Active Directory

проф. д-р инж. Венета Алексиева

Основни моменти

- Active Directory – директорийни услуги
- Физическа структура
- Логическа структура
- Репликация
- Роли
- Директорийни услуги

Active Directory (AD) - Предназначение

- Съхранява информация за потребители, компютри, разпределени мрежови ресурси.
- Прави ресурсите достъпни за потребители и приложения, чрез имена, описание, местонахождение, достъп, управление и политики за сигурност.
- Предлага унифициран интерфейс за управление с възможност за репликация и резервираност.

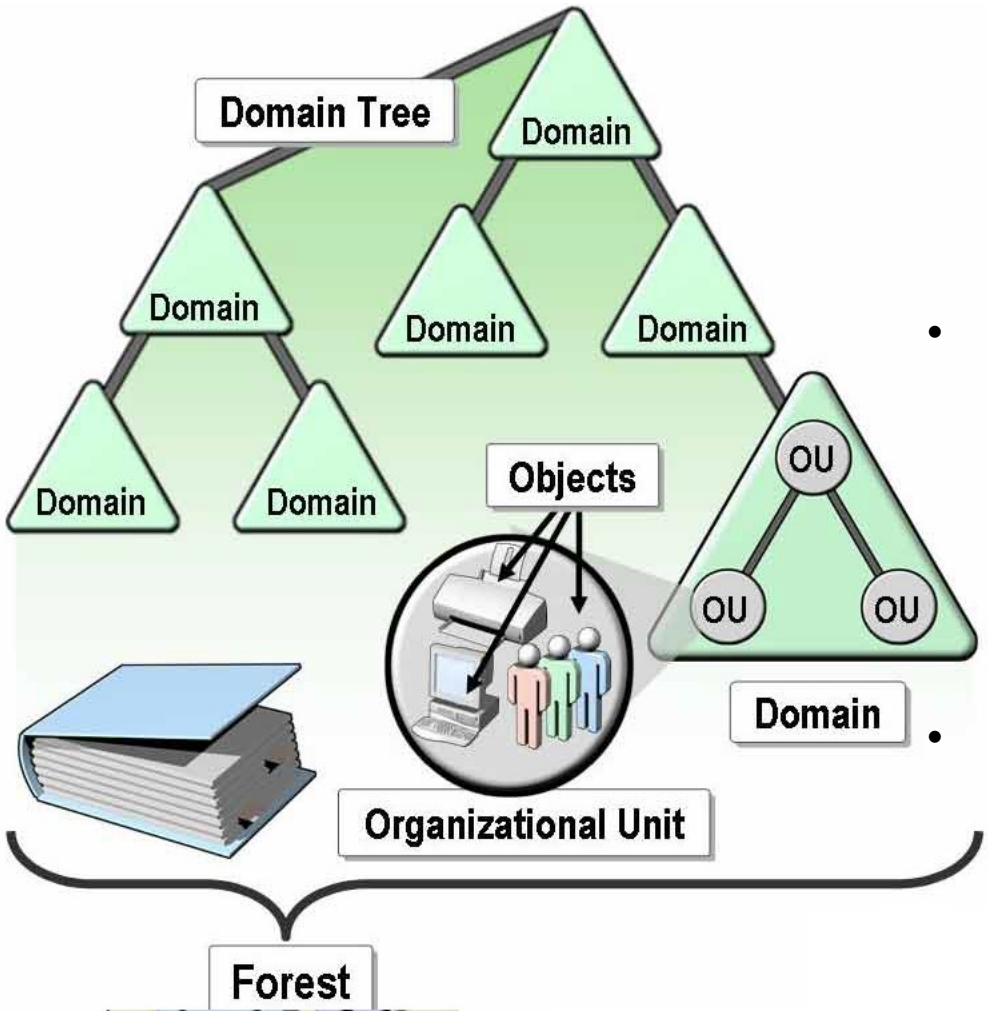
Функции

- Централизиран контрол на мрежови ресурси
  - само за оторизирани потребители
- Централизира и децентрализира управлението на ресурсите.
  - управление на разпределени клиентски компютри, мрежови услуги и приложения от централно място
  - разпределя административни задачи, като делегира контрола на ресурси, за други администратори.
- Съхранява обекти в сигурна, йерархична логическа структура.
- Оптимизира мрежовия трафик
  - Физическата структура на Active Directory позволява да се управлява мрежовия трафик по-ефективно (чрез оторизация от най-близкия компютър до клиента, което намалява количеството на мрежовия трафик).

