# Seguridad en MS SQL Server

## Introducción

- Permisos y usuarios
- Auditoría
- Cifrado
- Alta disponibilidad
- Copias de seguridad

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Permisos y usuarios

## Entidades

- SQL Server puede conceder permisos a las siguientes entidades:
  - Usuarios
  - Grupos de usuarios
  - Roles
  - Logins
  - Schemas

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Permisos y usuarios

## Niveles de seguridad

- Nivel Windows
  - Sencillo. Utilizar este método cuando sea posible.
  - Credenciales de la cuenta de usuario de S.O.
  - Por defecto: Win. admin → Server admin
- Nivel Sql Server
- Nivel base de datos

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Permisos y usuarios

## Niveles de seguridad

- Nivel Windows
- Nivel Sql Server
  - Logins y roles de servidor
  - Para usuarios que se conecten fuera de la empresa
  - Roles prefedinidos de servidor
    - bulkadmin: bulk insert operations; dbcreator: creates databases; diskadmin: manage disk resources; securityadmin: create, alter, drop; serveradmin: instance settings; sysadmin: any action
- Nivel base de datos

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Permisos y usuarios

## Niveles de seguridad

- Nivel Windows
- Nivel Sql Server
- Nivel base de datos
  - Usuarios asociados a Windows o Sql Server logins.
  - Estos login tienen asociados roles que a su vez contienen permisos sobre objetos (tablas, vistas, usuarios, bases de datos, claves de cifrado, procedimientos...)

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Permisos y usuarios

## Usuarios predefinidos

- guest: permite a un usuario de nueva creación poder acceder a la BD para concederle permisos
- dbo: tiene todos los permisos de la BD
- INFORMATION_SCHEMA: acceder a vistas y metadatos del sistema
- sys

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Permisos y usuarios

## Roles predefinidos de base de datos

- public: rol asignado por defecto a todos los usuarios, cualquier permiso asignado a public es compartido por todos los usuarios
- db_accessadmin
- db_datareader
- db_ddladmin
- db_owner
- db_securityadmin

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Permisos y usuarios

## Entidad Schema

- Se usa a modo de plantilla de permisos para BDs.
- Contenedor con todos los objetos y permisos de una BD
- El propietario del schema es el creador de BD
- Esto permite eliminar usuarios dentro del “esquema” propietarios de un objeto sin tener que borrar también el objeto.

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Permisos y usuarios

## Entidad login

- Los hay de 5 tipos
  - Standard SQL Server login
  - Windows login
  - Windows group
  - Certificate
  - Asymmetric key

