IDERA® | SQL Management Suite

THE TRADE-OFF BETWEEN DATABASE SECURITY AND DATABASE PERFORMANCE

INTRODUCTION

With the increased use of databases, the need to protect databases effectively to ensure security and regulatory compliance also has increased drastically. Securing databases becomes problematic when not factoring the impact of security into the database design and the allocation of relevant system resources.

The security of any database can be improved. However, that likely degrades the performance of the database. The cost will increase to improve database security while maintaining database performance. That is, the trade-off consists of three axes: Performance, security, and cost. The existence of the three trade- off axes means that security and performance can co-exist. However, it comes at the expense of increased cost (such as effort, planning, and system resources). Fundamentally, it is necessary to choose between a database that is secure and performing, a database that is secure and not costly, or a database that is performing and not costly. It is not feasible to choose a database that is secure, performing, and not costly.

Maintaining database performance involves ensuring that end-users can get to everything that they need. In contrast, improving database security focuses on controlling the access of end-users to the available resources. Database security and performance are two of the critical quality attributes used in evaluating the service being delivered by databases to the end-users. While these attributes are highly desirable for databases, end-users often see them as almost inversely related.

SECURITY VERSUS PERFORMANCE TRADE-OFF

In general, the security of databases impacts their performance. That is, when one increases, then the other requires additional cost to prevent a decrease. The reason is that database security needs system resources. Organizations often trade off security compliance to achieve the database performance that is required. It is difficult to eliminate the performance degradation associated with enhancing security. It is usually only possible to minimize the extent of degradation. However, enhanced security can improve database performance in some cases, so do not overlook this beneficial relationship. That is why it is crucial to estimate the impact of security on performance before implementing security methods and also to measure the effect of the implementation.

Security compliance has become not only a vital but also a strategic consideration for any organization. However, often organizations flout the compliance rules and readily trade off security features to meet performance requirements. When a security feature aimed at protecting a database is disabled, the probability that the database is not security compliant anymore increases. That is why it is important to frequently and regularly assess the compliance of databases. The trade-off presents the need to understand and quantify the impact of security compliance, particularly the security methods on databases and the need to design the database capacity and system resources to deliver the performance quality required by end-users.

DATABASE ADMINISTRATOR VERSUS SECURITY ADMINISTRATOR

Asking database administrators to act as a security administrator to manage database security is counterproductive. The two job categories have conflicting incentives. The goal of a database administrator is to ensure database availability, health, and performance. The objective of a security administrator is to control access to databases. As such, the goals of those two jobs are often in conflict. The contradiction is problematic because many database administrators are also part-time security administrators. It is best practice to avoid assigning the same person to both database security and database administration.

A security administrator needs to be someone who understands database administration, but whose job it is to think about security first and performance second. The security administrator needs to work closely with the database administrator. Moreover, both people need to collaborate well. However, in the intersection between performance and security, conflict is unavoidable. Only by having two people with different goals is it possible to find the optimal balance between security and performance. It is also valuable to have access to two separate sets of tools to manage security versus performance while being able to share common views such as via reporting.

CAPACITY PLANNING

To ensure acceptable database performance and security compliance, it is necessary to specify adequate database capacity and system resources. Therefore, it is essential to grasp the impact of security compliance via security methods on database performance to aid database design and capacity planning. A well-designed database with sufficient system resources minimizes, if not entirely removes, the need for the trade-off. That is why it is vital to measure the historical trends of critical metrics and estimate future patterns.

METRICS TO OPTIMIZE SECURITY AND PERFORMANCE

The impact of database security on database performance is far from clear so that the effect remains a subject for debate. Furthermore, it remains unclear how the impact of security on performance can be evaluated and used in provisioning the required system resources capable of satisfying the database performance expectations.

It is essential to evaluate the impact of database security on database performance to improve decision-making in the database design process. Established metrics for database performance exist. In contrast, database security tends to suffer from inferior metrics. Overcome inferior metrics for database security by considering indirect metrics (such as the computational cost of database security). As such, it is possible to formulate metrics that express the trade-off between database performance and database security.

It is possible to find database parameters that optimize the trade-off metrics. These parameters are optimal for the combination of both performance and security combined, but not for each separately. Accomplish that by viewing the key metrics at a high level while also being able to drill down to detailed information.

ENSURE SECURITY BY MONITORING PERFORMANCE

Within the metrics for database performance an abundance of insight is hidden. That makes database performance metrics an often overlooked and underused indirect metric for database security. That is, performance metrics can bring into clear view critical information about the state of database security to mitigate risk.

To protect databases, develop a detailed understanding of how they typically behave. After understanding baseline performance, it is possible to monitor the database more effectively and audit the database activity accordingly. Then, identify any deviation from regular patterns that may indicate security problems.

After establishing some baseline knowledge, improve database security via best practices. For example: Inventory which groups, individuals, devices, and application can access sensitive data and by which methods. Establish a security policy, distribute the policy throughout the organization, and train all relevant staff on following the policy. Implement security methods that inform the IT team when performance metrics deviate from standard values. Develop response plans for when performance abnormalities trigger alerts and ensure that the entire IT team fully understands these plans. Verify that the organization adequately documents security compliance for regulatory and audit purposes. Review performance metrics frequently and regularly as the baseline performance metrics may change when the organization evolves. Simplify these tasks by using dedicated tools with relatively easy learning curves.

