CT UNIVERSITY

BIG DATA SECURITY LAB

(CSE414-22)

PRACTICAL FILE

SUBMITTED TO:

MR. OMKANT SHARMA

SUBMITTED BY:

NAME: SIMRAN JAWLA

ROLL NO.: 72212075

CLASS: B.TECH 4rd SEM SEC-B

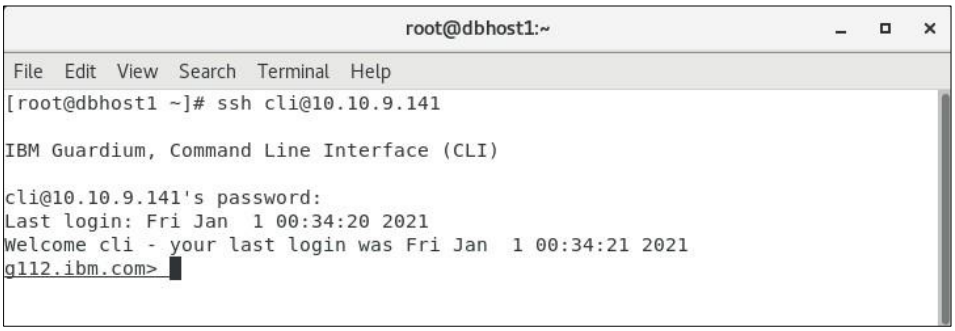
Index

Practical -1

Task 1: Access the command interface and run CLI commands

You use CLI commands to manage Guardium infrastructure. Most Guardium CLI commands consist of a command word followed by one or more arguments. The argument might be a keyword, or a keyword followed by a variable value. Commands and keywords are not case-sensitive, but element names are.

1. Access the Guardium Server.
   a. Start a terminal window on the database server.
   b. Use the command ssh cli@10.10.9.141 to log in to the Guardium server with user **cli,** authenticating with password **guardium** to gain access to



   the CLI command prompt.
2. The prompt is made up of the machine hostname and domain name, which were configured when Guardium was installed. You can inspect these directly by entering the following CLI commands. To view the results, press Enter at the end of each command.
   show system hostname show
   system domain

   show network interface all

   You can also abbreviate Guardium CLI commands, usually to a minimum of three characters to ensure no ambiguity. For example, you can abbreviate the command this way:

   sho net int all

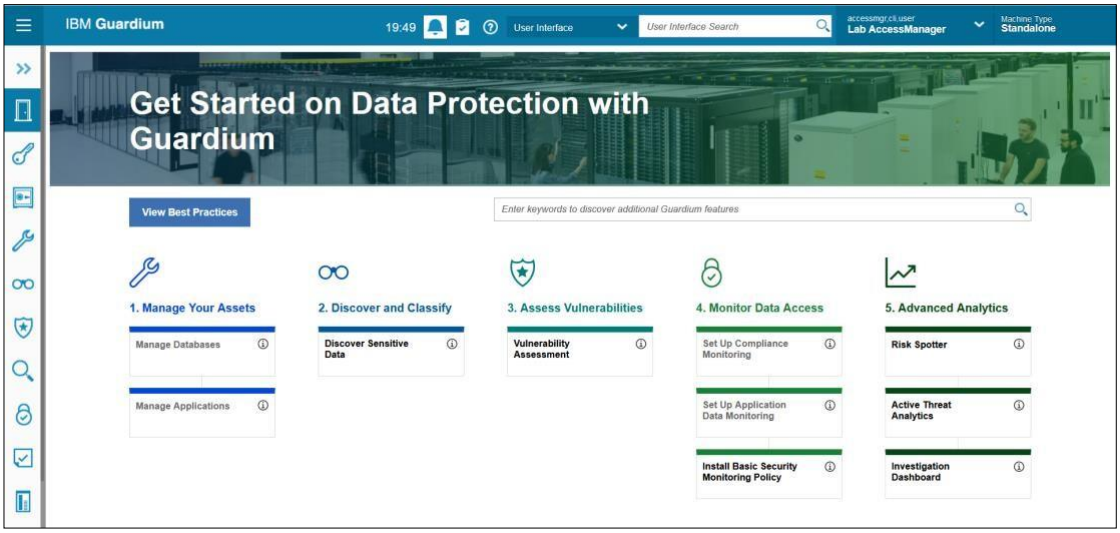
3. If you cannot remember all the command arguments, the Guardium CLI can list them for you. Enter show ? to see all the possible arguments that can follow the show command.
4. Similarly, show network ? lists the possible arguments that can follow the show network command.
5. To list all possible commands, enter ? at the CLI prompt

Practical -2

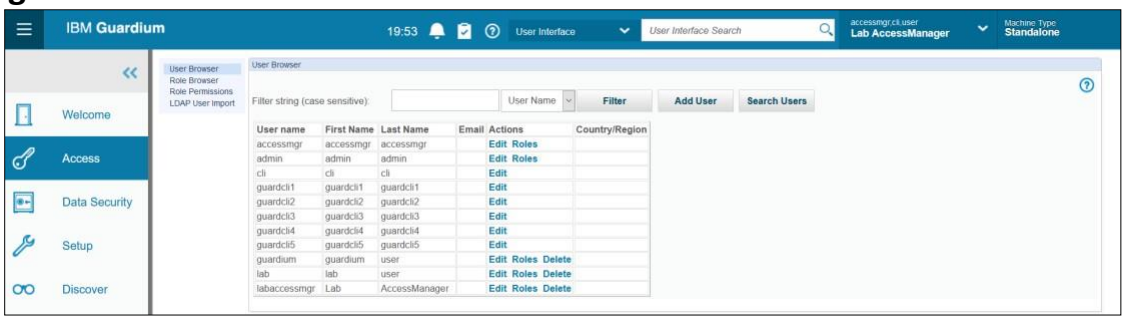
Task 2: Access Management

Exercise1: Creating Guardium Users

1. On the database server, start the Firefox web browser and go to *https://10.10.9.141:8443.*
2. Log in with username ***labaccessmgr*** and password ***guardium*.**The Guardium console opens.

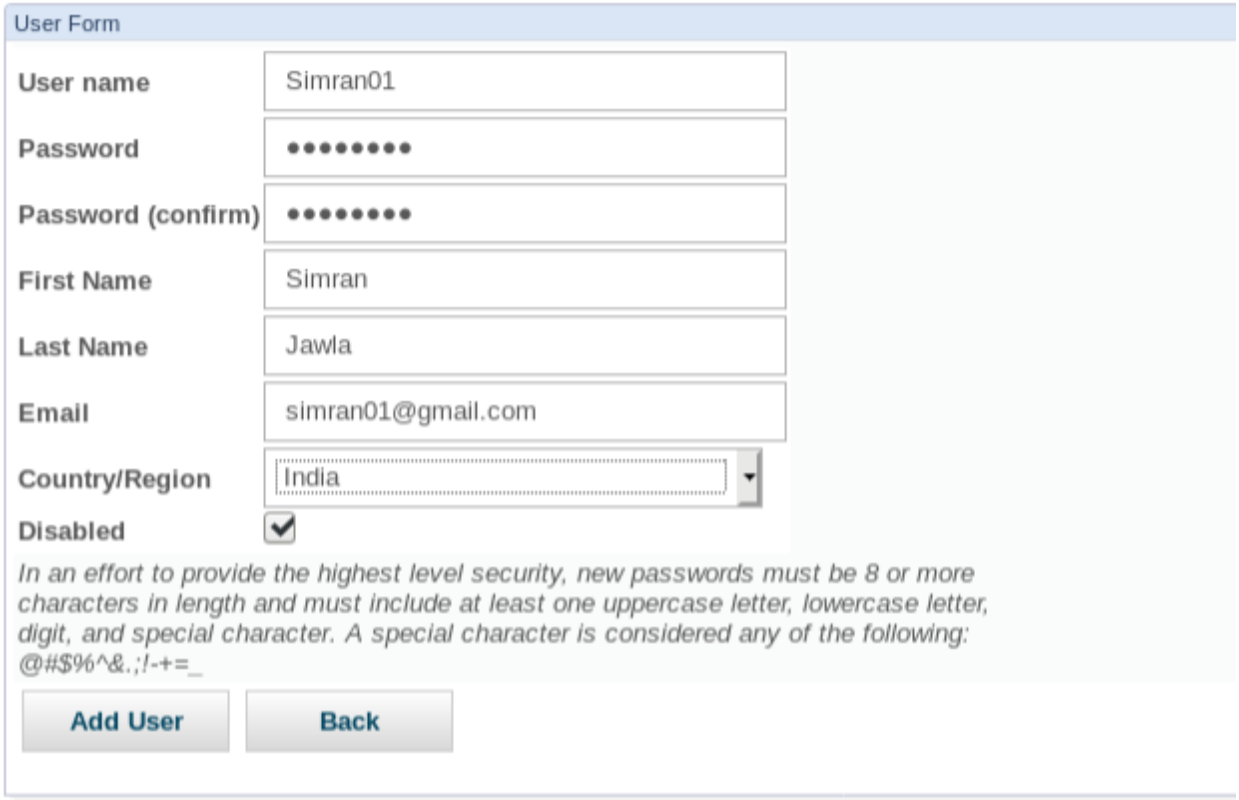


3. In the navigation menu on the left, click **Access** **> Access Management**.

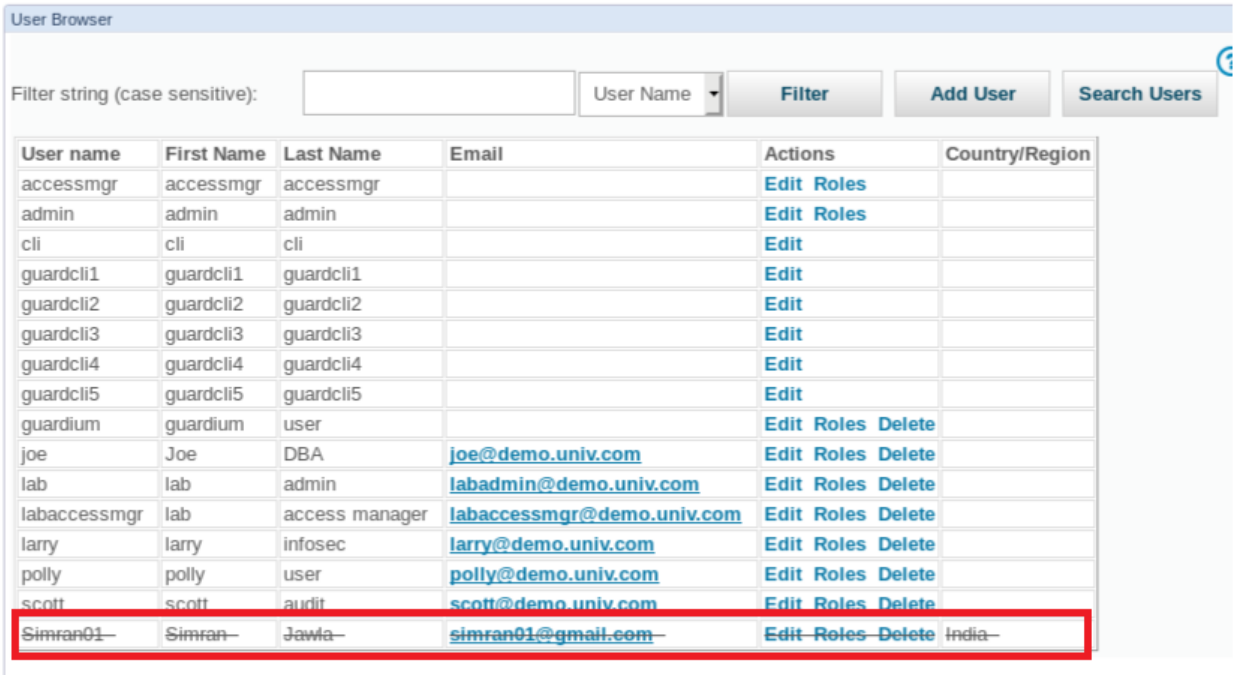


4. To add a new user, click **Add User**, then enter the following information:

- Username: User01
- Password: guardium
- First Name: Simran
- Last Name: Jawla
- Email:simran01@gmail.com
- Disabled check box: not selected

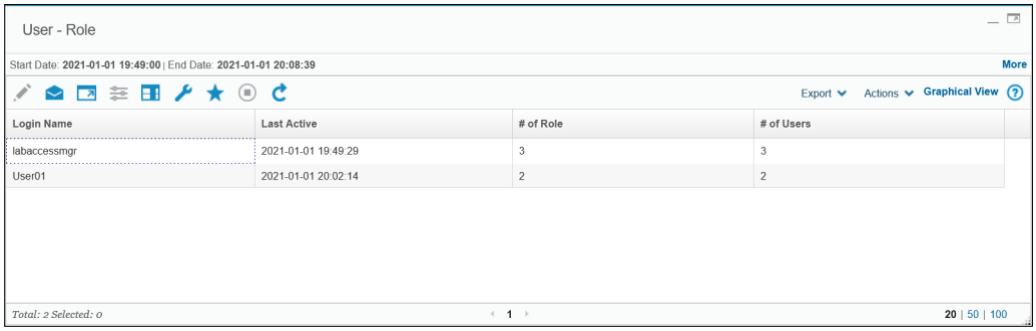


5. Click **Add User**, The user browser displays the new user.



6. For User01, click the **Roles** link.
7. To add users to the infosec role, select the appropriate checkbox. Scroll down and click **Save**.

8. To display summary information about user and role memberships, click **Access > User & Role Reports** from the navigation menu on the left side of the window.



9. To display summary information about user and role memberships, click **Access > User & Role Reports** from the navigation menu on the left side of the window.

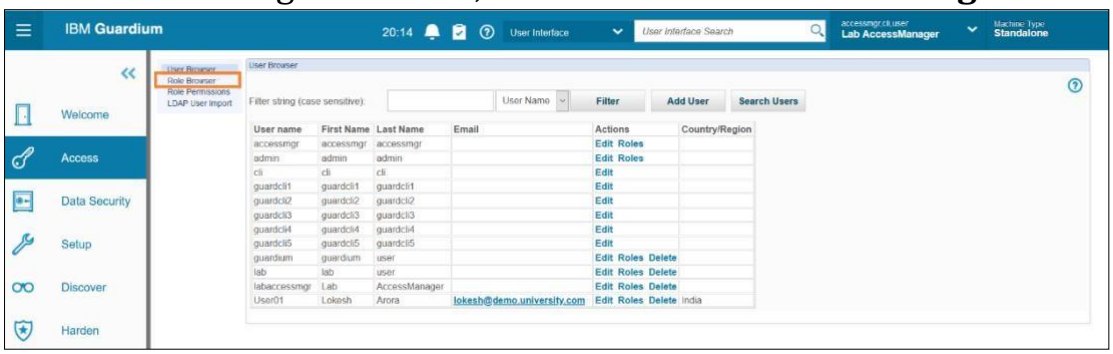
10. To display a report with the user roles, right-click the user that you created and select **Record Details**.

11. Close the window and go back to the GUI.

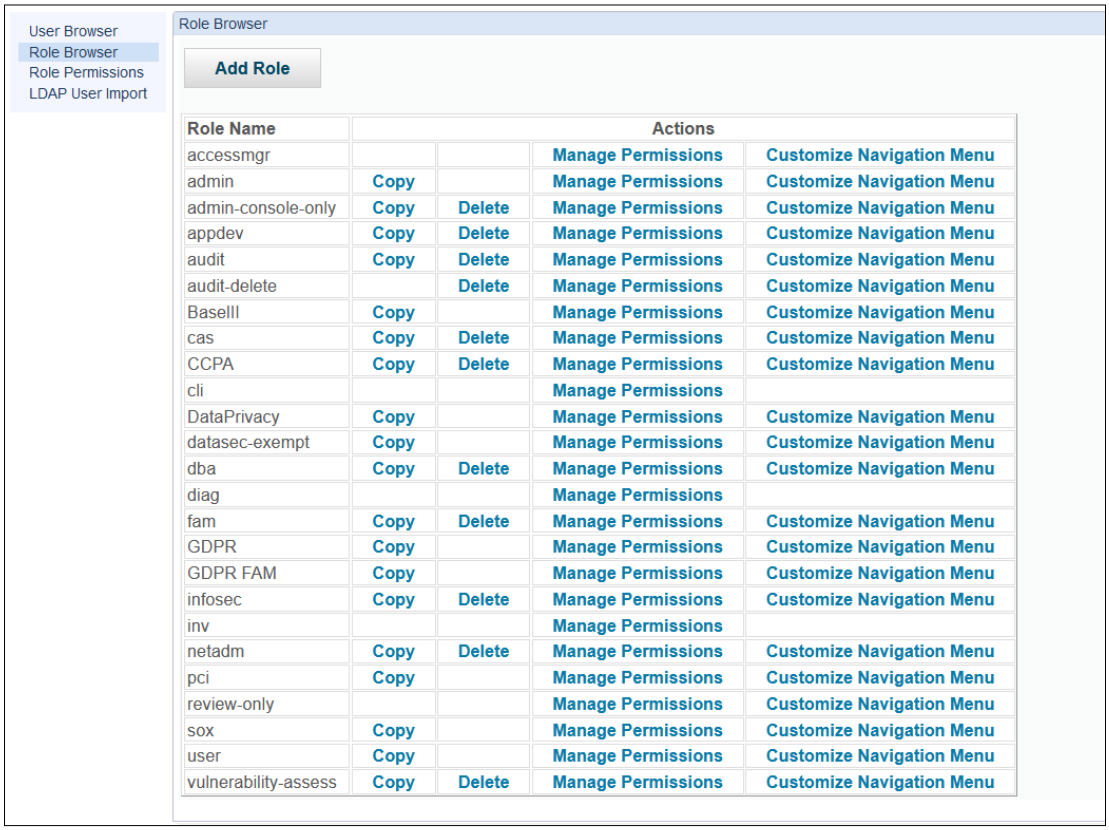
Exercise2: Creating Guardium Roles

In this exercise, you create a role, then you set the access permissions for therole.

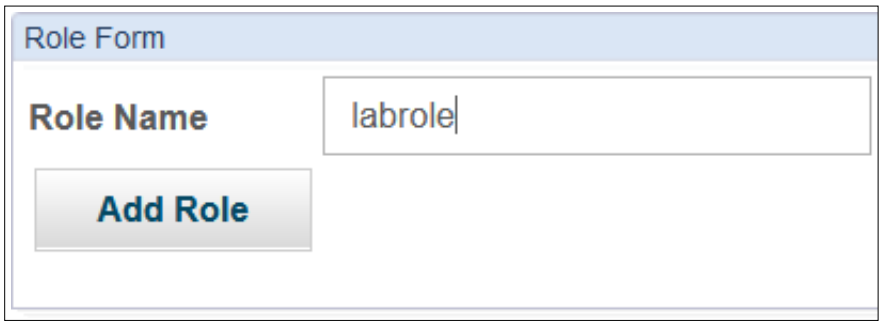
1. In the left navigation menu, select **Access > Access Management**.



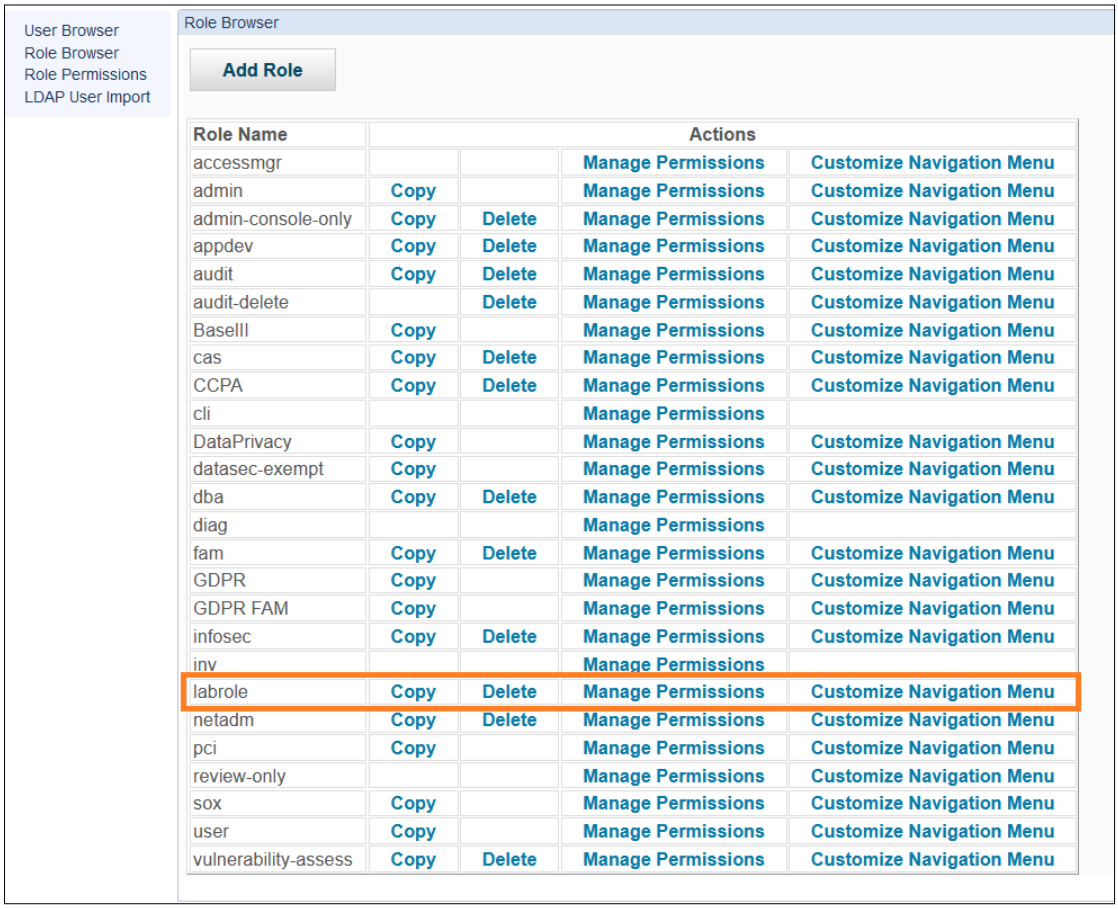
2. Select **Role Browser**. The Role Browser window opens.



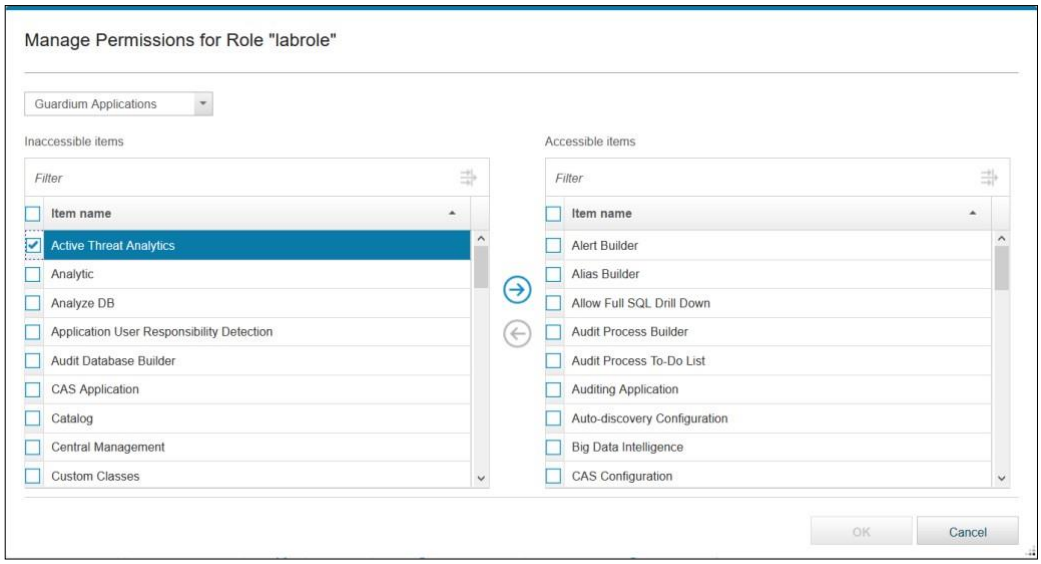
3. Click **Add Role**. The Role Form window opens.
4. Enter the Role Name *labrole* and click **Add Role**.