Структура на AD

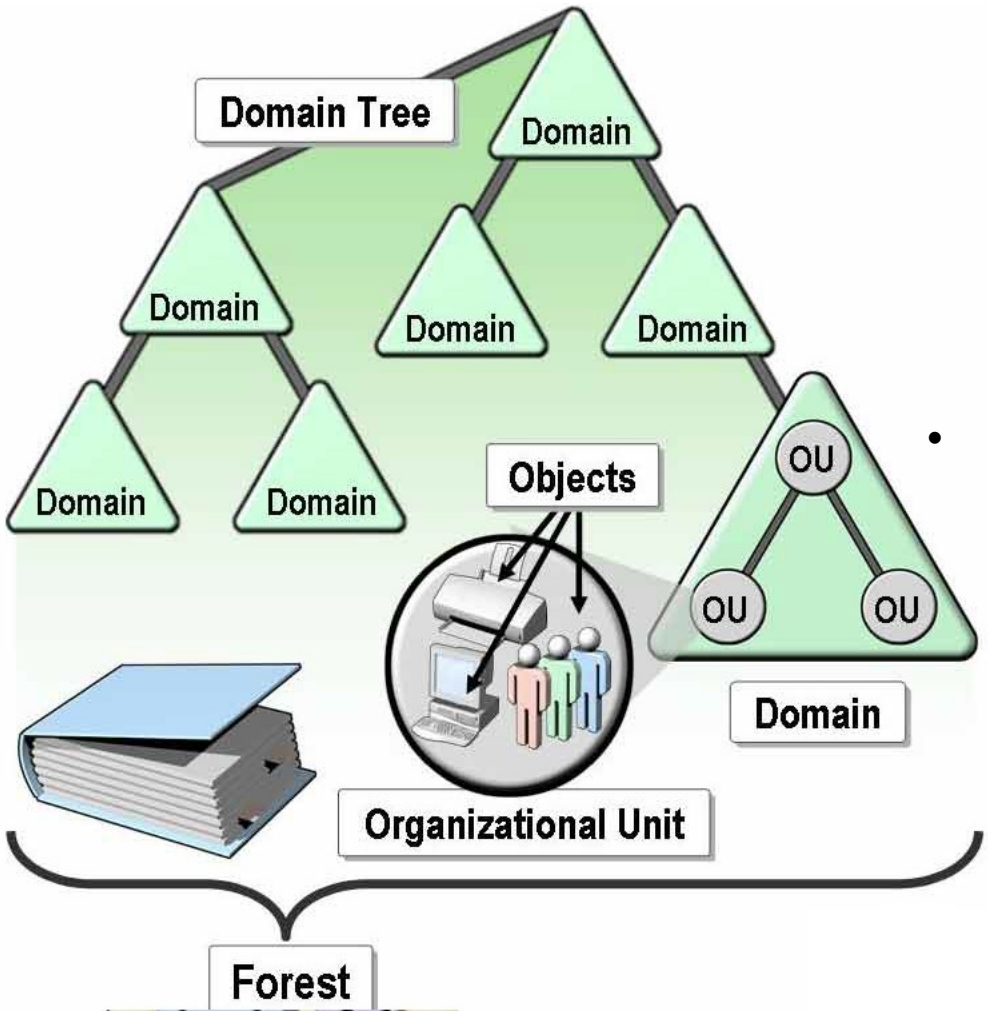
- Логическа
  - моделира административните изисквания
- Физическа
  - оптимизира мрежовия трафик, като определя кога и къде ще се прави репликация и логване в AD.

Логическа структура (1)



- **Обекти** – потребители и ресурси (компютри и принтери).
  - Описват се с обектен клас с атрибути стойностите, асоциирани с обекта.
  - Те представляват уникална комбинация за обекта.
- **Организационна единица** - Някои обекти са контейнери за други обекти. Това улеснява :
  - локализирането на обектите,
  - управлението на обектите,
  - делегирането на права за управление на организационната единица.
- **Домейни**– колекция от обекти, които имат БД, политики за сигурност и връзки на доверие с други домейни. Функции:
  - Административна граница за обекти
  - Средство за управление на сигурността на споделени ресурси
  - Единица на репликация за обекти

Логическа структура (2)

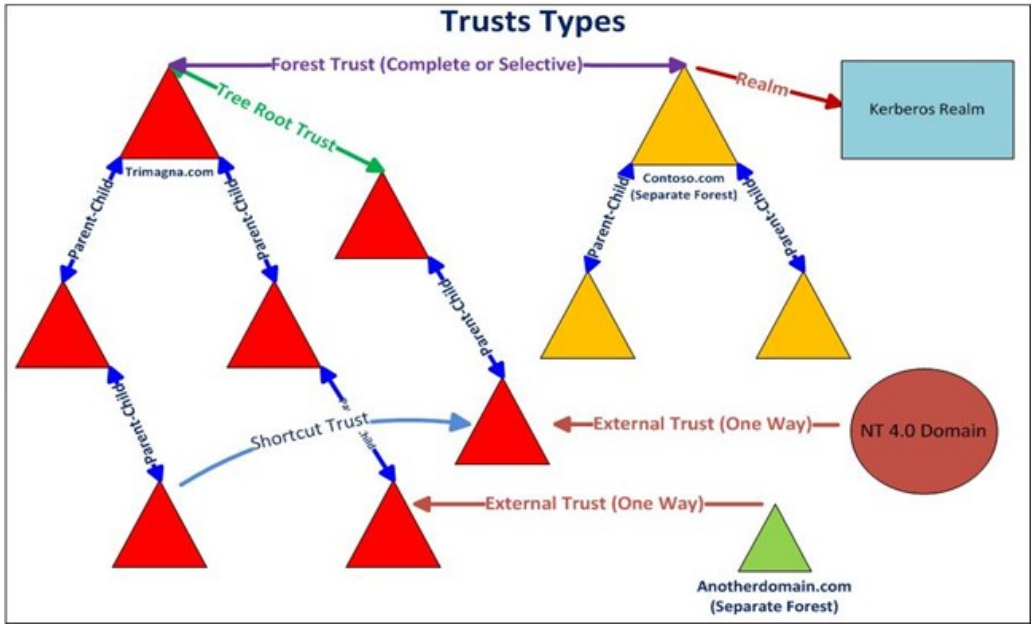


- **Домейн дървета** – домейни, групирани в йерархична структура :
  - Корен на домейна – дава име на гората (nwtraders.msft)
  - родителски домейни,
  - деца-домейни – името им е комбинация от името на родителя и уникално DNS име (corp.nwtraders.msft)
- **Гора** – най-оглемият логически контейнер в AD, пълно копие на AD:
  - Състои се от >=1 дървета.
  - В едно дърво на две нива, което се препоръчва за повечето организации, всички поддомейни са деца на корена, за да образуват едно непрекъснато дърво.
  - По подразбиране информация в AD се споделя само в гората.
  - Гората е граница на сигурност за информацията, която се съдържа в AD.

Отношение на доверие

- Това е сигурен метод за комуникация между домейни, дървета и гори.
- Доверието е връзка за автентициране между два домейна, чрез която потребителите могат да бъдат оторизирани за достъп до ресурси в други домейни.
  - Ако не са конфигурирани отношения на доверие, домейнът е ограничен при достъпа до ресурси **единствено в рамките на организацията**.
  - Ако доверието е конфигурирано, автентикационният механизъм за всеки домейн се доверява на автентикационния механизъм на другите доверени домейни. Ако потребител или приложение се автентицира от един домейн, неговата автентикация се приема от всички други домейни, които се доверяват на първия.

