

Certificación
avanzada en

DevOps



Seguridad



mundosE
PEOPLE & BUSINESS SCHOOL

¿Qué vamos a ver en este encuentro?

- ▶ Tipos de cuentas
- ▶ Autorizaciones
- ▶ Autenticaciones
- ▶ Políticas
- ▶ Buenas practicas
- ▶ Practica en Azure portal
- ▶ Seguridad en bases de datos
- ▶ Practica en Azure SQL Server
- ▶ Roles
- ▶ Usuarios inactivos, que hacemos con ellos?

Account types

- Users
- Organization owner
- Service accounts
- Service principals
- Job agents

Authentication

- User credentials
- Windows authentication
- Two-factor authentication (2FA)
- SSH key authentication
- Personal access tokens
- OAuth configuration
- Active Directory authentication library

Authorization

- Security group membership
- Role-based access control
- Access levels
- Feature flags
- Security namespaces & permissions

Policies

- Privacy policy URL
- Application connection and security policies
- User policies
- Git repository and branch policies

Cuentas

Si bien los principales tipos de cuentas de interés son las cuentas de usuario que agrega a su organización o proyecto, Azure DevOps admite otros tipos de cuentas para realizar diversas operaciones.

ks, service connections, or other third-party applications.

Cuentas / TIPOS



- **Organization owner:** The creator of an Azure DevOps Services organization or assigned owner. To learn who is the organization owner for your organization, see [Increase your permissions; find an admin](#).
- **Service accounts:** Internal Azure DevOps accounts used to support a specific service, such as Agent Pool Service, Pipelines SDK. For descriptions of service accounts, see [Security groups, service accounts, and permissions](#).
- **Service principals:** Internal Azure DevOps accounts to support internal operations.
- **Job agents:** Internal accounts used to run specific jobs on a regular schedule.
- **Third party accounts:** Accounts that require access to support Web hooks, service connections, or other third-party applications.



¿Qué es la política de seguridad de TI?

Una estrategia integral de seguridad de TI es un plan que guía a la organización hacia el objetivo de proteger los datos y las redes de las amenazas a la seguridad. Es un vínculo entre las personas, los procesos y la tecnología, todos los cuales deben trabajar en conjunto para evitar brechas de seguridad.

La implementación de una estrategia de seguridad de TI comunica las expectativas de la organización de los empleados y los educa sobre las medidas de seguridad que deben seguir. Estas medidas pueden incluir cómo configurar los equipos de TI y los puntos finales, cómo los empleados deben iniciar sesión en los sistemas corporativos, quién debe recibir acceso a los datos, cómo capacitar a los empleados en los procesos de seguridad y cómo la organización logrará el cumplimiento de TI.

¿Cuál es el propósito de una política de seguridad de TI?

Las políticas de seguridad de TI pueden ayudar a las organizaciones a mantener la confidencialidad, integridad y disponibilidad de los sistemas y la información.

Estos tres principios conforman la tríada de la CIA:

- **La confidencialidad** incluye proteger los activos del acceso no autorizado.
- **La coherencia** garantiza que la información y los sistemas solo se puedan

modificar en las formas permitidas por la organización.

- **Disponibilidad** significa que los usuarios autorizados tienen acceso constante a la información y los sistemas de los que dependen.

Mejores prácticas de políticas de seguridad de TI



Independientemente de la estructura, lo que importa en una política de seguridad de TI es que está enviando un mensaje claro a toda la organización y sus partes interesadas sobre lo que se requiere desde el punto de vista de la seguridad de TI.

La política debe ser **clara e inequívoca**, con el nivel de detalle adecuado para la audiencia, y debe ser fácil de leer y comprender, especialmente para los que no son expertos en seguridad.

mE



Mejores prácticas de políticas de seguridad de TI

Al igual que otras políticas de toda la organización, debe crear la política de seguridad de TI con la participación de todas las partes interesadas relevantes. Sería imprudente que la administración de TI desarrollara una política por sí misma, sin la aceptación de los usuarios comerciales y los proveedores externos que esperarían que la cumplieran. Obtener el aporte de las partes interesadas asegura un amplio apoyo en su implementación y cumplimiento.

