Prinzipale (Datenbankmodul)

SQL Server 2016 and later

DIESES THEMA GILT FÜR: SQL Server (ab 2008) Azure SQL-Datenbank Azure SQL Data Warehouse Parallel Data Warehouse

Prinzipale sind Entitäten, die SQL Server -Ressourcen anfordern können. Wie bei anderen Komponenten des SQL Server -Autorisierungsmodells können Prinzipale hierarchisch angeordnet werden. Der Einflussbereich eines Prinzipals richtet sich nach dem Definitionsbereich des Prinzipals (Windows, Server, Datenbank) und danach, ob der Prinzipal unteilbar ist oder es sich um eine Auflistung handelt. Ein Windows-Anmeldename ist ein Beispiel eines unteilbaren Prinzipals und eine Windows-Gruppe das eines Prinzipals, der eine Auflistung darstellt. Jeder Prinzipal weist eine Sicherheits-ID (SID) auf.

Prinzipale auf Windows-Ebene

- Windows-Domänenanmeldename
- Lokaler Windows-Anmeldename

SQL Server-Ebenen Prinzipale

- SQL Server -Anmeldename
- Serverrolle

Prinzipale auf Datenbankebene

- Datenbankbenutzer
- Datenbankrolle
- Anwendungsrolle

Der SQL Server-Anmeldename sa

Der SQL Server-Anmeldename „sa“ ist ein Prinzipal auf Serverebene. Er wird standardmäßig bei der Installation einer Instanz erstellt. Ab SQL Server 2005 ist die Standarddatenbank von sa „Master“. Dieses Verhalten unterscheidet sich von früheren Versionen von SQL Server.

Datenbankrolle public

Jeder Datenbankbenutzer gehört der Datenbankrolle public an. Wenn einem Benutzer keine bestimmten Berechtigungen für ein sicherungsfähiges Element erteilt oder verweigert werden, erbt der Benutzer die Berechtigungen, die der Datenbankrolle public für dieses sicherungsfähige Element erteilt wurden.

INFORMATION_SCHEMA und sys

Jede Datenbank enthält zwei Entitäten, die in Katalogsichten als Benutzer angezeigt werden: INFORMATION_SCHEMA und sys. Diese Entitäten werden von SQL Server benötigt. Es handelt sich dabei nicht um Prinzipale, die geändert oder gelöscht werden können.

Zertifikatbasierte SQL Server-Anmeldenamen

Serverprinzipale, deren Name von doppelten Nummernzeichen (##) eingeschlossen ist, sind nur für die systeminterne Verwendung vorgesehen. Die folgenden Prinzipale werden bei der Installation von SQL Server aus Zertifikaten erstellt und sollten nicht gelöscht werden.

- ##MS_SQLResourceSigningCertificate##
- ##MS_SQLReplicationSigningCertificate##
- ##MS_SQLAuthenticatorCertificate##
- ##MS_AgentSigningCertificate##
- ##MS_PolicyEventProcessingLogin##
- ##MS_PolicySigningCertificate##
- ##MS_PolicyTsqlExecutionLogin##

Der guest-Benutzer

Jede Datenbank enthält einen **Gast**. Dem **guest** -Benutzer erteilte Berechtigungen werden von Benutzern geerbt, die Zugriff auf die Datenbank, jedoch kein Benutzerkonto in der Datenbank besitzen. Der **guest** -Benutzer kann nicht gelöscht werden. Er kann jedoch deaktiviert werden, indem seine **CONNECT** -Berechtigung aufgehoben wird. Die **CONNECT**-Berechtigung kann durch Ausführen von `REVOKE CONNECT FROM GUEST` in einer beliebigen Datenbank mit Ausnahme der master- oder tempdb-Datenbank aufgehoben werden.

Client und Datenbankserver

Laut Definition sind ein Client und ein Datenbankserver Sicherheitsprinzipale und können gesichert werden. Diese Entitäten können gegenseitig authentifiziert werden, bevor eine sichere Netzwerkverbindung hergestellt wird. SQL Server unterstützt das Kerberos -Authentifizierungsprotokoll, das festlegt, wie Clients mit einem Netzwerkauthentifizierungsdienst interagieren.

Verwandte Aufgaben

Informationen zum Entwerfen eines Berechtigungssystems finden Sie unter Getting Started with Database Engine Permissions.

Dieser Abschnitt der SQL Server-Onlinedokumentation umfasst die folgenden Themen:

- Verwalten von Anmeldungen, Benutzern und Schemas: Vorgehensweisen
- Rollen auf Serverebene

- Rollen auf Datenbankebene
- Anwendungsrollen

Siehe auch

Sichern von SQL Server
sys.database_principals (Transact-SQL)
sys.server_principals (Transact-SQL)
sys.sql_logins (Transact-SQL)
sys.database_role_members (Transact-SQL)
Rollen auf Serverebene
Rollen auf Datenbankebene

Community-Beiträge