Active Directory

Domain service

Lesson 1: Overview of AD DS

- Overview of AD DS
  What Are AD DS Domains?
  What Are OUs?
  What Is an AD DS Forest?
  What Is the AD DS Schema?
  What Is New for Windows Server 2012 Active Directory?
  What Is New for Windows Server 2012 R2 Active Directory?

Overview of AD DS

AD DS is composed of both logical and physical components

Logical components

- Partitions
- Schema
- Domains
- Domain trees
- Forests
- Sites
- OUs
- Containers

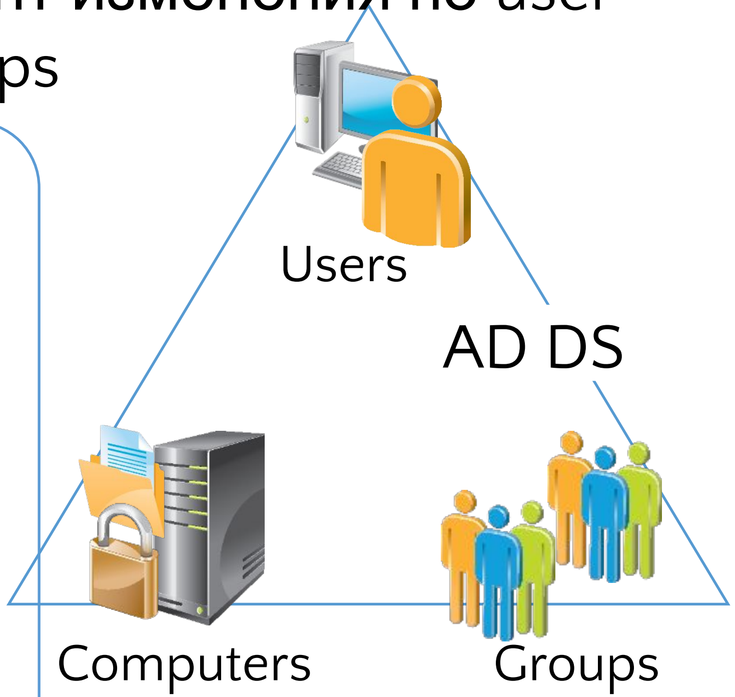
Physical components

- Domain controllers
- Data stores
- Global catalog servers
- RODCs

AD DS Domains

- AD DS наличия наличия более одного domain controllers
- Все domain controllers обслуживают рабочую копию БД домена и реплицируют контент изменения по user accounts, computer accounts, groups

- Domain –граница репликации
- Domain – административный центр для конфигурирования и управления объектами
- Любой domain controller аутентифицирует попытку sign-in из любомого места в domain
- The domain предоставляет authorization

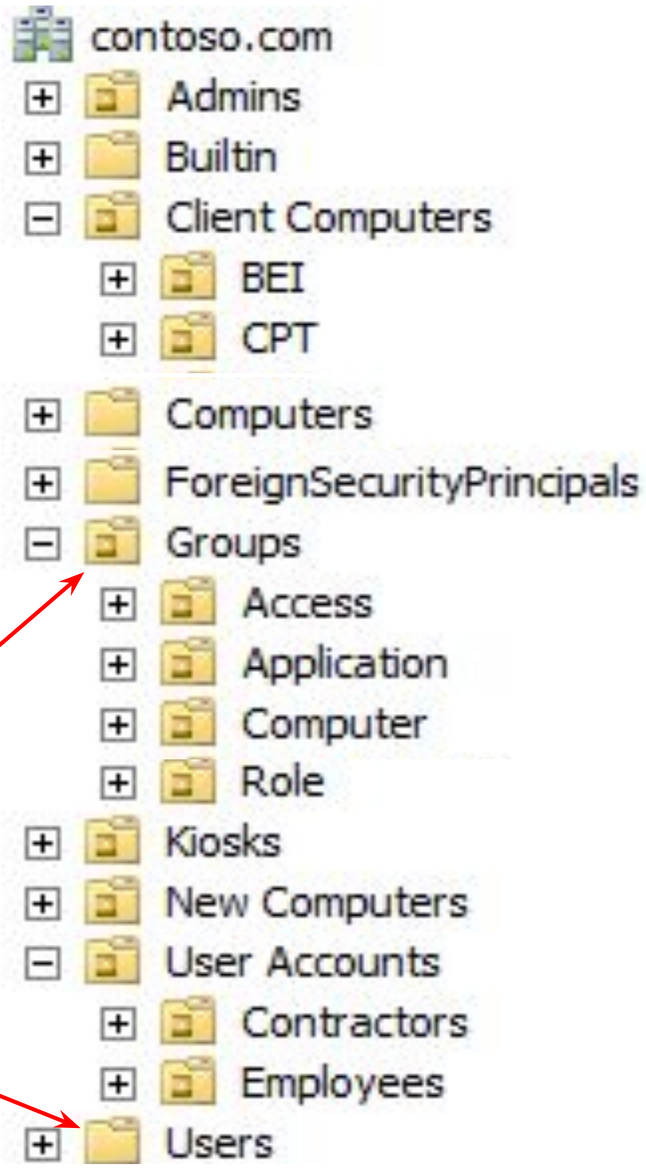


OU

- Containers может использоваться для группировки объектов в домене
- OU для:
  - Группировки объектов с последующим назначением на нее GPOs
  - Делегирование административных

