Вербицкий Илья
WebStoating s.r.o.

PGDAY'17 RUSSIA
КОНФЕРЕНЦИЯ ПО БАЗАМ ДАННЫХ

Все, что разработчики хотели знать о безопасности баз данных, но боялись спросить.

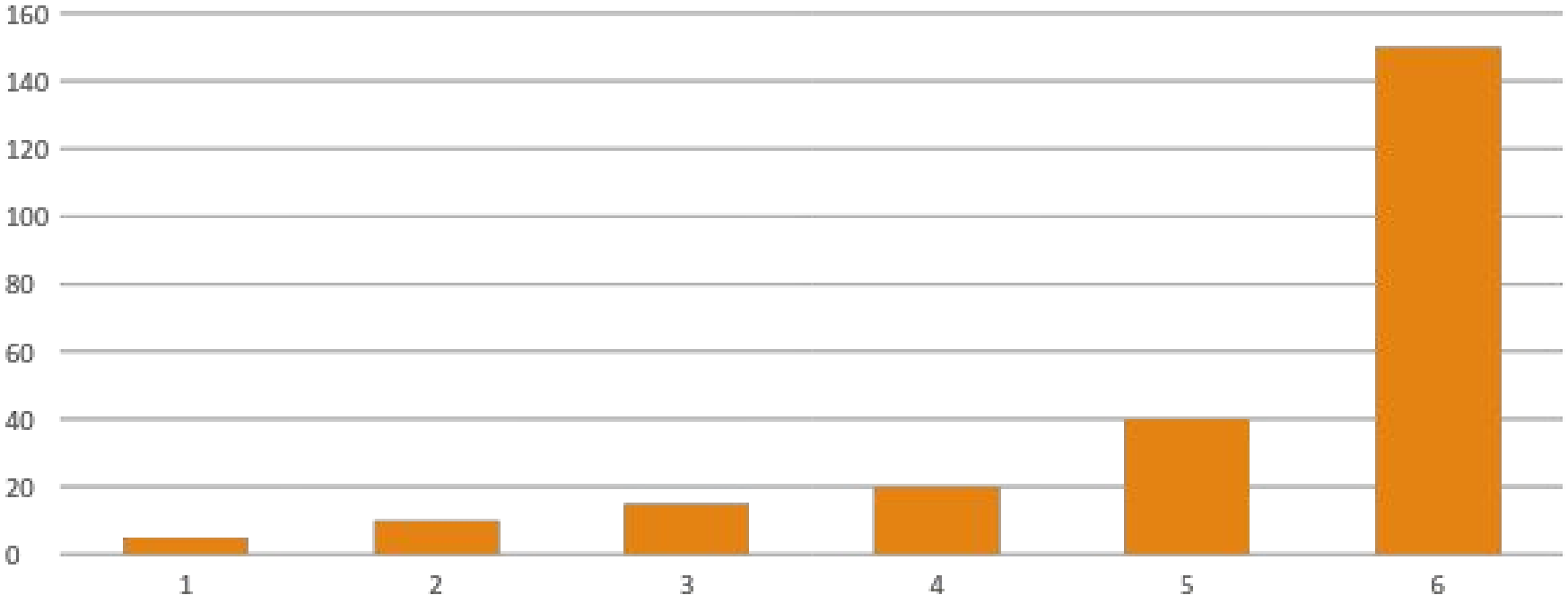
Вербицкий Илья

- 15 лет в финансах и электронной коммерции.
- Основатель компании WebStoating.
- Архитектура информационных систем, системная интеграция и электронная коммерция.
- https://verbitskiy.co/
- Twitter: @ilich_x86
- GitHub: https://github.com/ilich

О чем пойдет речь?

- Угрозы информационной безопасности;
- Сертификация SQL Server;
- Авторизация и аутентификация;
- Шифрование данных;
- Безопасность приложений.

Сколько стоит баг?



Основные угрозы безопасности БД

- Ошибки в настройках прав доступа к объектам БД;
- Инъекции;
- Отсутствие аудита;
- Небезопасное хранение резервных копий;
- Уязвимости в СУБД и ошибки конфигурации;
- Ошибки при работе с чувствительными данными;
- Небезопасные пароли пользователей;
- DoS-атаки.