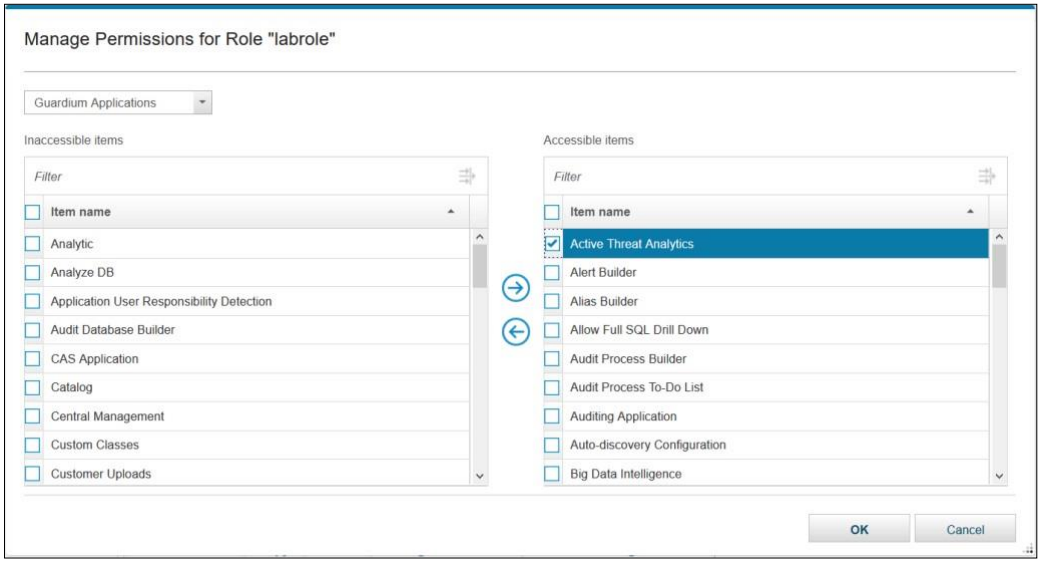
5. You see the new role in the Role Browser. For "*labrole*", click **ManagePermissions**.



6. The Manage Permissions for Role “labrole” window opens.
7. Add the Active Threat Analytics Application to the new role.
   a. In the Inaccessible items list, search for and select **Active ThreatAnalytics**.



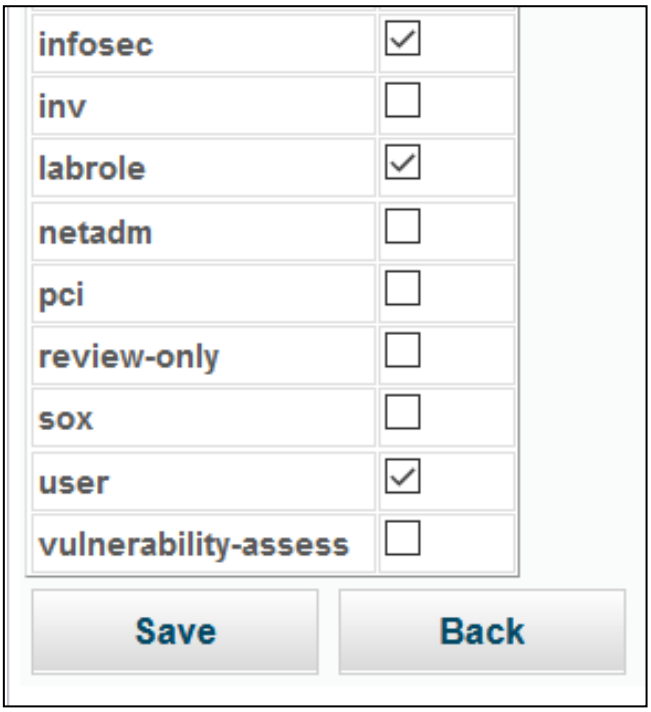
   b. To move Active Threat Analytics to the Accessible items list, click the **Right arrow** icon .



c. Click **OK** and clock the confirmation message.

8. Add your role to a user.
   a. Go to the user browser
   b. Click **Roles** for User01, from the previous exercise.

c. You see **labrole** is available to add as a role.



   d. Select the **labrole** role.
   e. Click **Save**.

9. **Sign out** of the Guardium Console.

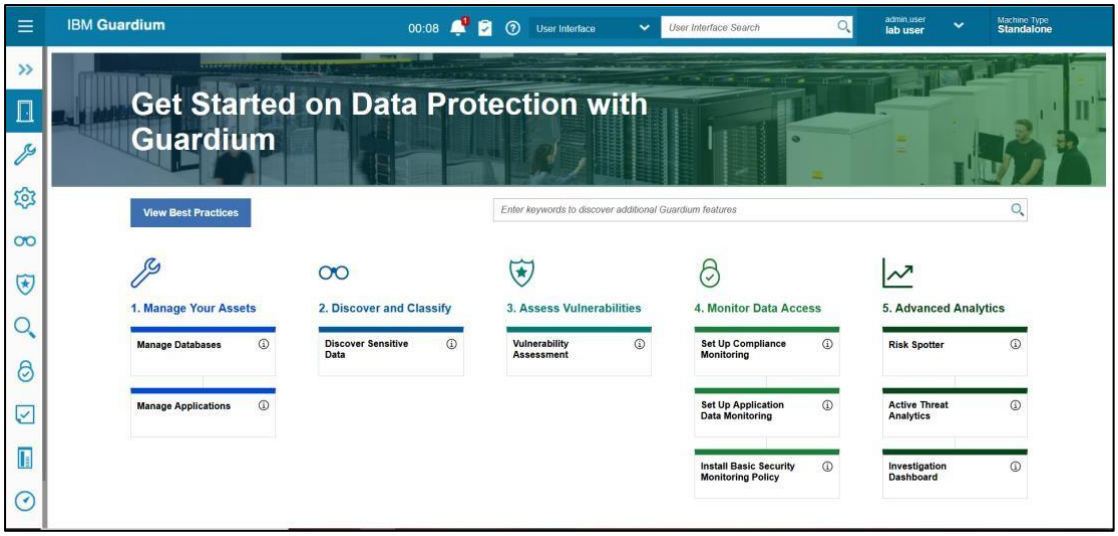
Practical -3

Task 3: POPULATING GROUPS

Exercise1: Creating and populating Guardium Groups

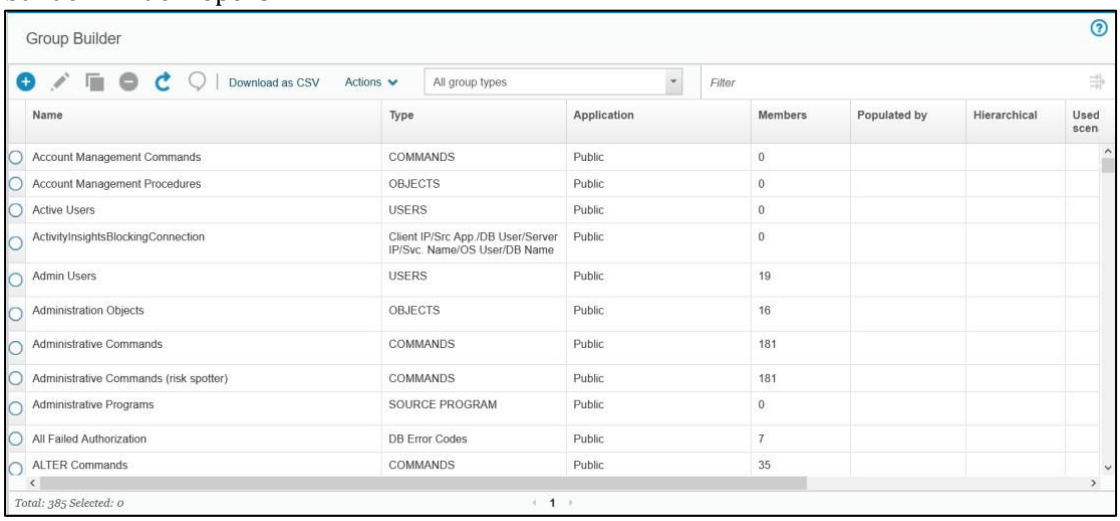
ollow these instructions to perform the exercise.

1. On the database server, start the web browser and log in to the Guardium Console as a user ***lab*** with the password ***guardin*.**



2. In the navigation menu on the eft side of the page, go to **Setup > Tools and Views > Group Builder**.

The Group builder window opens.

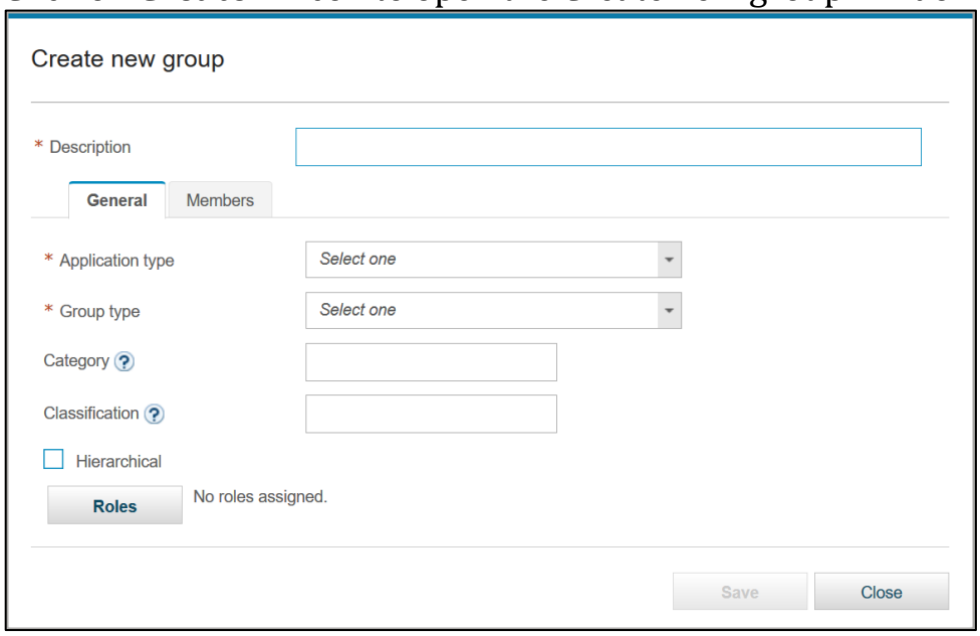


3. The Group Builder window shows the following features:
   - A header, with icons to create , edit , clone , and delete groups, and an icon to refresh the view
   - A button to download the list of groups as a CSV file
   - An actions menu

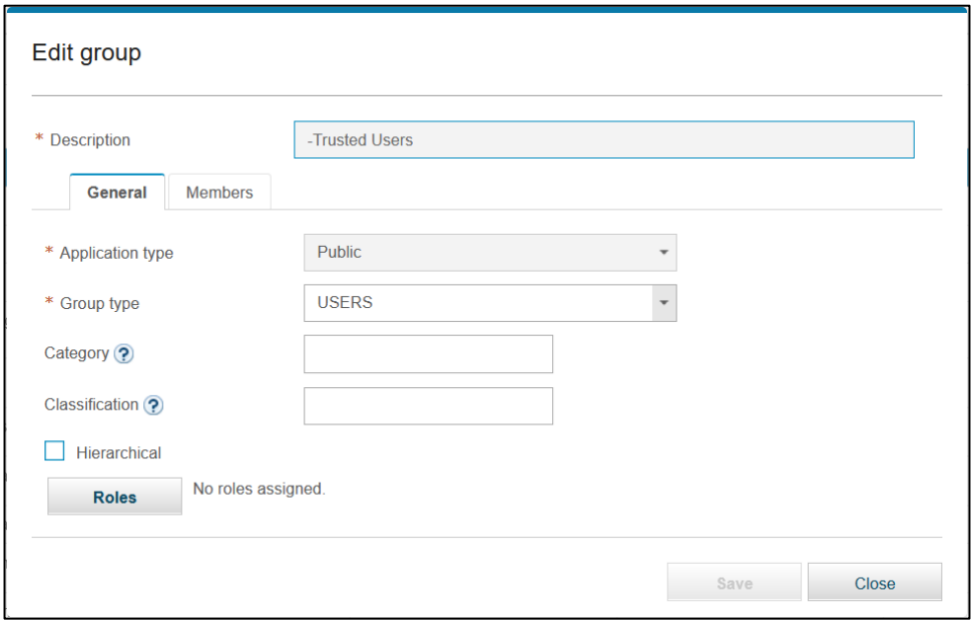
- Methods to filter the group by type or name
- Column headings that describe the group:
- Group name.
- Type of group. In the screen capture, you see the following types of groups:
  Objects: Correspond to tables.

Commands: Refer to SQL or other commands that might be used to manage databases.
Users: Refer to database, application, or operating system users.

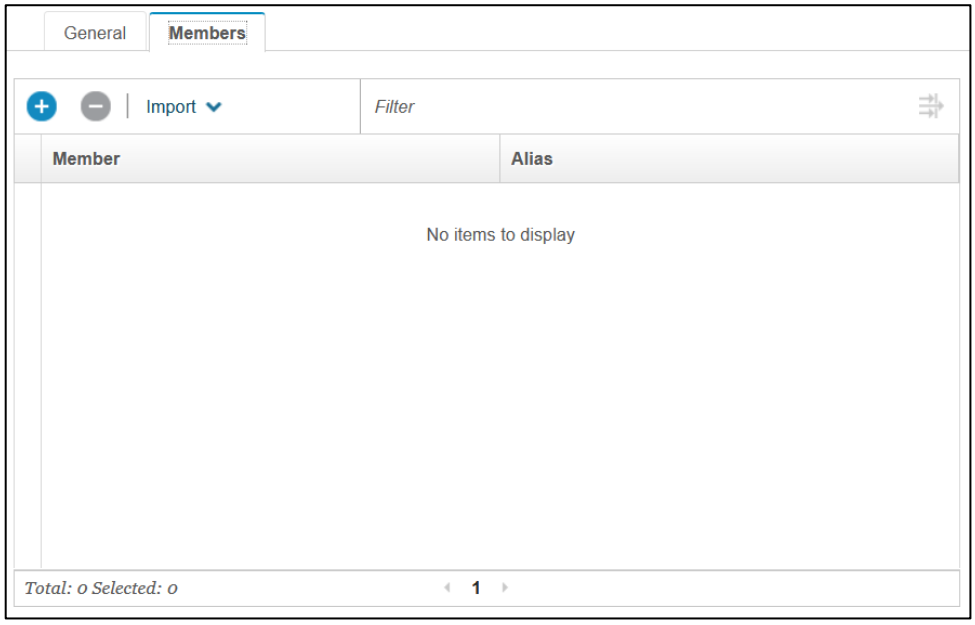
4. There are already many preconfigured groups, you can manage the membership of one of these groups, but we will create a new group in this exercise. One useful group to create is a list of database users that you trust. This might include applications that use the database. You can use this list to write a policy that ignores sessions that are created by these users, which reduces the processing load on the network and the Guardium server.
   a. Click on **Create** icon to open the Create new group window.



   b. In the **General** tab, complete the fields as follow:
      i. **Description**: -Trusted Users
      ii. **Application Type**: Public
      iii. **Group Type**: USERS
      iv. **Category** and **Classification**: Leave blank
      v. **Hierarchical**: not selected
      vi. Click **Save** and close the confirmation message.



c. You have a new group with no members. To add members to the group, click the **Members** Tab.



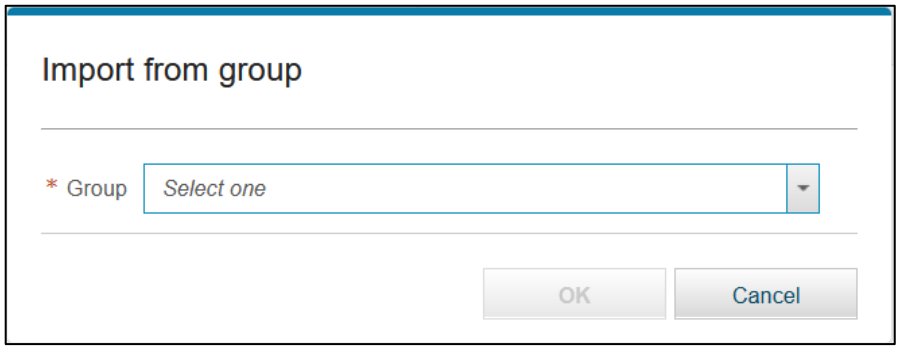
d. To examine the options, click the **Import**  menu. The options include:

   i. From CSV: You can import group members from a simple file.
   ii. From Group: This option adds members from another group.
   iii. From and External datasource: This option adds members from an external database table
   iv. Form Query: This option adds members based on a Guardium Query

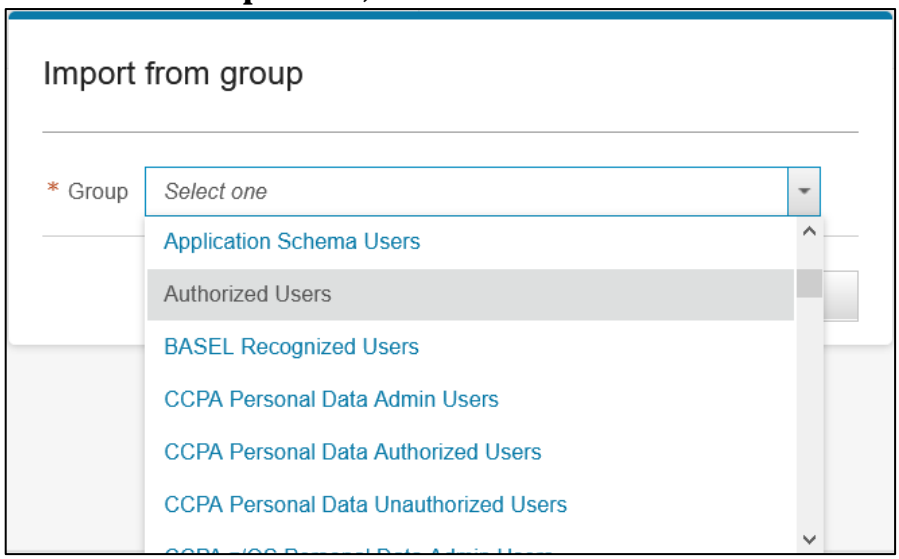
v. From LDAP Server.

e. In this exercise, you add users from another Group. From the **Import**

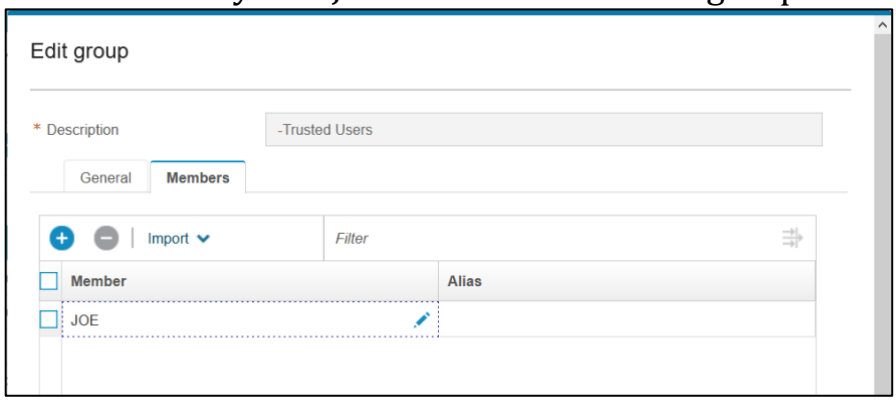
menu, select **From group**. The Import from group window opens.



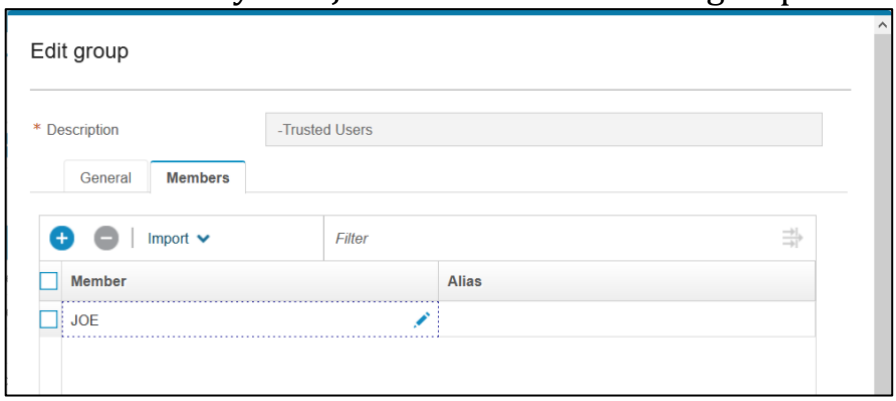
f. From the **Group** menu, select **Authorized Users**.



g. Click **OK**. Verify that Joe is added to the new group.

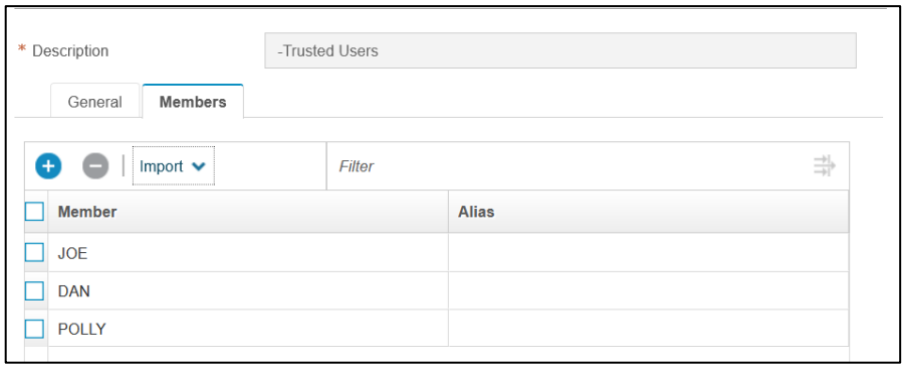


h. Click **OK**. Verify that Joe is added to the new group.



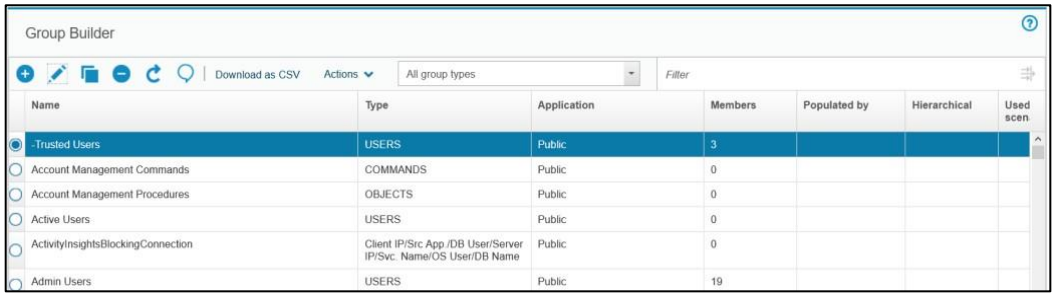
i. Now add the users from the group **Lab Trusted Users.**

Two more members are added.



