

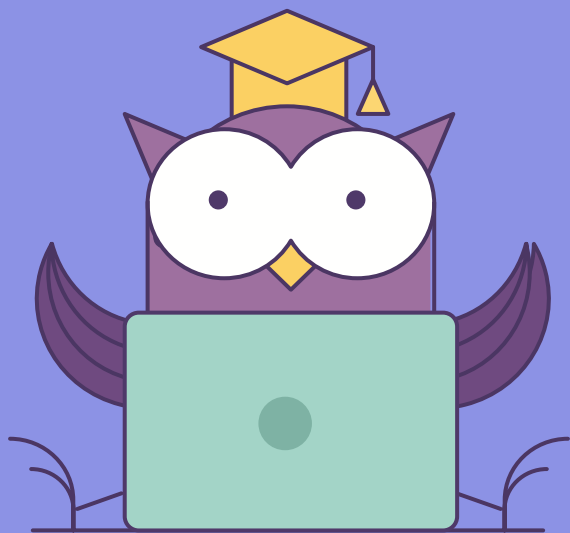


ОНЛАЙН-ОБРАЗОВАНИЕ


Проверить включена  
ли запись?



# Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте  если все хорошо  
Или напишите, какие есть проблемы

# Безопасность в SQL Server

Курс “MS SQL Server разработчик”  
Группа 2021-03



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