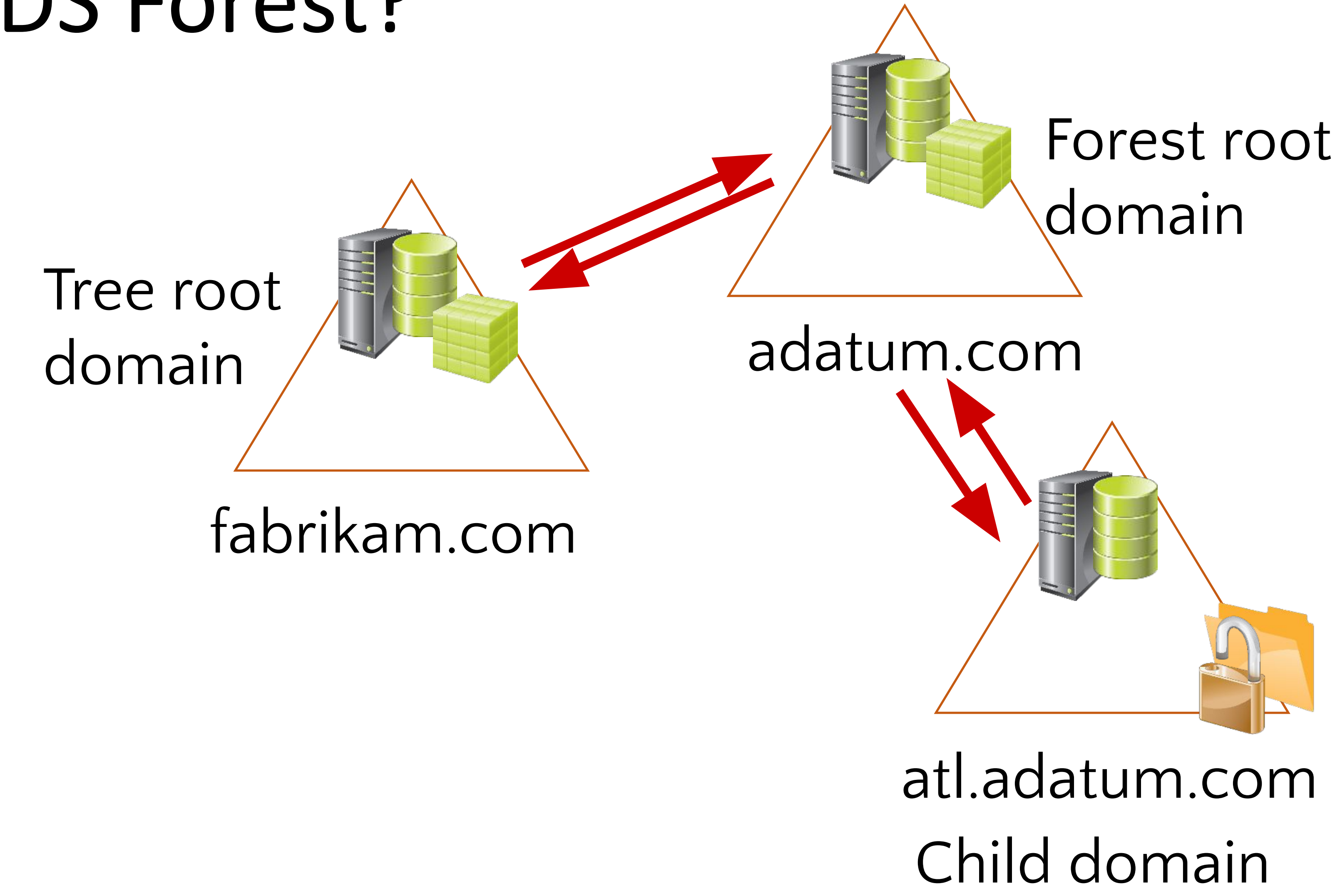
OU выглядит как папка с книгой внутри

Containers выглядит как папка



- contoso.com
  - Admins
  - Builtin
  - Client Computers
    - BEI
    - CPT
  - Computers
  - ForeignSecurityPrincipals
  - Groups
    - Access
    - Application
    - Computer
    - Role
  - Kiosks
  - New Computers
  - User Accounts
    - Contractors
    - Employees
  - Users

AD DS Forest?



Forest root domain

adatum.com

Tree root domain

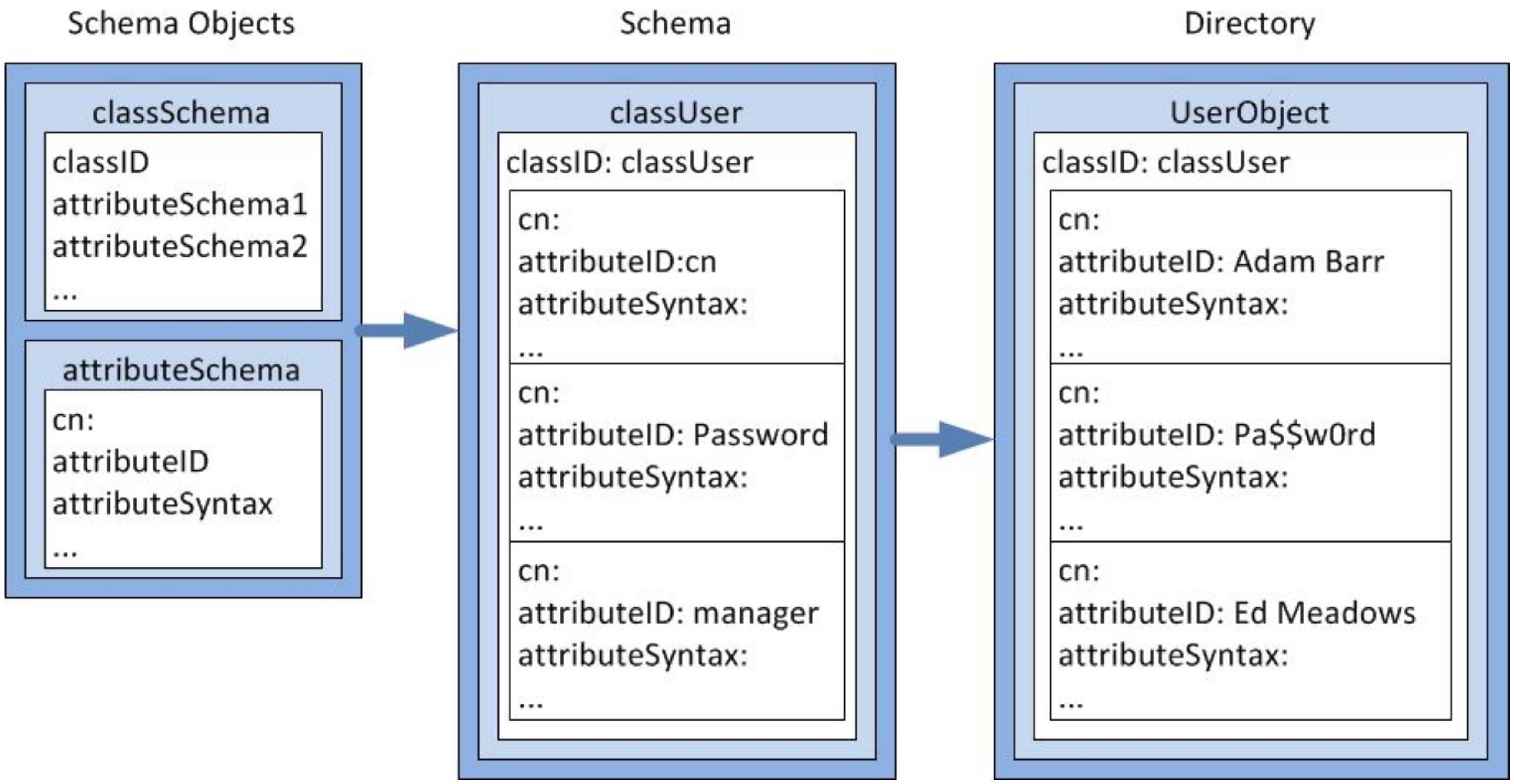
fabrikam.com

atl.adatum.com

Child domain

AD DS Schema

Schema определяет объекты хранимые в AD DS



Schema Objects

classSchema

classID
attributeSchema1
attributeSchema2
...

attributeSchema

cn:
attributeID
attributeSyntax
...

