and click **'Update'** if changes are made. Otherwise, click **'Cancel.'**

Customize Portlet	
Report: Request Rate	Based on Query: Request Rate 
Title	Request Rate
Run Time Parameters	
QUERY_FROM_DATE Enter Period From	>= NOW -2 HOUR  
QUERY_TO_DATE Enter Period To	<= NOW  

4. Standard Reports – DB Activities.

a. Click **Activity By Client IP** under the **DB Activities** tab.

This report displays a list of Object Names accessed by Client IP, and unique SQL Verb with a total of the number of unique accesses.

The screenshot shows the IBM Security Center for Compliance interface. The left sidebar has 'DB Activities' and 'Activity By Client IP' highlighted with red boxes. The main area displays the 'Client IPs Activity' report with the following filters: Start Date: 2010-07-01 00:00:00, End Date: 2012-02-01 00:00:00, Aliases: ON, ObjectNameLike: LIKE %, SessionStartsAfter: >= 2010-07-01 00:00:00. The report table is as follows:

Client IP	SQL Verb	Object Name	Total access
10.10.9.240	CREATE TABLE	CC	6
10.10.9.240	CREATE TABLE	creditcard	6
10.10.9.240	DROP TABLE	CC	5
10.10.9.240	INSERT	CC	12
10.10.9.240	INSERT	creditcard	60
10.10.9.240	SELECT	CC	1
10.10.9.240	SELECT	creditcard	11
10.10.9.240	SELECT	SESSION_COUNTERS	8
10.10.9.240	SELECT	sysDummy	8
10.10.9.248	ALTER SESSION	NLS_TIMESTAMP_FORMAT	794
10.10.9.248	ALTER SESSION	NLS_TIMESTAMP_TZ_FORMAT	794
10.10.9.248	CALL	close	8
10.10.9.248	CALL	curDBA_ROLE_PRIVS	2
10.10.9.248	CALL	curDBA_SYS_PRIVS	2
10.10.9.248	CALL	curDBA_USERS	4
10.10.9.248	CALL	SYSIBM.SQLTABLES	24
10.10.9.248	DATABASE	idsgame	11
10.10.9.248	DATABASE	stores	11
10.10.9.248	DATABASE	stores_demo	11
10.10.9.248	DATABASE	sysadmin	11

At the bottom of the report, it shows 'Records 1 to 20 of 2201'.

b. Click Database Servers.

This report displays a list of database servers accessed, and a list of database servers discovered by Database Auto-Discovery.

The screenshot shows the IBM Guardium Database Auto-Discovery interface. The left sidebar contains a navigation menu with 'DB Activities' and 'Database Servers' highlighted. The main content area is divided into two sections: 'Servers Accessed' and 'Databases Discovered'.

Servers Accessed
 Start Date: 2010-07-01 00:00:00 End Date: 2012-02-01 00:00:00
 Aliases: ON

Server IP	Server Type	Database Name	Service Name	Count of Source Program	Count of Sessions
10.10.9.251	MS SQL SERVER			1	1
10.10.9.251	MS SQL SERVER		MS SQL SERVER 4		31
10.10.9.251	MS SQL SERVER	FINANCIAL	MS SQL SERVER 2		9
10.10.9.251	MS SQL SERVER	MASTER	MS SQL SERVER 3		56
10.10.9.251	MS SQL SERVER	MODEL	MS SQL SERVER 2		4
10.10.9.251	MS SQL SERVER	MSDB	MS SQL SERVER 2		7
10.10.9.251	MS SQL SERVER	REPORTSERVER	MS SQL SERVER 2		4
10.10.9.251	MS SQL SERVER	REPORTSERVERTEMPDB	MS SQL SERVER 2		4
10.10.9.251	MS SQL SERVER	SENSITIVEDB	MS SQL SERVER 2		4
10.10.9.251	MS SQL SERVER	TEMPDB	MS SQL SERVER 2		4
10.10.9.252	DB2		DB2	1	1
10.10.9.252	DB2	TESTDB	DB2	1	1
10.10.9.253	MS SQL SERVER	FINANCIAL	MS SQL SERVER 1		2
10.10.9.253	MS SQL SERVER	MASTER	MS SQL SERVER 1		1
Mainframe	DB2		DB9G	1	11
Mainframe	VSAM		ADCD	1	21
10.10.9.56	DB2		DB2INST2	2	21
10.10.9.56	DB2	SAMPLE	DB2INST2	3	299
10.10.9.56	MYSQL	MYSQL	10.10.9.56:5.5.191		169
10.10.9.56	MYSQL	MYSQL_NATIVE_PASSWORD	10.10.9.56:5.5.191		2

Databases Discovered
 Start Date: 2010-07-01 00:00:00 End Date: 2012-02-01 00:00:00
 Aliases: ON PortNotLike: NOT LIKE

Time Probed	Server IP	Server Host Name	DB Type	Port	Port Type	#
2010-08-27 03:49:22.0	Guardium Appliance	G82.ibm.com	MySQL	3306	tcp	1
2011-07-25 08:58:15.0	SAP DB Server	SAP DB Server	Oracle	16020	tcp	1
2011-07-25 08:58:15.0	SAP DB Server	SAP DB Server	Oracle	16021	tcp	1
2011-07-25 08:58:33.0	SAP DB Server	SAP DB Server	Oracle	16019	tcp	1
2011-07-25 08:58:35.0	SAP DB Server	SAP DB Server	Oracle	16018	tcp	1
2011-07-25 08:58:45.0	SAP DB Server	SAP DB Server	Oracle	16016	tcp	1
2011-07-25 08:58:45.0	SAP DB Server	SAP DB Server	Oracle	16017	tcp	1
2011-07-25 08:58:47.0	SAP DB Server	SAP DB Server	Oracle	9501	tcp	1
2011-07-25 08:59:07.0	SAP DB Server	SAP DB Server	Oracle	9500	tcp	1
2011-07-25 08:59:09.0	SAP DB Server	SAP DB Server	Oracle	8443	tcp	1
2011-07-25 08:59:26.0	SAP DB Server	SAP DB Server	MySQL	3306	tcp	1
2011-07-25 08:59:26.0	SAP DB Server	SAP DB Server	Oracle	8081	tcp	1
2011-07-25 08:59:53.0	Oracle DB Server	QA	Oracle	25502	tcp	1
2011-07-25 08:59:58.0	Oracle DB Server	QA	Oracle	25501	tcp	1
2011-07-25 09:00:00.0	Oracle DB Server	QA	Oracle	25500	tcp	1
2011-07-25 09:00:04.0	Oracle DB Server	QA	Oracle	25002	tcp	1
2011-07-25 09:00:06.0	Oracle DB Server	QA	Oracle	25001	tcp	1
2011-07-25 09:00:09.0	Oracle DB Server	QA	Oracle	25000	tcp	1
2011-07-25 09:00:11.0	Oracle DB Server	QA	Oracle	23500	tcp	1
2011-07-25 09:00:16.0	Oracle DB Server	QA	Oracle	23000	tcp	1

c. Click **DML Execution on Sensitive Objects**.

This report displays a list of objects as defined by the Sensitive Objects group upon which SQL changes (DML) have been performed.

SQL Verb	Object Name	Period Start	Client IP	Source Program	Total access
INSERT	creditcard	2010-08-27 00:00:00.010.10.9.56	DB2BP		2
INSERT	creditcard	2010-08-27 13:00:00.010.10.9.240	SQLI		60
INSERT	creditcard	2010-09-02 14:00:00.010.10.9.57	DB2BP		31
INSERT	payroll	2010-08-27 00:00:00.010.10.9.56	DB2BP		3

d. Click **IMS Access**.

This report details IMS access activity occurring on the mainframe.

Server Type	Client IP	Server IP	Event Type	DB Protocol	DB User Name	Program Type/Job Name	Terminal Id	IMS Name
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54
IMS	Mainframe	Mainframe	DLI	IMS		MPP		PERF54

__i. Click **Sessions by Server Type**.

This report is similar to the earlier graphical report under the Overview tab, but does not include a count of Database Servers, only a total count of Sessions per DB Type.

The screenshot displays the IBM InfoSphere Guardium interface. At the top, there are navigation tabs: 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. Below these is a sidebar menu under the 'Overview' section. Two items are highlighted with red boxes: 'DB Activities' and 'Sessions By Server Type'. The main content area shows the 'Sessions By Server Type' report. It includes a date range: 'Start Date: 2010-07-01 00:00:00 End Date: 2012-02-01 00:00:00' and 'Aliases: ON'. Below this is a table with two columns: 'Server Type' and 'Count of Sessions'. The table data is as follows:

Server Type	Count of Sessions
DB2	820
IMS	11
INFORMIX	92
IMS SQL SERVER	127
MYSQL	173
ORACLE	994
POSTGRESQL	28
SYBASE	261
VSAM	21

At the bottom of the report area, there is a 'Records' section showing '1' to '9 of 9' records, along with various icons for navigation and actions.

5. Standard Reports – Exceptions.

a. Click **Active Users Last Login** under the **Exceptions** tab.

This report displays the Last Login recorded for each member of the Active Users group for each Source Program used during the reporting period. Unlike most other reports, members will be listed, even if no logins occurred during the reporting period. In those cases where the DB User did not login during the reporting period, Count of Sessions is 0 and Max Session Start is N/A.

The Active Users group is empty at installation time, but has been populated for this lab.

DB User Name	Client IP	Server IP	Server Type	Source Program	Max Session Start	Count of Sessions
albert	N/A	N/A	N/A	N/A	N/A	0
bill	10.10.9.240	10.10.9.253	MS SQL SERVER	AQUA_DATA_STUDIO	2010-08-26 10:18:30	10
bill	10.10.9.57	10.10.9.57	ORACLE	SQLPLUS@OSPREY	2010-08-25 20:13:44	1
david	N/A	N/A	N/A	N/A	N/A	0
db2inst2	10.10.9.240	10.10.9.58	DB2	DB2JCC_APPLICATION	2011-08-27 22:05:56	14
db2inst2	10.10.9.248	10.10.9.57	DB2	DB2JCC_APPLICATION	2010-09-15 12:44:57	11
db2inst2	10.10.9.248	10.10.9.58	DB2	DB2JCC_APPLICATION	2010-09-09 22:05:24	52
db2inst2	10.10.9.56	10.10.9.56	DB2	DB2ACD	2011-12-29 22:56:07	11
db2inst2	10.10.9.56	10.10.9.56	DB2	DB2BP	2011-12-29 22:43:00	3
db2inst2	10.10.9.56	10.10.9.56	DB2	DB2HMON	2010-08-27 00:59:27	16
db2inst2	10.10.9.57	10.10.9.57	DB2	DB2ACD	2010-12-03 16:13:23	564
db2inst2	10.10.9.57	10.10.9.57	DB2	DB2BP	2010-12-03 16:16:08	14
db2inst2	10.10.9.57	10.10.9.57	DB2	DB2HMON	2010-10-26 18:59:59	326
db2inst2	10.10.9.58	10.10.9.58	DB2	DB2ACD	2011-08-27 22:03:52	8
db2inst2	10.10.9.58	10.10.9.58	DB2	DB2BP	2010-09-09 22:47:01	18
db2inst2	10.10.9.58	10.10.9.58	DB2	DB2HMON	2011-08-26 16:23:31	9
db2inst2	10.10.9.58	10.10.9.58	DB2	DB2JCC_APPLICATION	2010-09-09 22:43:00	37
db2inst2	10.10.9.58	10.10.9.58	DB2	DB2JCC_APPLICATION	2011-08-27 22:05:56	12
harry	10.10.9.240	10.10.9.253	MS SQL SERVER	AQUA_DATA_STUDIO	2010-08-26 10:22:34	9
harry	10.10.9.251	10.10.9.251	MS SQL SERVER	MICROSOFT SQL SERVER MANAGEMENT STUDIO	2010-11-17 07:48:37	19

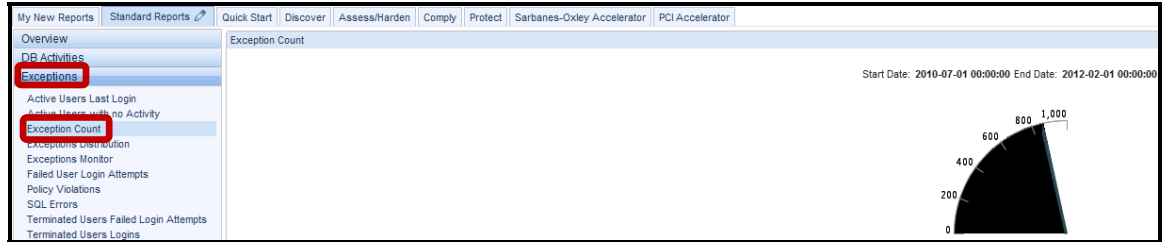
b. Click **Active Users with no Activity**.

This report displays a list of members of the Active Users group with no activity since the Start Date of the report. If you compare this report with the previous report, you will see a corresponding entry for each entry in the previous report where Count of Sessions is 0.

DB User Name	Count of Sessions
albert	0
david	0
joeb	0
larry	0
marc	0
mike	0
rodrigo	0
upesh	0

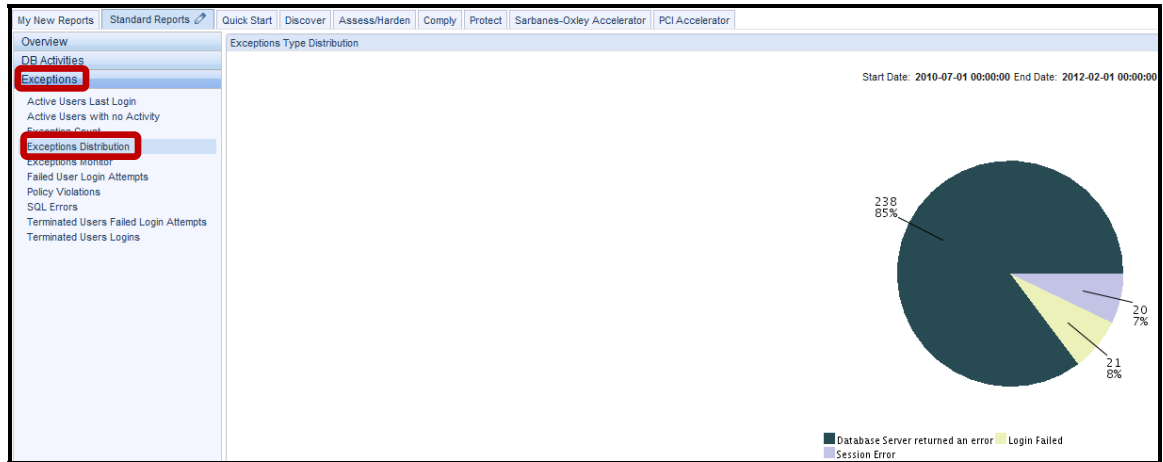
__c. Click **Exception Count**.

This graphical report displays a total of all exceptions that occurred during the reporting period.



__d. Click **Exception Distribution**.

This graphical report displays a distribution of all Database Server and Session exceptions that occurred during the reporting period.



e. Click Failed User Login Attempts.

This report displays all Failed User Login Attempts for each unique combination of DB User, Source IP Address, Destination IP Address, and Database Protocol.

My New Reports		Standard Reports		Quick Start	Discover	Assess/Harden	Comply	Protect	Sarbanes-Oxley Accelerator	PCI Accelerator	
Overview											
DB Activities											
Exceptions											
Active Users Last Login											
Active Users with no Activity											
Exception Count											
Exceptions Distribution											
Exceptions Monitor											
Failed User Login Attempts											
Policy Violations											
SQL Errors											
Terminated Users Failed Login Attempts											
Terminated Users Logins											

Failed Login Attempts					
Start Date: 2009-01-01 00:00:00		End Date: 2012-01-01 00:00:00			
Aliases: OFF		ServerIPLike: LIKE %			
DB User Name	Source Address	Destination Address	Database Protocol	Count of Exceptions	
?	10.10.9.248	10.10.9.57	ORACLE	1	
?	9.70.147.98	9.70.147.98	ORACLE	4	
DB2ADMIN	10.10.9.248	10.10.9.57	DB2	1	
DB2INST	10.10.9.240	10.10.9.252	DB2	3	
DB2INST1	9.70.147.106	9.70.147.106	DB2	2	
HARRY	10.10.9.240	10.10.9.253	MS SQL SERVER	1	
HARRY	10.10.9.57	10.10.9.57	ORACLE	1	
JOE	10.10.9.240	10.10.9.252	DB2	1	
JOE	10.10.9.240	10.10.9.57	MYSQL	9	
JOE	10.10.9.251	10.10.9.251	MS SQL SERVER	3	
JOE	10.10.9.57	10.10.9.57	MYSQL	1	
JOE	10.10.9.57	10.10.9.57	ORACLE	1	
JOE	9.70.147.106	9.70.147.106	DB2	1	
JOED	10.10.9.57	10.10.9.57	ORACLE	9	
JOED	10.10.9.58	10.10.9.58	DB2	1	
OWBSYS	9.70.147.98	9.70.147.98	ORACLE	2	
ROOT	10.10.9.240	10.10.9.57	MYSQL	4	
ROOT	10.10.9.57	10.10.9.57	MYSQL	12	
SA	10.10.9.248	10.10.9.57	SYBASE	1	
SAPPE61	9.70.147.106	9.70.147.106	DB2	1	

Records 1 to 20 of 23

f. Click Policy Violations.

This report displays all Policy Violations triggered during the reporting period.

My New Reports		Standard Reports		Quick Start	Discover	Assess/Harden	Comply	Protect	Sarbanes-Oxley Accelerator	PCI Accelerator	
Policy Violations Details											
Start Date: 2009-01-01 00:00:00		End Date: 2012-01-01 00:00:00									
Aliases: OFF		ServerIPLike: LIKE %									
Timestamp	Category	Policy Name	Access Rule Description	Client IP	Server IP	DB User Name	DB SQL Status	Severity	Count of Policy Rule Violations		
2010-06-18 02:24:23.0	Data Security	Terminate on Privilege User Access to Sensitive Information	10.10.9.58 10.10.9.58 S137EN select * from credential					RED	1		
2011-07-15 22:26:54.8	Quarantine	Quarantine brute force attack	10.10.240.10 10.9.252.JOE					RFO	1		
2011-07-15 22:25:57.9	Quarantine	Quarantine brute force attack	10.10.240.10 10.9.252.JOE					RFO	1		
2010-07-19 21:53:29.9	Data Security	Terminate on Privilege User Access to Sensitive Information	10.10.9.58 10.10.9.58 S137EN select * from credential					RED	1		
2010-07-19 21:53:29.9	Data Security	Terminate on Privilege User Access to Sensitive Information	10.10.9.58 10.10.9.58 S137EN select * from credential					RED	1		
2010-07-19 21:53:29.9	Data Security	Terminate on Privilege User Access to Sensitive Information	10.10.9.58 10.10.9.58 S137EN select * from credential					RED	1		
2010-07-19 21:53:29.9	Data Security	Terminate on Privilege User Access to Sensitive Information	10.10.9.58 10.10.9.58 S137EN select * from credential					RED	1		
2010-07-19 21:53:29.9	Data Security	Terminate on Privilege User Access to Sensitive Information	10.10.9.58 10.10.9.58 S137EN select * from credential					RED	2		
2010-10-01 10:44:34.9	Rule 1	Rule 1	10.10.9.57 10.10.9.57 JOE www3.us.oracle.com from credential					RFO	1		
2010-10-01 10:44:34.9	Rule 1	Rule 1	10.10.9.57 10.10.9.57 JOE select * from credential where rand()=1					RFO	1		
2010-10-01 10:44:34.9	Audit Only Rule	Audit Only Rule	10.10.9.57 10.10.9.57 JOE select * from dbi					RFO	1		
2010-10-01 10:44:34.9	Audit Only Rule	Audit Only Rule	10.10.9.57 10.10.9.57 JOE BEGIN DBMS_APPLICATION_INFO SET_MODULE('null',null); END;					RFO	1		
2010-10-01 10:44:34.9	Audit Only Rule	Audit Only Rule	10.10.9.57 10.10.9.57 JOE BEGIN DBMS_APPLICATION_INFO SET_MODULE('null',null); END;					RFO	1		
2010-10-01 10:44:34.9	Audit Only Rule	Audit Only Rule	10.10.9.57 10.10.9.57 JOE SELECT DECODE('A','T','2') FROM DUAL					RFO	1		
2010-10-01 10:44:34.9	Audit Only Rule	Audit Only Rule	10.10.9.57 10.10.9.57 JOE BEGIN DBMS_OUTPUT DISABLE; END;					RFO	1		
2010-10-01 10:44:34.9	Audit Only Rule	Audit Only Rule	10.10.9.57 10.10.9.57 JOE SELECT ATTRIBUTE_SCOPE_NUMERIC_VALUE_CHAR_VALUE_DATE_VALUE FROM SYSTEM_PRODUCT_PRIVS WHERE (UPPER('SQL')) LIKE UPPER(PRODUCT) AND UPPER('USER')					RFO	1		
2010-10-01 10:44:34.9	Audit Only Rule	Audit Only Rule	10.10.9.57 10.10.9.57 JOE SELECT DATA_VALUE FROM SYSTEM_PRODUCT_PRIVS WHERE (UPPER('SQL')) LIKE UPPER(PRODUCT) AND (UPPER('USER')) LIKE UPPER('PUBLIC') AND (UPPER('ATTRIBUTE')) = 'ROLE'					RFO	1		
2010-10-01 10:44:34.9	Audit Only Rule	Audit Only Rule	10.10.9.57 10.10.9.57 JOE SELECT USER FROM DUAL					RFO	1		
2010-11-30 10:57:37.2	Terminate on Privilege User Access to Sensitive Information	10.10.9.252 10.10.9.252 DB2ADMIN select * from credential						RED	1		
2010-11-30 10:57:37.2	Terminate on Privilege User Access to Sensitive Information	10.10.9.252 10.10.9.252 DB2ADMIN select * from credential						RED	1		

Records 1 to 26 of 264

g. Click **SQL Errors**.

This report displays all SQL Errors during the reporting period.

Note: We can see that JoeD has generated numerous exceptions. This could be an indication that someone is “fishing” for Database objects that they are not authorized to access. Your procedures may warrant a meeting with JoeD to determine whether he has violated any organizational policies.

Client IP	Server IP	Server Type	DB User Name	Database	Error Text	Exception Timestamp	Count of Exceptions
10.10.9.240	10.10.9.252	DB2	JOED		An error occurred during implicit system action type action-type. Information returned: for the error includes SQLCODE sqlcode, SQLSTATE sqlstate and message tokens token-let	2011-07-31 22:27:48.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An error occurred during implicit system action type action-type. Information returned: for the error includes SQLCODE sqlcode, SQLSTATE sqlstate and message tokens token-let	2011-07-31 22:27:52.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An error occurred during implicit system action type action-type. Information returned: for the error includes SQLCODE sqlcode, SQLSTATE sqlstate and message tokens token-let	2011-07-31 23:27:04.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An error occurred during implicit system action type action-type. Information returned: for the error includes SQLCODE sqlcode, SQLSTATE sqlstate and message tokens token-let	2011-07-31 23:27:46.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An error occurred during implicit system action type action-type. Information returned: for the error includes SQLCODE sqlcode, SQLSTATE sqlstate and message tokens token-let	2011-07-31 23:28:45.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An error occurred during implicit system action type action-type. Information returned: for the error includes SQLCODE sqlcode, SQLSTATE sqlstate and message tokens token-let	2011-07-31 23:29:03.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An error occurred during implicit system action type action-type. Information returned: for the error includes SQLCODE sqlcode, SQLSTATE sqlstate and message tokens token-let	2011-07-31 23:40:14.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An error occurred during implicit system action type action-type. Information returned: for the error includes SQLCODE sqlcode, SQLSTATE sqlstate and message tokens token-let	2011-07-31 23:42:32.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An error occurred during implicit system action type action-type. Information returned: for the error includes SQLCODE sqlcode, SQLSTATE sqlstate and message tokens token-let	2011-07-31 23:44:45.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An error occurred during implicit system action type action-type. Information returned: for the error includes SQLCODE sqlcode, SQLSTATE sqlstate and message tokens token-let	2011-08-01 00:00:51.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An error occurred during implicit system action type action-type. Information returned: for the error includes SQLCODE sqlcode, SQLSTATE sqlstate and message tokens token-let	2011-08-01 00:35:01.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An error occurred during implicit system action type action-type. Information returned: for the error includes SQLCODE sqlcode, SQLSTATE sqlstate and message tokens token-let	2011-08-01 10:20:59.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An error occurred during implicit system action type action-type. Information returned: for the error includes SQLCODE sqlcode, SQLSTATE sqlstate and message tokens token-let	2011-07-31 23:27:04.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An unexpected token token was found following text. Expected tokens may include: token-let	2011-07-31 23:28:45.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An unexpected token token was found following text. Expected tokens may include: token-let	2011-07-31 23:29:03.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An unexpected token token was found following text. Expected tokens may include: token-let	2011-07-31 23:40:14.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An unexpected token token was found following text. Expected tokens may include: token-let	2011-07-31 23:42:33.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An unexpected token token was found following text. Expected tokens may include: token-let	2011-07-31 23:44:45.0	1
10.10.9.240	10.10.9.252	DB2	JOED		An unexpected token token was found following text. Expected tokens may include: token-let	2011-08-01 00:00:51.0	1

h. Click **Terminated Users Failed Login Attempts**.

This report displays Failed Login Attempts by members of the Terminated Users group.

User Name	Source Address	Destination Address	Database	Protocol	Exception Timestamp	Count of Exceptions
TOM	10.10.9.57	10.10.9.57	ORACLE		2010-08-25 20:11:51.0	1
TOM	10.10.9.57	10.10.9.57	ORACLE		2010-08-25 20:11:54.0	1
TOM	10.10.9.57	10.10.9.57	ORACLE		2010-08-25 20:11:55.0	1

i. Click **Terminated Users Logins**.

This report displays successful logins by members of the Terminated Users group.

DB User Name	Client IP	Server IP	Server Type	Source Program	Max Session Start	Count of Sessions
BILL	10.10.9.240	10.10.9.253	MS SQL	SERVERAQUA_DATA_STUDIO	2010-08-26 10:18:30.0	10
BILL	10.10.9.57	10.10.9.57	ORACLE	SQLPLUS@OSPNEY	2010-08-25 20:13:44.0	1
TOM	10.10.9.251	10.10.9.251	MS SQL	SERVERMICROSOFT SQL SERVER MANAGEMENT STUDIO	2010-11-17 07:49:10.06	1
TOM	10.10.9.57	10.10.9.57	ORACLE	SQLPLUS	2010-08-25 20:11:55.02	1
TOM	10.10.9.57	10.10.9.57	ORACLE	SQLPLUS@OSPNEY	2010-08-25 20:11:51.01	1

6. Standard Reports – DB Administration.

a. Click **Admin Users Login** under the **DB Administration** tab.

This report displays all Sessions recorded for each member of the Admin Users group for each Source Program used during the reporting period.

Client IP	DB User Name	Source Program	Session Start	Count of Sessions
10.10.9.240	DB2INST2	DB2JCC_APPLICATION	2011-07-30 14:12:41.02	
10.10.9.240	DB2INST2	DB2JCC_APPLICATION	2011-08-25 23:06:49.01	
10.10.9.240	DB2INST2	DB2JCC_APPLICATION	2011-08-26 17:05:28.01	
10.10.9.240	DB2INST2	DB2JCC_APPLICATION	2011-08-26 17:08:56.03	
10.10.9.240	DB2INST2	DB2JCC_APPLICATION	2011-08-26 17:16:37.03	
10.10.9.240	DB2INST2	DB2JCC_APPLICATION	2011-08-27 21:23:39.01	
10.10.9.240	DB2INST2	DB2JCC_APPLICATION	2011-08-27 21:50:02.01	
10.10.9.240	DB2INST2	DB2JCC_APPLICATION	2011-08-27 22:03:52.01	
10.10.9.240	DB2INST2	DB2JCC_APPLICATION	2011-08-27 22:05:56.01	
10.10.9.240	INFORMIX	SQLI	2010-08-27 13:06:41.02	
10.10.9.240	INFORMIX	SQLI	2010-09-10 13:48:06.01	
10.10.9.240	JOE	DB2JCC_APPLICATION	2011-07-31 22:26:04.01	
10.10.9.240	JOE	DB2JCC_APPLICATION	2011-08-18 06:26:52.01	
10.10.9.240	JOE	MYSQL CLIENT	2010-09-15 16:32:21.01	
10.10.9.240	JOE	MYSQL CLIENT	2010-09-15 16:32:53.01	
10.10.9.240	JOE	MYSQL CLIENT	2010-09-15 16:44:25.01	
10.10.9.240	JOE	MYSQL CLIENT	2010-09-15 16:44:37.01	
10.10.9.240	JOE	MYSQL CLIENT	2010-09-15 16:45:40.01	
10.10.9.240	JOE	MYSQL CLIENT	2010-09-15 16:46:17.01	
10.10.9.240	JOE	MYSQL CLIENT	2010-09-15 16:50:00.01	

b. Click **Administrative Commands Usage**.

This report displays all usage of commands from the Administrative Commands group by unique combination of SQL Verb, Object Name, and Client IP.

SQL Verb	Depth	Object Name	Client IP	Total access
ALTER SESSION	0	NLS_TIMESTAMP_FORMAT	10.10.9.248	28
ALTER SESSION	0	NLS_TIMESTAMP_FORMAT	10.10.9.58	13
ALTER SESSION	0	NLS_TIMESTAMP_FORMAT	9.70.147.11537	
ALTER SESSION	0	NLS_TIMESTAMP_TZ_FORMAT	10.10.9.248	28
ALTER SESSION	0	NLS_TIMESTAMP_TZ_FORMAT	10.10.9.58	13
ALTER SESSION	0	NLS_TIMESTAMP_TZ_FORMAT	9.70.147.11537	
ALTER SESSION	0	REMOTE_DEPENDENCIES_MODE	9.70.147.98	88
ALTER USER	0	joed	10.10.9.57	1
CREATE DATABASE	0	financial	10.10.9.253	1
CREATE LOGIN	0	bill	10.10.9.253	1
CREATE LOGIN	0	financial	10.10.9.253	3
CREATE LOGIN	0	harry	10.10.9.253	1
CREATE LOGIN	0	joe	10.10.9.251	1
CREATE LOGIN	0	tom	10.10.9.253	1
CREATE ROLE	0	gdmmonitor	10.10.9.57	1
CREATE SCHEMA	0	bill	10.10.9.253	1
CREATE SCHEMA	0	creditcard	10.10.9.253	1
CREATE SCHEMA	0	harry	10.10.9.253	1
CREATE SCHEMA	0	invoice	10.10.9.253	1
CREATE SCHEMA	0	payments	10.10.9.253	1

c. Click DB Predefined Users Login.

This report displays a list of all Predefined Database User logins by unique combinations of DB User Name, Client IP, Server IP, Source Program, and Database Name.

DB User Name	Client IP	Server IP	Source Program	Database Name	Service Name	Count of Sessions
ADMINISTRATOR	10.10.9.251	10.10.9.251	SQLCMD	MASTER	MS SQL SERVER	18
ADMINISTRATOR	10.10.9.251	10.10.9.251	SQLCMD.EXE		MS SQL SERVER	4
ADMINISTRATOR	10.10.9.251	10.10.9.251	SQLCMD.EXE	MASTER	MS SQL SERVER	14
ADMINISTRATOR	10.10.9.251	10.10.9.251	SQLWB.EXE		MS SQL SERVER	1
ADMINISTRATOR	10.10.9.252	10.10.9.252	DB2BP.EXE	DB2		6
ADMINISTRATOR	10.10.9.252	10.10.9.252	DB2BP.EXE	SAMPLE	DB2	4
ADMINISTRATOR	10.10.9.252	10.10.9.252	DB2BP.EXE	TESTDB	DB2	3
ADMINISTRATOR	10.10.9.253	10.10.9.253	SQLCMD.EXE		MS SQL SERVER	3
ADMINISTRATOR	10.10.9.253	10.10.9.253	SQLWB.EXE		MS SQL SERVER	1
ADMINISTRATOR	10.10.9.253	10.10.9.253	SQLWB.EXE	FINANCIAL	MS SQL SERVER	1
ADMINISTRATOR	10.10.9.253	10.10.9.253	SQLWB.EXE	MASTER	MS SQL SERVER	1
APPLSYSUB	9.70.147.98	9.70.147.98	IORACLEVISIAPPSITECH_ST10.1.2\BIN\FRMWEB.EXE		VIS	16
APPLSYSUB	9.70.147.98	9.70.147.98	JDBC THIN CLIENT		VIS	433
APPS	9.70.147.1159	9.70.147.98	JDBC CONNECT CLIENT		VIS	37
APPS	9.70.147.98	9.70.147.98	IORACLEVISIAPPSIAPPS_ST1APPL\FND12.0.0\BIN\FNDLIBR.EXE		VIS	350
APPS	9.70.147.98	9.70.147.98	IORACLEVISIAPPSITECH_ST10.1.2\BIN\FRMWEB.EXE		VIS	16
APPS	9.70.147.98	9.70.147.98	IORACLEVISIAPPSITECH_ST10.1.2\BIN\SQLPLUS.EXE		VIS	21
APPS	9.70.147.98	9.70.147.98	JDBC THIN CLIENT		VIS	732
DB2ADMIN	10.10.9.248	10.10.9.57	DB2BP	SAMPLE	DB2INST2	1
DB2ADMIN	10.10.9.252	10.10.9.252	DB2BP.EXE	SAMPLE	DB2	2

d. Click DML Execution on Administrative Objects.

This report displays a list of objects as defined by the Administrative Objects group upon which SQL changes (DML) have been performed.

DB User Name	Client IP	Server IP	Server Type	Service Name	Database Name	SQL Verb	Object Name	Total access
BILL	10.10.9.240	10.10.9.253	MS SQL SERVER	MS SQL SERVER	FINANCIAL	INSERT	customer	7
DB2INST2	10.10.9.58	10.10.9.58	DB2	DB2INST2	SAMPLE	INSERT	EMP	1
HARRY	10.10.9.240	10.10.9.253	MS SQL SERVER	MS SQL SERVER	FINANCIAL	INSERT	customer	7

e. Click GRANT Commands Execution.

This report displays all SQL GRANT Commands Execution by unique combinations of Client IP, Server IP, DB User Name, Source Program, Database Name, and Object Name.

Note: The importance of this report can be seen by examining it more closely. It shows that Bill, Tom and Harry have been granted command execution privileges for the Financial Database. This is an example of how reports provide the capability to see, report, and audit compliance and business risk with your organization. Your organization can then make the decisions based on easily reported facts.

Client IP	Server IP	Service Name	DB User Name	Source Program	Database Name	Object Name	SQL Verb	Total access
10.10.9.240	10.10.9.57	10.10.9.57:4.1.20	JOE	MYSQL CLIENT	MYSQL	joe.ssn	GRANT	1
10.10.9.240	10.10.9.57	10.10.9.57:4.1.20	JOE	MYSQL CLIENT	MYSQL	mysql	GRANT	3
10.10.9.240	10.10.9.57	10.10.9.57:4.1.20	JOE	MYSQL CLIENT	MYSQL	root	GRANT	5
10.10.9.240	10.10.9.57	10.10.9.57:4.1.20	JOE	MYSQL CLIENT	MYSQL	ssn	GRANT	1
10.10.9.240	10.10.9.57	10.10.9.57:4.1.20	ROOT	MYSQL CLIENT	MYSQL	information_schema	GRANT	1
10.10.9.240	10.10.9.57	10.10.9.57:4.1.20	ROOT	MYSQL CLIENT	MYSQL	mysql	GRANT	1
10.10.9.240	10.10.9.57	10.10.9.57:4.1.20	ROOT	MYSQL CLIENT	MYSQL	root	GRANT	2
10.10.9.253	10.10.9.253	MS SQL SERVER ADMINISTRATOR	SQLWB.EXE	FINANCIAL	bill	GRANT	1	
10.10.9.253	10.10.9.253	MS SQL SERVER ADMINISTRATOR	SQLWB.EXE	FINANCIAL	harry	GRANT	1	
10.10.9.253	10.10.9.253	MS SQL SERVER ADMINISTRATOR	SQLWB.EXE	FINANCIAL	tom	GRANT	1	

f. Click REVOKE Commands Execution.

This report displays all SQL REVOKE Commands Execution by unique combinations of Client IP, Server IP, DB User Name, Source Program, Database Name, and Object Name.

Note: Using this report, we can see that FINANCE has had command execution privileges REVOKED. Why did this occur, and does it comply with our compliance standards? Again, armed with this knowledge, we can investigate, and make decisions based on easily reported facts.

Client IP	Server IP	Service Name	DB User Name	Source Program	Database Name	Object Name	SQL Verb	Total access
10.10.9.57	10.10.9.57	ORACLEXE	FINANCE	SQLPLUS@OSPREY	bill	REVOKE	1	
10.10.9.57	10.10.9.57	ORACLEXE	FINANCE	SQLPLUS@OSPREY	TransactionTable	REVOKE	1	

7. Standard Reports – Schema Changes.

- a. Click **ALTER Commands Execution** under the **Schema Changes** tab.

This report displays all ALTER Commands Execution by unique combinations of Client IP, Server IP, Service Name, DB User Name, Source Program, Database Name, and Object Name.

Client IP	Server IP	Service Name	DB User Name	Source Program	Database Name	Object Name	SQL Verb	Total access
10.10.9.57	10.10.9.57	ORACLEXE	JOE	SQLPLUS@OSPREY	joed	ALTER USER1	ALTER USER1	1

- b. Click **CREATE Commands Execution**.

This report displays all CREATE Commands Execution by unique combinations of Client IP, Server IP, Service Name, DB User Name, Source Program, Database Name, SQL Verb, and Object Name along with the actual SQL, and a count of Total access.

