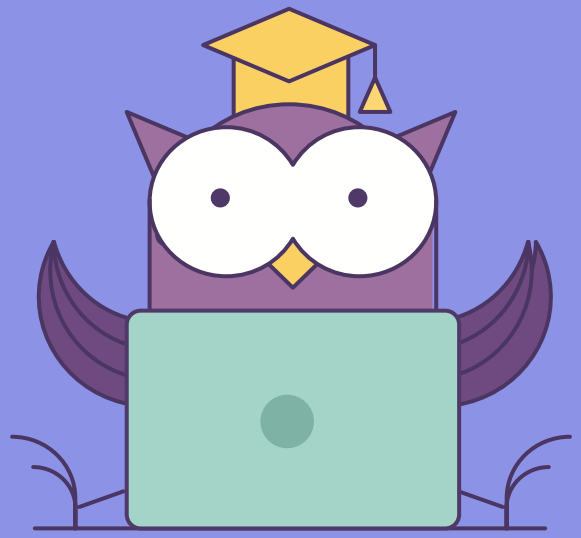
ОНЛАЙН-ОБРАЗОВАНИЕ

Проверить включена ли запись?

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Или напишите, какие есть проблемы

OTUS

Безопасность в SQL Server

Курс “MS SQL Server разработчик”

Павел Стрекалов

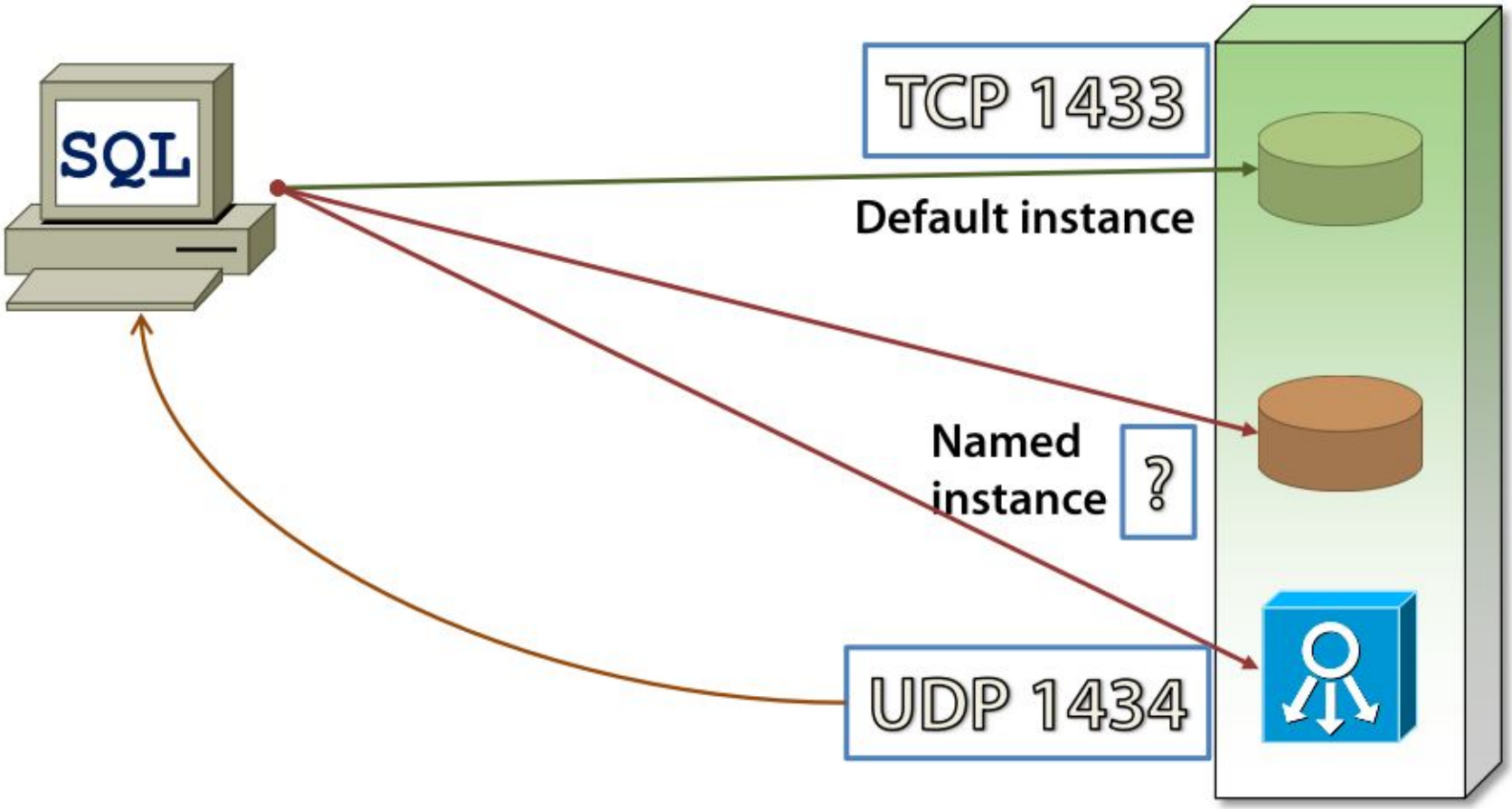
Содержание

1. Логины, пользователи, роли
2. Шифрование
3. Row-Level Security
4. Dymanic Data Masking

Уровни

- Сеть
- Сервер
- Экземпляр SQL Server
- База данных
- Таблица
- ХП, функции, ...