Отношения между домейни



Всички домейни в гората поддържат транзитивно двупосочно отношение на доверие с всеки друг домейн в гората:

- Parent-child
- Forest trust
- Shortcut trust- между домейни, които не са в наследствена връзка (не са транзитивни)

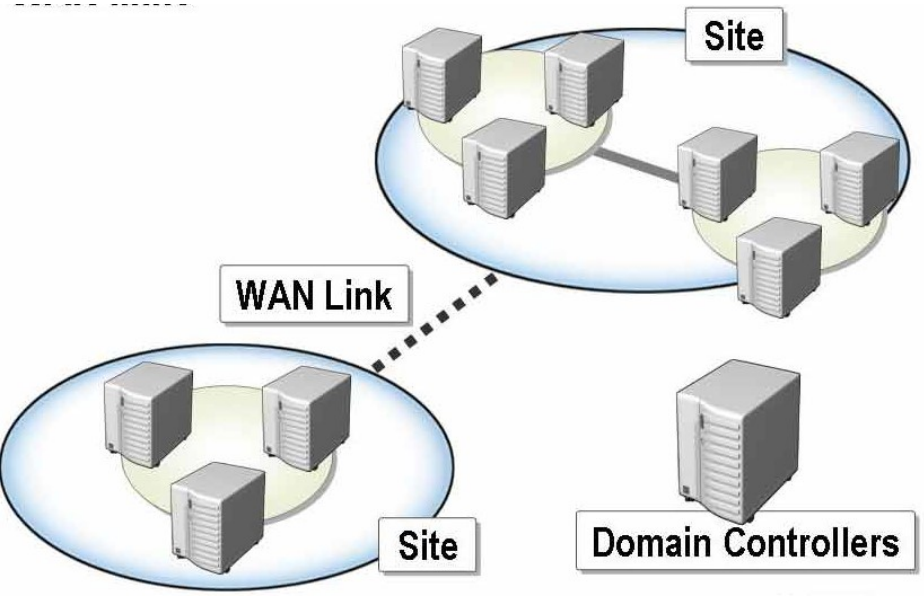
Групи в AD

- Локални за машината – за обектите, които са в локалната за компютъра БД. Те могат да имат за членове:
  - глобални групи,
  - домейн локални групи от техния собствен домейн
  - универсални групи от техния собствен домейн или от други домейни, на които се доверяват
- Домейн локални групи– създават се на домейн контролер (използват се за огромни инфраструктури с много домейни)
- Домейн глобални групи - създават се на домейн контролер
- Универсални групи - могат да бъдат от всеки домейн в AD гора.

Глобален каталог

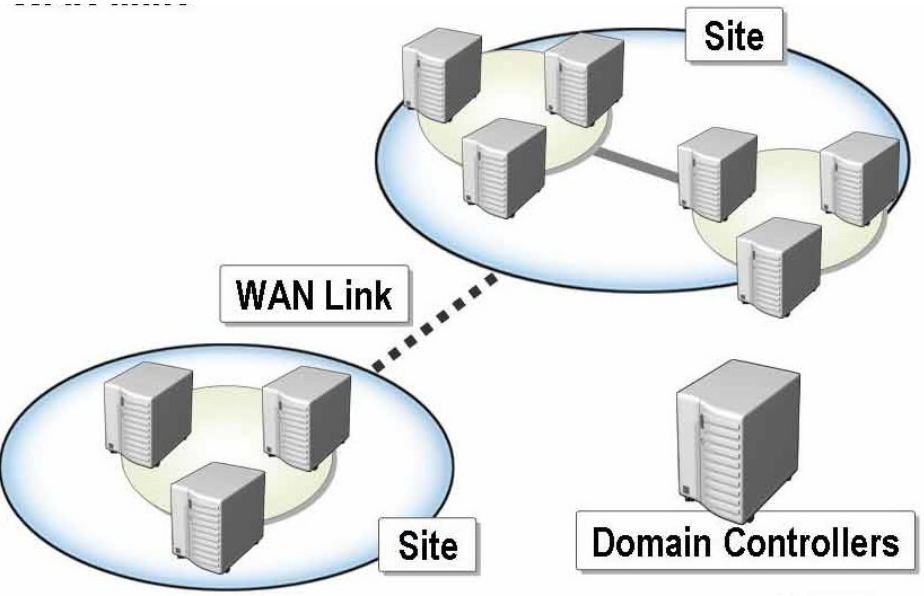
- Ресурсите в AD може да се споделят между домейни и гори.
- Глобалният каталог улеснява потребителя в търсенето на обект, т.к. е без значение той къде се намира и не се налага да се търси по отделно във всеки домейн.
- **Глобалният каталог** е репозитория с информация, която съдържа подмножество от атрибути за всички обекти
- Членовете на админ групата на схемата могат да променят кои атрибути да се съхраняват в глобалния каталог. Това са атрибутите, които най-често се използват в заявките за търсене:
  - име или фамилия на потребителя, logon name
  - Информация, необходима за локализацията на обект
  - Правата за достъп до обекта (ако няма права за да се вижда обекта, той няма да се появи в резултатите от търсенето), т.е. потребителят може да намери само обектите, до които има права за достъп
- **Global catalog server** е DC, който ефективно изпълнява заявки от вътрешността на гората в глобалния каталог.
- Първият създаден DC в AD става **global catalog server**.
- Могат да се създадат допълнителни global catalog servers за балансиране на трафика за автентикация и заявки за търсене.

Физическа структура (1)



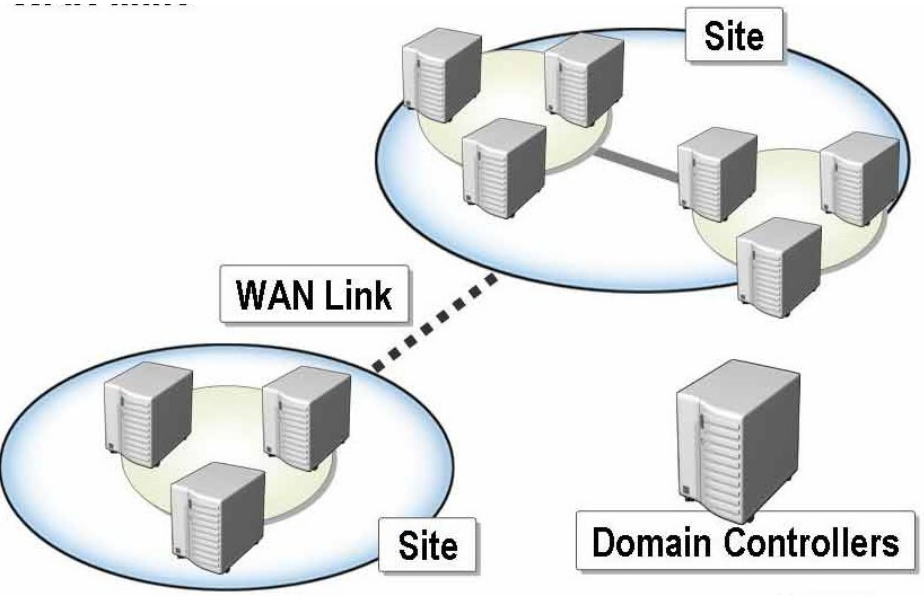
- **Домейн контролери** - компютри с WindowsServer и AD.
  - Всеки домейн контролер изпълнява функции за съхранение и репликация.
  - Един домейн контролер може да поддържа само един домейн.
  - Всеки домейн трябва да има повече от един домейн контролер, за да е налична AD 24/7.