Schema

classUser

classID: classUser

cn:
attributeID:cn
attributeSyntax:
...

cn:
attributeID: Password
attributeSyntax:
...

cn:
attributeID: manager
attributeSyntax:
...

Directory

UserObject

classID: classUser

cn:
attributeID: Adam Barr
attributeSyntax:
...

cn:
attributeID: Pa$$w0rd
attributeSyntax:
...

cn:
attributeID: Ed Meadows
attributeSyntax:
...

Domain Controller

Domain controllers

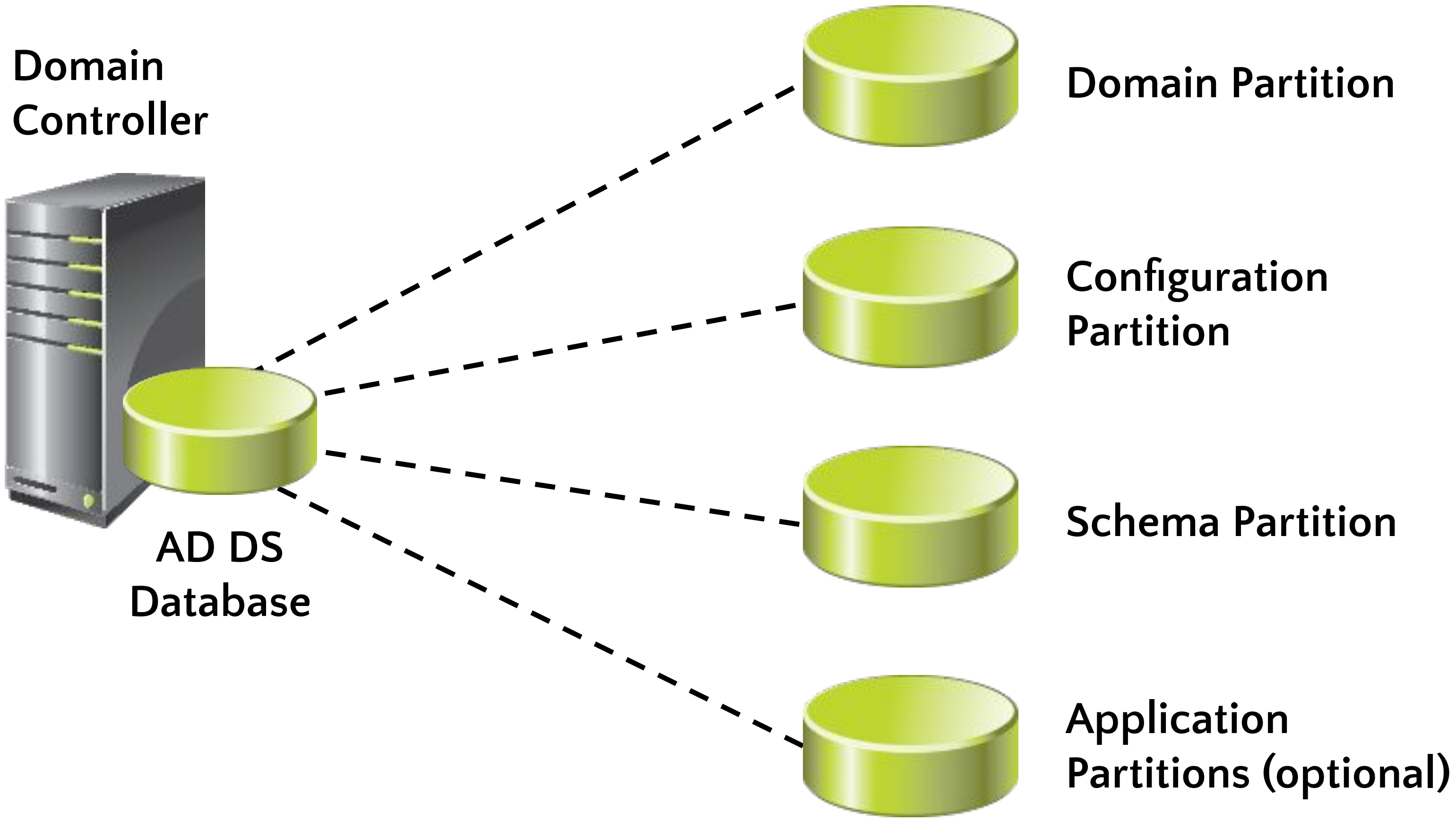
- Servers на котором развернута AD SA с AD DS database (Ntds.dit) и папкой SYSVOL
- Kerberos authentication service и KDC services производят authentication
- Best practices:
  - Availability (Доступность-надежность):

    Не менее двух domain controllers на один domain
  - Security (Безопасность:

    RODC и BitLocker

AD DS Database

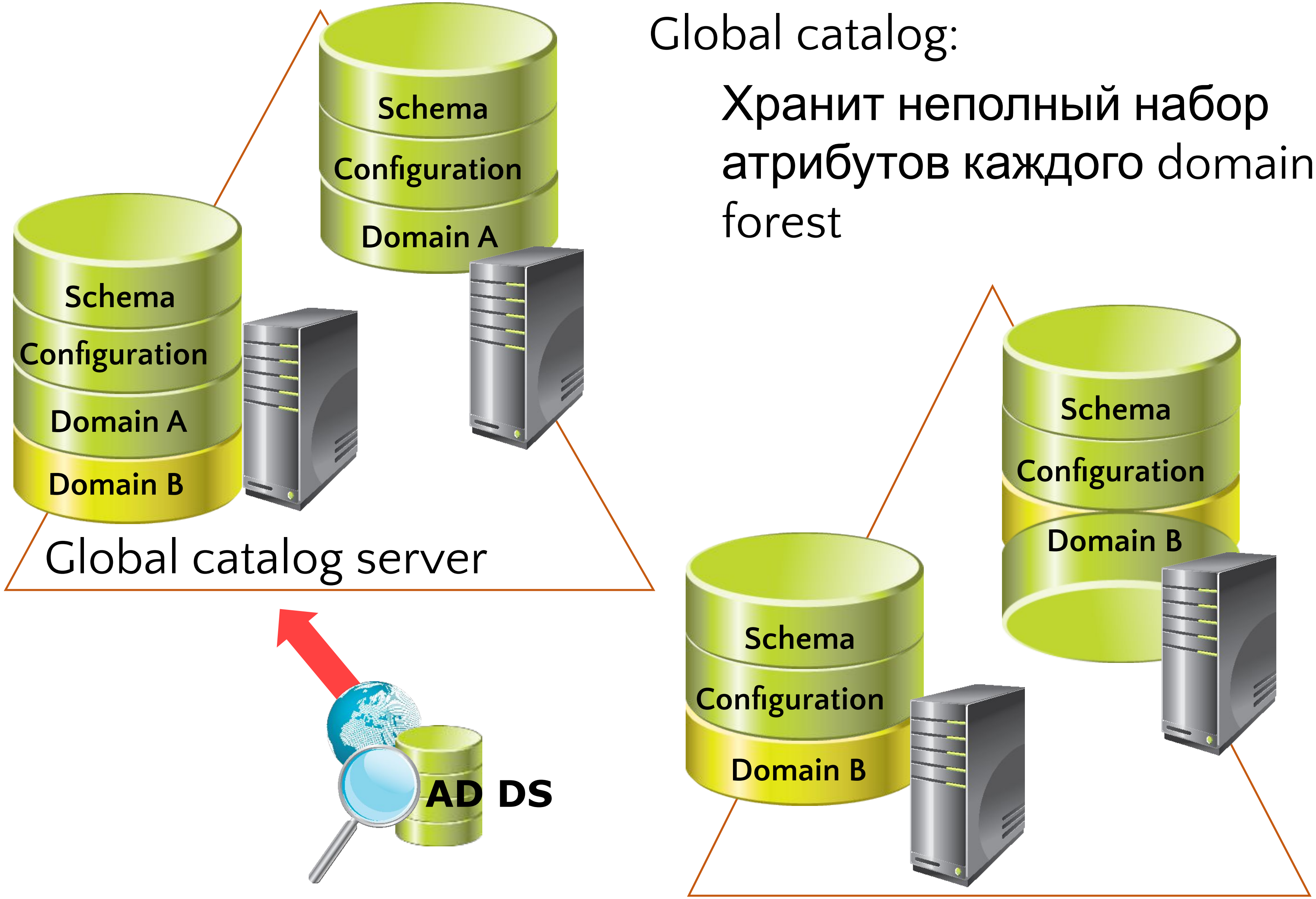
The AD DS database храниться и обслуживается всеми domain, каждая состоит из 4-х разделов



Global Catalog

Global catalog:

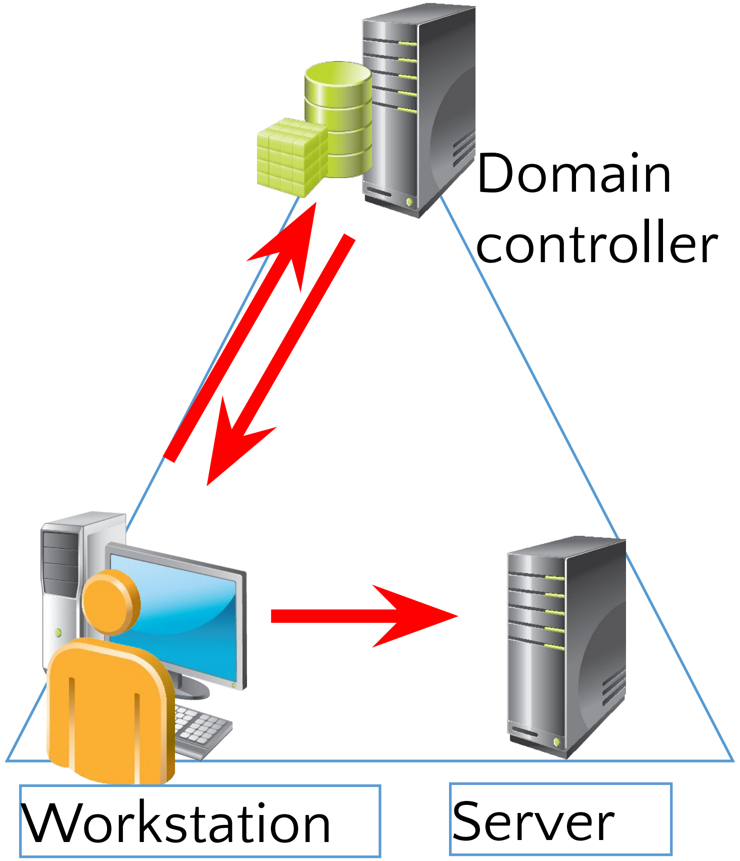
Хранит неполный набор атрибутов каждого domains в forest



The AD DS Sign-in Process

The AD DS sign-in process:

1. user account проходит authentication на domain controller.
2. domain controller возвращает TGT обратно клиенту.
3. client использует TGT для доступа к workstation.
4. domain controller предоставляет доступ к workstation.
5. client использует TGT для доступа к server.
6. domain controller возвращает доступ к серверу.



Operations Masters

Multi-master replication model, несколько ролей может быть на каждом сервере

Множество синонимов есть у single master operations в AD DS, включая:

- Operations master (или operations master роли)
- Single master роли
- Flexible single master operations (FSMOs)

The five FSMOs are:

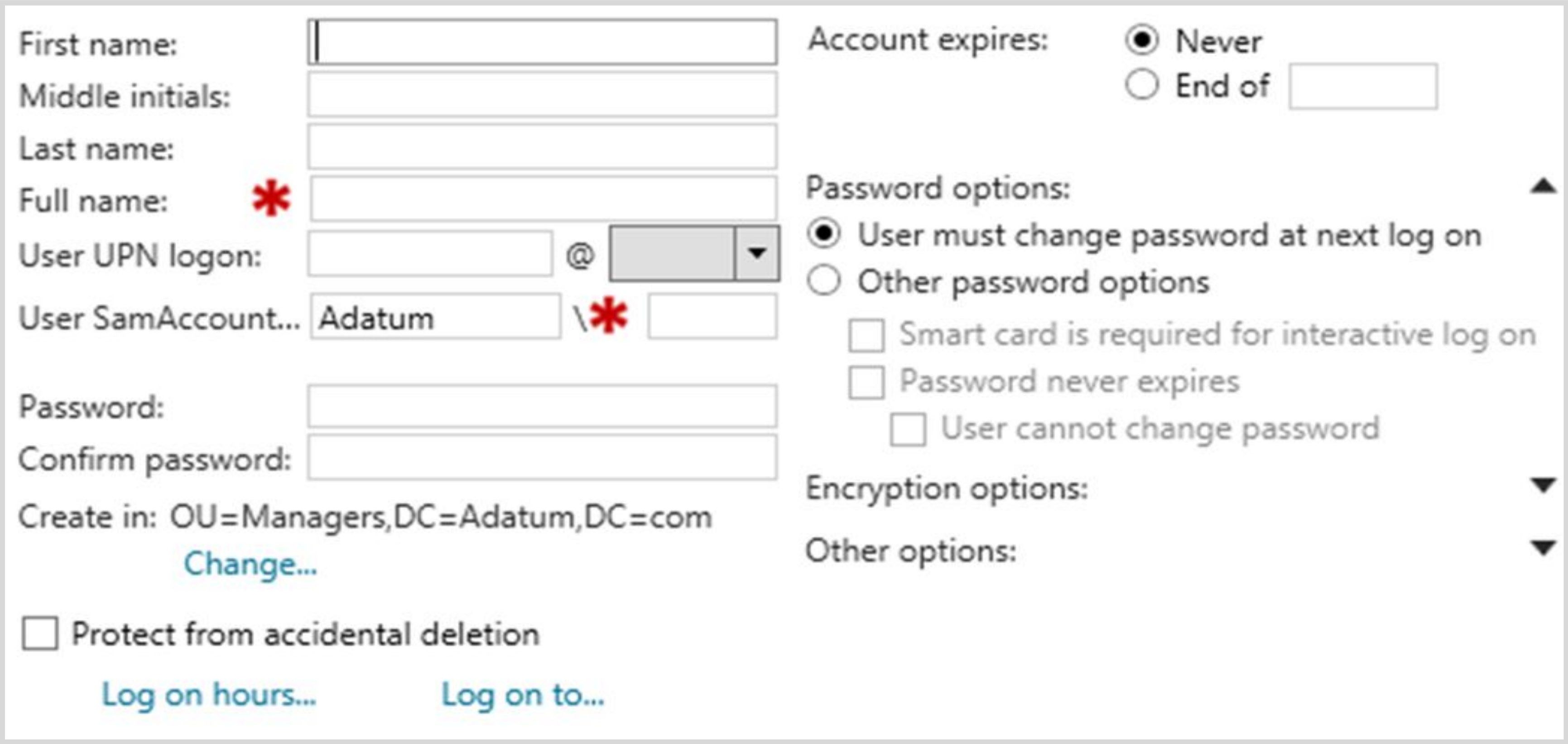
- Forest:
  - Domain naming master
  - Schema master