Políticas de seguridad

Para proteger su organización y su código, puede establecer una serie de políticas. Específicamente, puede habilitar o deshabilitar las siguientes políticas:

mE



Políticas de seguridad y conexión de aplicaciones



- **Third-party application access via OAuth:** When enabled, allows third-part applications to connect using OAuth. To learn more, see [Change application connection & security policies for your organization](#).
- **SSH authentication access:** When enabled, allows applications to connect using SSH authentication. To learn more, see [Change application connection & security policies for your organization](#).
- **Allow public projects:** When enabled, users can create public projects which allows non-members of a project and users who aren't signed in read-only, limited access to the project's artifacts and services. Learn more at [Make your project public](#) and [Enable anonymous access to projects for your organization](#).

mE



Políticas de seguridad y conexión de aplicaciones



- **Restrict organization creation via Azure AD tenant policy** (*Only valid when the organization is backed by*

Azure Active Directory): When enabled, restricts users from creating additional Azure DevOps organizations that

would automatically be backed by the Azure AD. To learn how to enable, see Restrict organization creation via

[Azure AD tenant policy](#).

mE



Políticas de seguridad y conexión de aplicaciones



- **Enable Azure Active Directory (Azure AD) Conditional Access Policy (CAP) validation** (*Only valid when the organization is backed by Azure Active Directory*): When enabled, allows you to set additional conditions on accessing the organization. Depending on which conditions the user satisfies, you can require multi-factor authentication, further checks, or block access. This policy is set to *off* by default and only applies to alternative credentials. This policy doesn't apply for CAPs set in Azure AD, no matter the settings in Azure DevOps. To learn more, see [Change application connection & security policies for your organization](#).

mE



- **External guest access** (*Only valid when the organization is backed by Azure Active Directory.*): When enabled, invitations can be sent to email accounts of users who aren't members of the tenant Azure Active Directory through the **Users** page. To learn more, see [Add external users to your organization](#).
- **Allow team and project administrators to invite new users**: Only valid when the organization is backed by Azure Active Directory. When enabled, team and project administrators can add users through the **Users** page. To learn more, see [Restrict new user invitations from Project and Team Administrators](#).
- **Request access**: Only valid when the organization is backed by Azure Active Directory. When enabled, users can request access to a resource. A request results in an email notification to the administrators asking for review and access, as needed. To learn more, see [Add external users to your organization](#).
- **Invite GitHub users**: Only valid when the organization isn't backed by Azure Active Directory. When enabled, administrators can add users based on their GitHub user accounts from the **Users** page. To learn more, see [Authenticating & inviting GitHub users FAQs](#).

AUTHENTICATION

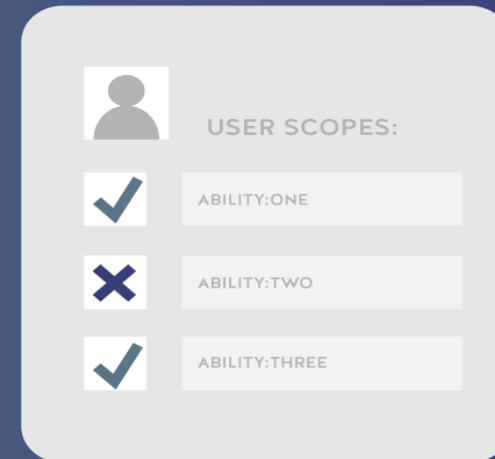


A diagram of an authentication form. At the top is a grey silhouette of a person's head and shoulders. Below it is a label 'USERNAME' followed by a white input field containing ten asterisks. Below that is a label 'PASSWORD' followed by another white input field containing ten asterisks. At the bottom is a dark blue rounded rectangle button with the word 'LOGIN' in white capital letters.

WHO ARE YOU?

VS

AUTHORIZATION



A diagram of an authorization form. At the top left is a grey silhouette of a person's head and shoulders. To its right is the label 'USER SCOPES:'. Below this are three rows, each with a small square icon on the left and a white input field on the right. The first row has a blue checkmark icon and the text 'ABILITY:ONE'. The second row has a blue 'X' icon and the text 'ABILITY:TWO'. The third row has a blue checkmark icon and the text 'ABILITY:THREE'.

