* + - 1. Показать и объяснить, какой режим аутентификации используется для экземпляра SQL Server.

Сущ-ет 2 режима аутентификации:

* + - * + Виндовс (для доменных БД – внутри организации)
        + Смешанная аутентификация скл сервер (не исп.домены, доступ сторонних юзеров)
      1. Создать необходимые учетные записи, роли и пользователей. Объяснить назначение привилегий.

Есть 2 типа учетных записей логины и пользователи:

* + - * + Логин – понятие всего sql. У них мб права на какие-то административные задачи (бэкап).Для того, чтобы у логина были права на базу на основе него создается юзер
        + Пользователь – понятие в рамках одной бд. Им нельзя дать права по админ.части, но можно дать права на работу с бд.

ЛОГИН:

--имя логика - наташа, пароль - каспер.

--у этого логина уже будет право на вход.

-- проверить: Desktop => Безопасность => имена для входа => Natasha\_K

СОЗДАНИЕ ПОЛЬЗОВАТЕЛЯ ПРИВЯЗАННОГО К ЛОГИНУ:

-- проверить: Desktop => БД => publishing\_house => безопасность => пользователи => Natasha\_KUser

-- пользователь дб в той базе, откуда выполняем запрос

СОЗДАНИЕ ПОЛЬЗОВАТЕЛЯ:

-- проверить: Desktop => БД => publishing\_house => безопасность => пользователи => JustUser

Пользователи создаются без каких=либо прав на базу.

Привилегии – те действия, которые может выполнять пользователь. Т.е.они нужны для того, чтобы разрешить либо отменить какие-либо действия пользователя.

* + - 1. Продемонстрируйте заимствование прав для любой процедуры в базе данных.

Имперсонификация – разрешение заимствовать права у другого пользователя для выполнения определенного блока кода.

SETUSER остается в силе, пока не будет выполнен другой оператор SETUSER или пока текущая база данных не будет изменена с помощью оператора USE.

* + - 1. Создать для экземпляра SQL Server объект аудита.

Аудит – отслеживание и протоколирование событий, происходящих на сервере.

Аудит SQL Server:

\*аудит сервера для событий на уровне сервера

\*аудит бд для событий на уровне бд

Журнал аудита:

\*файл файловой системы

\*журнал windows application log

\*windows security log

СОЗДАНИЕ АУДИТА CAusit:

* queue\_delay – задержка очереди сброса на диск (0 – синхронно, 1000 – 1 сек)
* on\_failure – действия в случае невозможности продолжения аудита (continue, fail operation, shutdown)
* reserve\_disk\_space – заранее размещает на диске файл в соответствии с maxsize
* MAX\_ROLLOVER\_FILES – максимальное количество файлов кроме текущего
* MAX\_FILES - максимальное число файлов аудита, которые могут быть созданы. При достижении предела переключение на первый файл не производится. При достижении предела MAX\_FILES любое действие, которое вызывает создание дополнительных событий аудита, завершится ошибкой

--проверить: DESKTOP => безопасность => аудит (через св-ва посмотреть где созданы можно)

* + - 1. Задать для серверного аудита необходимые спецификации.

--сделать: DESKTOP => безопсность => спецификации аудита сервера => создать спецификацию аудита сервера => **картинка 5\_1**

Типы действия аудита:

|  |  |
| --- | --- |
| database\_change\_group | Изменение баз данных |
| database\_object\_change\_group | Изменения над объектами базы данных |
| login\_change\_password\_group | Изменения паролей |
| server\_state\_change\_group | Модификация служб |
| successful\_login\_group | Успешный вход |
| failed\_login\_group | Неудачная попытка входа |
| logout\_group | Выход пользователя из SQL Server |

* + - 1. Запустить серверный аудит, продемонстрировать журнал аудита.

ВКЛЮЧИТЬ АУДИТ: картинка ***4\_1***

--запуск: DESKTOP => безопасность => аудит => правой конпкой мыши (включить аудит)

--журнал аудита: DESKTOP => безопасность => аудит => правой конпкой мыши (посмотреть журналы)

* + - 1. Создать необходимые объекты аудита БД + создать спецификацию + запустить аудит + журнал

Картинка 7\_1, 7\_2

--сделать: БД lab10 => безопасность => спецификации аудита бд => создать

(insert, object, выбираем имя объекта (таблица), выбираем имя участника (dbo))

* + - 1. Остановить аудит БД и сервера.

Все откючить

* + - 1. Создать для экземпляра SQL Server ассиметричный ключ шифрования.

Шифрование:

\* Service Master Key – шифрует мастер-ключи БД

\* Database Master Key – шифрует симметричные ключи

\* Симметричные ключи – шифруют данные

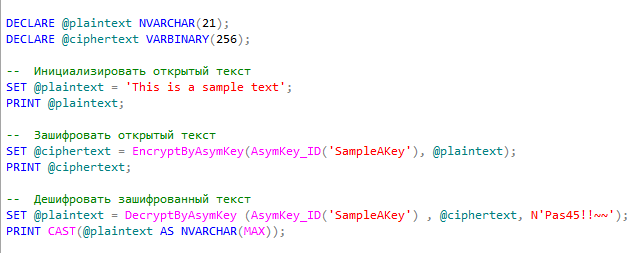
Асимм.ключи – пара ключей public и private;

\* алгоритма rsa

\* create, alter, drop

--проверить что ключ создан: БД lab10 => безопасность => ассиметричные ключи

* + - 1. Зашифровать и расшифровать данные при помощи этого ключа.