Стандарты безопасности:

- Common Criteria – EAL4+
- FIPS 140-2
- HIPPA
- PCI
- ФСТЭК
  - https://www.microsoft.com/ru-ru/securitycertification/products.aspx
  - SQL Server 2005, 2008, 2012, 2014

Common Criteria

- Resource Information Protection (RIP);
  - **ПРОИЗВОДИТЕЛЬНОСТЬ!**
- Аудит попыток подключения к базе данных;
- DENY таблицы имеет более высокий приоритет, чем GRANT столбца

```
sp_configure 'show advanced options', 1;
GO
RECONFIGURE;
GO
sp_configure 'common criteria compliance enabled', 1;
GO
RECONFIGURE WITH OVERRIDE;
GO
```

FIPS 140-2

- Требования безопасности для криптографических модулей;
  - NIST (США)
  - CSE (Канада)
- Необходимо запускать SQL Server в сертифицированной операционной системе или подключить сертифицированные криптографические модули;
  - Windows Server 2012+
  - Windows 8+
- **ПРОИЗВОДИТЕЛЬНОСТЬ!**

Учетная запись службы SQL Server

- Виртуальная учетная запись службы (по умолчанию);
- Управляемая учетная запись;
- Учетная запись домена;
- Локальная учетная запись;
- ~~NETWORK SERVICE~~
- ~~LOCAL SYSTEM~~

Рекомендации

- Используйте виртуальную учетную запись или управляемую учетную запись;
- Используйте SQL Server Configuration Manager, чтобы изменить учетную запись сервиса;
- Если используете аккаунт домена, то регулярно меняйте пароль;
- Безопасность агента SQL Server.
  - Создавайте специально выделенные учетные записи-посредники и для выполнения шагов заданий пользуйтесь только ими.
  - Предоставляйте разрешения только необходимым учетным записям-посредникам.

Сетевые протоколы

- Общая память;
- Именованные каналы;
- Протокол TCP/IP;
- Выделенное административное соединение (DAC).

Сетевая безопасность

- Используйте только необходимые сетевые протоколы;
- Порт SQL Server по умолчанию – TCP/1433;
- Не используйте динамические порты для запуска именованных экземпляров SQL Server;
- Разрешить подключение только из локальной/доверенной подсети или только с локального компьютера;
- Запретите протоколы NetBIOS и SMB (UDP/137, UDP/138, TCP/139, TCP/445);
- Используйте расширенную защиту проверки подлинности;
- Пропишите, какие пользователи имеют право CONNECT к вашим конечным точкам (ENDPOINT). Для всех остальных пользователей и групп пропишите, что они не могут этого делать (DENY CONNECT).

Проверка подлинности в SQL Server

- Режим проверки подлинности Windows:
  - Имеется контроллер домена;
  - Приложение и база данных находятся на одном компьютере.
- Режим смешанной аутентификации:
  - При наличии рабочей группы;
  - Пользователи подключаются из разных недоверенных доменов;
  - Интернет-приложения, например, ASP.NET.

Типы имен входа (LOGIN)

- Учетная запись локального пользователя Windows или учетная запись доверенного домена;
- Группа пользователей Windows;
- Имя входа SQL Server.

Политика паролей

- Учетные записи Windows используют локальную политику безопасности или политику безопасности домена;
- Учетные записи SQL Server:
  - CHECK_POLICY
  - CHECK_EXPIRATION
  - MUST_CHANGE

Рекомендации

- Используйте режим проверки подлинности Windows;
- Используйте пользователей Windows вместо групп;
- Используйте триггеры входа, если необходим дополнительный контроль за процедурой аутентификации;
- Всегда используйте политику паролей;
- Режим смешанной аутентификации:
  - Всегда указывайте параметр MUST_CHANGE;
  - Разрешайте только зашифрованные соединения с сервером баз данных;
  - Используйте сертификат доверенного корневого центра сертификации.