- Domain:
  - RID master
  - Infrastructure master
  - PDC Emulator master

Manage Account

Creating User Accounts

Active Directory Administrative Center Create User window



First name:

Middle initials:

Last name:

Full name: *

User UPN logon: @

User SamAccount... Adatum *

Password:

Confirm password:

Create in: OU=Managers,DC=Adatum,DC=com

Change...

□ Protect from accidental deletion

Log on hours... Log on to...

Account expires: ● Never ○ End of

Password options:

● User must change password at next log on

○ Other password options

□ Smart card is required for interactive log on

□ Password never expires

□ User cannot change password

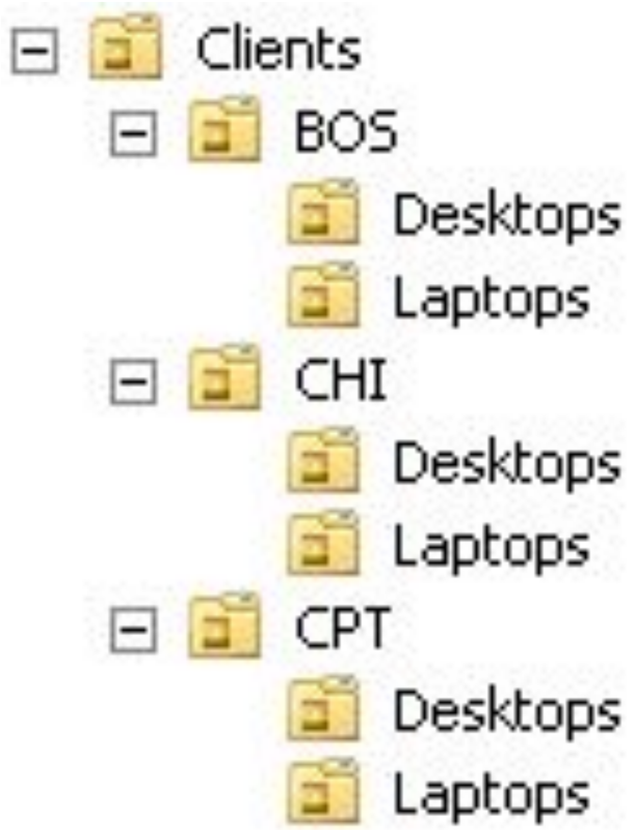
Encryption options:

Other options:

Specifying the Location of Computer Accounts

- Best practice is to create OUs for computer objects
  - Servers
    - Typically subdivided by server role
  - Client computers
    - Typically subdivided by region

- Divide OUs:
  - By administration
  - To facilitate configuration with Group Policy

