



Administración de Microsoft® Usuarios con SQL Server® (DB Best Practices)

1. Conceptos Básico

Administración de Usuarios, Autenticación

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.

Conceptos Básicos



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

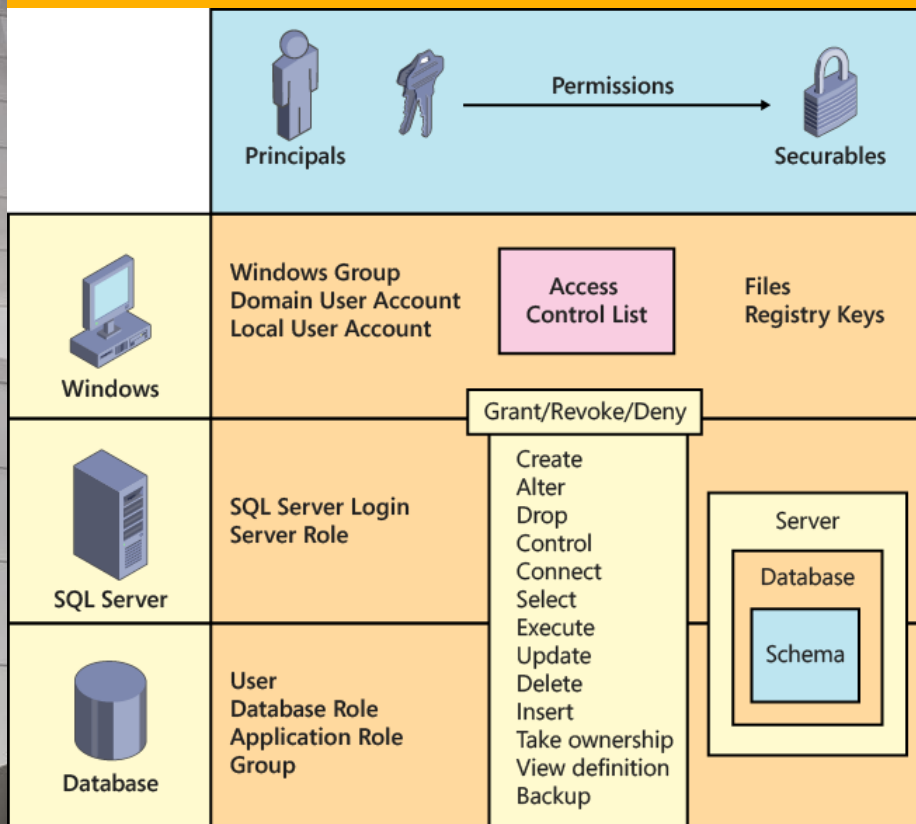
Conjunto de Reglas o Normativas para el mantenimiento de cierto nivel de seguridad en la organización



Microsoft®
SQL Server®

2. SQL Server Securing Model

SQL Server Security Model



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

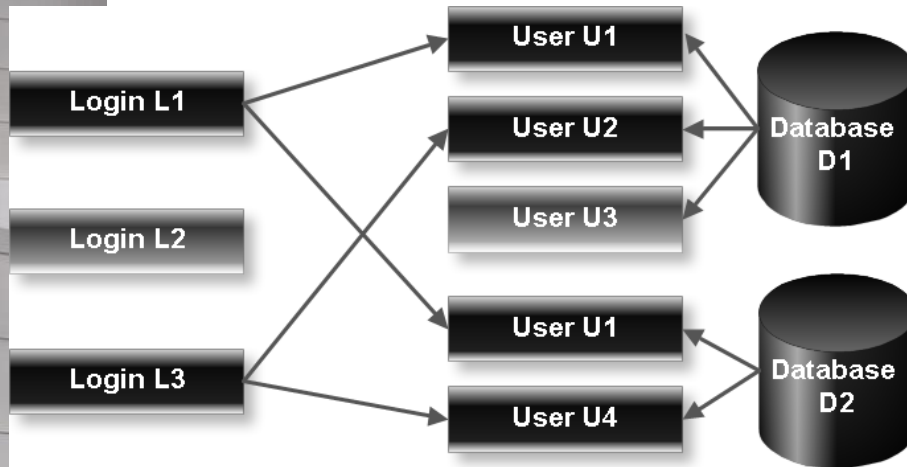
Securable: Resource within SQL Server, such as a Securable database, table, procedure, or feature.

