Use data-level security for granular access control of auditing results in InfoSphere Guardium

Ensure separation of duties based on the originating data source

Tansel Zenginler
Kathryn Zeidenstein

February 21, 2013

IBM® InfoSphere® Guardium® offers enterprise-wide data activity monitoring for data protection and auditing. Two critical elements to consider for a successful enterprise implementation of InfoSphere Guardium for enterprise-wide data protection and audit include support for separation of duties, and enterprise deployment capabilities that eliminate redundant configurations and streamline enterprise deployments to match your organizational structures. By using Guardium data-level security mechanisms, administrators can assign responsibilities for particular databases or systems to individuals (or groups) which aligns with their hierarchical organizational structure. This article describes the benefits of data-level security as well as step-by-step instructions for implementing the solution for a sample scenario.

The importance of data-level security for separation of duties

Organizations who handle data need to be concerned with complying with varying degrees of enforcement of separation of duties. This means ensuring that tasks cannot be complete without the involvement and review of multiple people, as there is less likelihood of fraud and human error. This is why typical audit processes require the review and sign-off of multiple people to act as a checks and balance system.

With regard to data, a similar concept is to ensure that people have access to data only to the extent that they need to complete their jobs. In other words, there is no reason for a customer support representative to see customer social security numbers, or for a department manager to see the payroll data for a peer manager's team. This problem is why some database vendors have implemented more granular security options such as DB2 row and column access control, or Oracle Virtual Private Databases.

InfoSphere Guardium, which is an enterprise-wide data activity monitoring and auditing solution, also supports an infrastructure for separation of duties by role and by data. In other words, with InfoSphere Guardium, you can model your organizational roles and hierarchy in the system,
and automatically filter audit data as appropriate for the role. This is a key element to ensure efficiency and eliminate redundancy with enterprise deployments because you don't have to change your processes in order to seamlessly incorporate database activity monitoring into your audit processes.

Defining the stakeholders and their responsibilities enforces separation of duties, but more importantly, it simplifies the process of creating and updating audit reports, removing the need to create separate audit reports for different stakeholders. This is especially important for large environments with multiple stakeholders. Consider the scenarios of personnel changes, changes in responsibilities, and consolidations. By defining your organizational structure, all you need to do is specify the new responsibilities and the audit process remains intact. There is no need to update all of your audit reports and workflows. This is a hidden cost that could be the difference between a successful implementation versus a costly ongoing operation requiring more resources than originally anticipated.

This article will describe in more detail how Guardium data-level security works and then, using an example scenario, show it in action.

**Understanding data-level access controls in InfoSphere Guardium**

**Users and roles**

In the Guardium system, defining and modifying users involves deciding who will be using the Guardium system, and to what roles they will be assigned. Guardium uses security roles to control access to the solution components and application (reports, alerts, audit process definitions, and so on). When a security role is assigned to any of its components, only those Guardium users who are also assigned that security role can access that component. A security role can thus be viewed as a group of Guardium users, all of whom have the same access privileges.

**Compliance workflows**

The IBM InfoSphere Guardium Compliance Workflow Automation application streamlines the entire compliance workflow process, helping to 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. All of this information is available for your audit reports, which helps strengthen the security of your internal processes.

A compliance workflow enables you to bundle a set of reports, classify (automatic location of sensitive data) jobs or Vulnerability Assessment (VA) runs, and schedule their delivery to specified recipients. As shown in Figure 1, individuals to whom actions have been assigned are notified of specific actions required on their part as the workflow process is executed, using automatic email notification as well as updates of the To-Do list on their InfoSphere Guardium web interface.
In addition, InfoSphere Guardium manages the distribution status automatically by keeping track of which recipients have reviewed or signed off. All required actions can be securely executed through the web interface, including reviewing results, providing approvals, commenting, and escalating an action.

Actions are executed on a line-item basis, allowing rapid but thorough review, and ensuring processes are not blocked by individual line items requiring investigation. For example, an individual receiving a daily PCI DSS exception report may find that it contains five incidents, four of which were caused by a known issue that has been resolved. Those four line items can quickly be marked as reviewed and approved, while the fifth item will not be approved until the incident is investigated and resolved. The four approved items will proceed to the next step in the workflow process immediately, with the fifth proceeding subsequently. Comments, such as those indicating which remediation actions have been taken, can also be added on a line item basis.