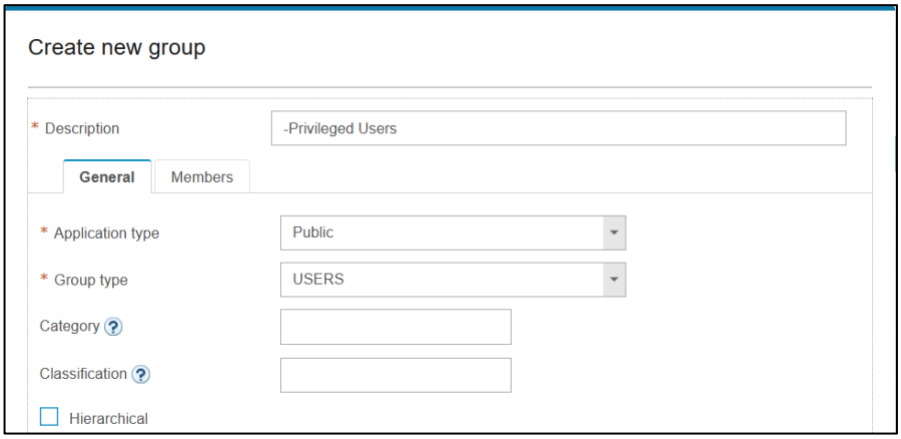
j. Scroll down and click **Save**.

k. Click **OK**, then click **Close**, to close the confirmation message. You can see your new group in the Group Builder Window.

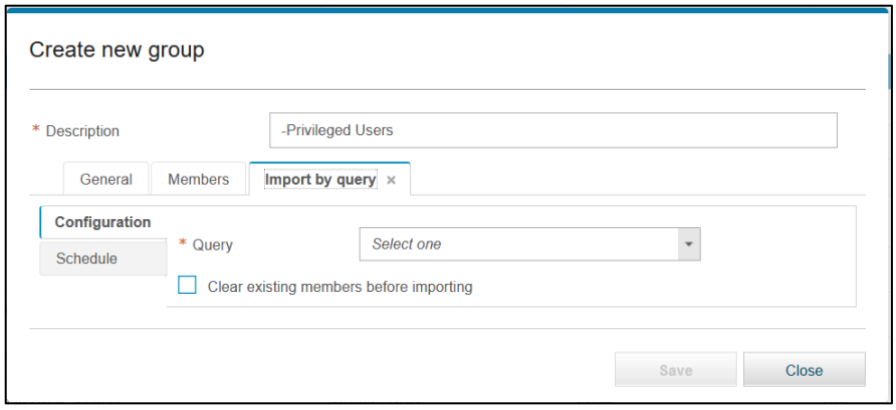


5. Now you create another group and use a query to populate it. In this **scenario**, you want to create a group of users who have a high level of privilege on databases that contain sensitive data. You might want to monitor actions by these users more closely to ensure that these privileges are not abused.
   a. Create a group with the following characteristics:

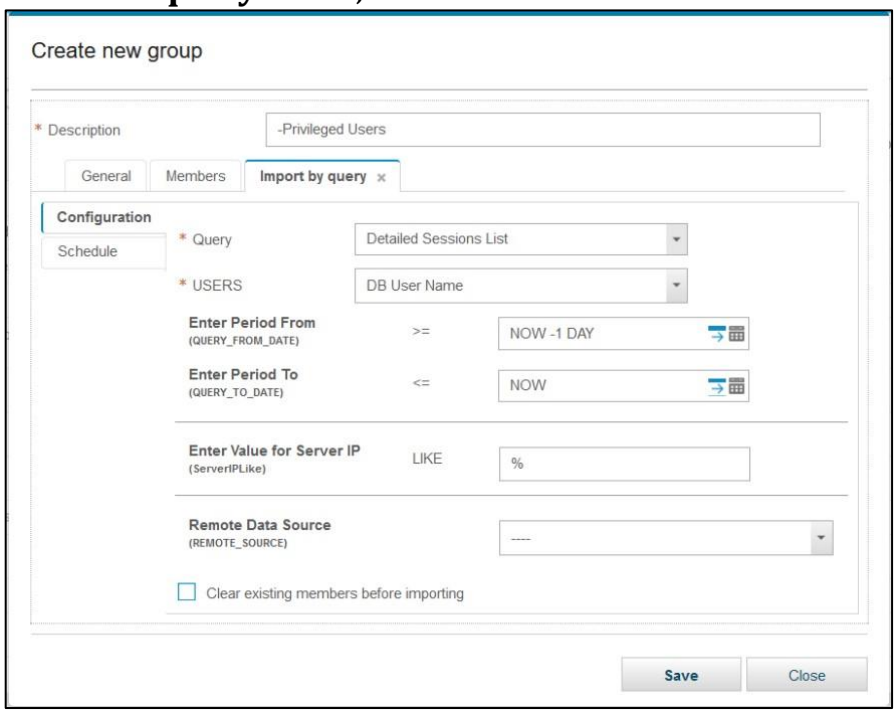
i. **Group Description**: -Privileged Users
ii. **Application Type**: Public
iii. **Group Type Description**: USERS
iv. **Category** and **Classification**: leave blank **Hierarchical**:



e. On the **Members** tab, select **From query** from the **Import** menu. A New tab that is called **import by query** is created.

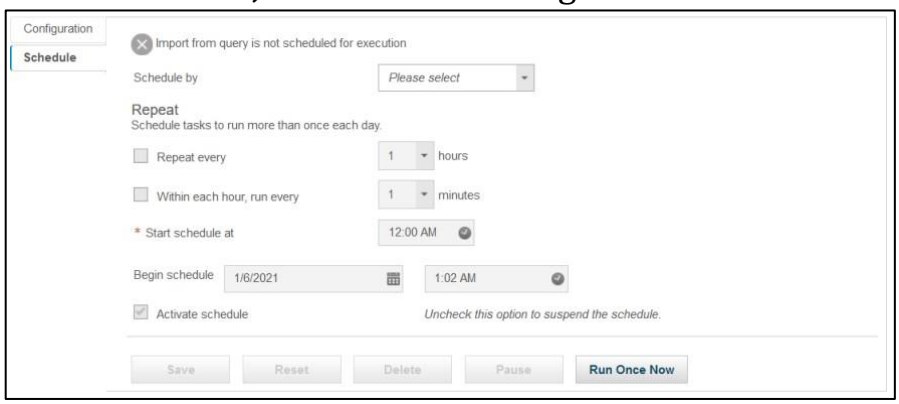


f. From the **query** menu, select **Detailed Sessions List**.

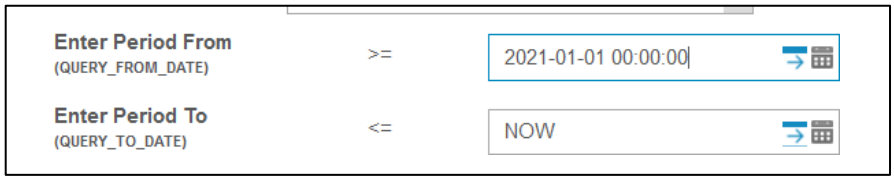


g. In the Enter Period From field, click the Calendar icon. Set the values in the calendar window to January 1, 2021. Leave all the other fields at their default setting and click **Save.**

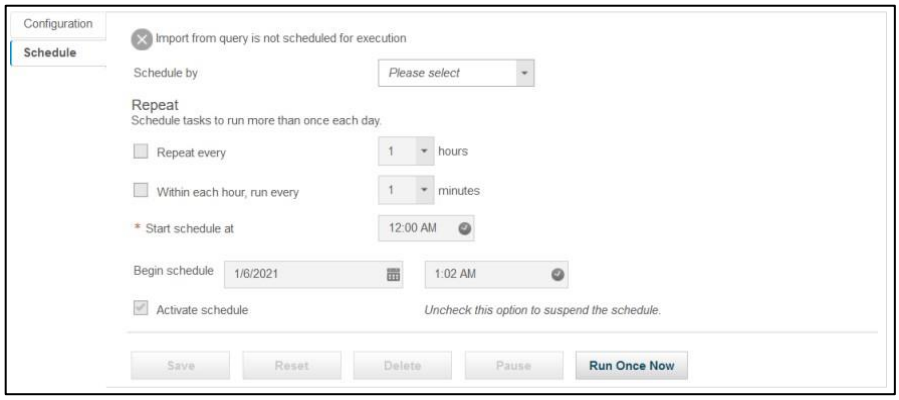
h. On the left side of the window, click the **Schedule** tab. And Click **Run Once Now,** to run the scanning.



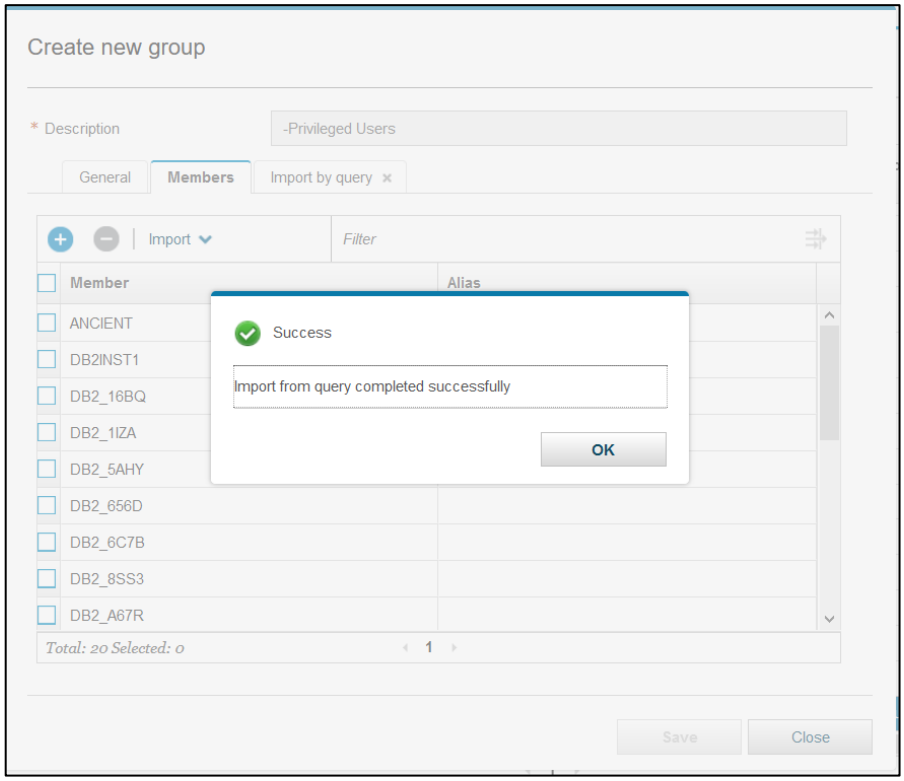
i. In the Enter Period From field, click the Calendar icon. Set the values in the calendar window to January 1, 2021. Leave all the other fields at their default setting and click **Save.**



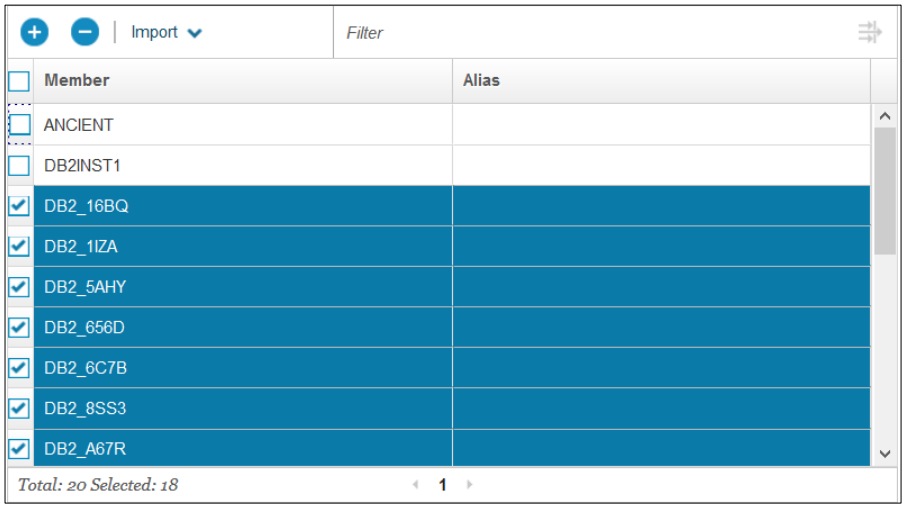
j. On the left side of the window, click the **Schedule** tab. And Click **Run Once Now,** to run the scanning.



k. Click **Ok**, and return to **Members** tab.

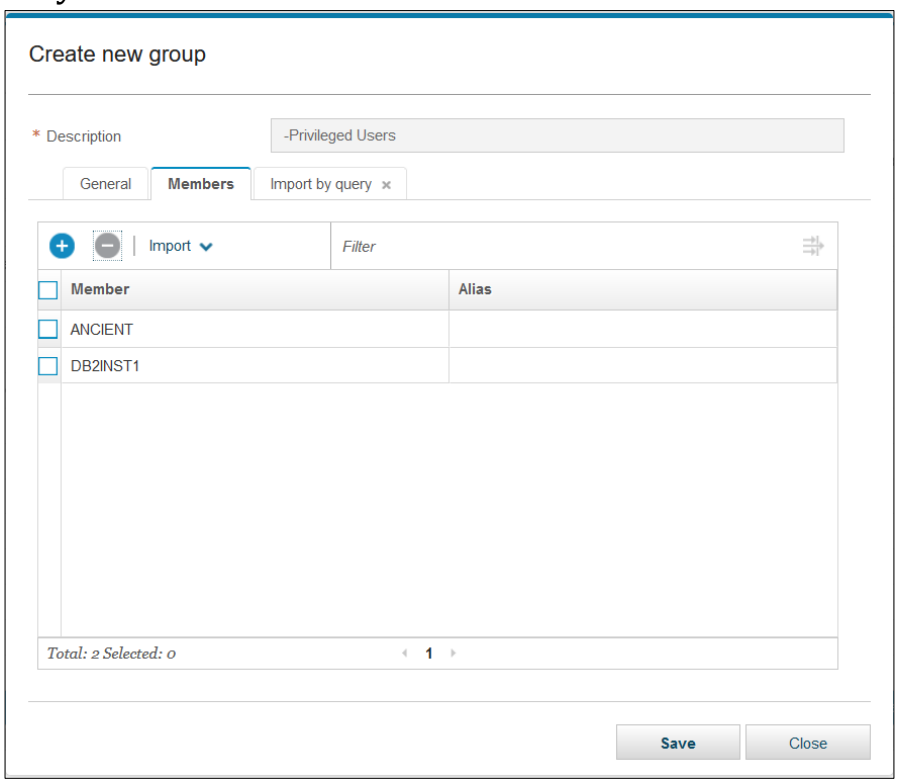


l. Select all users except DB2INST1, ANCIENT. Click the Delete



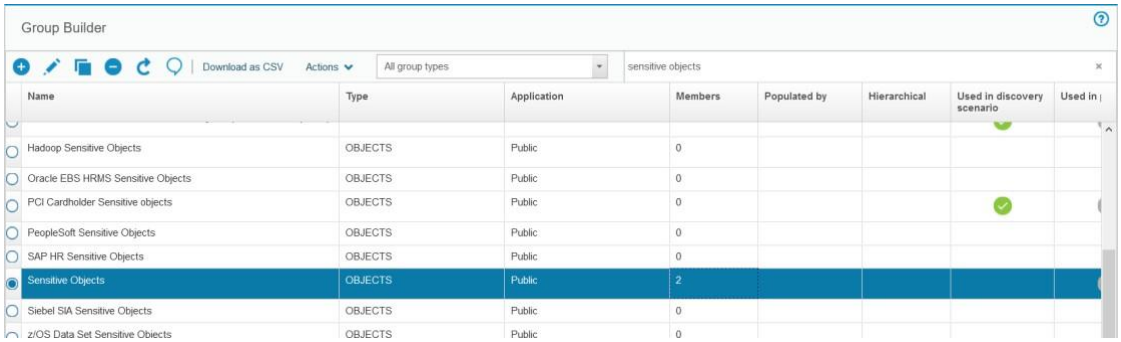
icon.

m. Only two users remain. Click on **Save**.



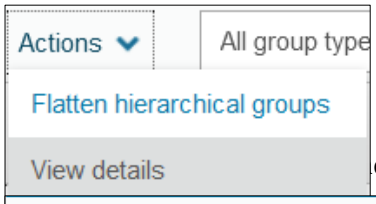
6. Your new groups are added to the Group Builder window.

7. To view an existing group, search for and select the **Sensitive Objects** group. You can narrow the list of groups by typing the name into the filter field.

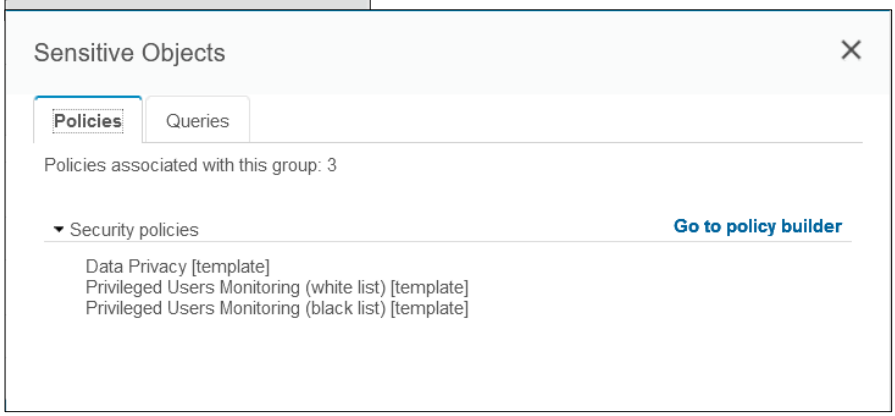


This group has 2 members as per the above screenshot, and is used in one or more classifier policy, security policy, and queries. The Gray mark indicates that none of the policy that are associated with this group is active.

a. From the **Actions** menu, select **View Details**.

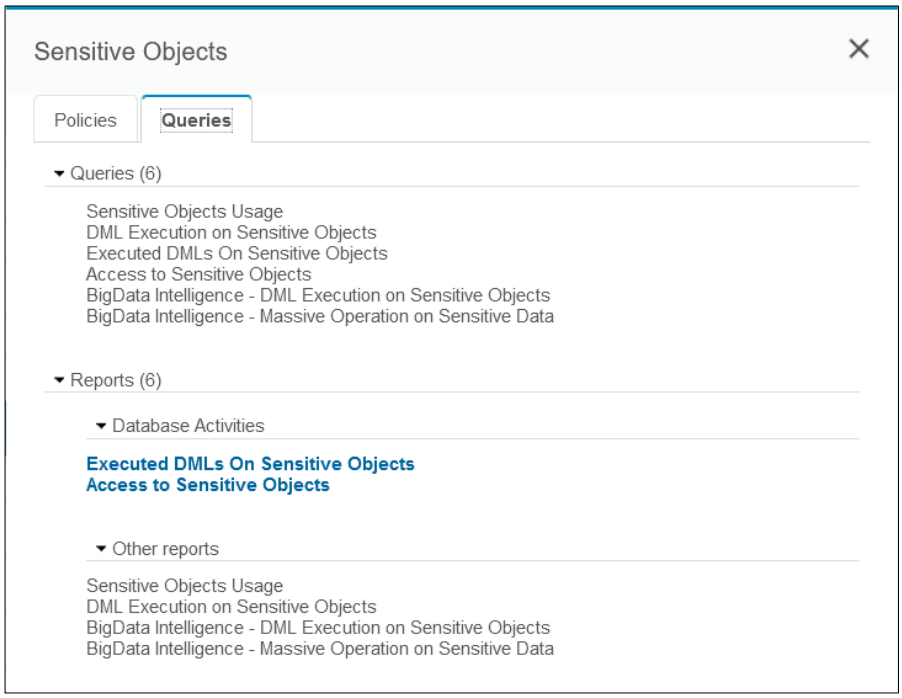


ew window opens.



You see that the Sensitive Objects group is associated with several security policies.

b. Select the **Queries** Tab.



You see that the Sensitive Objects group is associated with six queries and six reports.

c. Close the details window.

d. To open the Edit group window, click the Edit icon and then click the **Members**

Practical -4

Task 4: System view and data Management

In this exercise, you learn System Shared Secret and Data Archive process of Guardium to an external storage. In this Lab, we will use our database VM as an external storage for backup and archival purpose.

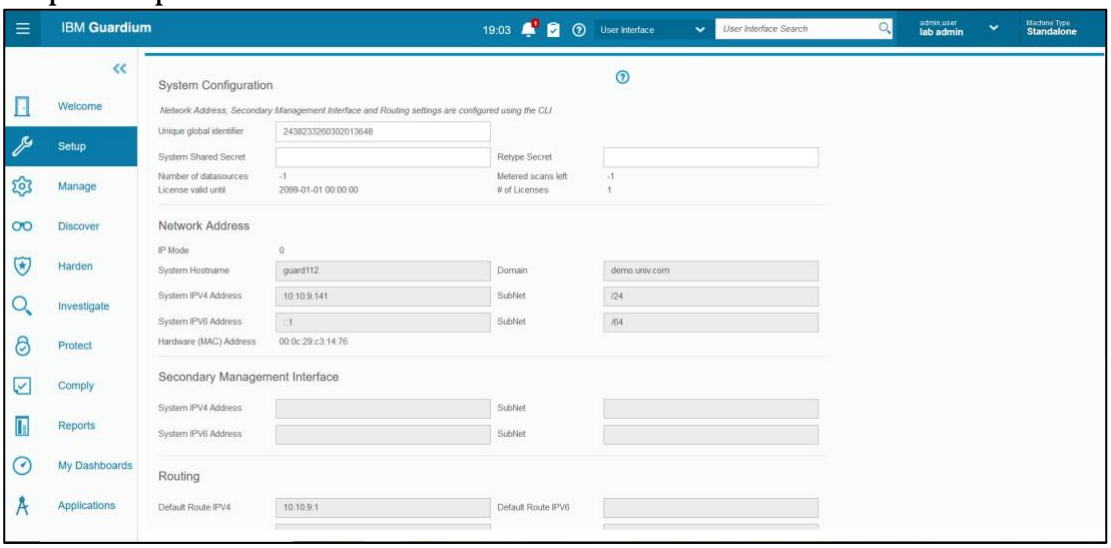
Exercise 1: System Shared Secret and DNS Resolver

The system shared secret is used for two general purposes:

- To encrypt files that are exported from the appliance by archive/export activities
- To establish secure communications between Central Managers and managed units

The system shared secret value is null at installation time. In this exercise, you prepare the system for data archival by setting the system shared secret.

1. On the DB server, open Firefox Browser and open guardium GUI https://10.10.9.141:8443. Log in with credential *lab/guardium*.
2. Navigate to **Setup > Tools and Views > System**. The System Configuration pane opens.



3. In the **System Shared Secret** and **Retype Secret** fields, enter *guardium123* or another phrase of your choice.

   Note: It is very important to remember or keep record of the system shared secret key. If the key is lost, Guardium certain operations might become impossible to run.

4. Click Apply and close any warning messages.

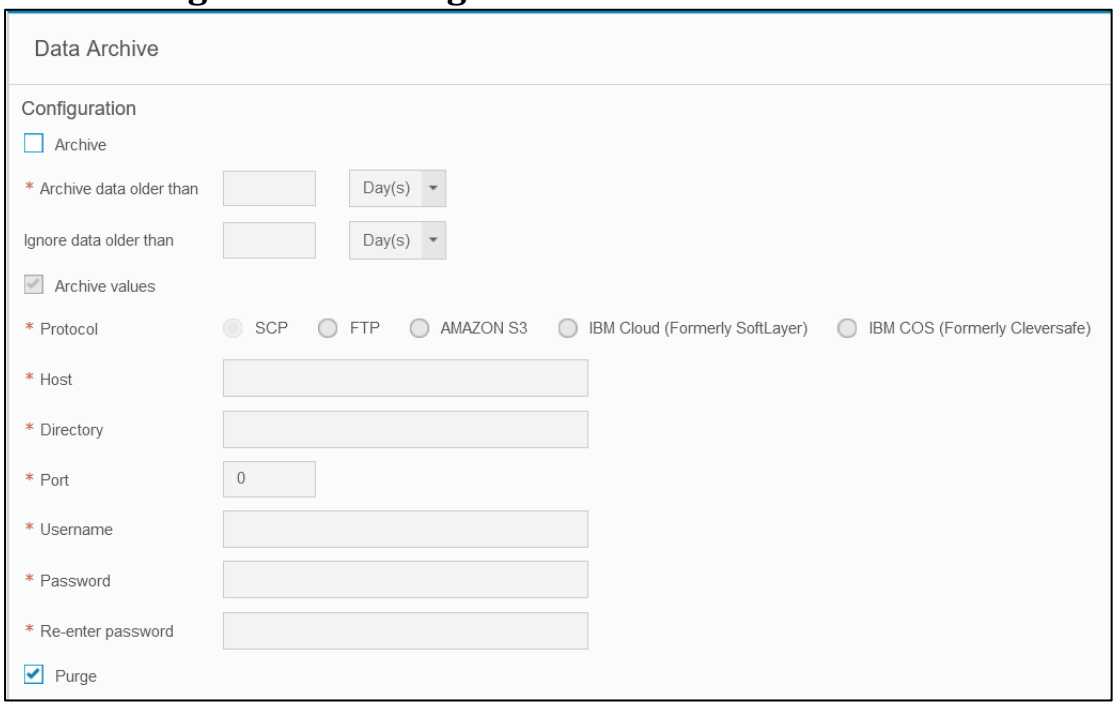
You configured the shared secret on the Guardium system. This shared secret encrypts the files that you archive in the next exercise.