CAN YOU DO THAT?

Authentication vs. authorization



► **Autenticación:** La autenticación es el proceso de demostrar que eres quien dices ser. A veces se abrevia a AuthN.

► **Autorización:** La autorización es el acto de otorgar permiso a una parte autenticada para hacer algo. Especifica a qué datos puede acceder y qué puede hacer con esos datos. La autorización a veces se abrevia a AuthZ.

mE



Autenticación

E

La autenticación verifica la identidad de una cuenta según las credenciales proporcionadas cuando inician sesión en Azure DevOps. Estos sistemas se integran y dependen de las características de seguridad proporcionadas por estos sistemas adicionales:

- Azure Active Directory (Azure AD)
- Cuenta de Microsoft (MSA)
- Directorio activo (AD)

Azure AD y MSA admiten la autenticación en la nube. Recomendamos Azure AD cuando necesite administrar un gran grupo de usuarios. De lo contrario, si tiene una base de usuarios pequeña que accede a su organización en Azure DevOps, puede usar cuentas de Microsoft

mE



Azure AD Multi-Factor Authentication

► How it works:

Azure AD Multi-Factor Authentication es un proceso en el que se solicita al usuario durante el proceso de inicio de sesión una forma adicional de identificación, como ingresar un código en su teléfono celular o proporcionar un escaneo de huellas digitales.

Si solo usa una contraseña para autenticar a un usuario, deja un vector inseguro para el ataque. Si la contraseña es débil o se ha expuesto en otro lugar, ¿es realmente el usuario que inicia sesión con el nombre de usuario y la contraseña, o es un atacante? Cuando necesita una segunda forma de autenticación, la seguridad aumenta, ya que este factor adicional no es algo que sea fácil de obtener o duplicar para un atacante.

Azure AD Multi-Factor Authentication

► How it works:

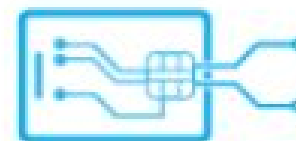
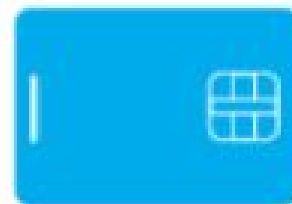
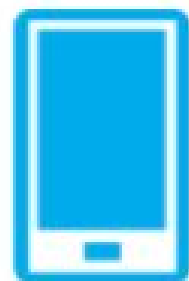
Azure AD Multi-Factor Authentication es un proceso en el que se solicita al usuario durante el proceso de inicio de sesión una forma adicional de identificación, como ingresar un código en su teléfono celular o proporcionar un escaneo de huellas digitales.

Si solo usa una contraseña para autenticar a un usuario, deja un vector inseguro para el ataque. Si la contraseña es débil o se ha expuesto en otro lugar, ¿es realmente el usuario que inicia sesión con el nombre de usuario y la contraseña, o es un atacante? Cuando necesita una segunda forma de autenticación, la seguridad aumenta, ya que este factor adicional no es algo que sea fácil de obtener o duplicar para un atacante.

Username

someone@example.com

Password




mE



Sign in to Microsoft Azure


Secure | https://login.microsoftonline.com/common/login

Microsoft Azure

 Microsoft


bals@contoso.com


Verify your identity

 Approve a request on my Microsoft Authenticator app

123

 Use a verification code from my mobile app

 Text +X XXXXXXXX40

 Call +X XXXXXXXX40

[More information](#)

Cancel

©2018 Microsoft Terms of use Privacy & cookies



mE



Métodos de verificación disponibles

Cuando un usuario inicia sesión en una aplicación o servicio y recibe un mensaje de MFA, puede elegir una de sus formas registradas de verificación adicional. Los usuarios pueden acceder a [Mi perfil](#) para editar o agregar métodos de verificación.

