

Privileged Database User Activity Management

February 19, 2008

Contents

Introduction	2
Database Admin Issues	2
Previous Options	2
Solution	2
Summary	4

Introduction

Many companies are not only facing slew of global regulatory compliance requirements for monitoring database activity of their most privileged users, but also trying to get a better understanding of their most privileged users activity to protect them against any internal threats. This paper highlights several of these challenges and how they can be addressed by a comprehensive database activity auditing solution.

Database Admin Issues

International regulatory compliance requirements such as S-OX, HIPAA, GLBA, PCI-DSS and SB-1386 fundamentally require the management to have a better understanding of who is doing what. In particular, the requirements have shifted the focus from merely understanding who has access to critical information to what activities are being done that might

potentially compromise integrity and security of the data. The only way organizations are going to response to this requirement is by continuous monitoring of database activities, specifically privileged users including DBAs and other administrators, who have direct access to the databases.

Previous Options

Traditionally, privileged users were created to manage and administer the data. Once, the privileged users leave the company their access was simply terminated. Organization didn't spend too much time in auditing the activities of these so called "super-users". As more and more companies realized the importance of protecting the data from internal threat, they are trying to explore the various options to control the activities of the privileged database users.

Solution

It takes time, effort and money to really understand the operational risks posed by the activities of privileged users. However, there are several solution provided by the third-party vendors in the leading database platforms to monitor privileged user activities.

The five-step approach in securing organization's data is to understand:

1) What are the sources of data?

Unless the organization understands what they are trying to

protect - Any solution that is put in place, no matter how cool the technology - is not going to be effective. In particular, Organization doesn't need to spend time and effort to protect all the data that's stored within the IT department which might unnecessarily shift the focus from protecting the most important and critical data to terabytes of redundant data stored in the data centers. **Understand the big picture.**

2) Categorizing the database on the risk factor

Categorization of data based on the risk exposure is one of the key steps in leveraging the best security practice. Also, the author suggests designing and storing the high-risk data on separate servers and/or separate user base to have better control of the resources. For e.g., storing key financial data and personal information in several different databases, backups and tapes introduces additional risks and effort to manage. A risk flag that is attached with different type of data stored in the database would be of great help for securing the most important data. **Keep it short and specific.**

3) Put controls in place to monitor the high-risk database activities

Most database vendors provide some form of native auditing options. Microsoft SQL Server and Oracle Database Server provide a fairly robust set of auditing capabilities. Many database vendors provide off-the-shelf configuration parameters to audit the data at table, column and database level. Leveraging out-of-the-box functionality would be good first step to understand the database activities. While setting up the monitoring of database activities, failed logon attempts to the database, privilege credential changes and tampering of log files by the privileged user also need to be considered for a robust design of the solution. **Start simple.**

4) Reviewing the logs to identify unusual activities

Reviewing the connection and activity logs is the key for any database activity solution. In large scale enterprises this usually means millions of records to mine. However, identifying and analyzing the suspicious activities by privileged users have proven to be formidable challenge to the organization. In particular, having an automated process in place to report the connection time, username and activity log is the most efficient way to review the activities. The ultimate condensed report of any unusual behavior needs to be escalated to management on a timely manner. **Understand the landscape.**

5) Preventing future threats by securing the data

Mining the activity and connection log helps the security group to identify the pattern and manage the controls in place to report very specific incidents. The purpose of the review is to identify potential risk bearing activities to investigate. Again, the investigation or database forensics could be further augmented by leveraging out-of-the-box functionalities from Oracle and Microsoft using database log mining tools. **Get control of things.**

Possible solution for consideration

Benefits to the organization

1. Knowing what is going on in your critical databases is the first step in getting control of things. If the management and security group doesn't understand who is connecting to the database and why, it is pretty challenging to investigate any further.

2. Enabling database audit helps companies to record the activities of privileged user which could even be referred for any regulatory compliance purposes and database forensics.

3. Get control of database access and activities.

Conclusion

Monitoring and security auditing of your organization's database applications is a critical component of achieving a strong defense-in-depth strategy around your critical and sensitive data. However, to be efficient and effective you must use the right combination of tools. Database activity monitoring of privileged users is continuously evolving process from detective to preventive approach. There is several vendor based solution including Guardium, Application Security, Agilance etc. However, most of the IT environment is really fluid with several changes happening at the same time. Out of the box solution needs to be carefully considered to monitor database activities.