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Permisos y usuarios

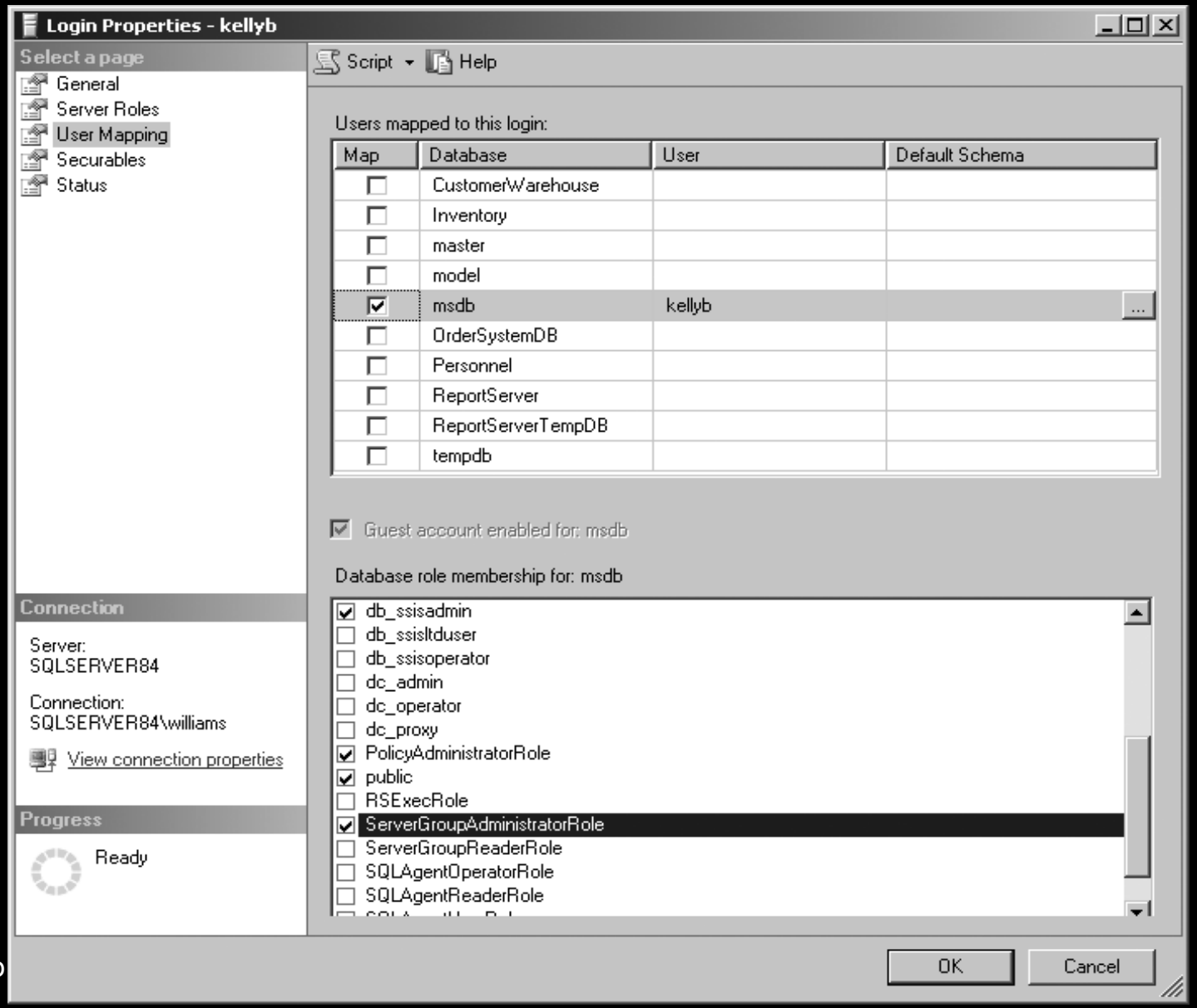
## Entidad login

- Standard SQL Server login
  - CREATE LOGIN sqltest WITH PASSWORD = 'P@55w0rd'
  - Mejor con Sql Server Management Studio...