Las siguientes formas adicionales de verificación se pueden usar con la autenticación multifactor de Azure AD:

- Aplicación Microsoft Authenticator
- Token de hardware OATH (versión preliminar)
- Token de software OATH
- SMS
- Llamada de voz

Cómo administrar cuentas de usuario inactivas en Azure AD

En entornos grandes, las cuentas de usuario no siempre se eliminan cuando los empleados dejan una organización. Como administrador de TI, desea detectar y manejar estas cuentas de usuario obsoletas porque representan un riesgo de seguridad.

¿Qué son las cuentas de usuario inactivas?

Las cuentas inactivas son cuentas de usuario que los miembros de su organización ya no necesitan para obtener acceso a sus recursos. Un identificador clave para las cuentas inactivas es que no se han utilizado *durante un tiempo* para iniciar sesión en su

entorno. Debido a que las cuentas inactivas están vinculadas a la actividad de inicio de sesión, puede usar la marca de tiempo del último inicio de sesión que se realizó correctamente para detectarlas.

mE



¿Qué son las cuentas de usuario inactivas?

El desafío de este método es definir qué significa *por un tiempo* en el caso de su entorno. Por ejemplo, es posible que los usuarios no inicien sesión en un entorno *durante un tiempo* porque están de vacaciones. Al definir cuál es su delta para las cuentas de usuario inactivas, debe tener en cuenta todas las razones legítimas para no iniciar sesión en su entorno. En muchas organizaciones, el delta para las cuentas de usuario inactivas es de entre 90 y 180 días.

El último inicio de sesión exitoso proporciona información potencial sobre la necesidad continua de un usuario de acceder a los recursos. Puede ayudar a determinar si la membresía del grupo o el acceso a la aplicación aún son necesarios o podrían eliminarse. Para la administración de usuarios externos, puede comprender si un usuario externo todavía está activo dentro del inquilino o si debe limpiarse.

¿Qué son las cuentas de usuario inactivas?

El desafío de este método es definir qué significa *por un tiempo* en el caso de su entorno. Por ejemplo, es posible que los usuarios no inicien sesión en un entorno *durante un tiempo* porque están de vacaciones. Al definir cuál es su delta para las cuentas de usuario inactivas, debe tener en cuenta todas las razones legítimas para no iniciar sesión en su entorno. En muchas organizaciones, el delta para las cuentas de usuario inactivas es de entre 90 y 180 días.

El último inicio de sesión exitoso proporciona información potencial sobre la necesidad continua de un usuario de acceder a los recursos. Puede ayudar a determinar si la membresía del grupo o el acceso a la aplicación aún son necesarios o podrían eliminarse. Para la administración de usuarios externos, puede comprender si un usuario externo todavía está activo dentro del inquilino o si debe limpiarse.

mE



Quitar usuarios de Azure DevOps



Si los usuarios ya no necesitan acceso a un equipo, proyecto o su organización, puede eliminar su acceso. Los elementos de trabajo asignados a los usuarios no se ven afectados por la eliminación del acceso de los usuarios.

Quitar a un usuario de la organización no quita su membresía a ningún grupo de seguridad. Si el usuario es miembro de un grupo de seguridad que otorga acceso, el usuario aún tiene acceso a Azure DevOps, incluso después de eliminarlo de la organización. Si desea eliminar por completo al usuario de la organización, asegúrese de que no esté en ninguno de sus grupos de seguridad.

mE



Explicación practica!!

Project-level groups



For each project that you create, the system creates the followings project-level groups. These groups are assigned project-level permissions.

- Build Administrators
- Contributors
- Readers
- Project Administrators
- Project Valid Users
- Release Administrators
- *TeamName*

