



Importancia de la Seguridad BD





- El control de acceso representa una operación importante en la gestión de la seguridad sobre un servidor de bases de datos.
- La Gestión de Seguridad en BD permite un control de las autorizaciones y privilegios necesarios a cada usuario para que puedan trabajar de manera autónoma.
- La Gestión de Seguridad en BD, realiza una organización jerárquica de los elementos de seguridad, de manera que la gestión de los derechos de acceso sea simple y eficaz.





Administración de Usuarios

Es la gestión de accesos y permisos que los usuarios tendrán dentro del Servidor y las Base de Datos.

Autenticación

La Autenticación es el proceso para determinar que alguien es realmente quien dice ser.

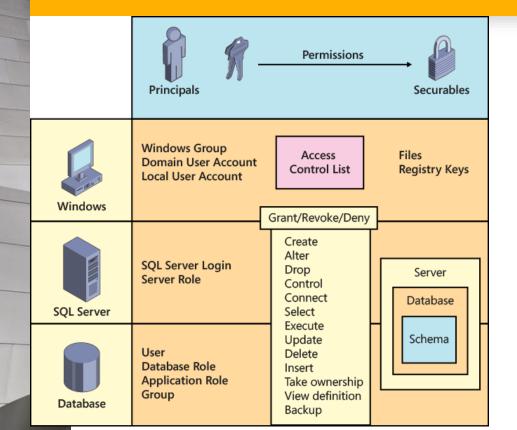
Política de Seguridad

Conjunto de Reglas o Normativas para el mantenimiento de cierto nivel de seguridad en la organización



SQL Server Security Model





Principal: Object to which permissions can be Principal assigned, such as a login or certificate.

Securable: Resource within SQL Server, such as a Securable database, table, procedure, or feature.

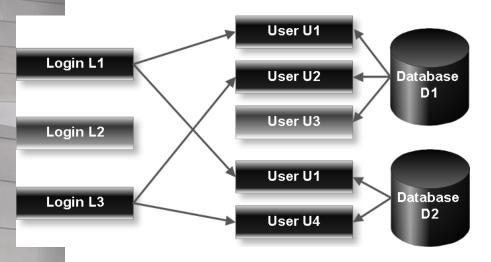
Permission: Activity on the securable that is granted Permission to the principal, such as read or view.

Fuente:

http://programming.wmlcloud.com/database/22 488.aspx

SQL Server Security Model





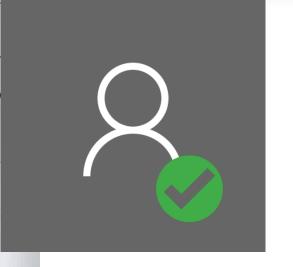
Login L1 is mapped with user U1 of the database D1 as well as user U1 of the database D2. In the same way Login L3 is mapped with user U2 of the database D1 and users U4 of the database D2. Login L2 has not mapped with any users of any databases. In the same way users U3 has not mapped with any login of the sql server.

Fuente:

https://www.exacthelp.com/2014/12/understanding-sql-server-security.html

SQL Server Security Model





Types of Login\authentication in SQL server:

SQL server supports two types of authentication mode:

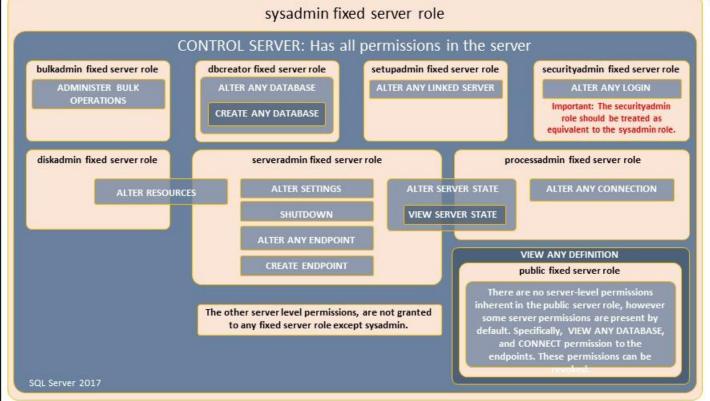
- a. Window authentication
- b. Mixed authentication (Window authentication and Sql server authentication)

Server Roles
Database Roles









Database Roles



CONTROL DATABASE: Has all permissions in the database

db_datareader

db datawriter

GRANT INSERT ON DATABASE::<name>

GRANT UPDATE ON DATABASE::<name>

GRANT DELETE ON DATABASE::<name>

GRANT SELECT ON DATABASE::<name>

db_denydatareader

DENY SELECT ON DATABASE::<name>

db denydatawriter

DENY INSERT ON DATABASE::<name>

DENY UPDATE ON DATABASE::<name>

DENY DELETE ON DATABASE::<name>

db_accessadmin

db_securityadmin

CREATE SCHEMA

ALTER ANY USER

public

There are no database-level permissions inherent in the public database role, however some database permissions are present by default. Specifically, VIEW ANY COLUMN MASTER KEY DEFINITION, VIEW ANY COLUMN ENCRYPTION KEY DEFINITION, and SELECT permission on many individual system tables. These permissions can be revoked.