Физическа структура (2)



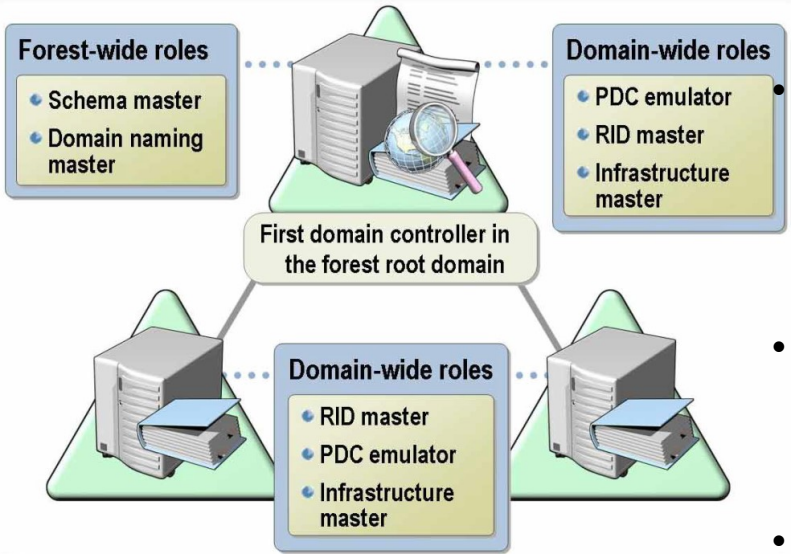
- **Сайтове**- групи от свързани компютри.
  - Домейн-контролерът в рамките на сайта общува често - тази комуникация намалява закъснението в рамките на на сайта при промени.
  - Намалява времето за репликация на един домейн контролер в друг.
  - Сайтовете оптимизират използването на честотната лента между контролери на домейни, които са в различни места.

Физическа структура (3)



- **AD partitions**
  - съдържа копия на всички обекти в този домейн.
  - Един partition на домейна се репликира само с друг домейн контролер в същия домейн.
  - ***domain partition*** - реплики на всички обекти в домейна,
  - ***configuration partition*** -структурата на гората, т.е. запис на всички домейн контролери и връзките между тях
  - ***schema partition*** – схемата на цялата гора със съответната дефиниция на всеки обект клас
  - ***Optional application partition*** - съдържат обекти, които не са свързани със сигурност, но се използват от >=1 приложения. Те се репликират на определени домейн контролери в гората.