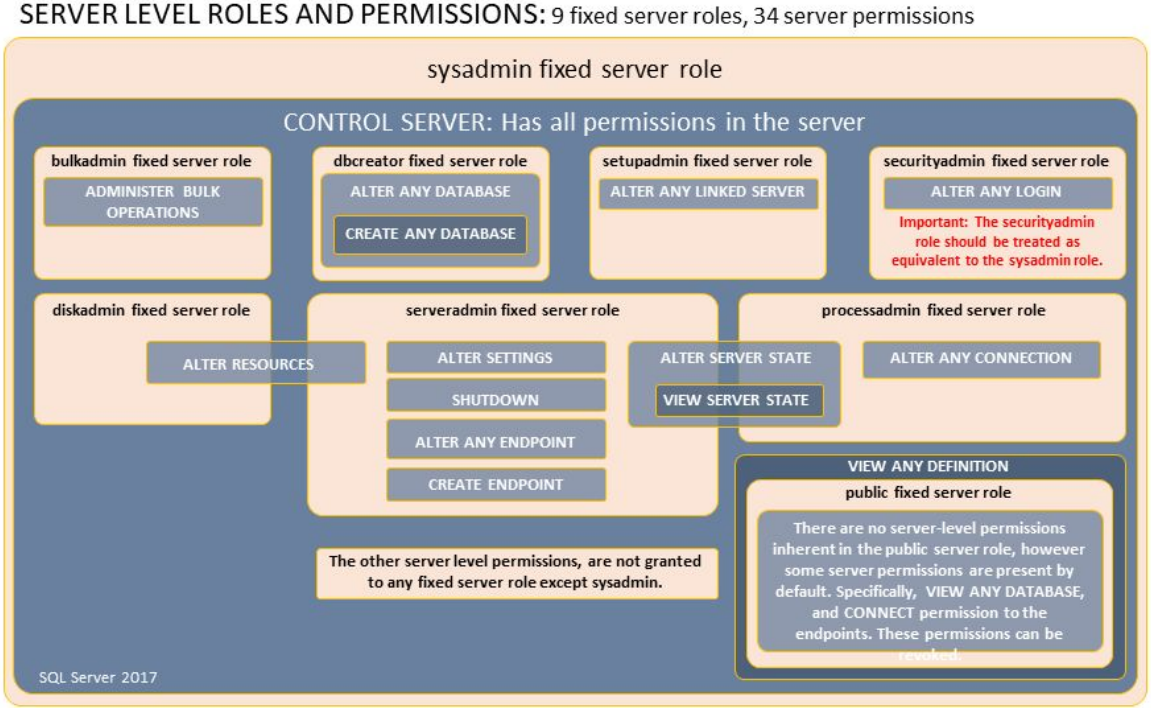
Автономные базы данных

- Метаданные хранятся в базе данных;
- База данных может выполнять проверку подлинности пользователей;
- Зачем?
  - Простота переноса;
  - Группа доступности AlwaysOn;
  - Простота в разработке и развертывании;
  - Простота в администрировании.

Безопасность автономных баз данных

- Пользователь автономной базы данных имеет доступ guest к другим базам данных на сервере, если пользователь guest не заблокирован;
- Отказ в обслуживании, если имя пользователя и пароль автономной базы данных совпадает с пользователем SQL Server
  - Пользователи серверной роли sysadmin должны подключаться без использования параметра исходного каталога;
  - Не создавать пользователей автономной базы данных с паролями, имена которых совпадают с именами входа SQL Server;
  - При наличии автономных баз данных пользователи баз данных, не являющихся автономными, должны подключаться, указывая в качестве исходного каталога имя неавтономной базы данных или не указывая каталог вообще.