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

Fuente:

<http://programming.wmlcloud.com/database/22488.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:

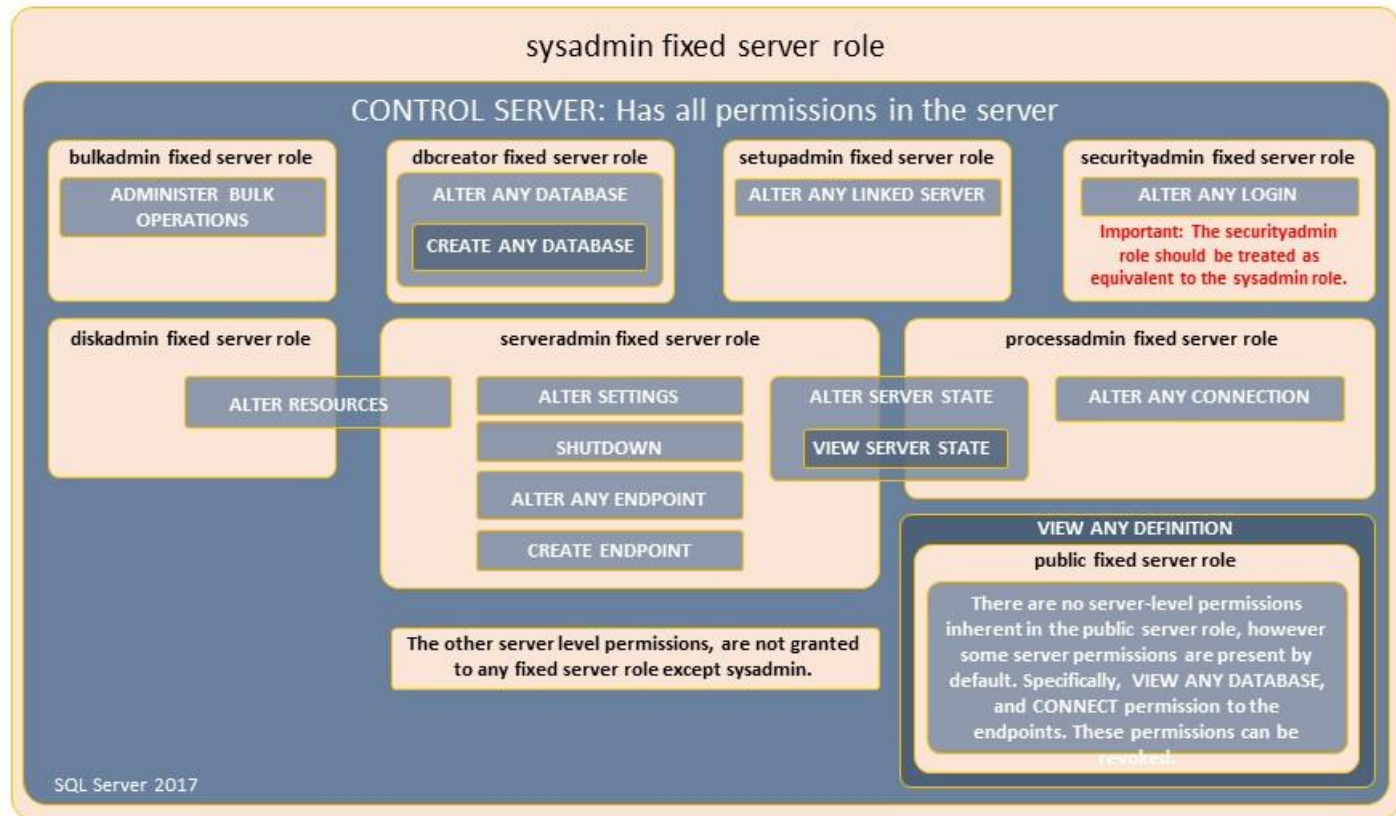
SQL server supports two types of authentication mode:

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

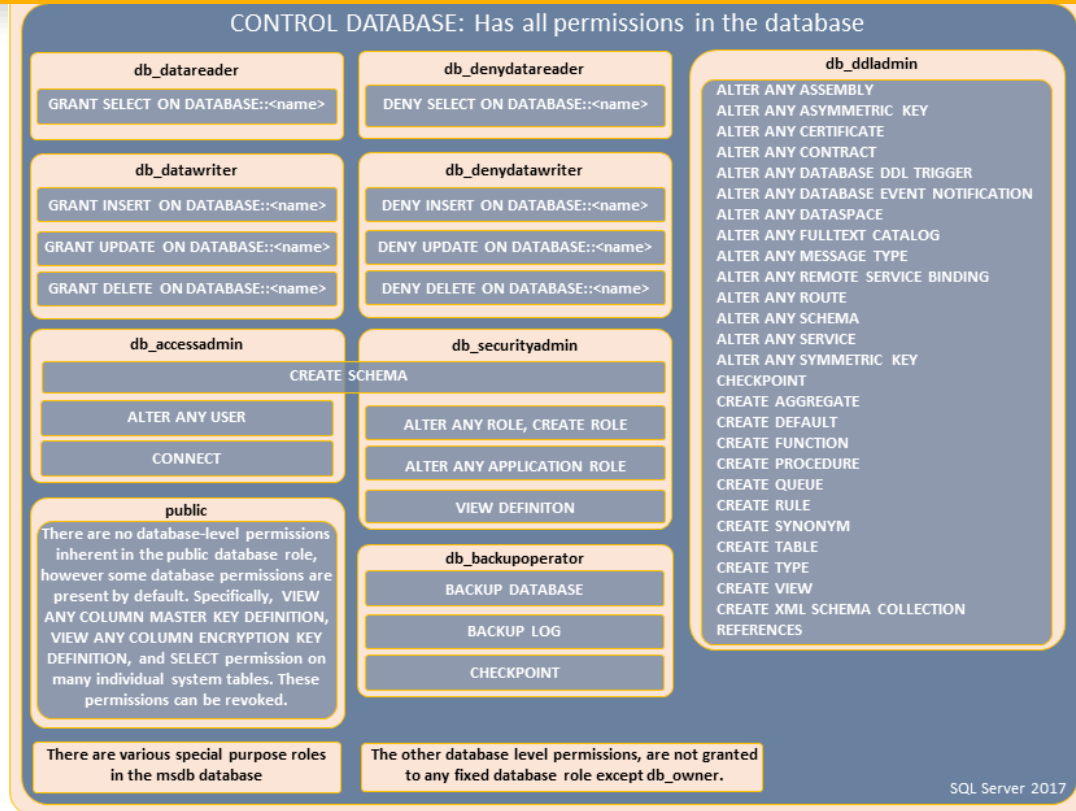
Server Roles

Database Roles

Server Roles



Database Roles

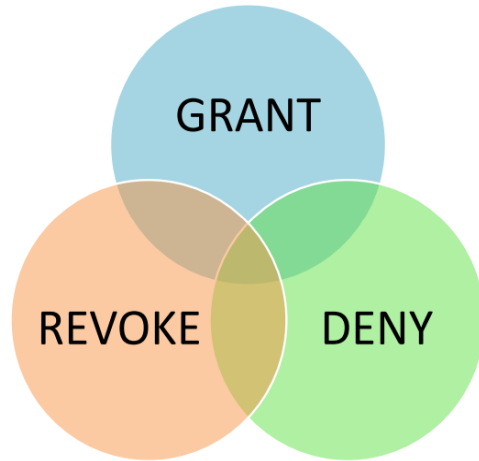


Answers:

1. Yes, it's a true, direct participation in the activity of the activity of the activity.
2. Yes, it's a true, direct participation in the activity of the activity of the activity.
3. Yes, it's a true, direct participation in the activity of the activity of the activity.
4. Yes, it's a true, direct participation in the activity of the activity of the activity.
5. Yes, it's a true, direct participation in the activity of the activity of the activity.
6. Yes, it's a true, direct participation in the activity of the activity of the activity.
7. Yes, it's a true, direct participation in the activity of the activity of the activity.
8. Yes, it's a true, direct participation in the activity of the activity of the activity.
9. Yes, it's a true, direct participation in the activity of the activity of the activity.
10. Yes, it's a true, direct participation in the activity of the activity of the activity.



Permissions



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

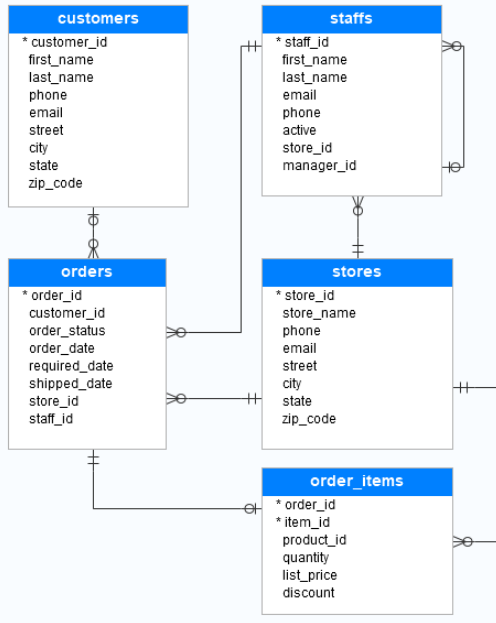
- `-- Insert`
- `-- Update`
- `-- Execute`
- `-- Function`

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

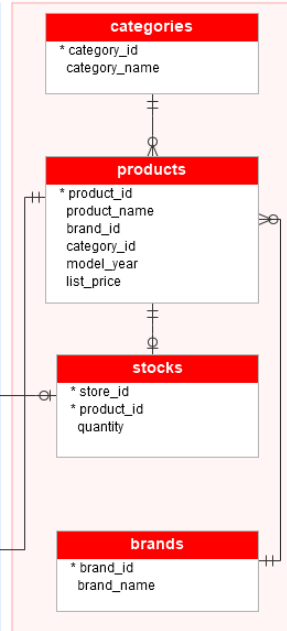
`Deny Select on [Person].[Address] to
Acceso`

SCHEMAS

Sales



Production



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 exitosa 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?

-
-

Microsoft®
SQL Server®