Client IP	Server IP	Service Name	DB User Name	Source Program	Database Name	SQL Verb	Total access
10.10.9.240	10.10.9.252	DBE2	JOE	DBJCC_APPLICATION	TESTDB	CREATE TABLE create table empbyesamp0 int, empname VARCHAR(7), empDOC sML)	1
10.10.9.240	10.10.9.252	DBE2	JOE	DBJCC_APPLICATION	TESTDB	CREATE TABLE Student(1
10.10.9.240	10.10.9.252	DBE2	JOE	DBJCC_APPLICATION	TESTDB	ID INT NOT NULL, SCORE1 INT NOT NULL, SCORE2 INT NOT NULL, SCORE3 INT NOT NULL, CREDIT INT.	1
10.10.9.240	10.9.203MS	SQL	SERVERBELL	AQUA_DATA_STUDIO	FINANCIAL	CONSTRAINT STUDENT_SOLE_MJM PRIMARY KEY (ID)	1
10.10.9.240	10.9.203MS	SQL	SERVERHARRY	AQUA_DATA_STUDIO	FINANCIAL	CREATE TABLE create table customerid int, name varchar(7)	1
10.10.9.240	10.9.203MS	SQL	SERVERHARRY	AQUA_DATA_STUDIO	FINANCIAL	CREATE TABLE create table cc 0 int, cardnumber varchar(7), name varchar(7)	1
10.10.9.240	10.9.203MS	SQL	SERVERHARRY	AQUA_DATA_STUDIO	FINANCIAL	CREATE TABLE create table creditcard0 int, cardnumber varchar(7), name varchar(7)	1
10.10.9.240	10.9.203MS	SQL	SERVERHARRY	AQUA_DATA_STUDIO	FINANCIAL	CREATE TABLE create table customerid int, name varchar(7)	1
10.10.9.240	10.10.9.57	A.1.20	JOE	MYSQL_CLIENT	MYSQL	CREATE TABLE user (1
10.10.9.240	10.10.9.58	DBE2	DBE2	DBJCC_APPLICATION	SAMPLE3	CREATE TABLE Student(4
10.10.9.240	10.10.9.58	DBE2	DBE2	DBJCC_APPLICATION	SAMPLE3	ID INT NOT NULL, SCORE1 INT NOT NULL, SCORE2 INT NOT NULL, SCORE3 INT NOT NULL, CREDIT INT.	2
10.10.9.240	10.10.9.60	DEMO_ON	INFORMIX	SQL	SYMASTER	CONSTRAINT STUDENT_SOLE_MJM PRIMARY KEY (ID)	7
10.10.9.240	10.10.9.60	DEMO_ON	INFORMIX	SQL	SYMASTER	CREATE TABLE CREDITCARD (CARDID INT, FIRSTNAME VARCHAR(7), LASTNAME VARCHAR(7), CARDNUMBER VARCHAR(7),	7
10.10.9.240	10.10.9.60	DEMO_ON	INFORMIX	SQL	SYMASTER	CREATE TABLE creditcard (CARDID INT, FIRSTNAME VARCHAR(7), LASTNAME VARCHAR(7), CARDNUMBER VARCHAR(7), TIN_ID VARCHAR(7), SECURITYCODE VARCHAR(7), NAME_ON_CARD VARCHAR(7))	7
10.10.9.240	10.10.9.60	DEMO_ON	INFORMIX	SQL	SYMASTER	CREATE TABLE create table pzo0 int)	1

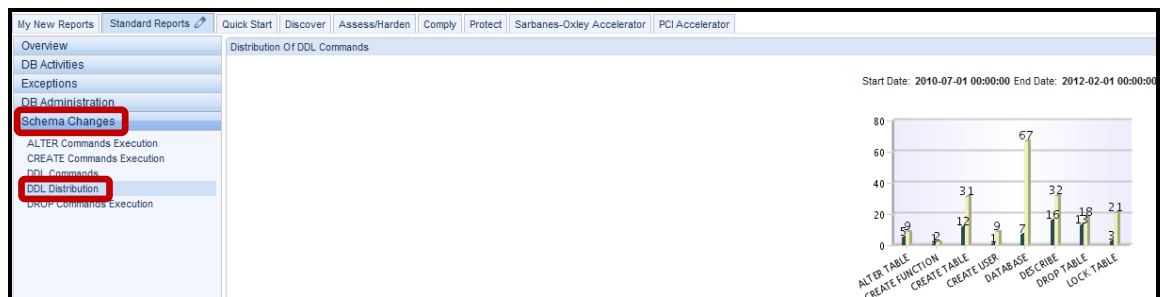
c. Click **DDL Commands**.

This report displays all SQL DDL Commands by unique combinations of Client IP, Server IP, Server Type, and SQL Verb along with counts of Object Names, and Total access.

Client IP	Server IP	Server Type	SQL Verb	Count of Object Name	Total access
10.10.9.240	10.10.9.252	DB2	CREATE TABLE	2	2
10.10.9.240	10.10.9.253	MS SQL SERVER	CREATE TABLE	4	5
10.10.9.240	10.10.9.253	MS SQL SERVER	DROP TABLE	2	2
10.10.9.240	10.10.9.57	MYSQL	CREATE TABLE	1	1
10.10.9.240	10.10.9.57	MYSQL	GRANT	5	14
10.10.9.240	10.10.9.58	DB2	CREATE TABLE	2	6
10.10.9.240	10.10.9.58	DB2	DROP TABLE	1	3
10.10.9.240	10.10.9.60	INFORMIX	CREATE TABLE	3	15
10.10.9.240	10.10.9.60	INFORMIX	DROP TABLE	2	13
10.10.9.248	10.10.9.60	INFORMIX	DATABASE	7	189
10.10.9.251	10.10.9.251	MS SQL SERVER	CREATE TABLE	2	2
10.10.9.251	10.10.9.251	MS SQL SERVER	CREATE USER	1	8
10.10.9.251	10.10.9.251	MS SQL SERVER	DROP TABLE	3	3
10.10.9.252	10.10.9.252	DB2	CREATE FUNCTION	1	2
10.10.9.252	10.10.9.252	DB2	CREATE TABLE	3	3
10.10.9.253	10.10.9.253	MS SQL SERVER	CREATE DATABASE	1	1
10.10.9.253	10.10.9.253	MS SQL SERVER	CREATE SCHEMA	6	6
10.10.9.253	10.10.9.253	MS SQL SERVER	CREATE USER	6	6
10.10.9.253	10.10.9.253	MS SQL SERVER	DROP DATABASE	1	1
10.10.9.253	10.10.9.253	MS SQL SERVER	DROP LOGIN	3	3

d. Click **DDL Distribution**.

This graphical report displays a distribution of SQL DDL Commands executed during the reporting period.



e. Click DROP Commands Execution.

This report displays a list of all DROP commands by unique combinations of Client IP, Server IP, Service Name, Source Program, Database Name, Object Name, and SQL Verb.

Execution Of DROP Commands									
Start Date: 2009-01-01 00:00:00		End Date: 2012-01-01 00:00:00							
Aliases: OFF		DBUserNameLike: LIKE %							
ServerPLike: LIKE %		SessionStartsAfter: >= 2009-01-01 00:00:00							
Client IP	Server IP	Service Name	DB User Name	Source Program	Database Name	Object Name	SQL Verb	Total access	
10.10.9.240	10.10.9.253	MS SQL SERVERBILL		AQUA_DATA_STUDIO	FINANCIAL	creditcard.customer	DROP TABLE	1	
10.10.9.240	10.10.9.253	MS SQL SERVERHARRY		AQUA_DATA_STUDIO	FINANCIAL	invoice.customer	DROP TABLE	1	
10.10.9.240	10.10.9.58	DB2INST2	DB2INST2	DB2JCC_APPLICATION	SAMPLE3	emp1	DROP TABLE	3	
10.10.9.240	10.10.9.60	DEMO_ON	INFORMIX	SQLI	SYSMASTER	CC	DROP TABLE	6	
10.10.9.240	10.10.9.60	DEMO_ON	INFORMIX	SQLI	SYSMASTER	creditcard	DROP TABLE	7	
10.10.9.251	10.10.9.251	MS SQL SERVERADMINISTRATOR	SQLCMD.EXE	MASTER	FINANCIAL	creditcard	DROP TABLE	1	
10.10.9.251	10.10.9.251	MS SQL SERVERADMINISTRATOR	SQLCMD.EXE	MASTER	FINANCIAL	SSN	DROP TABLE	1	
10.10.9.251	10.10.9.251	MS SQL SERVERSYSTEM	SYSTEM	FINANCIAL	FINANCIAL	patient	DROP TABLE	1	
10.10.9.253	10.10.9.253	MS SQL SERVERADMINISTRATOR	SQLWB.EXE	FINANCIAL	FINANCIAL	creditcard	DROP SCHEMA	1	
10.10.9.253	10.10.9.253	MS SQL SERVERADMINISTRATOR	SQLWB.EXE	FINANCIAL	FINANCIAL	invoice	DROP SCHEMA	1	
10.10.9.253	10.10.9.253	MS SQL SERVERADMINISTRATOR	SQLWB.EXE	FINANCIAL	FINANCIAL	payments	DROP SCHEMA	1	
10.10.9.253	10.10.9.253	MS SQL SERVERADMINISTRATOR	SQLWB.EXE	MASTER	FINANCIAL	financial	DROP DATABASE	1	
10.10.9.56	10.10.9.56	DB2INST2	DB2INST2	DB2BP	SAMPLE	CC	DROP TABLE	1	
10.10.9.56	10.10.9.56	DB2INST2	DB2INST2	DB2BP	SAMPLE	payroll	DROP TABLE	1	
10.10.9.57	10.10.9.57	ORACLEXE	HARRY	SQLPLUS@OSPREY		patient	DROP TABLE	4	
10.10.9.57	10.10.9.57	ORACLEXE	HARRY	SQLPLUS@OSPREY		payroll	DROP TABLE	2	
10.10.9.57	10.10.9.57	ORACLEXE	JOE	SQLPLUS@OSPREY		finance	DROP USER	1	
10.10.9.57	10.10.9.57	ORACLEXE	JOE	SQLPLUS@OSPREY		joe	DROP TABLE	1	
10.10.9.57	10.10.9.57	ORACLEXE	JOE	SQLPLUS@OSPREY		net_sales_us	DROP TABLE	1	
10.10.9.57	10.10.9.57	ORACLEXE	JOE	SQLPLUS@OSPREY		PhoneRecord	DROP TABLE	1	

8. Standard Reports – Detailed Activities.

- a. Click **Classification Process Results** under the **Detailed Activities** tab.

This report lists classification processes and should be quite familiar from our previous Sensitive Data Finder lab, where we used it to identify Credit Card Number data.

Process Description	Category	Schema	Table Name	Column Name	Rule Description	Comments	Classification Name	Category	Data Source	Description	Start Date/Time	Count of Classification Process Results
PUT Dms Find CC Objects	BENU	CREDITCARD	CARDNUMBER	Find PUT Dms CC	Rule: Search For Data: Find PUT Dms CC	Date: Thursday, December 29, 2011 9:53:53 PM EST Severity: ORACLE 10.10.9.56 Object: BENU.CREDITCARD.CARDNUMBER Category: PCI Classification: CreditCard	CreditCard	PCI	Wsprey_system	ORACLE 10.10.9.56	12-29-21:56:59.9	1
PUT Dms Find CC Objects	BENU	LOYALTYFRAUD	CREDIT_CARD_NO	Find PUT Dms CC	Rule: Search For Data: Find PUT Dms CC	Date: Thursday, December 29, 2011 9:53:53 PM EST Severity: ORACLE 10.10.9.56 Object: BENU.LOYALTYFRAUD.CREDIT_CARD_NO Category: PCI Classification: CreditCard	CreditCard	PCI	Wsprey_system	ORACLE 10.10.9.56	12-29-21:56:59.9	1
PUT Dms Find CC Objects	BILL	CREDITCARD	CARDNUMBER	Find PUT Dms CC	Rule: Search For Data: Find PUT Dms CC	Date: Thursday, December 29, 2011 9:53:53 PM EST Severity: ORACLE 10.10.9.56 Object: BILL.CREDITCARD.CARDNUMBER Category: PCI Classification: CreditCard	CreditCard	PCI	Wsprey_system	ORACLE 10.10.9.56	12-29-21:56:59.9	1
PUT Dms Find CC Objects	HARRY	CC	CARDNUMBER	Find PUT Dms CC	Rule: Search For Data: Find PUT Dms CC	Date: Thursday, December 29, 2011 9:53:53 PM EST Severity: ORACLE 10.10.9.56 Object: HARRY.CC.CARDNUMBER Category: PCI Classification: CreditCard	CreditCard	PCI	Wsprey_system	ORACLE 10.10.9.56	12-29-21:56:59.9	1
PUT Dms Find CC Objects	JOE	BNU-ExtCCObjSnsrData=0	CARDNUMBER	Find PUT Dms CC	Rule: Search For Data: Find PUT Dms CC	Date: Thursday, December 29, 2011 9:53:53 PM EST Severity: ORACLE 10.10.9.56 Object: JOE.BNU-ExtCCObjSnsrData=0.CARDNUMBER Category: PCI Classification: CreditCard	CreditCard	PCI	Wsprey_system	ORACLE 10.10.9.56	12-29-21:56:59.9	1

- b. Click **Client IP Activity Summary**.

This report displays all database Activity by Client IP for the reporting period.

Client IP	Server IP	Source Program	SQL Verb	Object Name	DB User Name	Total access
10.10.9.56	10.10.9.56	DB2ACD	CALL	DB2_CLP_PROC	DB2INST2	11
10.10.9.56	10.10.9.56	DB2ACD	CALL	DB2_DBMGR_GET_CONFIG	DB2INST2	6
10.10.9.56	10.10.9.56	DB2ACD	CALL	DB2_INSTANCE_SQLMON	DB2INST2	4
10.10.9.56	10.10.9.56	DB2ACD	CALL	DB2_INSTANCE_SQLMON_SNAPSHOT	DB2INST2	4
10.10.9.56	10.10.9.56	DB2ACD	SELECT	SESSION_COUNTERS	DB2INST2	11
10.10.9.56	10.10.9.56	DB2ACD	SELECT	sysDummy	DB2INST2	11
10.10.9.56	10.10.9.56	DB2BP	ALTER TABLE	payroll	DB2INST2	1
10.10.9.56	10.10.9.56	DB2BP	CALL	SQLC2F0A	DB2INST2	1
10.10.9.56	10.10.9.56	DB2BP	CREATE FUNCTION	cc_function	DB2INST2	1
10.10.9.56	10.10.9.56	DB2BP	CREATE TABLE	CC	DB2INST2	3
10.10.9.56	10.10.9.56	DB2BP	CREATE TABLE	creditcard	DB2INST2	1
10.10.9.56	10.10.9.56	DB2BP	CREATE TABLE	customerinfo	DB2INST2	1
10.10.9.56	10.10.9.56	DB2BP	CREATE TABLE	payroll	DB2INST2	1
10.10.9.56	10.10.9.56	DB2BP	CREATE TABLE	ssn	DB2INST2	1
10.10.9.56	10.10.9.56	DB2BP	DROP TABLE	CC	DB2INST2	1
10.10.9.56	10.10.9.56	DB2BP	DROP TABLE	payroll	DB2INST2	1
10.10.9.56	10.10.9.56	DB2BP	INSERT	CC	DB2INST2	6
10.10.9.56	10.10.9.56	DB2BP	INSERT	creditcard	DB2INST2	2
10.10.9.56	10.10.9.56	DB2BP	INSERT	customerinfo	DB2INST2	38
10.10.9.56	10.10.9.56	DB2BP	INSERT	payroll	DB2INST2	3

c. Click **Commands List**.

This report displays a list of all unique SQL Verbs occurring within one-hour time slices, and a count of Total Access for the same time slice over the course of the reporting period.

Period Start	SQL Verb	Depth	Total access
2010-08-25 20:00:00.0	BEGIN	0	45
2010-08-25 20:00:00.0	CALL	1	45
2010-08-25 20:00:00.0	CREATE TABLE	0	6
2010-08-25 20:00:00.0	CREATE USER	0	2
2010-08-25 20:00:00.0	DROP TABLE	0	2
2010-08-25 20:00:00.0	DROP USER	0	1
2010-08-25 20:00:00.0	GRANT	0	14
2010-08-25 20:00:00.0	INSERT	0	33
2010-08-25 20:00:00.0	REVOKE	0	1
2010-08-25 20:00:00.0	SELECT	0	67
2010-08-25 20:00:00.0	UPDATE	0	4
2010-08-25 21:00:00.0	CREATE TABLE	0	1
2010-08-25 21:00:00.0	DROP TABLE	0	1
2010-08-25 21:00:00.0	EXECUTE	0	6
2010-08-25 21:00:00.0	GRANT	0	2
2010-08-25 21:00:00.0	INSERT	0	15
2010-08-25 21:00:00.0	SELECT	0	14
2010-08-26 10:00:00.0	CREATE DATABASE	0	1
2010-08-26 10:00:00.0	CREATE LOGIN	0	3
2010-08-26 10:00:00.0	CREATE SCHEMA	0	3

d. Click **Full SQL By Client IP**.

This report displays a list of Full SQL IDs for each monitored session broken down by Client IP during the capturing of Full SQL details for the reporting period.

Full SQL ID	Timestamp	Client IP	DB User Name	Session Start	Source Program	Full Sql	Count of FULL SQLs
0		10.10.9.56	DB2INST2	2010-08-27 00:39:47.0	DB2BP	N/A	0
0		10.10.9.56	DB2INST2	2010-08-27 00:44:27.0	DB2ACD	N/A	0
0		10.10.9.56	DB2INST2	2010-08-27 00:44:27.0	DB2HMON	N/A	0
0		10.10.9.56	DB2INST2	2010-08-27 00:45:27.0	DB2ACD	N/A	0
0		10.10.9.56	DB2INST2	2010-08-27 00:45:27.0	DB2HMON	N/A	0
0		10.10.9.56	DB2INST2	2010-08-27 00:49:27.0	DB2ACD	N/A	0
0		10.10.9.56	DB2INST2	2010-08-27 00:49:27.0	DB2HMON	N/A	0
0		10.10.9.56	DB2INST2	2010-08-27 00:51:27.0	DB2ACD	N/A	0
0		10.10.9.56	DB2INST2	2010-08-27 00:51:27.0	DB2HMON	N/A	0
0		10.10.9.56	DB2INST2	2010-08-27 00:54:27.0	DB2ACD	N/A	0
0		10.10.9.56	DB2INST2	2010-08-27 00:54:27.0	DB2HMON	N/A	0
0		10.10.9.56	DB2INST2	2010-08-27 00:54:56.0	DB2BP	N/A	0
0		10.10.9.56	DB2INST2	2010-08-27 00:57:27.0	DB2ACD	N/A	0
0		10.10.9.56	DB2INST2	2010-08-27 00:57:27.0	DB2HMON	N/A	0
0		10.10.9.56	DB2INST2	2010-08-27 00:59:27.0	DB2ACD	N/A	0
0		10.10.9.56	DB2INST2	2010-08-27 00:59:27.0	DB2HMON	N/A	0
0		10.10.9.56	DB2INST2	2011-12-29 22:43:00.0	DB2BP	N/A	0
0		10.10.9.56	DB2INST2	2011-12-29 22:46:07.0	DB2ACD	N/A	0
0		10.10.9.56	DB2INST2	2011-12-29 22:47:07.0	DB2ACD	N/A	0
0		10.10.9.56	DB2INST2	2011-12-29 22:53:07.0	DB2ACD	N/A	0

g. Click Object Activity Summary.

This report displays a list of all activity associated with a defined object name or wildcard. For the purposes of this lab, we have set the ObjectName value equal to **CreditCard**.

Client IP	Source Program	SQL Verb	Depth	Object Name	Total access
10.10.9.240	IBM-6CD8U7TIXYD:DB2JCC_APPLI	SELECT	0	CreditCard	15
10.10.9.240	SQLI	CREATE TABLE	0	creditcard	7
10.10.9.240	SQLI	DROP TABLE	0	creditcard	7
10.10.9.240	SQLI	INSERT	0	creditcard	77
10.10.9.240	SQLI	SELECT	0	creditcard	1
10.10.9.248	JCONNECT 0.6.0.0	SELECT	0	creditcard	10
10.10.9.248	JDBC CONNECT CLIENT	SELECT	0	CREDITCARD	96
10.10.9.251	MICROSOFT SQL SERVER MANAGEMENT STUDIO - QUERY	SELECT	0	creditcard	18
10.10.9.251	SQLCMD	SELECT	0	creditcard	8
10.10.9.251	SQLCMD.EXE	CREATE TABLE	0	CreditCard	1
10.10.9.251	SQLCMD.EXE	DROP TABLE	0	creditcard	1
10.10.9.251	SQLCMD.EXE	INSERT	0	creditcard	15
10.10.9.251	SQLCMD.EXE	SELECT	0	creditcard	4
10.10.9.251	SQLWB.EXE	SELECT	0	creditcard	4
10.10.9.251	SYSTEM	SELECT	0	creditcard	2
10.10.9.252	DB2BP.EXE	CREATE TABLE	0	creditcard	1
10.10.9.252	DB2BP.EXE	INSERT	0	creditcard	2
10.10.9.252	DB2BP.EXE	SELECT	0	creditcard	4
10.10.9.252	DB2BP.EXE	SELECT	1	creditcard	1
10.10.9.253	SQLCMD.EXE	SELECT	0	creditcard	3

h. Click Objects List.

This report displays a list of all unique Objects, and a count of Total Access for hourly time slices during the entire reporting period.

Period Start	Object Name	Total access
2010-08-25 20:00:00.0	AccountTable	10
2010-08-25 20:00:00.0	bill	4
2010-08-25 20:00:00.0	DBMS_APPLICATION_INFO.SET_MODULE	30
2010-08-25 20:00:00.0	DBMS_OUTPUT.DISABLE	15
2010-08-25 20:00:00.0	DECODE	15
2010-08-25 20:00:00.0	DUAL	32
2010-08-25 20:00:00.0	finance	9
2010-08-25 20:00:00.0	finance.TransactionTable	1
2010-08-25 20:00:00.0	harry	2
2010-08-25 20:00:00.0	harry.payroll	1
2010-08-25 20:00:00.0	joe	3
2010-08-25 20:00:00.0	payroll	26
2010-08-25 20:00:00.0	resource	2
2010-08-25 20:00:00.0	Revenue	11
2010-08-25 20:00:00.0	SYSTEM.PRODUCT_PRIVS	30
2010-08-25 20:00:00.0	TEMP	2
2010-08-25 20:00:00.0	to_char	1
2010-08-25 20:00:00.0	TransactionTable	10
2010-08-25 20:00:00.0	UPPER	30
2010-08-25 20:00:00.0	USERS	2

i. Click **One User One IP**.

This report displays the number of client sessions, and unique Client IPs corresponding to each DB User Name executing SQL transactions during the reporting period.

DB User Name	Count of Client IP	Count of Sessions
?	2	22
ADMINISTRATOR	3	56
APPLSYSUB	1	449
APPS	2	1156
BILL	2	11
CSLVI	1	8
DB2ADMIN	2	3
DB2INST	1	3
DB2INST1	1	2
DB2INST2	5	1095
FINANCE	1	4
GU0002	1	8
GUARDIUM_AUDIT	1	3
HARRY	3	46
IBMUSER	1	11
INFORMDX	3	225
JOE	6	136
JOED	4	57
OWBSYS	1	2

j. Click **Sessions List**.

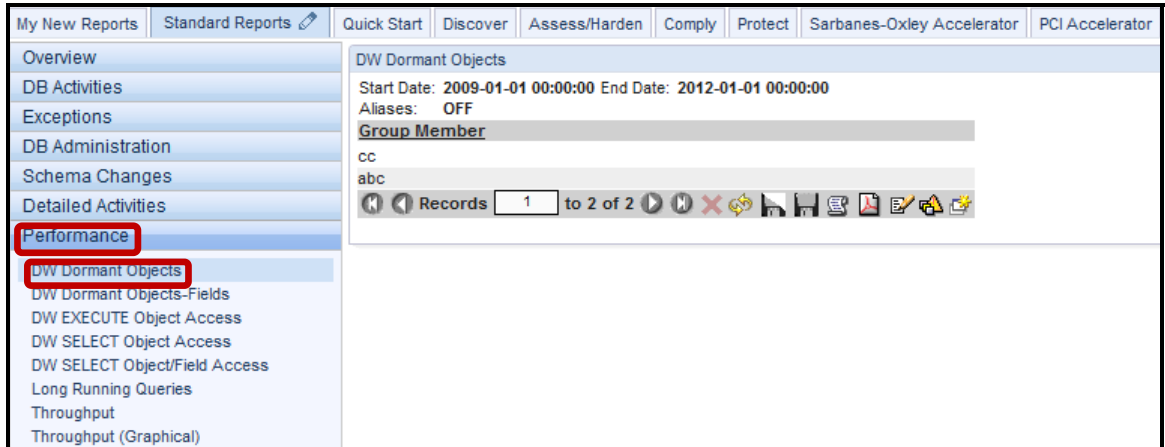
This report displays Session details for all sessions occurring during the reporting period.

Timestamp	Session Start	Server Type	Client IP	Server IP	Client Port	Server Port	Network Protocol	DB Protocol	DB Protocol Version	DB User Name	Source Program	Count of Sessions
2010-08-26 00:32:51.0	2010-08-25 20:00:33.0	ORACLE	10.10.9.57	10.10.9.57	24546	161	BEQUEATH	TNS	3.13	JOE	SQLPLUS@OSPREY1	1
2010-08-26 00:39:33.0	2010-08-25 20:07:06.0	ORACLE	10.10.9.57	10.10.9.57	24949	42	BEQUEATH	TNS	3.13	JOE	SQLPLUS@OSPREY1	1
2010-08-26 00:39:33.0	2010-08-25 20:07:24.0	ORACLE	10.10.9.57	10.10.9.57	24970	60	BEQUEATH	TNS	3.13	HARRY	SQLPLUS@OSPREY1	1
2010-08-26 00:39:33.0	2010-08-25 20:08:19.0	ORACLE	10.10.9.57	10.10.9.57	25031	115	BEQUEATH	TNS	3.13	HARRY	SQLPLUS@OSPREY1	1
2010-08-26 00:43:06.0	2010-08-25 20:11:51.0	ORACLE	10.10.9.57	10.10.9.57	25242	71	BEQUEATH	TNS	3.13	TOM	SQLPLUS@OSPREY1	1
2010-08-26 00:43:06.0	2010-08-25 20:11:54.0	ORACLE	10.10.9.57	10.10.9.57	25243	74	BEQUEATH	TNS	3.13	TOM	SQLPLUS	1
2010-08-26 00:43:06.0	2010-08-25 20:11:55.0	ORACLE	10.10.9.57	10.10.9.57	25250	75	BEQUEATH	TNS	3.13	TOM	SQLPLUS	1
2010-08-26 00:46:26.0	2010-08-25 20:13:44.0	ORACLE	10.10.9.57	10.10.9.57	25349	184	BEQUEATH	TNS	3.13	BILL	SQLPLUS@OSPREY1	1
2010-08-26 00:46:26.0	2010-08-25 20:14:11.0	ORACLE	10.10.9.57	10.10.9.57	25368	211	BEQUEATH	TNS	3.13	HARRY	SQLPLUS@OSPREY1	1
2010-08-26 00:46:26.0	2010-08-25 20:14:40.0	ORACLE	10.10.9.57	10.10.9.57	25413	240	BEQUEATH	TNS	3.13	JOE	SQLPLUS@OSPREY1	1
2010-08-26 00:46:26.0	2010-08-25 20:15:55.0	ORACLE	10.10.9.57	10.10.9.57	25528	59	BEQUEATH	TNS	3.13	JOE	SQLPLUS@OSPREY1	1
2010-08-26 00:46:26.0	2010-08-25 20:16:17.0	ORACLE	10.10.9.57	10.10.9.57	25555	81	BEQUEATH	TNS	3.13	JOE	SQLPLUS@OSPREY1	1
2010-08-26 00:46:26.0	2010-08-25 20:16:44.0	ORACLE	10.10.9.57	10.10.9.57	25575	108	BEQUEATH	TNS	3.13	JOE	SQLPLUS@OSPREY1	1
2010-08-26 00:49:46.0	2010-08-25 20:17:05.0	ORACLE	10.10.9.57	10.10.9.57	25605	129	BEQUEATH	TNS	3.13	FINANCE	SQLPLUS@OSPREY1	1
2010-08-26 00:49:46.0	2010-08-25 20:18:53.0	ORACLE	10.10.9.57	10.10.9.57	25719	236	BEQUEATH	TNS	3.13	FINANCE	SQLPLUS@OSPREY1	1
2010-08-26 00:49:46.0	2010-08-25 20:19:37.0	ORACLE	10.10.9.57	10.10.9.57	25758	25	BEQUEATH	TNS	3.13	HARRY	SQLPLUS@OSPREY1	1
2010-08-26 00:49:46.0	2010-08-25 20:19:43.0	ORACLE	10.10.9.57	10.10.9.57	25765	31	BEQUEATH	TNS	3.13	HARRY	SQLPLUS	1
2010-08-26 00:51:00.0	2010-08-25 20:20:14.0	ORACLE	10.10.9.57	10.10.9.57	25809	62	BEQUEATH	TNS	3.13	FINANCE	SQLPLUS@OSPREY1	1
2010-08-26 00:56:41.0	2010-08-25 20:24:12.0	ORACLE	10.10.9.57	10.10.9.57	26039	44	BEQUEATH	TNS	3.13	FINANCE	SQLPLUS@OSPREY1	1
2010-08-26 01:40:33.0	2010-08-25 21:35:06.0	SYBASE	10.10.9.57	10.10.9.57	32969	4200	TCP	TDS	5.0	SA	ISQL	1

__9. **Standard Reports – Performance.**

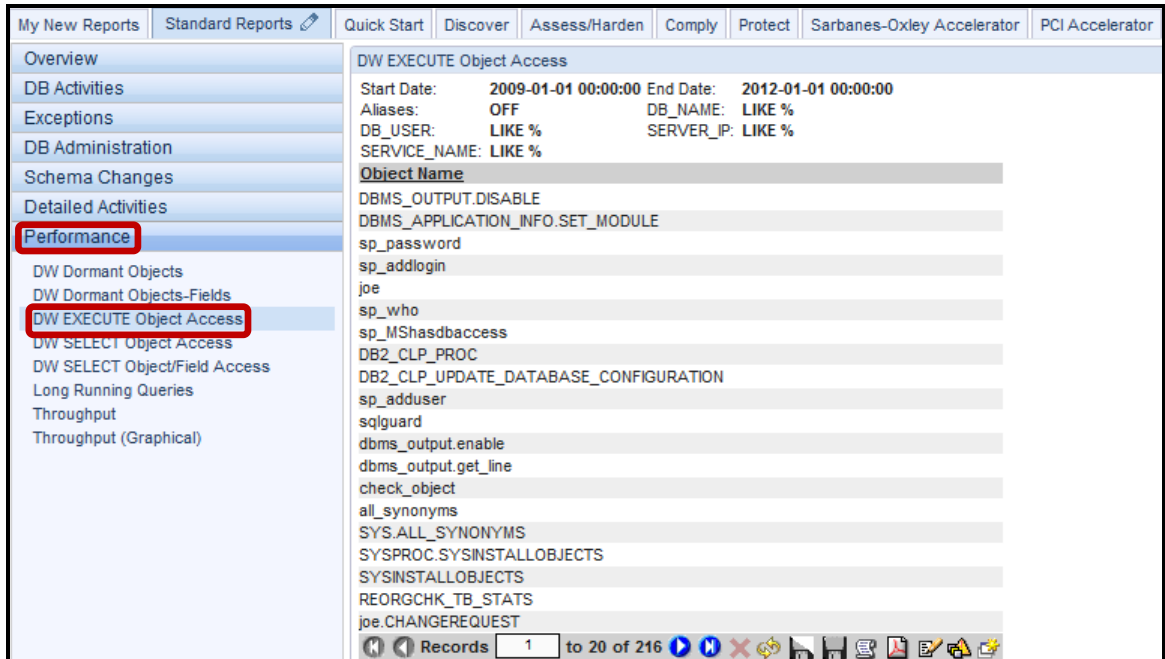
- __a. Click **DW Dormant Objects** under the **Performance** tab.

This report displays the list of Data Warehouse group members that were dormant during the reporting period based upon those members of the DW Objects group.



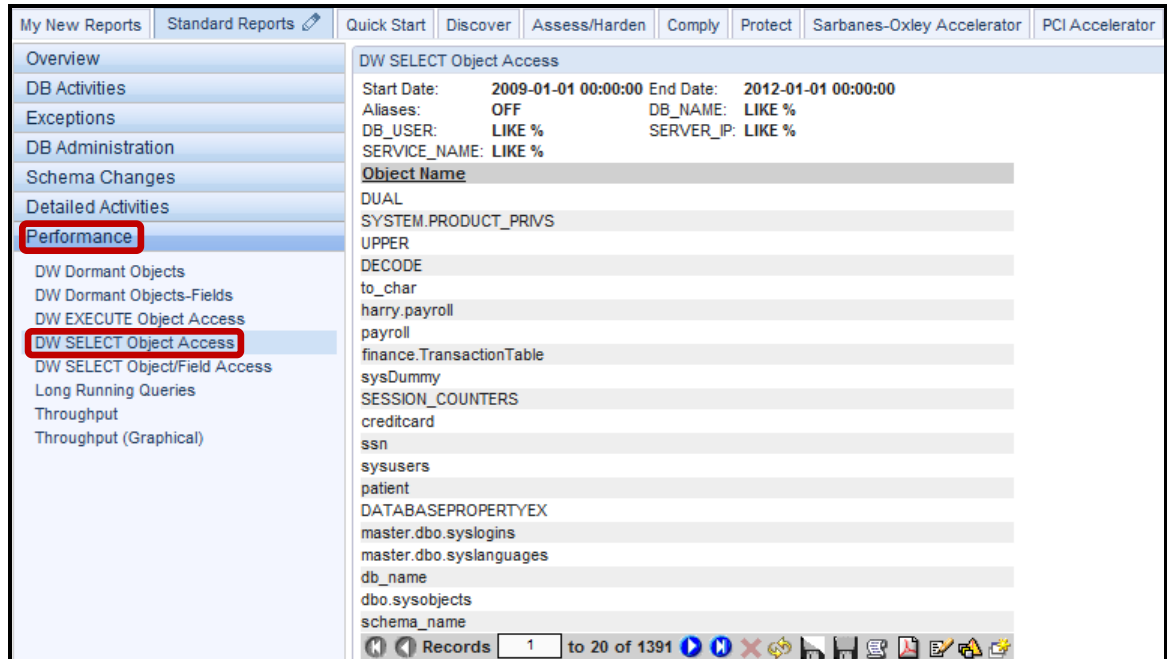
- __b. Click **DW EXECUTE Object Access**.

This report displays the list of objects upon which an Execute command (Execute, Exec, or Call) was issued during the reporting period.



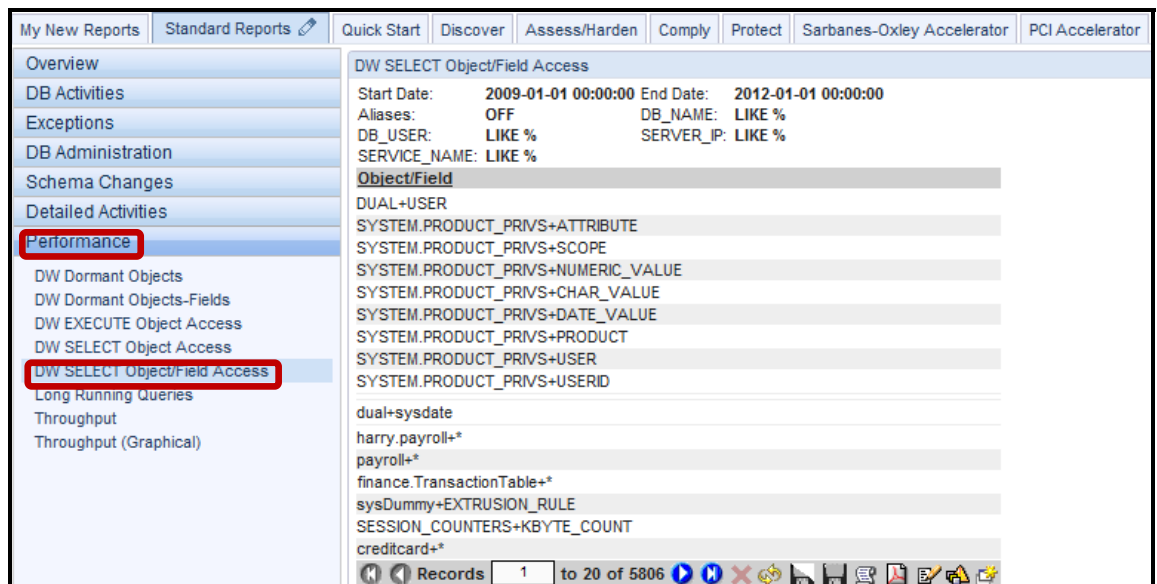
c. Click **DW SELECT Object Access**.

This report displays a list of objects upon which a Select command was issued during the reporting period.



d. Click **DW SELECT Object/Field Access**.

This report displays a combination of Object and Field upon which a Select command was issued during the reporting period.



e. Click **Long Running Queries.**

This report displays long running queries for the reporting period, with the longest average execution time first. For each SQL query, it lists the Client IP, Server IP, SQL, Period Start (from the Access Period entity), Average Execution Time, and the count of occurrences. Would your DBA's find this to be an interesting type of report?