Предопределенные роли сервера

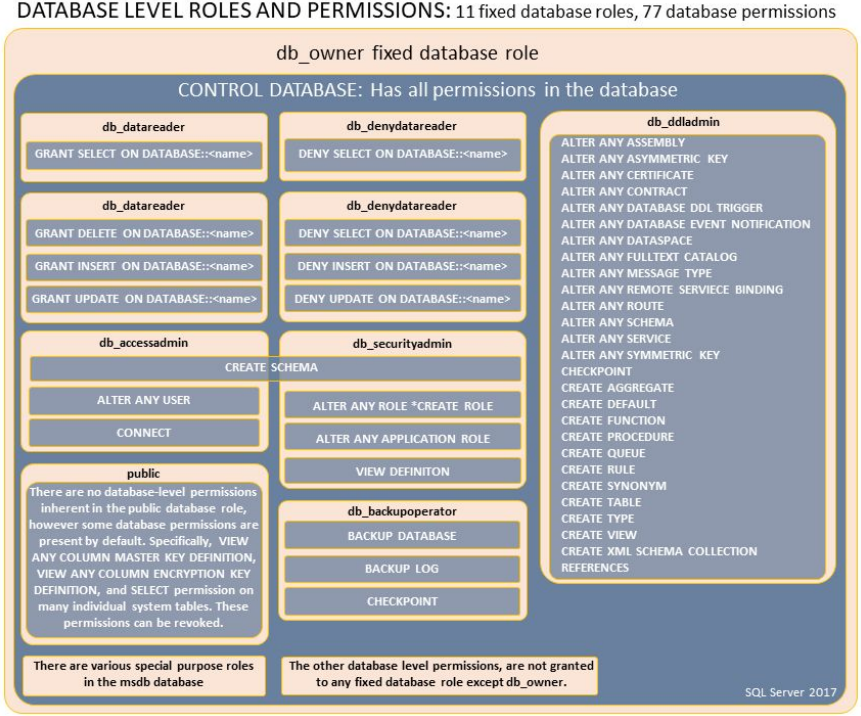


Источник:
https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/server-level-roles

Роль sysadmin

- Члены данной роли сервера могут выполнять любые действия на сервере;
- Любой пользователь, у которого есть права CONTROL SERVER;
- Члены роли по-умолчанию:
  - sa
  - BUILTIN\Administrators
- Минимизируйте количество администраторов;
- Не используйте sa аккаунт и заблокируйте его;
- Удалите BUILTIN\Administrators из роли sysadmin;
- Роль должна назначаться только конкретным пользователям;
- Разрешите администратору VIEW SERVER STATE вместо CONTROL SERVER или роли sysadmin.

Предопределенные роли базы данных



Источник:
https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/database-level-roles

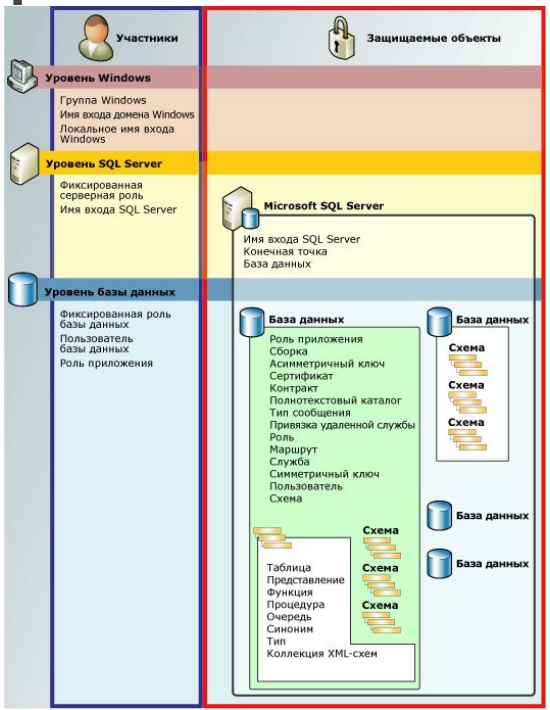
Роли приложений

- Позволяют приложению выполняться с определенными правами доступа;
- Роли приложения имеют доступ к другим базам данных с правами пользователя guest;
- Роль приложения активируется при помощи хранимой процедуры sp_setapprole и пароля;
- При передаче пароля по сети следует использовать шифрование канала.