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Permisos y usuarios

## Entidad login




Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Permisos y usuarios

## Usuarios

- Creación de usuarios
  - ```
    CREATE USER user_name
    [ { { FOR | FROM }
    {
    LOGIN login_name
    | CERTIFICATE cert_name
    | ASYMMETRIC KEY asym_key_name
    }
    | WITHOUT LOGIN
    ```
- ¿WITHOUT LOGIN? → EXECUTE AS (impersonation)

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor
    ```

# Permisos y usuarios

## Permisos sobre objetos

- Objetos

  Application roles
  Asymmetric keys
  Certificates
  Database roles
  Databases
  Synonyms
  User-defined data types
  Views
  Assemblies
  Full-text catalogs
  Functions
  Schemas
  Stored procedures
  Symmetric keys
  Tables
  Users
  XML schema collections

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Permisos y usuarios

## Permisos sobre objetos

- Permisos

SELECT
INSERT
UPDATE
DELETE
EXECUTE
REFERENCES
CONTROL
ALTER
VIEW DEFINITION
TAKE OWNERSHIP

CREATE DATABASE
CREATE DEFAULT
CREATE FUNCTION
CREATE PROCEDURE
CREATE RULE
CREATE TABLE
CREATE VIEW
BACKUP DATABASE
BACKUP LOG

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Permisos y usuarios

## Permisos sobre objetos

- GRANT permiso ON objeto TO entidad

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Auditoría

## Creación de una auditoría

- Crear una auditoría y definir el destino (mediandte CREATE SERVER AUDIT o Management Studio)
  - Nombre auditoría, retardo cola, acción en caso de error, destino, tamaño máximo del log
- Crear una especificación de auditoría que se asigne a la auditoría anteriomente creada
  - A nivel de servidor
  - A nivel de base de datos
    - Acciones de auditoría a nivel de base de datos
  - A nivel de auditoría
- Habilitar la auditoría

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Auditoría

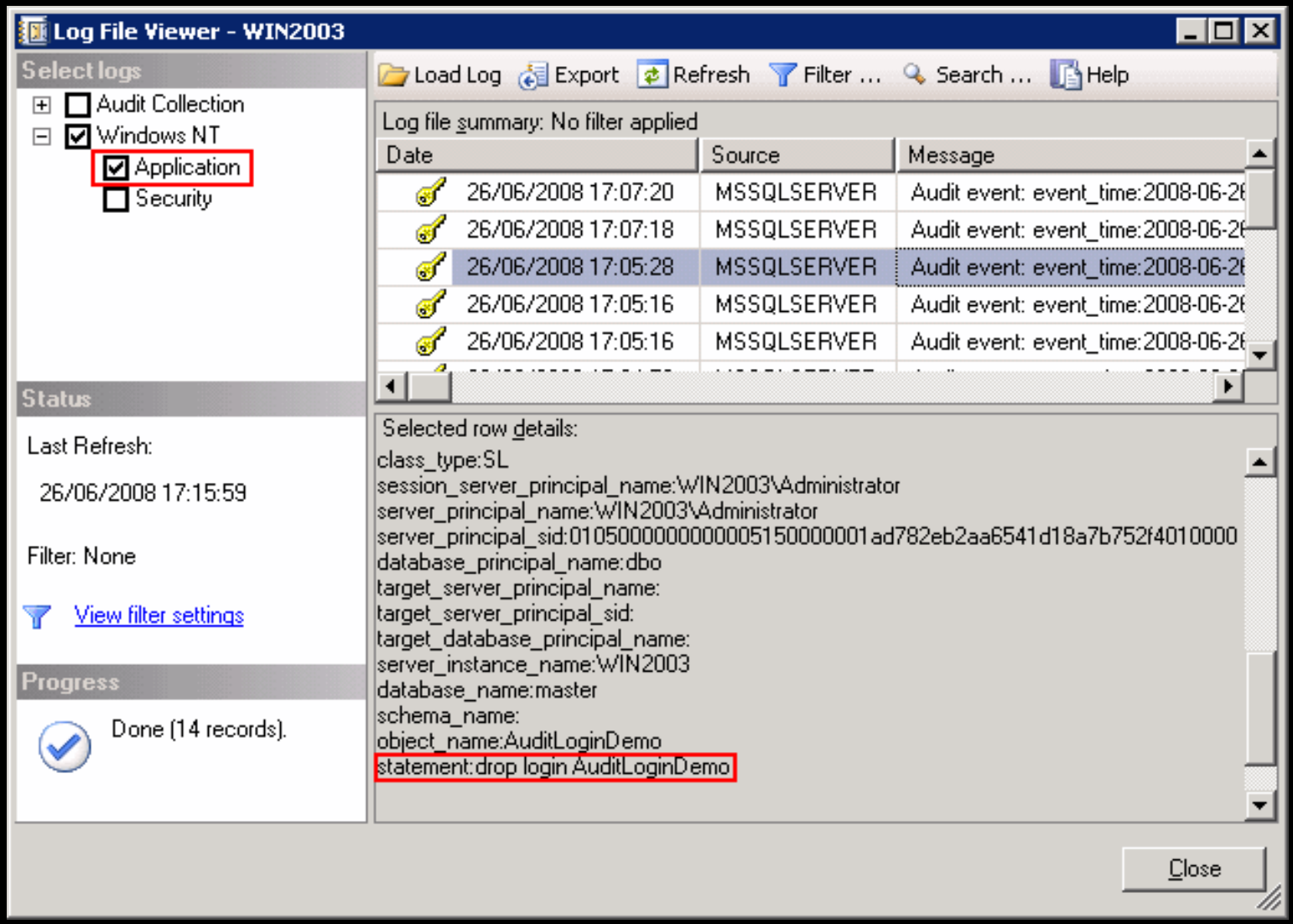
## Tipos de especificaciones

- CREATE SERVER AUDIT SPECIFICATION, CREATE DATABASE AUDIT SPECIFICATION
- A nivel de servidor
  - APPLICATION_ROLE_CHANGE_PASSWORD_GROUP, LOGOUT_GROUP, DATABASE_PERMISSION_CHANGE_GROUP, SERVER_OPERATION_GROUP
- A nivel de base de datos
  - DATABASE_PRINCIPAL_CHANGE_GROUP, DATABASE_ROLE_MEMBER_CHANGE_GROUP
  - select, update, insert, delete, execute, receive, references
- A nivel de auditoría
  - AUDIT_ CHANGE_GROUP

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Auditoría

## Registro de eventos




event_time
succeeded
message
instance
user
session_id
database_na
mestatement
...

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Encriptación

## Encriptación de datos transparente (TDE)

- Inconvenientes existentes en el pasado
  - Los tipos de las columnas debías ser cambiados por **varbinary**
  - Determinados tipos de búsquedas no eran permitidas (rango e igualdad)
  - Consultas por medio de procedimientos almacenados que contenían las herramientas de desencriptado
- Con TDE
  - Encriptación a nivel de celda y de base de datos
  - Se realizan un scan en segundo plano de todos los .mdf para su encriptación (operaciones normales contra la base de datos no entran en conflicto con esto)
  - Los datos en caché también son encriptados
  - Algoritmos soportados: AES hasta 256 bits y triple DES
  - Habría que habilitar seguridad SSL para comunicación cliente –

# Encriptación

## Cómo habilitar TDE

- Crear la database master key
  - CREATE MASTER KEY ENCRYPTION BY PASSWORD = ‘some password’;
- Crear la database encryption key (o añadir certificado ya existente)
  - Certificado autofirmado
  - CREATE CERTIFICATE tdeCert WITH SUBJECT = ‘TDE Certificate’;
- Crear backup del certificado y de la clave privada
  - BACKUP CERTIFICATE tdeCert TO FILE = ‘path_to_file’

    WITH PRIVATE KEY ( FILE = ‘path_to_private_key_file’,

    ENCRYPTION BY PASSWORD = ‘cert password’);

# Encriptación

## Cómo habilitar TDE

- (Opcional) Habilitar protocolo SSL
- Encriptar la database encryption key con el certificado creado en pasos anteriores
  - CREATE DATABASE ENCRYPTION KEY
  - WITH ALGORITHM = AES_256
  - ENCRYPTION BY SERVER CERTIFICATE tdeCert
- Habilitar TDE
  - ALTER DATABASE myDatabase SET ENCRYPTION ON
- Monitorizar los cambios
  - sys.dm_database_encryption_keys

# Encriptación

## Otras tecnologías

- Cell-level encryption
- Basadas en Windows
  - Encrypting File System (EFS)
  - BitLocker™ Drive Encryption

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Alta disponibilidad

## Herramientas y mejoras

- El conjunto de herramientas de AD se llama *Always ON* desde SQL-Server 2012.

- Principal novedad son los grupos de disponibilidad.
  - Conjunto de bases de datos.
  - Una réplica principal y hasta cuatro secundarias.
  - Réplicas auxiliares de solo lectura.

- http://msdn.microsoft.com/es-es/library/cc645581.aspx

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Copias de seguridad

## Estrategias

- Recomendable usar sp_spaceused para calcular el tamaño.
- Dos estrategias recomendadas:
  - Backup completo.
  - Backup parcial
- Además si queremos hacerla por marca de tiempo podemos incluir la clausula: “*WITH DIFFERENTIAL*”

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Copias de seguridad

## Backup completo

- Utilizar solo en períodos de baja actividad.
- **Deben** hacerse periodicamente.

