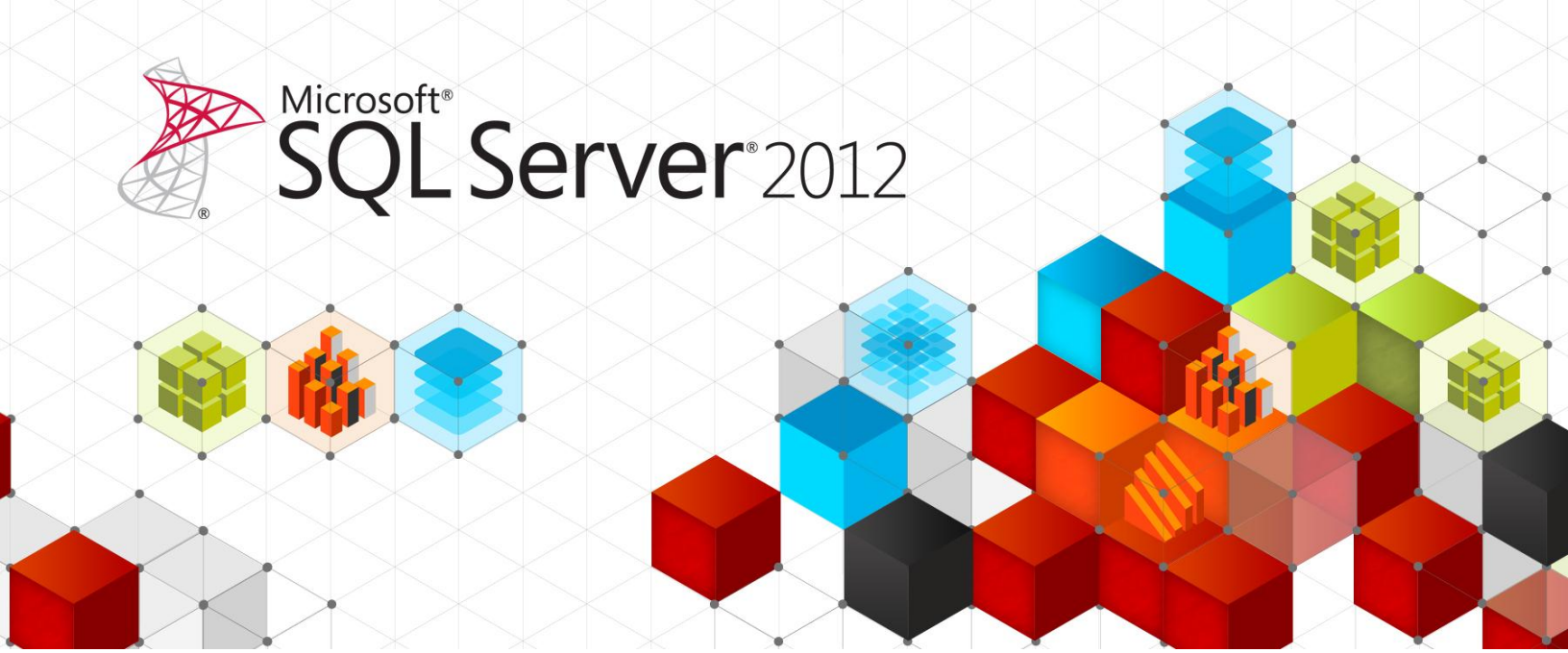


Security & Compliance

Highlights

Microsoft® SQL Server® 2012 brings additional flexibility, usability for auditing and security manageability across SQL Server environment to help making it even easier for organizations to meet compliance policies.

COMPLIANCE & CERTIFICATIONS

SQL Server 2008 SP2 Enterprise edition (32 & 64 bit) has completed EAL4+ evaluation with compliance to the "U.S. Government Profile for Database Management Systems in Basic Robustness environments, V1.2".

SQL Server 2008 has been audited for Payment Card Industry (PCI) Data Security Standard (DSS) Compliance.
SQL Server 2008 has been audited for HIPAA Compliance.