Exercise 2: Guardium Data Archiving

The Guardium archive function creates signed, encrypted files that cannot be tampered with. Archive files are transferred and stored on external systems such as file servers or storage systems.

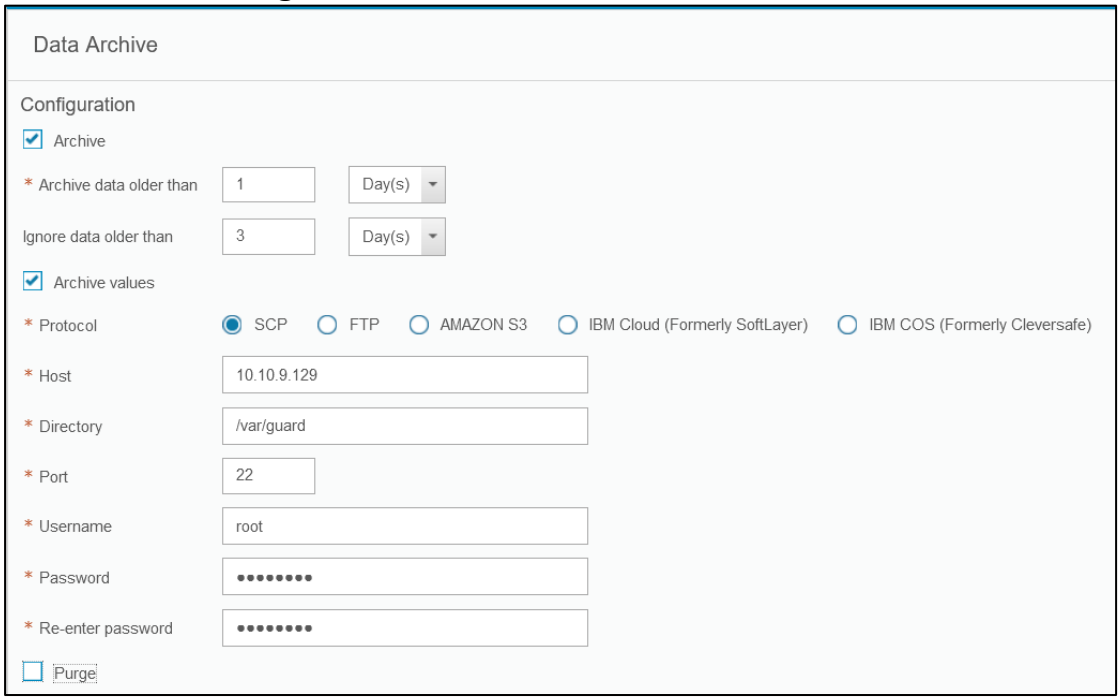
Normally, to archive only the previous day's activity, you archive data older than one day and ignore data older than two days. However, in this training environment, that criteria likely result in nothing archived. To see results from this exercise by picking up some previously collected data, you extend the archive data set well into the past.

1. Go to **Manage > Data Management > Data Archive**.



2. Select **Archive** checkbox.
3. Configure the settings as follow:
   a. Archive Data older than 1 day and ignore data older than 3 days. You might need to go further back in time. Check with your instructor.
   b. Select **Archive Values**.
   c. Select the SCP Protocol because you are sending the data to only a filesystem.
      - Host: 10.10.9.129
      - Directory: /var/guard
      - Port: 22
      - Username: root
      - Password: guardium

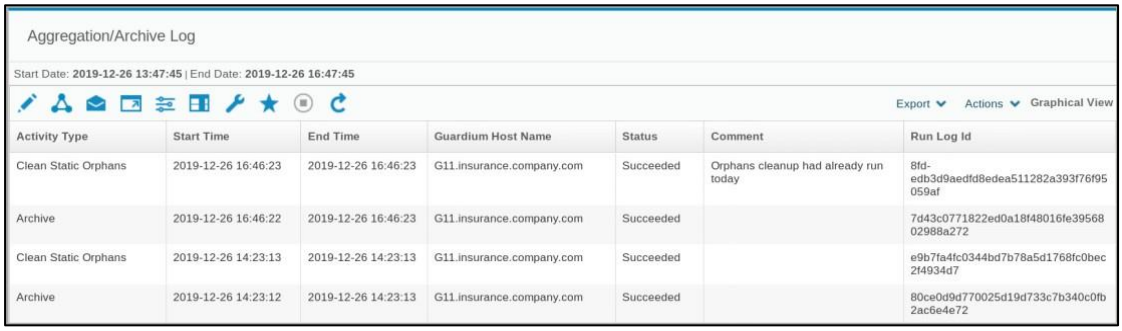
Scroll down and clear **Purge**.



4. Scroll down, click **Save**, and close the confirmation message.

The Guardium Implementation Best Practices Guide recommends a 1:30 AM start time dependent on your specific requirements. However, because that is a long time to wait to see the effects, in this exercise, to observe the result, you run the activity immediately.

5. Click **Run Once Now** and close the confirmation message.
6. To view the job as it runs, navigate to **Manage > Reports > Data Management > Aggregation/Archive Log**

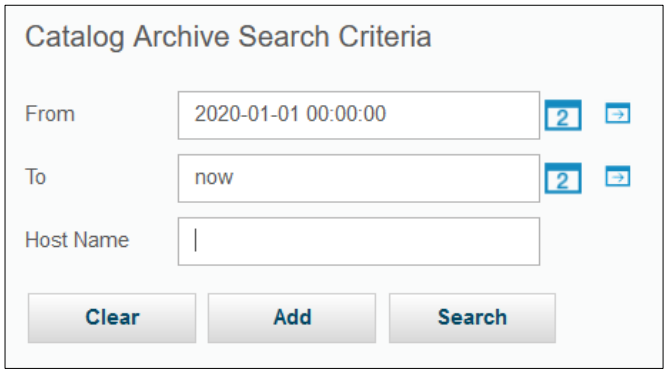


7. On the database server, to find the archive files, open a terminal window and run *ls -l /var/guard*.

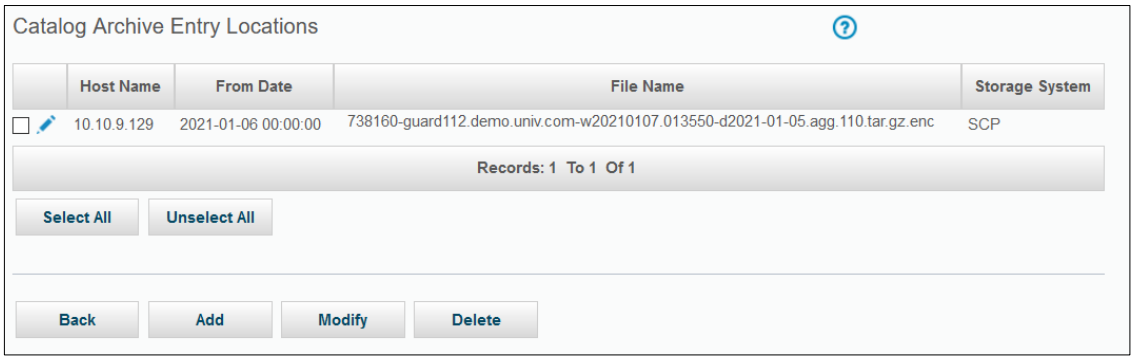
This example has multiple files. One is a test file that Guardium puts on the target host to verify connectivity. The others are archive files. Each of

the archive files contains the data for a single day, and each is labeled with the date of the data.

8. Guardium keeps a record of archives. Navigate to **Manage > Data Management > Catalog Archive**.
9. Enter the search criteria.
   a. In the **From** field, use the **Calendar** icon to choose a date that is at least one year ago.
   b. In the To field, enter NOW.
   c. Leave the Host field blank.
   d. Click Search.



10. The Catalog Archive Entry Locations pane opens.



Practical -5

Task 5: How to create a role with minimal access

This topic explains how to create a new role with minimal access permissions, for example an auditor role that can only access the Audit Process To-Do List and viewspecific reports.

Procedure

1. Create a new role.
    a. Log in as *accessmgr*, navigate to **Access** > **Access Management**, and select the **Role Browser**.
    b. Click the **Add Role** button, give the role a name, and click the **Add Role** button to create the new role.
2. Manage permissions so the new role can only access the **Audit Process To-Do List** and the **Report Builder** (which is required for viewing reports).
    a. From the **Role Browser**, click the **Manage Permissions** link for the new role.
    b. Select the checkbox in the header of the **Accessible Items** list and use the arrow to move all items to the **Inaccessible Items** list.

    When creating a highly restricted role, it is easier to begin by removingpermissions.

    c. In the **Inaccessible items** list, select the **Audit Process To-Do List** and the **Report Builder**, and use the arrow to move them back to the **Accessible items** list.

    The new role now has access to only these two specific applications.

    d. Click the **OK** button to commit your changes.
3. Customize the menus and navigation by defining which reports and applications are available to the new role.
    a. From the **Role Browser**, click the **Customize Navigation Menu** link for the new role.
    b. In the **Navigation Menu** list, select the **Reports** group so it is highlighted.

    The selected group acts as the destination for menu items added insubsequent steps.

    c. In the **Available Tools and Reports** list, expand the **Reports** section or use the **Filter** to identify specific reports, select the check box next to each item that should be available to the new role, and use the arrow to add the items to the **Navigation Menu** list.

    Items moved into the **Navigation Menu** list will become visible to usersassigned to this role.

d. In the **Navigation Menu** list, remove access to the **Report Builder** by clicking the icons next to the **Reports** > **Report Configuration Tools** and **Investigate** groups.

This further simplifies the menu structure for this role and removes access to the **Report Builder** tool without also removing applicationpermissions that are required to access reports.

e. Click the **OK** button to commit your changes.

You have now created a new role with very minimal privileges that can beassigned to users.

4. Optionally specify a custom home page for the new role.
   a. From the **Role Browser**, click the **Customize Navigation Menu** link for the new role.
   b. In the **Navigation Menu** list, specify a new default home page by selecting **Comply** > **Tools and Views** > **Audit Process To-Do List** and clicking the icon in the toolbar.

      Users assigned to this role will now see the **Audit Process To-Do List** asthe default screen after logging in.

   c. Click the **OK** button to commit your changes.
5. Create a new user and add that user to the new role.
   a. Navigate to **Access** > **Access Management** and select **User Browser**.
   b. Click **Add User**, provide the required information, and click **Add User** to create the new user.

      You will now see the user you created listed in the **User Browser**.

      When a new user is created, the account is disabled by default. Deselect the **Disabled** check box if you want the user to have immediate access totheir account.

   c. From the **User Browser**, click the **Roles** link for the new user to view a list of available roles.
   d. Select the **Assign** check box next to the custom role you created earlier.

      This will assign the user to the new role.

   e. Deselect the **Assign** check box next to the *user* role.

      Deselecting the *user* role prevents the new user from inheriting thedefault *user* access and permissions.

   f. Click **Save** to commit your changes.

Practical -6

Task 6: Policy Management

In this exercise, you learn to create and install a guardium policy.

Exercise 1: Creating and Installing a Simple Policy

A security policy contains an ordered set of rules to be applied to the observed traffic between database clients and servers. Each rule can apply to a request from a client, or to a response from a server. Multiple policies can be defined, and multiple policies can be installed on a Guardium appliance at the same time.

You define what Guardium collects by using a policy. You define one or more rules in a policy that control what database activity Guardium stores and if a rule's conditions are triggered, what actions it takes.

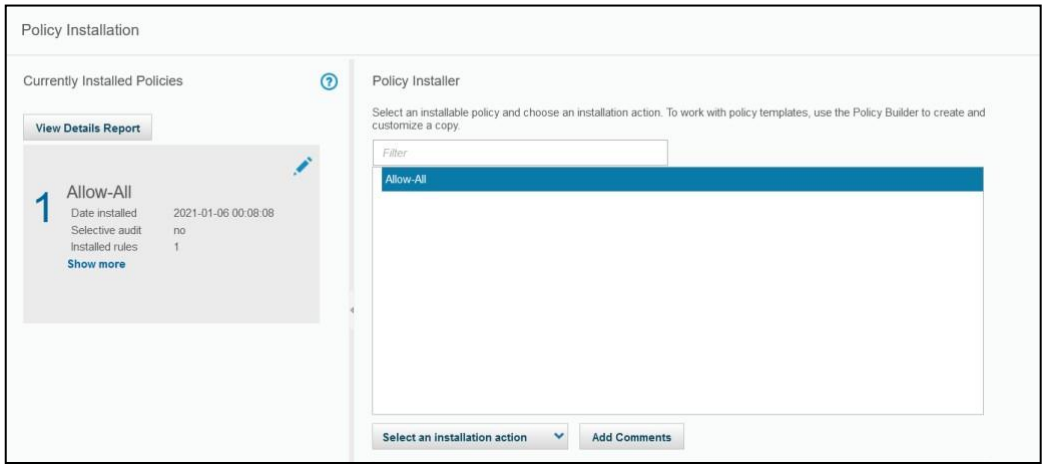
Guardium has two types of policies for data. The data security policy provides the most options for criteria and actions. Session-level policy is a specialized type of policy that improves performance by validating criteria at the beginningof processing, but only works on session-level criteria. In this exercise, you create a data security policy.

In this exercise, you create a policy that contains two rules:

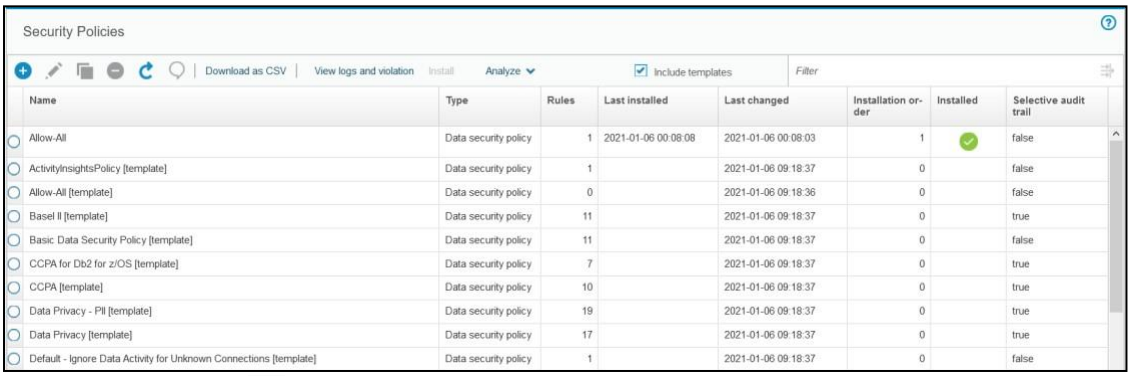
- **Ignore S-TAP Session for Trusted Users**: When the rule triggers, the sniffer process instructs the S-TAP to stop sending traffic for that particular session generated from Trusted Users.
- **Alert on Access to Sensitive Objects**: This rule triggers when any privileged user touches one of the sensitive database objects that are listed in the group.

Follow the below steps to perform this exercise.

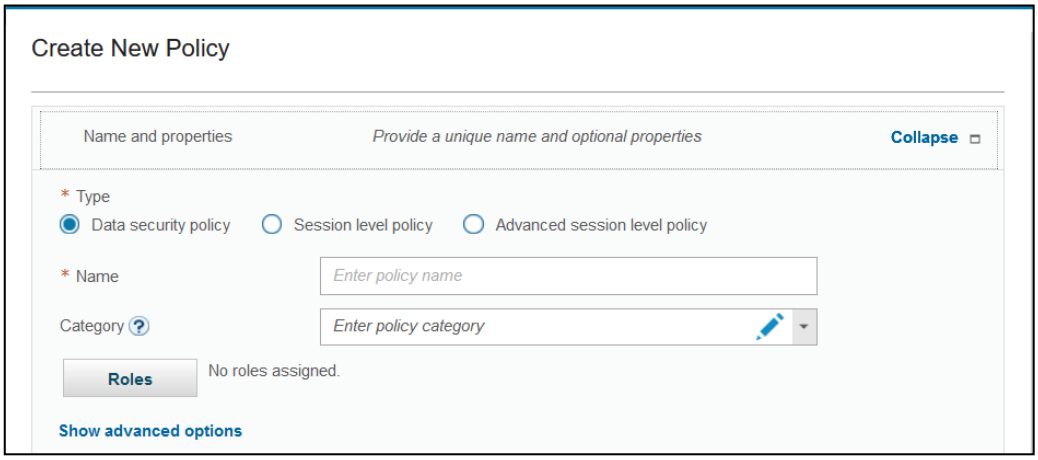
1. Start the web browser on Database Server and login to Guardium UI @ https://10.10.9.141:8443 using credentials lab/guardium.
2.
3. Go to Protect > Security Policies > Policy Installation.



4. The policy Installation pane opens. Here, you notice that only installed policy is “Allow All”. This is a policy with only one rule, which is to log all details, without any condition.
5. To create your own policy, Go to **Protect > Security Policies > Policy Builder for Data**. The Security Policies pane opens.



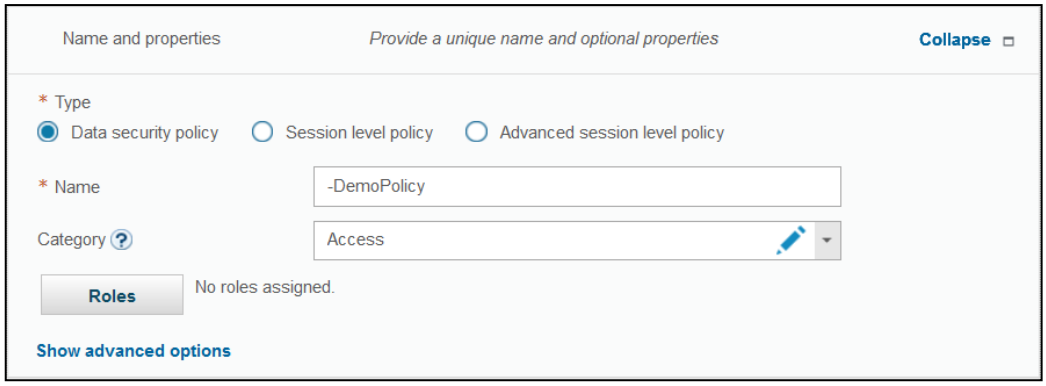
Click the **Create** icon.



6. Ensure that **Data security policy** is selected.

7. Provide a name, such as **-DemoPolicy**, for your policy and select **Access**

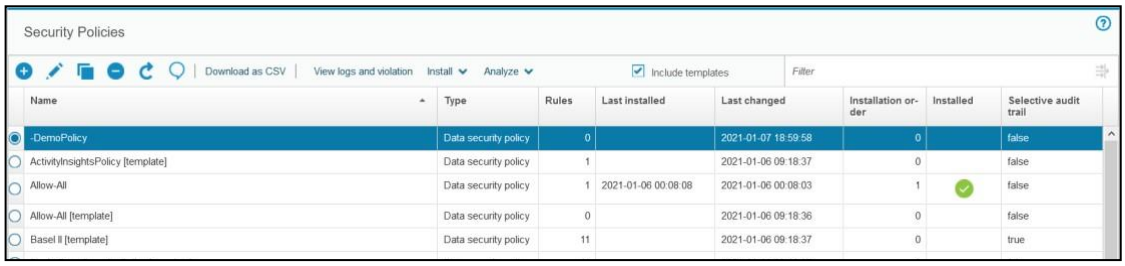
from the Category list.



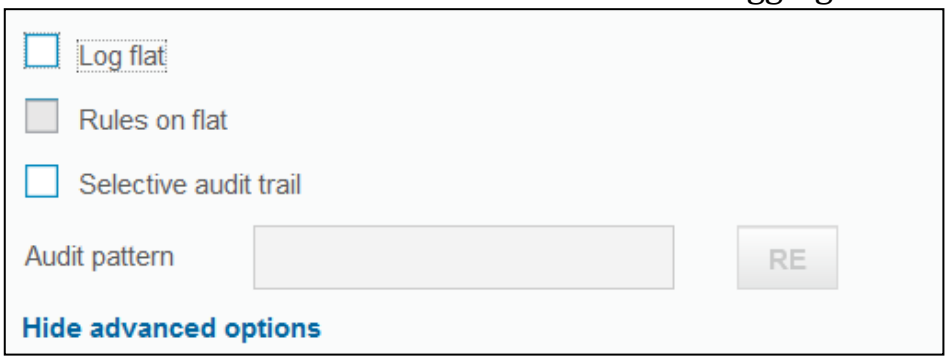
8. To save your new, but still empty policy, scroll down and click **OK**.

Your settings are saved, and you see the new policy in the security policiespane. The policy is not yet installed and has no rules.

9. To sort your policies by name, click the **Name** tab. Your new policy is at the top of the list, due to the "-" prefix

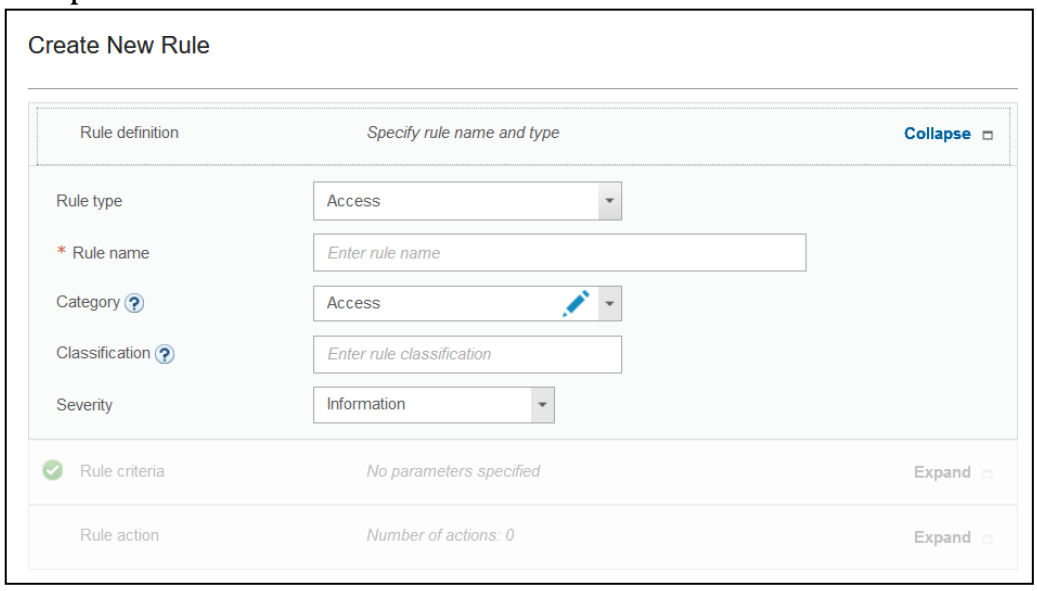


10. Select your new policy and click the **Edit** icon. The policy editing pane opens.
11. Click **Show Advanced options**.
    - **Log Flat** allows Guardium to log traffic immediately, while it postpones detailed analysis until a later time. This can reduce the load on tee collector.
    - **Rules on Flat** option is only enabled when log flat is selected it examines session-level rules in real time, but not regular rules.
    - **Selective audit trail** limits the amount of logging on the system.