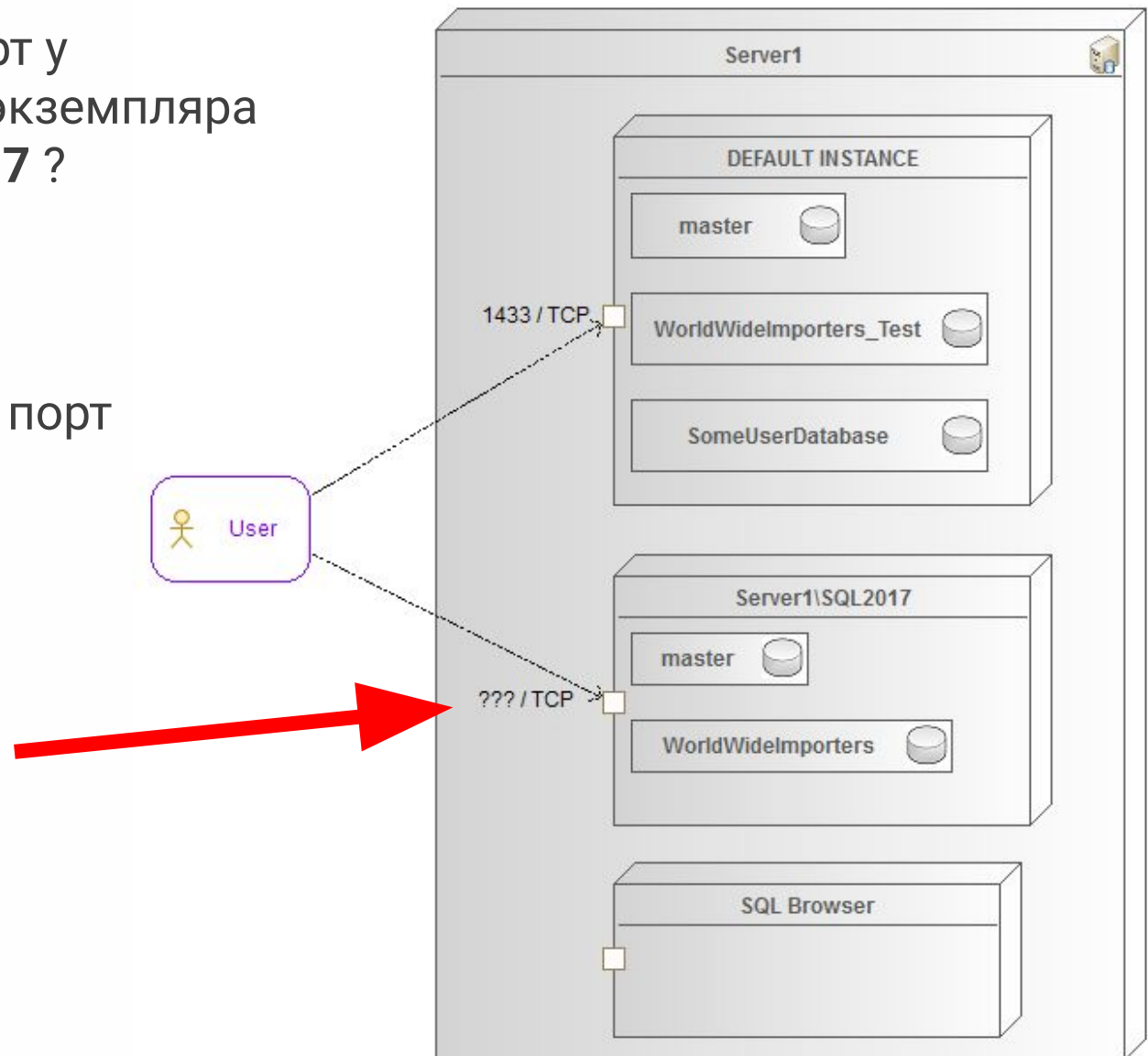


- Физическая безопасность (заборы и тп)
- Сеть (фаерволы, VPN и тд)
- Сервер (ОС)
- Экземпляр SQL Server
- База данных
- Таблица (SELECT/UPDATE/DELETE/INSERT; колонки, строки)
- Другие объекты БД: ХП, функции, ...

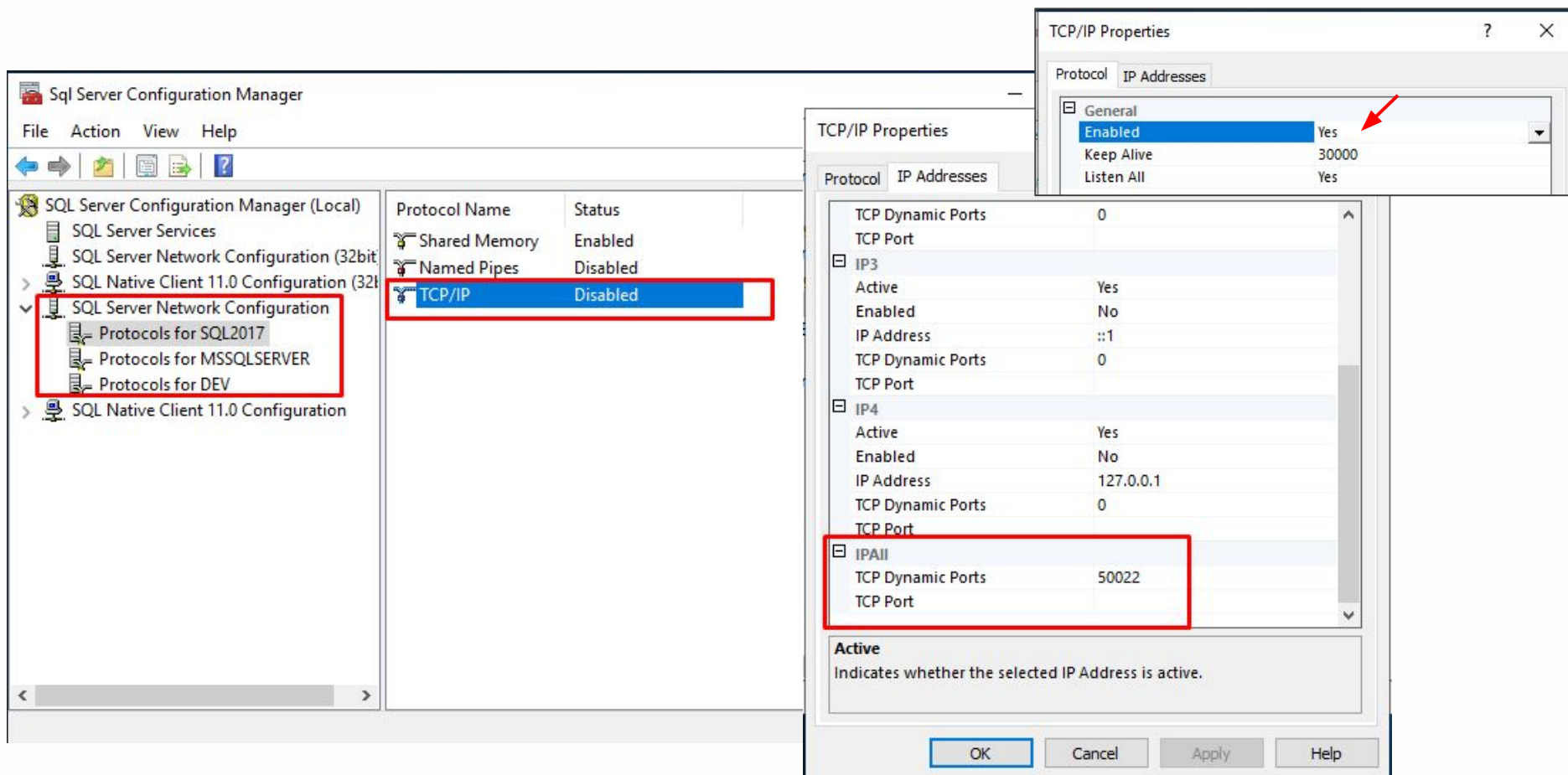
1. Какой будет порт у  
именованного экземпляра  
**Server1\SQL2017** ?