Client IP	Server IP	SQL	Period Start	Average Execution Time	Total Access
10.10.9.240	10.10.9.252	select TABNAME, TABSCHEMA, TYPE, BASE_TABNAME, BASE_TABSCHEMA, CREATE_TIME from syscat.tables where type = 7 AND TABSCHEMA = 7 ORDER BY TABNAME	2011-08-01 18:00:00	0.4203344	1
10.10.9.240	10.10.9.58	select * from salary	2010-09-09 22:00:00	0.2600016	1
10.10.9.240	10.10.9.252	CALL SYSIBM.SQLTABLES(?, ?, ?, ?)	2011-08-01 10:00:00	0.2554234	1
10.10.9.240	10.10.9.58	Select id,frame,name,zip,email from emp1	2011-08-27 21:00:00	0.2312124	1
10.10.9.58	10.10.9.58	Select id,frame,name,zip,email from emp1	2011-08-27 21:00:00	0.2312121	1
10.10.9.57	10.10.9.57	grant update (name,sn_card) on creditcard to joe	2010-09-15 12:00:00	0.1815882	1
10.10.9.58	10.10.9.58	select * from emp1	2011-08-27 22:00:00	0.1755345	1
10.10.9.58	10.10.9.58	select * from emp1	2011-08-27 22:00:00	0.1580968	1
10.10.9.252	10.10.9.252	select * from creditcard	2010-11-30 15:00:00	0.1477312	1
10.10.9.240	10.10.9.252	SELECT ?, ?, ?, ? FROM SYSIBM.SYSDUMMY1	2011-08-01 10:00:00	0.0294125	1
10.10.9.252	10.10.9.252	select * from creditcard	2010-11-30 15:00:00	0.108953	1
10.10.9.58	10.10.9.58	select * from payroll	2010-08-27 00:00:00	0.155519	1
10.10.9.57	10.10.9.57	exec sp_who	2010-11-02 11:00:00	0.144544	1
10.10.9.58	10.10.9.58	select * from joe	2011-07-30 14:00:00	0.138381	2
10.10.9.57	10.10.9.57	select * from creditcard	2010-10-26 18:00:00	0.090224	1
10.10.9.252	10.10.9.252	select create_function(?) FROM SYSIBM.SYSDUMMY1	2010-11-30 15:00:00	0.089863	1
10.10.9.59	10.10.9.59	DECLARE SEQUENCE_OWNER VARCHAR(7); SEQUENCE_NAME VARCHAR(7); v_user_id number; v_commands VARCHAR(7); NEW_VALUE NUMBER	2010-09-22 00:00:00	0.76089	5
10.10.9.59	10.10.9.59	BEFORE SELECT user_id INTO v_user_id FROM user_users; v_commands = ? ? v_user_id ? ?; SEQUENCE_OWNER = ?; SEQUENCE_NAME = ? v_commands ?; NEW_VALUE = ?; SYS.DIMS_CDC_MPP.BUMP_SEQUENCE(SEQUENCE_OWNER => SEQUENCE_OWNER, SEQUENCE_NAME => SEQUENCE_NAME, NEW_VALUE => NEW_VALUE); END;	2010-09-22 00:00:00	0.76089	5
10.10.9.57	10.10.9.57	select text from dba_source where owner = ?	2010-08-01 03:00:00	0.75950	1
10.10.9.57	10.10.9.57	select DISTINCT(TYPENAME)owner_text from dba_source where owner=?	2010-09-01 03:00:00	0.62132	1

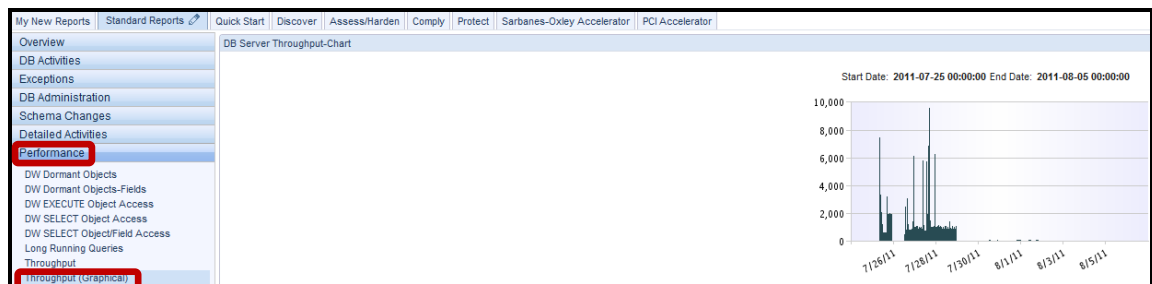
f. Click Throughput.

This report displays throughput details in terms of total access over a series of hourly time slices during the reporting period.

Period Start	Total access
2010-08-25 20:00:00.0	175
2010-08-25 21:00:00.0	39
2010-08-26 10:00:00.0	244
2010-08-26 12:00:00.0	3
2010-08-27 00:00:00.0	227
2010-08-27 03:00:00.0	1
2010-08-27 13:00:00.0	129
2010-08-29 06:00:00.0	92
2010-08-29 07:00:00.0	6
2010-08-31 15:00:00.0	71
2010-08-31 16:00:00.0	70
2010-09-01 03:00:00.0	42
2010-09-01 04:00:00.0	22
2010-09-01 10:00:00.0	52
2010-09-02 03:00:00.0	48
2010-09-02 04:00:00.0	52
2010-09-02 06:00:00.0	266
2010-09-02 07:00:00.0	229
2010-09-02 08:00:00.0	90
2010-09-02 09:00:00.0	89

g. Click Throughput (Graphical).

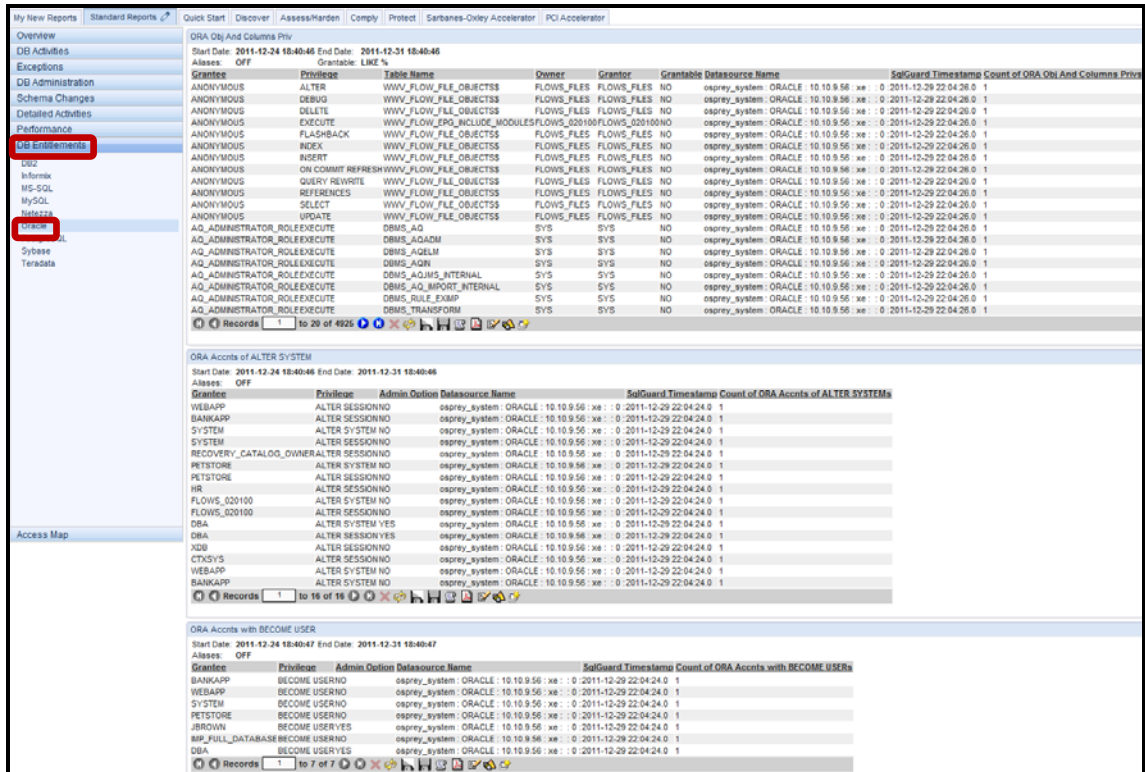
This graphical report displays throughput details in terms of total access over the entire reporting period. We can see from this report that activity peaked during 28 July 2011 before dropping significantly on subsequent days.



10. Standard Reports – DB Entitlements.

a. Click Oracle under the DB Entitlements tab.

Note: We have already explored details on DB Entitlement reports during a previous lab. If you have not performed that lab, and have a deeper interest in Entitlement reports, please take the time to complete the previous lab on DB Entitlement Reports.



Along with authenticating users and restricting role-based access privileges to data, even for the most privileged database users, there periodically is a need to perform entitlement reviews. This process can validate and ensure that users only have the privileges required to perform their duties. This also is known as database user rights attestation reporting.

Use the predefined database entitlement (privilege) reports of InfoSphere Guardium to see who has system privileges and who has granted these privileges to other users and roles. Database entitlement reports are important for auditors tracking changes to database access and to ensure that security holes do not exist from expired accounts or ill-granted privileges.

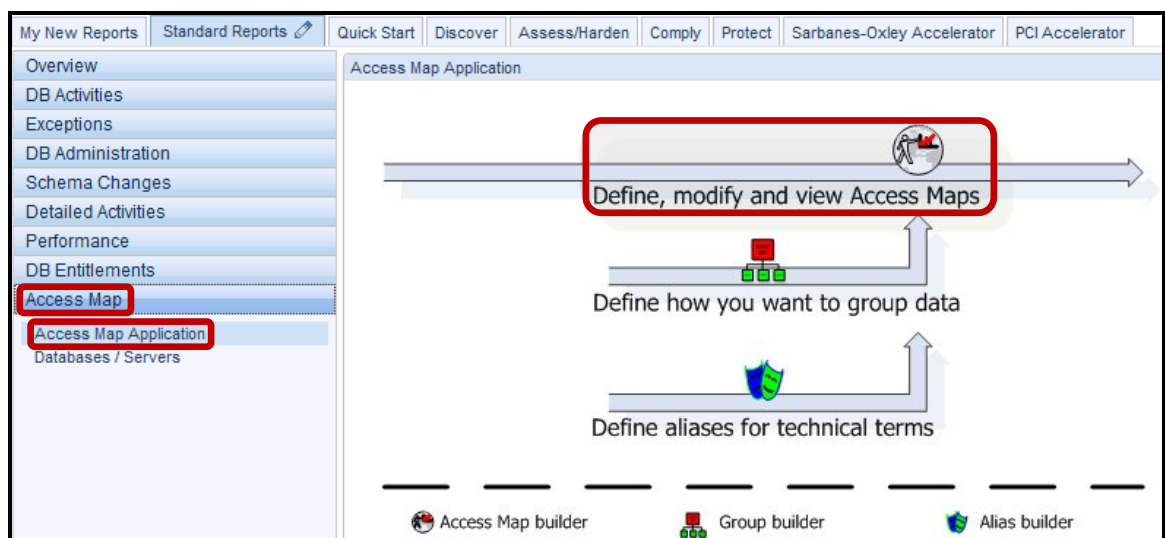
Custom database entitlement reports have been created to save configuration time and to facilitate the uploading and reporting of data from the following databases: DB2; Informix; MS SQL; MySQL; Netezza; Oracle; PostgreSQL; Sybase; and Teradata.

11. Standard Reports – DB Access Map.

- a. Click **Access Map Application** under the **Access Map** tab.

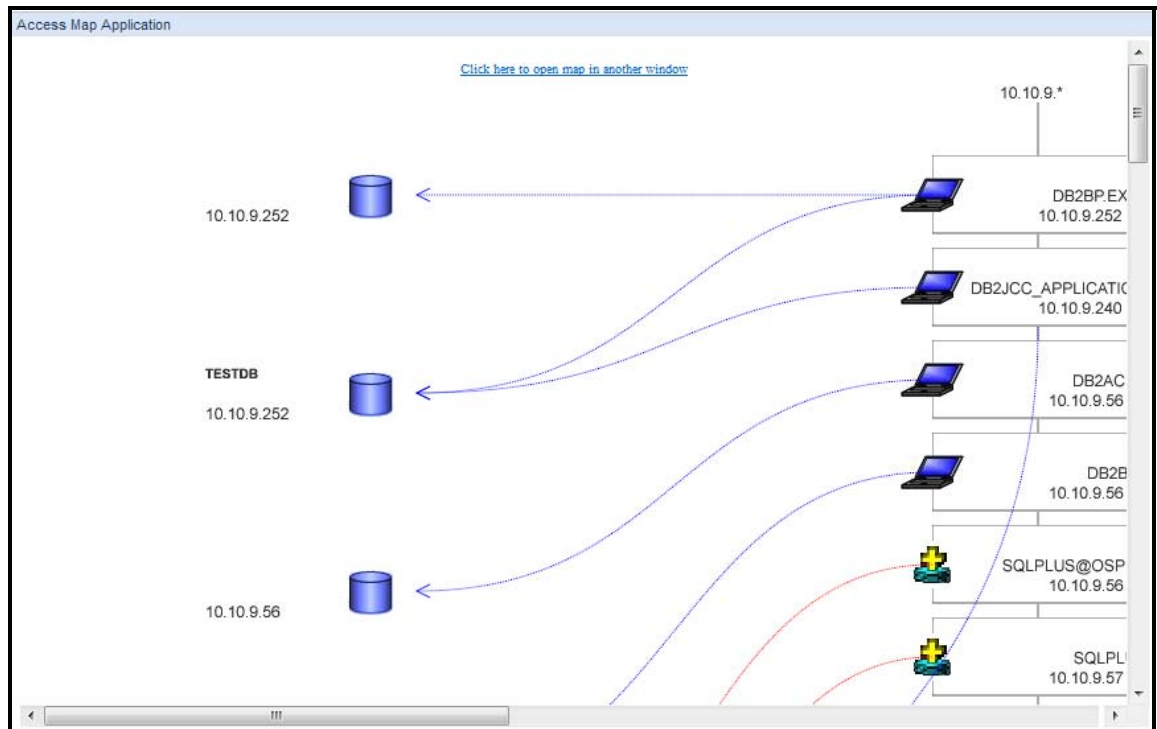
Access maps provide a convenient way to create a mapping of data access. This report displays in a visual map that shows all access paths derived from a set of criteria that you define. Criteria can be set based on any combination, including server type or location on the network (IPs and subnets). In addition, you can group access patterns together, since one of the main problems in reviewing access data is the detailed granularity. You are able to get a visual map by grouping similar access paths, which can be meaningful in understanding your access environment. Using this visual depiction, you can then navigate and get further information on any one access path in the map.

- b. Click **Define, modify and view Access Maps**.

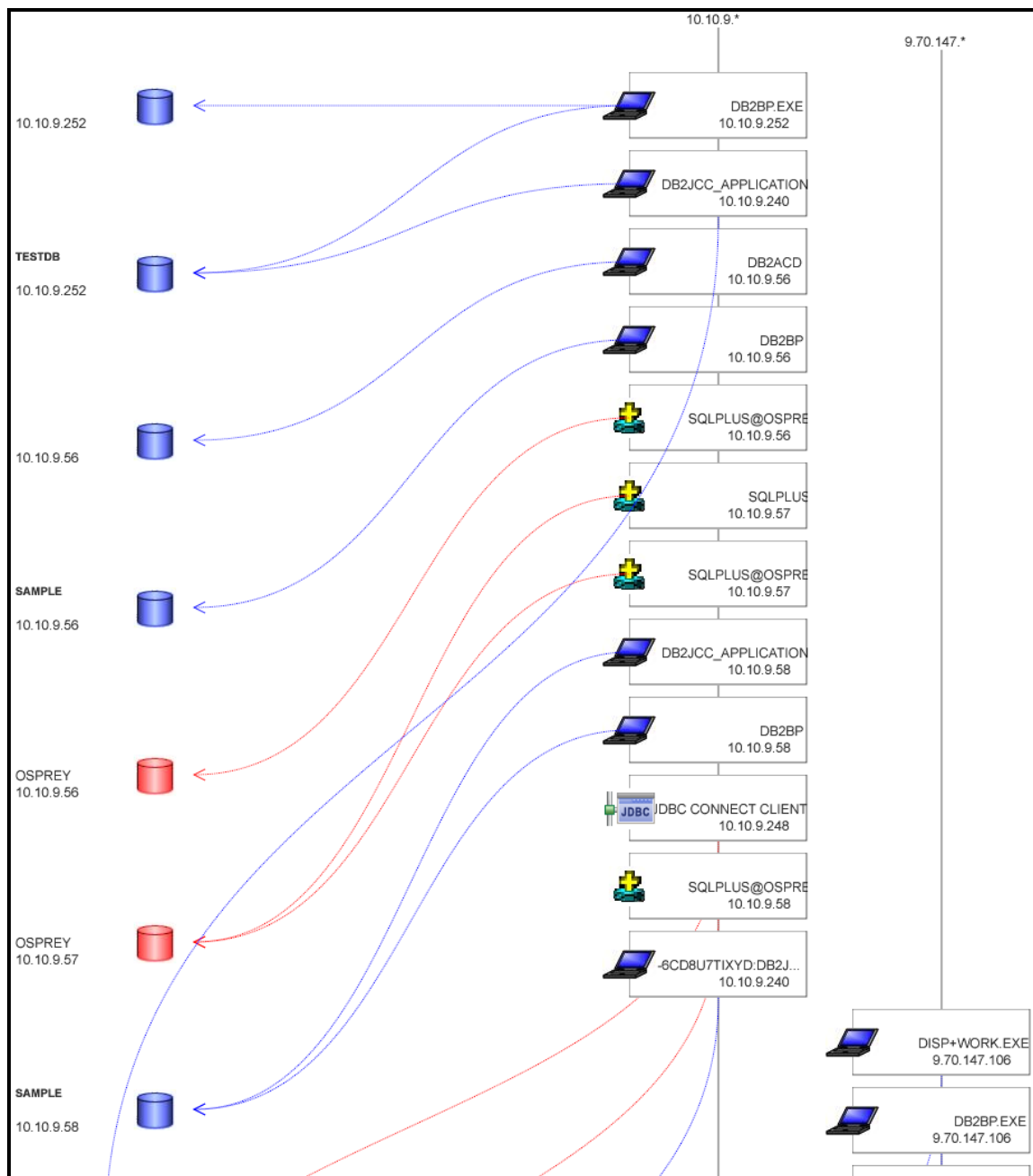


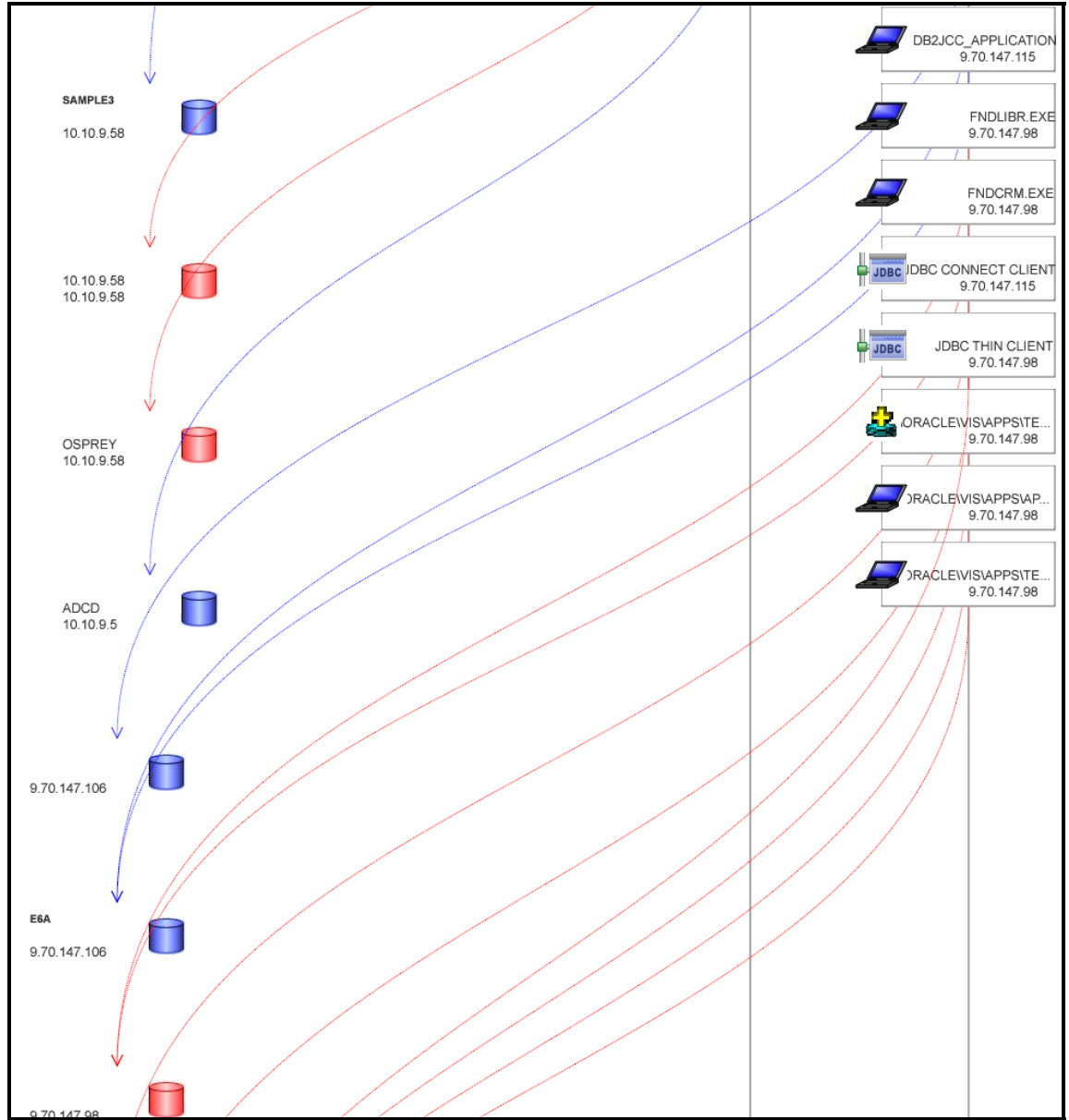
- c. Select an existing map name – '**Access Map**' – from the drop-down list, and then click **Save & View**.

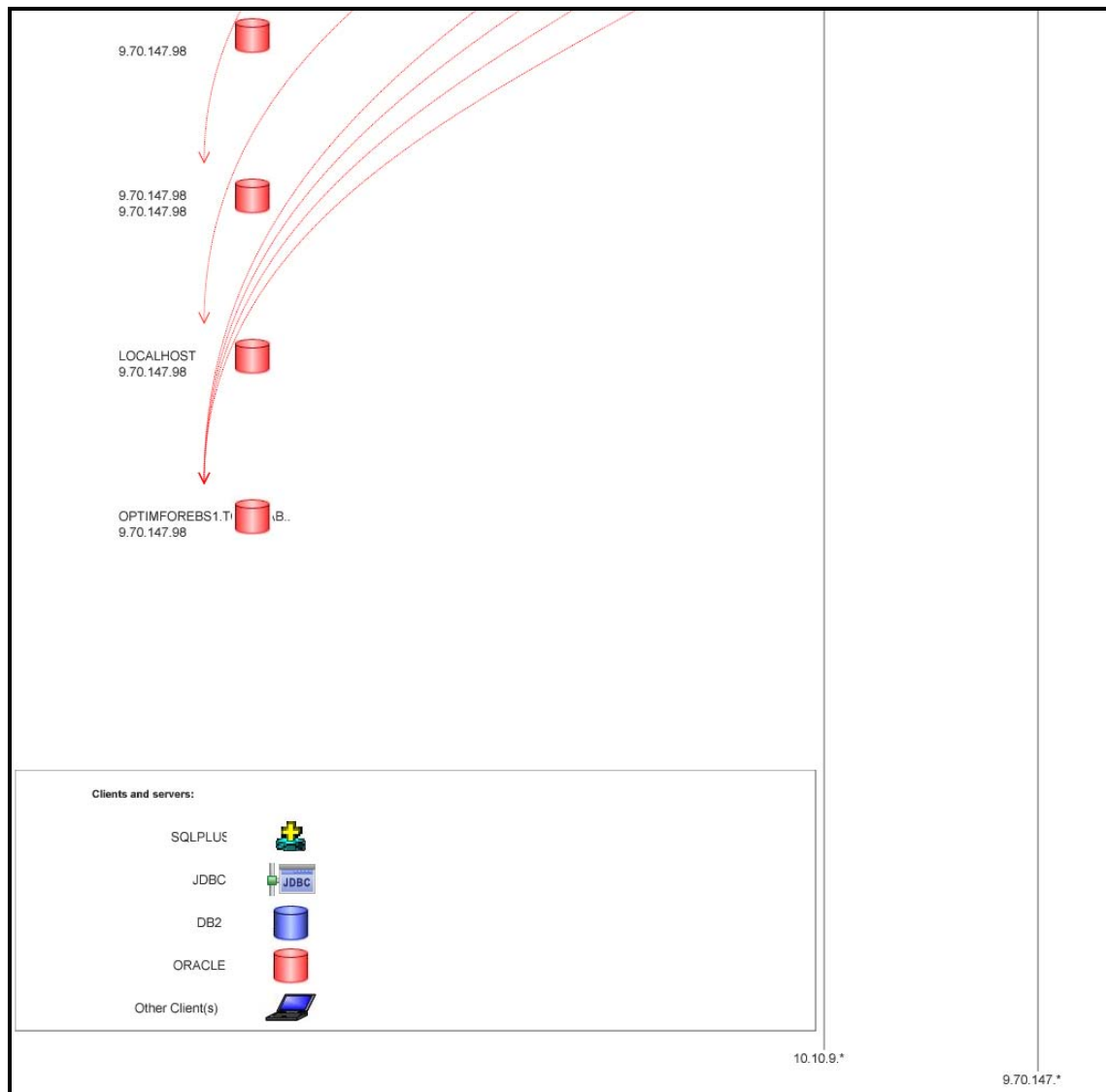
- d. Click the link [Click here to open map in another window](#) for the large view once the initial map appears.



A full view displays a handy visual of access to your database systems.

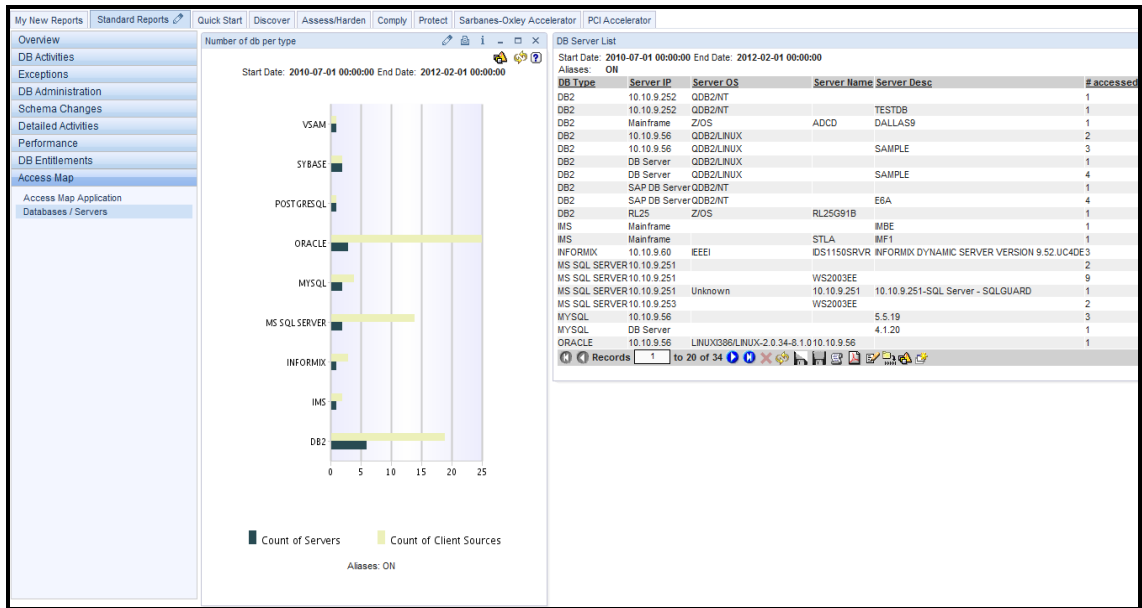






e. Click **Databases / Servers**.

We see two reports side by side.



The 'Number of db per type' report is the same one we saw earlier in the Overview tab. It displays a double bar for each type of database server for which traffic was seen. Each double bar is labeled with the server type. For each server type, the top bar represents the number of Client IPs, and the bottom bar represents the total number of Server IPs.

The 'DB Server List' report is similar to other reports that we have seen. It lists all database servers seen during the reporting period. It displays the Server Type, Server IP, Server OS, Server Host Name, Server Description, and the total count of Client/Server entities for that row (the total number of clients).

This is the end of the exploration of standard reports. Now it is up to you to put what you have seen to good use for you and your organization.

Thank You

11.2 Standard Reports Layout

Overview Tab

- Overview
 - Number of db per type
 - Request Rate
 - View Installed Policy

DB Activities Tab

- Activity By Client IP
- Database Servers
 - Databases Discovered
 - Servers Accessed
- DML Execution on Sensitive Objects
- IMS Access
- IMS Data Access Details
- IMS Event
- IMS Object
- Sensitive Objects Usage
- Sessions By Server Type

Exceptions Tab

- Active Users Last Login
- Active Users with No Activity
- Exception Count
- Exceptions Distribution
- Exceptions Monitor
- Failed User Login Attempts
- Policy Violations
- SQL Errors
- Terminated Users Logins
- Terminated Users Failed Login Attempts

DB Administration Tab

- Admin Users Login
- Administrative Commands Usage
- Administrative Objects Usage
- BACKUP Commands Execution
- DB Predefined Users Login
- DBCC Commands Execution
- DML Execution on Administrative Objects
- GRANT Commands Execution
- KILL Commands Execution
- RESTORE Commands Execution
- REVOKE Commands Execution

Schema Changes Tab

- ALTER Commands Execution
- CREATE Commands Execution
- DDL Commands
- DDL Distribution
- DROP Commands Execution

Detailed Activities Tab

- Archive Candidates
- Classification Process Results
- Client IP Activity Summary
- Commands List
- Flat LOG List
- Full SQL By Client IP
- Full SQL By DB User Name
- Hourly Access Details
- Object Activity Summary
- Objects List
- One User One IP
- Sessions List
- Windows File Share Activity

Performance Tab

- DW Dormant Objects
- DW Dormant Objects-Fields
- DW EXECUTE Object Access
- DW SELECT Object Access
- DW SELECT Object/Field Access
- Long Running Queries
- Throughput
- Throughput (Graphical)

DB Entitlements Tab

- DB2
- Informix
- MS-SQL
- MYSQL
- Netezza
- Oracle
- PostgreSQL
- Sybase
- Teradata

Access Map Tab

- Access Map Application
- Databases / Servers (DB Server List / Number of db per type)

Standard Reports review

- __1. All of the standard reports are displayed for:
- __a. Users with the "User" role.
 - __b. Users with the "Admin" role.
 - __c. Users with the "User", "Admin", "PCI", "SOX" and "Data Privacy" roles.
 - __d. Not all standard reports are displayed; others can be added by customizing the user interface.
- __2. Can default reports be modified?
- __a. Yes, but only to change the sort order.
 - __b. Yes, in any way.
 - __c. No, but they can be cloned (copied).
- __3. Reports can be filtered on any field.
(**True** or **False**).
- __4. The dates entered for selecting report ranges can be:
- __a. Absolute (for example, 2011-08-21 17:53:00).
 - __b. Relative (Now -1 day).
 - __c. Both absolute and relative.
- __5. To view/edit the report query when viewing a report, use:
- __a. The pencil icon on the top right of the report.
 - __b. The report/pencil icon at the bottom of the report.
 - __c. Editing the report query cannot be accessed from the report view.
- __6. To view/change the report runtime parameters, use:
- __a. The pencil icon on the top right of the report.
 - __b. The report/pencil icon at the bottom of the report.
 - __c. Editing runtime parameters cannot be accessed from the report view.

__7. Exceptions in the Guardium system are:

- __a. Policy violations.
- __b. SQL errors and failed logins.
- __c. System errors.
- __d. Really great reports.

Standard Reports review (Answers)

__1. All of the standard reports are displayed for:

D – Not all standard reports are displayed; others can be added by customizing the user interface.

__2. Can default reports be modified?

C – No, but they can be cloned (copied).

__3. Reports can be filtered on any field.
(True or False)

False. Reports can only be filtered on runtime parameters.

__4. The dates entered for selecting report ranges can be:

C – Both absolute and relative.

__5. To view/edit the report query when viewing a report, use:

B - The report/pencil icon at the bottom of the report.

__6. To view/change the report runtime parameters, use:

A - The pencil icon on the top right of the report.

__7. Exceptions in the Guardium system are:

B – SQL Errors and failed logins.

Lab 12 Payment Card Industry (PCI) Accelerator

12.1 Exploring the PCI Accelerator

Overview

IBM® InfoSphere® Guardium® provides a comprehensive solution that addresses database security and auditing needs across the enterprise, securing all kinds of sensitive data such as financial statements, personnel records and intellectual property. The PCI Accelerator is designed to harness the capabilities of the core InfoSphere Guardium product in order to address the specific requirements of PCI DSS. Built-in reports and policies accelerate your ability to comply with PCI by providing a base upon which you can build, either by customizing the Accelerator or complementing it with custom reports and policies. The PCI Accelerator's capabilities, along with interfaces to a variety of tools in the underlying system, are organized in a tabular fashion by Requirement, making the product fast to implement and easy to use.

The PCI Accelerator provides a wealth of insight into sensitive data access by both regular and privileged users. This includes specific objects accessed, SQL verbs used, total accesses, date/time of access, user ID, client address, invalid logical access attempts, and more. All this data is stored in a single secure repository. Workflow automation tools are provided to ensure required actions are taken promptly, and a verifiable audit trail is maintained as required by Section 10.

The InfoSphere Guardium solution provides:

- Built-in preconfigured reports developed specifically for SOX and PCI environments that usually include enterprise applications within their scope.
- Built-in SOX and PCI DSS policies for Oracle EBS and SAP.
- Separation of duties for SOX, PCI DSS, Basel II and data privacy regulations.
- Automation to reduce manual labor, improved data security and simplified compliance validation with major mandates, such as SOX, PCI DSS and data privacy regulations.
- Significant up-front and ongoing labor cost savings by identifying sensitive tables in common enterprise applications (for example, SAP, Oracle EBS and PeopleSoft) requiring protection, such as those containing PCI DSS or financial (SOX) information.

The InfoSphere Guardium Vulnerability Assessment module incorporates an extensive library of assessment tests, based on industry best practices, to flag missing patches, misconfigured privileges, default accounts, weak passwords and other static vulnerabilities. It also identifies dynamic or behavioral vulnerabilities, such as sharing of administration accounts and excessive administrator logins, by monitoring actual user activity over time. Finally, it includes embedded knowledge about enterprise applications such as Oracle EBS and SAP to protect critical tables reserved for these applications. A quarterly subscription service ensures that assessment tests are always up to date.

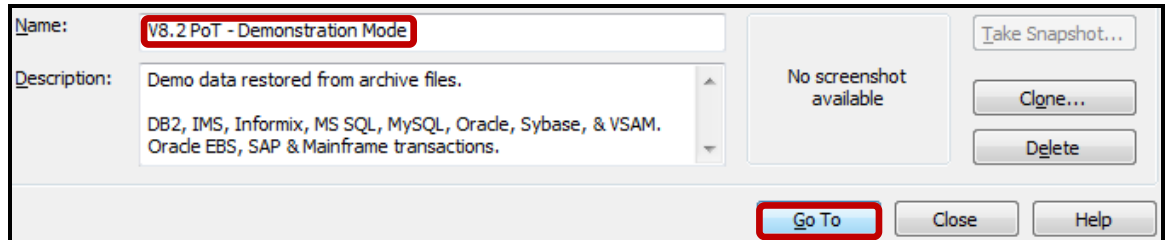
Objectives

This lab will demonstrate the ease of use meeting PCI Standards within the InfoSphere Guardium solution using the PCI Accelerator. This lab will focus on how the InfoSphere Guardium solution can accelerate PCI compliance using the following steps:

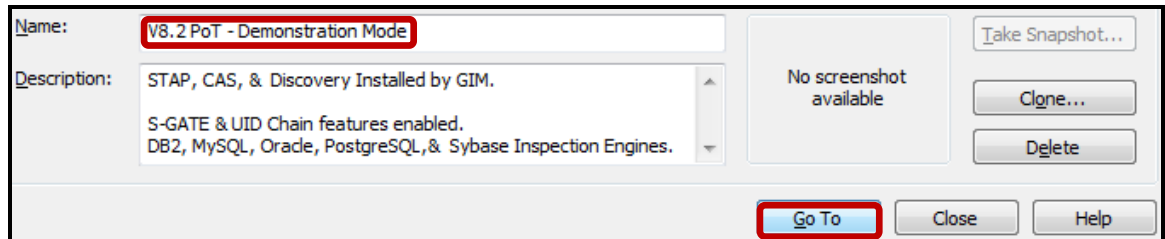
- __1. Explore the PCI Accelerator.
- __2. Find who accessed cardholder data.
 - __a. See Section 10.2.1 – Data Access.
 - __b. See Section 10.2.4 – Invalid Access.
- __3. Find who used Unauthorized Applications.
 - __a. See Plan and Organize Section – Unauthorized Application Access.
- __4. Show completed PCI reports.

