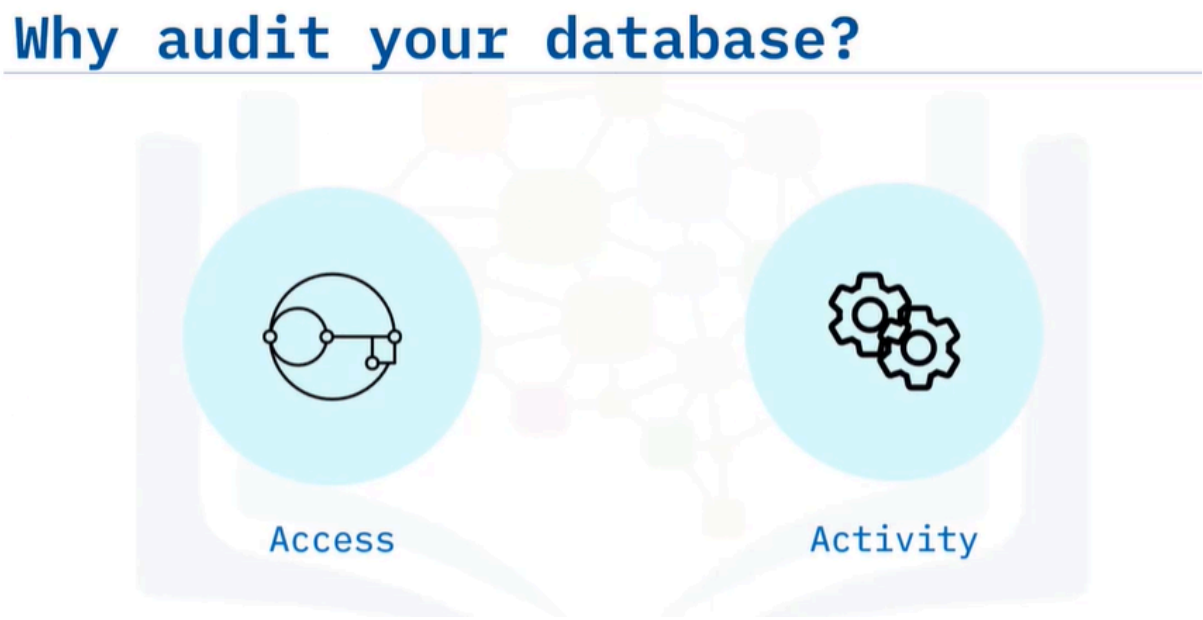
Auditing Database Activity

Sure! Let's talk about the importance of auditing database activity in simple terms.

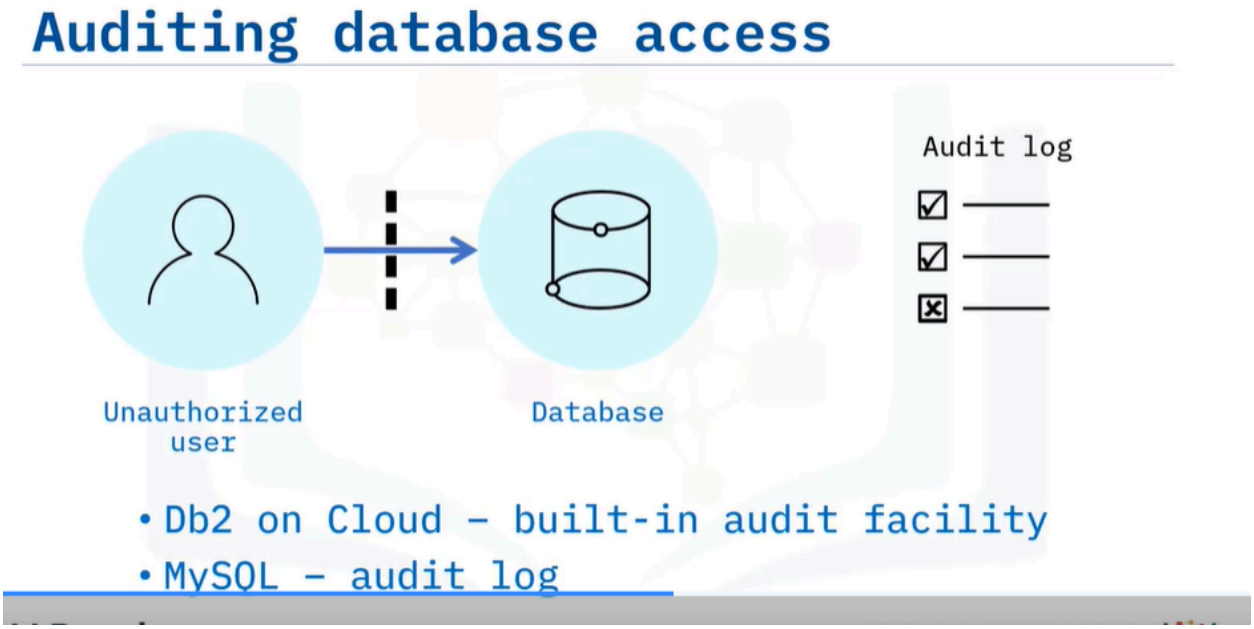
Auditing database activity is like keeping a diary of who visits your house and what they do while they are there. Just as you would want to know if someone unauthorized entered your home, auditing helps you track who accesses your database and what actions they take. This is crucial because it allows you to spot any suspicious behavior or mistakes in how permissions are managed. For example, if someone tries to enter your house but doesn't have the key, you would want to know about those failed attempts to prevent a break-in. Similarly, tracking failed access attempts to your database can help you identify potential security threats.