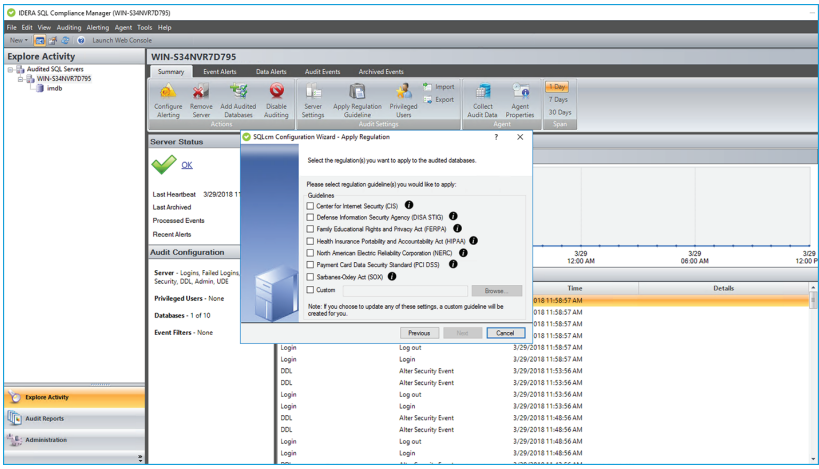
SUMMARY

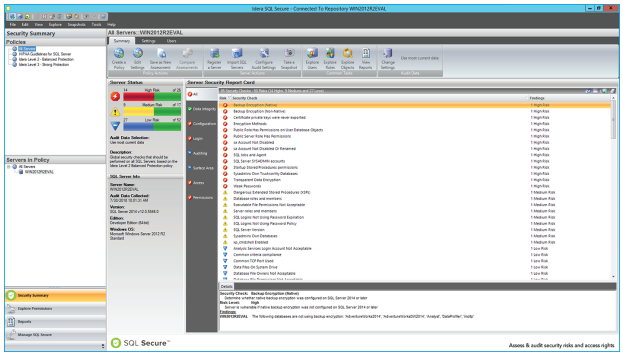
As database security becomes more important over time, this brings its effects on database performance to the forefront. Security methods cannot overly impact end-users. At the same time, it is not possible to sacrifice security compliance due to the risk of data breaches and the requirements to meet regulatory guidelines.

Because of conflicting goals, it is best practice not to combine the roles of database administrator and system administrator. Proper capacity planning ensures that databases have sufficient capacity and system resources to meet the demands of security and performance. However, the exact relationship between security and performance is not well understood. As such, security suffers from inferior metrics. Via indirect metrics, it is possible to optimize the combined security and performance of databases. It is necessary to incur additional cost to achieve both security and performance. Performance metrics can be used to detect security issues. Understand baseline behavior to recognize abnormal patterns. After establishing normal activities, maintain security by following best practices. These steps will help to improve the ability to achieve the apparently conflicting goals of improving both database security and performance.

HOW IDERA CAN HELP

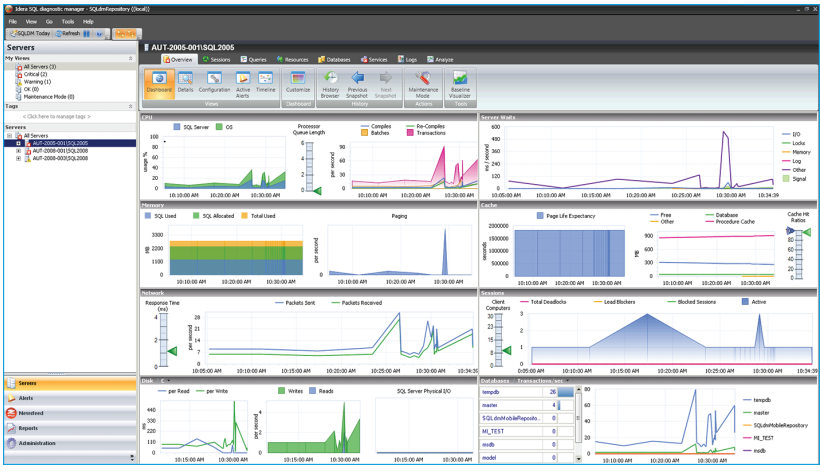
SQL Compliance Manager is a comprehensive auditing solution that monitors and tracks changes to SQL Server objects and data, and sends alerts on suspicious activity. Get detailed visibility to determine who did what, when, where, and how, whether privileged users or intruders initiated the event. Ensure compliance with requirements for industry regulations and data security. Go beyond traditional auditing approaches by providing real-time monitoring, alerting, and auditing of all data access, selects, updates, schema modifications and permission changes to SQL Server databases.





SQL Secure discovers security vulnerabilities and permissions for SQL Server and Azure SQL databases. Find out who has access to what and identify each user's effective rights across all SQL Server and Azure SQL Database objects. Alert on violations of organizational policies, monitor changes made to security settings, and generate security audit reports as well as recommendations on how to improve the security model.

SQL Diagnostic Manager Pro is a robust performance monitoring, alerting and diagnostics solution for SQL Server. It proactively notifies administrators to health, performance or availability problems via a desktop console, a web console add-on, and a mobile console. It provides agentless, real-time monitoring and alerting for fast diagnosis and remediation.



The included **SQL Workload Analysis** add-on provides a granular breakdown of wait states with easy drill-down to isolate problems quickly. It delivers valuable real-time and historical data with actionable advice to improve performance.

The included **SQL Query Tuner** add-on maximizes database and application performance by quickly finding and fixing poor-performing queries. It eliminates bottlenecks by graphically profiling critical metrics inside the database.

SQL MANAGEMENT SUITE

SQL Management Suite is a bundle of five essential products for complete SQL Server management. It covers performance, compliance, security, backup, and index fragmentation. It includes SQL Diagnostic Manager Pro (with SQL Workload Analysis and SQL Query Tuner), SQL Compliance Manager, SQL Secure, SQL Safe Backup, and SQL Defrag Manager.

Start a FREE Trial of SQL Management Suite

To learn more visit idera.com today!

IDERA