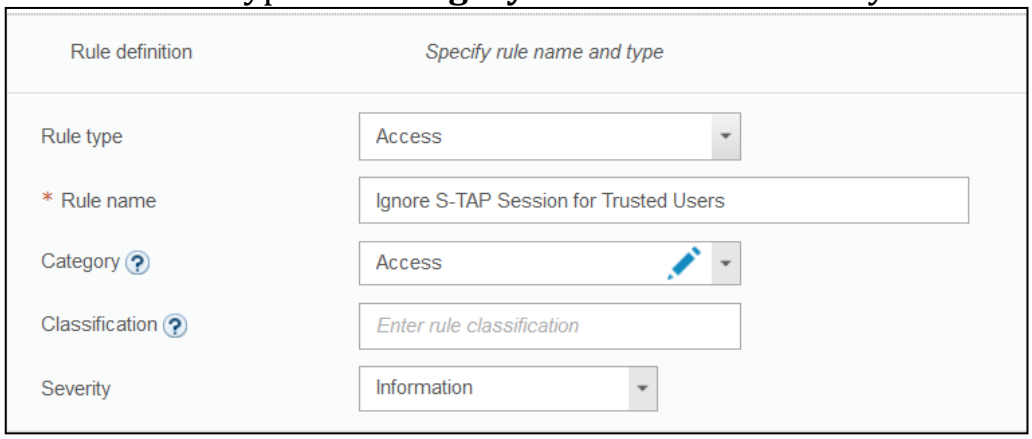


12. To configure the rules, in the Rules Section, click **Expand**. The Rules tableopens.

13. Click on **Create** icon, to add a new rule. Create New rule window opens.

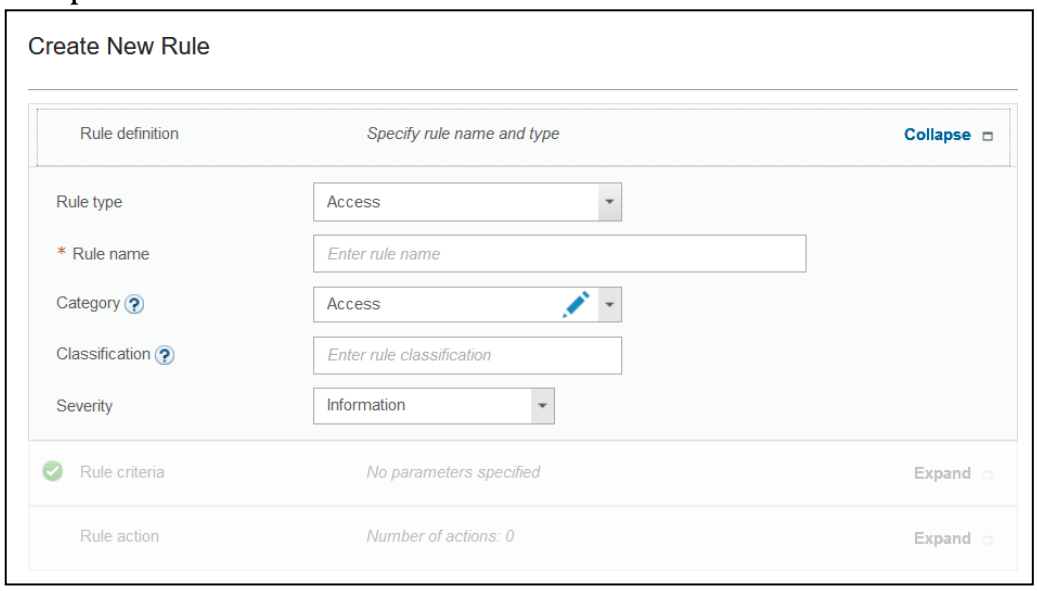


14. Enter name, **Ignore S-TAP Session for Trusted Users** into the rule namefield.
15. Leave Rule type and **category** as Access and severity as **Information**.

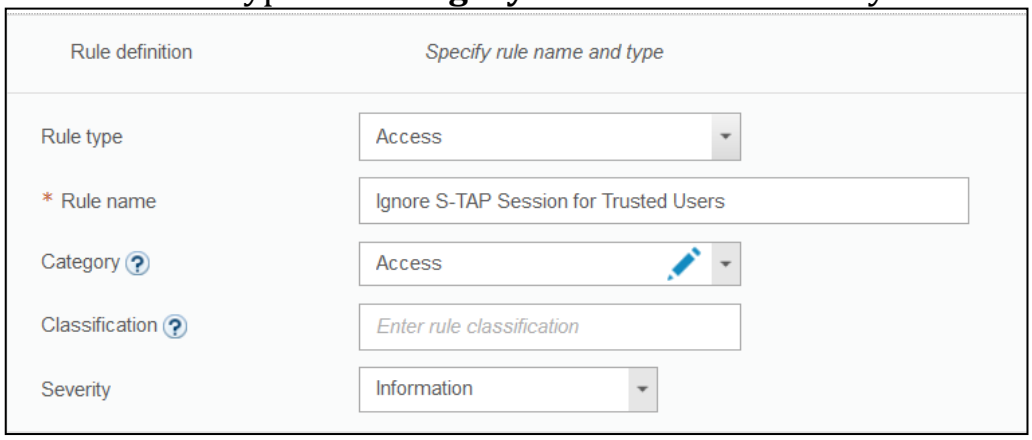


16. Click **Expand** in the rule criteria section, there are 3 subsections forcriteria.
    - Session level Criteria
    - SQL Criteria

17. Click on **Create** icon, to add a new rule. Create New rule window opens.

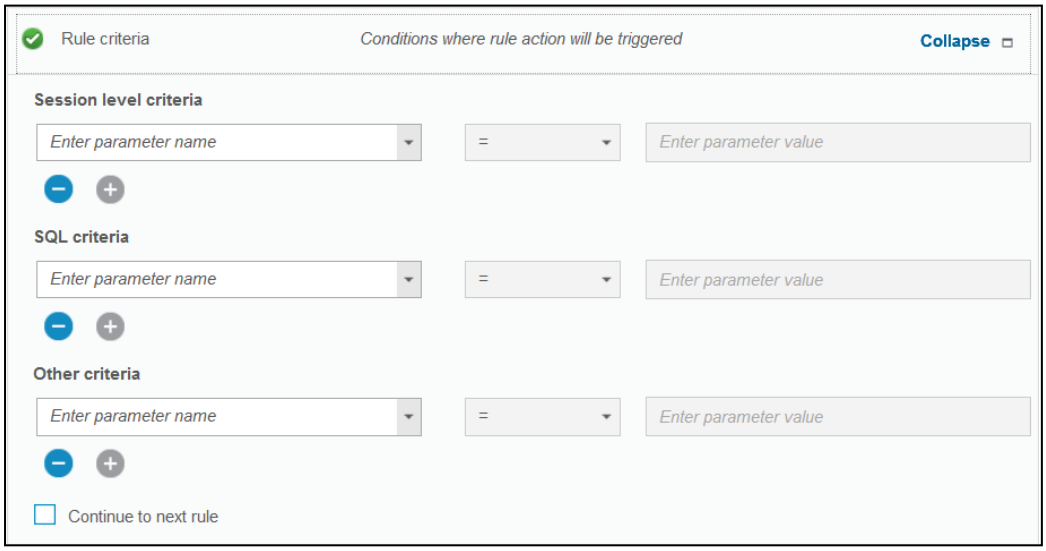


18. Enter name, **Ignore S-TAP Session for Trusted Users** into the rule namefield.
19. Leave Rule type and **category** as Access and severity as **Information**.



20. Click **Expand** in the rule criteria section, there are 3 subsections forcriteria.
    - Session level Criteria
    - SQL Criteria

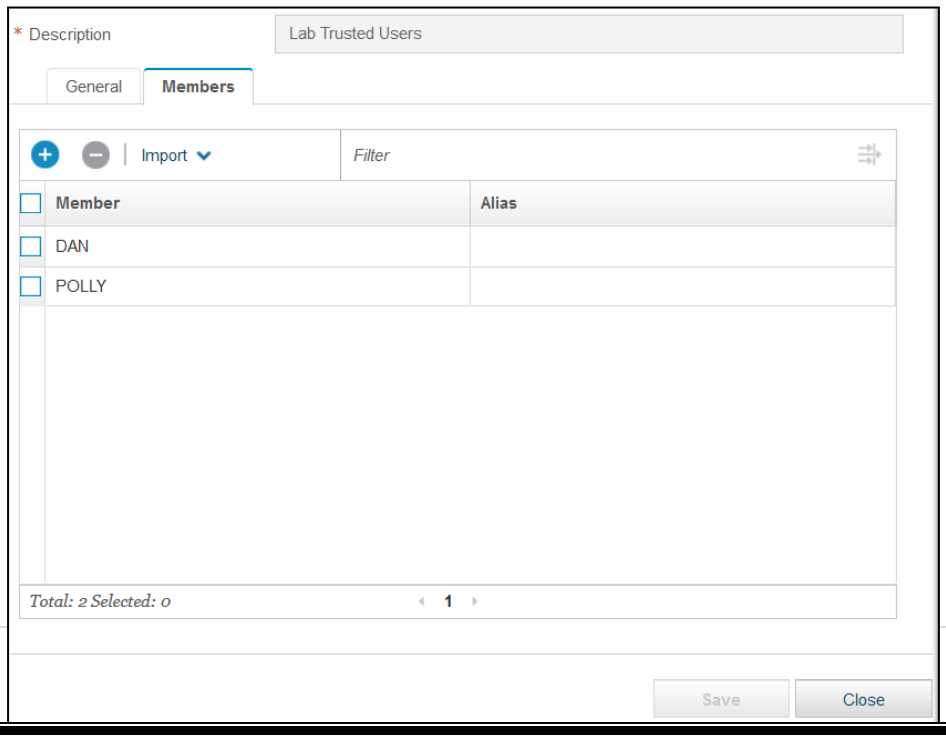
- Other Criteria



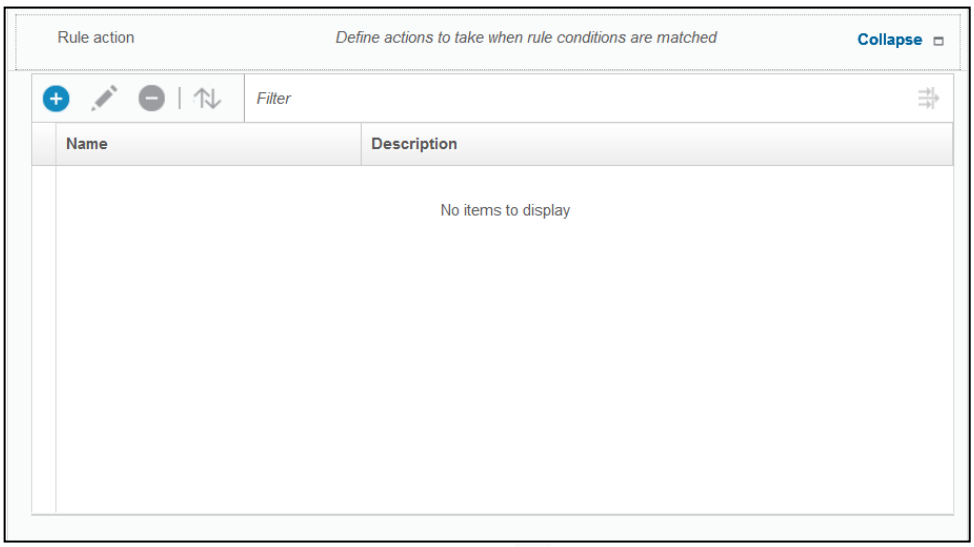
21. In the Session level Criteria, set the fields as follows.
    - Parameter Name: **Database User**
    - Condition: **In Group**
    - Parameter value: **Lab Trusted Users**

22. View the group members.
    a. Click the **Edit** icon by the group **Lab Trusted Users** and select the **member** tab to view group members.

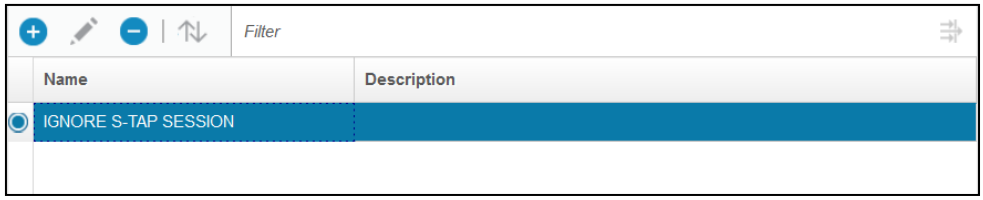
To return to the create new rule pane, scroll down and close group pane.



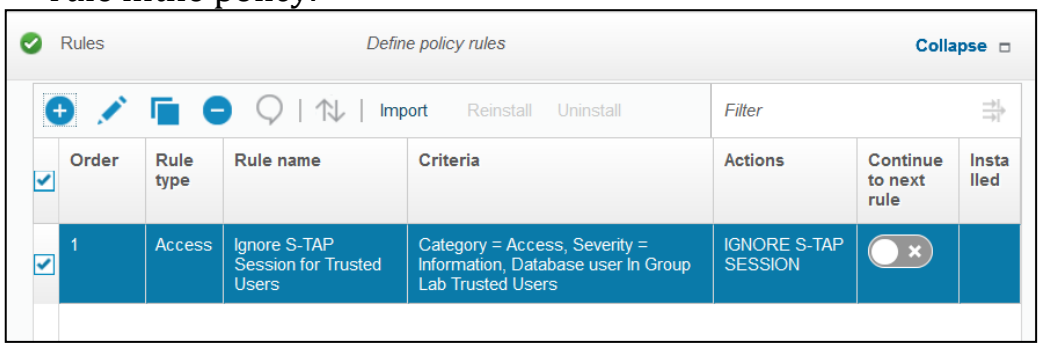
23. Define the actions to take when a database access event meets the RuleCriteria.
    a. Click **Expand** in the Rule action section.



    b. Select **IGNORE S-TAP SESSION**.

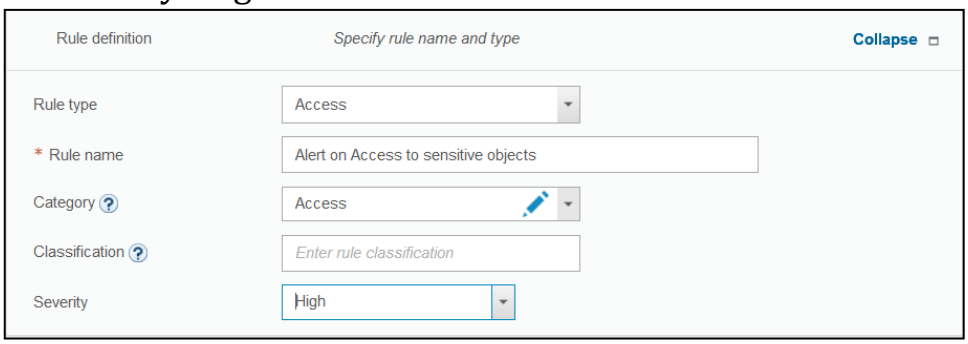


24. To save your new rule, scroll down, and click **OK**. You see the new rule inthe policy.

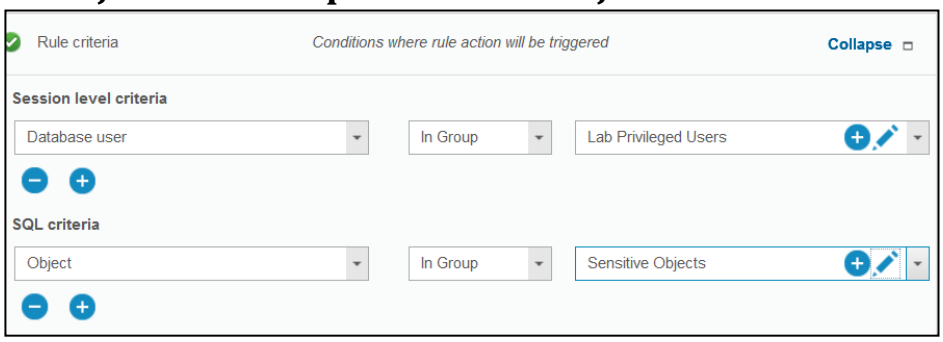


25. To dd a second access rule to your policy, follow the same process fromsteps 12-20. With following information.
    a. Rule Definition
        - Rule Type: Access
        - Description: Alert on Access to sensitive objects.

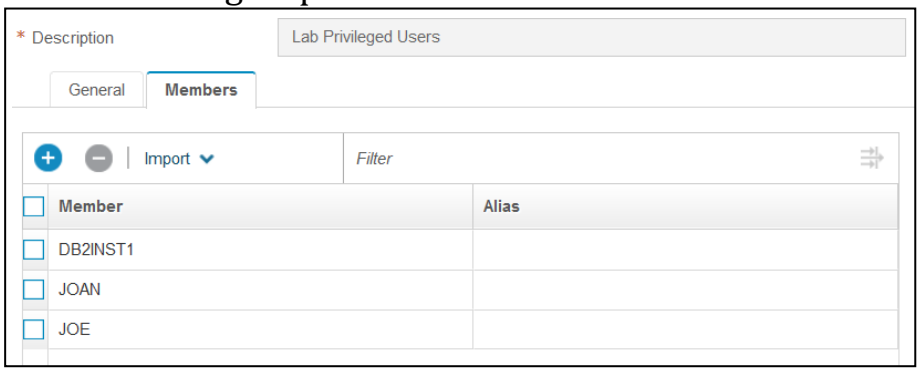
- Severity: High



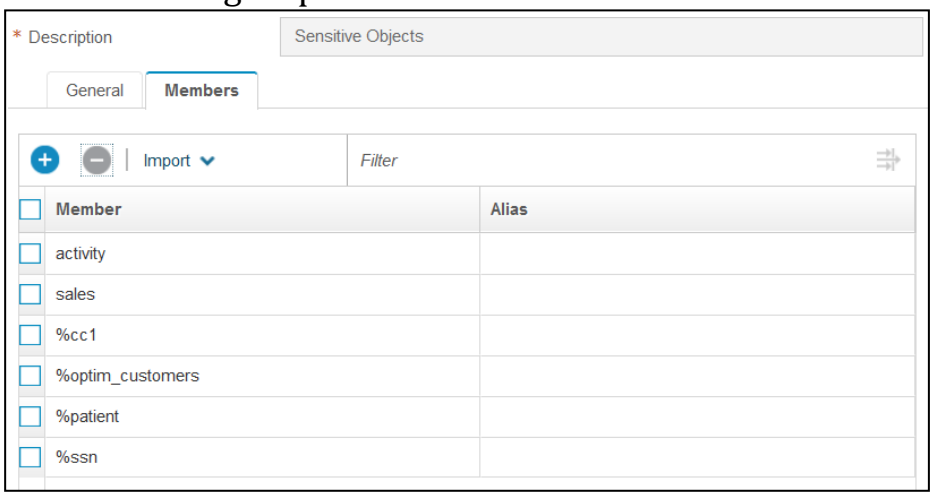
b. Session Criteria
   - Database User > In Group > Lab Privileged Users
   - **Object > In Group > Sensitive Objects**



c. Verify the member of Privilege Users Group and Sensitive objects
   - Click on  by the **Lab Privileged Users** and verify the member ofgroup and click **Close**

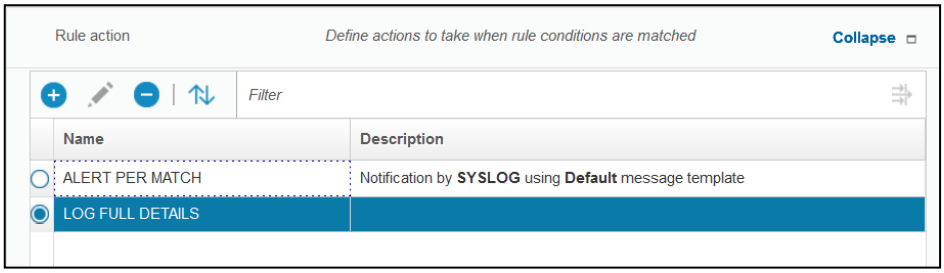


- Click on **Edit** by the **Sensitive Objects** and verify the memberof group and click **Close**

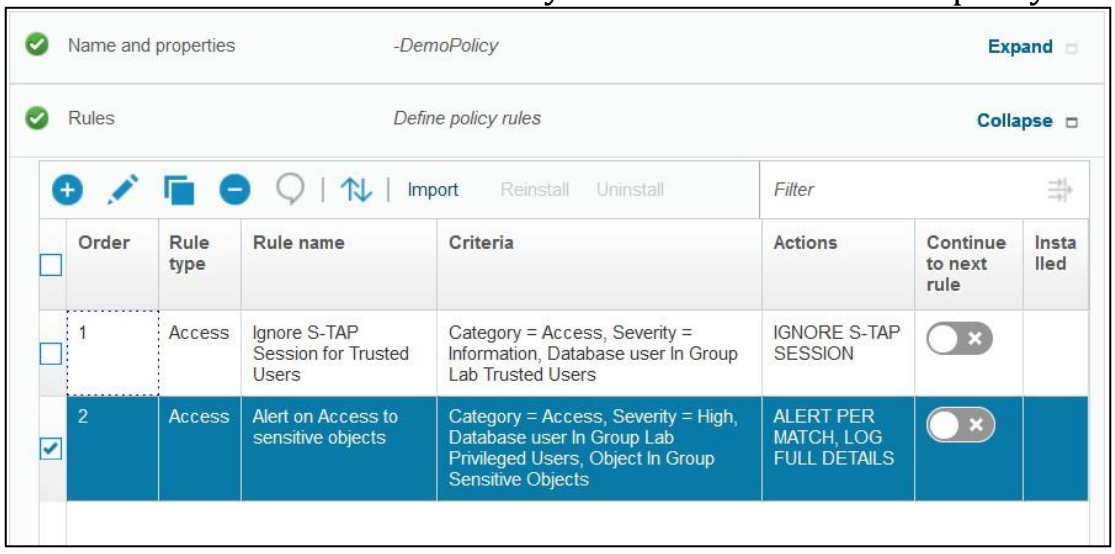


d. Rule Actions

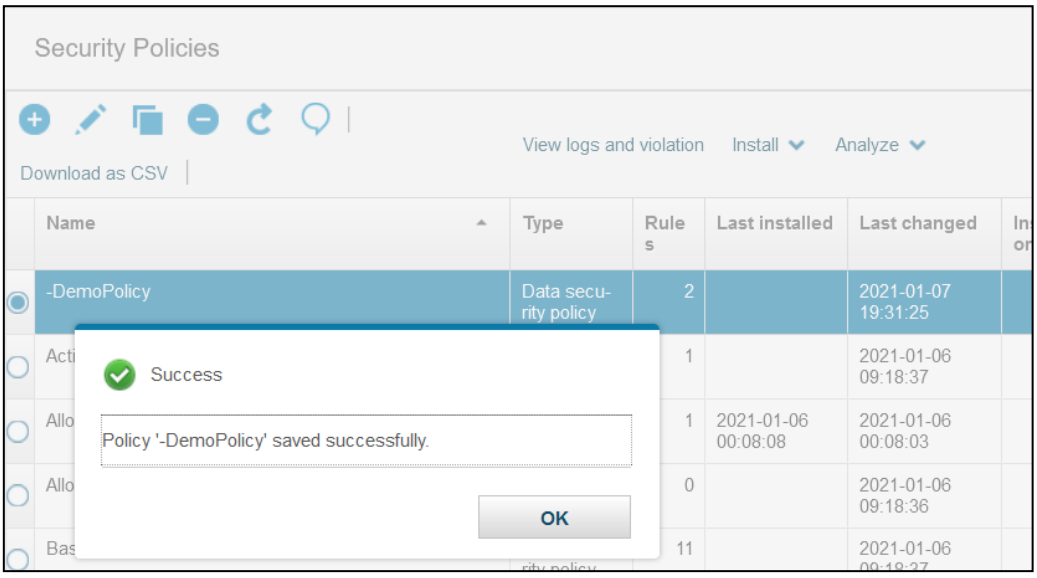
- Action1: **ALERT PER MATCH**, with default message template andSYSLOG as the Notification type.
- Action2: **LOG FULL DETAILS**



26. Scroll down and click **OK**. Now you have two rules in the policy.

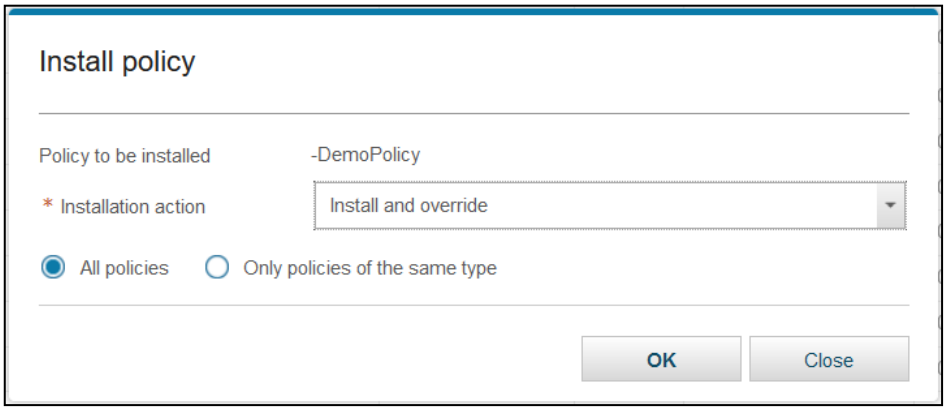


To save your policy, return to Security policy pane, scroll down and click **OK**.