Пользовательские схемы

- Именованный контейнер для объектов базы данных;
- Владелец схемы – пользователь, роль базы данных или роль приложения;
- Управляйте правами доступа к объектом баз данных, используя схемы;
- Минимизируйте количество владельцев схемы;
- Схема dbo представляет собой схему по умолчанию для вновь созданной базы данных;
- Пользователи, которым назначена схема dbo, не наследуют разрешения пользовательской учетной записи dbo.

Иерархия разрешений



Источник:
https://docs.microsoft.com/ru-ru/sql/relational-databases/security/permissions-hierarchy-database-engine

Принцип наименьших привилегий

- Пользователям из отдела кадров не нужны права администратора базы данных;
- Web-приложение для отображения отчетов по продажам может выполнять операцию SELECT, при этом CRUD операции должны быть запрещены;
- Менеджер может редактировать информацию об адресе сотрудника, ни никак не размер его заработной платы, ФИО и дату рождения;
- Сервису для ведения логирования нужно разрешить только операцию INSERT и только в таблицу, где хранится информация о событиях.

Контекст выполнения

- EXECUTE AS CALLER (по умолчанию)
- EXECUTE AS OWNER
- EXECUTE AS SELF
- EXECUTE AS 'username’
- Рекомендации:
  - Явно указывайте контекст выполнения хранимых процедур;
  - Явно указывайте права на объекты базы данных при написании скриптов;
  - Автоматическая проверка скриптов.

Свойство TRUSTWORTHY

- ON – SQL Server доверяет базе данных и ее содержимому, и она может обращаться к ресурсам вне ее видимости.
  - Повышение привилегий через выполнение процедур с опцией EXECUTE AS OWNER в базах данных, которыми владеет администратор системы (sa, роль sysadmin);
  - База данных может содержать вредоносные сборки с параметром разрешения EXTERNAL_ACCESS или UNSAFE.
- OFF по умолчанию.

Источник: https://technet.microsoft.com/ru-ru/library/ms188304(v=sql.105).aspx

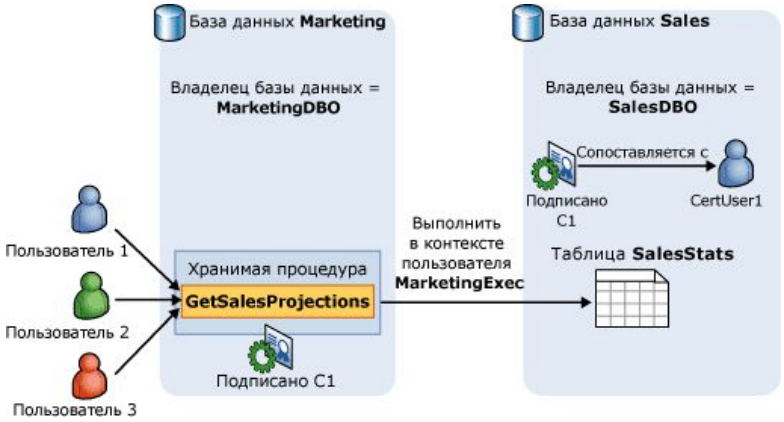
Привилегия IMPERSONATE

- Пользователь может запускать код с привилегиями другого пользователя.

```
EXECUTE AS LOGIN = 'sa'
SELECT SYSTEM_USER
SELECT IS_SRVROLEMEMBER('sysadmin’)
```

- Не используйте привилегию IMPERSONATE.
- Используйте подписанные хранимые процедуры в качестве альтернативы.
  - **Будьте внимательны с SQL инъекциями в подписанных хранимых процедурах. Это может привести к эскалации привилегий!**

Подписанные хранимые процедуры



- Код GetSalesProjections может быть изменен только пользователем, который владеет закрытым ключом к сертификату C1.

Источник: https://technet.microsoft.com/ru-ru/library/ms188304(v=sql.105).aspx

Инъекции

- Инъекции в клиентском коде;
- Инъекции при выполнении динамического SQL внутри хранимых процедур;
- Инъекции в строке подключения к базе данных.