(в Windows)

2. Для чего нужен порт  
1434/UDP?



Настройка портов через SQL Server Configuration Manager.

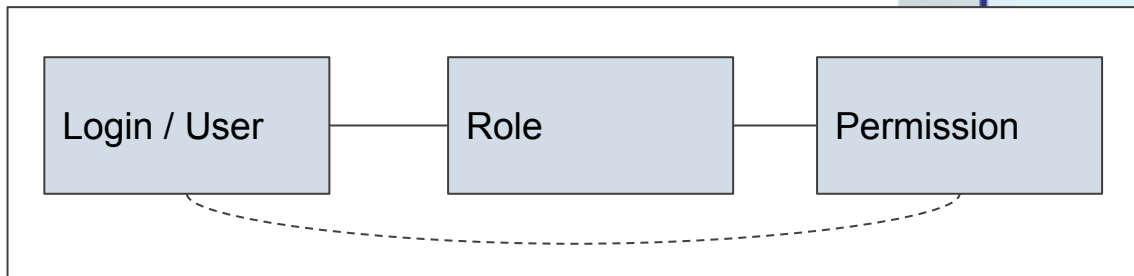
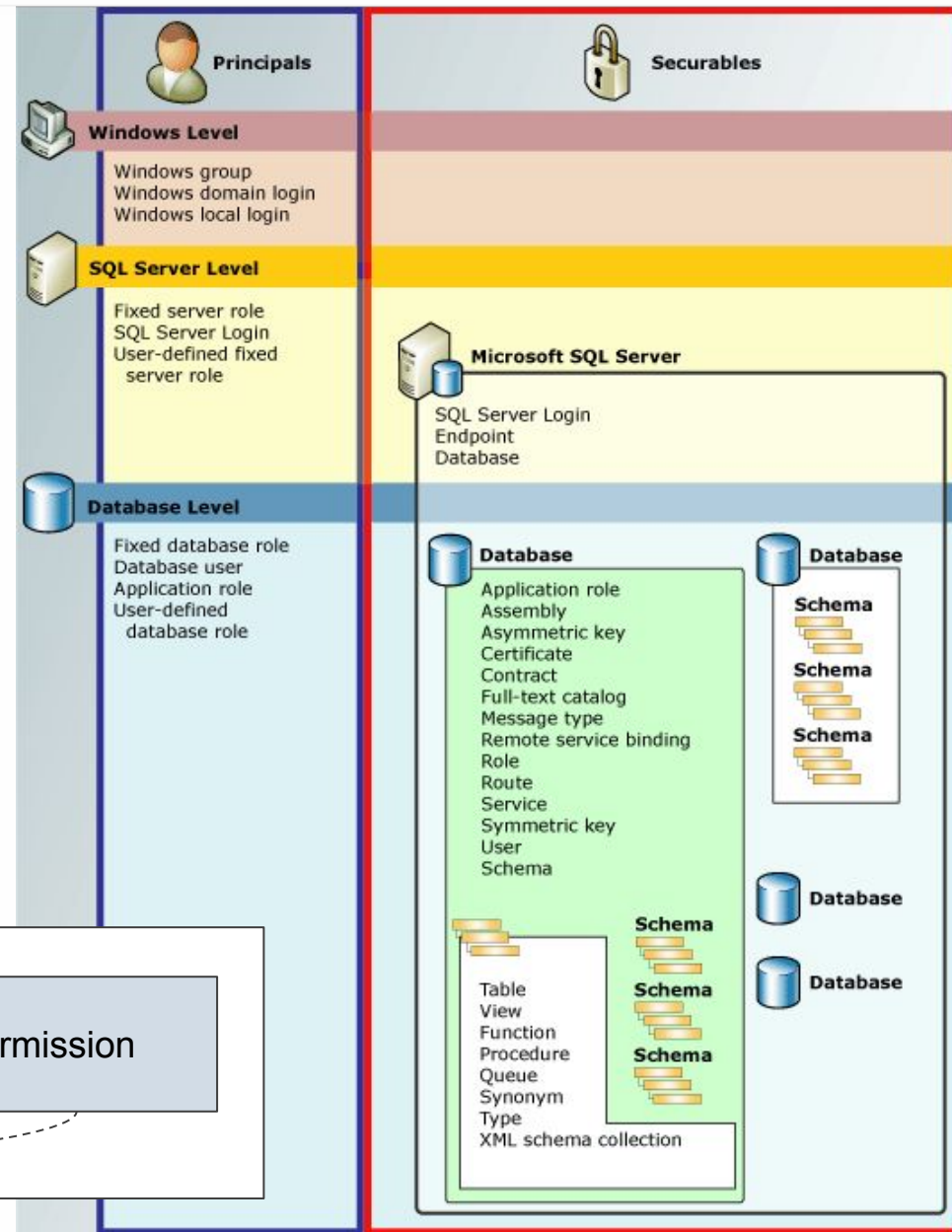