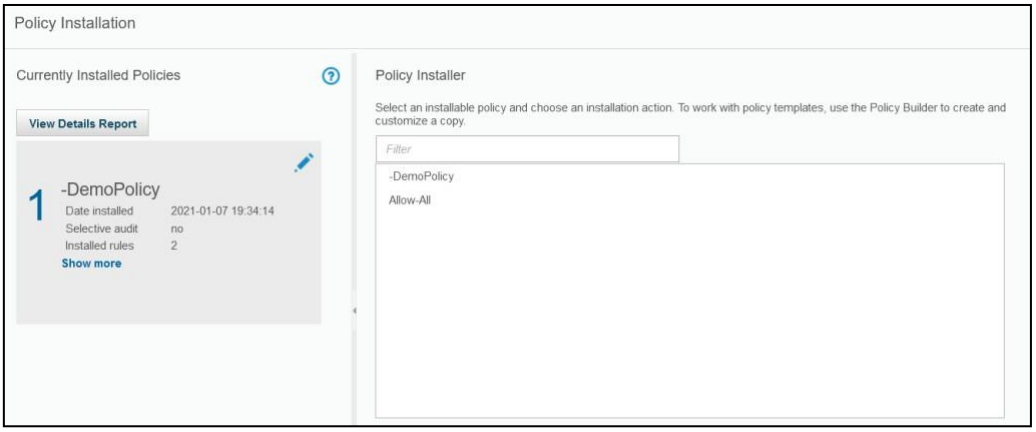
27. To install the new policy you just created.
    - Select your new policy, **-Demo Policy**
    - From the **Install Menu**, select **Install.**

- In the pop-up window, select the Installation action **Install & Override**. Leave **All Policies** selected.



- Click **OK** and close the confirmation message.

28. The policy is installed, To verify, go to **Protect > Security Policies > Policy Installation**.



Practical -7

Task 7: Policy Management (complex)

In this exercise, you learn to create and install a guardium policy.

Exercise 1: Creating and Installing a simple Policy

A security policy contains an ordered set of rules to be applied to the observed traffic between database clients and servers. Each rule can apply to a request from a client, or to a response from a server. Multiple policies can be defined, and multiple policies can be installed on a Guardium appliance at the same time.

You define what Guardium collects by using a policy. You define one or more rules in a policy that control what database activity Guardium stores and if a rule's conditions are triggered, what actions it takes.

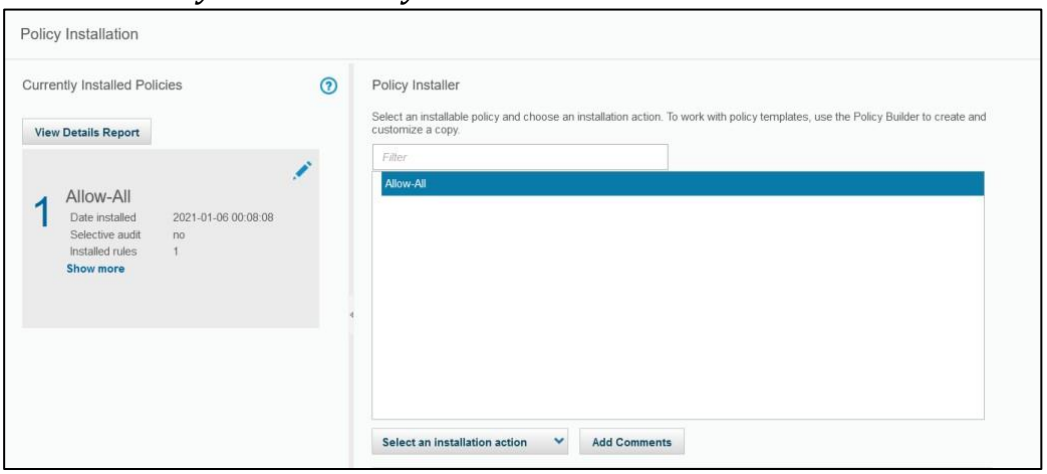
Guardium has two types of policies for data. The data security policy provides the most options for criteria and actions. Session-level policy is a specialized type of policy that improves performance by validating criteria at the beginning of processing, but only works on session-level criteria. In this exercise, you create a data security policy.

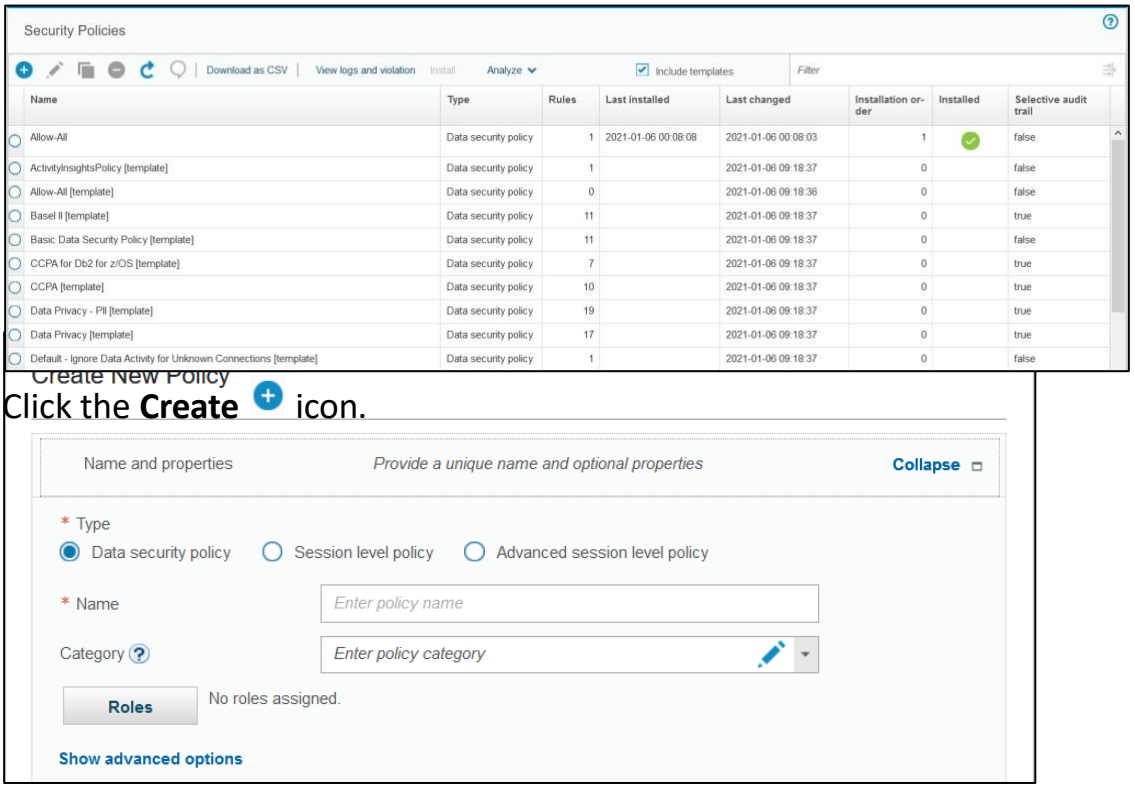
In this exercise, you create a policy that contains two rules:

- **Ignore S-TAP Session for Trusted Users**: When the rule triggers, the sniffer process instructs the S-TAP to stop sending traffic for that particular session generated from Trusted Users.
- **Alert on Access to Sensitive Objects**: This rule triggers when any privileged user touches one of the sensitive database objects that are listed in the group.

Follow the below steps to perform this exercise.

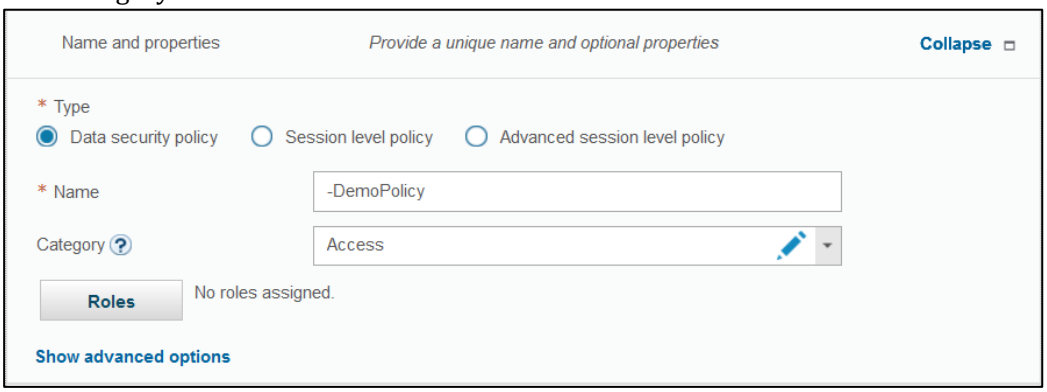
1. Start the web browser on Database Server and login to Guardium UI @ https://10.10.9.141:8443 using credentials lab/guardium.
2. *Go to **Protect > Security Policies > Policy Installation**.*



3. The policy Installation pane opens. Here, you notice that only installed policy is “Allow All”. This is a policy with only one rule, which is to log all details, without any condition.
4. To create your own policy, Go to **Protect > Security Policies > Policy Builder for Data**. The Security Policies pane opens.
5. 

Create New Policy
Click the **Create** icon.

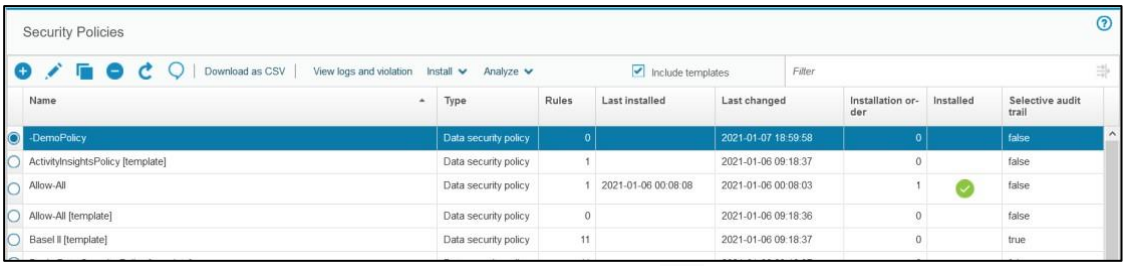
6. Ensure that **Data security policy** is selected.
7. Provide a name, such as **-DemoPolicy**, for your policy and select **Access** from the Category list.



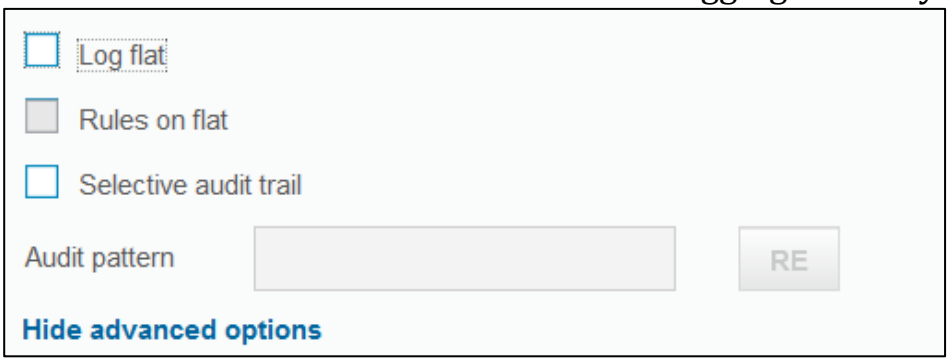
8. To save your new, but still empty policy, scroll down and click **OK**.

Your settings are saved, and you see the new policy in the security policies pane. The policy is not yet installed and has no rules.

9. To sort your policies by name, click the **Name** tab. Your new policy is at the top of the list, due to the "-" prefix.

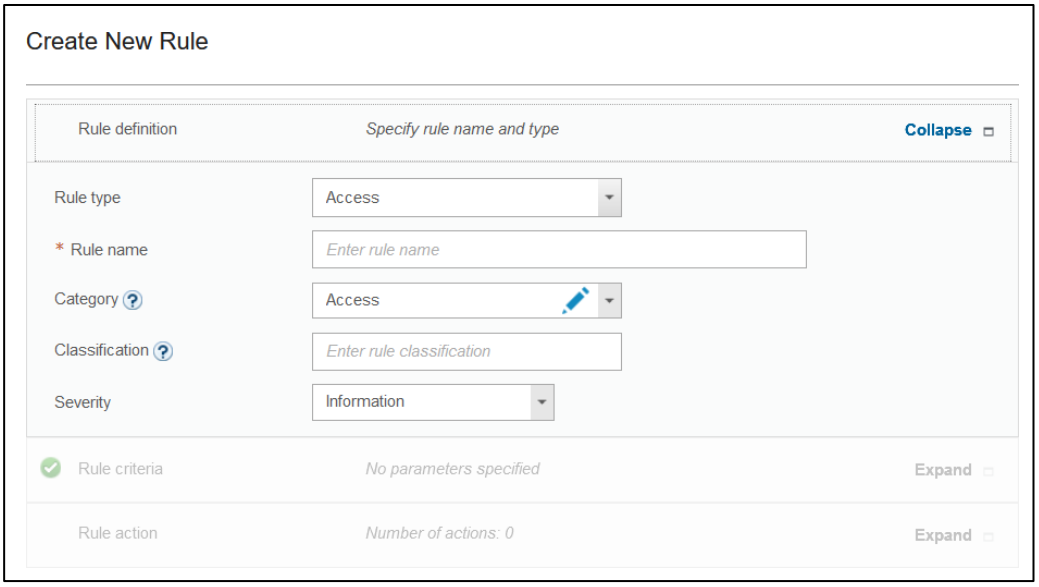


10. Select your new policy and click the **Edit** icon. The policy editing pane opens.
11. Click **Show Advanced options**.
    - **Log Flat** allows Guardium to log traffic immediately, while it postpones detailed analysis until a later time. This can reduce the load on tee collector.
    - **Rules on Flat** option is only enabled when log flat is selected it examines session-level rules in real time, but not regular rules.
    - **Selective audit trail** limits the amount of logging on the system.

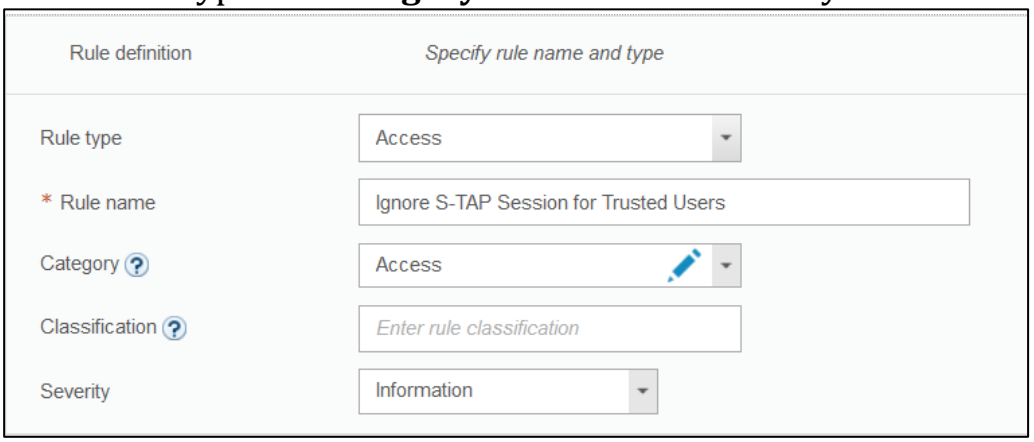


12. To configure the rules, in the Rules Section, click **Expand**. The Rules table opens.

13. Click on **Create** icon, to add a new rule. Create New rule window opens.

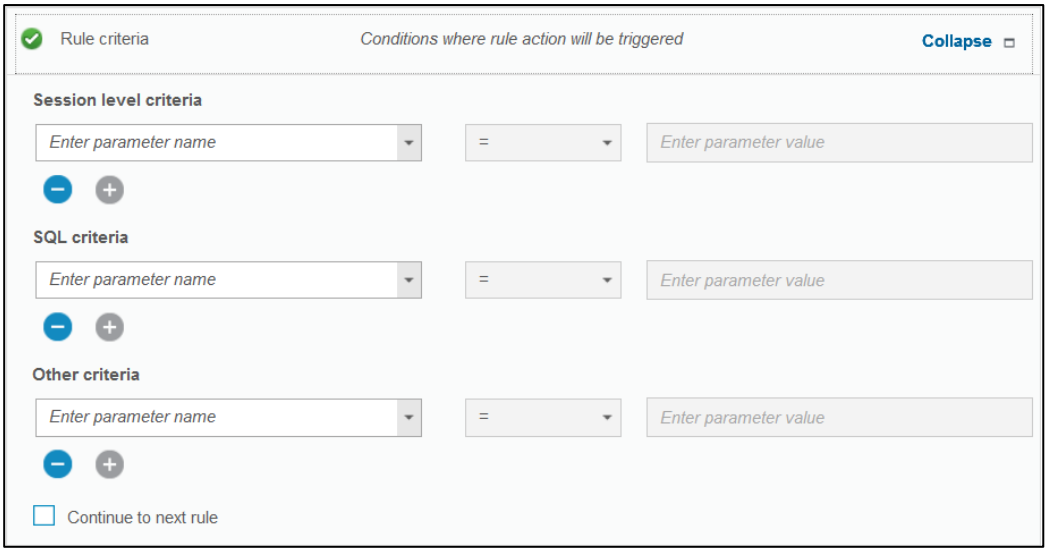


14. Enter name, **Ignore S-TAP Session for Trusted Users** into the rule name field.
15. Leave Rule type and **category** as Access and severity as **Information**.



16. Click **Expand** in the rule criteria section, there are 3 subsections for criteria.
    - Session level Criteria
    - SQL Criteria

- Other Criteria



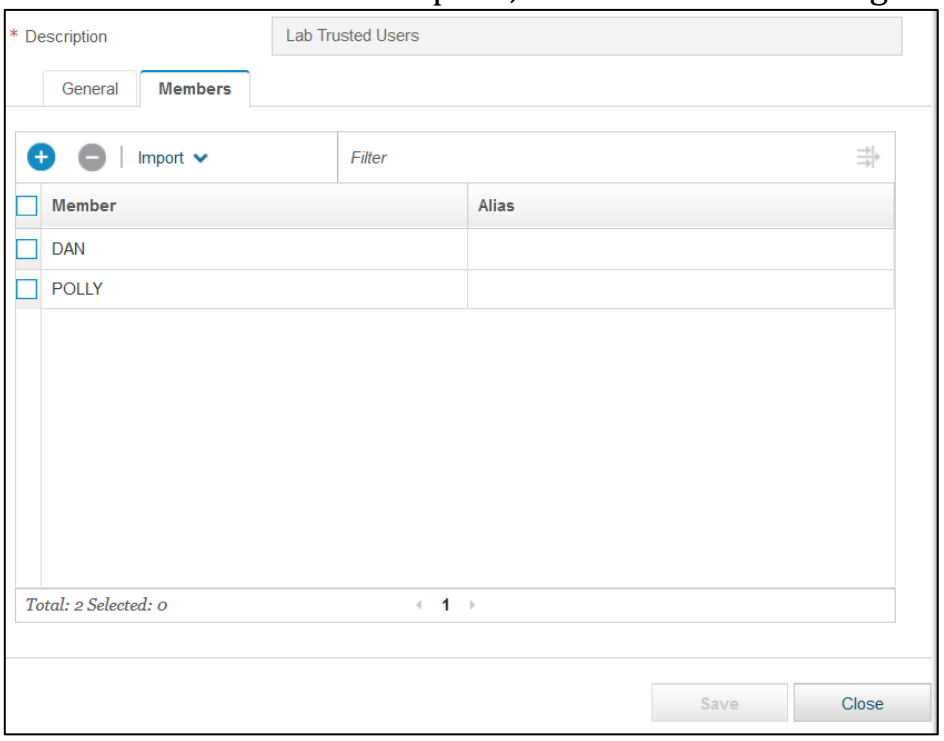
17. In the Session level Criteria, set the fields as follows.
    - Parameter Name: **Database User**
    - Condition: **In Group**
    - Parameter value: **Lab Trusted Users**

18. In the Session level Criteria, set the fields as follows.
    - Parameter Name: **Database User**
    - Condition: **In Group**
    - Parameter value: **Lab Trusted Users**

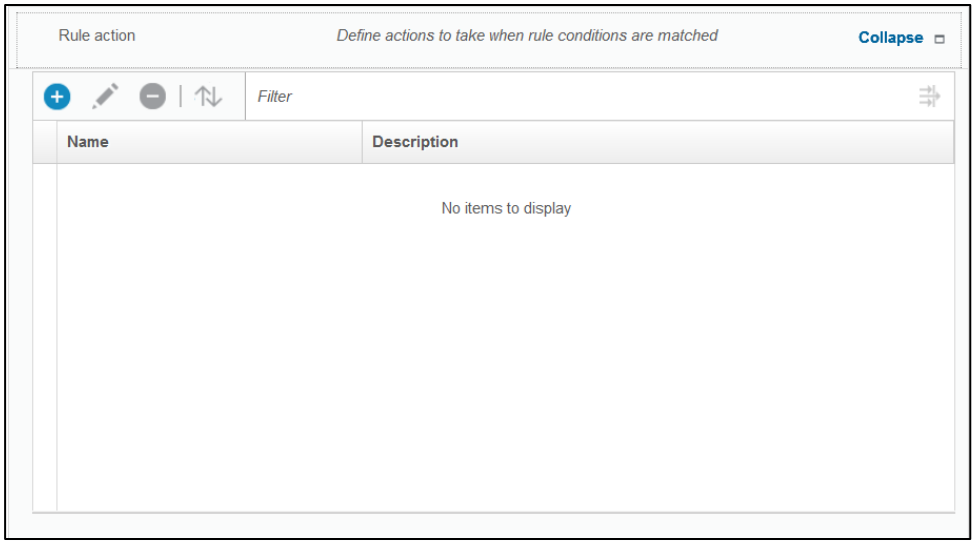
19. In the Session level Criteria, set the fields as follows.
    - Parameter Name: **Database User**
    - Condition: **In Group**
    - Parameter value: **Lab Trusted Users**

20. View the group members.
    a. Click the **Edit** icon by the group **Lab Trusted Users** and select the **member** tab to view group members.