mE





Project Settings

DeploySQLDB



General



Overview



Teams



Permissions



Notifications



Service hooks



Dashboards



Boards



Project configuration



Team configuration



GitHub connections



Pipelines



Agent pools



Parallel jobs

Permissions













Groups Users

Search groups



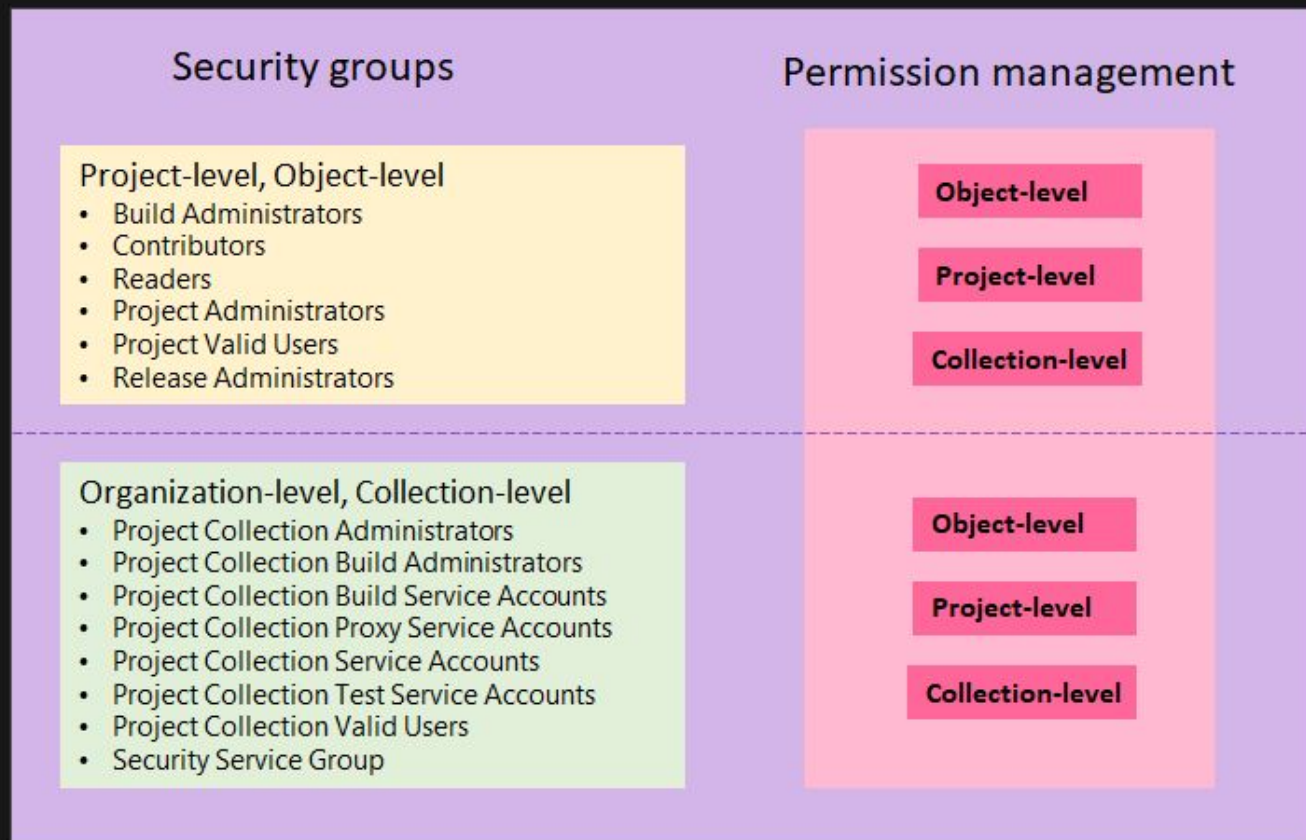
New Group

Total 9

Name	Description	Type ↓	Members
 Build Administrators	Members of this group can create, modify and delete build definitions and manage queued and completed builds.	Group	 0
 Contributors	Members of this group can add, modify, and delete items within the team project.	Group	 1
 Endpoint Administrators	Members of this group should include accounts for people who should be able to manage all the service connections.	Group	 1
 Endpoint Creators	Members of this group should include accounts for people who can create service connections.	Group	 2
 Project Administrators	Members of this group can perform all operations in the team project.	Group	 1
 Project Valid Users	Members of this group have access to the team project.	Group	 8

Permissions

As shown in the following image, security groups defined at the project and collection-level can be assigned to permissions assigned at the object, project, and organization-level.