___1. **Critical Step** – Before beginning this lab, ensure that both the Appliance and Database Server VMs are set to the ‘V8.2 PoT – Demonstration Mode’ snapshot. This is a critical step since only this snapshot contains all of the report data required by this lab. **Only start the Appliance VM. The Database Server VM is not required for this lab.**

___a. Set the Appliance VM to ‘V8.2 PoT – Demonstration Mode’, and restart the VM.



___b. **Critical Step** – The Database Server VM is not required for this lab. Set the Database Server VM to ‘V8.2 PoT – Demonstration Mode’ to shut it down. **Do Not Restart.**



- __2. Using the InfoSphere Guardium GUI, demonstrate the ease of use within the InfoSphere Guardium solution using the PCI Accelerator. Start the InfoSphere Guardium appliance VM and login.
- __a. From your laptop, go to <https://10.10.9.248:8443>
- __b. Login as **pot / guardium**.

Login

Please enter your information

User name:

Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

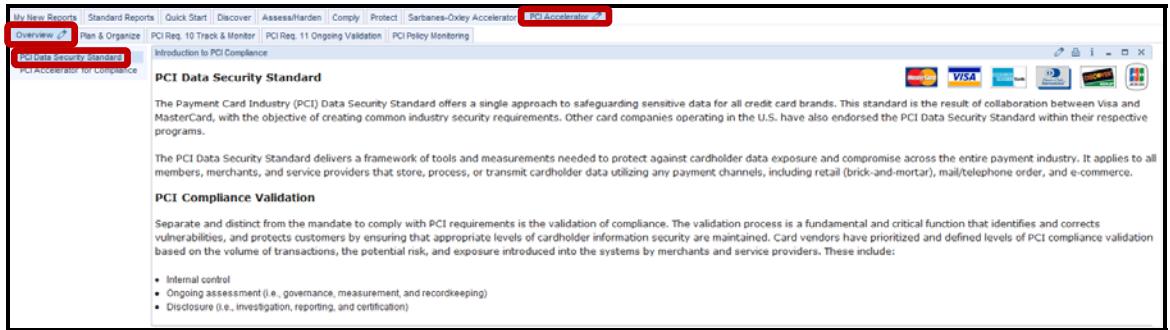
Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl, Jregistry/key © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

__3. PCI Accelerator – Overview.

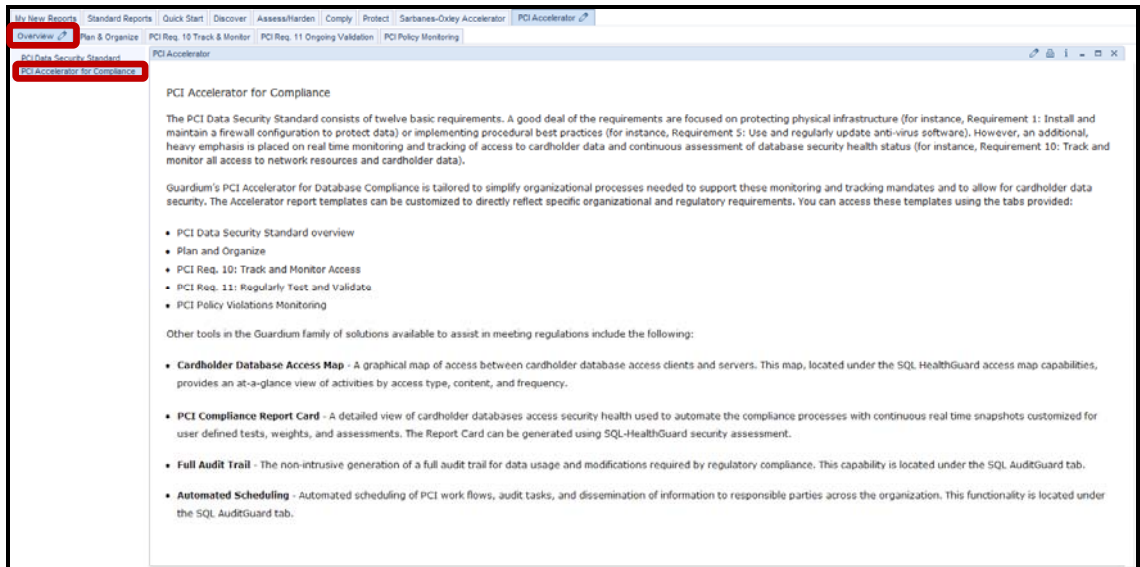
__a. Click **PCI Data Security Standard** under the **PCI Accelerator** and **Overview** tabs.

Read about the PCI Data Security Standard and PCI Compliance Validation.



__b. Click **PCI Accelerator for Compliance**.

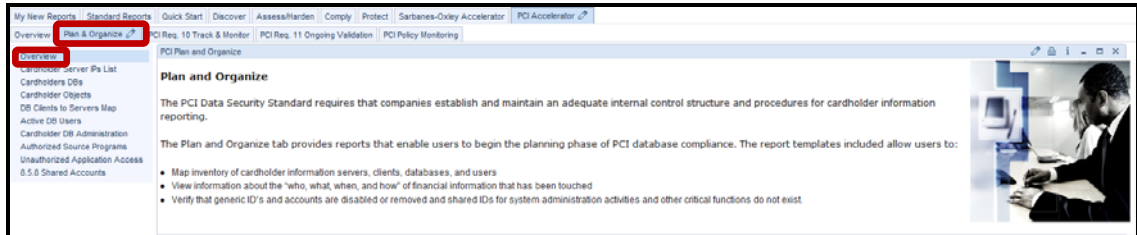
Read about the PCI Accelerator for Compliance.



4. PCI Accelerator – Plan & Organize.

a. Click Overview under the Plan & Organize tab.

The PCI Data Security Standard requires that companies establish and maintain an adequate internal control structure and procedures for cardholder information reporting.



b. Click Cardholder Server IPs List.

Server IP	Server Type	Database Name	Count of Sessions
10.10.9.251	MS SQL SERVER		48
10.10.9.251	MS SQL SERVER	FINANCIAL	12
10.10.9.251	MS SQL SERVER	MASTER	83
10.10.9.251	MS SQL SERVER	MODEL	4
10.10.9.251	MS SQL SERVER	MSDB	7
10.10.9.251	MS SQL SERVER	REPORTSERVER	4
10.10.9.251	MS SQL SERVER	REPORTSERVERTEMPDB	4
10.10.9.251	MS SQL SERVER	SENSITIVEDB	4
10.10.9.251	MS SQL SERVER	TEMPDB	4
10.10.9.56	DB2		11
10.10.9.56	DB2	SAMPLE	19
10.10.9.56	ORACLE		1
10.10.9.57	DB2		568
10.10.9.57	DB2	SAMPLE	348
10.10.9.57	MYSQL		29
10.10.9.57	MYSQL	MYSQL	42
10.10.9.57	ORACLE		183
10.10.9.57	SYBASE		1
10.10.9.57	SYBASE	GUARDIUM_QA	63
10.10.9.57	SYBASE	MASTER	32

- c. Click the 'Count of Sessions' column heading twice to sort the number of sessions from highest to lowest. This can give you an idea of the scale of sessions.

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

Overview | Plan & Organize | PCI Req. 10 Track & Monitor | PCI Req. 11 Ongoing Validation | PCI Policy Monitoring

Overview
 Cardholder Server IPs List
 Cardholders DBs
 Cardholder Objects
 DB Clients to Servers Map
 Active DB Users
 Cardholder DB Administration
 Authorized Source Programs
 Unauthorized Application Access
 8.5.8 Shared Accounts

PCI - Cardholder Server IPs
 Start Date: 2009-01-01 00:00:00 End Date: 2012-01-01 00:00:00
 Aliases: ON

Server IP	Server Type	Database Name	Count of Sessions
10.10.9.57	DB2		68
10.10.9.57	DB2	SAMPLE	48
10.10.9.57	ORACLE		83
10.10.9.251	MS SQL SERVER	MASTER	3
10.10.9.57	SYBASE	GUARDIUM_QA	3
10.10.9.251	MS SQL SERVER		8
10.10.9.57	MYSQL	MYSQL	2
10.10.9.57	SYBASE	MASTER	2
10.10.9.57	MYSQL		9
10.10.9.57	SYBASE	MODEL	7
10.10.9.57	SYBASE	SYBSYSTEMPROCS	7
10.10.9.57	SYBASE	TEST	7
10.10.9.57	SYBASE	SYBSYSTEMDB	5
10.10.9.57	SYBASE	TEMPDB	5
10.10.9.56	DB2	SAMPLE	9
10.10.9.251	MS SQL SERVER	FINANCIAL	2
10.10.9.56	DB2		1
10.10.9.251	MS SQL SERVER	MSDB	
10.10.9.251	MS SQL SERVER	REPORTSERVERTEMPDB	
10.10.9.251	MS SQL SERVER	TEMPDB	

Records 1 to 20 of 25

- d. Click **Cardholders DBs**.

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

Overview | Plan & Organize | PCI Req. 10 Track & Monitor | PCI Req. 11 Ongoing Validation | PCI Policy Monitoring

Overview
 Cardholder Server IPs List
Cardholders DBs
 Cardholder Objects
 DB Clients to Servers Map
 Active DB Users
 Cardholder DB Administration
 Authorized Source Programs
 Unauthorized Application Access
 8.5.8 Shared Accounts

PCI - Cardholder DBs
 Start Date: 2009-01-01 00:00:00 End Date: 2012-01-01 00:00:00
 Aliases: ON

Database Name	Server Type	Server IP	Count of Sessions
MASTER	MS SQL SERVER	10.10.9.251	83
MASTER	MS SQL SERVER	10.10.9.253	11
MASTER	SYBASE	10.10.9.57	32
SAMPLE	DB2	10.10.9.252	6
SAMPLE	DB2	10.10.9.56	19
SAMPLE	DB2	10.10.9.57	348
SAMPLE	DB2	10.10.9.58	123

Records 1 to 7 of 7

__e. Click Cardholder Objects.

The PCI - Cardholder Sensitive Objects report appears showing the tables where sensitive data has been accessed as well as the total count of object accesses.

PCI - Cardholder Sensitive Objects

Start Date: 2009-01-01 00:00:00 End Date: 2012-01-01 00:00:00
Aliases: OFF

Object Name	Database Name	Server IP	Server Type	Total access
CC		10.10.9.57	ORACLE	34
cc	FINANCIAL	10.10.9.253	MS SQL SERVER	5
CC	SAMPLE	10.10.9.252	DB2	1
CC	SAMPLE	10.10.9.56	DB2	14
CC	SAMPLE	10.10.9.57	DB2	5
CC	SYSMaster	10.10.9.60	INFORMIX	28
creditcard		10.10.9.251	MS SQL SERVER	21
creditcard		10.10.9.253	MS SQL SERVER	3
CreditCard		10.10.9.5	DB2	15
creditcard		10.10.9.57	ORACLE	128
creditcard		10.10.9.58	ORACLE	9
creditcard	FINANCIAL	10.10.9.253	MS SQL SERVER	3
creditcard	GUARDIUM_QA	10.10.9.57	SYBASE	11
creditcard	MASTER	10.10.9.251	MS SQL SERVER	32
creditcard	SAMPLE	10.10.9.252	DB2	8
creditcard	SAMPLE	10.10.9.56	DB2	4
creditcard	SAMPLE	10.10.9.57	DB2	55
creditcard	SAMPLE	10.10.9.58	DB2	1
creditcard	SYSMaster	10.10.9.60	INFORMIX	92
DB2_DBMGR_GET_CONFIG		10.10.9.56	DB2	6

Records 1 to 20 of 175

__f. Click DB Clients to Servers Map.

The Count of sessions can be very useful in the case that an unexpectedly large session count appears for a client server connection pair.

PCI - Database Clients to Servers Map

Start Date: 2009-01-01 00:00:00 End Date: 2012-01-01 00:00:00
Aliases: OFF

Client IP	Server IP	Server Type	Count of Database Name	Count of Sessions
10.10.9.240	10.10.9.57	MYSQL	1	21
10.10.9.240	10.10.9.57	ORACLE	1	3
10.10.9.248	10.10.9.251	MS SQL SERVER	1	1
10.10.9.248	10.10.9.57	DB2	1	12
10.10.9.248	10.10.9.57	MYSQL	1	25
10.10.9.248	10.10.9.57	ORACLE	1	27
10.10.9.248	10.10.9.57	SYBASE	8	208
10.10.9.251	10.10.9.251	MS SQL SERVER	9	169
10.10.9.56	10.10.9.56	DB2	2	30
10.10.9.56	10.10.9.56	ORACLE	1	1
10.10.9.57	10.10.9.57	DB2	2	904
10.10.9.57	10.10.9.57	MYSQL	2	25
10.10.9.57	10.10.9.57	ORACLE	1	153
10.10.9.57	10.10.9.57	SYBASE	3	19

Records 1 to 14 of 14

__g. Click **Active DB Users**.

The screenshot shows the IBM Guardium interface with the 'Plan & Organize' menu item highlighted. The main content area displays the 'PCI - Cardholder Database Active Users' report. The report includes a table with columns for DB User Name, Database Name, Server Type, Server IP, and Count of Sessions. The table lists various users such as ADMINISTRATOR, HARRY, JOED, and TOM, along with their respective database connections and session counts.

DB User Name	Database Name	Server Type	Server IP	Count of Sessions
?		ORACLE	10.10.9.57	1
ADMINISTRATOR		MS SQL SERVER	10.10.9.251	5
ADMINISTRATOR	MASTER	MS SQL SERVER	10.10.9.251	32
DB2ADMIN	SAMPLE	DB2	10.10.9.57	1
FINANCE		ORACLE	10.10.9.57	4
HARRY		MS SQL SERVER	10.10.9.251	9
HARRY		ORACLE	10.10.9.57	14
HARRY	FINANCIAL	MS SQL SERVER	10.10.9.251	5
HARRY	MASTER	MS SQL SERVER	10.10.9.251	7
HARRY	MSDB	MS SQL SERVER	10.10.9.251	2
JOED		ORACLE	10.10.9.57	24
JOED	MASTER	MS SQL SERVER	10.10.9.251	2
ROOT		MYSQL	10.10.9.57	29
ROOT	MYSQL	MYSQL	10.10.9.57	23
SQLGUARD		ORACLE	10.10.9.57	1
TOM		MS SQL SERVER	10.10.9.251	3
TOM		ORACLE	10.10.9.57	3
TOM	MASTER	MS SQL SERVER	10.10.9.251	2
TOM	MSDB	MS SQL SERVER	10.10.9.251	1

__h. Click **Cardholder DB Administration**.

The screenshot shows the IBM Guardium interface with the 'Cardholder DB Administration' menu item highlighted. The main content area displays the 'PCI - Cardholder DB Administrators' report. The report includes a table with columns for DB User Name, Database Name, Server Type, Server IP, and Count of Sessions. The table lists various users such as BILL, DB2INST2, JOE, SA, and REPORTSERVER, along with their respective database connections and session counts.

DB User Name	Database Name	Server Type	Server IP	Count of Sessions
BILL		ORACLE	10.10.9.57	1
DB2INST2		DB2	10.10.9.56	11
DB2INST2		DB2	10.10.9.57	568
DB2INST2	SAMPLE	DB2	10.10.9.56	19
DB2INST2	SAMPLE	DB2	10.10.9.57	347
JOE		MS SQL SERVER	10.10.9.251	3
JOE		ORACLE	10.10.9.57	69
JOE	MASTER	MS SQL SERVER	10.10.9.251	10
JOE	MASTER	SYBASE	10.10.9.57	5
JOE	MYSQL	MYSQL	10.10.9.57	19
SA		MS SQL SERVER	10.10.9.251	28
SA		SYBASE	10.10.9.57	1
SA	FINANCIAL	MS SQL SERVER	10.10.9.251	4
SA	GUARDIUM_QA	SYBASE	10.10.9.57	63
SA	MASTER	MS SQL SERVER	10.10.9.251	25
SA	MASTER	SYBASE	10.10.9.57	27
SA	MODEL	MS SQL SERVER	10.10.9.251	4
SA	MODEL	SYBASE	10.10.9.57	27
SA	MSDB	MS SQL SERVER	10.10.9.251	4
SA	REPORTSERVER	MS SQL SERVER	10.10.9.251	4

__i. Click **Authorized Source Programs**.

This report displays access to applications approved by your organization. This is expected and approved behavior.

The next question you may ask is: Who is violating this rule by accessing data using non-Approved Applications? See the next report for that important answer.

Source Program	Client IP	Server IP	Server Type	Count of Sessions
DB2ACD	10.10.9.56	10.10.9.56	DB2	11
DB2ACD	10.10.9.57	10.10.9.57	DB2	564
DB2BP	G82.ibm.com	10.10.9.57	DB2	1
DB2BP	10.10.9.56	10.10.9.56	DB2	3
DB2BP	10.10.9.57	10.10.9.57	DB2	14
SQLPLUS	10.10.9.57	10.10.9.57	ORACLE	12
SQLPLUS@OSPNEY	10.10.9.56	10.10.9.56	ORACLE	1
SQLPLUS@OSPNEY	10.10.9.57	10.10.9.57	ORACLE	141

__j. Click **Unauthorized Application Access**.

This report displays access by programs not authorized by your organization, and is the inverse of the previous report. It provides details with Client IPs, Server IPs, Server type and Count of sessions.

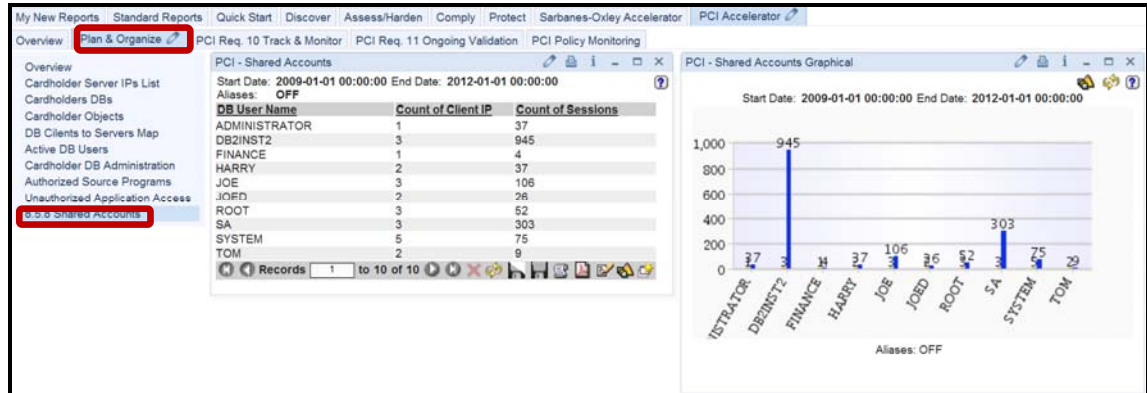
Perhaps your organization would make different choices on the list of Authorized Applications, but is this a useful capability for your organization?

Source Program	Client IP	Server IP	Server Type	Count of Sessions
	10.10.9.248	10.10.9.57	ORACLE	1
DB2HMON	10.10.9.56	10.10.9.56	DB2	16
DB2HMON	10.10.9.57	10.10.9.57	DB2	326
DB2JCC_APPLICATION	10.10.9.248	10.10.9.57	DB2	11
GuardClassifier	10.10.9.248	10.10.9.251	MS SQL SERVER	1
GuardClassifier	10.10.9.248	10.10.9.57	ORACLE	1
ISQL	10.10.9.248	10.10.9.57	SYBASE	1
ISQL	10.10.9.57	10.10.9.57	SYBASE	19
JCONNECT 0.6.0.0	10.10.9.248	10.10.9.57	SYBASE	207
JDBC CONNECT CLIENT	10.10.9.248	10.10.9.57	ORACLE	25
JDBC THIN CLIENT	10.10.9.240	10.10.9.57	ORACLE	3
MICROSOFT SQL SERVER MANAGEMENT STUDIO	10.10.9.251	10.10.9.251	MS SQL SERVER	76
MICROSOFT SQL SERVER MANAGEMENT STUDIO - QUERY	10.10.9.251	10.10.9.251	MS SQL SERVER	36
MYSQL CLIENT	10.10.9.240	10.10.9.57	MYSQL	21
MYSQL CLIENT	10.10.9.248	10.10.9.57	MYSQL	25
MYSQL CLIENT	10.10.9.57	10.10.9.57	MYSQL	25
SQLCMD	10.10.9.251	10.10.9.251	MS SQL SERVER	30
SQLCMD.EXE	10.10.9.251	10.10.9.251	MS SQL SERVER	18
SQLWB.EXE	10.10.9.251	10.10.9.251	MS SQL SERVER	1
SYSTEM	10.10.9.251	10.10.9.251	MS SQL SERVER	8

__k. Click **8.5.8 Shared Accounts**.

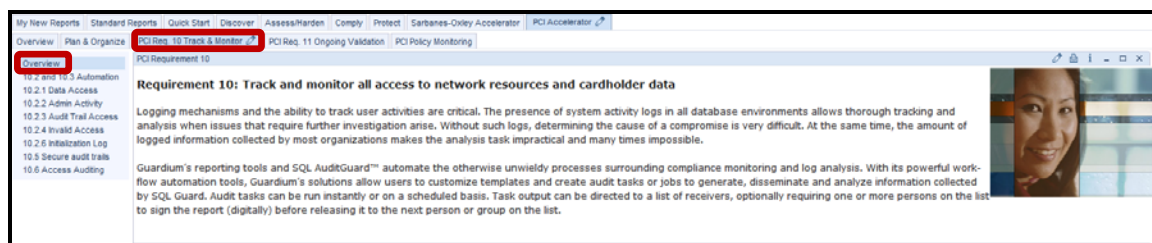
Payment Card Industry – Data Security Standard 8.5.8 is the requirement to not use group, shared, or generic accounts and passwords.

Note: These reports are a matching pair displaying the same data. One report is in tabular form, and the other is in graphical form.



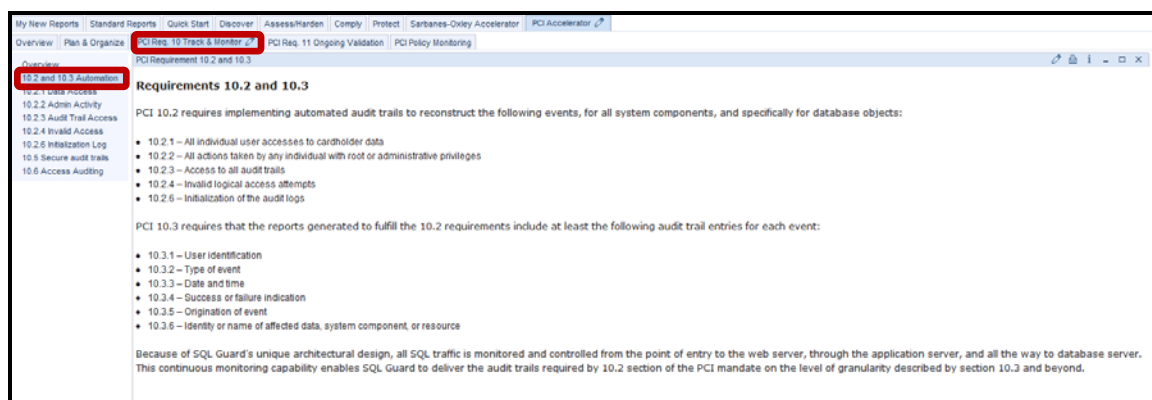
5. PCI Accelerator – PCI Requirement 10 Track & Monitor.

- a. Click **Overview** under the **PCI Req. 10 Track & Monitor** tab.



- b. Click **10.2 and 10.3 Automation**.

The PCI accelerator eases the meeting of requirements 10.2 and 10.3 right out of the box.



c. Click 10.2.1 Data Access.

This report tracks activity of users who have access to Cardholder Data.

DB User Name	Client IP	Server IP	Database Name	Server Type	SQL Verb	Count of Object Name	Total access
?	10.10.9.248	10.10.9.57		ORACLE	SELECT	2	2
ADMINISTRATOR	10.10.9.251	10.10.9.251		MS SQL SERVER	SELECT	6	18
ADMINISTRATOR	10.10.9.251	10.10.9.251	MASTER	MS SQL SERVER	CREATE TABLE	2	2
ADMINISTRATOR	10.10.9.251	10.10.9.251	MASTER	MS SQL SERVER	DROP TABLE	2	2
ADMINISTRATOR	10.10.9.251	10.10.9.251	MASTER	MS SQL SERVER	EXECUTE	1	3
ADMINISTRATOR	10.10.9.251	10.10.9.251	MASTER	MS SQL SERVER	INSERT	2	36
ADMINISTRATOR	10.10.9.251	10.10.9.251	MASTER	MS SQL SERVER	SELECT	6	78
DB2ADMIN	10.10.9.248	10.10.9.57	SAMPLE	DB2	SELECT	2	2
FINANCE	10.10.9.57	10.10.9.57		ORACLE	CALL	2	12
FINANCE	10.10.9.57	10.10.9.57		ORACLE	CREATE TABLE	3	3
FINANCE	10.10.9.57	10.10.9.57		ORACLE	GRANT	4	16
FINANCE	10.10.9.57	10.10.9.57		ORACLE	INSERT	2	19
FINANCE	10.10.9.57	10.10.9.57		ORACLE	REVOKE	2	2
FINANCE	10.10.9.57	10.10.9.57		ORACLE	SELECT	4	28
HARRY	10.10.9.251	10.10.9.251		MS SQL SERVER	EXECUTE	1	8
HARRY	10.10.9.251	10.10.9.251		MS SQL SERVER	IF	2	2
HARRY	10.10.9.251	10.10.9.251		MS SQL SERVER	SELECT	18	118
HARRY	10.10.9.251	10.10.9.251		MS SQL SERVER	USE	1	1
HARRY	10.10.9.251	10.10.9.251	FINANCIAL	MS SQL SERVER	SELECT	15	46
HARRY	10.10.9.251	10.10.9.251	FINANCIAL	MS SQL SERVER	USE	2	7

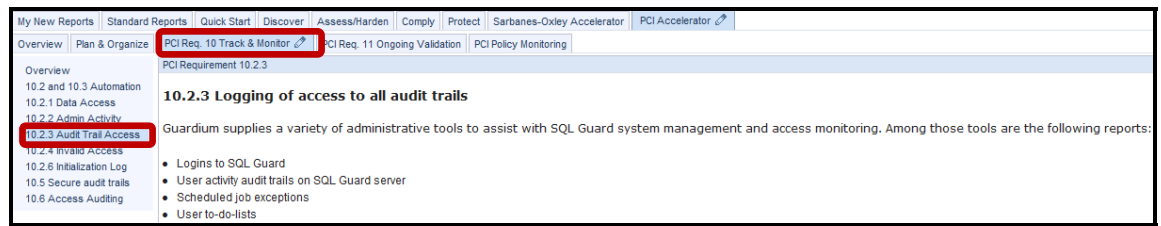
d. Click 10.2.2 Admin Activity.

This report tracks activity of users who have Administration level access.

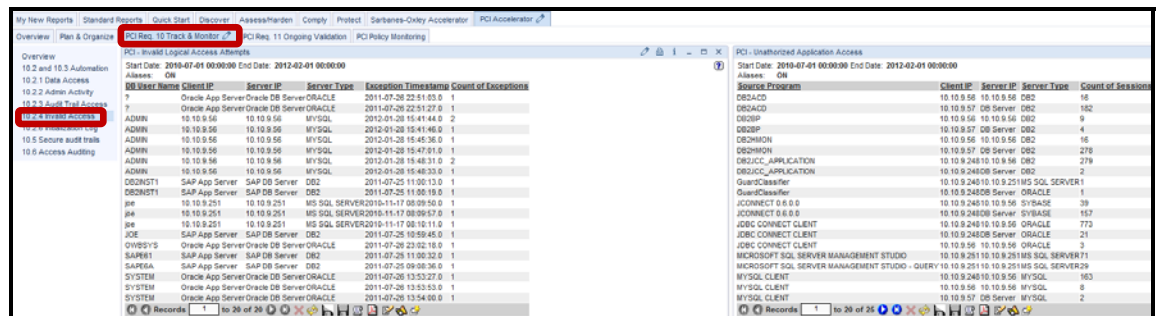
DB User Name	Client IP	Server IP	Database Name	Server Type	SQL Verb	Count of Object Name	Total access
BILL	10.10.9.57	10.10.9.57		ORACLE	CALL	2	3
BILL	10.10.9.57	10.10.9.57		ORACLE	SELECT	6	9
DB2INST2	G82.ibm.com	10.10.9.57	SAMPLE	DB2	CALL	1	24
DB2INST2	G82.ibm.com	10.10.9.57	SAMPLE	DB2	SELECT	26	371
DB2INST2	G82.ibm.com	10.10.9.57	SAMPLE	DB2	SET CLIENT WRKSTNAME	1	11
DB2INST2	10.10.9.56	10.10.9.56		DB2	CALL	4	25
DB2INST2	10.10.9.56	10.10.9.56		DB2	SELECT	2	22
DB2INST2	10.10.9.56	10.10.9.56	SAMPLE	DB2	ALTER TABLE	1	1
DB2INST2	10.10.9.56	10.10.9.56	SAMPLE	DB2	CALL	3	17
DB2INST2	10.10.9.56	10.10.9.56	SAMPLE	DB2	CREATE FUNCTION	1	1
DB2INST2	10.10.9.56	10.10.9.56	SAMPLE	DB2	CREATE TABLE	5	7
DB2INST2	10.10.9.56	10.10.9.56	SAMPLE	DB2	DROP TABLE	2	2
DB2INST2	10.10.9.56	10.10.9.56	SAMPLE	DB2	INSERT	5	96
DB2INST2	10.10.9.56	10.10.9.56	SAMPLE	DB2	SELECT	8	51
DB2INST2	10.10.9.57	10.10.9.57		DB2	CALL	3	904
DB2INST2	10.10.9.57	10.10.9.57		DB2	SELECT	2	1136
DB2INST2	10.10.9.57	10.10.9.57	SAMPLE	DB2	CALL	5	327
DB2INST2	10.10.9.57	10.10.9.57	SAMPLE	DB2	CREATE FUNCTION	1	1
DB2INST2	10.10.9.57	10.10.9.57	SAMPLE	DB2	CREATE TABLE	4	4
DB2INST2	10.10.9.57	10.10.9.57	SAMPLE	DB2	DELETE	1	6

e. Click 10.2.3 Audit Trail Access.

Read about the 10.2.3 Logging of access to all audit trails.

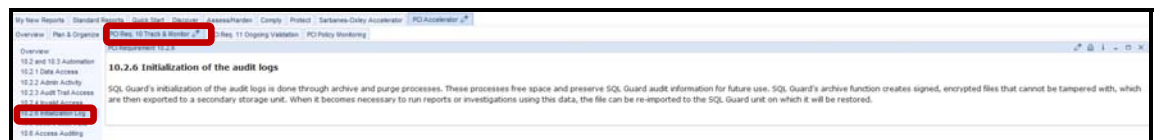


f. Click 10.2.4 Invalid Access.



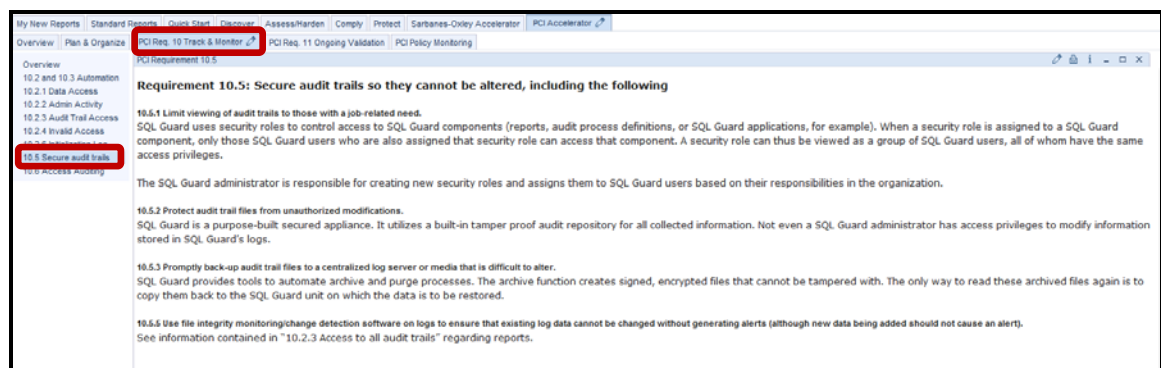
g. Click 10.2.6 Initialization Log.

Read about 10.2.6 Initialization of the audit logs.



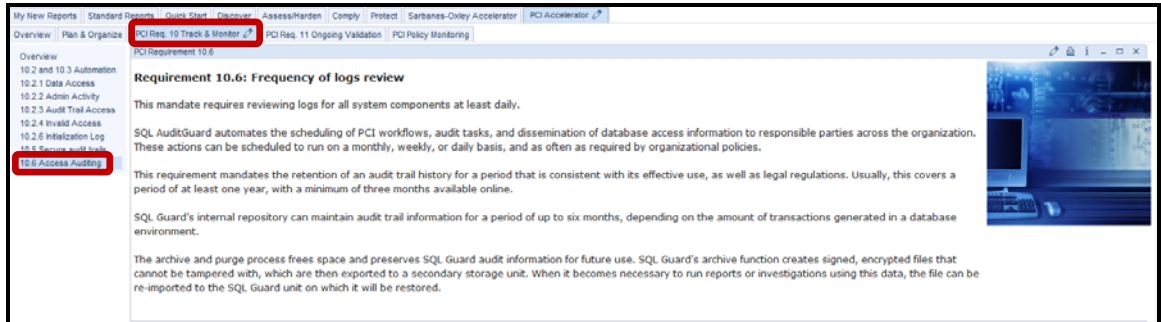
h. Click 10.5 Secure audit trails.

Read about Requirement 10.5: Secure audit trails so they cannot be altered.



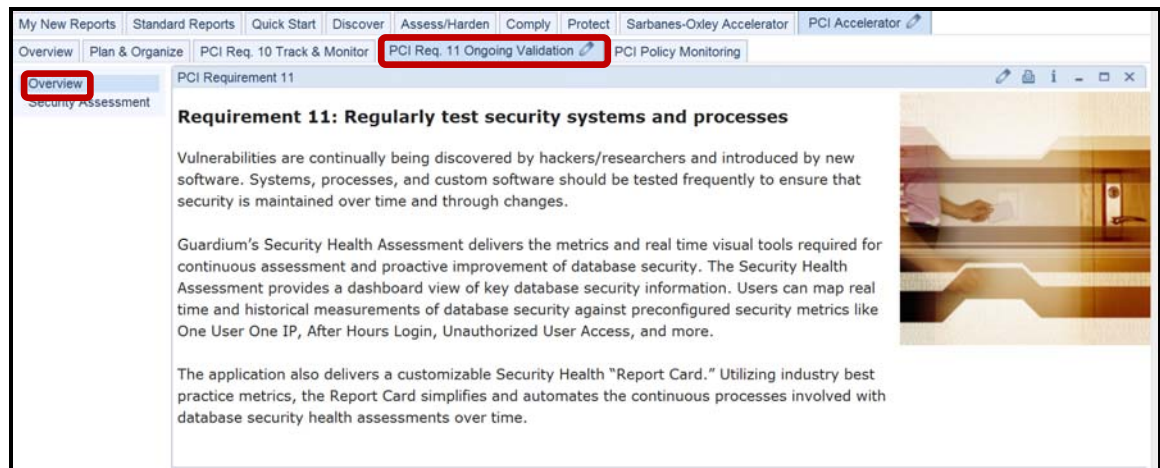
__i. Click **10.6 Access Auditing**.

Read about Requirement 10.6: Frequency of logs review.



__6. PCI Accelerator – PCI Requirement 11 Ongoing Validation.

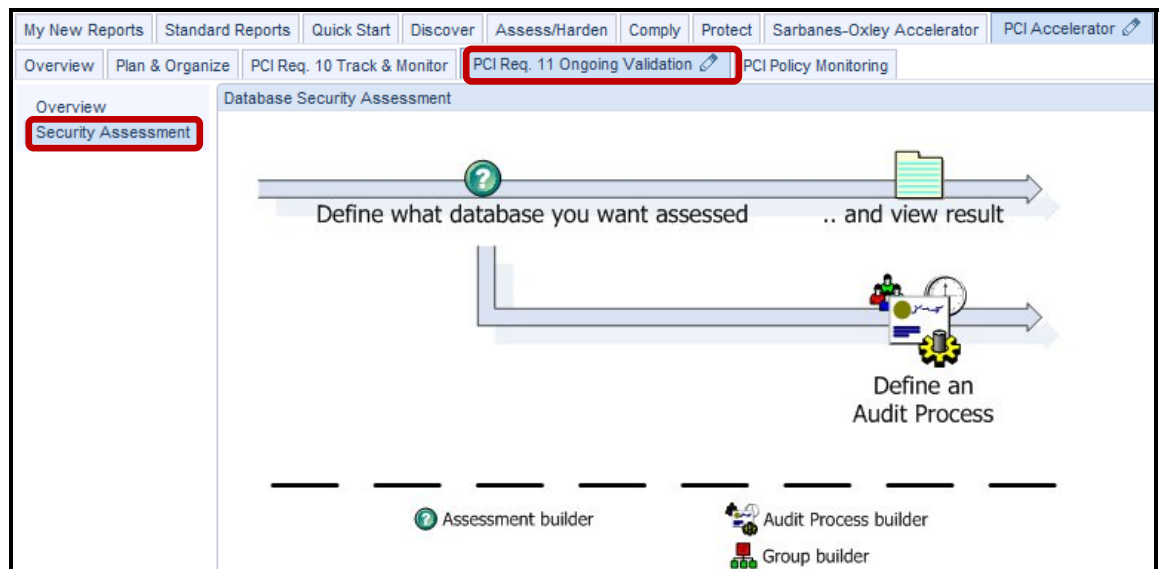
- __a. Click **Overview** under the **PCI Req. 11 Ongoing Validation** tab.



- __b. Click **Security Assessment**.

This customizable Report Card simplifies and automates the continuous processes involved with database security health assessments over time.