**User hierarchies and user-database associations**

Guardium supports separation of duties by enabling administrators to assign responsibilities for particular databases or systems to users and their hierarchical management.

- The **data security user hierarchy** defines the organizational management tree. Managers can optionally inherit the view of data assigned to managed personnel.
- The **user-database association** is how particular users are assigned particular database servers (by database name and IP). That user will only see audits for assigned servers. This aligns very well with enterprise organizational structures that support lines of business from a centralized IT department.

As was previously mentioned, by implementing data-level security, a single report can be distributed to different users for their review. Each user will see the part that he or she is responsible for.

**Overview of the scenario**

A simple example illustrates the benefits of data-level security. Assume that Sample Company would like to create a generic report designed for reviewing database activities. A critical requirement is to ensure that DBAs are only reviewing activity reports for the databases they are responsible for. This is not just to enforce separation of duties, but also to help focus DBA efforts on their direct responsibilities by filtering out information that is not relevant to them.

As shown in Figure 2, the DB2 DBA (a member of the DBA group who was granted InfoSphere Guardium rights for all DB2 databases) will only see activity reports related to DB2 databases,
while the Oracle DBA who was granted rights to the Oracle database activity reports, will only see those results.

**Figure 2. Sample company organizational structure for audit purposes**

![Organizational Structure Diagram](image)

The MySQL DBA is granted rights to see the MySQL database activity reports. In this scenario, the DBA group manager is responsible for all database administrators, and is allowed to see all database activity reports.

There is also an auditing department responsible for internal audits. In the auditors group, the SOX auditor is responsible for the financial data such as sales, salaries, and orders, no matter where that data is stored. The HIPAA auditor audits data related to patient information, no matter where that data is stored.

The following section will show you how to set up this environment.

**Enable data-level security**

The Data Level Security feature can be easily configured through IBM InfoSphere Guardium web console.

1. Log in as an administration user. Click the **Administration Console**, click **Configuration** and then select **Global Profile**, as shown in Figure 3.
2. Scroll down the Global Profile until you find the **Data level security option**.

3. Click **Enable**. The **Data level security filtering** will be selected, as shown in Figure 4.

The following discusses a couple of other related items on this Global Profile screen.

- The **Default filtering** option has two separate check boxes with the following values:
  - **Show all** is used only with a special data security exempt role, which means that the person with this role will always see all data in the reports.
  - **Include indirect records** is a way to turn on the global default that enables users higher in the hierarchy to see report data for people lower in the hierarchy. You will not turn this on for now. You will learn how to use that option on individual reports.

- The **Escalate results to all users** check box pertains to compliance workflow processes. Enabling this feature means that someone who is a receiver in a compliance task flow can escalate that to any other user, not just their manager (or another user above them in the hierarchy). If you are using data-level security filtering, those settings will be honored, which means that another user may or may not have authority to see the data in the tasks reports. If this box remains cleared, they can only escalate to someone higher in their hierarchy.
Define users and roles

The management of users and roles within the Guardium system is usually reserved for the access manager account to help enforce separation of duties within the Guardium environment. This is the Guardium user that is assigned the **accessmgr** user name. Defining and modifying users involves deciding both who will be using the Guardium system and to what roles they will be assigned. A role is a group of users, all of whom are granted the same access privileges.

The scenario mentioned previously can be created by the access manager using the Guardium web user interface, as follows.

1. Log in to Guardium as **accessmgr**.
2. Click the **Access Management** tab.
3. Click the **Add User** button, as shown in Figure 5.
   - Guardium can also import from your existing Active Directory or LDAP directory to provide user access and definitions.

![Figure 5. User browser in Guardium](image)

4. This brings up the form in which you can add users. Click **Add User** when you have finished entering each user, as shown in Figure 6.