Server-Level Roles



SQL Server proporciona roles a nivel de servidor para ayudarlo a administrar los permisos en un servidor. Estos roles son los principales de seguridad que agrupan a otros principales. Los roles a nivel de servidor son para todo el servidor en su ámbito de permisos. (Los *roles* son como *grupos* en el sistema operativo Windows).

Se proporcionan roles de servidor fijos por conveniencia y compatibilidad con versiones anteriores. Asigne permisos más específicos siempre que sea posible.

Puede agregar entidades principales de nivel de servidor (inicios de sesión de SQL Server, cuentas de Windows y grupos de Windows) en roles de nivel de servidor. Cada miembro de un rol de servidor fijo puede agregar otros inicios de sesión a ese mismo rol. Los miembros de roles de servidor definidos por el usuario no pueden agregar otros principales de servidor al rol.

mE



Fixed Server-Level Roles

- Sysadmin
- Serveradmin
- Securityadmin
- Processadmin
- Setupadmin
- Bulkadmin
- Diskadmin
- Dbcreator
- public

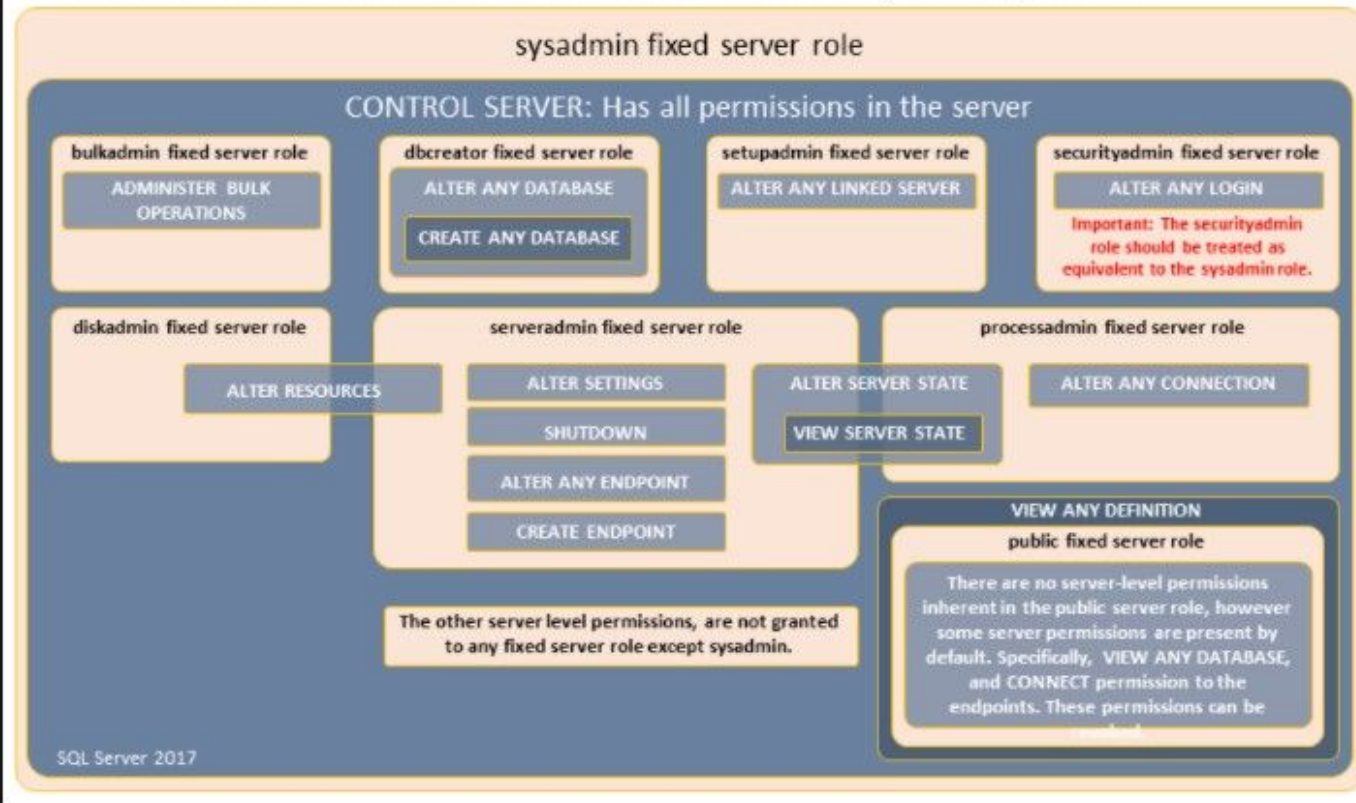
mE



Permissions of Fixed Server Roles

Each fixed server role has certain permissions assigned to it. The following graphic shows the permissions assigned to the server roles.

SERVER LEVEL ROLES AND PERMISSIONS: 9 fixed server roles, 34 server permissions



Roles de base de datos

E

Utilice roles de base de datos para gestionar con mayor facilidad los privilegios de los grupos de usuarios.

Los roles de base de datos simplifican el proceso de gestión de privilegios, ya que se pueden otorgar privilegios a un rol y luego otorgar el rol a usuarios. Cuando desee revocar privilegios para un usuario, simplemente tiene que revocar la autorización de rol del usuario, en vez de revocar cada privilegio individual.

mE



Roles de base de datos

E

Para administrar con facilidad los permisos en las bases de datos, SQL Server proporciona varios roles

, que son las entidades de seguridad que agrupan a otras entidades de seguridad. Son como los grupos del sistema operativo Microsoft Windows. Los roles de nivel de base de datos se aplican a toda la base de datos en lo que respecta a su ámbito de permisos.