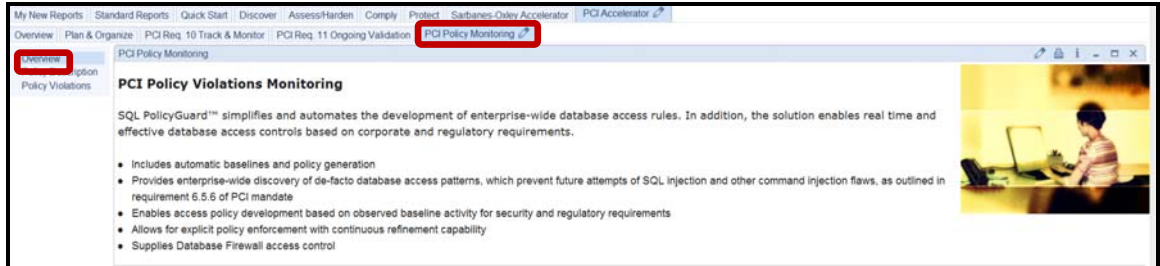
Note: In a subsequent lab, we will explore the InfoSphere Guardium Vulnerability Assessment solution in much greater detail.



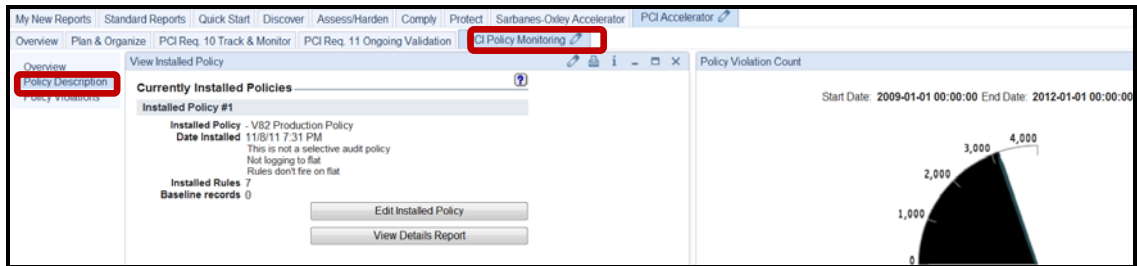
7. PCI Accelerator – PCI Policy Monitoring.

a. Click **Overview** under the **PCI Policy Monitoring** tab.

Read the ‘PCI Policy Violations Monitoring’ overview that appears.



b. Click **Policy Description**.



c. Click **Policy Violations**.

Timestamp	Category Name	Access Rule Description	Client IP	Service ID	DB User Name	Full SQL Statement	Severity Description	Count of Policy Rule Violations
2011-08-10 10:10:54.0	Data Security	Terminate on Privilege User Access to Sensitive Information	10.10.9.18	10.10.9.18	SYSTEM	select * from creditcard	Med	1
2011-07-31 22:28:44.0	Quarantine brute force attack	Quarantine brute force attack	10.10.9.240	10.10.9.252	JOE		Info	1
2011-07-31 22:28:44.0	Quarantine brute force attack	Quarantine brute force attack	10.10.9.240	10.10.9.252	JOE		Info	1
2011-07-31 22:28:44.0	Data Security	Terminate on Privilege User Access to Sensitive Information	10.10.9.18	10.10.9.18	SYSTEM	select * from creditcard	Med	1
2011-07-31 20:41:09.0	Data Security	Terminate on Privilege User Access to Sensitive Information	10.10.9.18	10.10.9.18	SYSTEM	select * from creditcard	Med	1
2011-07-31 20:40:59.0	Data Security	Terminate on Privilege User Access to Sensitive Information	10.10.9.18	10.10.9.18	SYSTEM	select * from creditcard	Med	1
2011-07-31 20:23:19.0	Data Security	Terminate on Privilege User Access to Sensitive Information	10.10.9.18	10.10.9.18	SYSTEM	select * from creditcard	Med	2
2011-07-31 20:23:19.0	Data Security	Terminate on Privilege User Access to Sensitive Information	10.10.9.18	10.10.9.18	SYSTEM	select * from creditcard	Med	2
2010-12-03 10:10:54.0	Rule 1	Rule 1	10.10.9.17	10.10.9.17	JOE	select cardid from creditcard	Info	1
2010-12-03 10:10:53.0	Rule 1	Rule 1	10.10.9.17	10.10.9.17	JOE	select * from creditcard where cardid=1	Info	1
2010-12-03 10:10:53.0	Audit Only Rule	Audit Only Rule	10.10.9.17	10.10.9.17	JOE	select * from job	Info	1
2010-12-03 10:10:53.0	Audit Only Rule	Audit Only Rule	10.10.9.17	10.10.9.17	JOE	BEGIN DBMS_APPLICATION_INFO SET_MODULE('SQL*W',NULL); END;	Info	1
2010-12-03 10:10:53.0	Audit Only Rule	Audit Only Rule	10.10.9.17	10.10.9.17	JOE	BEGIN DBMS_APPLICATION_INFO SET_MODULE(1,NULL); END;	Info	1
2010-12-03 10:10:53.0	Audit Only Rule	Audit Only Rule	10.10.9.17	10.10.9.17	JOE	SELECT DECODE('A','Y','Z') FROM DUAL;	Info	1
2010-12-03 10:10:53.0	Audit Only Rule	Audit Only Rule	10.10.9.17	10.10.9.17	JOE	BEGIN DBMS_OUTPUT DISABLE; END;	Info	1
2010-12-03 10:10:53.0	Audit Only Rule	Audit Only Rule	10.10.9.17	10.10.9.17	JOE	SELECT ATTRIBUTE_SCORE_NUMERIC_VALUE,CHAR_VALUE,DATE_VALUE FROM SYSTEM_PRODUCT_PRIVS WHERE (UPPER(SQL*W) LIKE UPPER(PRODUCT)) AND (UPPER(USER) LIKE USER);	Info	1
2010-12-03 10:10:53.0	Audit Only Rule	Audit Only Rule	10.10.9.17	10.10.9.17	JOE	SELECT CHAR_VALUE FROM SYSTEM_PRODUCT_PRIVS WHERE (UPPER(SQL*W) LIKE UPPER(PRODUCT)) AND (UPPER(USER) LIKE USER) OR (USER = PUBLIC) AND (OPER(ATTRIBUTE) = 'ROLE');	Info	1
2010-12-03 10:10:53.0	Audit Only Rule	Audit Only Rule	10.10.9.17	10.10.9.17	JOE	SELECT USER FROM DUAL;	Info	1
2010-12-03 10:10:53.0	Terminate on Privilege User Access to Sensitive Information	Terminate on Privilege User Access to Sensitive Information	10.10.9.252	10.10.9.252	ADMINISTRATOR	select * from creditcard	Med	1

Thank You

12.2 Adding Users with PCI Role (Optional)

Overview

Access control mechanisms built into the core InfoSphere Guardium solution allow administrators to assign responsibilities for particular databases or systems to individuals (or roles) and their hierarchical management.

The InfoSphere Guardium solution makes it possible to define efficient processes with parallel actions without compromising security or burdening users with information that is not relevant to their specific responsibilities.

Objectives

- __1. Add an InfoSphere Guardium User with the PCI role.
- __2. Show PCI group members via GUI and via InfoSphere Guardium API.
- __3. Add and Remove a member of a PCI group via GUI.
- __4. Add a member of a PCI group via InfoSphere Guardium API.
- __5. Populate group information for PCI Accelerator from the InfoSphere Guardium API.

- __1. Add a user with the PCI role.
 - __a. Login as **accessmgr** / **guardium**.

Note: The accessmgr account is a special administrative account used to add, delete or modify users of InfoSphere Guardium.

Login

Please enter your information

User name:

Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM. 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistry/key © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

__b. Click the **Add User** button.

The screenshot shows the 'User Browser' interface. On the left is a navigation menu with options: User Browser, User Role Browser, User Role Permissions, User LDAP Import, and User & Role Reports. The main area is titled 'User Browser' and contains a search bar with a filter string, a dropdown for 'User Name', a 'Filter' button, and an 'Add User' button highlighted with a red box. Below the search bar is a table of users:

Username	First Name	Last Name	Email	Actions
accessmgr	accessmgr	accessmgr	guardium_accessmgr@us.ibm.com	Edit Roles Change Layout
admin	admin	admin	guardium_admin@us.ibm.com	Edit Roles Change Layout
poc	poc	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
poc_pci	poc_pci	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
poc_sox	poc_sox	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
pot	pot	admin	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete

__c. Enter 'pjones' in the *Username* field, 'guardium' in the *Password* fields, 'Paula' in the *First Name* field, and 'Jones' in the *Last Name* field. Then, uncheck the *Disabled* checkbox, and click **Add User**.

The screenshot shows the 'User Form' interface. On the left is a navigation menu with options: User Browser, User Role Browser, User Role Permissions, User LDAP Import, and User & Role Reports. The main area is titled 'User Form' and contains several input fields: Username (pjones), Password (masked with dots), Password (confirm) (masked with dots), First Name (Paula), Last Name (Jones), and Email (empty). Below the fields is a 'Disabled' checkbox, which is unchecked and highlighted with a red box. At the bottom, there is an 'Add User' button highlighted with a red box and a 'Back' button. A note at the bottom reads: "In an effort to provide the highest level security, new passwords must be 8 or more characters in length and must include at least one uppercase letter, lowercase letter, digit, and special character. A special character is considered any of the following: @# \$%^&.!-+=_".

__d. Click **Roles** for the new user Paula Jones.

The screenshot shows the 'User Browser' interface in the IBM InfoSphere Guardium console. On the left, there is a navigation menu with options: 'User Browser', 'User Role Browser', 'User Role Permissions', 'User LDAP Import', and 'User & Role Reports'. The main area is titled 'User Browser' and contains a search bar with a 'Filter string (case sensitive):' input field, a 'User Name' dropdown, and 'Filter', 'Add User', and 'Search Users' buttons. Below the search bar is a table of users with columns for Username, First Name, Last Name, Email, and Actions. The user 'pjones' (Paula Jones) is listed, and the 'Roles' link in the Actions column is circled in red.

Username	First Name	Last Name	Email	Actions
accessmgr	accessmgr	accessmgr	guardium_accessmgr@us.ibm.com	Edit Roles Change Layout
admin	admin	admin	guardium_admin@us.ibm.com	Edit Roles Change Layout
pjones	Paula	Jones		Edit Roles Change Layout Delete
poc	poc	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
poc_pci	poc_pci	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
poc_sox	poc_sox	user	guardium_poc@us.ibm.com	Edit Roles Change Layout Delete
pot	pot	admin	guardium_pot@us.ibm.com	Edit Roles Change Layout Delete

- __e. Add the **pci** role using the check boxes, and click **Save** to complete the role assignment.

Note: The **user** role has already been assigned by default.

The screenshot shows the 'User Role Form' for 'Paula Jones' in the 'Access Management' section. The form displays a list of roles with checkboxes for assignment. The 'pci' role is selected, and the 'Save' button is highlighted.

Role Name	Assign
accessmgr	<input type="checkbox"/>
admin	<input type="checkbox"/>
appdev	<input type="checkbox"/>
audit	<input type="checkbox"/>
Baselll	<input type="checkbox"/>
cas	<input type="checkbox"/>
cli	<input type="checkbox"/>
DataPrivacy	<input type="checkbox"/>
datasec-exempt	<input type="checkbox"/>
dba	<input type="checkbox"/>
diag	<input type="checkbox"/>
infosec	<input type="checkbox"/>
inv	<input type="checkbox"/>
netadm	<input type="checkbox"/>
pci	<input checked="" type="checkbox"/>
review-only	<input type="checkbox"/>
sox	<input type="checkbox"/>
user	<input checked="" type="checkbox"/>

Buttons: **Save** (highlighted), **Back**

- __2. Verify Paula Jones user with PCI role.
 - __a. **Logout** as accessmgr and login as **pjones / guardium**.

Login

Please enter your information

User name:

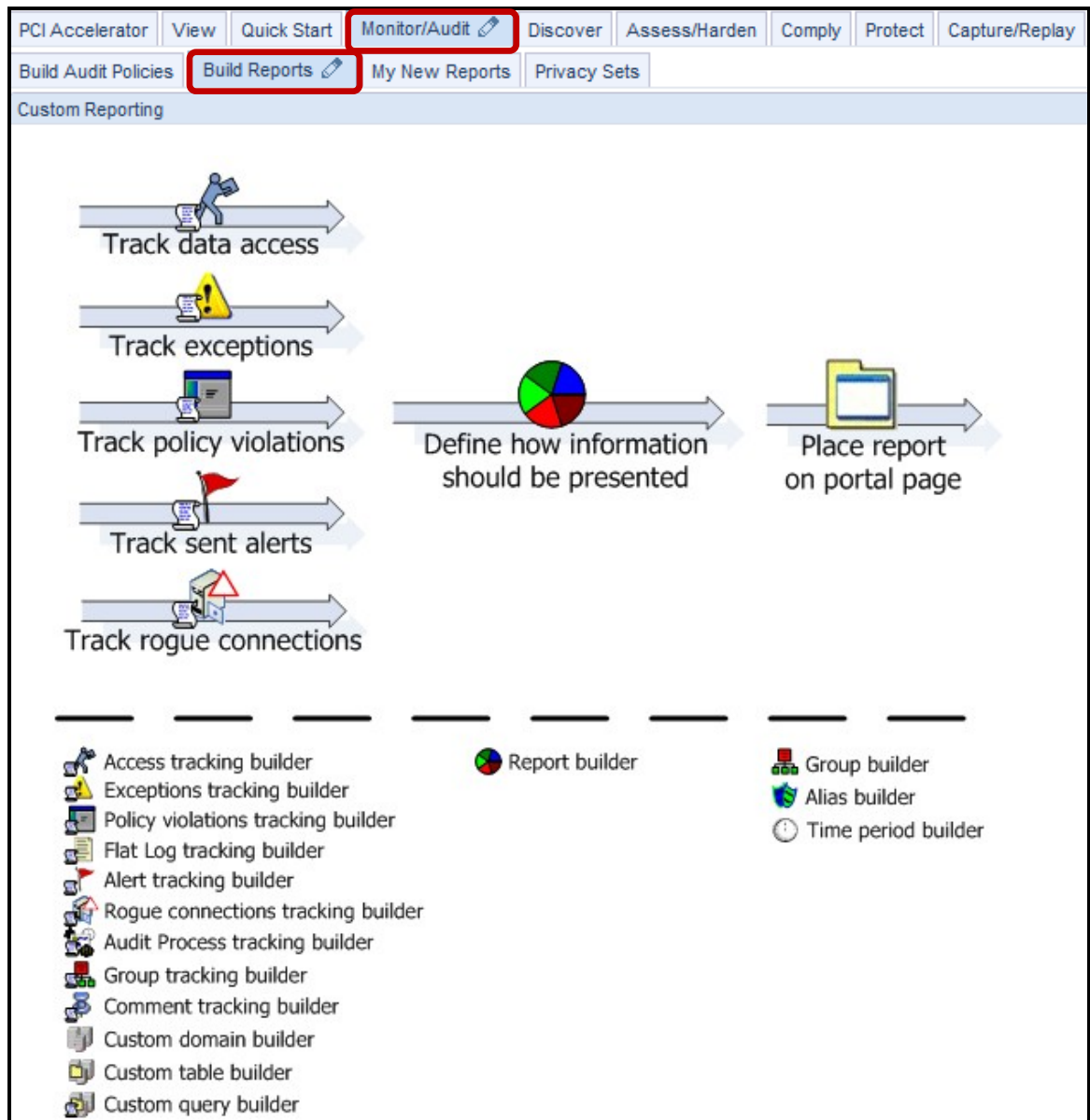
Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM. 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl, Jregistrykey © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

__b. Click **Build Reports** under the **Monitor/Audit** tab, and then logout.



- __3. Show PCI Admin Users group members via GUI.
 - __a. Login as **pot / guardium**.

Login

Please enter your information

User name:

Password:

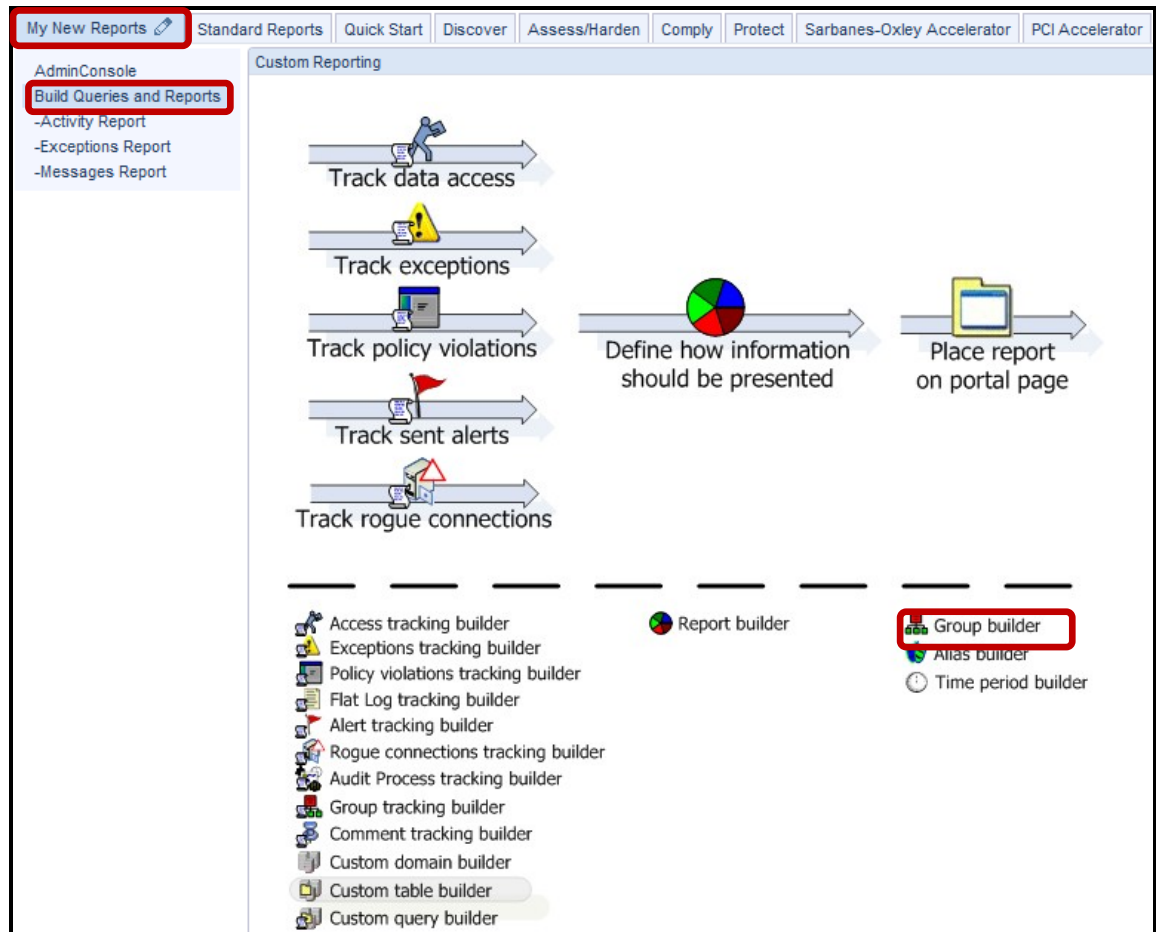
Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

Licensed Materials - Property of IBM. 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

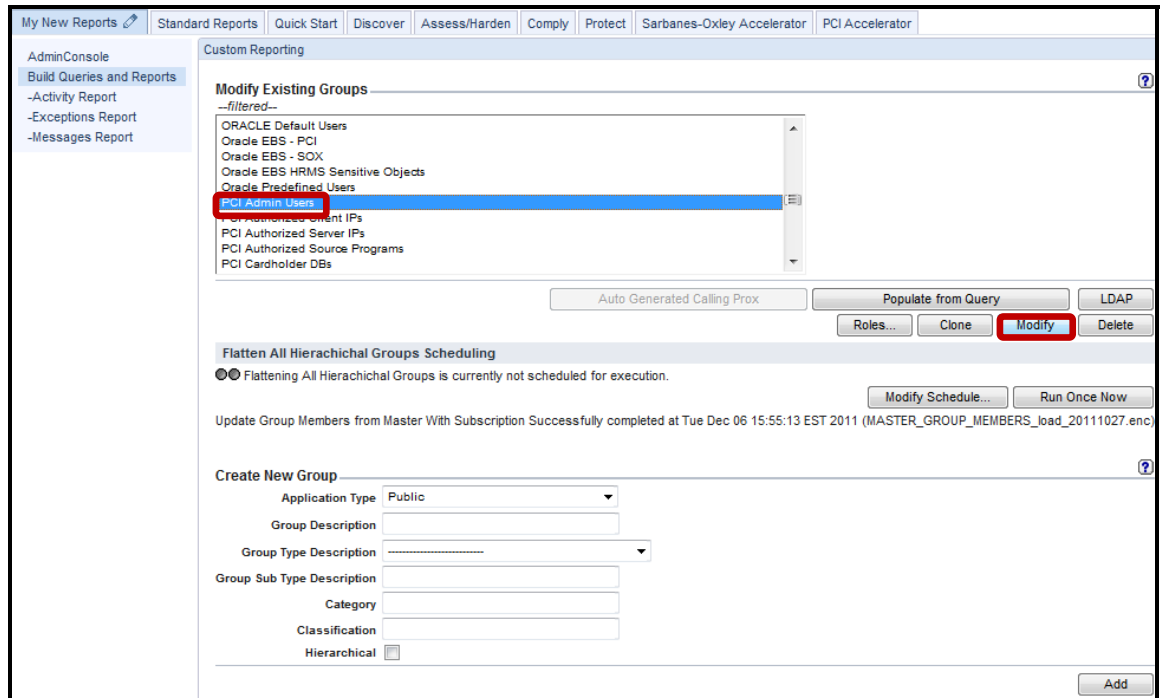
CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl, Jregistrykey © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

- b. Click **Build Queries and Reports** under the **My New Reports** tab, and then click **Group Builder**.

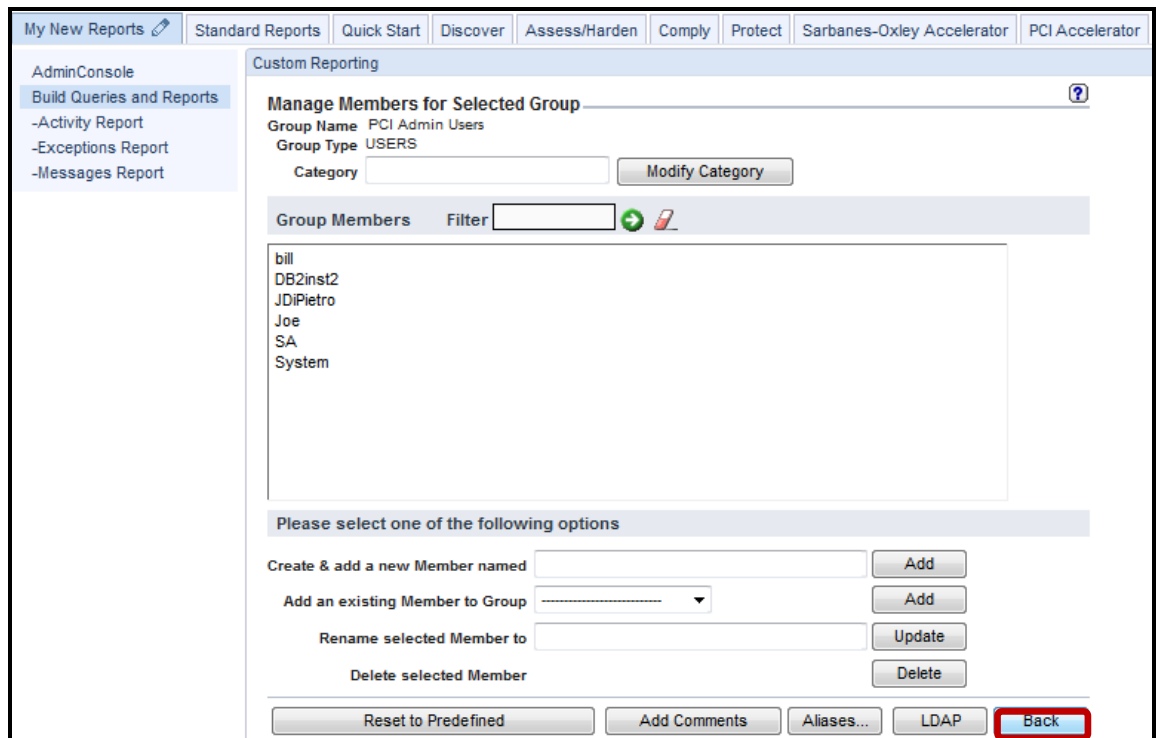
Group Builder can be used to show PCI group members and update the members.



- c. Select 'PCI Admin Users' from the drop-down list, and click **Modify** to view the contents of the PCI Admin Users group.



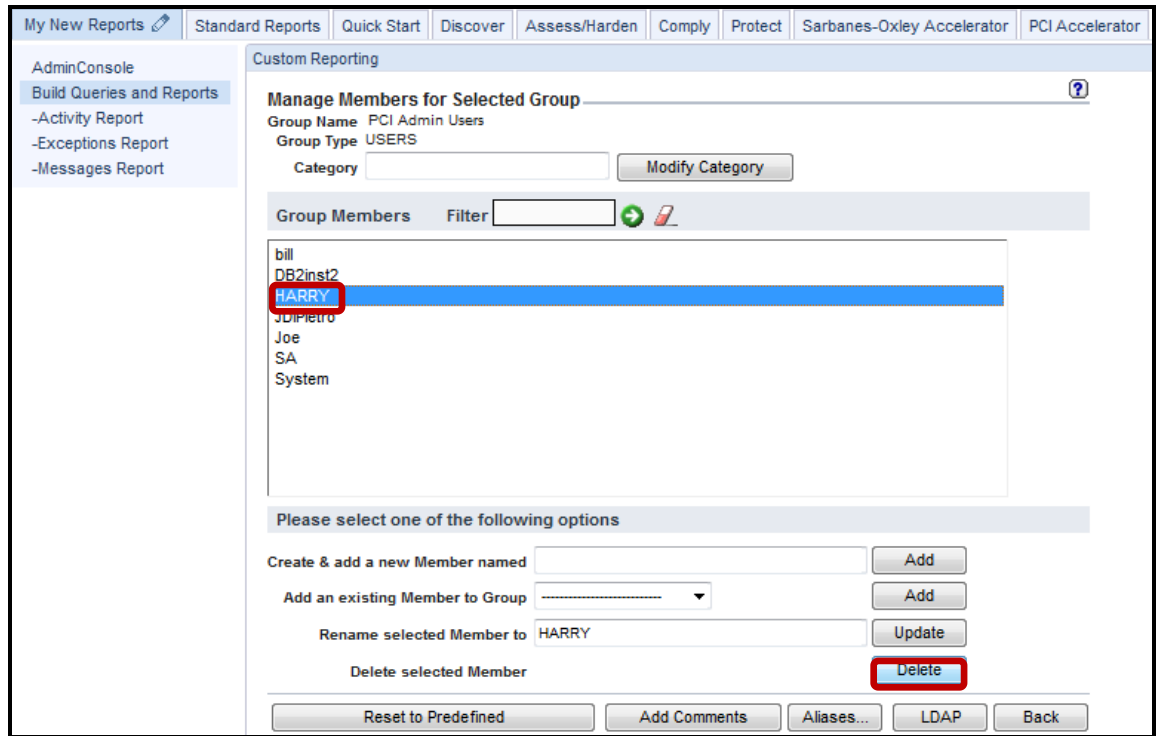
- d. Click **Back** to cancel the modification of the 'PCI Admin Users' group contents.



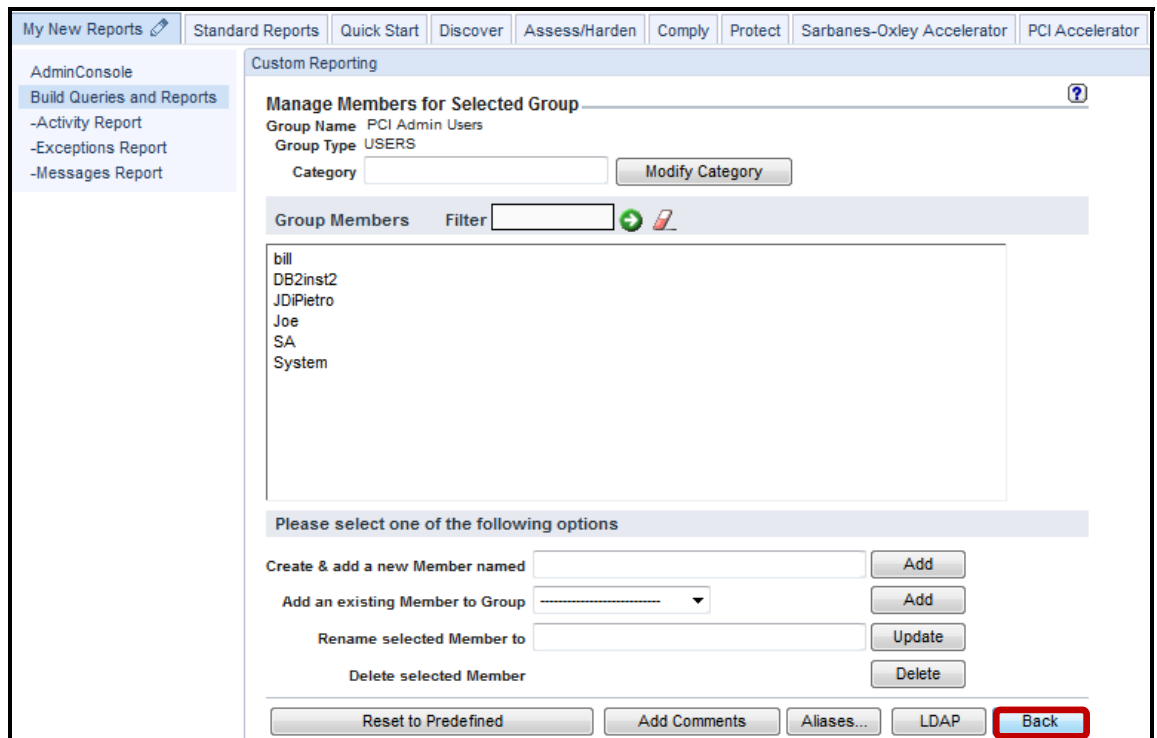
- __4. Add and delete a member of PCI group via GUI.
- __a. Select the user **HARRY** from the 'Add an existing Member to Group' drop-down list, and click **Add**. Another option is to Create & Add a new Member.

The screenshot displays the 'Manage Members for Selected Group' interface within the Custom Reporting section. The group name is 'PCI Admin Users' and the group type is 'USERS'. A list of group members is shown, including 'bill', 'DB2inst2', 'JDiPietro', 'Joe', 'SA', and 'System'. Below the list, there are four options for managing members: 'Create & add a new Member named', 'Add an existing Member to Group', 'Rename selected Member to', and 'Delete selected Member'. The 'Add an existing Member to Group' dropdown menu is currently set to 'HARRY', and the 'Add' button next to it is highlighted with a red box. At the bottom of the interface, there are buttons for 'Reset to Predefined', 'Add Comments', 'Aliases...', 'LDAP', and 'Back'.

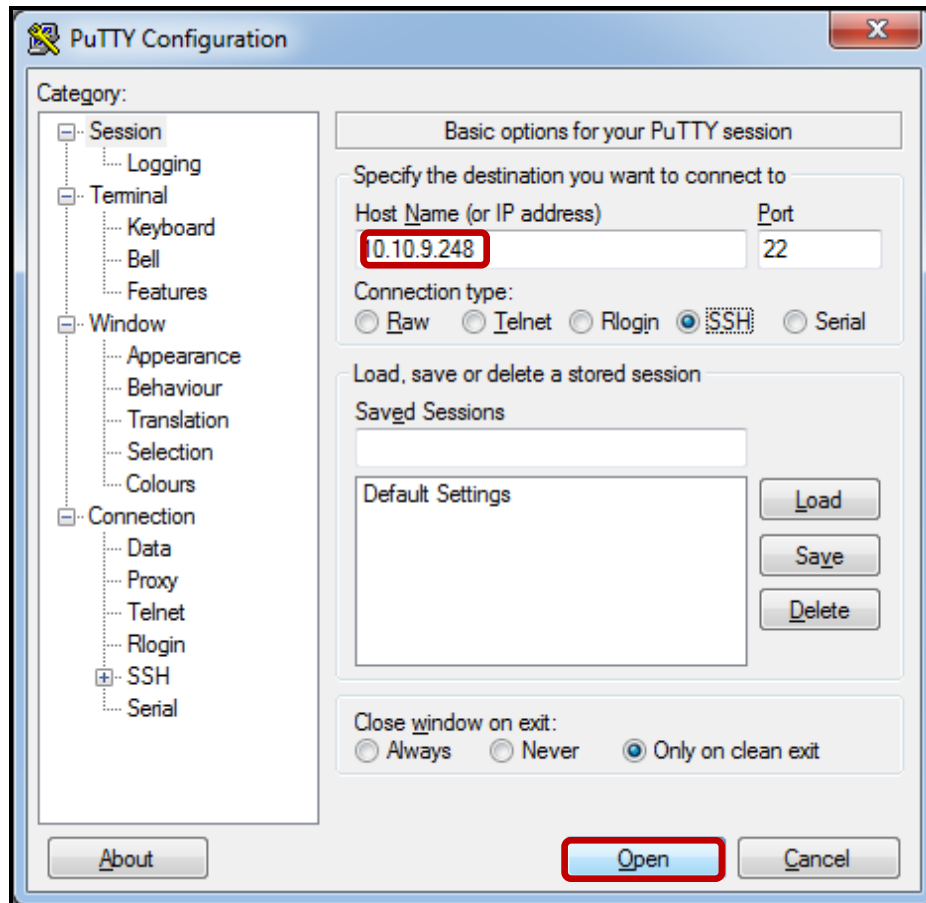
__b. Now select **HARRY** from the PCI Admin Users member list and click **Delete**.



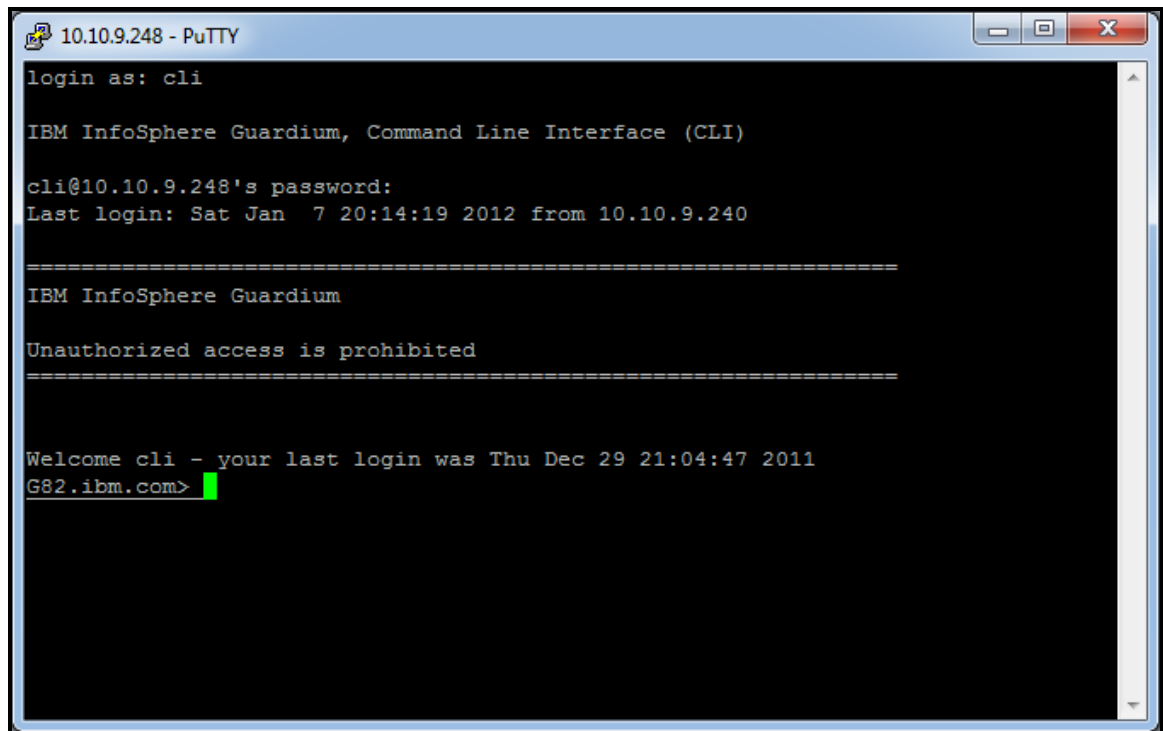
__c. Here the user **HARRY** has been deleted as a member of the PCI Admin Users group. Click **Back** to return.



- __5. Using a PuTTY SSH client, access the VM Appliance to demonstrate the ease with which the InfoSphere Guardium solution can configure and view group information.
- __a. Start the PuTTY SSH client login.
 - __b. From your laptop, launch PuTTY, enter **10.10.9.248**, and click **Open**.



- __6. Populate PCI Accelerator group information from the InfoSphere Guardium API.
 - __a. Login as **cli / guardium**. After logging in, the following prompt will be displayed:



Type (***Copy and Paste***) the following Guardium API commands.

