combit GmbH
Untere Laube 30
78462 Konstanz

Whitepaper

Produkt: combit Relationship Manager

HowTo: Microsoft SQL Server Datenbank verschlüsseln

Inhalt

SQL Datenbank mit EFS verschlüsseln, sichern und wiederherstellen

EFS (Encrypting File System) ist eine Funktion von Microsoft Windows, mit der Sie Informationen auf Ihrer Festplatte in einem verschlüsselten Format speichern können. EFS ermöglicht eine transparente Verschlüsselung sowie die Entschlüsselung von Dateien durch Verwendung erweiterter, standardmäßiger Verschlüsselungsalgorithmen.

Diese Verschlüsselungsmethode ist in den Microsoft SQL Server Editionen Standard und Enterprise ab Version 2008 verfügbar.

SQL Datenbank mit EFS verschlüsseln

Vorbereitende Schritte

Diese Art von Verschlüsselung setzt voraus, dass

1. Sie ein Windows Konto für den SQL Server-Dienst ausgewählt haben, das
   - für die Laufzeit der verschlüsselten Datenbank und der zugehörigen Sicherung verfügbar bleibt

   und
   - bei Bedarf zum Übertragen der Datenbank oder der zugehörigen Sicherung im gesamten Netz verwendet werden kann.
2. Sie den Dateipfad der Datenbank lokalisiert haben, wenn er sich von dem Standardspeicherpfad unterscheidet. Öffnen Sie das Microsoft SQL Server Management Studio, um den Speicherpfad der Datenbank anzuzeigen. Klicken Sie mit der rechten Maustaste auf die Datenbank, welche verschlüsselt werden soll. Klicken Sie auf *Eigenschaften > Dateien > Datenbankdateien* (*Properties > Files > Database Files*) und merken oder notieren Sie sich den Pfad für beiden Dateien, welche in der Spalte 'Pfad' angezeigt werden.

Vorgehensweise

1. Rufen Sie *Start > Systemsteuerung > Verwaltung > Dienste* (Start > Control Panel > Administration > Services) auf und stoppen Sie den SQL Server-Dienst. Standardmäßig heißt dieser "SQL Server (MSSQLSERVER)".
2. Klicken Sie mit der rechten Maustaste auf den SQL Server-Dienst und anschließend auf Eigenschaften, um das Dialogfenster für die Eigenschaften des Dienstes zu öffnen. Wählen Sie auf der Registerkarte Anmelden unter Dieses Konto das Windows Konto aus, welches Sie im Abschnitt 'Vorbereitende Schritte' für diesen Zweck ausgewählt haben. Geben Sie anschließend die Berechtigungsnachweise des Windows Kontos ein und klicken Sie auf OK.
3. Klicken Sie im Windows Explorer mit der rechten Maustaste auf den Ordner, in dem sich die Datenbank befindet, und wechseln Sie zu *Eigenschaften > Sicherheit* (*Properties > Security*), um dem Windows Konto Lese- und Ausführberechtigungen sowie Leseberechtigungen für die Datei <Datenbankname.mdf> und den übergeordneten Ordner zu erteilen.
   Anmerkung: Die Berechtigungsnachweise des angemeldeten Benutzers werden zum Verschlüsseln der Datenbank verwendet. Wenn Sie nicht beim Service-Account angemeldet sind, melden Sie sich jetzt an.
4. Klicken Sie mit der rechten Maustaste auf die Datei <Datenbankname.mdf>, rufen Sie *Eigenschaften > Allgemein > Erweitert > Inhalt verschlüsseln, um Daten zu schützen* (*Properties > General > Advanced > Encrypt contents to secure data*) auf und klicken Sie auf OK.
   Anmerkung: Wenn der übergeordnete Ordner noch nicht verschlüsselt ist, wählen Sie *Datei und übergeordneten Ordner verschlüsseln* (*Encrypt the file and the parent folder*) aus, wenn Sie dazu

aufgefordert werden. Anderenfalls können Sie im Microsoft SQL Server Management Studio nicht auf die verschlüsselte Datenbank zugreifen.

5. Wiederholen Sie die Schritte 3 und 4 für die Datei <Datenbankname.ldf>.
6. Starten Sie den SQL Server-Dienst neu.

Wichtig:
Nur der Benutzer, der die Datei verschlüsselt hat, kann sie entschlüsseln. Im Abschnitt 'Details' in der Anzeige *Eigenschaften > Erweiterte Attribute* (*Properties > Advanced Attributes*) können Sie festlegen, wer die jeweiligen Dateien verschlüsselt hat. Die Sicherung der verschlüsselten Datenbank wird NICHT automatisch verschlüsselt. Führen Sie die Schritte im Abschnitt 'EFS verschlüsselte Datenbank sichern und wiederherstellen' aus.