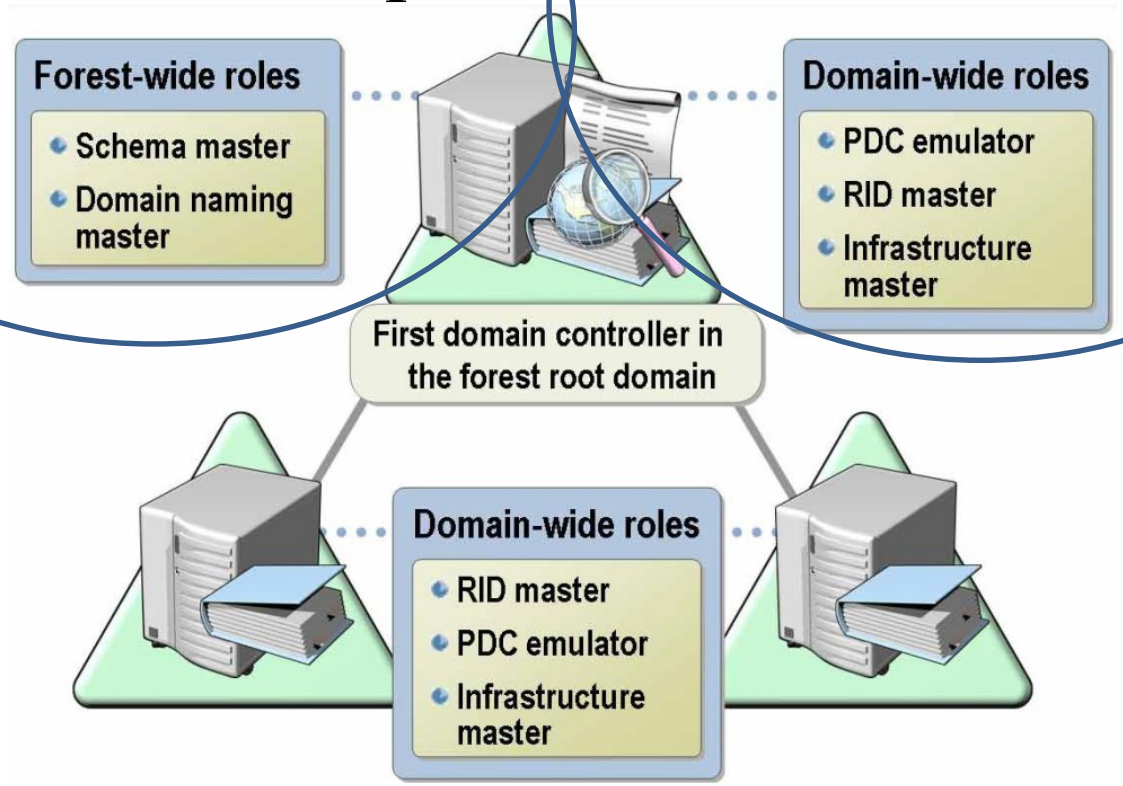
Single/Multi master репликация



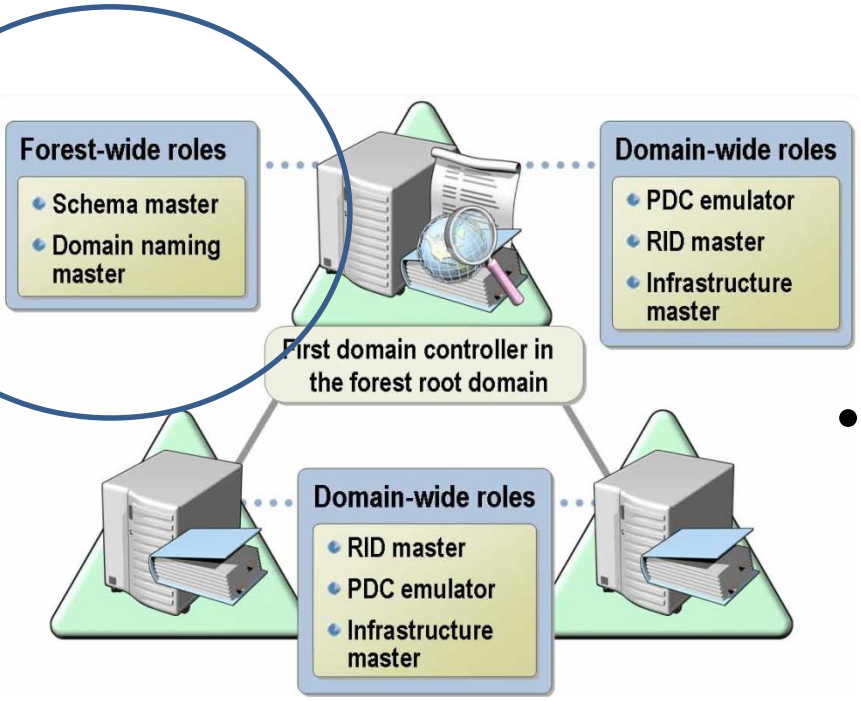
- **Multimaster репликация-** промени, направени в схемата се повтарят във всички домейни в гората. При промяна в домейн тя се повтаря във всички контролери в домейна.
- По време на **Multimaster репликация**, може да се случи конфликт, ако актуализации на атрибут на един и същ обект се изпълняват едновременно от два домейн контролера.
- Избягва се като се ползва **една master репликация-** единствен домейн контролер, на който могат да бъдат направени промени - добавяне на нов домейн или промяна на схемата на цялата гора.
- Операциите, които използват **единична master репликация** са подредени заедно в специфични роли в една гора или домейн.
- Контролерът на домейн, който е отговорен за определена роля, се нарича операционен master за тази роля.
- AD съхранява кой домейн контролер притежава специфична роля.

Работни master роли

- forest-wide – уникални за гората
- domain-wide - уникални за всеки домейн в гората.

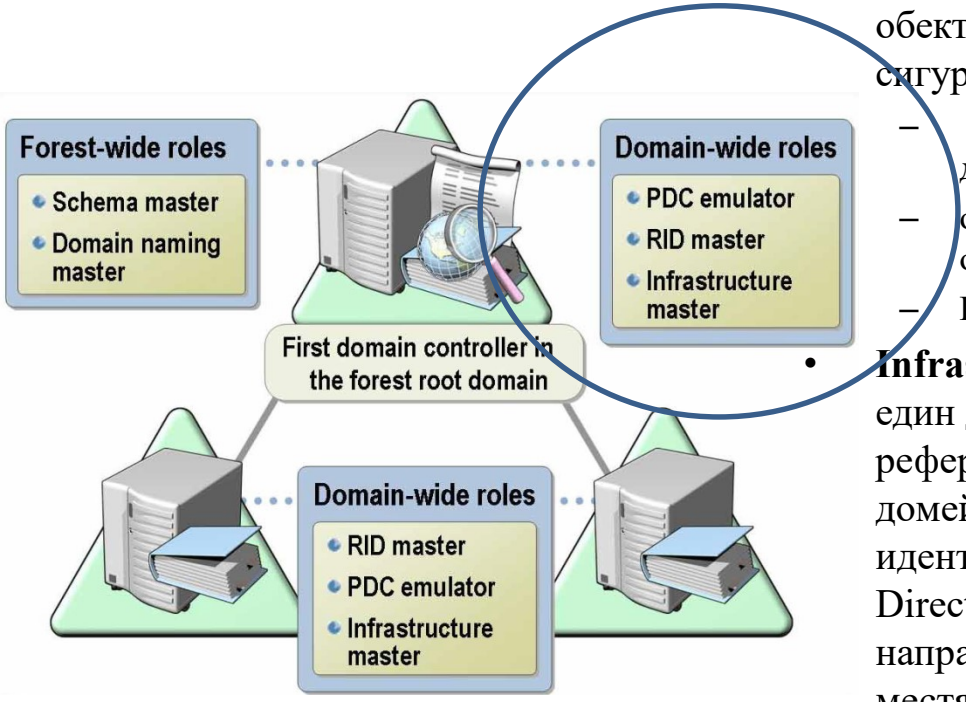


Forest-wide master роли



- **Schema master** –контролира ъпдейтите на схемата. Съдържа master списък с обектните класове и атрибути, които се използват за създаване на обекти в AD като потребители, компютри, принтери
- **Domain naming master-** контролира добавяне или изтриване на домейни в гората. Само домейн контролера, който държи domain naming master ролята може да добави домейн.