Системные хранимые процедур и внешние источники данных

- OPENROWSET и OPENDATASOURCE;
  - Используйте связанные серверы.
- xp_cmdshell ;
- xp_servicecontrol;
- Электронная почта (sp_send_dbmail и другие);
- Файловая система (xp_dirtree, xp_subdirs и другие);
- Реестр (xp_regread, xp_regwrite и другие);
- COM-компоненты (sp_OACreate и другие);
- Хранимые процедуры CLR.

Контроль доступа к записям в таблице

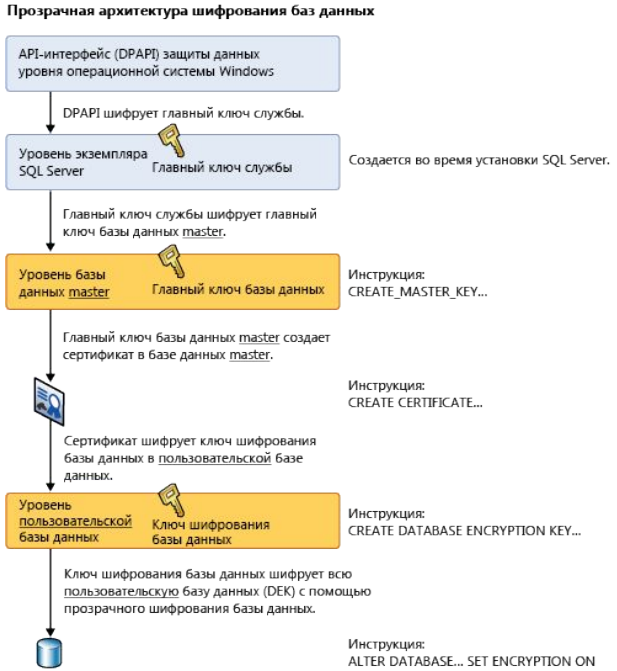
```
CREATE FUNCTION Security.fn_JohnCanSeeOnlyVolumeDiscount(@Type
sysname)
    RETURNS TABLE
WITH SCHEMABINDING
AS
    RETURN SELECT 1 AS AccessResult
    WHERE (@Type = 'Volume Discount' AND USER_NAME() = 'john’)
        OR USER_NAME() <> 'john';
GO

CREATE SECURITY POLICY Security.SampleSecurityPolicy
ADD FILTER PREDICATE
Security.fn_JohnCanSeeOnlyVolumeDiscount(Type) ON
```

Аудит пользователей, ролей и прав

- https://goo.gl/9FXQH6
- https://goo.gl/HbvnUs
- https://goo.gl/na7EEE
- https://goo.gl/EB55nC

Прозрачное шифрование данных (TDE)