# 01

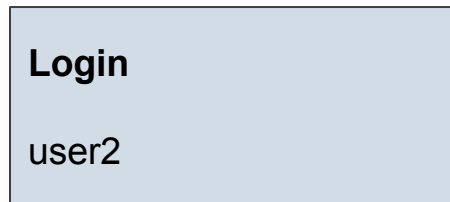
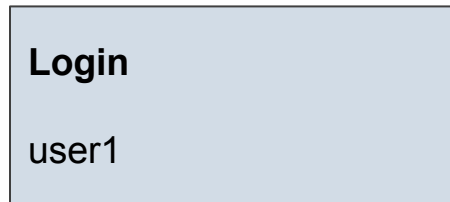
## Login, User, Role

- **Principals**  
(субъекты безопасности)
  - Логины, пользователи, роли и тд
- **Securables**  
(объекты безопасности, защищаемые объекты)
  - Инстанс, БД и тд
  - Схема, таблицы, ХП и тд
- **Permissions**  
(разрешения)
  - Просмотр таблицы, запуск ХП и тд
  - Диаграмма разрешений SQL Server



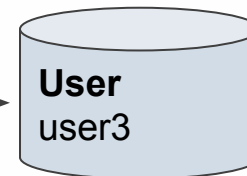
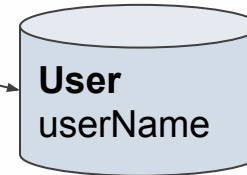
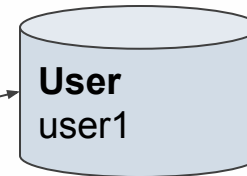
## Экземпляр SQL Server