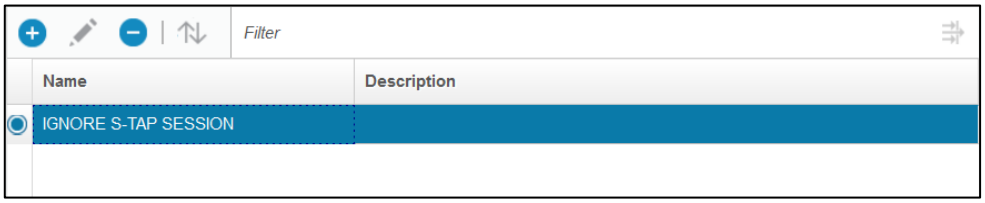
    b. To return to the create new rule pane, scroll down and close group pane.



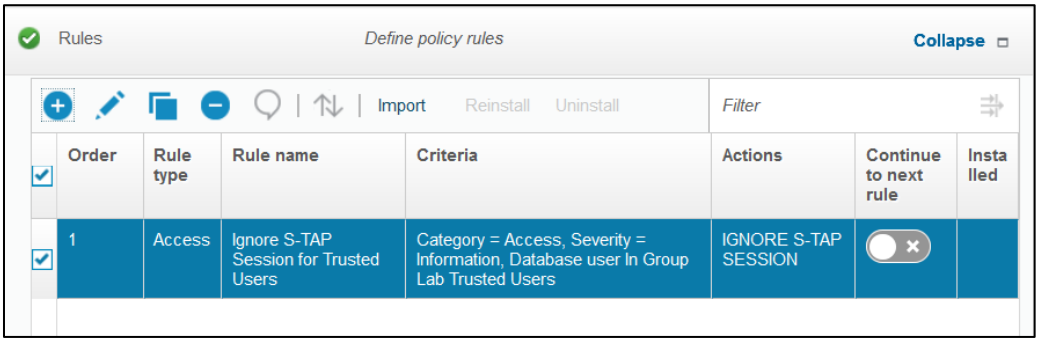
21. Define the actions to take when a database access event meets the Rule Criteria.
    a. Click **Expand** in the Rule action section.



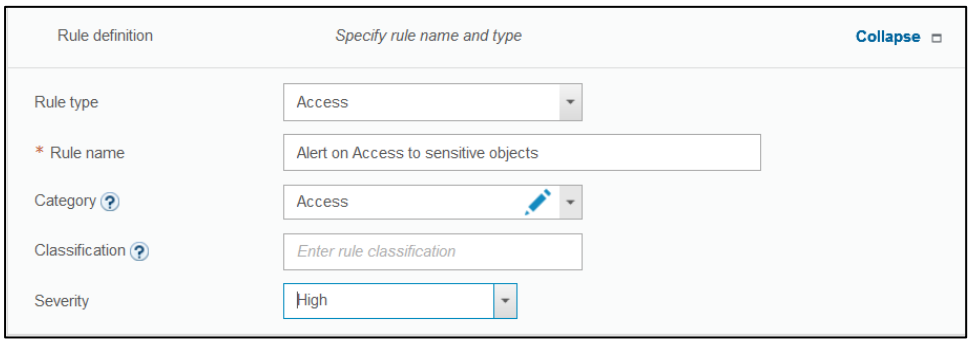
c. Select **IGNORE S-TAP SESSION.**



22. To save your new rule, scroll down, and click **OK**. You see the new rule in the policy.

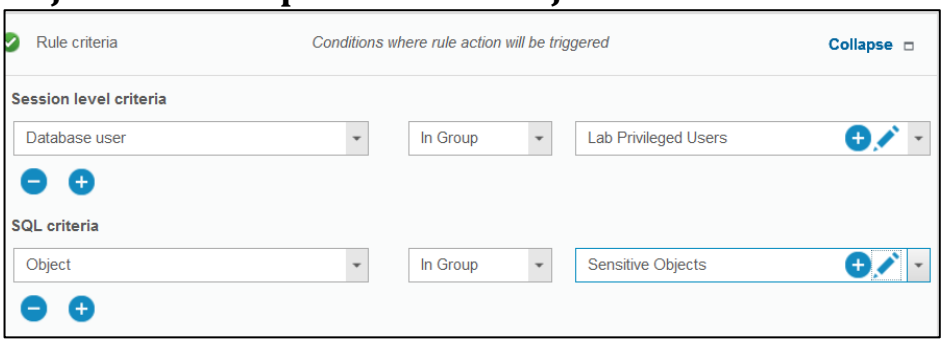


23. To dd a second access rule to your policy, follow the same process from steps 12-20. With following information.
    a. Rule Definition
        - Rule Type: Access
        - Description: Alert on Access to sensitive objects.
        - Severity: High



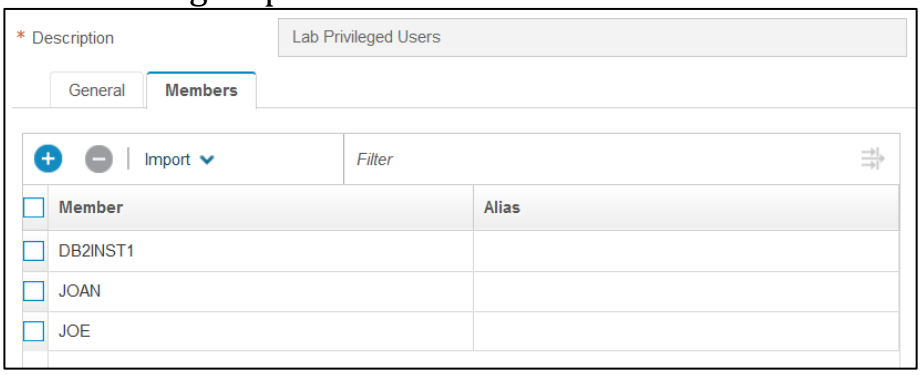
b. Session Criteria

- ***Database User > In Group > Lab Privileged Users***
- **Object > In Group > Sensitive Objects**

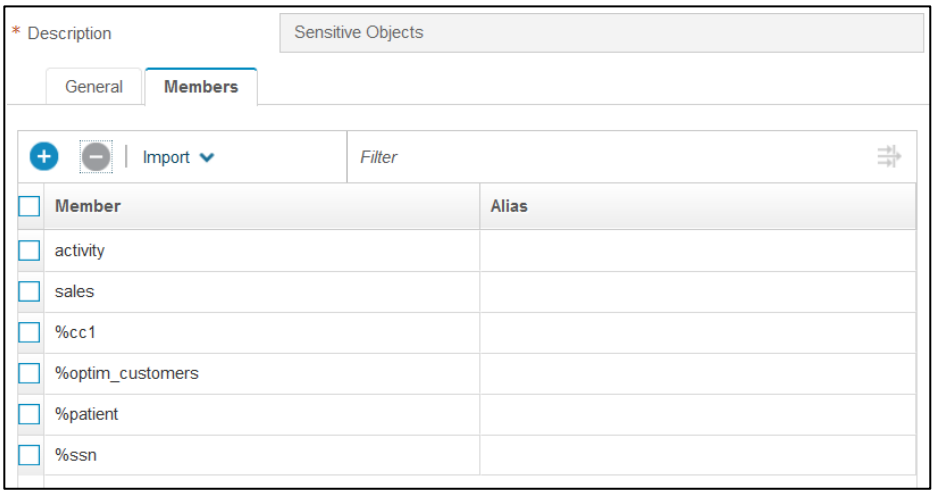


c. Verify the member of Privilege Users Group and Sensitive objects

- Click on  by the **Lab Privileged Users** and verify the member of group and click **Close**

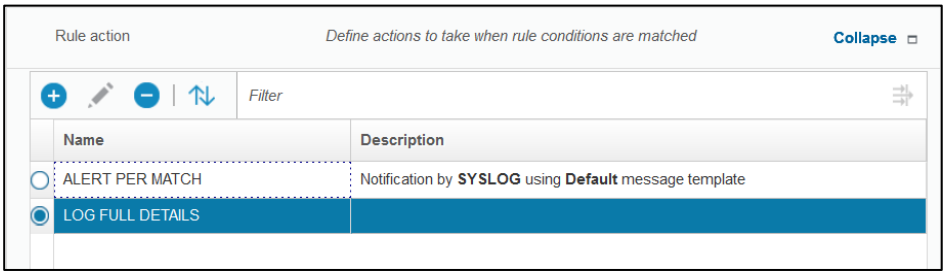


Click on **Edit**  by the **Sensitive Objects** and verify the member of group and click **Close**

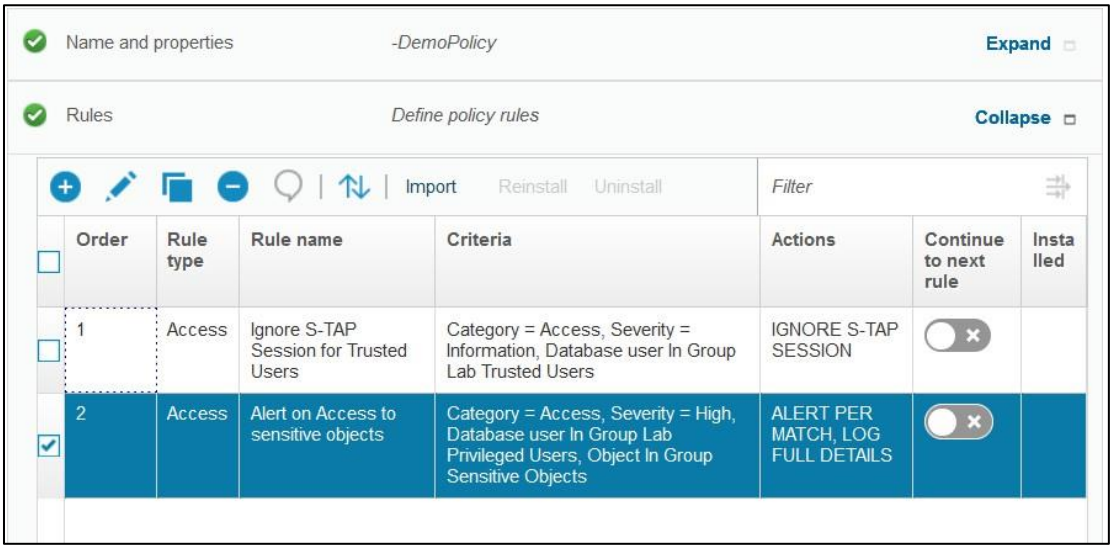


d. Rule Actions

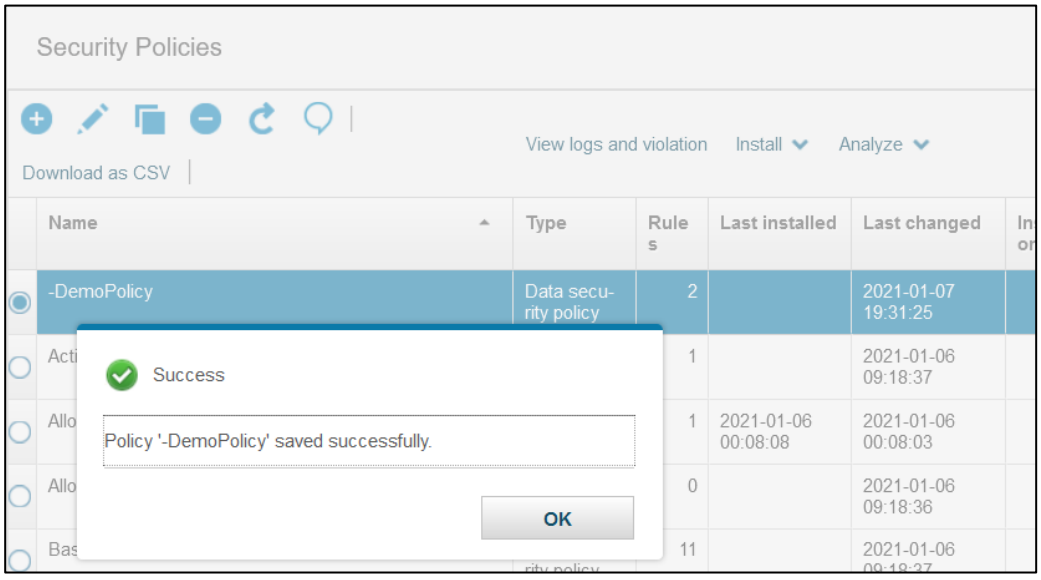
- Action1: **ALERT PER MATCH**, with default message template and SYSLOG as the Notification type.
- Action2: **LOG FULL DETAILS**



24. Scroll down and click **OK**. Now you have two rules in the policy.

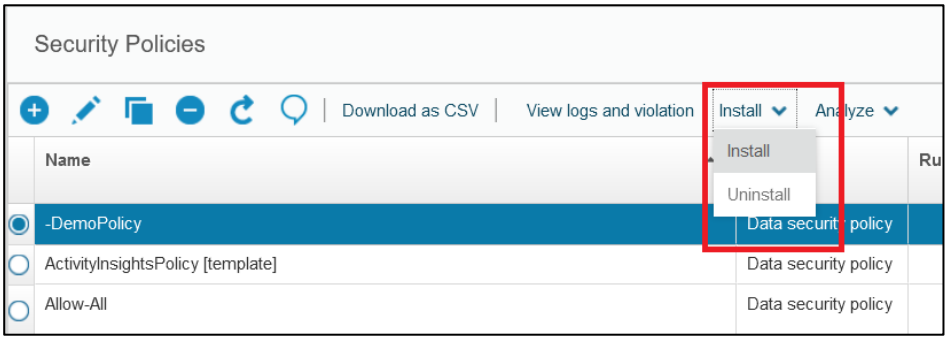


23. To save your policy, return to Security policy pane, scroll down and click

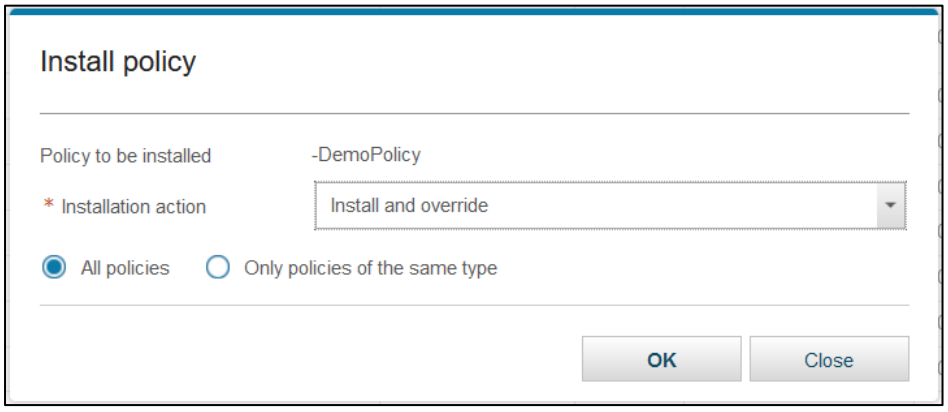


24.To install the new policy you just created.

- Select your new policy, **-Demo Policy**
- From the **Install Menu**, select **Install.**

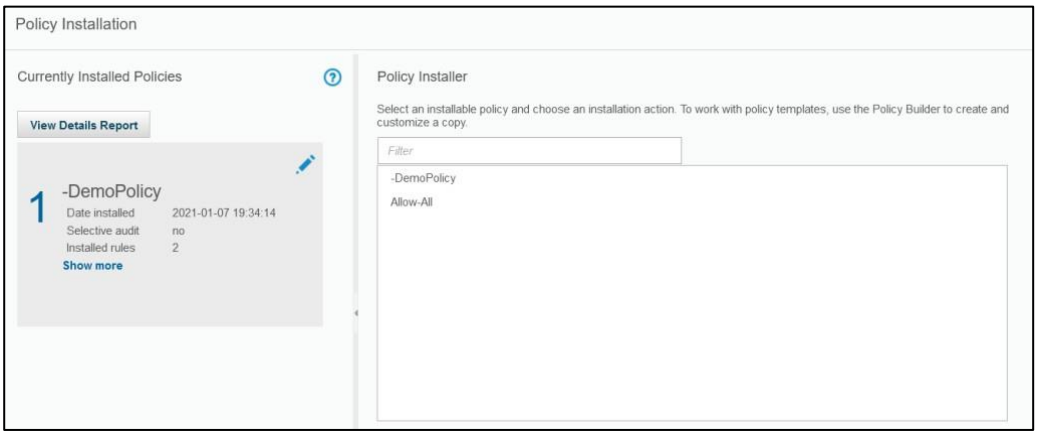


- In the pop-up window, select the Installation action **Install & Override**. Leave **All Policies** selected.



- Click **OK** and close the confirmation message.

25.The policy is installed, To verify, go to **Protect > Security Policies > Policy.**

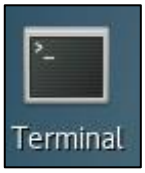


Exercise 2: Test your new Policy

Now you generate some data, then test your policy and review your results. You start with the privileged users rule and generate some data. You access the tables: CC, CREDITCARD, PATIENT, and SSN as users JOE and JOAN. JOE and JOAN are both members of the privileged users group.

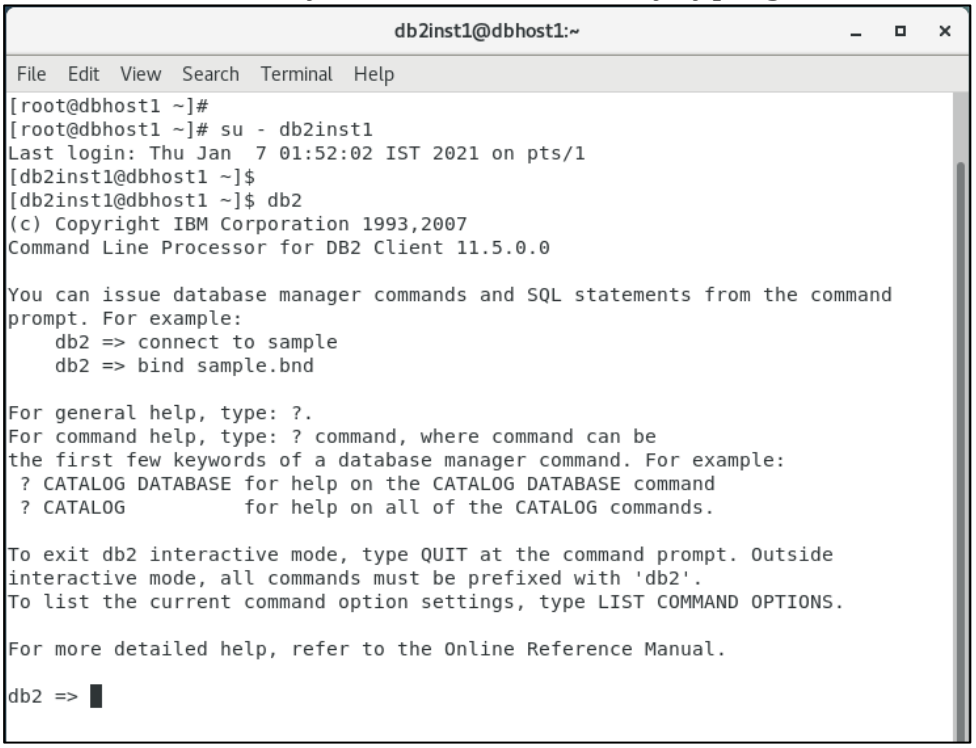
Follow the below steps.

1. Login on the Database Server "DBHost1" using root user. Click the **Terminal** Icon on Desktop.



2. Change to the user **db2inst1** using the command, *su – db2inst1.*

3. Initiate a shared memory connection to DB2 by typing, run *db2.*



4. Run the following commands in the Db2 command environment.

   connect to sample user joe using guardium select * from db2inst1.patient

   select * from db2inst1.cc

   select * from db2inst1.creditcard select * from db2inst1.ssn

   connect to sample user joan using guardium
   select * from db2inst1.patient

   select * from db2inst1.cc

   select * from db2inst1.creditcard select * from db2inst1.ssn

5. In your Guardium GUI, go to **Reports > Real-Time Guardium Operational Reports > Incident Management**.
   You see policy violations for privileged users (JOE and JOAN) accessing database tables in sensitive objects. You might need to wait a few minutes for some results to appear.

You see that the access to the SSN and PATIENT tables result in violations, but the access to the CC and CREDITCARD tables do not. That is because the SSN and PATIENT match objects in the Sensitive

Objects groups.

Practical -8

Task 8: Reports and Queries

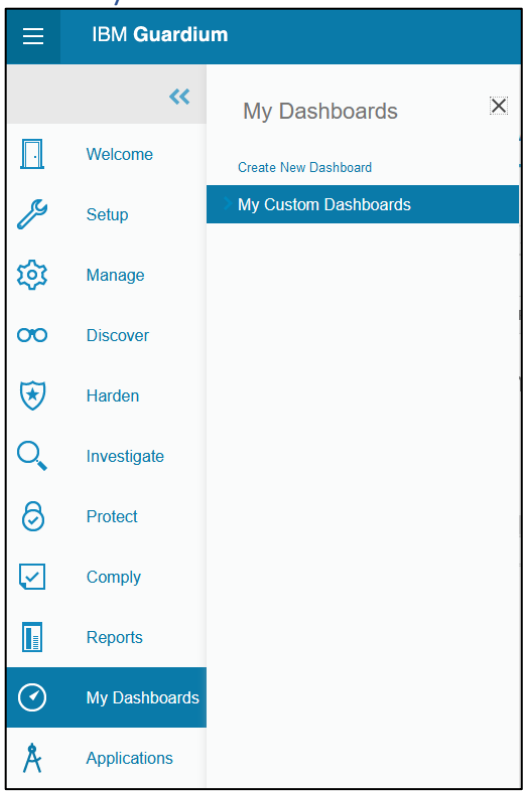
In this lab, you will learn about custom reports and queries.

Exercise 1: Creating a simple query and report

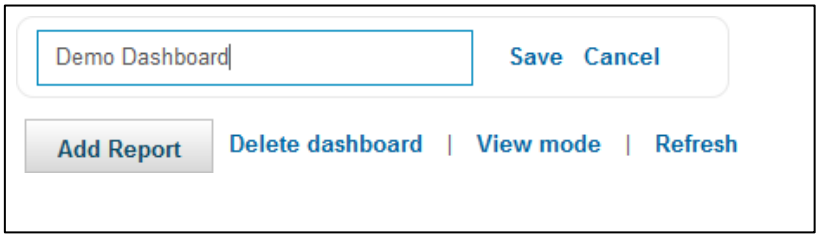
In this exercise, we will create our own console tab to display our report. And create a simple query and a report that uses that query.

Query – Details of sessions opened by -Trusted Users

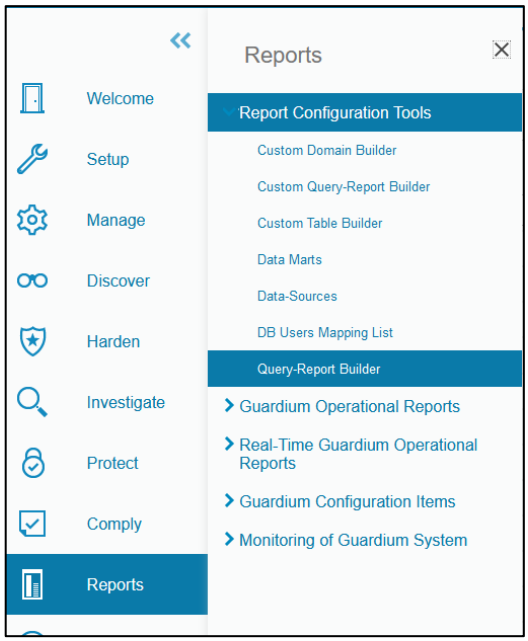
1. Open Firefox browser on the database server, and login to **https://10.10.9.141:8443** with user *lab* and password *guardium*
2. Create a new dashboard to hold or display the report.
   a. Go to My Dashboards > Create New Dashboard



   b. To edit the dashboard, click the **Edit** icon. Rename the dashboard to *Demo Dashboard* and then click **Save**.