Подключение к SQL Server



ДЕМО

Настройка портов

01

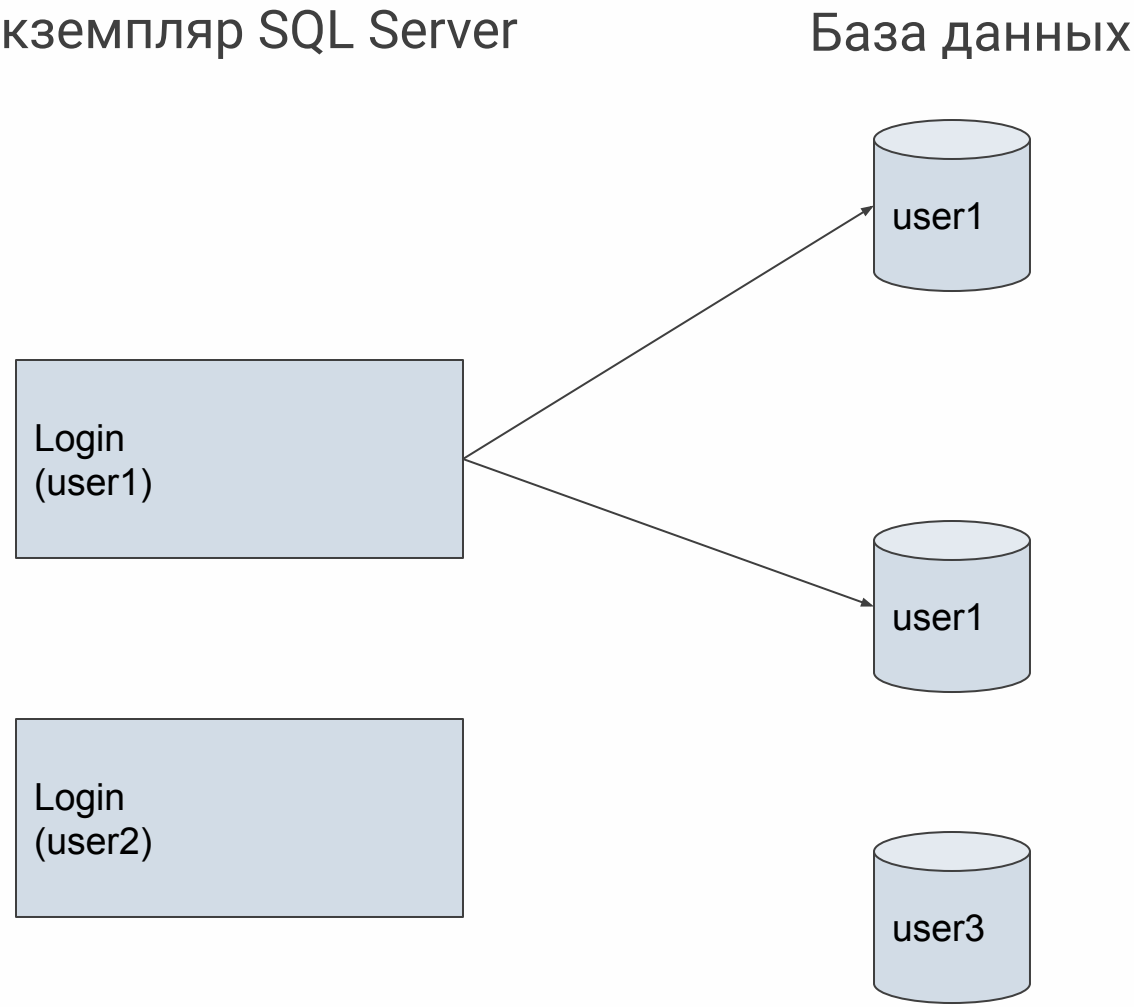
Login, User, Role

Объекты

- Principals (субъекты безопасности)
  - Логины, пользователи, роли и тд
- Securables (объекты безопасности)
  - Схема, таблицы, ХП и тд
- Permissions (разрешения)
  - Просмотр таблицы, запуск ХП и тд

- Управление через DCL (Data Control Language) или ХП
  - CREATE
  - GRANT
  - REVOKE
  - DENY

Логины и пользователи



Аутентификация

- Windows
- SQL Server
- Сертификаты
- Открытый/закрытый ключ

Роли

- Роли уровня сервера
  - встроенные (sysadmin, securityadmin, serveradmin, setupadmin, processadmin, diskadmin, dbcreator, bulkadmin)
  - пользовательские
- Роли уровня БД
  - встроенные (db_owner, db_securityadmin, db_accessadmin, db_backupoperator, db_ddladmin, db_datawriter, db_datareader, db_denydatawriter, db_denydatareader)
  - пользовательские
  - роли приложений (sp_setapprole)

ДЕМО

Логины, пользователи

Нужно новому пользователю предоставить доступ на чтение всех таблиц в БД. Какие объекты надо создать? Какие роли назначить?

02

Шифрование

Шифрование в SQL Server

Шифрование — обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней.

- **Вручную отдельные поля**, T-SQL (с 2005)
  - симметричное или ассиметричное с сертификатами
- Прозрачное шифрование данных, TDE (с 2008)
  - сертификат + DEK
- Резервные копии
- **Always Encrypted** (с 2016)
  - ключи вне базы