![Figure 6. Use global profile configuration to enable data-level security](image)

In the organization shown previously in Figure 2, there are two departments with seven users. Each user can be created using the simple procedure described previously. The end result will look similar to what is shown in Figure 7.
Create the user hierarchy

As with users and roles, the management of user hierarchy is reserved for the access manager. Defining and modifying the user hierarchy involves deciding who will be reporting to whom (the hierarchy), and who will need which data.

With the user hierarchy information, the access manager can define the hierarchical order between the users as follows.

1. Log in to the Guardium user interface as accessmgr.
2. Click the Data Security tab.
3. From the left navigation, click User Hierarchy, which brings up the portlet shown in Figure 8.

   Figure 8. User hierarchy - first screen

4. Use the pull-down menus to select the DBA manager. This will bring up another panel on the right.
5. Right-click the DBA manager, and select Add user to add users to that specific manager, as shown in Figure 9.
Figure 9. Adding users under the DBA manager

Note: You need to create the hierarchy from the top down.

In your Sample Company, the audit manager is responsible for all auditors. The structure is the same for the DBA department, in which all DBAs report to a DBA manager, as shown in Figure 10.

Figure 10. Auditor and DBA hierarchy

Create the association between users and database servers

The Data Security user-to-database association represents the relationships between users and instances (databases), and enforces the data-level security for users at the instance level, permitting only specified users to look at specific servers and databases. To create this association, do the following.

1. Log in to the Guardium user interface as accessmgr.
2. Click the Data Security tab.
3. Click User-DB Association from the left navigation, which brings up the portlet shown in Figure 11.
Figure 11. Select one or more sources to provide data server suggestions

You can have Guardium look for Server & Service Names (databases) from one or more of the following sources.

- **Observed Accesses**: The Server & Service Name is picked from data that InfoSphere Guardium has collected. Because this option does not require the existence of an S-TAP (a monitoring agent on the database server), it can be used, for example, on an aggregator appliance.

- **Datasource Definitions**: This option looks at existing datasource definitions in the Guardium system. You may have such a list for any activities that require data sources, such as vulnerability assessments or data classification.

- **S-TAP Definitions**: This option looks at database information associated with S-TAPs that are installed and configured. Even if an S-TAP is not actively collecting data, the database information can be pulled from this.

- **Auto-Discovered Hosts**: This option relies on database information that was returned from the database discovery capability in InfoSphere Guardium.

- **GIM-Discovered Systems**: This option relies on information that was returned from the Guardium Installation Manager (GIM) discovery.

4. Click on the suggestions sources you want to use and then click Go.

5. Guardium will bring up a tree structure of IP addresses and instance names for your databases. Right click on any of the appropriate nodes to associate a user with that database or with all databases included in the node. For example, Figure 12 shows **DB2INST1** selected.
6. As shown in Figure 13, the SOX auditor and the DB2DBA are associated to this server.

**Figure 13. Users associated with DB2INST1**

7. When you are done adding users, click on the **Full Update Active User-DB Association Map** button.

To validate your work, you can use Guardium reports (in the left navigation of the Data Security tab) to see the relations you just created, or to see where there are no associations defined. One such report called **Servers Associated**, is shown in Figure 14.
Use data-level security for granular access control of auditing results in InfoSphere Guardium

Figure 14. Associations between users and servers

Since, by default, the Global Profile does not include indirect access records, none of the auditing managers has direct access to any database auditing data.

The Data Security User to Database Association filters reports from the Access, Exception, and Policy Violations domains. All other domains (reports) are not filtered by the Data Security User to Database Association.

Filtering in action: Report results

Now check to see if data-level security was successfully configured. If all is well, users can see the activities for the data sources for which they are directly associated. In addition, by selecting the Include indirect records check box on a given report, managers can see the data of data servers for those users who report to him or her.

For example, see the pre-defined report called Number of db per type in Figure 15. This report is available from the initial View tab when you log in as a user.

Figure 15. Audit manager sees no records because indirect records not included

In this example, the audit manager has not selected the Include indirect records check box. If you recall from Figure 14, the audit manager has no direct access and thus will not see any data by default.
However, as shown in Figure 16, the same report with the **Include indirect records** option is selected, and the audit manager can now see information from the databases that the SOX and HIPAA auditors are associated with.