EFS verschlüsselte Datenbank sichern und wiederherstellen

Sie können eine verschlüsselte Datenbanksicherungsdatei an einen im Netz gemeinsam genutzten Ort verschieben, die auf derselben Windows-Version gehostet wird, um die Dateiverschlüsselung zu erhalten. Sie können die Datenbank von jedem Ort aus, an dem die verschlüsselte Datenbankdatei gespeichert ist, wiederherstellen.

Wenn Sie die Datei auf einem SQL Server wiederherstellen, sollte der SQL Server Dienst dieses Servers mit den Windows Konto Berechtigungsnachweisen des Benutzers ausgeführt werden, der die Datenbank verschlüsselt hat. Eine wiederhergestellte Datenbank ist jedoch NICHT verschlüsselt. Sie müssen sie daher mithilfe der oben genannten Schritte wieder verschlüsseln. Nur das zuvor eingetragene Windows Konto hat die Berechtigung die Datenbank wiederherzustellen!

Vorgehensweise

1. Erweitern Sie im Windows Explorer den Ordner, in dem sich die Datenbanksicherung befindet, und erteilen Sie dem Windows Konto Lese- und Ausführberechtigungen sowie Leseberechtigungen für die Datei <Datenbankname.bak>.
   Anmerkung: Die Berechtigungsnachweise des angemeldeten Benutzers werden zum Verschlüsseln der Datenbank verwendet. Wenn Sie nicht mit dem Windows Konto angemeldet sind, melden Sie sich jetzt an.
2. Klicken Sie mit der rechten Maustaste auf die Datei <Datenbankname.bak>, rufen Sie *Eigenschaften > Allgemein > Erweitert > Inhalt verschlüsseln, um Daten zu schützen* (*Properties > General > Advanced > Encrypt contents to secure data*) auf und klicken Sie auf OK.
3. Jetzt kann die Datenbanksicherung auf dem SQL Server wiederhergestellt werden.

SQL Datenbank mit einer Transparenten Datenverschlüsselung (TDE) verschlüsseln und wiederherstellen

Sie können eine verschlüsselte Datenbanksicherungsdatei an einen im Netz gemeinsam genutzten Ort verschieben, die auf derselben Windows-Version gehostet wird, um die Dateiverschlüsselung zu erhalten. Sie können die Datenbank von jedem Ort aus, an dem die verschlüsselte Datenbankdatei gespeichert ist, wiederherstellen. Wenn Sie die Datei auf einem SQL Server wiederherstellen, sollte der Dienst dieses Servers mit den Dienstekonto-Berechtigungsnachweisen des Benutzers ausgeführt werden, der die Datenbank verschlüsselt hat.

Eine wiederhergestellte Datenbank ist jedoch NICHT verschlüsselt. Sie müssen sie daher mithilfe der oben genannten Schritte verschlüsseln. Nur das zuvor eingetragene Dienstekonto hat die Berechtigung die Datenbank wiederherzustellen!

Die Transparente Datenverschlüsselung (TDE) ist nur in der Microsoft SQL Server Enterprise Edition verfügbar. Falls Sie keine Enterprise Edition haben, müssen Sie die SQL Datenbank mit EFS verschlüsseln. Die Anleitung hierzu finden Sie im Abschnitt 'SQL Datenbank mit EFS verschlüsseln'.

SQL Datenbank mit TDE verschlüsseln

Vorbereitende Schritte

Zum Aktivieren von TDE auf einem SQL Server müssen Sie über die normalen Berechtigungen zum Erstellen eines Datenbankmasterschlüssels und von Zertifikaten in der Masterdatenbank verfügen. Sie müssen zudem über Steuerungsberechtigungen auf der Benutzerdatenbank verfügen.

Einfachheitshalber können Sie für diese Art von Verschlüsselung dieses SQL-Script verwenden:
https://www.combit.net/de/support/files/cmbtkb/EnableTDE.zip