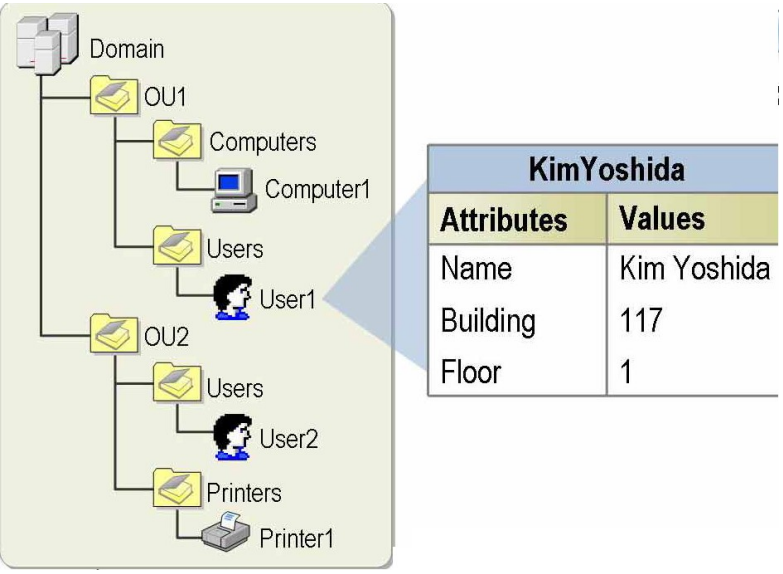
Domain-wide master роли



- **Primary domain controller emulator (PDC)** –Създава се първи в новия домейн. Поддържа **backup domain controllers** (BDCs) в *mixed-mode domain.*
- **Relative identifier master-(RID master).** При създаване на нов обект DC създава нов, отговарящ за сигурността на обекта, и възлага на обекта уникален идентификатор за сигурност (SID), който се състои от:
  - домейн SID, който е един и същ за всички създадени в домейна,
  - относителен идентификатор (RID), който е уникален за всеки отговарящ за сигурността, създаден в домейна.
  - RID master разпределя блокове RIDs за всеки DC
- **Infrastructure master-** Когато обектите са преместени от един домейн в друг**,** Infrastructure master актуализира референциите на обекта от неговия домейн в другия домейн. Референцията на обект съдържа глобално уникален идентификатор (GUID), съдържащ име и SID. Active Directory периодично актуализира GUID, за да отрази направени промени в действителните обекти, които се местят в рамките на домейн и между домейни или изтриване на обекти.

Директорийни услуги (1)

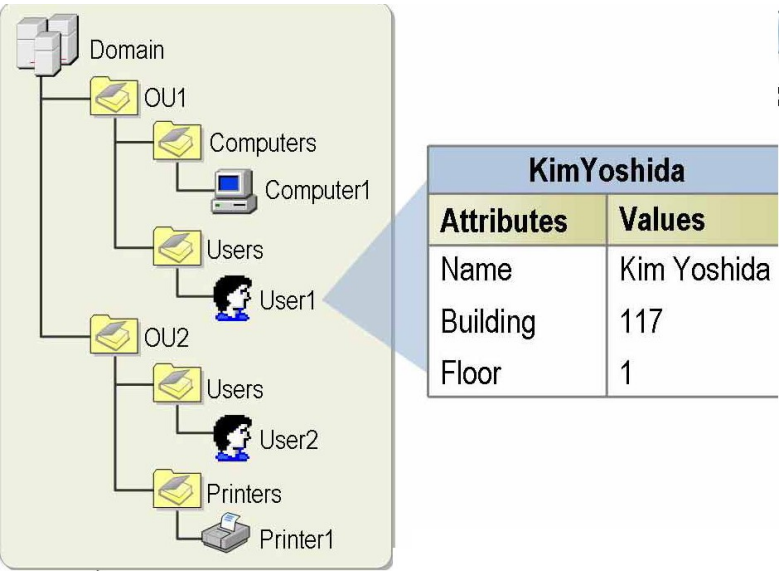
Ресурсите в големи мрежи се споделят от много потребители и приложения.



- **Директорийната услуга (**Active Directory) съхранява структурирана информация за хора и ресурси в една организация.
- **Директорийната услуга** дава възможност на потребители и приложения за достъп до ресурсите и информация за тях. Тя:
  - Именова ресурсите
  - Описва ги
  - Локализира ги
  - Дава достъп до информация за обекти
  - Управлява ги
  - Пази сигурно информация за тях
  - Предлага търсене на обекти по техния обектен клас, атрибути, стойности на атрибутите, тяхното местоположение в рамките на структурата на AD, или всяка комбинация от тези стойности.
  - Така без да се знае физическата топология се дава достъп до всички ресурси

Директорийни услуги (2)

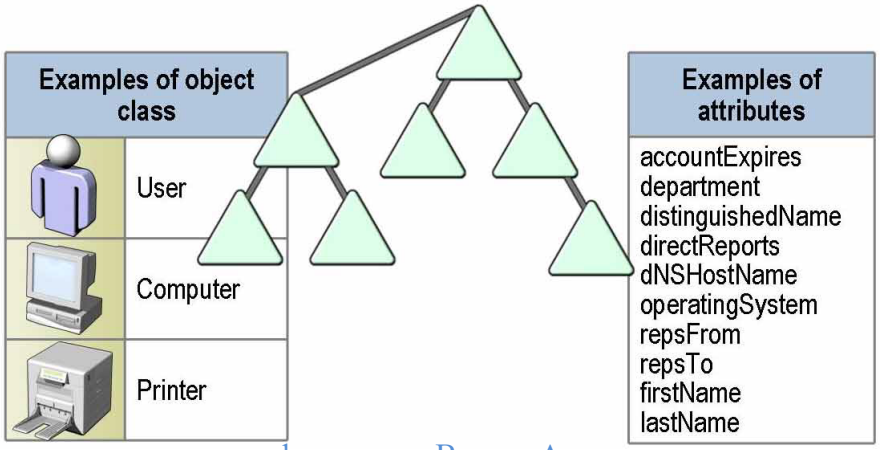
Ресурсите в големи мрежи се споделят от много потребители и приложения.