In practical terms, many database systems have built-in tools that help you log these activities automatically. For instance, if you use a database like MySQL, it can keep a record of when users connect or disconnect. This way, you can review the logs to ensure that everyone is following the rules and that no one is accessing information they shouldn't. Just like a good security system, auditing helps you maintain a safe environment for your data.

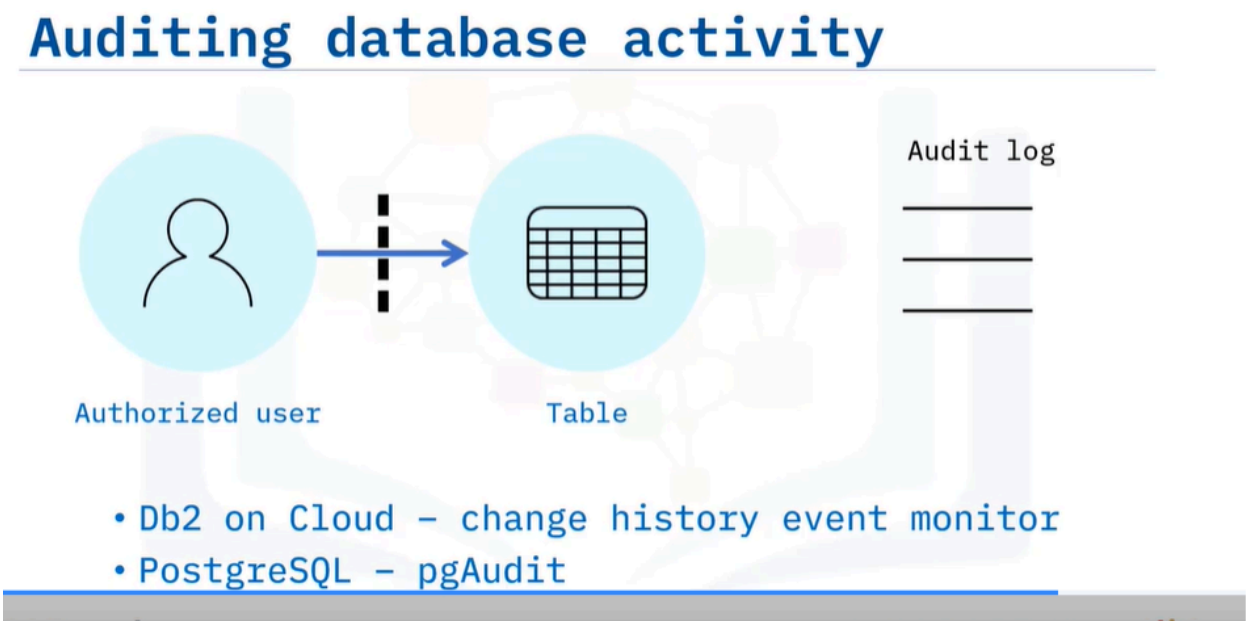


- Even though auditing doesn't directly protect the database, it can help you to identify gaps in your security system and to track errors in privilege administration. In some industries and countries, it is even a requirement to audit access to sensitive data. You should consider implementing auditing in all your database solutions, whether they be on premise or in the cloud.
- Auditing a database involves recording the access and the activity of database users on your database objects.