If a member already exists, you will receive the following error message:

ERR=143

Could not create member - member might already exist.

```
grdapi create_member_to_group_by_desc desc="PCI Admin Users" member="Joe"
grdapi create_member_to_group_by_desc desc="PCI Admin Users" member="JDiPietro"
grdapi create_member_to_group_by_desc desc="PCI Admin Users" member="SA"
grdapi create_member_to_group_by_desc desc="PCI Admin Users" member="System"
grdapi create_member_to_group_by_desc desc="PCI Admin Users" member="DB2inst2"
grdapi create_member_to_group_by_desc desc="PCI Admin Users" member="bill"
```

```
grdapi create_member_to_group_by_desc desc="PCI Authorized Client IPs" member="10.10.9.56"
grdapi create_member_to_group_by_desc desc="PCI Authorized Client IPs" member="10.10.9.251"
grdapi create_member_to_group_by_desc desc="PCI Authorized Client IPs" member="10.10.9.57"
grdapi create_member_to_group_by_desc desc="PCI Authorized Client IPs" member="10.10.9.250"
grdapi create_member_to_group_by_desc desc="PCI Authorized Client IPs" member="10.10.9.249"
```

```
grdapi create_member_to_group_by_desc desc="PCI Authorized Server IPs" member="10.10.9.56"
grdapi create_member_to_group_by_desc desc="PCI Authorized Server IPs" member="10.10.9.57"
grdapi create_member_to_group_by_desc desc="PCI Authorized Server IPs" member="10.10.9.251"
grdapi create_member_to_group_by_desc desc="PCI Authorized Server IPs" member="10.10.9.250"
```

```
grdapi create_member_to_group_by_desc desc="PCI Authorized Source Programs" member="%SQLPLUS%"
grdapi create_member_to_group_by_desc desc="PCI Authorized Source Programs" member="SQLPLUS"
grdapi create_member_to_group_by_desc desc="PCI Authorized Source Programs" member="SAP"
grdapi create_member_to_group_by_desc desc="PCI Authorized Source Programs" member="Oracle EBS"
```

```
grdapi create_member_to_group_by_desc desc="PCI Cardholder DBs" member="master"
grdapi create_member_to_group_by_desc desc="PCI Cardholder DBs" member="creditcard"
```

```
grdapi create_member_to_group_by_desc desc="PCI Cardholder Sensitive objects" member="creditcard"
grdapi create_member_to_group_by_desc desc="PCI Cardholder Sensitive objects" member="cc"
grdapi create_member_to_group_by_desc desc="PCI Cardholder Sensitive objects" member="patient"
```

```
grdapi create_member_to_group_by_desc desc="PCI Limited Access Users" member="harry"
```

__7. Verify PCI group members have been added via the grdapi.

__a. Type the following InfoSphere Guardium API commands to show the PCI group members:

grdapi list_group_members_by_desc desc="PCI Limited Access Users"

Results should look like:

ID=6007
Group: PCI Limited Access Users
Members:
harry
ok

grdapi list_group_members_by_desc desc="PCI Cardholder Sensitive objects"

Results should look like:

ID=6006
Group: PCI Cardholder Sensitive objects
Members:
cc
creditcard
patient
ok

grdapi list_group_members_by_desc desc="PCI Cardholder DBs"

Results should look like:

ID=6005
Group: PCI Cardholder DBs
Members:
creditcard
master
ok

grdapi list_group_members_by_desc desc="PCI Authorized Source Programs"

Results should look like:

ID=6002
Group: PCI Authorized Source Programs
Members:
%SQLPLUS%
Oracle EBS
SAP
SQLPLUS
ok

grdapi list_group_members_by_desc desc="PCI Authorized Server IPs"

Results should look like:

```
ID=6004
Group: PCI Authorized Server IPs
Members:
10.10.9.250
10.10.9.251
10.10.9.56
10.10.9.57
ok
```

grdapi list_group_members_by_desc desc="PCI Authorized Client IPs"

Results should look like:

```
ID=6003
Group: PCI Authorized Client IPs
Members:
10.10.9.249
10.10.9.250
10.10.9.251
10.10.9.56
10.10.9.57
ok
```

grdapi list_group_members_by_desc desc="PCI Admin Users"

Results should look like:

```
ID=6001
Group: PCI Admin Users
Members:
bill
DB2inst2
JDiPietro
Joe
SA
System
ok
```

Thank You

Payment Card Industry (PCI) Accelerator review

- __1. The PCI Accelerator is an optional component enabled by a product key.
(**True** or **False**).
- __2. How would you implement the following PCI requirement?
“Prohibit vendor-supplied defaults for system passwords and other security parameters.”
- __a. Run a daily audit process and send the result to the DBA.
 - __b. Implement Vulnerability Assessment for those databases containing cardholder data.
 - __c. Check the default accounts during DB installation.
 - __d. InfoSphere Guardium is not the right product to support this requirement.
- __3. How would you implement the following PCI requirement?
“Restrict access to cardholder data by business need to know.”
- __a. Create classifier job(s) to detect cardholder data objects and add them to a sensitive objects group.
 - __b. Implement Data Level Access Control (S-GATE or Redaction) for DBAs on database objects containing cardholder data.
 - __c. Create Entitlement Reports that show which users have access to those objects that contain cardholder data.
 - __d. All of the above.
- __4. To run PCI reports, a user needs the PCI role.
(**True** or **False**).
- __5. A user runs the PCI reports, but the reports results are empty. What could be the problem?
- __a. Wrong FROM and TO date runtime parameters.
 - __b. The PCI groups are empty.
 - __c. The network cable is disconnected.
 - __d. A and B.

Payment Card Industry (PCI) Accelerator review (Answers)

__1. The PCI Accelerator is an optional component enabled by a product key.
(**True** or **False**).

False.

__2. How would you implement the following PCI requirement?

“Prohibit vendor-supplied defaults for system passwords and other security parameters”

B – Implement Vulnerability Assessment for those databases containing cardholder data.

__3. How would you implement the following PCI requirement?

“Restrict access to cardholder data by business need to know”

D – All of the above.

__4. To run PCI reports, a user needs the PCI role.
(**True** or **False**).

True.

__5. A user runs the PCI reports, but the reports results are empty. What could be the problem?

D – A (Wrong FROM and TO data runtime parameters) and B (The PCI groups are empty).

Lab 13 Application End-User Identifier

13.1 Configuring Application End-User Identifier

Overview

InfoSphere Guardium Application End-User Identifier provides a packaged solution that addresses security and compliance requirements for the data managed by major enterprise applications — without requiring changes to existing business processes or application source code. These applications include:

- Oracle E-Business Suite
- SAP ERP and NetWeaver BW
- PeopleSoft
- IBM Cognos®
- Siebel
- Business Objects Web Intelligence

The InfoSphere Guardium solution provides granular, preconfigured policies for SAP and Oracle EBS applications to rapidly identify suspicious or unauthorized activities, such as changes to sensitive objects or multiple failed logins. Sensitive objects, which can require significant research to locate, are identified through the Guardium Knowledgebase service to facilitate the development of custom policies.

The InfoSphere Guardium solution also identifies application user IDs for custom and packaged applications built upon standard application-server platforms, such as: IBM WebSphere®, BEA WebLogic, Oracle Application Server or JBoss Enterprise Application Platform.

Objectives

This lab will give an overview of Application User Translation and the different approaches available for determining a specific user from a pooled connection. This lab will concentrate on SAP Applications illustrating the difference between ABAP and JAVA Stacks as well as determining which SAP kernel is installed and why it matters. This lab will discuss the different requirements and approaches for SAP Application User Translation, keying on the following topics:

- __1. Application User Translation methods
- __2. Verifying SAP Kernel for ABAP and JAVA Stacks
- __3. Logging activation
- __4. Populate Pre-Defined Application Groups
- __5. Application End User Configuration (SAP-DB)
- __6. Application End User Configuration (SAP-Observed)
- __7. Create/run reports

Implementing SAP Application User Translation

There are 3 Methods of SAP Application User Translation:

1. New Method (Full capability, ready for immediate use)
2. SAP database method
3. SAP observed method

New Method: This new method only requires you to populate two SAP groups (SAP APP Servers, SAP DB Servers) and restart Inspection Engines. This method currently supports only IBM DB2 and Oracle databases and has minimum SAP kernel version requirements as listed below:

DB2 with SAP Version 7.00 or higher, Oracle with SAP Version 7.10 or higher

SAP database method: SAP audit has to be enabled and Application End User Translation on appliance window configured. It also requires SAP database user name and password. It relies on reading the audit data produced by SAP on the database. Guardium simply connects, reads it and places it in a custom domain. Customers did not like this method because of the need to save on appliance the database user name password for looking at the audit data produced by SAP on the database. That is why we developed the SAP observed method.

SAP observed method: It requires Application End User Translation on appliance window configured (only Application code, type, version and IP are required) and scheduled and an inspection engine restart. It works with the same logic as the SAP database method but instead of connecting to the database and reading what's done on a set of tables used by the SAP application, it gets this info from the observed traffic.

The SAP-DB and SAP observed methods are essentially the same in terms of functionality. The same internal SAP tables are being referenced, but with the SAP observed method, the extract is from the actual traffic (insert commands) to the same tables.

For the SAP database method, a database connection will be required and the customer will more than likely want to know what tables Guardium will need access to, regardless of whether they are sensitive objects. Following is a list of SAP tables that will be accessed to upload information into Guardium (internal audit SAP tables).

VBHDR – Update Header Record Table

VBMOD – Update Function Modules Table (Functions accessed for updates)

VBDATA – Update Data Table (includes actual update data)

CDHDR – Change document header record (changed data header info)

STXH – SAPscript text file header

VBERROR – Update Error Table (Includes error msgs)

Understanding ABAP and JAVA Stacks

Before discussing how to validate the SAP kernel, it's very important to understand the difference between SAP Stacks.

How to Validate SAP Stack for Application User Translation

When supporting InfoSphere Guardium SAP Application User Translation, there is a difference between the ABAP Stack and Java Stack.

Note: ABAP Stack and Java Stack have different kernel specifications.

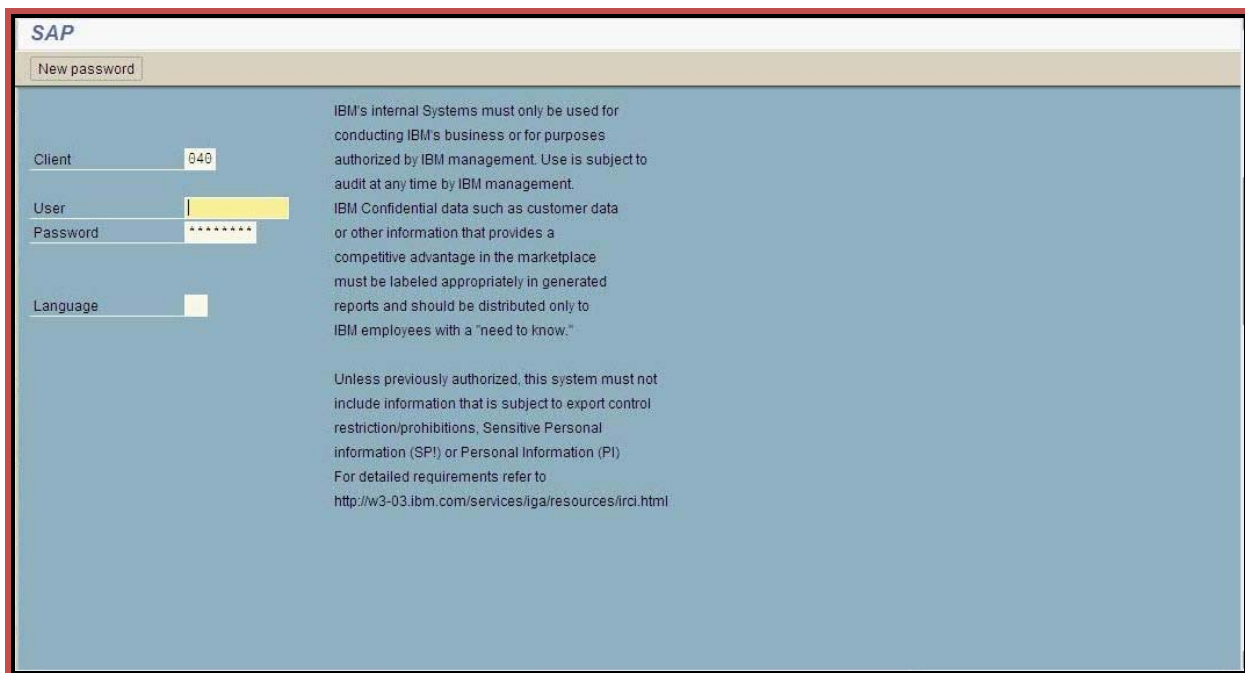
Note: ABAP Stack and Java Stack systems will have different tables.

ABAP STACK

Traditional ECC (Enterprise Core Components) SAP systems are written in ABAP code and are predominantly accessed by means of the SAP GUI, although web access is possible.

SAP ABAP systems have direct (read/write/update) access to traditional SAP databases. The databases are very large and contain all the sensitive data. This is where InfoSphere Guardium will be best used.

The following screen will appear when you enter the SAP GUI (ABAP STACK)



SAP GUI (ABAP Stack)

- __1. To validate the ABAP Stack SAP Kernel module for Application User Translation, follow these steps:
 - __1. Login to SAP.
 - __2. Go to System > Status

The screenshot shows the 'System: Status' dialog box with the following data:

Usage data			
Client	001	Previous logon	07.12.2010 05:46:08
User	DDIC	Logon	09.12.2010 11:59:01
Language	EN	System time	13:41:05
		Time zone	CET 19:41:05

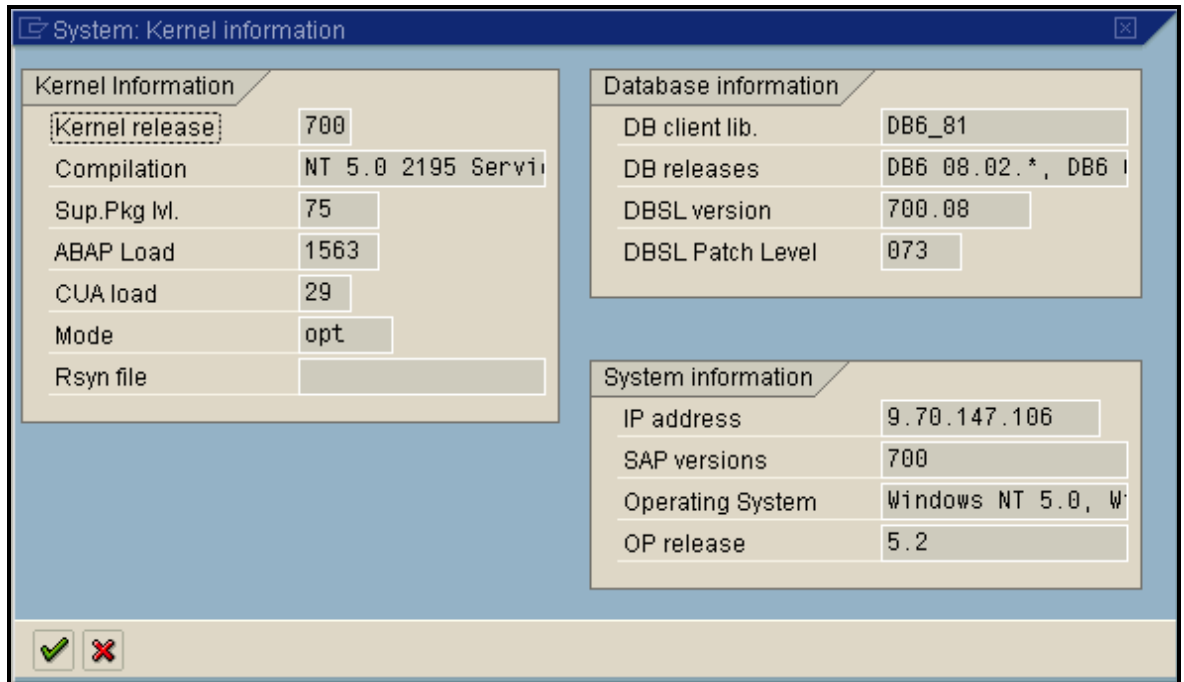
SAP data	
Repository data	
Transaction	SM51
Program (screen)	SAPLSLVC_FULL:
Screen number	500
Program (GUI)	RSM51000_ALV
GUI status	STANDARD
SAP System data	
Component version	SAP ECC 6.0
Installation number	0020306546
License expiration	31.12.9999
Unicode System	Yes

Host data		Database data	
Operating system	Windows NT	Database system	DB6
Machine type	2x Intel 8	Release	09.01.0000
Server name	pu10wsapec6a	Name	E6A
Platform ID	560	Host	pu10wsapec6a
		Owner	SAPE6A

At the bottom of the dialog, there is a 'Navigate' button with a green arrow icon, which is highlighted with a red box. Below the buttons is the text 'Other kernel info. (Shift+F5)'.

__3. System Status (ABAP Stack)

- __a. Click the “Other Kernel Info” button at the bottom of the System Status screen



System Kernel Information (ABAP Stack)

In this example, the kernel is 700.

SAP with a DB2 backend is also available for SAP kernel 640, but the user needs to set DB6_DBSL_ACCOUNTING=1 (in kernel 700 and up, this DB6_DBSL_ACCOUNTING value is 1 by default).

SAP for Oracle backend requires a kernel of 710 or higher.

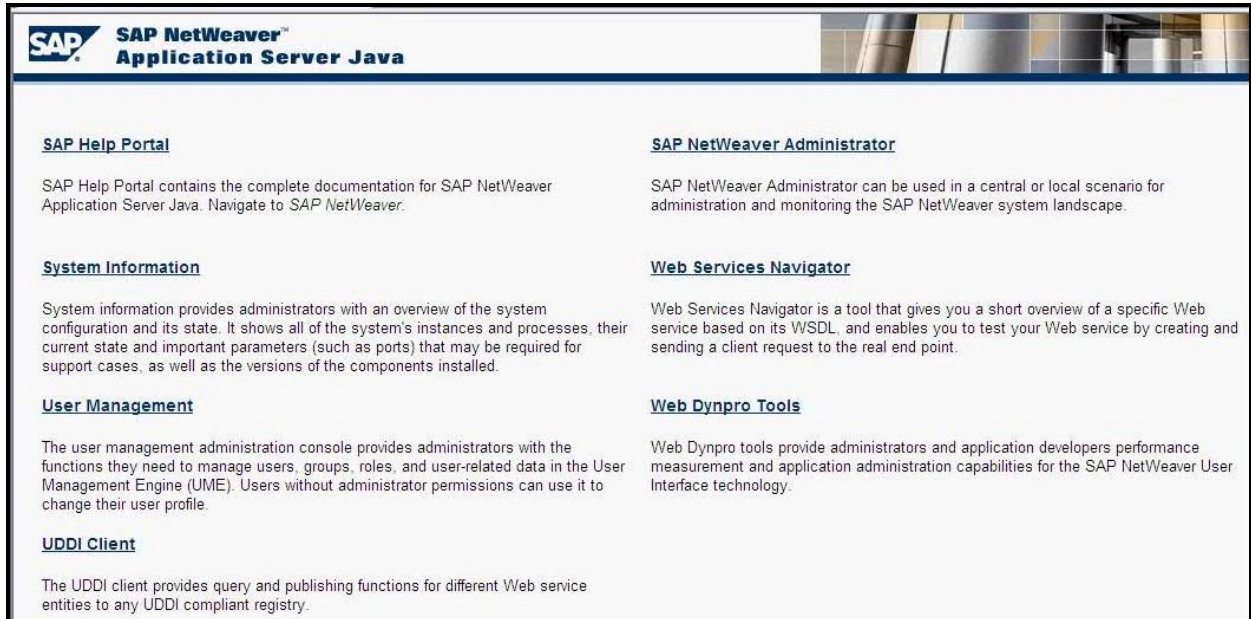
Data gets put into the app user field and the app event string

JAVA STACK

SAP Portal systems are written in Java code and are the front-end web applications using pre-canned queries to display SAP-related web pages.

Portal systems can only be accessed with a web browser. Portal system databases are much smaller with only a few table spaces.

__1. The following screen will appear when you enter SAP Portal System (Java Stack).



SAP NetWeaver™ Application Server Java

<p><u>SAP Help Portal</u></p> <p>SAP Help Portal contains the complete documentation for SAP NetWeaver Application Server Java. Navigate to <i>SAP NetWeaver</i>.</p>	<p><u>SAP NetWeaver Administrator</u></p> <p>SAP NetWeaver Administrator can be used in a central or local scenario for administration and monitoring the SAP NetWeaver system landscape.</p>
<p><u>System Information</u></p> <p>System information provides administrators with an overview of the system configuration and its state. It shows all of the system's instances and processes, their current state and important parameters (such as ports) that may be required for support cases, as well as the versions of the components installed.</p>	<p><u>Web Services Navigator</u></p> <p>Web Services Navigator is a tool that gives you a short overview of a specific Web service based on its WSDL, and enables you to test your Web service by creating and sending a client request to the real end point.</p>
<p><u>User Management</u></p> <p>The user management administration console provides administrators with the functions they need to manage users, groups, roles, and user-related data in the User Management Engine (UME). Users without administrator permissions can use it to change their user profile.</p>	<p><u>Web Dynpro Tools</u></p> <p>Web Dynpro tools provide administrators and application developers performance measurement and application administration capabilities for the SAP NetWeaver User Interface technology.</p>
<p><u>UDDI Client</u></p> <p>The UDDI client provides query and publishing functions for different Web service entities to any UDDI compliant registry.</p>	

SAP Portal System (Java Stack)

- __1. To validate the Java Stack SAP Kernel module for Application User Translation, follow these steps:
 - __a. Click on System Information.

System TCJ

Find other systems in SLD...

Message Server	Enqueue Server	Database	Software Components	all components...	Licenses
Host: magn13	Host: magn13	Name: TCJ	Name	Applied	Installation Number 0020278108
Port: 3901	Port: 3201	Host: magn13	sap.com/SAP-JEECOR	20110523201119	System Number 00000000310632781
		Type: DB2/AIX64 (SQL09056)	sap.com/SAP-JEE	20110106170950	Software Product Days Until Expiry
			7.00 SP22 (1000.7.00.22.6.20110114162028)		J2EE-Engine_DB6 2917625
			7.00 SP22 (1000.7.00.22.0.20100607123451)		

Instance JC00

Host: magn13 OS: AIX (ppc64) 5.3

dispatcher

VM	system properties...	Cluster
PID:	1003758	Node ID: 2919900
Name:	IBM J9 VM	Kernel Version: 7.00 PatchLevel 97159.450
Vendor:	IBM Corporation	HTTP Port: 50000
Version:	2.3	HTTPS Port: 50001
VM Parameters		P4 Port: 50004
		Telnet Port: 50008

server0

VM	system properties...	Cluster
PID:	868526	Node ID: 2919950
Name:	IBM J9 VM	Kernel Version: 7.00 PatchLevel 97159.450
Vendor:	IBM Corporation	
Version:	2.3	
VM Parameters		

SDM

VM
PID: 569398
SDM Port: 50018

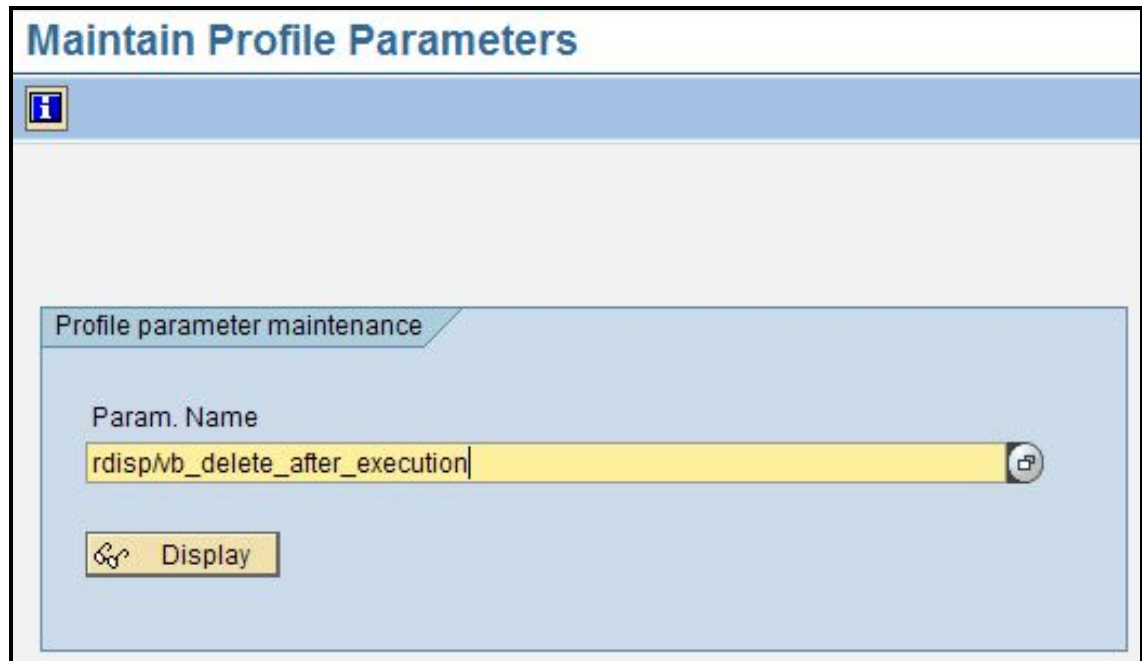
V-System TCJ (Java Stack)

In this example, the SAP Kernel version is 7.00.

SAP for either DB2 or Oracle requires a kernel of 7.02 or higher.

SAP sets similar client properties in the Java stack as it did for ABAP Stack.

- __2. Verify Logging is activated
- __a. Go to transaction RZ11 (Maintain Profile Parameters) and enter 'rdisp/vb_delete_after_execution' for Param Name, and then click **Display**



The screenshot shows the SAP 'Maintain Profile Parameters' transaction. The title bar reads 'Maintain Profile Parameters'. Below the title bar is a blue header with an information icon. The main content area is titled 'Profile parameter maintenance'. It contains a text field labeled 'Param. Name' with the value 'rdisp/vb_delete_after_execution' entered. To the right of the text field is a lock icon. Below the text field is a button labeled '& Display'.

The default value is 1 which means that update records will be deleted after execution. We want to change the value to 2.

This will have to be done by a member of the local SAP Basis staff with proper authority.

Display Profile Parameter Attributes

Documentation
Change Value

Param. Name
rdisp/vb_delete_after_execution

Short description(Engl)	Delete update requests after execution?
Appl. area	Update
ParameterTyp	Integer value
Changes allowed	Change generates warning
Valid for oper. system	All operating systems
Minimum	1
Maximum	2
DynamicallySwitchable	<input checked="" type="checkbox"/>
Same on all servers	<input type="checkbox"/>
Dflt value	1
ProfileVal	1
Current value	1

The Current Value must be set to 2 so that the logs will not be deleted after execution.

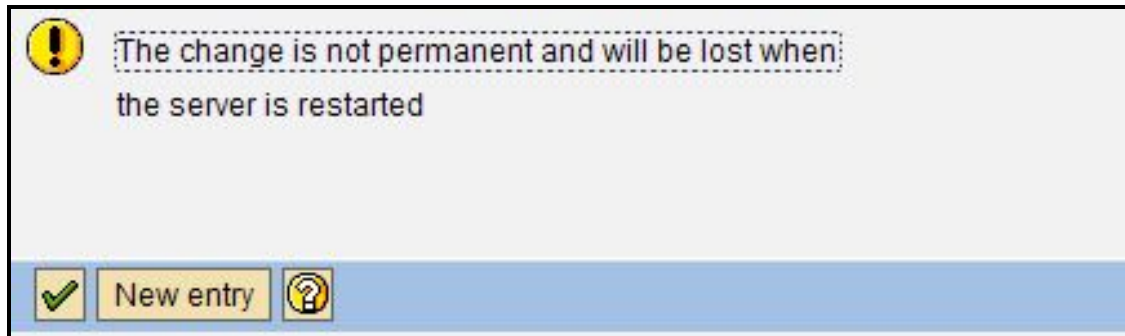
- __b. Click on **Change Value**.
- __c. Enter '2' for *New value*.

Parameter values

Param. Name rdisp/vb_delete_after_execution

Dflt value	1
ProfileVal	1
Current value	1
New value	2

Switch on all servers



- __d. Click on green check mark to save
- __e. Verify the Change

Display Profile Parameter Attributes

Documentation

Param. Name:

Short description(Engl)	Delete update requests after execution?		
Appl. area	Update		
ParameterTyp	Integer value		
Changes allowed	Change generates warning		
Valid for oper. system	All operating systems		
Minimum	<input type="text" value="1"/>		
Maximum	<input type="text" value="2"/>		
DynamicallySwitchable	<input checked="" type="checkbox"/>		
Same on all servers	<input type="checkbox"/>		
Dflt value	<input type="text" value="1"/>		
ProfileVal	<input type="text" value="1"/>		
Current value	<input type="text" value="2"/>		
Switched from	LARRY	27.09.2011	10:24:18

WARNING: When set to 2, automatic deletion is deactivated. This value can be used to get the update and database performance. In this case, the report rsm13002 with the parameter DELETE = X should run in the background at least once a day to prevent the update tables from becoming excessively large.

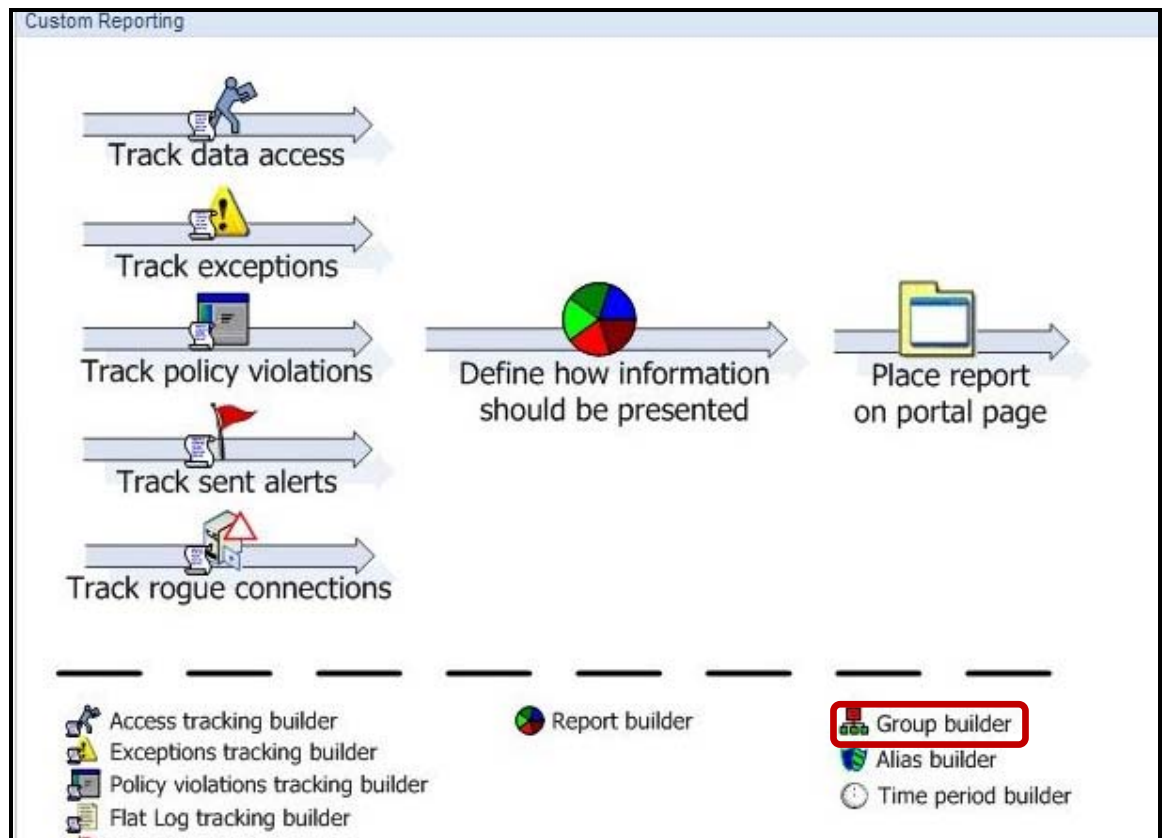
WARNING: These settings will revert back to default each time the system is restarted. This can be overridden via SAP Transaction RZ10.

__3. Populate Pre-Defined Application Groups

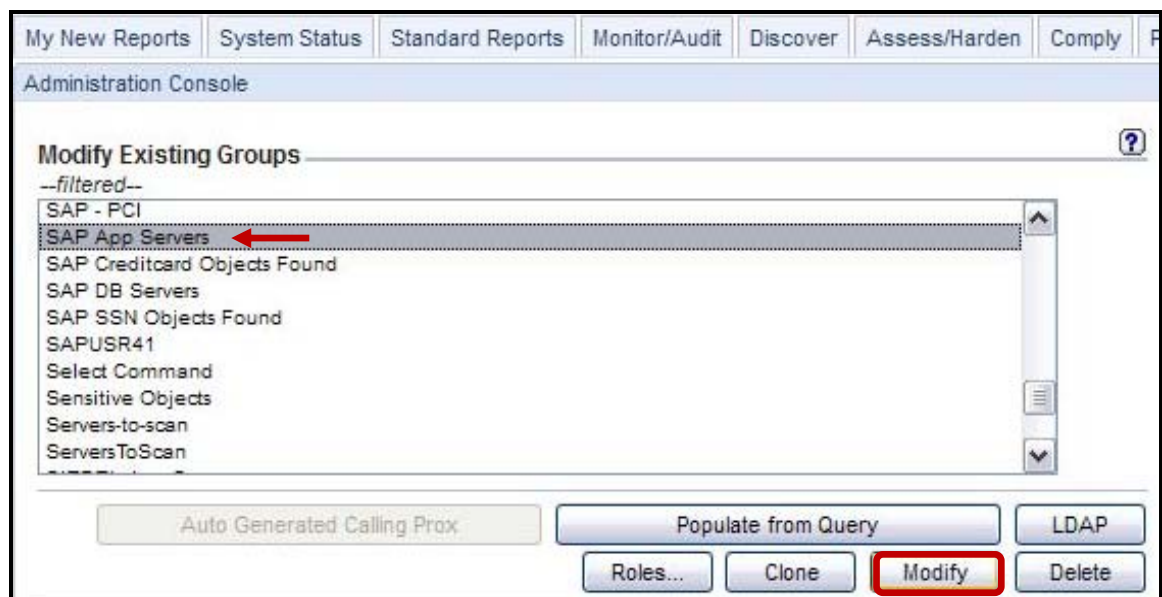
When Application User Translation has been configured, you must populate at least two pre-defined groups with information that will be specific to your environment. The table below identifies the groups that must be populated for each application type.

Application	Pre-Defined Group	Group Type
EBS	EBS App Servers EBS DB Servers	Client IP Server IP
PeopleSoft	PSFT App Servers PSFT DB Servers PeopleSoft Objects	Client IP Server IP Objects
Siebel	SIEBEL App Servers SIEBEL DB Servers	Client IP Server IP
SAP	SAP App Servers SAP DB Servers SAP - PCI	Client IP Server IP Objects

__a. Click **Group Builder**



__b. Select **SAP App Servers**, and then click **Modify**.



__c. Insert the **Client IP Address** value, and then click **Update**

The screenshot shows the 'Administration Console' interface for managing group members. At the top, there are navigation tabs: 'My New Reports', 'System Status', 'Standard Reports', 'Monitor/Audit', 'Discover', 'Assess/Harden', 'Comply', and 'Protect'. Below these is the 'Administration Console' header. The main section is titled 'Manage Members for Selected Group' with a help icon. It shows the 'Group Name' as 'SAP App Servers' and 'Group Type' as 'Client IP'. There is a 'Category' input field and a 'Modify Category' button. Below this is a 'Group Members' section with a 'Filter' input field and a refresh icon. A list of members is shown, with one member having the IP address '9.70.147.106'. At the bottom, there are four options: 'Create & add a new Member named' with an input field and an 'Add' button; 'Add an existing Member to Group' with a dropdown menu and an 'Add' button; 'Rename selected Member to' with an input field and an 'Update' button; and 'Delete selected Member' with a 'Delete' button that is highlighted with a red box.

Repeat the same process for SAP DB Servers group with the Server IP Address.

- __4. Application End User Configuration (SAP database)
- __a. Select Administration Console -> Application User Translation
- __b. Click on **+ Add App User Translation**

The following sample configuration is used for reference:

Administration Console

Configuration

- Alerter
- Anomaly Detection
- Application User Translation**
- Custom ID Procedures
- Customer Uploads
- Flat Log Process
- Global Profile
- Guardium for z/OS
- Incident Generation
- Inspection Engines
- IP-to-Hostname Aliasing
- Policy Installation
- Portal
- Query Hint
- Session Inference
- System
- Upload Key File

Data Management

Central Management

Local Taps

Guardium Definitions

Custom Alerting

Module Installation

Application User Translation Configuration ?

+ Add App User Translation

Application Code: SAP DB

Application Type: SIEBEL DB

Application Version: R3 4.7

Database Type: ORACLE

Server IP: 192.168.100.100

Port: 1521

Instance Name:

DB Name:

Active:

User Name: sapr3

Password: ●●●●●●

Responsibility:

Reset Add

Scheduling

●● Application User Translation is currently not scheduled for execution.

Modify Schedule... Run Once Now

This step is optional and would not normally have to be used for SAP database Method with required kernel. In the case where this procedure must be performed, follow the steps on the next page.

- ___c. Application User Translation Configuration settings (SAP DB)
 - Application Code:* *Reference only but must be completed*
 - Application Type:* *SAP DB*
 - Application Version:* *Reference only but must be completed*
 - Application Server Type:* *DBMS used on the back end*
 - Server IP:* *DB server which SAP stores the data*
 - Port:* *DB Port that SAP uses*
 - Instance Name:* *DB Instance that SAP uses*
 - DB Name:* *This is left blank*
 - Active:* *Checked*
 - User Name:* *SAP pooled user name*
 - Password:* *SAP pooled user password*
 - Responsibility:* *Unchecked*

Schedule the process to run automatically so updates will be included in future reports.
For POCs, choose Run Once Now.