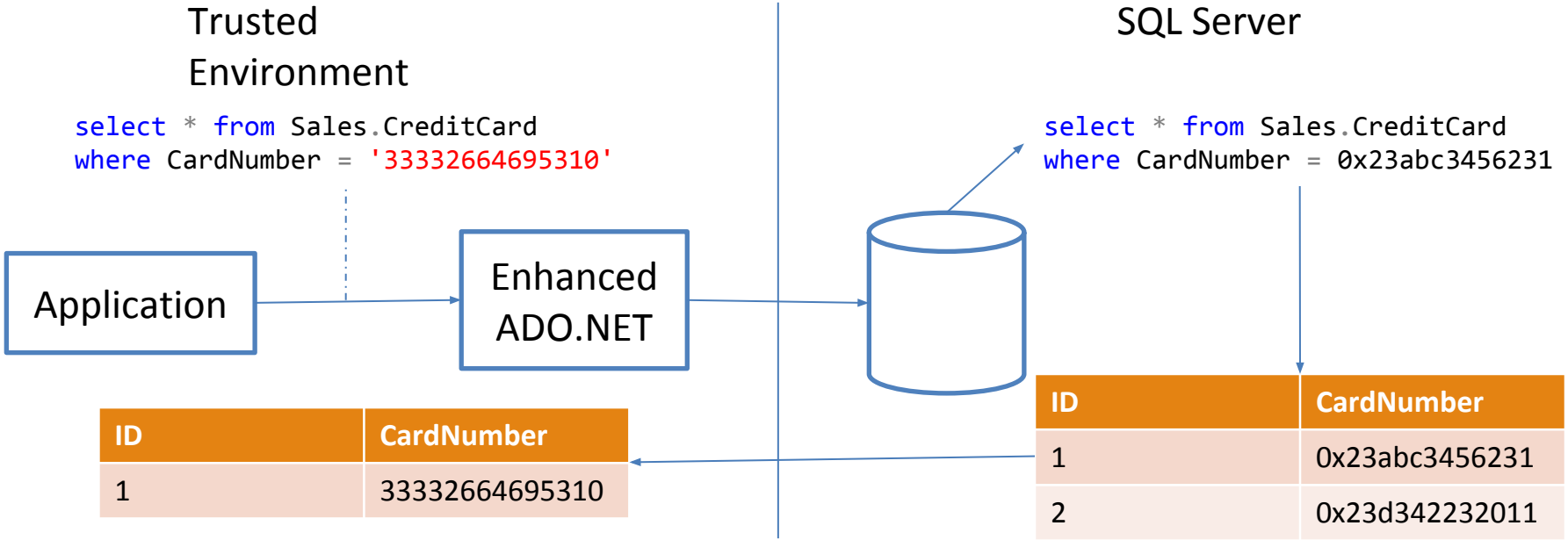


- Защита от физической кражи носителя данных;
- Шифрование файлов данных и журналов в реальном времени;
- Данные доступны системным администраторам (роль sysadmin).

Источник: https://docs.microsoft.com/ru-ru/sql/relational-databases/security/encryption/transparent-data-encryption-tde

Always Encrypted

- Пользовательские данные недоступны системным администраторам.



Криптографические функции

- HashBytes. Поддержка MD2, MD4, MD5, SHA, SHA1, SHA2 256, SHA2 512.
- EncryptByAsymKey / DecryptByAsymKey.
- EncryptByCert / DecryptByCert.
- EncryptByKey / DecryptByKey.
- EncryptByPassPhrase / DecryptByPassPhrase.
- VerifySignedByCert / SignByCert
- VerifySignedByAsymKey / SignByAsymKey
- Cert_ID.
- Crypt_Gen_Random.

Динамическое маскирование данных

```
ALTER TABLE Sales.CreditCard
ALTER COLUMN CardNumber ADD MASKED WITH (FUNCTION = 'partial(0, "XXXXXXXXXXX",
4)')

ALTER TABLE Sales.CreditCard
ALTER COLUMN ExpMonth ADD MASKED WITH (FUNCTION = 'default()')

ALTER TABLE Sales.CreditCard
ALTER COLUMN ExpYear ADD MASKED WITH (FUNCTION = 'default()')

GRANT UNMASK TO john

REVOKE UNMASK FROM john

ALTER TABLE Sales.CreditCard
ALTER COLUMN ExpMonth DROP MASKED
```

Защита интеллектуальной собственности

- Зашифрованные хранимые процедуры и функции;
- SQL Azure;
- VPN.

Шифрование резервных копий

```
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'P@ssw0rd'

CREATE CERTIFICATE AdventureWorks2016CTP3BackupCert
   WITH SUBJECT = 'AdventureWorks2016CTP3 Backup Encryption Certificate'

BACKUP DATABASE AdventureWorks2016CTP3
TO DISK = N'C:\SQL_Backup\AdventureWorks2016CTP3.bak'
WITH
  COMPRESSION,
  ENCRYPTION (
     ALGORITHM = AES_256,
     SERVER CERTIFICATE = AdventureWorks2016CTP3BackupCert),
  STATS = 10
```

Аудит

- Конфигурация аудита.
  1. Создайте аудит.
  2. Создается либо спецификация аудита сервера, либо базы данных;
  3. Включается спецификация аудита;
  4. Включите аудит.
- Аудит по стандарту безопасности C2.

```
sp_configure 'show advanced options', 1
GO
RECONFIGURE
GO
sp_configure 'c2 audit mode', 1
GO
RECONFIGURE
GO
```

Вопросы?