* + - 1. Создать для экземпляра SQL Server сертификат.

Сертификат – подписанная цифровой подписью инструкция, которая связывает значение открытого ключа с идентификатором пользователя, устройства или службы, имеющей соответствующий закрытый ключ.

Содержит след.сведения:

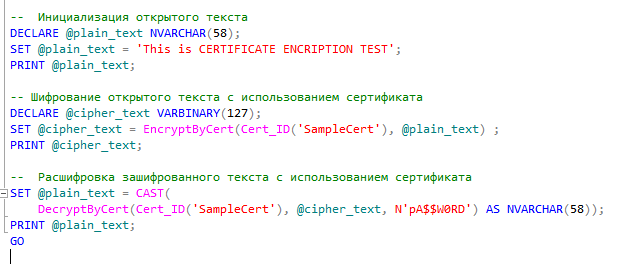
* Открытый ключ субъекта
* Идентификационные данные субъекта (имя и адрес эл.почты)
* Срок действия (valid from / valid to)
* Идентификационные данные поставщика
* Цифровая подпись поставщика

SQL м.генрировать автоподписанные сертификаты

\*create, alter, drop

--проверить: БД lab10 => безопасность => сертификаты

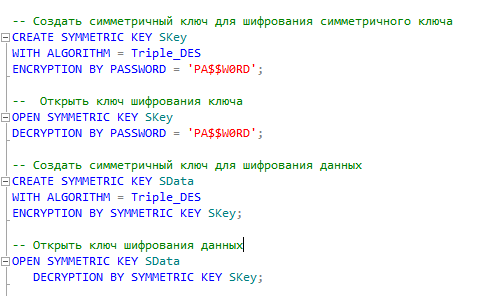
* + - 1. Зашифровать и расшифровать данные при помощи этого сертификата.



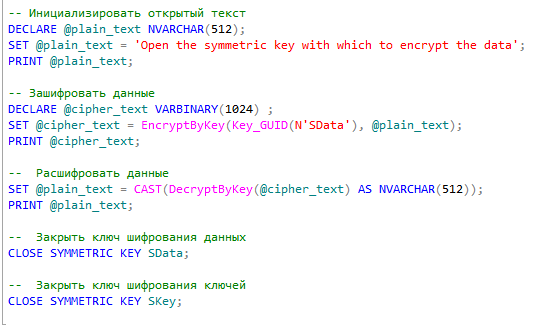
* + - 1. Создать для экземпляра SQL Server симметричный ключ шифрования данных.

Des, rc2 и т.д.

Create, alter, drop, open, close, close all symmetric keys;

****

* + - 1. Зашифровать и расшифровать данные при помощи этого ключа.



* + - 1. Продемонстрировать прозрачное шифрование базы данных.

Tde – transparent data encryption – прозрачное шифрование д-х.

Прозрачное шифрование данных используется для [шифрования и расшифровывания](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) данных и файлов журналов, соответственно, шифруя данные перед их записью на диск и расшифровывает данные перед их возвратом в приложение. Данный процесс выполняется на уровне [SQL](https://ru.wikipedia.org/wiki/SQL), полностью прозрачен для приложений и пользователей. В последующих резервных копиях файлов базы данных на диск или ленту конфиденциальные данные приложения будут зашифрованы.

Чтобы выполнить прозрачное шифрование необходимо:

* + - * + Создать главный ключ
        + Создать или получить сертификат, защищенный главным ключом
        + Создать ключ шифрования бд и защитить его с помощью сертификата
        + Задайте ведение шифрования бд

В коде – шифрование и дешифрование бд lab10 с помощью сертификата утсановленного на сервере

| **Команда или функция** | **Назначение** |
| --- | --- |
| [CREATE DATABASE ENCRYPTION KEY (Transact-SQL)](https://docs.microsoft.com/ru-ru/sql/t-sql/statements/create-database-encryption-key-transact-sql?view=sql-server-ver15) | Создает ключ, используемый для шифрования базы данных. |
| [ALTER DATABASE ENCRYPTION KEY (Transact-SQL)](https://docs.microsoft.com/ru-ru/sql/t-sql/statements/alter-database-encryption-key-transact-sql?view=sql-server-ver15) | Изменяет ключ, используемый для шифрования базы данных. |
| [DROP DATABASE ENCRYPTION KEY (Transact-SQL)](https://docs.microsoft.com/ru-ru/sql/t-sql/statements/drop-database-encryption-key-transact-sql?view=sql-server-ver15) | Удаляет ключ, использовавшийся для шифрования базы данных. |
| [Параметры ALTER DATABASE SET (Transact-SQL)](https://docs.microsoft.com/ru-ru/sql/t-sql/statements/alter-database-transact-sql-set-options?view=sql-server-ver15) | Объясняет параметр **ALTER DATABASE** , который используется для включения TDE. |

При включении в бд происходит обнуление оставшейся части виртуального журнала транзакций и принудительно начинается новый виртуальный журнал транзакций.

Это гарантирует, что после включения шифрования бд в журналах транзакций не останется простого текста.

* + - 1. Продемонстрировать применение хэширования.

Там все есть в коде

* + - 1. Продемонстрировать применение ЭЦП при помощи сертификата.

SignByCert (certificate\_ID, plaintext, password)

SignByAsymKey (asym\_key\_ID, plaintext, password)

VerifySignedByCert (certificate\_ID, plaintext, signature)

VerifySignedByAsymKey (asym\_key\_ID, plaintext, signature)

* + - 1. Сделать резервную копию необходимых ключей и сертификатов.