- __5. Application End User Configuration (SAP Observed)
- __a. Select Administration Console -> Application User Translation
- __b. Click on **+ Add App User Translation**

Administration Console

Configuration

- Alerter
- Anomaly Detection
- Application User Translation
- Custom ID Procedures
- Customer Uploads
- Flat Log Process
- Global Profile
- Guardium for z/OS
- Incident Generation
- Inspection Engines
- IP-to-Hostname Aliasing
- Policy Installation
- Portal
- Query Hint
- Session Inference
- System
- Upload Key File

Data Management

Central Management

Local Taps

Guardium Definitions

Custom Alerting

Module Installation

Application User Translation Configuration

+ Add App User Translation

Application Code: SAP

Application Type: SAP Observed

Application Version: R3 4.7

Database Type: [v]

Server IP: 192.168.100.100

Port: []

Instance Name: []

DB Name: []

Active:

User Name: root

Password: []

Responsibility:

Reset Add

Scheduling

●● Application User Translation is currently not scheduled for execution.

Modify Schedule... Run Once Now

Reference the following steps on next page to configure

- ___c. Application User Translation Configuration settings (SAP Observed)
 - Application Code:* *This must be filled in and is for reference only*
 - Application Type:* *SAP Observed*
 - Application Version:* *This must be filled in and is for reference only*
 - Database Type:* *This is left blank*
 - Server IP:* *Database server which SAP stores the data*
 - Port:* *This is left blank*
 - Instance Name:* *This is left blank*
 - DB Name:* *This is left blank*
 - Active:* *Checked*
 - User Name:* *This is left blank*
 - Password:* *This is left blank*
 - Responsibility:* *Unchecked*

Schedule the process to run automatically so updates will be included in future reports.
For POCs, choose Run Once Now.

- __6. Using the IBM InfoSphere Guardium GUI, demonstrate the ease of use within the IBM InfoSphere Guardium solution. Start the IBM InfoSphere Guardium appliance and login.
- __a. From your laptop, browse to <https://10.10.9.248:8443>
- __b. Login as **pot / guardium**.

Login

Please enter your information

User name:

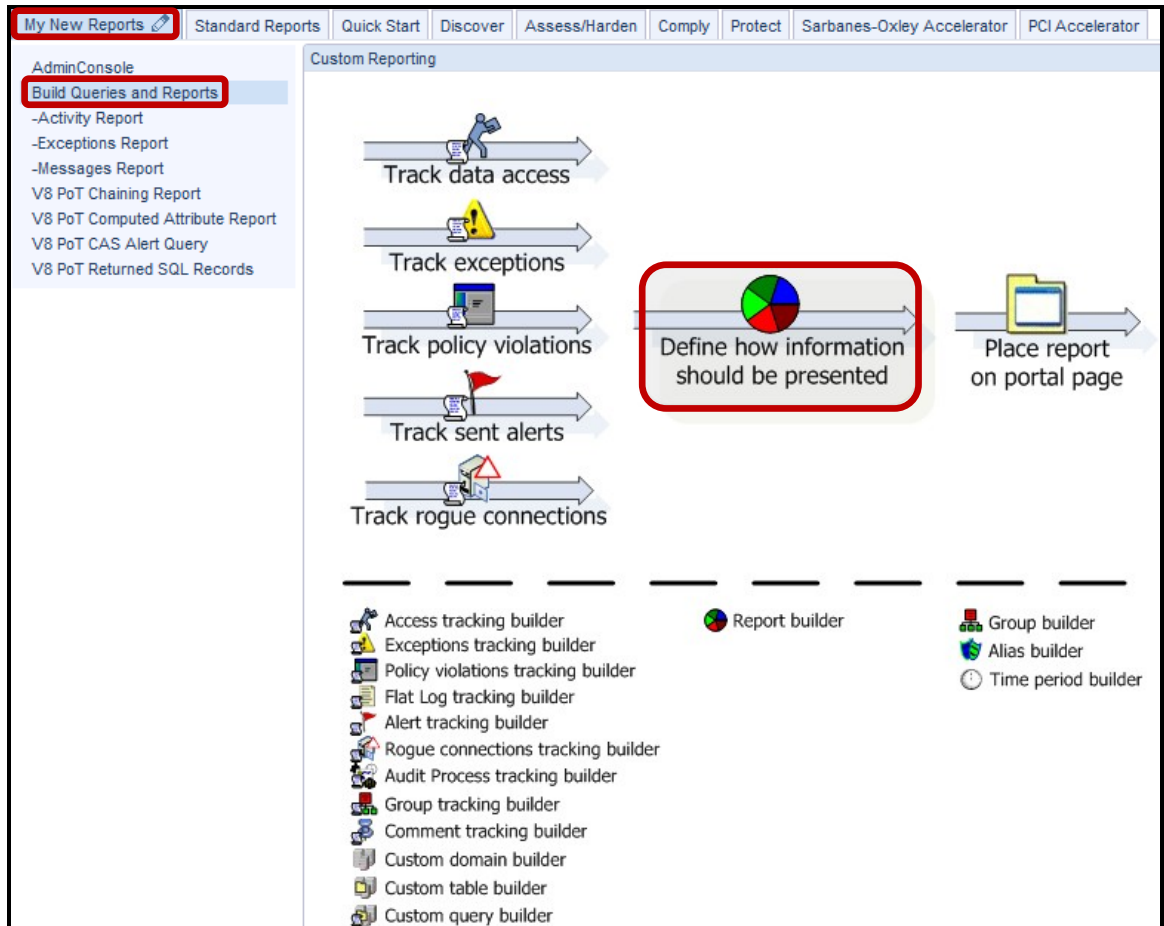
Password:

Please note that after some time of inactivity, the system will log you out automatically and ask you to sign in again.

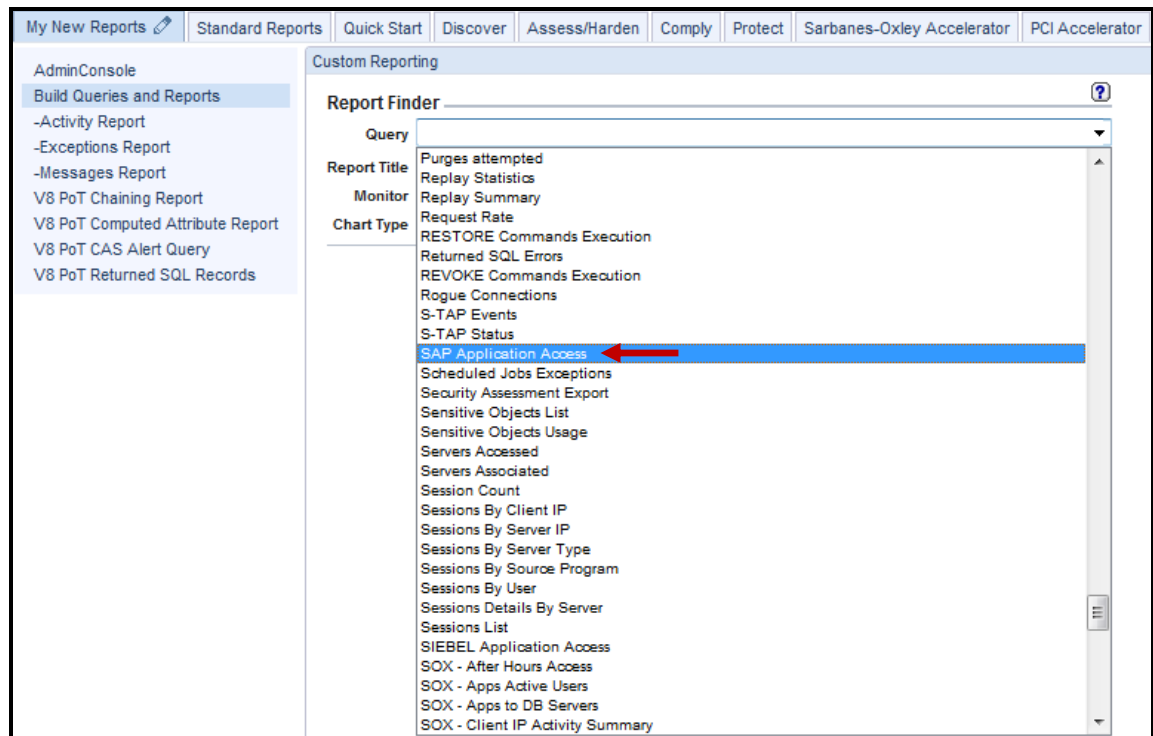
Licensed Materials - Property of IBM, 5725A85, 5725A86, 5725A87, 5725A89, 5725A90, 5725A91, 5725A92. © Copyright 2002, 2011 IBM Corporation. IBM, the IBM logo, and InfoSphere are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Guardium and S-TAP are trademarks of IBM, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other product and service names might be trademarks of IBM, Guardium, or other companies. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

CSS Parser © Copyright 1991, 1999 Free Software Foundation, Inc. Java CIFS Client Library © Copyright 2004, Michael B. Allen jcifs@samba.org. JRadius © Copyright 2004-2005, PicoPoint, B.V. JRadius Client © Copyright 2003, Robert J. Loihl. Jregistrykey © Copyright 2001, BEQ Technologies Inc. libui-dialog © Copyright 2003, Kevin C. Krinke kckrinke@opendoorsoftware.com. Zthread © Copyright 2000-2003, Eric Crahen.

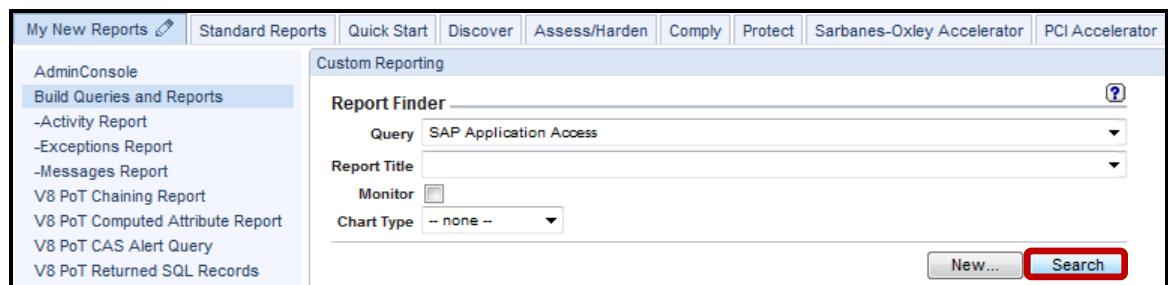
- c. Click **Build Queries and Reports** under the **My New Reports** tab and then select **'Define how information should be presented'**.



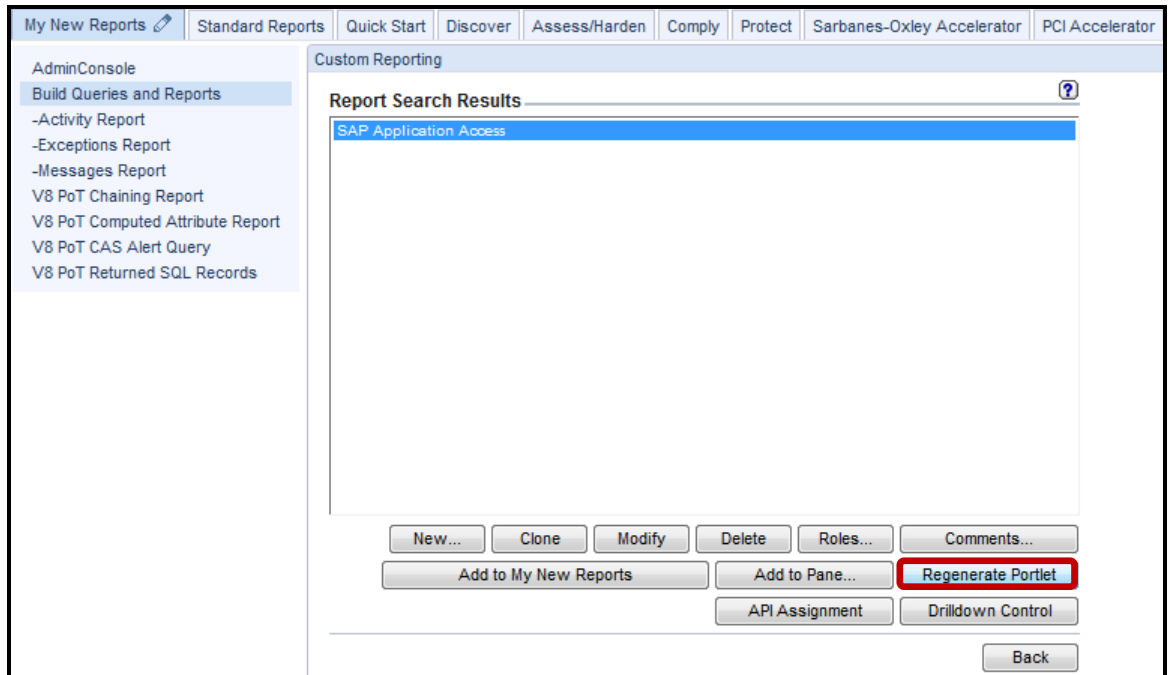
__d. Select **SAP Application Access** from the *Query* dropdown list.



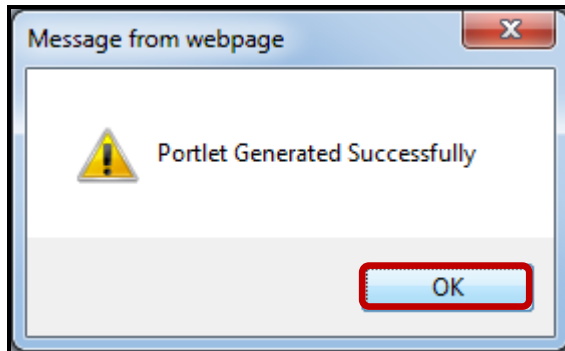
__e. Click **Search**.



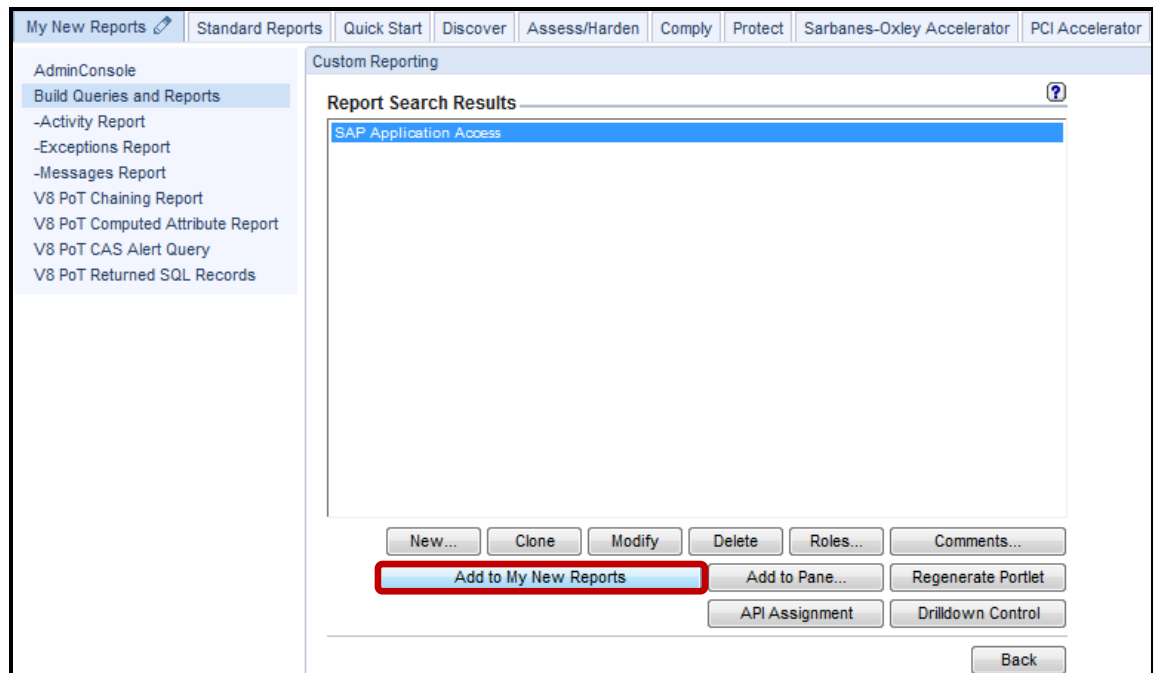
__f. Click **Regenerate Portlet**



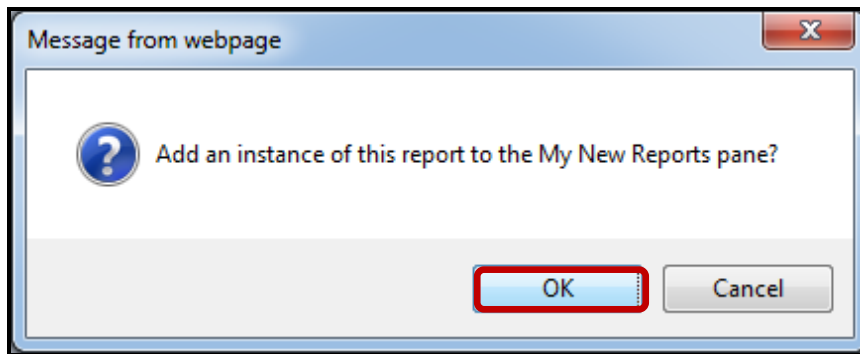
__g. Click **OK** to acknowledge.



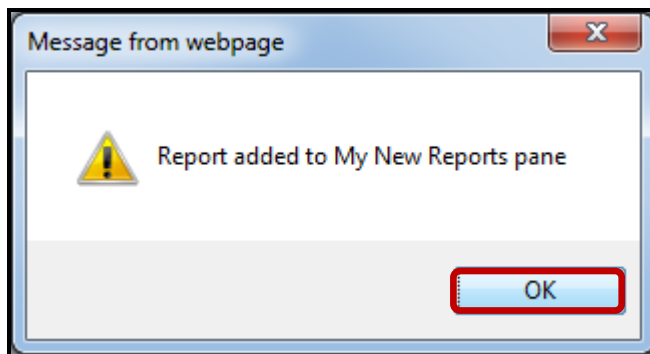
__h. Click **Add to My New Reports**



- __i. Click **OK** to confirm.



- __j. Click **OK** again to acknowledge.



__k. Confirm that report was added to My New Reports

The screenshot shows the 'Custom Reporting' section of the IBM Security Center for Applications (SCA) interface. On the left, a navigation pane lists various reports, with 'SAP Application Access' highlighted in red. The main workspace displays a sequence of steps for creating a report:

- 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

Below the workflow, a legend identifies the builders used:

- 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

SAP-DB Report Examples

SAP Application Access								
Start Date: 2011-04-02 19:44:09 End Date: 2011-10-02 20:44:09								
Aliases: OFF								
Application Type	Application Code	Item Name	User	Operation Type	Transaction Code	System Id	Change Date	Record Detail 1
SAP-DB	SAPs	ADRESSE	DDIC	U	XD01	000	2011-07-28 14:39:35.0	BP 0000023809
SAP-DB	SAPs	ADRESSE3	JOE	U	SU01	800	2011-07-28 22:32:51.0	BC0100000573530000008322
SAP-DB	SAPs	ADRESSE3	LARRYU		SU01	001	2011-09-30 14:18:29.0	BC0100000240690000009941
SAP-DB	SAPs	DEBI	DDIC	I	XD01	000	2011-07-28 14:39:35.0	A1111Z
SAP-DB	SAPs	NRINTERVALJOE	JOE	U	SU01	800	2011-07-28 22:32:51.0	SO_OBJ_FOL
SAP-DB	SAPs	NRINTERVALJOE	JOE	U	SU01	800	2011-07-28 22:32:51.0	SO_OBJ_USR

Records 1 to 6 of 6

Entity List

- Client/Server
- Session
- Application Data

SAP Application Access

Main Entity: Application Data Add Count Add Distinct Sort by count

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Application Data	Application Type	Value		<input type="checkbox"/>
<input type="checkbox"/>	2	Application Data	Application Code	Value		<input type="checkbox"/>
<input type="checkbox"/>	3	Application Data	Item Name	Value		<input type="checkbox"/>
<input type="checkbox"/>	4	Application Data	User	Value		<input type="checkbox"/>
<input type="checkbox"/>	5	Application Data	Operation Type	Value		<input type="checkbox"/>
<input type="checkbox"/>	6	Application Data	Transaction Code	Value		<input type="checkbox"/>
<input type="checkbox"/>	7	Application Data	System Id	Value		<input type="checkbox"/>
<input type="checkbox"/>	8	Application Data	Change Date	Value		<input type="checkbox"/>
<input type="checkbox"/>	9	Application Data	Record Detail 1	Value		<input type="checkbox"/>

Query Conditions

Addition mode: AND OR HAVING

Entity	Agg.	Attribute	Operator	Runtime Param.
<input type="checkbox"/> WHERE	Application Data	Application Type	LIKE	Value SAP%

SAP Application Access							
Start Date: 2007-03-15 00:00:00 End Date: 2007-05-26 00:00:00							
Application Type	Application Code	Item Name	User	Operation Type	Transaction Code	System Id	Change Date
SAP	SAP	BANK	DDIC	U	FI02	800	2007-03-22 23:00:42 800US 083000108
SAP	SAP	BANK	DDIC	U	FI02	800	2007-03-22 23:01:40 800US 083000108
SAP	SAP	BANK_WRITE_DOCUMENT	DDIC	2	FI02	800	2007-03-22 23:00:42 BD01FF050201020200003131303000
SAP	SAP	BANK_WRITE_DOCUMENT	DDIC	2	FI02	800	2007-03-22 23:01:40 C201FF050201020200003131303000
SAP	SAP	POST_BANK_ADDRESS	DDIC	1	FI02	800	2007-03-22 23:00:42 D200FF050201020200003131303000
SAP	SAP	POST_BANK_ADDRESS	DDIC	1	FI02	800	2007-03-22 23:01:40 D500FF050201020200003131303000

Aliases: OFF

Application User Translation does show the breakdown of the transactions – not in a SQL form but in a “SAP form.” For example, a single SAP transaction IW32 (shown in the transaction code) will show up as multiple lines revealing the precise drill down of “what happened” — which is the item name. The operation type and the item name are the details. Results can be grouped by their change date.

New Method Report Example – Custom Report

SAP Transaction Tracking				
Start Date:	2011-09-25 19:48:31	End Date:	2011-10-02 23:48:31	
Aliases:	OFF	ApplicationUserLike:	LIKE %LARRY	
CLIENTPLike:	LIKE %	DBUserLike:	LIKE %	
EventValueStrLike:	LIKE %	FULLSQLLike:	LIKE %	
ObjectName:	LIKE %	ServerPLLike:	LIKE %	
Timestamp	Client IP	DB User Name	Application User	Full Sql
2011-09-30 21:15:56.0	9.70.147.106	SAPE6A	LARRY	SET CLIENT USERID 'LARRY'
2011-09-30 21:15:16.0	9.70.147.106	SAPE6A	LARRY	SELECT * FROM "TPFYPROPTY" WHERE "PARAMNAME" LIKE ? FETCH FIRST 1 ROWS ONLY OPTIMIZE FOR 1 ROWS WITH UR -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLTHFB , 8750) -- SYSTEM(E6A , SAPE6A)
2011-09-30 21:15:16.0	9.70.147.106	SAPE6A	LARRY	SELECT * FROM "TPFYPROPTY" WHERE "PARAMNAME" LIKE 'rdisp/vb_delete_after_execution' FETCH FIRST 1 ROWS ONLY OPTIMIZE FOR 1 ROWS WITH UR -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLTHFB , 8750) -- SYSTEM(E6A , SAPE6A)
2011-09-30 21:15:16.0	9.70.147.106	SAPE6A	LARRY	SELECT * FROM "TPFYPROPTY" ORDER BY "PARAMNAME" WITH UR -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLSPFC , 13528) -- SYSTEM(E6A , SAPE6A)
2011-09-30 21:15:16.0	9.70.147.106	SAPE6A	LARRY	UPDATE "TPFYPROPTY" SET "SUSR" = ? , "SDATE" = ? , "STIME" = ? WHERE "PARAMNAME" = ? -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLTHFB , 8928) -- SYSTEM(E6A , SAPE6A)
2011-09-30 21:15:16.0	9.70.147.106	SAPE6A	LARRY	UPDATE "TPFYPROPTY" SET "SUSR" = 'LARRY' , "SDATE" = '20110930' , "STIME" = '211617' WHERE "PARAMNAME" = 'rdisp/vb_delete_after_execution' -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLTHFB , 8928) -- SYSTEM(E6A , SAPE6A)

AppUser with Full SQL

Thank you

13.2 Identify Users with GuardAppEvents API

Overview

For some applications that manage users internally, the application user cannot be identified from the traffic. When this happens, you can use the Guardium Application Events API. The Application Events API provides simple “no-op” calls that can be issued from within the application to signal Guardium when a user acquires or releases a connection, or when any other event of interest occurs.

This Lab section will focus on the following topics:

- Set the Application User using GuardAppUser
- Clear the Application User with GuardAppUserReleased
- Set an Application Event using GuardAppEvent

The syntax for each Guardium Application Events API is described below.

Note: If your Guardium security policy has Selective Audit Trail enabled, the Application Events API commands used to set and clear the application user and/or application events will be ignored by default, and the application user names and/or application events will not be logged. To log these items so that they will be available for reports or exceptions, you should include a policy rule to identify the appropriate commands, specifying the Audit Only rule action.

__1. Set the Application User using GuardAppUser

Use this call to indicate that a new application user has taken control of the connection. The supplied application user name will be available in the Application User attribute of the Access Period entity. For this session, from this point on, Guardium will attribute all activity on the connection to this application user, until Guardium receives either another GuardAppUser call or a GuardAppUserReleased call (which clears the application user name, as described below).

To signal when other events occur (you can define event types as needed), use the GuardAppEvent call, described in the following section.

Syntax: `SELECT 'GuardAppUser:user_name' FROM location`

user_name is a string containing the application user name. This string will be available as the Application User attribute value in the Access Period entity.

FROM location is used only for Oracle, DB2, or IBM Informix®. (Omit for other database types.) It must be entered exactly as follows:

Oracle: **FROM DUAL**

DB2: **FROM SYSIBM.SYSDUMMY1**

Informix: **FROM SYSTABLES**

__2. Clear the Application User by using GuardAppUserReleased

Use the GuardAppUserReleased call to signal that the current user has relinquished control of the connection. Guardium will clear the application user name, which will remain empty for the connection until it receives another GuardAppUser call.

Syntax: `SELECT 'GuardAppUserReleased' FROM location`

FROM location is used only for Oracle, DB2, or Informix. (Omit for other database types.) It must be entered exactly as follows:

Oracle: **FROM DUAL**

DB2: **FROM SYSIBM.SYSDUMMY1**

Informix: **FROM SYSTABLES**

__3. Set an Application Event using GuardAppEvent

This call provides a more generic method of signaling the occurrence of application events. You can define your own event types and provide text, numeric, or date values to be stored with the event — both when the event starts and when it ends. You may want to use this call together with the GuardAppUser call described above. Guardium will attribute all activity on the connection to this application event, until it receives either another GuardAppEvent:Start command or a GuardAppEvent:Released command.

Syntax: `SELECT 'GuardAppEvent:Start|Released' ,
 'GuardAppEventType:type' ,
 'GuardAppEventUserName:name' ,
 'GuardAppEventStrValue:string' ,
 'GuardAppEventNumValue:number' ,
 'GuardAppEventDateValue:date' FROM location`

Start | Released - Use the keyword Start to indicate that the event is taking control of the connection or Released to indicate that the event has relinquished control of the connection.

type identifies the event type. It can be any string value, for example: Login, Logout, Credit, Debit, etc. In the Application Events entity, this value is stored in the Event Type attribute for a Start call, or the Event Release Type attribute for a Released call.

name is a user name value to be set for this event. In the Application Events entity, this value is stored in the Event User Name attribute for a Start call, or the Event Release User Name attribute for a Released call.

string is any string value to be set for this event. For example, for a Login event you might provide an account name. In the Application Events entity, this value is stored in the Event Value Str attribute for a Start call, or the Event Release Value Str attribute for a Released call.

number is any numeric value to be set for this event. For example, for a Credit event you might supply the transaction amount. In the Application Events entity, this value is stored in the Event Value Num attribute for a Start call, or the Event Release Value Num attribute for a Released call.

date is a user-supplied date and optional time for this event. It must be in the format: **yyyy-mm-dd hh:mm:ss**, where the time portion (hh:mm:ss) is optional. It may be the current date and time or it may be taken from a transaction being tracked. In the Application Events entity, this value is stored in the Event Date attribute for a Start call, or the Event Release Date attribute for a Released call.

FROM location is used only for Oracle, DB2, or Informix. (Omit for other database types.) It must be entered exactly as follows:

Oracle: **FROM DUAL**

DB2: **FROM SYSIBM.SYSDUMMY1**

Informix: **FROM SYSTABLES**

The GuardAppEvent call populates an Application Events entity. When creating Guardium queries and reports, you can access the Application Events entity from either the Access Tracking domain or the Policy Violations domain.

If any Application Events entity attributes have not been set using the GuardAppEvent call, those values will be empty.

Regarding the two date attributes:

Event Date is set using the GuardAppEvent call, or from a custom identification procedure as described in the following section.

Timestamp is the time that Guardium stores the instance of the Application Event entity.

End Part 2

Thank you

13.3 Custom ID Procedures

__1. Identify Users by means of Stored Procedures

In many existing applications, all of the information needed to identify an application user can be obtained from existing database traffic, from stored procedure calls. Once Guardium knows what calls to watch for, and which parameters contain the user name or other information of interest, users can be identified automatically.

In the simplest case, an application might have a single stored procedure that sets a number of property values, one of which is the user name. A call to set the user name might look like this:

```
set_application_property('user_name', 'JohnDoe');
```

In a custom procedure mapping (described later), you can tell Guardium to:

Watch for a stored procedure named *set_application_property*, with a first parameter value of *user_name*.

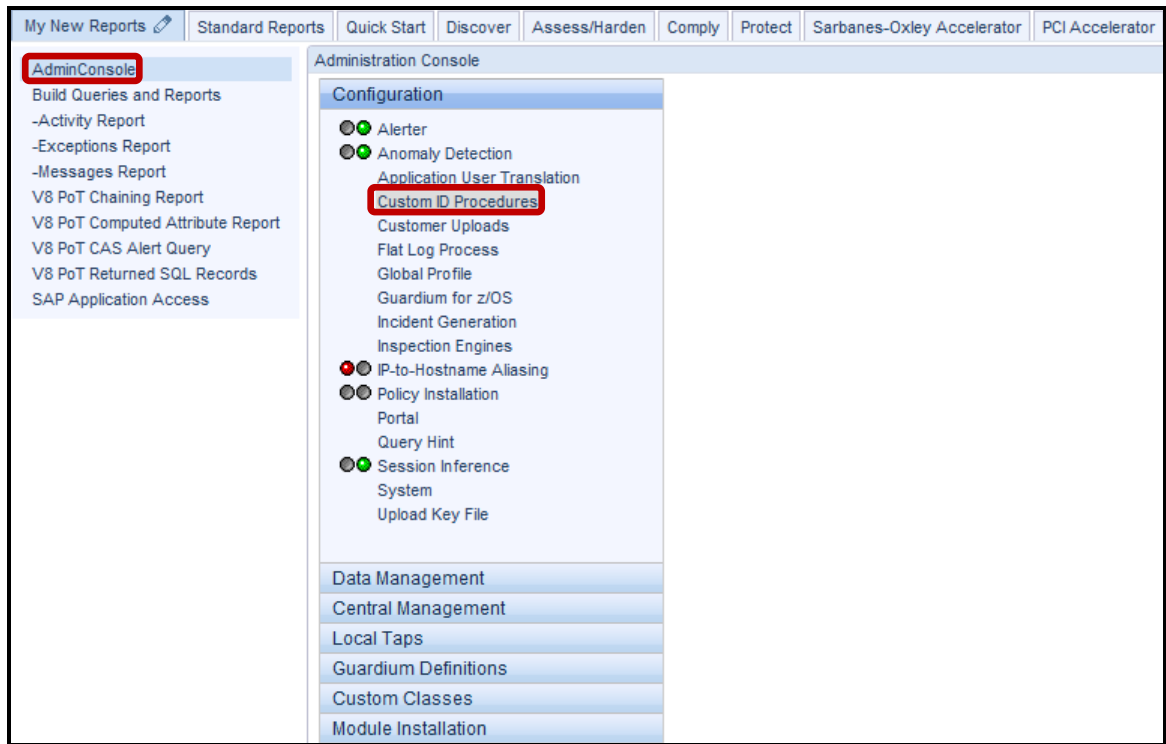
Set the application user to the value of the second parameter in the call (*JohnDoe*, in the example above).

There may be multiple stored procedures for an application: one to start an application user session, one to end a session, and others to signal key events particular to that application. Guardium's custom identification procedure mechanism can be used to track any application events you want to monitor.

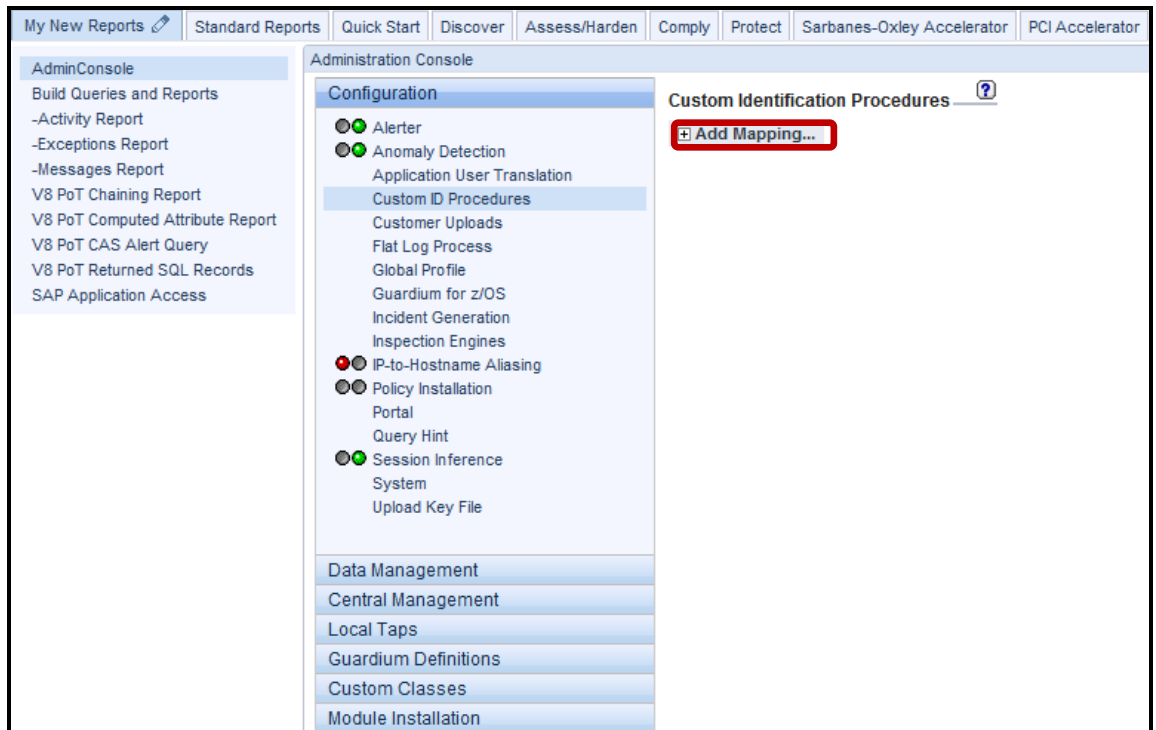
Since each of your applications may have a different way of identifying users, you may have to define separate custom identification procedure mappings for each application. To do that, follow the procedure outlined, below.

__2. Define a Custom Identification Procedure Mapping

__a. Click **AdminConsole** under the **My New Reports** tab, and click **Custom ID Procedures**.



__b. To add a mapping, click **+ Add Mapping** to expand the mapping dialogue.



- __c. In the **Custom Map Name** box, enter set_app_user as the name to be used for this mapping.
- __d. In the **Procedure Name** box, enter set_app_user as the name of the database procedure that will supply information.
- __e. Select **Set** or **Clear** from the Action list to indicate whether the procedure call will set or clear application values.

The screenshot shows the 'Custom Identification Procedures' configuration window. On the left is a 'Configuration' sidebar with various options like 'Alerter', 'Anomaly Detection', and 'Custom ID Procedures'. The main area is titled 'Custom Identification Procedures' and contains an 'Add Mapping...' section. Within this section, three fields are highlighted with a red box: 'Custom Map Name' (value: set_app_user), 'Procedure Name' (value: set_app_user), and 'Action' (value: Set). Below these are fields for 'Condition1 Location' (0), 'Condition1 Value', 'Condition2 Location' (0), and 'Condition2 Value'.

- __f. Use the Parameter Position pane to indicate which stored procedure parameters map to which Guardium application event attributes. The first procedure parameter is numbered 1. Use 0 (zero - the default) for all attributes that are not set by the call.

Application Username Position - Enter the parameter position of the application user name you want associated with database activity from this point forward (until reset, as described previously).

- __g. Enter 1 in Application Username Position for this Lab. This will indicate the first parameter. The *Event Type Position* field has a special use when the Clear action is selected (see below).