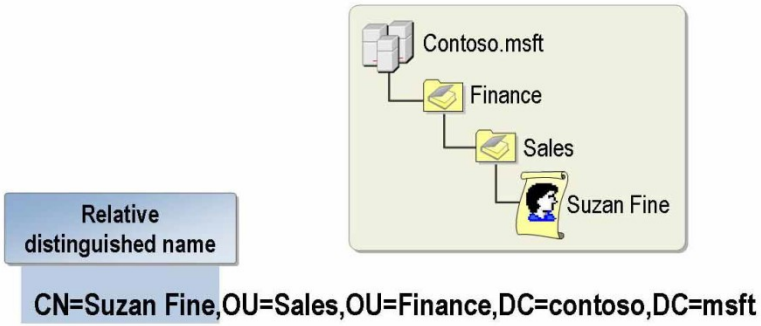
- Без да се знае физическата топология се дава достъп до всички ресурси.
- AD позволява съхраняване на голям брой обекти, които са организирани в partitions
- AD позволява лесно разрастване на организацията.
- AD позволява изпълняване на услуги не само от ОС, но и от приложения в режим **Application Mode (AD/AM)**
- AD/AM – няколко инстанции на AD/AM могат да се изпълняват едновременно на един сървър с независимо конфигуриране.

Схема

- **AD схема** дефинира множеството от обекти, типове информация за тях, конфигурациите по подразбиране за сигурността им.
- **AD схема** съдържа дефиниции на всички обекти- потребители, компютри, принтери, които се съхраняват в AD.
- Има само една схема в една гора, за да отговарят всички обекти на едни и същи правила.
- Схемата съдържа 2 типа дефиниции:
  - обектни класове – колекция от атрибути
  - Атрибути – дефинирани са отделно от обектните класове. Всеки атрибут се дефинира веднъж, но може да се ползва в няколко обектни класове
- Могат да се създават нови типове обекти в AD като се разширява схемата, предефинират се класове или атрибути.



AD и DNS (1)



- AD изисква DNS за откриване местоположението на ресурсите в мрежата.
- Всички версии на Windows използват DNS. Само при отказ на DNS компютрите ще използват системата за именуване WINS.
- Зоновите файлове на DNS могат да бъдат съхранени в AD хранилище на данни, което предоставя по-добра функционалност и сигурност.
- AD имената на домейни представляват DNS имена, т.е. **DNS реализацията трябва да съответства на AD домейн реализацията на организацията.**

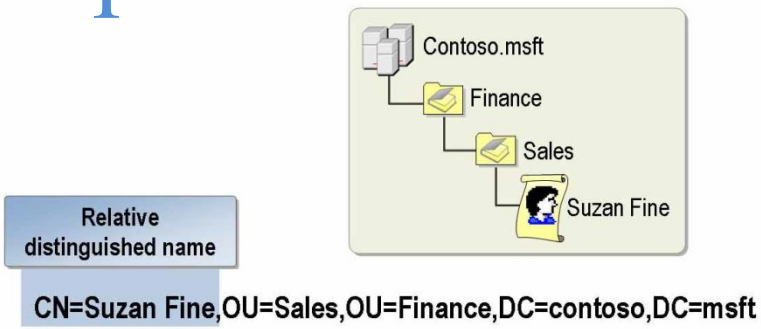
AD и DNS (2)

За откриване местоположението на домейн контролерите, AD използва специални ресурсни записи в DNS – SRV ресурсен запис. Например:

_ldap._tcp.corp.com. 600 IN SRV 0 100 389 DC.corp.com

Компонент	Пример	Описание
Услуга	_ldap	Услугата, идентифицирана от този запис. Това идентифицира услугата като сървър, който отговаря на LDAP (Lightweight Directory Access Protocol) заявки.
Протокол	_tcp	Използван транспортен протокол.
Име	corp.com	Името на домейна, за когото е този запис.
TTL	600	Времето за живот на записа в кеша (в секунди).
Клас	IN	Стандартен Интернет клас.
Ресурсен запис	SRV	Идентифицира записа като SRV.
Приоритет	0	Идентифицира приоритета на записа за клиента. Ако съществуват множество записи за една и съща услуга, клиентът ще се свърже към сървър с най-малка стойност на приоритета.
Тегло	100	Механизъм за балансирано натоварване. Ако има няколко записа с еднакъв приоритет, клиентът ще избере запис с най-високото тегло.
Порт	389	Портът, използван от тази услуга.
Цел	DC.corp.com	Машината, предоставяща указаната услуга.

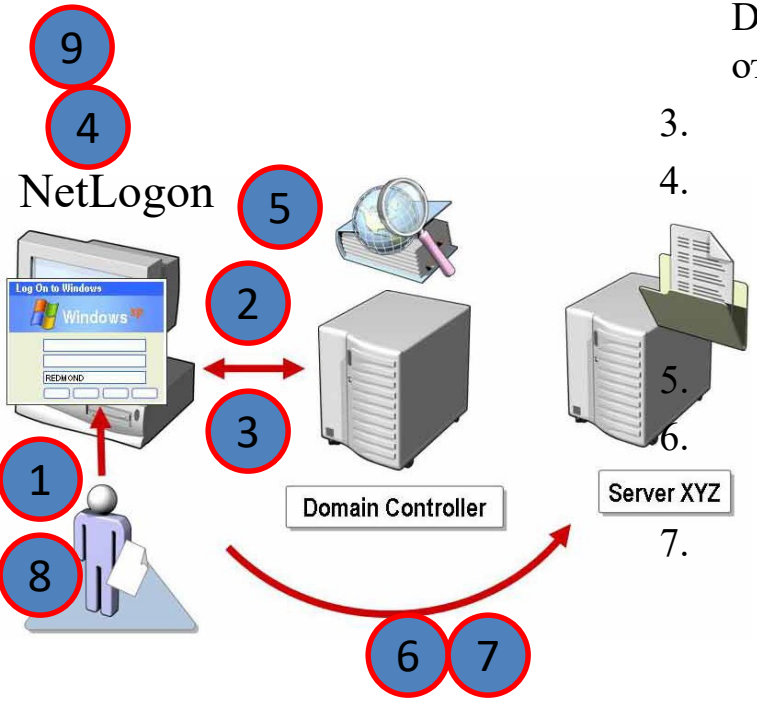
Разграничени и относително разграничени имена



- Клиентските компютри използват Lightweight Directory Access Protocol (LDAP) за търсене и модифициране на обектите в БД на AD.
- LDAP е част от X.500, който дефинира структурата на директориите , за да намери обектите по уникално име.
- **Разграничено име (Distinguished name)** – име на обекта, по което обекта се локализира в домейна и пълния път, по който да се достигне обекта. То е уникално в гората.
- **Относително разграничено име (relative distinguished name) –** уникално идентифицира обекта в контейнера. То е винаги първия компонент в distinguished name, но не винаги е CN.

