



Microsoft® SQL Server® 2008

Sichere Datenbankplattform

Microsoft® SQL Server® 2008 bietet Sicherheitsverbesserungen zur effektiven Verwaltung der Sicherheitskonfiguration, strengen Authentifizierung und Zugriffskontrolle, leistungsfähigen Verschlüsselung und zum umfangreichen Auditing.

HERAUSRAGENDE NEUE MÖGLICHKEITEN

- Mit dem richtlinienbasierten Management Sicherheitsrichtlinien für Datendienste im gesamten Unternehmen durchsetzen
- Daten verschlüsseln, ohne dafür Anwendungen zu verändern – durch die Verwendung der transparenten Datenverschlüsselung
- Verschlüsselungslösungen mit Extensible-Key-Management und Hardwaresicherheitsmodulen unternehmensweit einsetzen
- Alle Aktionen mit dem neuen Auditobjekt überwachen

Daten unternehmensweit schützen

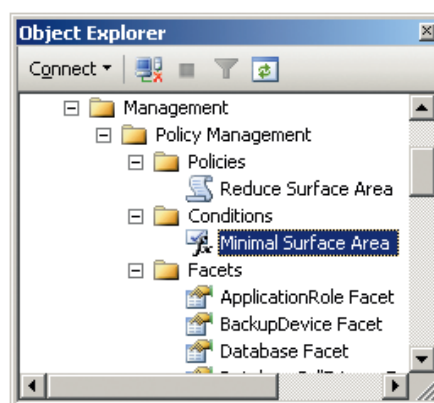
Schützen Sie Ihre Daten mit einer Datenbanklösung, die sich durch ein sicheres Design („Secure by Design“), sichere Standardeinstellungen („Secure by Default“) und eine sichere Bereitstellung („Secure in Deployment“) auszeichnet.

NEU

Oberflächenkonfiguration mit automatisierten Sicherheitsrichtlinien

Nutzen Sie das neue richtlinienbasierte Management, um Konfigurationsrichtlinien für Server, Datenbanken und Datenbankobjekte im gesamten Unternehmen durchzusetzen.

Verwenden Sie das neue Surface Area Facet für richtlinienbasiertes Management zur Steuerung aktiver Dienste und Funktionen, um weniger Sicherheitsbedrohungen ausgesetzt zu sein.



Schutz der Oberfläche mit richtlinienbasiertem Management

Softwareaktualisierungen automatisch aufspielen

Über Windows® Update können Sie SQL Server 2008-Patches automatisch aufspielen lassen. Dadurch wird die Gefahr reduziert, die von veröffentlichten Softwaresicherheitslücken ausgeht.

Den Zugriff auf Datenressourcen kontrollieren

Übernehmen Sie die Kontrolle über Ihre Daten, indem Sie nur solchen Benutzern Zugriff einräumen, die diesen tatsächlich benötigen. Authentifizierung und Autorisierung lassen sich auf effektive Weise verwalten.

Kennwortrichtlinien erzwingen

Wenden Sie automatisch die Kennwortrichtlinien von Windows Server® 2003 (oder höher) an, um eine minimale Kennwortlänge, geeignete Zeichenkombinationen und regelmäßige Kennwortwechsel auch bei Verwendung von SQL Server-Anmeldungen zu erzwingen.

Roles und Proxykonten verwenden

Verwenden Sie die msdb database fixed database roles, um die Kontrolle über Agentendienste zu verbessern. Nutzen Sie mehrere Proxys, um die Ausführung eines SQL Server Integration Services- (SSIS-) Packages als Job-Step sicherer zu machen.

Sicheren Zugang zu Metadaten bieten

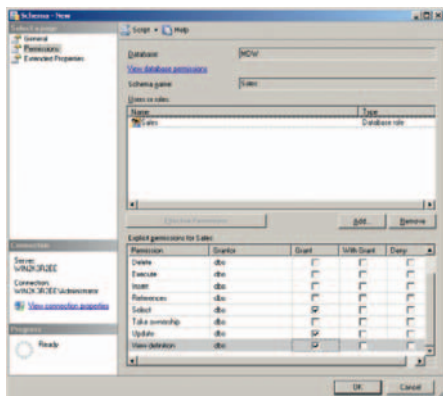
Bieten Sie durch Katalogansichten sicheren Zugang zu Metadaten. Benutzer bekommen Metadaten nur für Objekte gezeigt, auf die sie Zugriff besitzen.

Verbesserung der Sicherheit mit Execution-Context

Markieren Sie Module mit einem Ausführungskontext, sodass die Statements innerhalb der Module vom einem bestimmten Benutzer anstatt vom aufrufenden Benutzer ausgeführt werden. Gewähren Sie dem aufrufenden Benutzer Berechtigungen zur Ausführung des Moduls, aber verwenden Sie die Berechtigungen des Ausführungskontextes für Statements innerhalb des Moduls.

Die Verwaltung von Berechtigungen vereinfachen

Verwenden Sie Schemas, um die Flexibilität großer Datenbanken zu vereinfachen und zu verbessern. Gewähren Sie einem Schema Berechtigungen zur Vergabe von Rechten an jedes darin enthaltene und künftig erstellte Objekt.