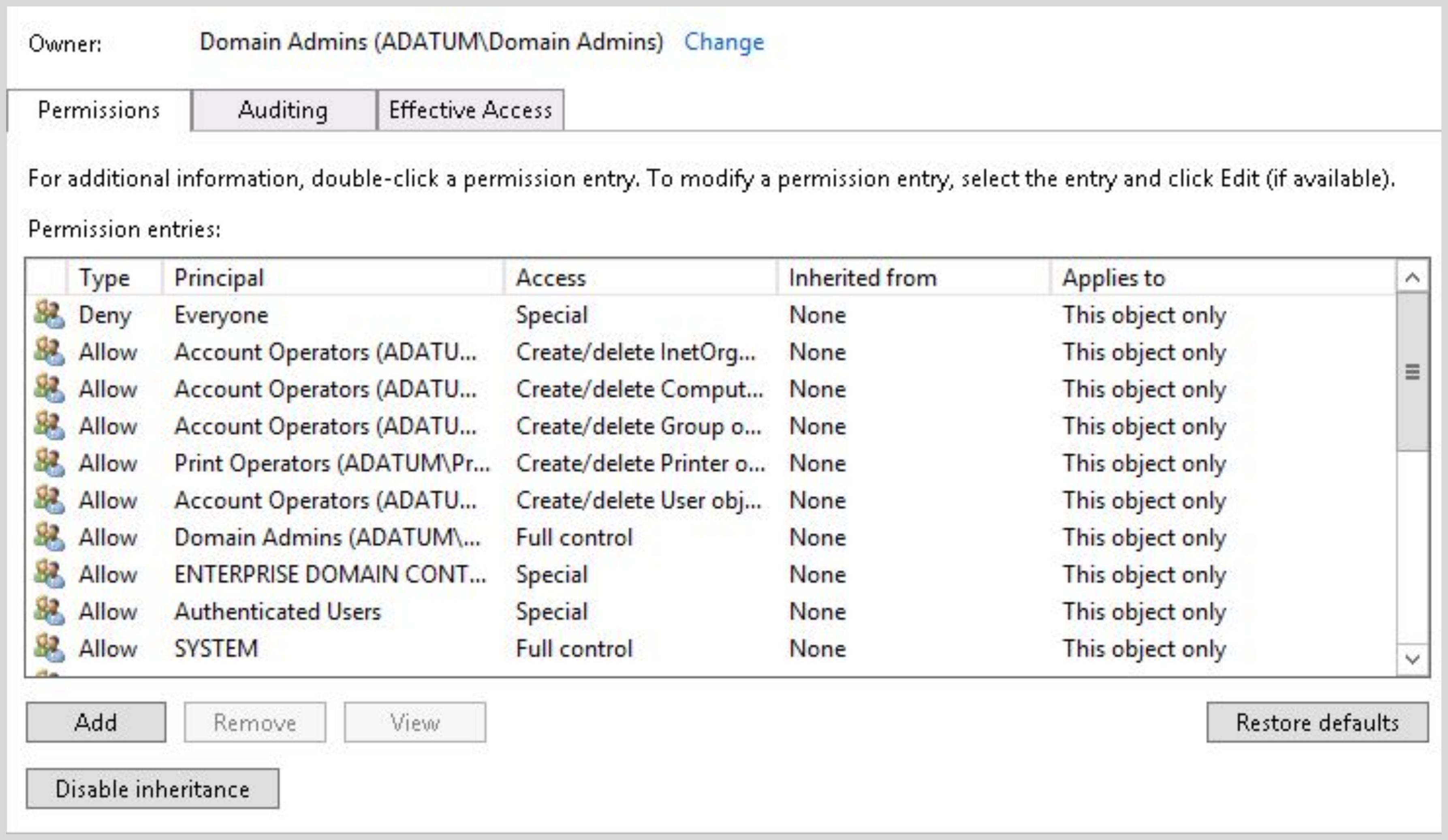


Resetting the Secure Channel

- Не удаляйте и не выводите computer из domain
  - Создание нового аккаунта = создание нового SID потеря членства в группах.
- Для сброса secure channel используем
  - Active Directory Users and Computers
  - Active Directory Administrative Center
  - **dsmod**
  - **netdom**
  - **nltest**
  - Windows PowerShell

AD DS Permissions

Advanced Security Settings for IT



Owner: Domain Admins (ADATUM\Domain Admins) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Deny	Everyone	Special	None	This object only
Allow	Account Operators (ADATU...	Create/delete InetOrg...	None	This object only
Allow	Account Operators (ADATU...	Create/delete Comput...	None	This object only
Allow	Account Operators (ADATU...	Create/delete Group o...	None	This object only
Allow	Print Operators (ADATUM\Pr...	Create/delete Printer o...	None	This object only
Allow	Account Operators (ADATU...	Create/delete User obj...	None	This object only
Allow	Domain Admins (ADATUM\...	Full control	None	This object only
Allow	ENTERPRISE DOMAIN CONT...	Special	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only

Effective AD DS Permissions

Разрешения, назначенные пользователям и группам, накапливаются

Лучшей практикой является назначение разрешений для групп, а не для отдельных пользователей

In the event of conflicts:

- Deny permissions побеждают Allow permissions
- Явные permissions побеждают Неявные permissions
  - Явный Allow побеждает Неявный Deny

effective permissions, покажут результирующие permissions :

Group Types

- Distribution groups
  - Используются email приложениями
  - Not security-enabled (no SID); не предоставляет permissions

- Security groups
  - Security principal имеет SID; предоставляет permissions
  - Так же может использоваться email приложениями

security groups и distribution groups можно конвертировать друг в друга

Group Scopes

Group scope	Members from same domain	Members from domain in same forest	Members from trusted external domain	Can be assigned permissions to resources
Local	U, C, GG, DLG, UG and local users	U, C, GG, UG	U, C, GG	On the local computer only
Domain-local	U, C, GG, DLG, UG	U, C, GG, UG	U, C, GG	Anywhere in the domain
Universal	U, C, GG, UG	U, C, GG, UG	N/A	Anywhere in the forest
Global	U, C, GG	N/A	N/A	Anywhere in the domain or a trusted domain

U	User
C	Computer
GG	Global group
DLG	Domain-local group
UG	Universal group

Implementing Group Management

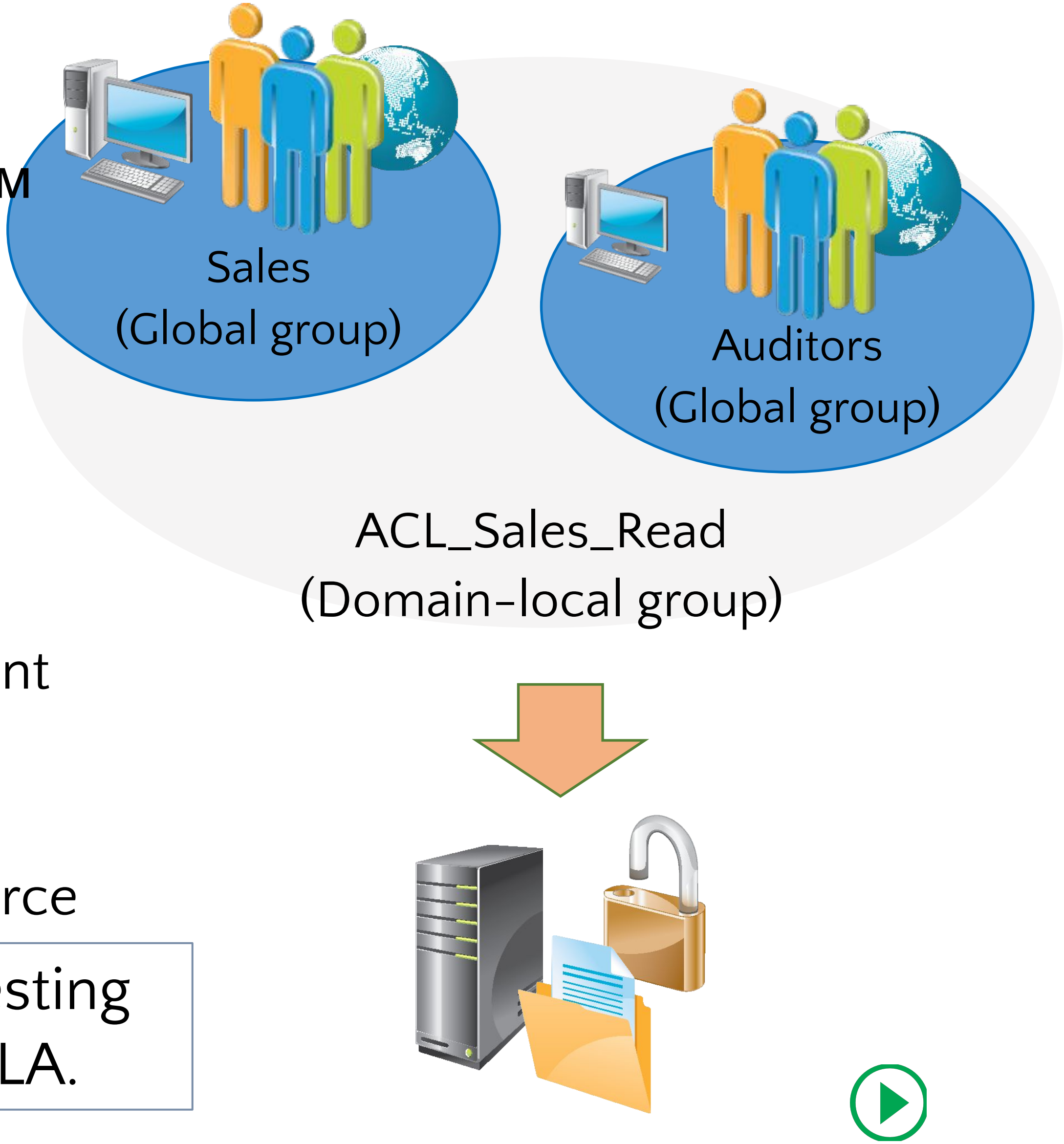
I Identities
Users или computers,
Который является членом