Хранятся в master



## База данных

Хранятся в БД

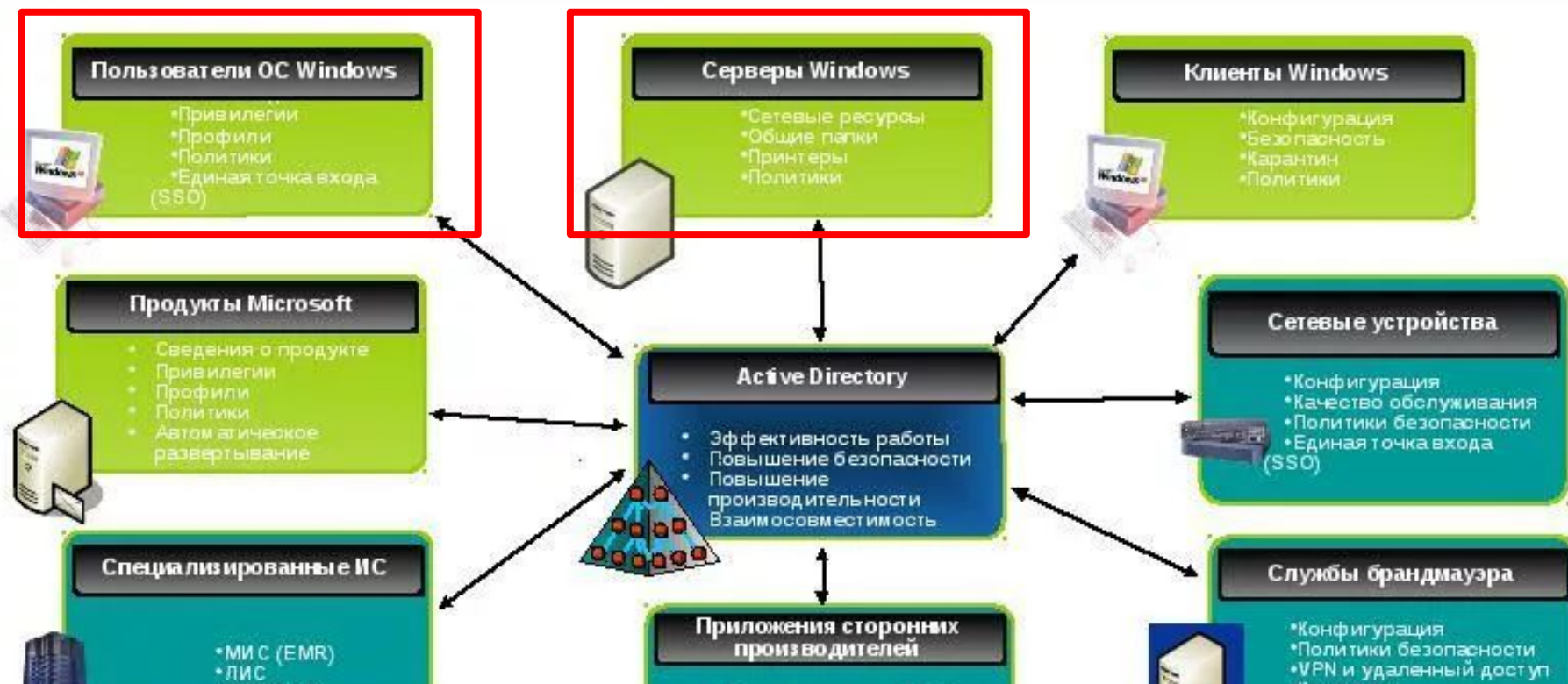


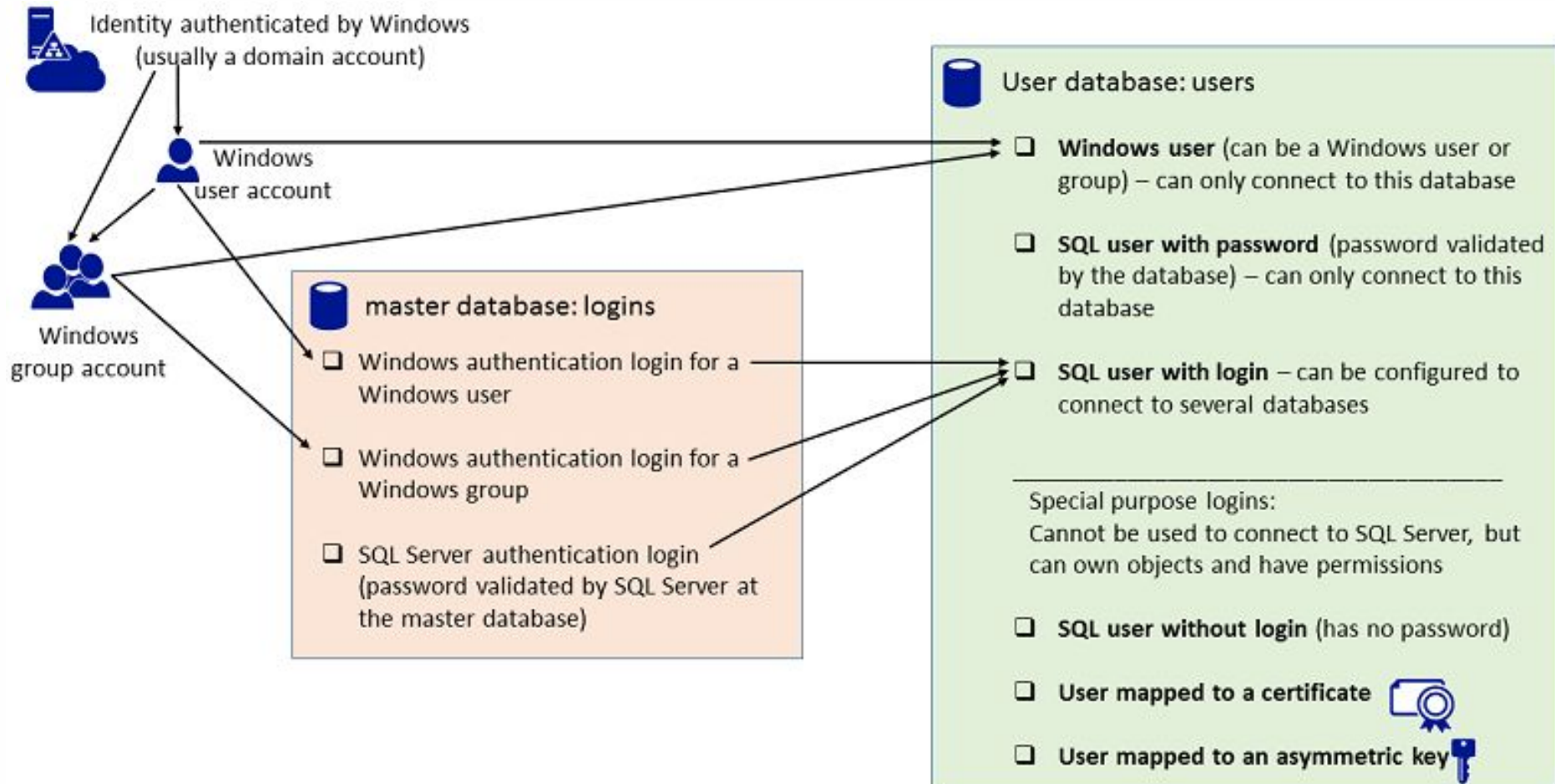
- Databases
- Stored procedures
- Tables
- Views
- Inline functions
- Scalar functions
- Table-valued functions
- Application roles
- Assemblies
- Asymmetric keys
- Certificates
- Database roles
- Aggregate functions
- Full-text catalogs
- Queues
- Schemas
- Symmetric keys
- Synonyms
- Users
- User-defined data types
- XML schema collections
- User-defined table types
- Sequences

Аутентификация:

- Windows
- SQL Server
- Сертификаты\*

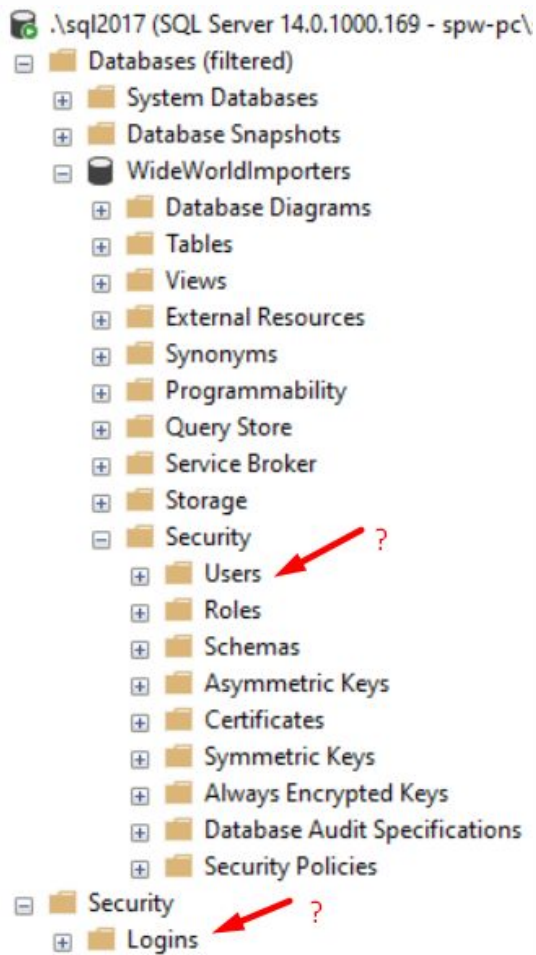
DOMAIN\APPSERVER\$





Требуется предоставить доступ на чтение таблицы.

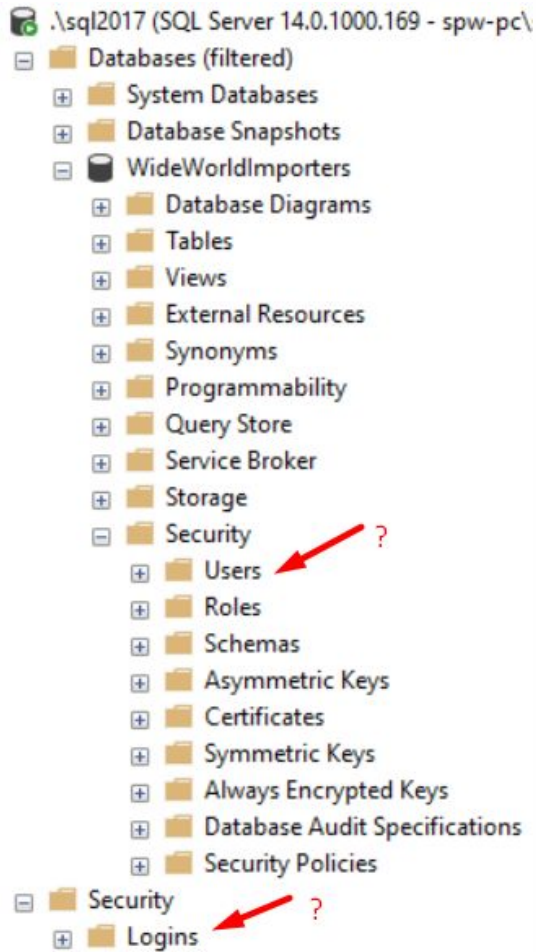
Надо настраивать логин или пользователя?





Требуется изменить пароль для доступа.

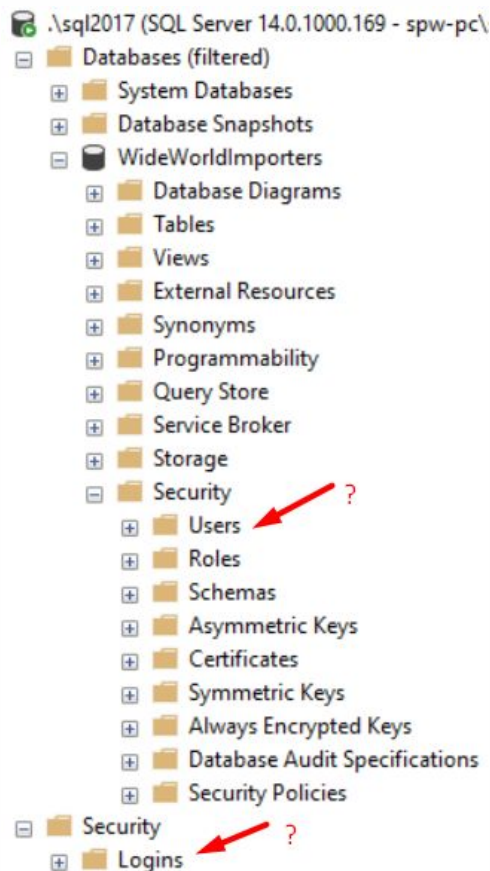
Надо настраивать логин или пользователя?



Вы создали бэкап БД и восстановили его на другом сервере.

Появятся ли на новом сервере логины SQL Server?

Появятся ли на новом сервере пользователи БД?