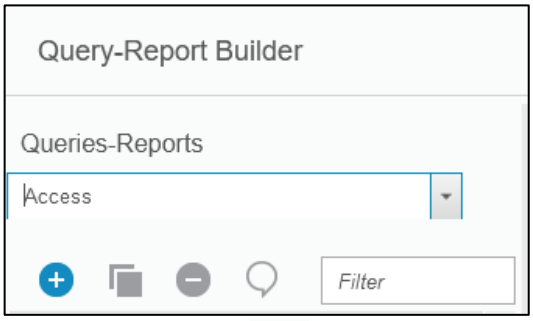


3. Create the query for the report to use. The query specifies what information is to be retrieved from the Guardium database and how it is displayed.
   a. Go to Reports > Report Configuration Tools > Query-



   Report Builder.

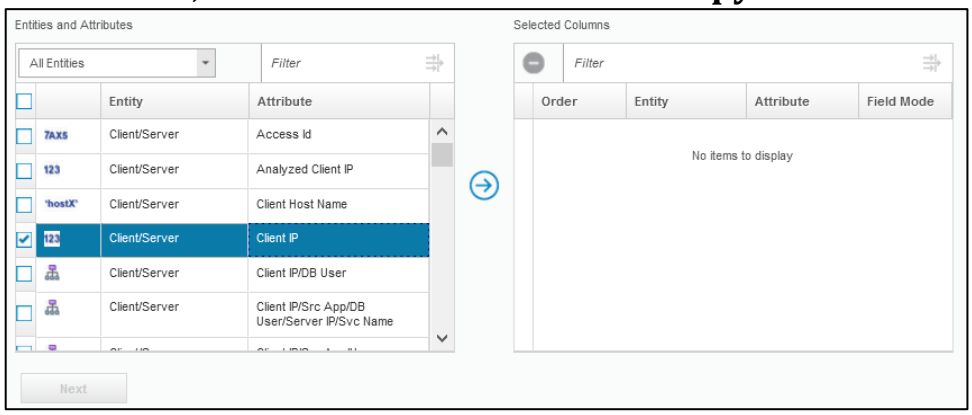
   b. Select Domain **Access**.



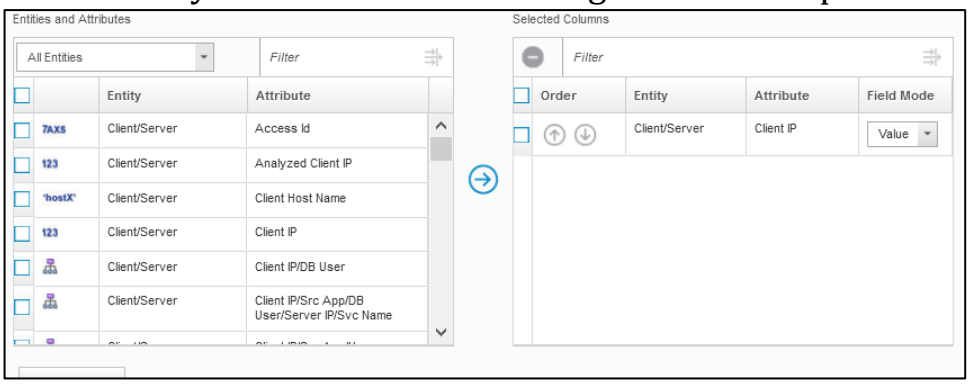
   c. Click the **Create** Icon, The New Query wizard opens.
   d. In the New query wizard sections, Enter below values.
      i. Query Name: **- Trusted Sessions**
      ii. May Entity: **Session**

   e. Click **Next**.

4. You choose the entities from the Entity list at the left side of the panel to add to the query filed.
   a. In the Table, select **Client IP** and click the **Copy** icon.



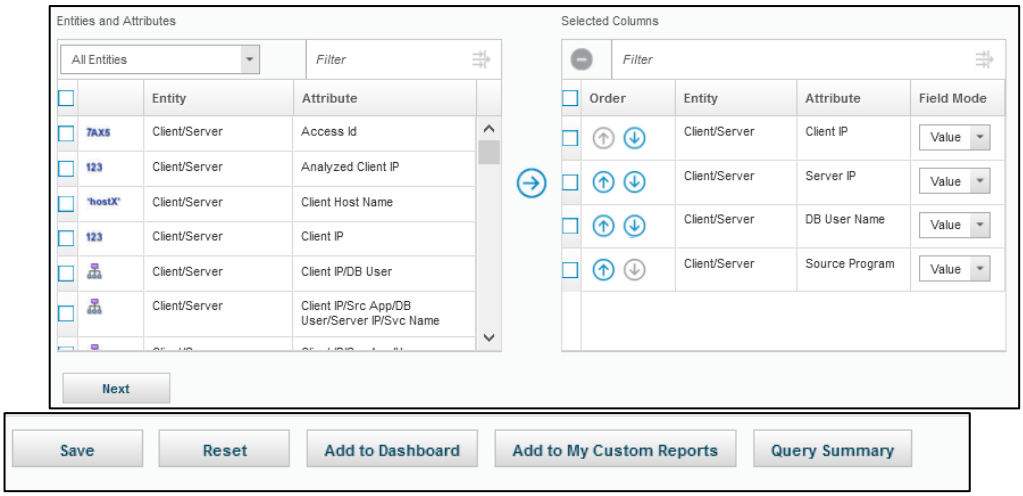
   b. The entity will be transferred to right side of the panel.



   c. Continue the same process to select
      i. Server IP
      ii. DB User name
      iii. Source Program

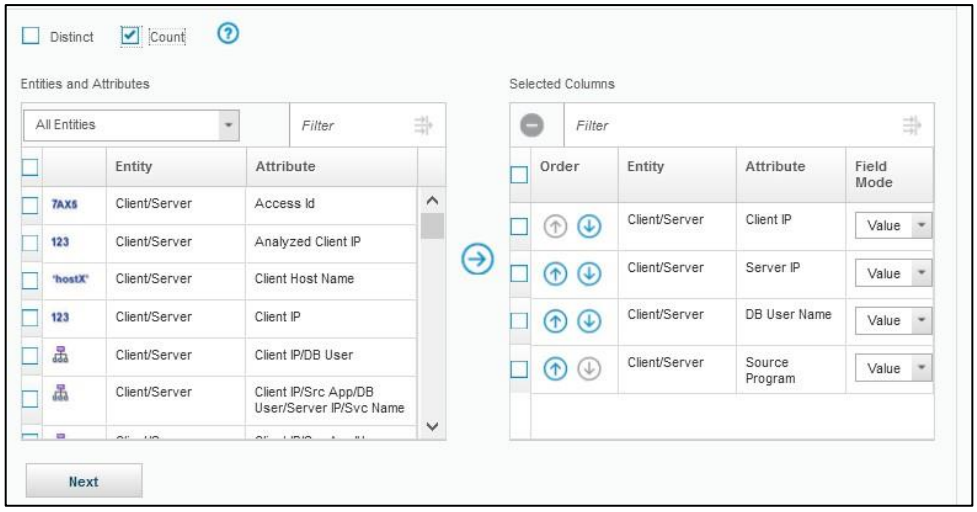
When you finished, the query builder contains four entities in the select columns table.

   d. Scroll down and click **Save** so that you do not lose your work.

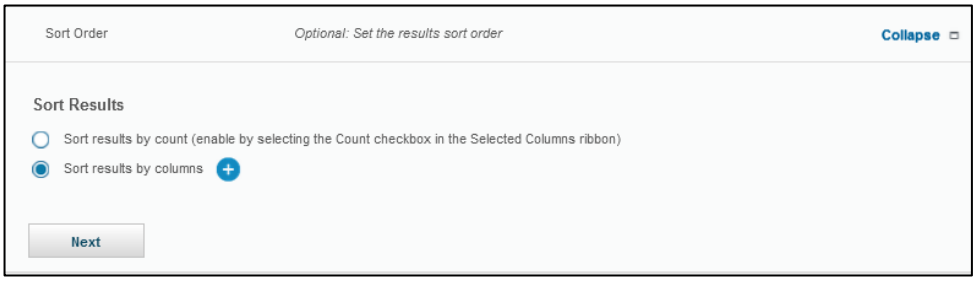


e. You can use the Blue arrows to put the fields in the current sequence. 

f. Rather than putting the individual rows for each similar session, it is recommended to put Count option, which display counts of the similar sessions. For doing so, Select **Count** checkbox.



g. To display the sort order, click **Next**.



h. Select **Sort results by columns** and then click the **Create** Icon.

i. For the drop-down list, select **Client IP** and to sort the data in ascending order, select **Ascending**

j. To add another sort entity, click the **Create** icon. Select **DB User name**
and **Ascending**.

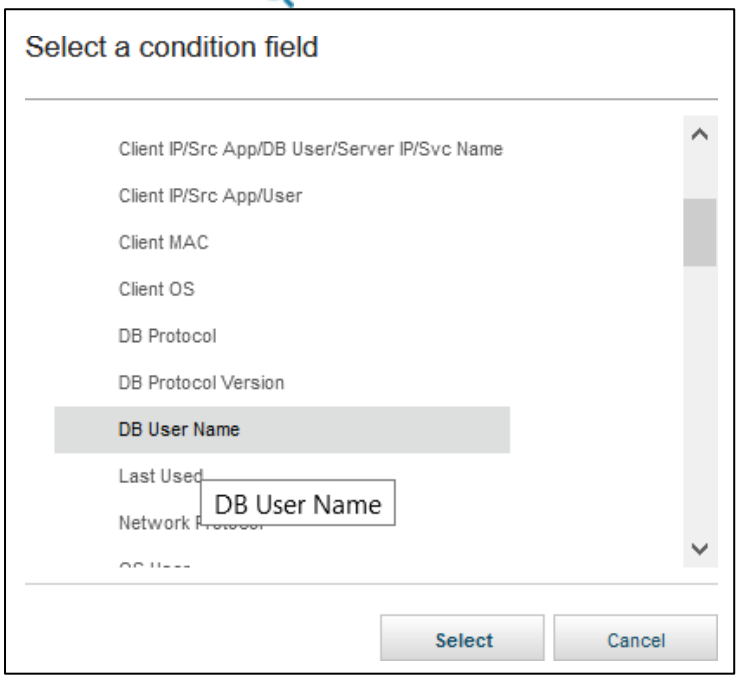
k. To move to the condition section, click **Next**.

5. Add conditions to the query. It controls the information to be displayed in the report.

a. To add a condition, click the **Add condition** icon.

b.

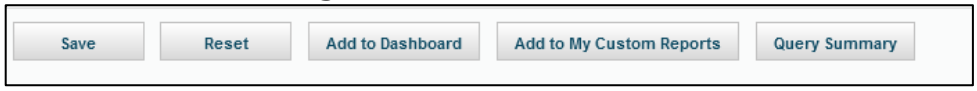
c. Expand **Client/Server**, select **DB User Name**, click **Select**. Click the **search** icon.

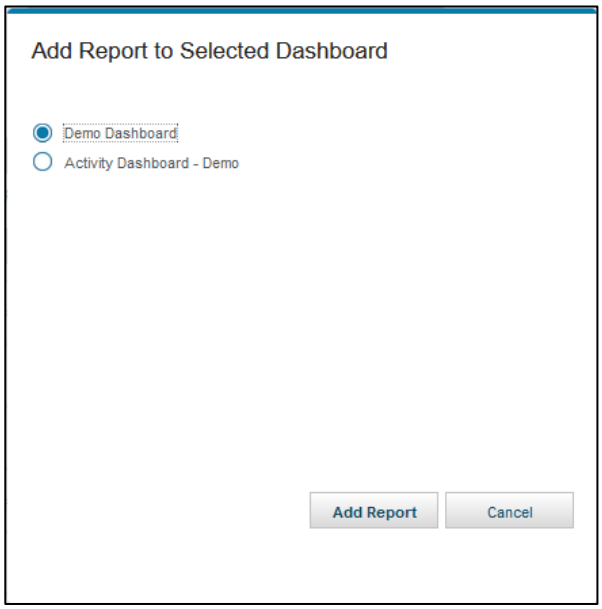


d. Select the **IN GROUP** operation and the **Lab Privileged Users** runtime parameter.

e. **Save** your work.

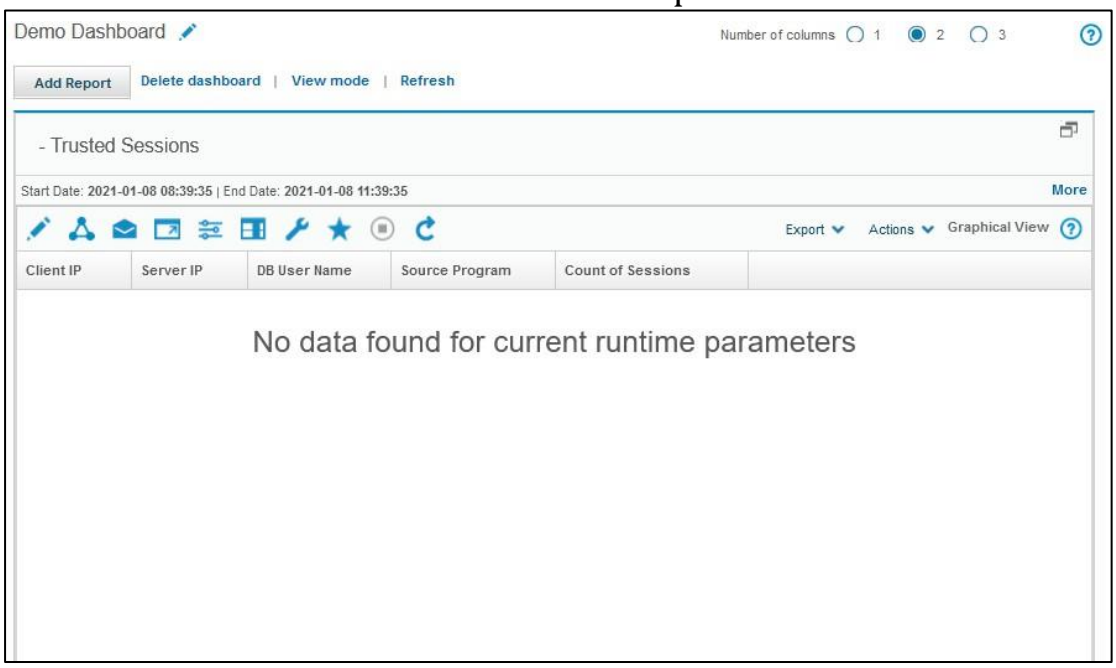
f. Click **Add to My Custom Report**. and click **No** on the confirmation message.





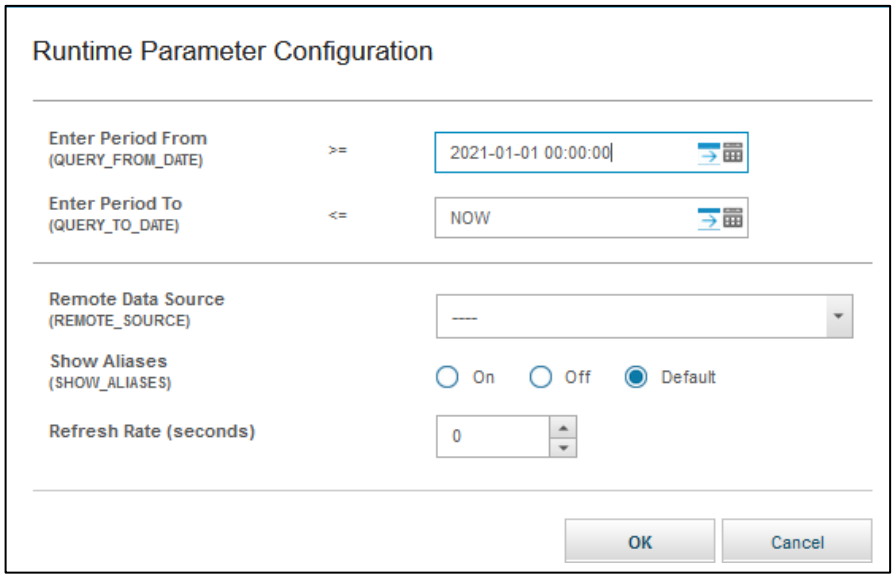
g. Click **Add to Dashboard**.
h. Select your dashboard and click **Add Report** created in Step 1.

6. Go to My Dashboards > My Custom Dashboards > Demo Dashboard.
7. Click on icon to maximize the size of report.

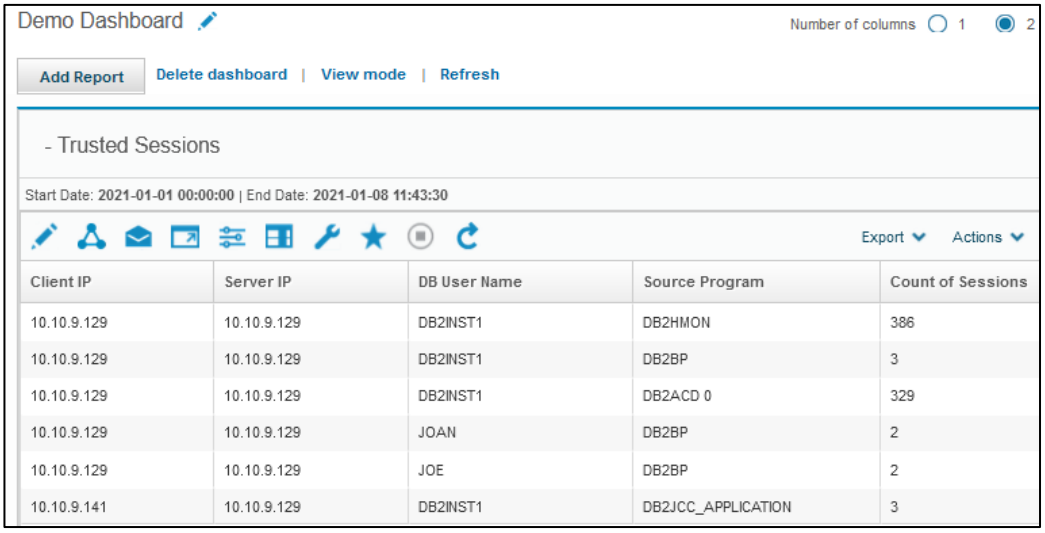


8. You might see no data in your report. If there is no data, try below steps.
   a. Click **Edit Mode**.
   b. Click the **Configure** icon.

c. Use the calendar icon Chan the **Enter Period From** field to *1 January 2021* and click **OK**.



d. No there should be data in your report.



Client IP	Server IP	DB User Name	Source Program	Count of Sessions
10.10.9.129	10.10.9.129	DB2INST1	DB2HMON	386
10.10.9.129	10.10.9.129	DB2INST1	DB2BP	3
10.10.9.129	10.10.9.129	DB2INST1	DB2ACD 0	329
10.10.9.129	10.10.9.129	JOAN	DB2BP	2
10.10.9.129	10.10.9.129	JOE	DB2BP	2
10.10.9.141	10.10.9.129	DB2INST1	DB2JCC_APPLICATION	3

Practical -9

Task 9: Reports and Queries

In this lab, you will learn about custom reports and queries.

Creating a query and report with drill-down capabilities

In this exercise, you will create a more detailed report of accessed objects in each sessions in - Trusted Sessions report in last exercise.

1. Go to **Reports > Report Configuration Tools > Query Report Builder** and create a new query with domain **Access** and main entity of type **Object**.
   Name: -*Accessed Database Object*
2. Add the Following attributes from Client/Sever Entity.
   a. **Client/Server**: Server IP
   b. **Client/Server**: Client IP
   c. **Client/Server**: DB User Name
   d. **Client/Server**: Service Name
   e. **Client/Server**: Source Program
   f. **Command**: SQL Verb
   g. **Object**: Object Name
   h. **Count** Selected
3. Add two conditions. You link these conditions with an **AND**, so both conditions must be met.
   a. Add attribute **DB User Name** from the **Client/Server** folder of the entity list, with Operator set to **LIKE**, runtime parameter set to **Parameter**, and parameter value set to **DBUser**.
   b. Add attribute **ClientIP** from the **Client/Server** folder of the entity list, with Operator set to **LIKE**, runtime parameter set **Parameter**, and parameter value set to **ClientIP**.
4. Save the Report and add it your dashboard.
5. You might see no data in your report. If there is no data, try below steps.

a. Click the **Configure** icon.

b. Use the calendar icon Chan the Enter Period From field to 1 January 2021 and click OK.

6. On the -Trusted Sessions report, right-click one of the entries under DB User Name. A pop-up window opens with a list of drill-down reports.

7. Select **-Accessed Database Objects.** A new window will open with -Accessed Database Objects report with entries only for the select session

Practical -10

Task 10: Minimal Access Role

How to create a role with minimal access

This topic explains how to create a new role with minimal access permissions, for

example an auditor role that can only access the Audit Process To-Do List and view

specific reports.

Procedure

1. Create a new role.

a. Log in as accessmgr, navigate to Access > Access Management, and select the Role Browser.

b. Click the Add Role button, give the role a name, and click the Add Role button to create the new role.

2. Manage permissions so the new role can only access the Audit Process To-Do List and the Report Builder (which is required for viewing reports).

a. From the Role Browser, click the Manage Permissions link for the new role.

b. Select the checkbox in the header of the Accessible Items list and use the arrow to move all items to the Inaccessible Items list.

When creating a highly restricted role, it is easier to begin by removing

permissions.

c. In the Inaccessible items list, select the Audit Process To-Do List and

the Report Builder, and use the arrow to move them back to

the Accessible items list.

The new role now has access to only these two specific applications.

d. Click the OK button to commit your changes.

3. Customize the menus and navigation by defining which reports and applications are available to the new role.

a. From the Role Browser, click the Customize Navigation Menu link for the new role.

b. In the Navigation Menu list, select the Reports group so it is highlighted. The selected group acts as the destination for menu items added in subsequent steps.

c. In the Available Tools and Reports list, expand the Reports section or use the Filter to identify specific reports, select the check box next to each item that should be available to the new role, and use the arrow to add the items to the Navigation Menu list.

Items moved into the Navigation Menu list will become visible to users assigned to this role.

d. In the Navigation Menu list, remove access to the Report Builder by clicking the icons next to the Reports > Report Configuration Tools and Investigate groups.

This further simplifies the menu structure for this role and removes access to the Report Builder tool without also removing application permissions that are required to access reports.

e. Click the OK button to commit your changes.

You have now created a new role with very minimal privileges that can be assigned to users.

4. Optionally specify a custom home page for the new role.

a. From the Role Browser, click the Customize Navigation Menu link for the new role.

b. In the Navigation Menu list, specify a new default home page by

selecting Comply > Tools and Views > Audit Process To-Do List and clicking the icon in the toolbar.

Users assigned to this role will now see the Audit Process To-Do List as the default screen after logging in.

c. Click the OK button to commit your changes.

5. Create a new user and add that user to the new role.

a. Navigate to Access > Access Management and select User Browser.

b. Click Add User, provide the required information, and click Add User to create the new user.

You will now see the user you created listed in the User Browser.

When a new user is created, the account is disabled by default. Deselect the Disabled check box if you want the user to have immediate access to their account.

c. From the User Browser, click the Roles link for the new user to view a list of available roles.

d. Select the Assign check box next to the custom role you created earlier.

This will assign the user to the new role.

e. Deselect the Assign check box next to the user role.

Deselecting the user role prevents the new user from inheriting the default user access and permissions.

f. Click Save to commit your changes.