G Global groups
Содержат членов на основе ролейmembers' roles,
which are members of

DL Domain-local groups
Which provide management such as resource access, which are

A Assigned access to a resource

This best practice for nesting groups is known as IGDLA.



Implementing Group Management

- Identities
  Users or computers,
  which are members of

Implementing Group Management

I Identities
Users or computers,
which are members of

G Global groups
Which collect members
based on members' roles,
which are members of

Sales
(Global group)

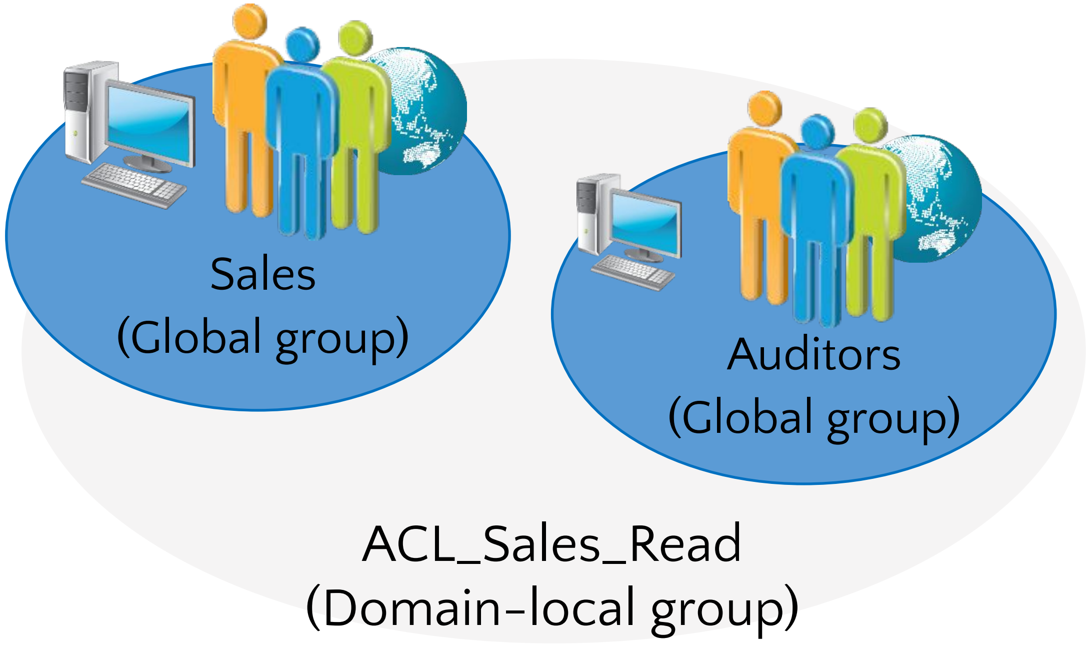
Auditors
(Global group)

Implementing Group Management

I Identities
Users or computers,
which are members of

G Global groups
Which collect members
based on members’ roles,
which are members of

DL Domain-local groups
Which provide management
such as resource access,
which are