- Роль — набор прав, который можно назначить определенному пользователю или группе пользователей.
- Роли уровня сервера
  - встроенные (**sysadmin**, **public**, 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)

- DCL (Data Control Language)
  - CREATE / ALTER
  - GRANT
  - REVOKE
  - DENY
- Хранимые процедуры
  - sp\_adduser
  - sp\_addrole
  - sp\_addrolemember
  - ...
- SSMS

# ДЕМО

## Логины, пользователи



Новому сотруднику требуется предоставить доступ на чтение всех таблиц в БД.

Как проще всего это сделать:

- Какие объекты надо создать?
- Какие роли назначить?



# 02

## Row-level Security

# Безопасность на уровне строк

## Row Level Security (RLS)

- SQL Server 2016
- Ограничение доступа к отдельным строкам

*Предоставление работникам доступ только к тем строкам данных, которые связаны с работой их отдела.*

*Предоставление доступа для клиентов только к тем данным, которые относятся к их компании.*

Начальник видит все данные:

OrderID	SalesUsername	Product	Qty
1	User1	Lemon	5
2	User1	Banana	2
3	User2	Orange	2
4	User2	Banana	5
5	User2	Tomato	5

```
SELECT * FROM Sales
```

User1 только свои:

OrderID	SalesUsername	Product	Qty
1	User1	Lemon	5
2	User1	Banana	2

User2 только свои:

OrderID	SalesUsername	Product	Qty
3	User2	Orange	2
4	User2	Banana	5
5	User2	Tomato	5

# Безопасность на уровне строк

## Row Level Security (RLS)

- predicate functions == “WHERE”
  - Filter predicate
  - Block predicate
- security policy

# ДЕМО

## Row Level Security





# 03

## Dynamic Data Masking

Динамическое маскирование данных.

Пользователям без разрешения **UNMASK** будет отображаться "мусор".

```
SELECT * FROM Users
```

Есть  
**UNMASK**

ID	FullName	Phone	Email	Age
1	Ivanov Ivan	8(900) 123-34-67	ivan@somedomain.com	30
2	Petrov Petr	8(900) 123-42-89	petd@somedomain.ro	30
3	Sidorov Alex	8(900) 123-12-75	alex@somedomain.org	30

Нет  
**UNMASK**

ID	FullName	Phone	Email	Age
1	Iv...an	xxxx	iXXX@XXXX.com	61
2	Pe...tr	xxxx	pXXX@XXXX.com	55
3	Si...ex	xxxx	aXXX@XXXX.com	57

# ДЕМО

## Dynamic Data Masking



# Динамическое маскирование данных Dynamic Data Masking (DDM)

Функция	Поведение	Типы данных		
		Строки	Числа	Даты
default()	Полное маскирование	XXXX	0	01.01.1900
partial(prefix, [padding], suffix)	Первые prefix-символов, padding, последние suffix	ИXXXXXXXXн	не применимо	не применимо
email()	Первая буква и XXX@XXXX.com	aXXX@XXX X.com	не применимо	не применимо
random(start, end)	Случайное значение между start и end	не применимо	случайное число	не применимо

```
{ EXEC | EXECUTE } AS { CALLER | SELF | OWNER | 'user_name' }
```

- Можно определять контекст выполнения для следующих модулей: функций, процедур, очередей и триггеров.
- Можно указать, какая учетная запись используется при проверке разрешений на объекты, на которые ссылается модуль (например, ХП).
- Необходимо будет предоставлять только разрешения на сам модуль, без выдачи явных разрешений на объекты, на которые он ссылается.
- Только пользователь, от имени которого выполняется модуль, должен будет иметь разрешения на объекты, к которым этот модуль обращается.
- Пользователь, который создает или изменяет модуль, должен иметь разрешение IMPERSONATE на этого участника.

```
CREATE PROCEDURE dbo.usp_Demo  
WITH EXECUTE AS 'CompanyDomain\SqlUser1'  
AS  
SELECT user_name();  
GO
```

04

Шифрование

**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 асимметричное с сертификатами
- **Прозрачное шифрование данных, TDE (с 2008)**
  - [Основы прозрачного шифрования MS SQL Server](#)
- **Резервные копии**
  - [Шифрование резервной копии](#)
- **Always Encrypted (с 2016)**

**The End**



**Заполните,  
пожалуйста,  
опрос в ЛК о занятии**