There are various special purpose roles in the msdb database

ALTER ANY ROLE, CREATE ROLE

ALTER ANY APPLICATION ROLE

VIEW DEFINITON

db_backupoperator

BACKUP DATABASE

BACKUP LOG

CHECKPOINT

db ddladmin

ALTER ANY ASSEMBLY
ALTER ANY ASYMMETRIC KEY
ALTER ANY CERTIFICATE

ALTER ANY CONTRACT

ALTER ANY DATABASE DDL TRIGGER

ALTER ANY DATABASE EVENT NOTIFICATION ALTER ANY DATASPACE

ALTER ANY FULLTEXT CATALOG

ALTER ANY MESSAGE TYPE

ALTER ANY REMOTE SERVICE BINDING

ALTER ANY ROUTE
ALTER ANY SCHEMA

ALTER ANY SERVICE

ALTER ANY SYMMETRIC KEY

CHECKPOINT CREATE AGGREGATE

CREATE DEFAULT

CREATE FUNCTION

CREATE PROCEDURE

CREATE QUEUE

CREATE RULE

CREATE SYNONYM

CREATE TABLE

CREATE TYPE
CREATE VIEW

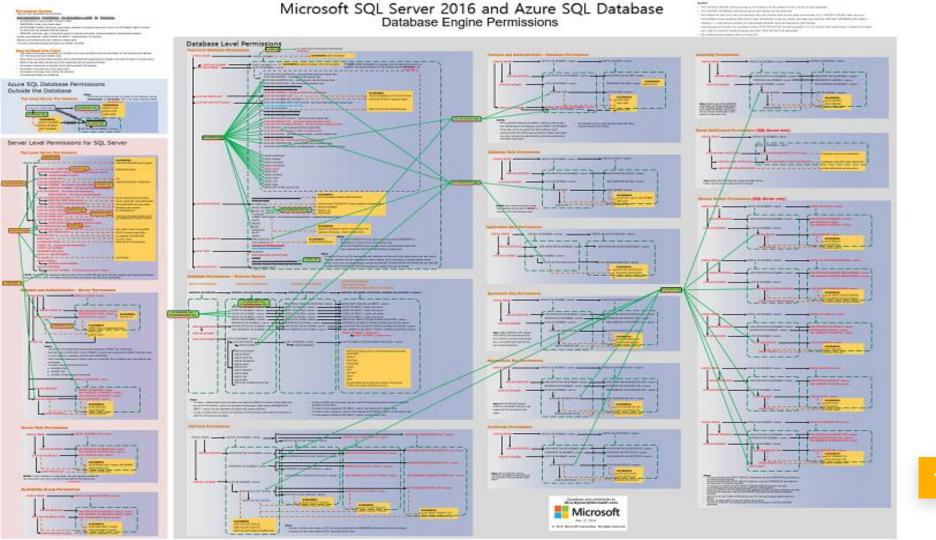
CREATE XML SCHEMA COLLECTION

REFERENCES



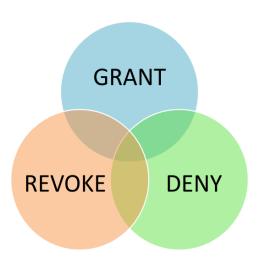
The other database level permissions, are not granted to any fixed database role except db_owner.

SQL Server 2017



Permissions





Grant Select on [Person].[Address]
to Acceso

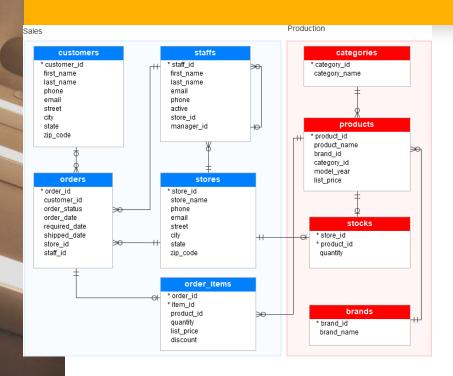
- -- Insert
- -- Update
- -- Execute
- -- Function

Revoke Select on [Person].[Address] to Acceso

Deny Select on [Person].[Address] to Acceso

SCHEMAS





El objetivo de los esquemas es separar los usuarios de base de datos de los objetos que pueden crear. De esta manera, es posible definir un esquema como un conjunto lógico de objetos de una base de datos.





Organizar los permisos de Acceso mediante ROLES

Establecer cuales serán los permisos necesarios al Rol de la BD y asignarlo al usuario.

Administración por Esquemas

Configurar los permisos de acceso de los roles mediante esquemas, de esta manera serán hererados al rol.





No utilizar el Super Usuario SA o SysAdmin (Roles)

Para usuarios que conectan al sistema de información deben tener permisos limitados a la aplicación.

Acceso a Objetos de la BD

Asignar permisos directamente con objetos de la base de datos otorgando permisos solo a procedimientos almacenados o funciones, y denegando permisos a objetos subyacentes tales como tablas.





Limitación de Permisos

Considerar la política de permisos mínimos. Solo los necesarios para la ejecución exitoso de su tarea.

Administración para los DBA

No conceder el mismo acceso para los administradores de bases de datos. Limitar sus funciones para establecer responsabilidades.

THANKS!

Any questions?