```
BACKUP DATABASE { database_name | @database_name_var }
  TO <backup_device> [ ,...n ]
  [ <MIRROR TO clause> ] [ next-mirror-to ]
  [ WITH { DIFFERENTIAL | <general_WITH_options> [ ,...n ] } ]
[;]
```

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Copias de seguridad

## Recuperación de una BD completa

```
RESTORE DATABASE { database_name | @database_name_var }
 [ FROM <backup_device> [ ,...n ] ]
 [ WITH   {
    [ RECOVERY | NORECOVERY | STANDBY =   {standby_file_name |
@standby_file_name_var }   ]
   | ,  <general_WITH_options> [ ,...n ]   | , <replication_WITH_option>
   | , <change_data_capture_WITH_option>   | , <FILESTREAM_WITH_option>
   | , <service_broker_WITH options>   | , <point_in_time_WITH_options—
RESTORE_DATABASE>    } [ ,...n ]
 ]
[;]
```

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Copias de seguridad

## Backup parcial

- Backup de archivos especificados o grupos de ellos.
- Contendrá:
  - Los grupos de archivos principales.
  - Los de escritura/lectura
  - Opcionalmente los de solo lectura.

# Copias de seguridad

## Backup parcial

```
BACKUP DATABASE { database_name | @database_name_var }
 <file_or_filegroup> [ ,...n ]
  TO <backup_device> [ ,...n ]
  [ <MIRROR TO clause> ] [ next-mirror-to ]
  [ WITH { DIFFERENTIAL | <general_WITH_options> [ ,...n ] } ]
[;]
```

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor

# Copias de seguridad

## Recuperación parcial

```
RESTORE DATABASE { database_name | @database_name_var }
   <file_or_filegroup> [ ,...n ]
 [ FROM <backup_device> [ ,...n ] ]
   WITH
   {  [ RECOVERY | NORECOVERY ]
      [ , <general_WITH_options> [ ,...n ] ]
   } [ ,...n ]
[;]
```

Juan Luis Carratalá Castillo
Víctor Perdomo Pastor