**Figure 16. Audit manager sees records from her staff**

Let's look at another example. A typical report used by DBAs is the **Throughput** report, which is available when you log on as a user.

Click the **View** tab, and then select **Performance > Throughput (Graphical)** from the left navigation.

This report produces a count of all Server IPs seen, and total accesses during the reporting period. At the outermost level, accesses are grouped by the Period Start time from the Access Period entity, which is usually one hour, on the hour.

As shown in Figure 17, the DBA manager cannot see any activity because he does not have any direct responsibility on databases.

**Figure 17. DBA manager sees no records because indirect records not included**

However, if the DBA manager wants to review the reports for his team, then he must select the **Include indirect records** check box, and then he can see the results, as shown in Figure 18.
Figure 18. DBA manager sees records from staff members

Filtering in action: Workflow results

Last but not least, the data-level security applies also to reports that are routed through compliance workflows. In this section, you will see how a single data server access report can be routed to different users for review and sign-off, and how those users will see only the information for data sources for which they are responsible. In addition, by selecting the Include indirect records check box on a given report, managers can see the data of data servers for those users who report to him or her.

To create a workflow do the following.

1. Log in to the Guardium user interface as admin.
2. Click Audit Process Builder under the Tools tab, as shown in Figure 19.
3. Click New.
4. Create an audit process definition called DB Server List.
5. Add the receivers of this audit process: **DBAManager**, **DB2DBA**, and **OracleDBA**. Figure 20 shows what this looks like when complete.

**Figure 20. Receiver table for receiving and reviewing the report**

6. Below the receivers table in the Audit Process Builder, you will see where you can create a task for this new process. In this case, you want to send the DB Server List report to your DBAs. Enter a description for the task, and then select the **Report** radio button to activate the fields that let you fill in the report name and other parameters for the report. Figure 21 shows you what your Audit Task definition looks like.

**Figure 21. Completed audit process task**

7. **Save** and then **Run** the audit process.
8. Now **OracleDBA**, **DB2DBA** and **DBAManager** can log in to Guardium and see the reports in their To-Do lists, as shown in Figure 22.
Use data-level security for granular access control of auditing results in InfoSphere Guardium

Figure 22. A To-Do list for a user

When the Oracle DBA views his report, he will see just the information related to the Oracle database, as shown in Figure 23.

Figure 23. Oracle DBA sees his version of report (partial)

When the DB2 DBA views her report, she will see just the information related to her DB2 database, as shown in Figure 24.

Figure 24. DB2 sees her version of report

Finally, when the database manager views his report, if he did not select the Include indirect records check box, he will not see any results, as shown in Figure 25.

Figure 25. DBA manager sees no data

The database manager needs to select the Include indirect records check box to see all of the records for his staff, as shown in Figure 26.
Conclusion

InfoSphere Guardium provides a data security and compliance solution that supports separation of duties while at the same time eliminating redundant configurations and enabling organizations to streamline enterprise deployments. As you have seen by reading this article, it is possible to automate process flows required for your compliance mandates. The ability to apply data-level security and user hierarchies enables the audit data to be tailored automatically and appropriately for the receiver without the need to create separate reports and processes for individual users.

Acknowledgements

The authors would like to thank Joe DiPietro for his review and support.
Related topics

- Visit the [InfoSphere Guardium web site](https://www.ibm.com/developerworks/) for links to white papers, demos, and more.
- Visit the [InfoSphere Guardium Tech Talk page](https://www.ibm.com/developerworks/) for information about past and upcoming InfoSphere Guardium tech talks.
- The [InfoSphere Guardium Information Center](https://www.ibm.com/developerworks/) includes information to help you make the most of the InfoSphere Guardium data activity monitoring solution.
- Watch videos on the [InfoSphere Guardium YouTube channel](https://www.ibm.com/developerworks/), including demos of support for SAP, DB2 for z/OS, and others.
- **Evaluate IBM products** in the way that suits you best: Download a product trial, try a product online, use a product in a cloud environment, or spend a few hours in the [SOA Sandbox](https://www.ibm.com/developerworks/) learning how to implement Service Oriented Architecture efficiently.