Para agregar y quitar usuarios en un rol de base de datos, use las opciones ADD MEMBER y DROP MEMBER de la instrucción ALTER ROLE . Sistema de la plataforma de análisis (PDW) y Azure Synapse no admiten este uso de ALTER ROLE. En su lugar, use los procedimientos sp_addrolemember y sp_droprolemember anteriores.

Existen dos tipos de roles en el nivel de base de datos: los roles fijos de base de datos que están predefinidos en la base de datos y los roles de base de datos definidos por el usuario que el usuario puede crear.

Los roles fijos de base de datos se definen en el nivel de base de datos y existen en cada una de ellas. Los miembros de los roles de base de datos db_owner pueden administrar la pertenencia a roles fijos de base de datos.

mE



Roles fijos de base de datos

En la tabla siguiente se muestran los roles fijos de base de datos y sus funcionalidades. Estos roles existen en todas las bases de datos. A excepción del rol de base de datos **public**, no se pueden cambiar los permisos asignados a los roles fijos de base de datos.

- **db_owner**
- **db_securityadmin**
- **db_accessadmin**
- **db_backupoperator**
- **db_ddladmin**
- **db_datawriter**
- **db_datareader**
- **db_denydatawriter**
- **db_denydatareader**

DATABASE LEVEL ROLES AND PERMISSIONS: 11 fixed database roles, 77 database permissions

db_owner fixed database role

CONTROL DATABASE: Has all permissions in the database

db_datareader

GRANT SELECT ON DATABASE::<name>

db_denydatareader

DENY SELECT ON DATABASE::<name>

db_datawriter

GRANT INSERT ON DATABASE::<name>

GRANT UPDATE ON DATABASE::<name>

GRANT DELETE ON DATABASE::<name>

db_denydatawriter

DENY INSERT ON DATABASE::<name>

DENY UPDATE ON DATABASE::<name>

DENY DELETE ON DATABASE::<name>

db_accessadmin

CREATE SCHEMA

ALTER ANY USER

CONNECT

db_securityadmin

ALTER ANY ROLE, CREATE ROLE

ALTER ANY APPLICATION ROLE

VIEW DEFINITION

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.

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

There are various special purpose roles in the msdb database

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



Casos reales

- ▶ Borrar un AZURE SQL SERVER y se borraron todas las dbs
- ▶ Drop database
- ▶ Manejos de cientos de usuarios con permisos cada uno diferentes.

mE



MUCHAS
GRACIAS!



CONTACTO



mundosE
PEOPLE & BUSINESS SCHOOL