Vorgehensweise

1. Öffnen Sie das Microsoft SQL Server Management Studio.
2. Stellen Sie eine Verbindung zu der Datenbank her, die Sie verschlüsseln möchten. Auf diese Weise wird sichergestellt, dass die Datenbank erstellt wurde und verfügbar ist.
3. Wechseln Sie zu dem Ort, an dem Sie die heruntergeladene Datei EnableTDE.zip gespeichert haben. Entpacken Sie die Datei und öffnen Sie das Script im Microsoft SQL Server Management Studio.
4. Bevor Sie das Script ausführen, müssen Sie drei Felder für Ihre Umgebung festlegen. Diese sind im Kommentarabschnitt des Scripts alle mit 'ACTION REQUIRED' (Erforderliche Aktion) markiert:
    a. DECLARE @MKPassword (@MKPassword festlegen): Das Masterschlüsselkennwort, mit dem der Masterschlüssel in der [Master-] Datenbank erstellt wird.
    b. DECLARE @DatabaseName (@DatabaseName festlegen): Der Name der Datenbank, auf der Sie die Verschlüsselung aktivieren möchten.
    c. (Optional) DECLARE @BackupPassword (@BackupPassword festlegen): Das Kennwort zum Sichern des Zertifikats. Dieses Kennwort wird verwendet, um die Zertifikatssicherung zu sichern. Dies ist erforderlich, um das Zertifikat in einer anderen Maschine wiederherzustellen.
5. Führen Sie nach der Anpassung der drei Felder das Script über das Microsoft SQL Server Management Studio aus.
6. Nachdem das Script ausgeführt wurde, wird das Ergebnis im Fenster 'Nachrichten' von Microsoft SQL Server Management Studio angezeigt.
   Anmerkung: Sie können die Prüfung auch über das Microsoft SQL Server Management Studio durchführen. Klicken Sie mit der rechten Maustaste auf *Datenbankname > Tasks >*

Datenbankverschlüsselung verwalten (*Database Name >Tasks >Manage Database Encryption*). Das Kontrollkästchen für *Datenbankverschlüsselung aktivieren* (*Set Database Encryption On*) ist ausgewählt.

Wichtig:
Stellen Sie sicher, dass Sie nach Abschluss die Kennwörter notieren, die in diesem Script verwendet werden, und erstellen Sie eine Kopie der Zertifikatssicherung. Die Zertifikatssicherung besteht aus zwei Dateien, combit_crm_cert.bak und combit_crm_cert.pvk. Sie werden in der .mdf-Datei der Datenbank gespeichert, standardmäßig in folgendem Ordner:

- SQL Server 2016: C:\Programme\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA
- SQL Server 2014: C:\Programme\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA
- SQL Server 2012: C:\Programme\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\DATA
- SQL Server 2008R2: C:\Programme\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA
- SQL Server 2008: C:\Programme\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA

TDE geschützte Datenbank auf einem anderen SQL Server wiederherstellen

Führen Sie die folgenden Schritte aus, wenn Sie eine TDE-geschützte Datenbank auf einem anderen Server wiederherstellen oder auf diesen verschieben müssen.

Vorbereitende Schritte
Einfachheitshalber können Sie für die Wiederherstellung dieses SQL-Script verwenden:
https://www.combit.net/de/support/files/cmbtkb/RestoreDBCertificate.zip

Vorgehensweise
1. Kopieren Sie die zwei Zertifikatsdateien (combit_crm_cert.bak und combit_crm_cert.pvk), die zuvor erstellt wurden, an einen beliebigen Ort auf Ihrer Maschine (zum Beispiel: C:\Certificate\).
2. Öffnen Sie das Microsoft SQL Server Management Studio.
3. Wechseln Sie zu dem Ort, an dem Sie die heruntergeladene Datei RestoreTDECertificate.zip gespeichert haben. Entpacken Sie die Datei und öffnen Sie das Script im Microsoft SQL Server Management Studio.
4. Bevor Sie das Script ausführen, müssen Sie drei Felder für Ihre Umgebung festlegen (sie sind im Kommentarabschnitt des Scripts alle mit 'ACTION REQUIRED' (Erforderliche Aktion) markiert):
    a. DECLARE @MKPassword (@MKPassword festlegen): Das Masterschlüsselkennwort, das zum Erstellen des Masterschlüssels in der [Master-] Datenbank verwendet wurde, in der Sie TDE aktiviert haben.
    b. DECLARE @BackupPassword (@BackupPassword festlegen): Das Kennwort, das zum Sichern des Zertifikats verwendet wurde, wenn dieses sich von @MKPassword unterscheidet.
    c. DECLARE @Path (@Path festlegen): Der Pfad der Position, an der Sie die Kopien der zwei Dateien combit_crm_cert.bak und combit_crm_cert.pvk gespeichert haben.
5. Führen Sie nach der Anpassung der drei Felder das Script über das Microsoft SQL Server Management Studio aus.

Nachdem das Script ausgeführt wurde, wird das Ergebnis im Fenster 'Nachrichten' des Microsoft SQL Server Management Studio angezeigt. Wenn die folgende Nachricht angezeigt wird, sollten Sie die Datenbank auf diesem SQL Server wiederherstellen können: "The certificate is restored successfully, you can restore the database." (Das Zertifikat wurde erfolgreich wiederhergestellt. Sie können die Datenbank wiederherstellen.)