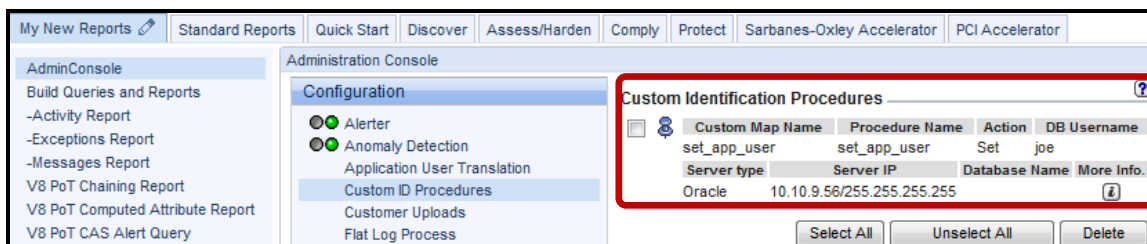
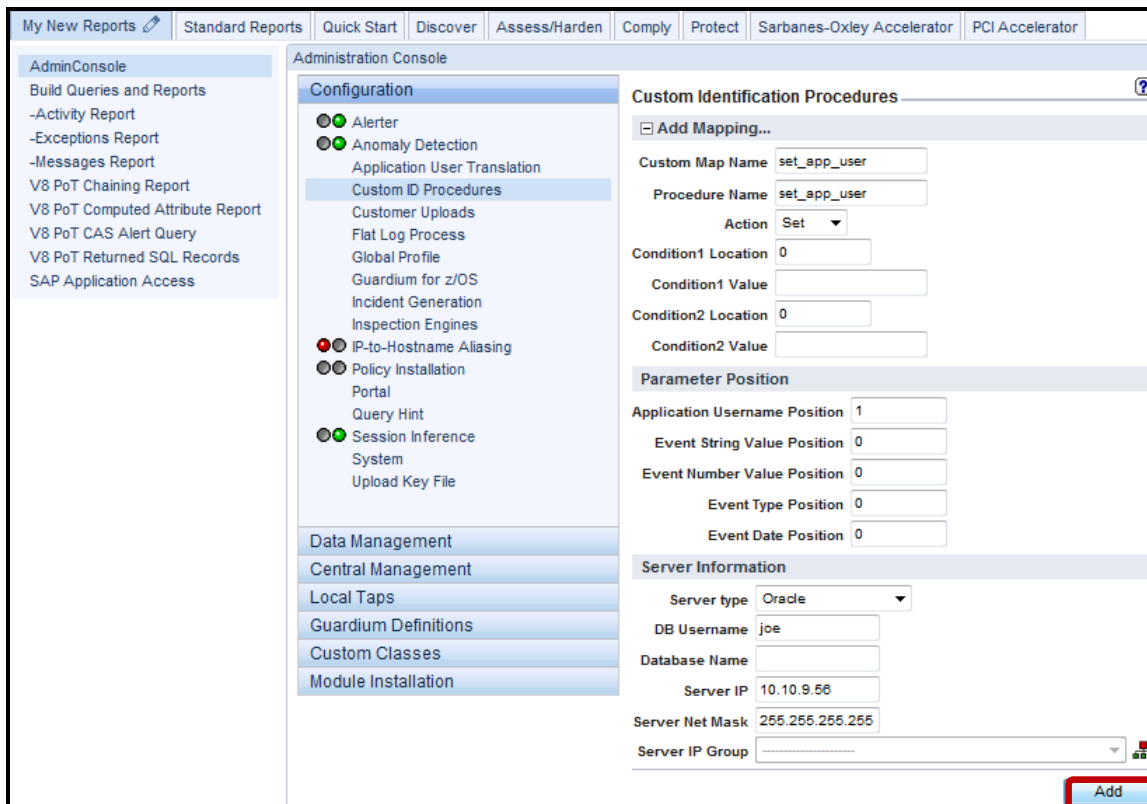
The screenshot shows the 'Parameter Position' configuration window. On the left is a sidebar with options like 'Policy Installation', 'Portal', 'Query Hint', 'Session Inference', 'System', and 'Upload Key File'. The main area is titled 'Parameter Position' and contains several fields. The 'Application Username Position' field is highlighted with a red box and has the value 1. Other fields include 'Event String Value Position' (0), 'Event Number Value Position' (0), 'Event Type Position' (0), and 'Event Date Position' (0).

- __h. In the Server Information pane select Oracle for database server type from the Server type list.
- __i. **DB Username:** Enter 'joe' for the database user name.
Database Name (Optional): Enter a database name in the Database Name box. If omitted, all databases will be monitored. Leave blank for this Lab
- __j. **Server IP (Optional):** Enter '10.10.9.56' for the Server IP to identify one or more servers. If no server is specified, all servers will be monitored.
- __k. **Server Net Mask:** Enter '255.255.255.255' for the server net mask.

To select a specific server only, enter the server IP address and network mask in the Server IP and Server Net Mask boxes; or, to select a group of servers, select a server group from the Server IP Group list or click the Groups button to define a new group of servers.

Central Management	Server Information										
Local Taps	<table border="1"> <tr> <td>Server type</td> <td>Oracle</td> </tr> <tr> <td>DB Username</td> <td>joe</td> </tr> <tr> <td>Database Name</td> <td></td> </tr> <tr> <td>Server IP</td> <td>10.10.9.56</td> </tr> <tr> <td>Server Net Mask</td> <td>255.255.255.255</td> </tr> </table>	Server type	Oracle	DB Username	joe	Database Name		Server IP	10.10.9.56	Server Net Mask	255.255.255.255
Server type	Oracle										
DB Username	joe										
Database Name											
Server IP	10.10.9.56										
Server Net Mask	255.255.255.255										
Guardium Definitions											
Custom Classes											
Module Installation											

- 1. When you are done, click the **Add** button to add the mapping to the list. This mapping will be used for the next steps of this lab.



__m. Click on the **More info.** icon for a listing of parameter settings.

The screenshot displays the Administration Console interface for IBM InfoSphere Guardium V8.2. The left sidebar shows the 'Configuration' menu with 'Custom ID Procedures' selected. The main area is titled 'Custom Identification Procedures' and contains a table of configurations. A 'More info.' icon (a question mark in a circle) is highlighted with a red box. Below the table, there are 'Add Mapping...' and 'Add Mapping...' buttons, and a 'Custom Map Name' field. A yellow callout box is overlaid on the right side of the table, showing the configuration details for the selected row.

Custom Map Name	Procedure Name	Action	DB Username
set_app_user	set_app_user	Set	joe

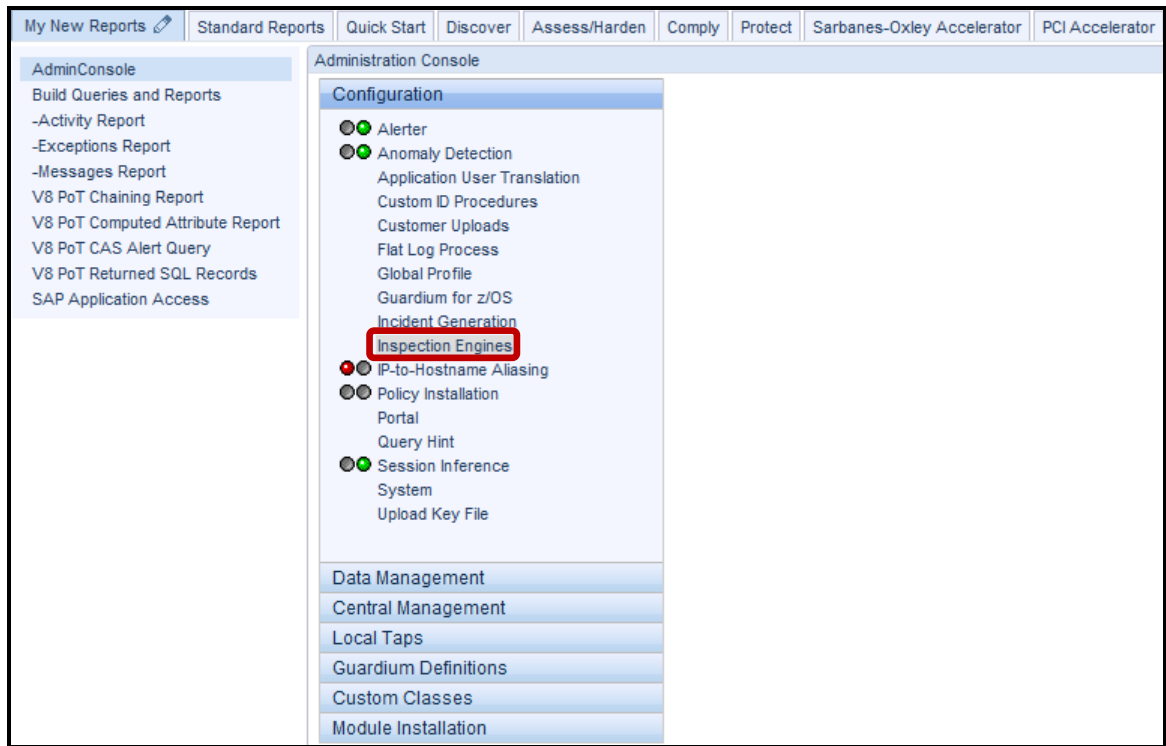
Server type: Oracle Server IP: 10.10.9.56/255.255.255.255 Database Name: **More info.**

Buttons: Select All, Unselect All

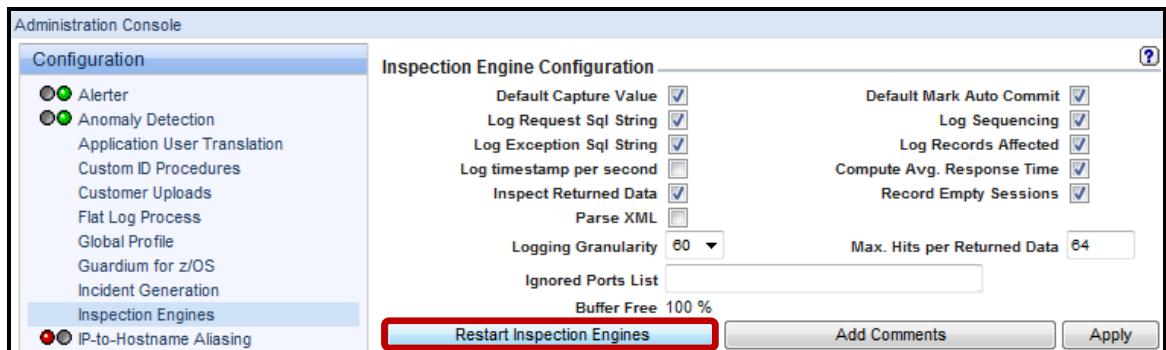
Custom Map Name: set_app_user
Condition1 Location: 0
Condition1 Value:
Condition2 Location: 0
Condition2 Value:
Application Username Position: 1
Event String Value Position: 0
Event Number Value Position: 0
Event Type Position: 0
Event Date Position: 0

__3. Restart inspection engines to activate the new mappings.

__a. Click **Inspection Engines** under the **Administrative Console** tab.



__b. Now click **Restart Inspection Engines** and then click **OK** to acknowledge.



- __4. Now let's validate that everything works. Execute the following steps:
- __a. Putty into database server 10.10.9.56 and login as root/guardium

sqlplus joe/guardium

exec set_app_user('Harry');

select 'joe' from dual;

```
login as: root
root@10.10.9.56's password:
Last login: Wed Dec 14 13:52:10 2011 from jdi
[root@osprey ~]# sqlplus joe/guardium

SQL*Plus: Release 10.2.0.1.0 - Production on Wed Dec 14 13:55:59 2011

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

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

SQL> exec set app user('Harry');

PL/SQL procedure successfully completed.

SQL> select 'joe' from dual;

'JO
---
joe

SQL> █
```

- __b. Click '-Activity Report' under My New Reports -> Build Queries and Reports to view the output.

The screenshot shows the IBM InfoSphere Guardium interface. The top navigation bar includes 'My New Reports', 'Standard Reports', 'Quick Start', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Sarbanes-Oxley Accelerator', and 'PCI Accelerator'. The left sidebar lists various reports, with '-Activity Report' selected. The main content area displays an activity report for the period 2011-12-14 12:58:34 to 2011-12-14 15:58:34. The report includes a table with the following columns: Timestamp, Server Type, Server IP, Client IP, Network Protocol, DB User Name, Application User, and Full Sql. The Application User field is highlighted with 'Harry' and the Full Sql field contains a complex SQL query.

Timestamp	Server Type	Server IP	Client IP	Network Protocol	DB User Name	Application User	Full Sql
2011-12-14 13:57:26.0	ORACLE	10.10.9.56	10.10.9.56	BEQUEATH	JOE	Harry	select 'joe' from dual
2011-12-14 13:56:43.0	ORACLE	10.10.9.56	10.10.9.56	BEQUEATH	JOE	Harry	BEGIN set_app_user('Harry'); END;
2011-12-14 13:56:00.0	ORACLE	10.10.9.56	10.10.9.56	BEQUEATH	JOE		BEGIN DBMS_OUTPUT.DISABLE; END;
2011-12-14 13:56:00.0	ORACLE	10.10.9.56	10.10.9.56	BEQUEATH	JOE		SELECT ATTRIBUTE.SCOPE,NUMERIC.VALUE,CHAR.VALUE,DATE.VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE ((UPPER('SQL*Plus') LIKE UPPER(PRODUCT)) AND (UPPER(USER) LIKE USERID) AND ((UPPER(USER) LIKE USERID) OR (USERID = 'PUBLIC')) AND (UPPER(ATTRIBUTE) = 'ROLES'))
2011-12-14 13:56:00.0	ORACLE	10.10.9.56	10.10.9.56	BEQUEATH	JOE		BEGIN DBMS_APPLICATION_INFO.SET_MODULE(,1,NULL); END;
2011-12-14 13:56:00.0	ORACLE	10.10.9.56	10.10.9.56	BEQUEATH	JOE		BEGIN DBMS_APPLICATION_INFO.SET_MODULE('SQL*Plus',NULL); END;

Note: The *Application User* field now contains 'Harry' and the *Full Sql* field contains the *select* statement.

Thank you

Application End-User Identifier review

- __1. Application user translation is useful in which environment?
- __a. Client/Server architecture
 - __b. Pooled user connections
 - __c. Thick clients
 - __d. A network switch
- __2. Application user translation is available ready for immediate use for all except:
- __a. SAP
 - __b. JD Edwards
 - __c. Microsoft Dynamics GP
 - __d. Siebel
 - __e. Oracle EBS
 - __f. Business Objects - Web Intelligence
 - __g. PeopleSoft
- __3. Application user translation is deterministic (meaning a 100% accurate correlation between users and traffic).
(**True** or **False**)
- __4. Application user translation happens in real time, and can be a condition in policy rules, including alerting and blocking.
(**True** or **False**)
- __5. Which of the following is not a valid method for implementing application user translation?
- __a. ATAP monitors the HTTP traffic, and makes a best guess to correlate this with new session information captured on the database
 - __b. A stored procedure with the application user is called when the user logs in
 - __c. Use Custom GuardAPI SQL to identify the user
 - __d. ATAP captures the application user at login by monitoring the HTTP traffic

Application End-User Identifier review (Answers)

__1. Application user translation is useful in which environment?

B – Pooled user connections.

__2. Application user translation is available out-of-the-box for all except:

C – Microsoft Dynamics GP.

__3. Application user translation is deterministic (meaning a 100% accurate correlation between users and traffic).
(**True or False**)

True.

__4. Application user translation happens in real-time, and can be a condition in policy rules, including alerting and blocking.
(**True or False**)

True.

__5. Which of the following is not a valid method for implementing application user translation?

__a. ATAP monitors the HTTP traffic, and makes a best guess to correlate this with new session information captured on the database

A – ATAP monitors the HTTP traffic, and makes a best guess to correlate this with new session information captured on the database.

Lab 14 Guardium Enterprise Deployment

14.1 Upgrade without Reboot (Flash demo)

Overview

InfoSphere Guardium provides an upgrade utility for both native installations as well as installations performed using the Guardium Installation Manager (GIM) capability. In the case of GIM, every database server can periodically check the Guardium appliance for new version updates. Upon finding a new release the installer agent running on the Guardium appliance (GIM server) shall retrieve the new version of software, either from its local database or by fetching it from a remote Central Manager machine, and sending it to the installer client (GIM Client) on the database server.

InfoSphere Guardium provides the capability to upgrade an S-TAP version across the enterprise without impact to production services. This essential capability automates consistent versions and configurations for all monitored database servers.

Objectives

The included flash demo (2.5 minutes) takes the user through the steps necessary to upgrade an existing version of the InfoSphere Guardium S-TAP agent to a newer release.

Thank you

14.2 S-TAP Failover (Flash demo)

Overview

Redundancy and failover are essential capabilities of an enterprise Database Activity Monitoring solution deployment. IT Infrastructure outages are an inevitable concern that must be accounted for in the initial Database Activity Monitoring deployment architecture. InfoSphere Guardium provides several features that ensure redundancy, and protect against the loss of critical audit data.

Objectives

The included flash demo (10 minutes) will illustrate the built-in mechanisms of the InfoSphere Guardium Database Activity Monitoring solution to ensure the reliable capture and transmission of audit data across the enterprise.

Thank you

14.3 Drilldown Report Controls (Flash demo)

Overview

InfoSphere Guardium's IBM predefined reports are available to the user from the following tabs in the Standard reports panel.

- DB Activities
- Exemptions
- DB Administration
- Schema Changes
- Detailed Activities
- Performance
- DB Exceptions Map

By default each predefined report will have a drill down menu which includes all related reports with run time parameters that can be supplied by attributes from the report given the usual security role restrictions.

Objectives

The included Flash demo will take you through the following steps:

- __1. Access DB Activities predefined report
- __2. Navigate through Drill Down Panels
- __3. Track User Activity
- __4. Verify that Policy is working as planned

Thank you

14.4 GrdAPI Linkage with Database Instance Discovery (Flash demo)

Overview

The GIM Discovery module requires an existing S-TAP installation, and provides the powerful capability to scan and detect multiple, active database instances. The results of these scans can be viewed by the “Database Instances” report. Since, the information gathered by GIM Discovery is sufficient to create an Inspection Engine, the InfoSphere Guardium drilldown feature has been enhanced to enable the results from a Discovery scan to automatically “invoke” the GrdAPI command line interface, and create an Inspection Engine.

One of the key advantages of taking advantage of this capability is that it saves time by eliminating the risk of manual error caused by a typing error or by utilizing bad information that was errantly produced. The end result is that in a matter of minutes, one or many Inspection Engines can be automatically created, and no time is wasted debugging an incorrect parameter on a manually created Inspection Engine.

Note that GIM Discovery has no connection to Database Auto-Discovery (which requires no software).

Objectives

The included flash demo will demonstrate the ease with which the IBM InfoSphere™ Guardium® solution can be deployed in an enterprise environment. We will focus on leveraging capabilities of the IBM InfoSphere Guardium Installation Manager (GIM) Discovery software module to perform automated database instance scans on database servers, and to automate the creation of a DB2 Inspection Engine.

Thank you

14.5 Guardium Alias Reporting (Flash demo)

Overview

An alias is a synonym that substitutes for a stored value of a specific attribute type. It is commonly used to display a meaningful or user-friendly name for a data value. For example, Financial Server might be defined as an alias for IP address 10.10.9.56. Once an alias has been defined, users can display report results, formulate queries, and enter parameter values using the alias instead of the data value. Note, however, that you cannot sort reports on alias values; sorts always use actual data values. There is only one set of aliases. If multiple users define aliases for the same value of an attribute, the most recently defined alias is the one that will be seen by all users.

Objectives

The included Flash demo will demonstrate how to enhance a Customer Report with more user-friendly Aliases. In doing so, it will first illustrate how to turn on the alias feature as well as accessing the alias drill down from an existing custom report. From there it will take you through the steps for creating an alias for a respective field name. Finally, the demo will show how you can switch back and forth between alias and non-alias reporting.

Thank you

14.6 Configuring Query-Based Tests (Flash demo)

Overview

Query based tests are user-defined tests that can be quickly and easily created by defining or modifying a SQL query to be run against a database datasource. The results of the query are then compared to a predefined test value enabling the user to check items such as database internals, structures, parameters, and even application data.

There are likely to be situations where a more specific or additional test may be required within the scope of a Vulnerability Assessment instance. IBM InfoSphere™ Guardium® offers the ability to create a Query-based Test in order to meet these unique requirements.

Objectives

The included Flash demo will illustrate how we can create a new Query-based test using the IBM InfoSphere™ Guardium® GUI. The following objectives will be targeted.

- __1. Accessing Query-based Test Builder
- __2. Build a Query-based test
- __3. Include the new test in a Test Configuration
- __4. Run a Vulnerability Assessment with a newly defined test
- __5. Verify a Successful Test Result

Thank you

14.7 Configuring Exception Tests (Flash demo)

Overview

There are likely to be situations where a more flexible test criterion is desired. IBM InfoSphere™ Guardium® offers the ability to create a VA Exception Tests in order to meet these unique requirements.

For example, a test ID that requires DB2 dbadm may get flagged and cause the test to fail despite the administrator's knowledge and acceptance. In such a case, the administrator may add an exception to the test criteria so that the flagging will be ignored instead of causing the test to fail.

Objectives

The included Flash demo will take you through the necessary steps for creating a new VA Test Exception

- __1. Accessing Test Exception Builder
- __2. Build a new VA Test Exception
- __3. Implement a Test Exception
- __4. Test the new Test Exception

Thank you

14.8 Application End-User Identifier (Flash demo)

Overview

InfoSphere Guardium Application End-User Identifier provides a packaged solution that addresses security and compliance requirements for the data managed by major enterprise applications—without requiring changes to existing business processes or application source code. These applications include:

- Oracle E-Business Suite
- SAP ERP and NetWeaver BW
- PeopleSoft
- IBM Cognos
- Siebel
- Business Objects Web Intelligence

The InfoSphere Guardium solution provides granular, preconfigured policies for SAP and Oracle EBS applications to rapidly identify suspicious or unauthorized activities, such as changes to sensitive objects or multiple failed logins. Sensitive objects, which can require significant research to locate, are identified through the Guardium Knowledgebase service to facilitate the development of custom policies.

The InfoSphere Guardium solution also identifies application user IDs for custom and packaged applications built upon standard application-server platforms, such as: IBM WebSphere®, BEA WebLogic, Oracle Application Server or JBoss Enterprise Application Platform

Objectives

The included Flash demo will give an overview of Application User Translation and the different approaches available for determining a specific user from a pooled connection. This lab will concentrate on SAP Applications illustrating the difference between ABAP and JAVA Stacks as well as determining which SAP kernel is installed and why it matters. This lab will discuss the different requirements and approaches for SAP Application User Translation keying on the following topics:

- __1. Application User Translation Methods
- __2. Verifying SAP Kernel for ABAP and JAVA Stacks
- __3. Logging Activation
- __4. Populate Pre-Defined Application Groups
- __5. Application End User Configuration (SAP-DB)
- __6. Application End User Configuration (SAP-Observed)
- __7. Create/Run Reports

Thank you

Lab 15 Frequently asked questions

Overview

This lab is not interactive, due to the in-depth nature of these topics. This is designed as discussion and reference material. The concept is to address some common issues and easy ways to resolve them.

Objectives

This lab will document steps to help diagnose various issues.

- __1. Diagnose blank or questionable reports
- __2. Diagnose S-TAP communication problems
- __3. Diagnose S-TAP capture
- __4. Diagnose S-GATE issues
- __5. Diagnose policy issues
- __6. Diagnose network capture issues
- __7. Diagnose collector performance

15.1 Diagnose empty or questionable reports

- __1. Guardium reports usually contain no data, or unexpected results because of the following:
 - __a. Time differences
 - __i. When using network monitoring (SPAN ports), the time assigned to the traffic is from the collector. When capturing from S-TAP, the time is from the database server. This means that if there is a time discrepancy between the collector and the database server, then "No -1 hour" to "Now" may not return current data. This will also happen if one is marked as a different time zone.
 - __ii. If there is a time issue, the easiest way to resolve this is to put a wide date/time range (e.g. "Now -2 week " to "Now +2 week"). If a large amount of data is displayed, then you can filter by other fields (for example, client IP, Database User).
 - __b. Groups
 - __i. Group conditions for a query may point to blank groups. This is common with the PCI and SOX Accelerators, for example, where they need the appropriate groups populated. The solution is to view the underlying query and understand the conditions for the report (third from right icon at bottom).
 - __c. Errors when viewing reports
 - __i. When working with a Query, the Regenerate button is only needed when changing the runtime parameters. This is because the parameter page where the user can change these when viewing the report is fixed. If viewing a report where the runtime parameters have changed but the report has not been regenerated, an error will be displayed.
 - __d. SQL not captured as expected
 - __i. If your report includes any of the fields from the Full SQL (or Full SQL Values, although this is rarely used) table, you must have the correct policy rule in place to capture this. For Full SQL, you will need the "Log Full Details" action on a rule applying to the traffic you want to see.
 - __ii. By default, we capture all database traffic at the SQL construct level (not the values in the SQL statement). If you install a policy of type "Selective audit trail," then by default no traffic is captured except what you explicitly create rules to capture.

15.2 Diagnose S-TAP communication issues

- __1. The Guardium S-TAP agent has various communication points; here are some general steps to understand how this works and where it can go wrong.
 - __a. Summary - there are three key places that this will normally fail:
 - __i. At S-TAP install, the S-TAP host or Guardium collector IP is entered wrong
 - __ii. There is a firewall involved (at network or on db server) that is blocking the traffic
 - __iii. There is something wrong with the Inspection Engine parameters
 - __b. General flow
 - __i. Install S-TAP on the database server, specifying the database server IP and the Guardium Collector IP. Hostnames are not recommended and will probably cause issues.
Result: The agent will then start communicating with the Collector, sending information about its host, and the IP that the Collector should use to communicate back. The entry will show up on the Collector as green.
 - __ii. Issues:
 - (1) If the Collector IP is wrong, the S-TAP entry will not show up. Try doing a ping on the db server to test the connection.
 - (2) If there is a firewall issue between the database and the Collector, the S-TAP entry will not show up. Try doing a "telnet [Collector IP] 16016" (or 8075 and 9500 on Windows) on the database server to test the connection.
 - __iii. Add an Inspection Engine on the Collector for monitoring a database.
Result: The Collector will initiate communication with the S-TAP (this is one of the few times communication is initiated by the Collector), sending the Inspection Engine information. The S-TAP will 1) take the existing guard_tap.ini, and write it as guard_tap.ini.bak, 2) apply the changes to the guard_tap.ini, 3) restart. If there is an issue with the changes, then the S-TAP will take the existing guard_tap.ini, rename it to guard_tap.ini.err, rename the guard_tap.ini.bak to guard_tap.ini, and restart.
If the changes are successfully applied, then the status on the Collector will go to green after a few seconds, if there is an error, then it will be yellow (indicating a discrepancy between what the Collector thinks should be set, and what S-TAP is reporting).

__iv. Issues:

- (1) If the S-TAP host IP is wrong (set when installing the S-TAP), then the Collector will not be able to communicate with the S-TAP. Try doing a ping on the Collector (under cli user) to the database server to test the connection.
- (2) If there is a firewall issue between the Collector and the database (firewalls allow blocking in one direction), the S-TAP agent will not receive any communication (so no guard_tap.ini.err or guard_tap.ini.bak file will be created). Try doing a ping (telnet is not available) on the Collector (under cli user) to the database server to test the connection. In some cases it may be possible to configure a test system to replace the collector (your laptop?) that you can replace the Collector with and try the telnet command on that system.
- (3) If there is an issue with the Inspection Engine parameters (for example, Process Name invalid), then there will be a guard_tap.ini.err file, Follow the instructions in the help documents to correct this.

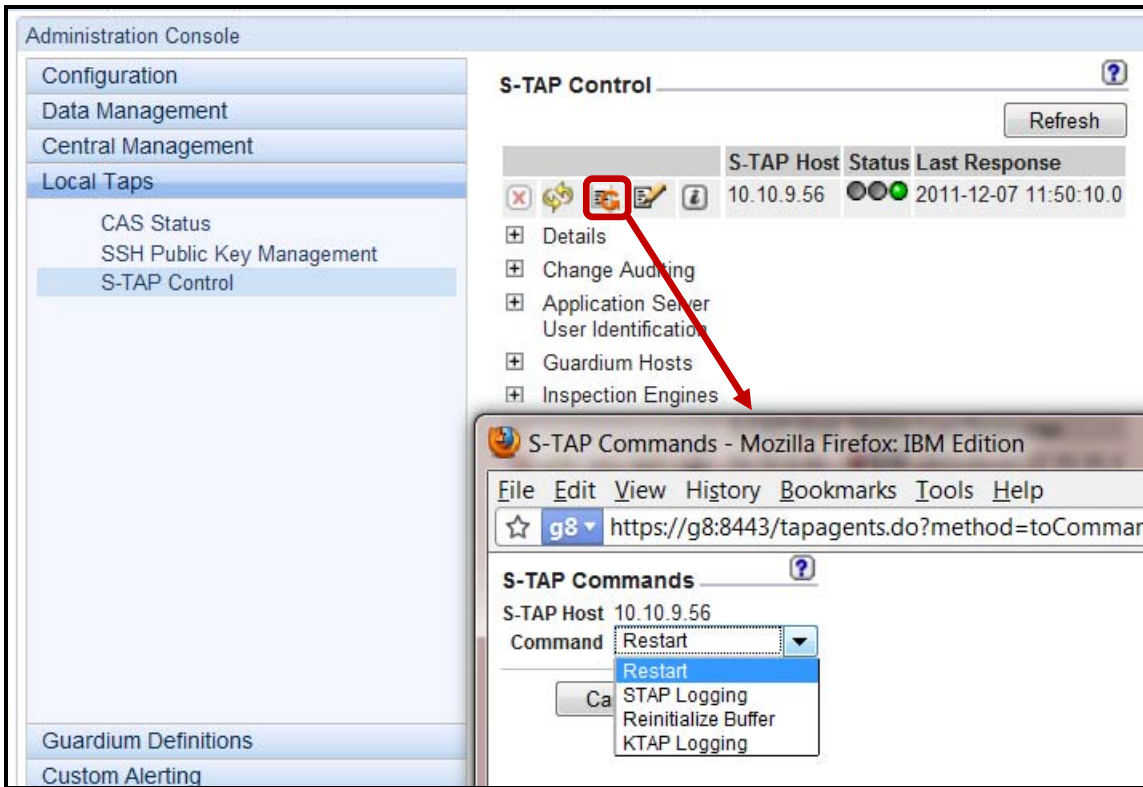
__2. You can see the S-TAP log information from the Collector.

The screenshot shows the Administration Console interface. On the left is a navigation menu with options like Configuration, Data Management, Central Management, Local Taps, CAS Status, SSH Public Key Management, S-TAP Control, Guardium Definitions, and Custom Alerting. The main area is titled 'S-TAP Control' and contains a table with columns 'S-TAP Host', 'Status', and 'Last Response'. A red box highlights an information icon in the first row, which points to a browser window titled 'S-TAP Events - Mozilla Firefox: IBM Edition'. The browser window shows a table of S-TAP Events with columns 'Event Type', 'Event Description', and 'Timestamp'.

S-TAP Host	Status	Last Response
10.10.9.56	●●●	2011-12-07 11:50:10.0

Event Type	Event Description	Timestamp
NOTICE	Server 10.10.9.248 wasnt heard from for 60 sec, closing and re-opening	2011-12-07 11:42:21.0
LOG_ERR	Connected to Primary Server 10.10.9.248	2011-12-07 11:42:21.0

__3. You can put S-TAP in debug mode from the collector, starting with version 8.



15.3 Diagnose S-TAP capture issues

There are a variety of tools to analyze the traffic; a few are listed here.

- __1. Put S-TAP in debug mode. This will generate traffic showing each packet sent to the collector. This is useful for seeing that the traffic is being captured.
- __2. Use Tcpcmdump to show network activity on the Collector. This is accessed under a cli user, using the diag command.
This is useful to see what kind of network traffic the Collector is seeing (useful for SPAN/Mirror ports).
- __3. Use SLON to capture details about what traffic is sent to the Collector. This is accessed under a cli user, using the diag command.
This is useful to see exactly what is sent to the Collector.
- __4. Very occasionally, there are different SQL formats that we have not seen before — normally due to a very old client. In this case, we may have trouble parsing the SQL. This can be captured and reported on using the cli command "store log sql parser_errors [on|off]." See the help system for further details.

15.4 Diagnose S-GATE issues

- __1. Verify that **firewall_installed=1** in the guard_tap.ini file.
- __2. Verify that the S-GATE Attach Policy Rule is being called (add a "Log Only" action to this rule), or verify that **firewall_default_state=1** in the guard_tap.ini file. To be safe, allow a 5-10 second gap before executing the SQL to block if not using **firewall_default_state=1**.
- __3. Verify that the S-GATE Terminate Policy is being called — look in the Policy Violations report
- __4. Add to the Policy Rule the action "Quarantine," to lock out the user, some client will automatically try to reconnect.
- __5. If advanced debugging is needed, then the S-TAP debug can be set to see the S-Gate processing.

15.5 Diagnose Policy issues

- __1. Install the Policy! A common mistake for people new to the system is to change a policy but to forget to install it.
- __2. Make sure previous rules that could match have "Continue to next rule" checked. If any doubt, move the rule to the top of the list.
- __3. Build a report to show all the fields that are conditions on your policy rule, verify each field in the report for current traffic (for example, IP may be different than expected).
- __4. Build a new policy with only the rule to test.
- __5. Verify each of the Groups that the rule uses.

15.6 Diagnose network capture issues

- __1. Traffic that is captured from a switch, using a SPAN/Mirror port, is not a confirmed traffic stream. The switch will forward this traffic, but if there is any issue, or the switch is extremely busy, then individual packets can be lost.
 - __a. Review the Dropped Requests report (admin user, Daily Monitor). This should normally be empty, but if there are entries it may indicate a network or switch capacity issue.

15.7 Diagnose collector performance issues

1. Monitor the amount of disk space used. This can be done visually using the System View tab under the admin user. This is also on the Buffer Usage report, and if it exceeds 50% an email is sent to the admin user if configured.

The screenshot displays the S-TAP Status Monitor interface. At the top, there are navigation tabs: System View, Administration Console, Tools, Daily Monitor, Guardium Monitor, Tap Monitor, Incident Management, and My New Reports. Below the tabs, the title is 'S-TAP Status Monitor' with a sub-header 'Aliases: ON'. A table lists several S-TAP instances with columns for Host, Version, DB Server Type, Status, Last Response, Primary Host Name, and various configuration options like KTAP, TEE, MSS Shm, Win DB2 Shm, Win Local TCP, Pipes, Encrypted?, and Firewall Installed. All instances shown are 'Inactive'.

Below the table is a 'Records' section showing '1 to 5 of 5' records. Underneath is the 'Current Status Monitor' dashboard. It features a system metrics table:

procs			memory			swap		io		system			cpu			
r	b	swpd	free	buff	cache	si	so	bi	bo	in	cs	us	sy	id	wa	st
0	0	738200	28996	16800	53320	0	0	0	0	706	62	0	0	100	0	0

Below the metrics table, there are several service status indicators with arrows pointing to a central 'Analysis Engine' box. The services shown are SQL Server, Teradata, Oracle, MySQL, DB2, XML, Sybase, and IMS. All these services show '0' for both active and inactive counts. A 'Net Inspection' icon is also present. A prominent warning icon on the right indicates 'Free Disk: 23GB' and 'DB 1% Full'.

- __2. The Collector has a key component called the Sniffer process that receives the traffic. If the system is overloaded, and continually getting more traffic than it can handle for a period, then eventually the queue for this process will fill up. At that point, the Sniffer process will restart, which flushes the queue. One of the key indicators for exceeding Collector capacity is if the Sniffer process is restarting.

Timestamp	% CPU Sniffer	% Mem Sniffer	% CPU Mysql	% Mem Mysql	Sniffer Process ID	Mem Sniffer	Time Sniffer	Free Buffer Space	Analyzer Rate	Logger Rate	Analyzer Queue Length	Analyzer Total	Logger Queue Length	Logger Total
2011-12-07 11:36:13.0	0	5	0	8	3599	872052	1207:113610	100	0	0	0	0	0	0
2011-12-07 11:35:09.0	0	5	0	8	3599	872052	1207:113506	100	0	0	0	0	0	0
2011-12-07 11:34:05.0	0	5	0	8	3599	872052	1207:113403	100	0	0	0	0	0	0

- __3. Check the number of violations that the system is processing. To do this, create a report that shows the Server IP, the violation name and a count. You may put a threshold alert if this exceeds a reasonable limit (for example, 100 per hour).

-Violation Counts

Main Entity: Policy Rule Violation Add Count Add Distinct Sort by count

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/> 1	Policy Rule Violation	Access Rule Description	Value	<input type="checkbox"/>		
<input type="checkbox"/> 2	Client/Server	Server IP	Value	<input type="checkbox"/>		

AND OR HAVING

	Entity	Agg.	Attribute	Operator	Runtime Param.
<input type="checkbox"/>	WHERE	Client/Server	-----	Server IP	LIKE Parameter ServerIP
<input type="checkbox"/>	AND	Client/Server	-----	DB User Name	LIKE Parameter DBuser

- __4. Review the amount of Full SQL that is captured, and try to limit this where possible, as it will fill up the system much more quickly.

Thank you

Appendix A. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have

been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental. All references to fictitious companies or individuals are used for illustration purposes only.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Appendix B. Trademarks and copyrights

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM	AIX	CICS	ClearCase	ClearQuest	Cloudscape
Cube Views	DB2	developerWorks	DRDA	IMS	IMS/ESA
Informix	Lotus	Lotus Workflow	MQSeries	OmniFind	
Rational	Redbooks	Red Brick	RequisitePro	System i	
System z	Tivoli	WebSphere	Workplace	System p	

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.



© Copyright IBM Corporation 2012.

The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. This information is based on current IBM product plans and strategy, which are subject to change by IBM without notice. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way.

IBM, the IBM logo, ibm.com, AIX, Cognos, DB2, Guardium, Informix, InfoSphere, RACF, the Smarter Planet icon, System z, Tivoli, WebSphere, z/OS and z10 are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

Other company, product and service names may be trademarks or service marks of others.



Please Recycle