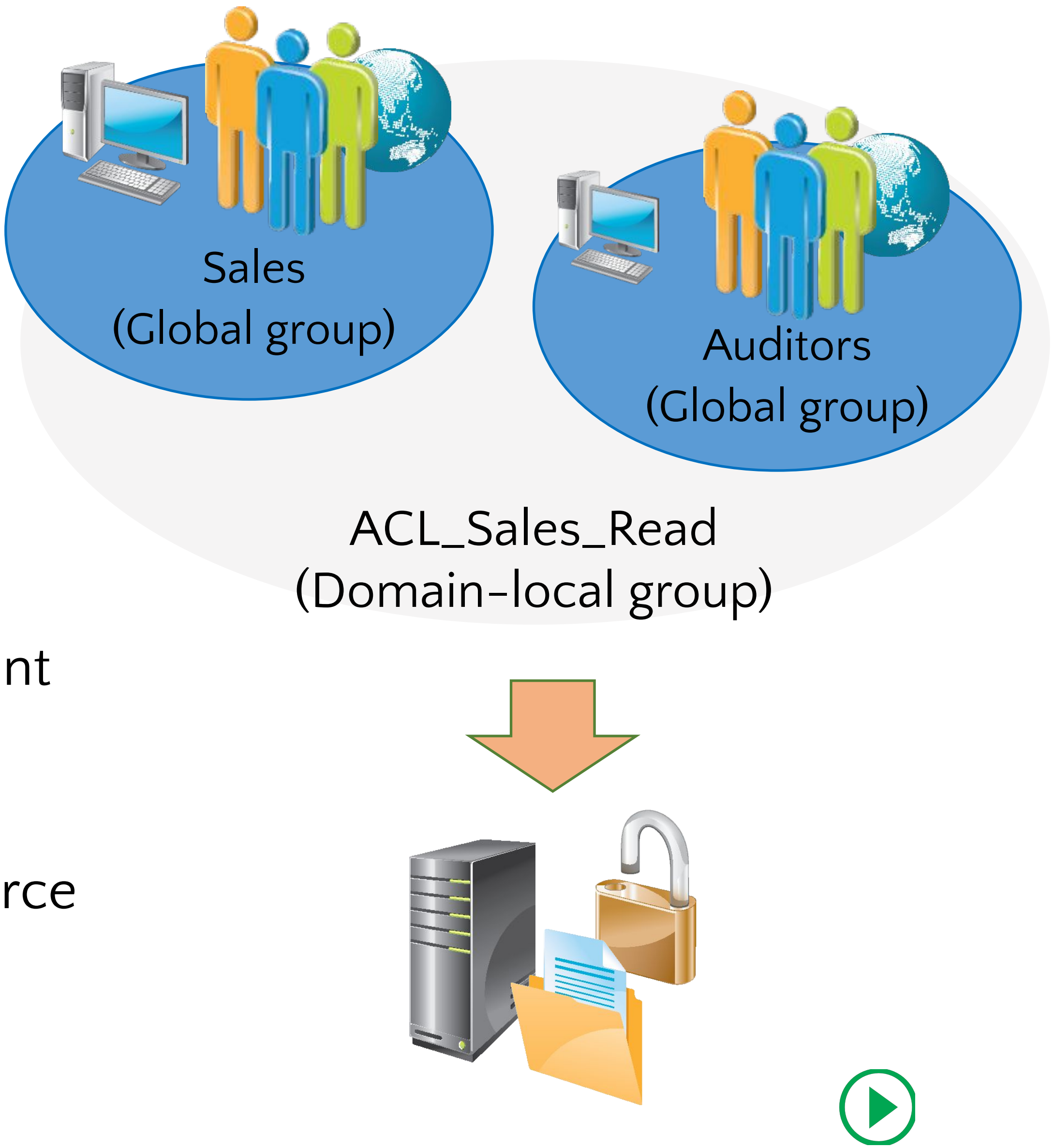
Implementing Group Management

I Identities
Users or computers, which are members of

G Global groups
Which collect members based on members' roles, which are members of

DL Domain-local groups
Which provide management such as resource access, which are

A Assigned access to a resource



Implementing Group Management

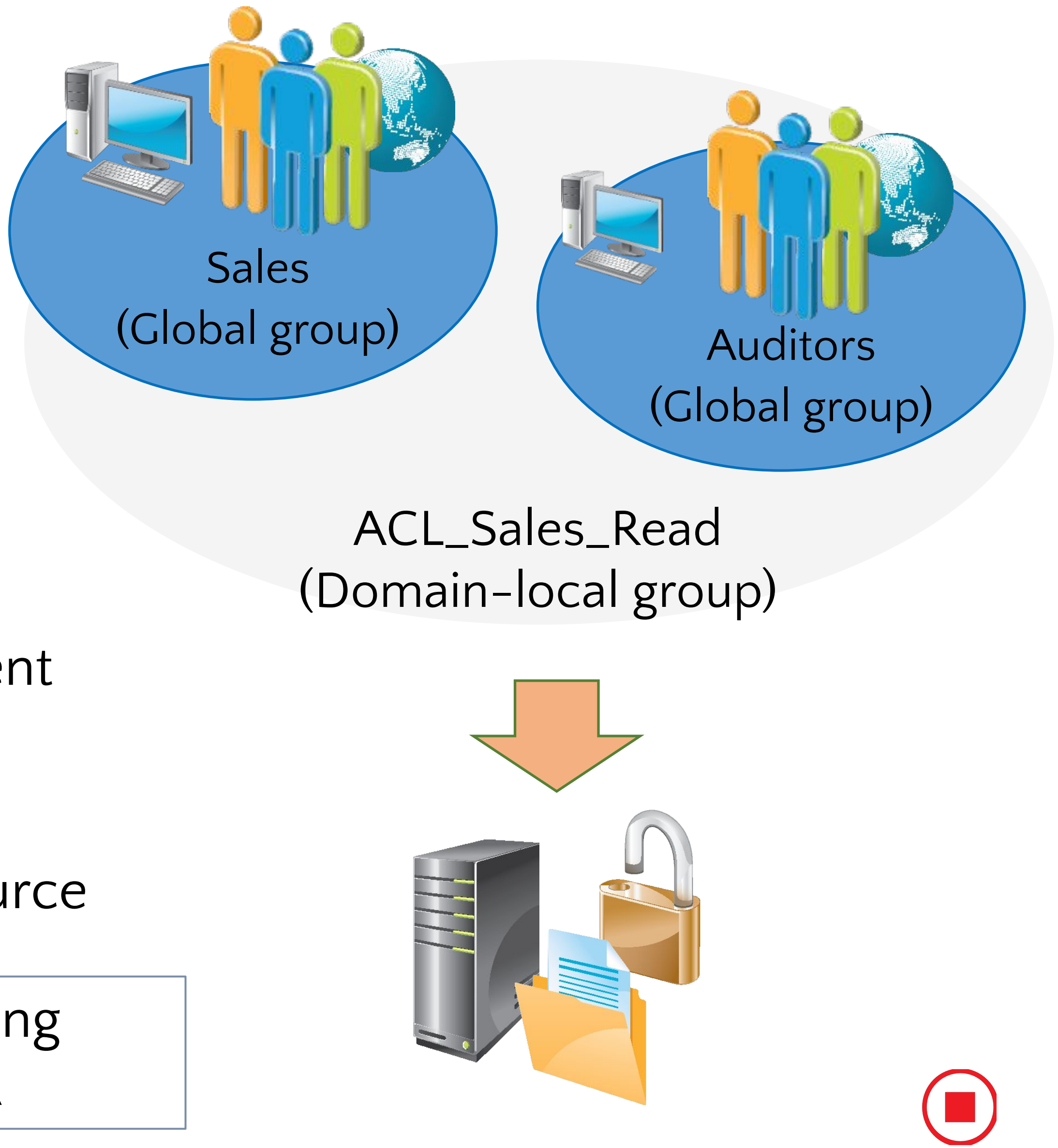
I Identities
Users or computers,
which are members of

G Global groups
Which collect members
based on members’ roles,
which are members of

DL Domain-local groups
Which provide management
such as resource access,
which are

A Assigned access to a resource

This best practice for nesting groups is known as IGDLA



Sales
(Global group)

Auditors
(Global group)

ACL_Sales_Read
(Domain-local group)

Default Groups

- Внимательно управляйте группами по умолчанию, т.к. они имеют расширенные административные привилегии

Group	Location
Enterprise Admins	Users container of the forest root domain
Schema Admins	Users container of the forest root domain
Administrators	Built-in container of each domain
Domain Admins	Users container of each domain
Server Operators	Built-in container of each domain
Account Operators	Built-in container of each domain
Backup Operators	Built-in container of each domain
Print Operators	Built-in container of each domain
Cert Publishers	Users container of each domain

Special Identities

- Special identities:
  - Группы членством в которых управляет ОС
  - Могут исопльзоваться для пердоставления доступа к ресурсам:
    - Anonymous Logon
    - Authenticated Users
    - Everyone
    - Interactive
    - Network
    - Creator Owner

Managing User and Service Accounts

User Account Policies

Use the following settings to set password requirements:

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Password complexity requirements
- Account lockout duration
- Account lockout threshold

User Account Policies

- Local Security Policy account settings:
  - Configured with secpol.msc
  - Применяется на local user accounts
- Group Policy account settings
  - Настраиваются в Group Policy Management console
  - Применяются на все accounts в AD DS и accounts, computers в домене