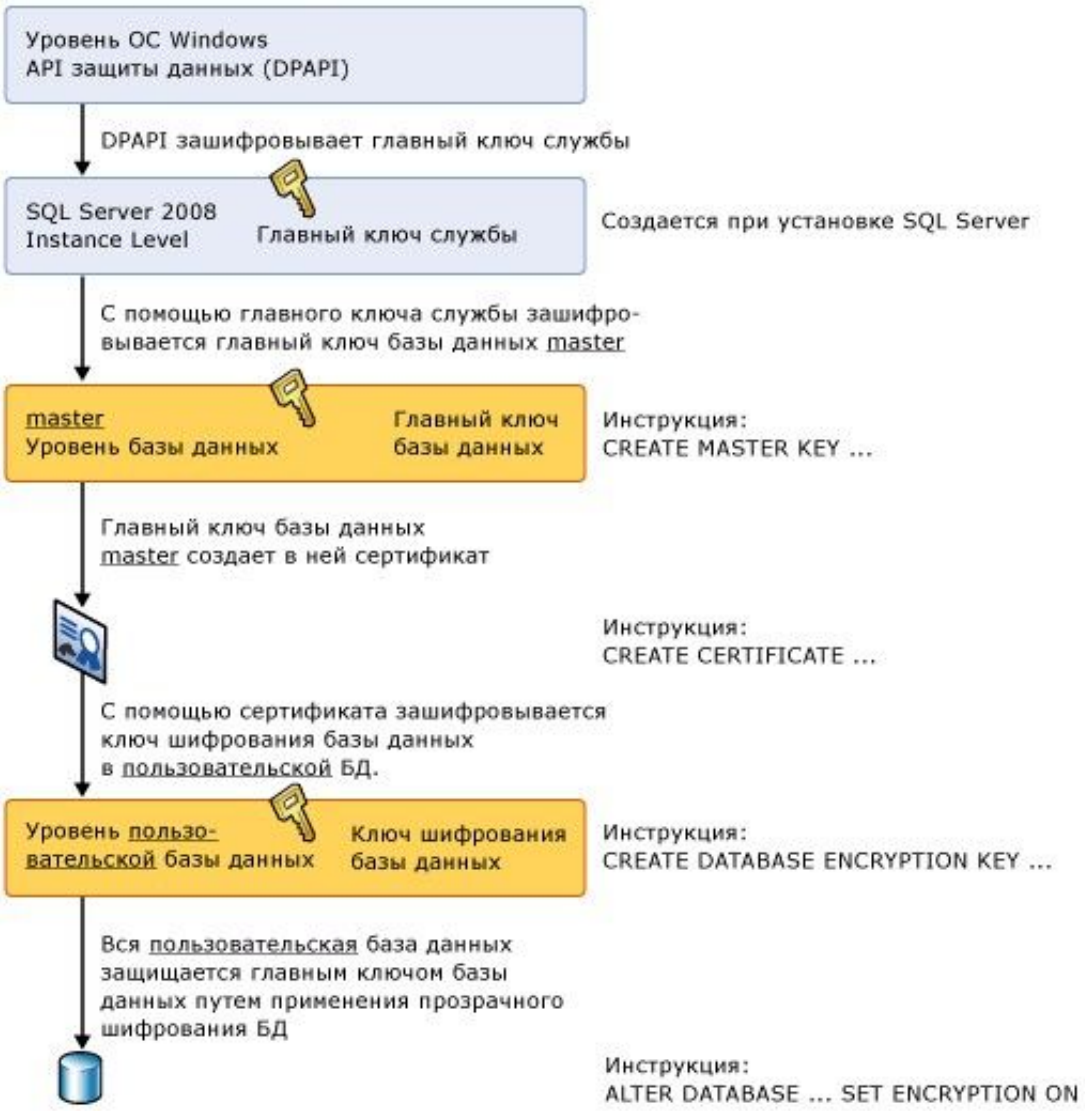
Асимметричное шифрование

Сертификаты

https://ru.wikipedia.org/wiki/X.509

TDE

Архитектура прозрачного шифрования базы данных



Always Encrypted

- Ключи хранятся вне БД
- Два типа
  - Randomized
    - Нет поддержки ==, != , join, group, index
  - Deterministic
- Column Encryption Keys (CEK) — Шифрование данных
- Column Master Keys (CMK) — Шифрование CEK, должен храниться во вне (Azure Key Vault, Certificate store, HSM)
- Не поддерживается
  - xml, rowversion, image, ntext, text, sql_variant, hierarchyid, geography, geometry
  - FILESTREAM, ROWGUIDCOL, IDENTITY, computed, sparse, or partitioning columns
  - ...

ДЕМО

Шифрование, сертификаты

03

Row-level Security

Row Level Security (RLS)

- Ограничение доступа к отдельным строкам
  - predicate functions
    - Filter predicate
    - Block predicate
  - security policy

ДЕМО

Row Level Security

04

Dynamic Data Masking

Dynamic Data Masking (DDM)

OTUS

Masking Function	Behavior	Strings	Numbers	Dates	Other Types
default()	Show **xxxx** mask (strings), or minimum value (other types)	Yes	Yes	Yes	Yes
partial(*a*, 'x', *b*)	Show first *a* characters, custom mask, and last *b* characters	Yes	No	No	No
email()	Show first character and **XXX@XXXX.com**	Yes	No	No	No
random(*a*, *b*)	Show random value between *a* and *b*	No	Yes	No	No

ДЕМО

Dynamic Data Masking

The End

О чем мы говорили сегодня?

OTUS

- Архитектура безопасности SQL Server
- Шифрование
- Row-Level Security
- Dynamic Data Masking

Заполните, пожалуйста, опрос в ЛК о занятии