Schemaerstellung

Sensible Daten verschlüsseln

Schützen Sie sensible Daten mit den eingebauten Verschlüsselungsmöglichkeiten sowie der Unterstützung für Enterprise-Lösungen zur Schlüsselverwaltung.

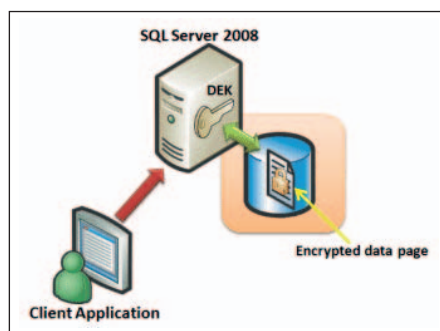
Profitieren Sie von der eingebauten Kryptografiehierarchie

Nutzen Sie die in SQL Server 2008 eingebaute Kryptografiehierarchie zur Erstellung asymmetrischer und symmetrischer Schlüssel sowie von Zertifikaten, um diese zur Verschlüsselung und Authentifizierung zu verwenden.

NEU

Daten transparent verschlüsseln

Reduzieren Sie die Komplexität bei der Entwicklung von Anwendungen, die eine Verschlüsselung von Daten erfordern, indem alle Verschlüsselungsoperationen mit einem sicheren Database Encryption Key (DEK) transparent auf Datenbankebene durchgeführt werden. Ermöglichen Sie allen Anwendungsentwicklern den Zugriff auf verschlüsselte Daten, ohne dass sie dafür ihre vorhandenen Anwendungen verändern müssen.



Transparente Datenverschlüsselung

NEU

Einsatz einer erweiterbaren Schlüsselverwaltung

Konsolidieren Sie Ihre Enterpriseverschlüsselung, indem Sie ein Enterprise-Key-Management-System verwenden. Trennen Sie Ihre Daten von den Schlüsseln durch die Verwendung von Hardware-sicherheitsmodulen, um die Schlüssel in separater Hardware zu speichern. Durch entsprechende Systeme wird die Schlüsselverwaltung vereinfacht.

Codemodule signieren

Verwenden Sie einen Schlüssel oder ein Zertifikat, um Codemodule wie Stored Procedures und Funktionen mit einer digitalen Signatur zu versehen. Anschließend können Sie mit der Signatur Berechtigungen für die Dauer der Ausführung des Codemoduls verknüpfen.

Datenbankaktivitäten überwachen – Audit

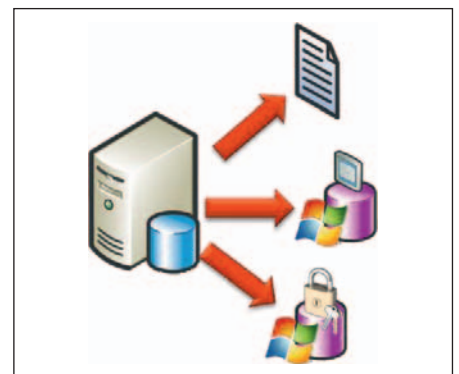
Für Haftungs- und Compliance-Fragen können Sie die Aktivitäten in Ihrer Datenbank überwachen.

NEU

Überwachen Sie alle Aktionen mit dem Auditobjekt

Definieren Sie Audits, um Aktivitäten in Protokolldateien, dem Windows-Anwendungsprotokoll oder dem Windows-Sicherheitsprotokoll automatisch aufzuzeichnen.

Übernehmen Sie die komplette Kontrolle über die Überwachung, indem Sie Auditspezifikationen erstellen, die die zu überwachenden Server- und Datenbankaktionen festlegen.



Alle Aktionen überwachen

Mit DDL-Triggern individuelle Überwachungslösungen erstellen

Anhand von Triggern erfassen und überwachen Sie Data-Definition-Language-(DDL)-Aktivitäten. Erweitern Sie Trigger, um auf DDL-Ereignisse ebenso wie auf Data-Manipulation-Language-(DML-) und Log-DDL-Ereignisse zu reagieren, was die Überwachung verbessert und die Sicherheit erhöht.

Mehr Informationen zu Microsoft SQL Server 2008 erhalten Sie unter www.microsoft.de/sql/2008

© 2008 Microsoft Corporation. Alle Rechte vorbehalten.

Dieses Dokument ist erstellt worden, bevor das Produkt zur Produktion frei gegeben wurde. Aus diesem Grund können wir nicht garantieren, dass alle hierin genannten Details exakt so auch im ausgelieferten Produkt enthalten sind. Die in diesem Dokument enthaltenen Informationen entsprechen der gegenwärtigen Ansicht der Microsoft Corporation im Hinblick auf die zum Zeitpunkt der Veröffentlichung diskutierten Themen. Da Microsoft auf Veränderungen der Marktbedingungen reagieren muss, kann dieses Dokument nicht als Zusicherung von Microsoft verstanden werden. Genauso kann Microsoft die Genauigkeit jeder Information im Anschluss an das Veröffentlichungsdatum nicht garantieren. Die Informationen beziehen sich auf das Produkt zu dem Zeitpunkt, als dieses Dokument gedruckt wurde, und sollten nur zu Planungszwecken verwendet werden. Angaben können jederzeit ohne vorherige Ankündigung von Microsoft geändert werden.