PROTECT DATA

Help protect your data with a database solution that is historically known for the lowest vulnerabilities* across the major DBMS vendors.

Cryptography Enhancements

We have greatly enhance SQL Server cryptography such as the ability to create certificates from bytes, default for Server Master Key (SMK), Database Master Key (DMK), backups key using AES256, new support for SHA2 (256 and 512), and usage of SHA512 for password hashes.

It is built on top of great SQL Server features to achieve the following:

- Take advantage of a built-in cryptography hierarchy
- Encrypt data transparently
- Employ Extensible Key Management
- Sign code modules

CONTROL ACCESS

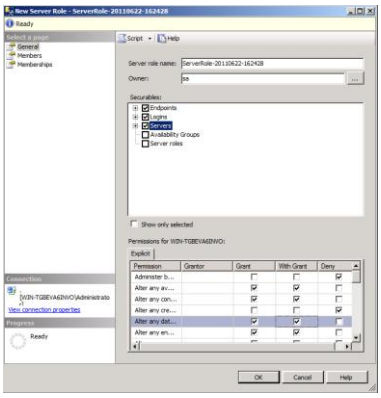
Control access to your data by managing authentication and authorization effectively and by providing access to only users who need it.

User-Defined Server Roles

User-Defined Server Roles increase flexibility, manageability, and facilitate compliance towards better separation of duties. It allows creation of new server roles to suit different organizations that separate multiple administrators according to roles. Roles can also be nested to allow more flexibility in mapping to hierarchical structures in organizations.
It also helps prevent organizations to use sysadmin for database administration.

Microsoft SQL Server 2012

Microsoft



Default Schema for Groups

Database schema can now be tied to Windows Group rather than individual users to increase database compliance. It eases administration of database schema, decreases the complexity of database schema management through individual Windows users, prevents errors of assigning schema to the wrong users when users changes groups, avoids unnecessary implicit schema creation, and greatly reduces the chance of query errors when wrong schema is being used.

Contained Database Authentication

Contained Database Authentication increases compliance by allowing users to be authenticated directly into user databases without logins. User information for login (username and password) is not stored inside the master database but user databases directly. It is very secure because users can only perform DML operations inside the user databases and not database instance level operations. It also reduces the need to login to the database instance and avoid orphaned or unused logins in the database instance. This feature is used in AlwaysOn to facilitate better portability of user databases among servers in the case of server failover without the need to configure logins for all database servers in the cluster.

SharePoint Active Directory

Help secure end user data analytics with built-in IT controls, including new SharePoint and Active Directory security models for end user reports published and shared in SharePoint. Enhanced security models provide control at row and column levels.

All are built on top of great SQL Server features to achieve the following:

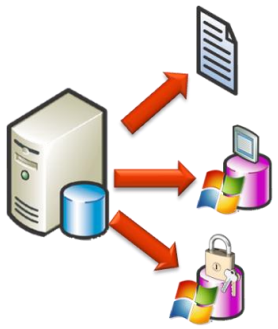
- Enforce password policies
- Use roles and proxy accounts
- Provide security enhanced metadata access
- Enhance security features with execution context

ENSURE COMPLIANCE

Ensure compliance with company policies and/or government regulations like HIPAA and PCI.

SQL Server Audit for All Editions

Allows organizations to expand the benefits of SQL Server Audit from Enterprise edition to all editions for more thorough auditing practices across SQL Server databases enabling audit standardization, better performance and richer features.



Audit Resilience

Delivers the ability to recover auditing data from temporary file and network issues.

User-Defined Audit

Allows application to write custom events into the audit log to allow more flexibility to store audit information.

Audit Filtering

Provides greater flexibility to filter unwanted events into an audit log.

All are built on top of great SQL Server features to achieve the following:

- Automatically apply software updates
- Configure the surface area with automated Policy-Based Management
- Enhanced auditing with the SQL Serve Audit
- Create custom auditing solutions with DDL triggers

Additional Information

http://www.microsoft.com/sqlserver

*nist.org