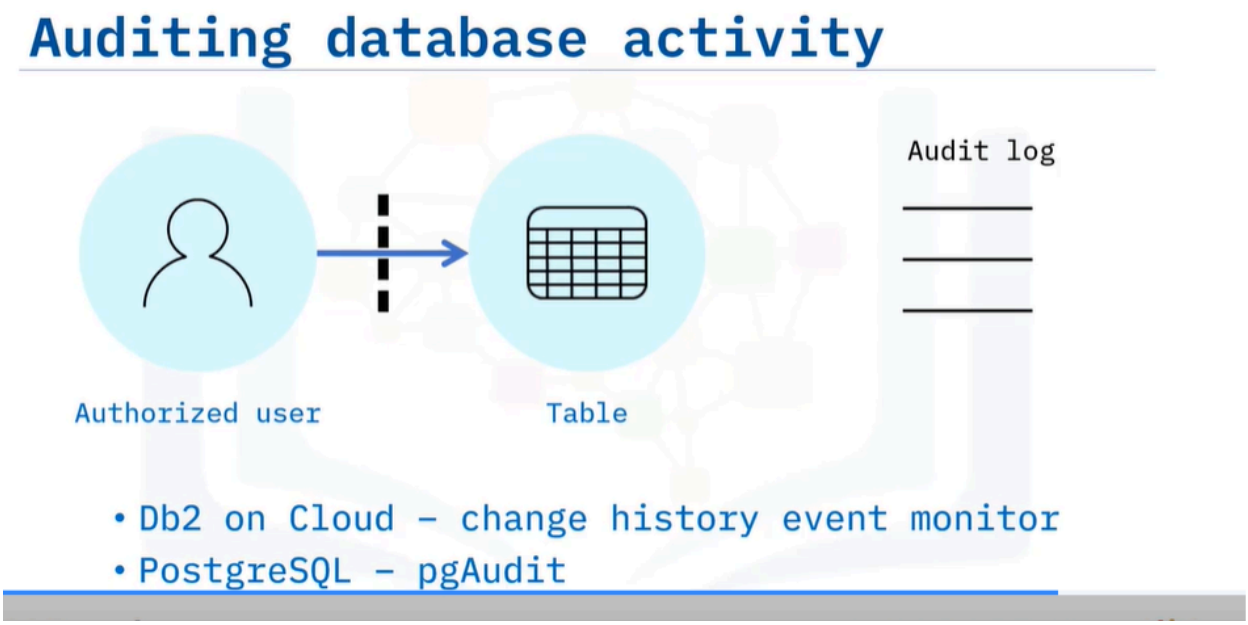
- By reviewing such records, also known as logs, you can identify suspicious activity and quickly respond to any security threats you find.



- If an unauthorized user accesses your database, they have already overcome one or more of the levels of security in your system. Therefore, it is imperative that you track who accesses your database and review the information to identify any unauthorized users.
- You should also track failed attempts to access the database, as these can help you to identify potential attacks, such as brute force attempts, on your system. Most database systems provide functionality that you can use to audit database access. For example, in Db2 on Cloud you can use the user validation category of the built-in audit facility to log user authentication events. In MySQL the audit log plugin tracks connect and disconnect events.



- Sometimes authorized users may find that they can view and edit data that they should not have permissions on. If you track all user activity, you can then use the output reports to review which users are accessing which tables and check whether those actions match your security plans. To audit database activity, some RDBMSs use triggers. These are special stored procedures that automatically log the activity after a DML statement event, such as an insert, occurs. Other systems enable you to attach actions to the events that occur in the database. In Db2 on Cloud you can use the change history event monitor to enable auditing on specific tables or objects. And in Postgres you can use the downloadable pgAudit tool to log individual action types or all actions in a database. You should ensure that whatever auditing implementation you use meets the compliance requirements of your customer or region.



What would happen if auditing is not performed on a database?

If auditing is not performed on a database, several issues can arise:

- **Increased Security Risks**: Without auditing, unauthorized access to sensitive data may go unnoticed. This can lead to data breaches, where attackers exploit vulnerabilities without being detected.
- **Lack of Accountability**: If user activities are not logged, it becomes difficult to hold individuals accountable for their actions. This can result in misuse of privileges or accidental data manipulation without a way to trace back to the responsible party.
- **Compliance Issues**: Many industries have regulations that require auditing of data access and activity. Failing to perform audits can lead to non-compliance, resulting in legal penalties or loss of business.

- **Difficulty in Identifying Errors**: Without logs, it can be challenging to identify and troubleshoot errors or issues within the database. This can lead to prolonged downtime or data loss.
- **Inability to Detect Suspicious Activity**: Regular auditing helps in identifying unusual patterns or behaviors that may indicate a security threat. Without it, potential attacks may go undetected until significant damage is done.

In summary, not performing audits can compromise the security, accountability, and integrity of the database, making it vulnerable to various risks.

What is the main purpose of auditing in databases?

The main purpose of auditing in databases is to **monitor and record user activity** to ensure security, compliance, and accountability. Here are the key objectives:

- **Identify Unauthorized Access**: Auditing helps track who accesses the database and what actions they perform, allowing you to detect any unauthorized users or suspicious activities.
- **Enhance Security**: By reviewing audit logs, you can identify gaps in your security measures and respond to potential threats before they escalate.
- **Ensure Compliance**: Many industries have regulations that require auditing of data access. Auditing helps organizations meet these legal requirements and avoid penalties.
- **Accountability**: Auditing provides a record of user actions, making it easier to hold individuals accountable for their activities within the database.
- **Error Tracking**: It helps in identifying and troubleshooting errors or issues, allowing for quicker resolution and maintaining data integrity.

In summary, auditing is essential for maintaining the security and integrity of database systems while ensuring compliance with regulations.