- CN (common name) – име на обекта в контейнера
- OU (organizational unit) – организационната единица, в която е обекта. Може да е повече от една, но са в йерархична структура
- DC (domain component) -.com. , .msft. Има поне 2 DC, но е възможно да са повече, ако домейнът е дъщерен домейн.

Логване на клиент в домейн



1. Потребителят се логва:
   1. клиентският компютър изпраща RPC (*Remote Procedure Call*) съобщение към локалната услуга *NetLogon*, инициирайки logon сесия.
   2. изпраща се: името на компютъра, името на домейна и името на сайта.
2. Услугата *NetLogon* изпраща заявка до конфигурирания на машината DNS сървър за получаване на адреса на домейн контролера, отговарящ за конкретния домейн.
3. DNS сървърът връща изисквания списък от сървъри.
4. Клиентът сортира списъка на базата на приоритета.
   1. Списък със сървъри с еднакъв приоритет се подрежда на основата на теглата.
   2. Клиентът започва да обработва списъка по ред.
5. Получава IP адресите на всеки сървър (отново от DNS системата).
6. Изпраща LDAP заявка на UDP порт 389 към всеки от адресите по реда на тяхното получаване.
7. След изпращане на заявка, клиентът изчаква за отговор. Ако не се получи отговор, се изпраща заявка към следващия домейн контролер. Този процес продължава до получаване на валиден отговор или до изчерпване на списъка с всички домейн контролери.
8. След получаване на положителен отговор от домейн контролер, клиентът започва процеса на логване с домейн контролера.
9. Клиентът кешира информацията за домейн контролера.

Управление с AD

- Позволява **централизирано и децентрализирано управление** на потребители, компютри, принтери и мрежови ресурси.
- Администраторът може да делегира административни привилегии на потребители или групи.

Централизирано управление с AD

- Държи информация за всички обекти и атрибути и от едно място могат да се управляват всички мрежови ресурси
- Лесно се локализира обект с търсене по определени атрибути на база LDAP
- Може да се групират обекти с подобни административни или security изисквания в организационни единици (OU)
- OU осигуряват няколко нива на привилегии и политики за сигурност и позволяват делегиране на административен контрол
- Може да се задават групови политики за сайт, домейн или OU
- Тези групови политики се прилагат за всички потребители и компютри в контейнера

Децентрализирано управление с AD

- Може да се делегират различни права за някои потребители и групи върху част от обектите в домейна
  - Например: Full Control за OU Sales.
- Може да се модифицират специфични атрибути за обект в OU
  - позволения да се промени име, адрес,…
  - да се смени паролата на акаунта от потребителя
  - да се ресетнат всички пароли в OUs за домейна…

AD snap-ins

- Active Directory Users and Computers
  - Управлява потребителски акаунти, групи, компютърни акаунти, добавя компютри в домейна, управлява политики, задава права на потребителите, съблюдава политиките
- Active Directory Domains and Trusts
  - Управлява доверието между домейни и гори, добавя на потребителя главния суфикс, променя функционалните нива на домейн и гора
- Active Directory Sites and Services
  - За репликация на данните за директорията
- Active Directory Schema
  - Управлява схемата и не е по подразбиране в менюто. Трябва да се добави ръчно.

AD tools

- Dsadd
  - Добавя обекти – компютри, потребители, групи, OU, контакти в AD.
- Dsmod
  - Модифицира обекти
- Dsquery
  - Изпълнява заявки в AD по специфични критерии.
- Dsmove
  - Мести обект в домейна на нова локация в AD
  - Преименува обекта без да го мести
  - Изтрива обект от AD
- Dsget
  - Извежда на екран избраните атрибути за обектите в AD.
- Csvde
  - Импортира/експортира данните за AD в comma-separated формат.
- Ldifde
  - Създава, модифицира и изтрива обекти в AD.
  - Разширява AD схемата
  - Експортира информация за потребители и групи към други приложения или услуги

AD scripts

- За бързо прилагане на по-сложна промяна в AD се създават скриптове, включващи по-сложни условия
- Те се създават за:
  - Комплексно търсене на информация за обекти в AD
  - Добавяне на обекти в AD
  - Модифициране на стойностите на атрибутите в обектите на AD
  - Изтриване на обекти от AD
  - Разширяване на схемата за AD

AD-планиране и реализация (1)

Стъпки	Описание
Дизайн на AD	На база на изискванията към организиране на самия бизнес
Планиране на AD	На база на техническите аспекти на дизайна
Реализация на AD	Създаване на гора и структура на домейна

AD-планиране и реализация (2)

Стъпки	Описание
Дизайн на AD	На база на изискванията към организиране на самия бизнес: •Събиране информация за организацията – профил на потребителите, локации на офисите, техническа и мрежова инфраструктура, планове за промяна и разрастване… •Анализ на събраната информация •Анализ на възможните решения – гъвкавост, разрастване… •Избор на дизайн – сравняване на предимства и недостатъци на възможни решения •Възможна е промяна на първоначалния избор на дизайн!
Планиране на AD	На база на техническите аспекти на дизайна
Реализация на AD	Създаване на гора и структура на домейна

AD-планиране и реализация (3)

Стъпки	Описание
Дизайн на AD	На база на изискванията към организиране на самия бизнес
Планиране на AD	На база на техническите аспекти на дизайна: •Стратегия за акаунти – именуване, политики… •Стратегия за одит- какво ще се наблюдава •План за създаване на OU –колко и какви OU- на географски, на функционален или друг принцип •План за създаване на групи •План за сайтовете и връзките между тях •План за разпространение на софтуера •План за избор на сървъри, разполагане на домейн контролери, сървъра с глобалния каталог, DNS сървъра, работни сървъри
Реализация на AD	Създаване на гора и структура на домейна

AD-планиране и реализация (4)

Стъпки	Описание
Дизайн на AD	На база на изискванията към организиране на самия бизнес
Планиране на AD	На база на техническите аспекти на дизайна
Реализация на AD	Създаване на гора и структура на домейна: •Структура на организационните единици •Създаване на потребителски и компютърни акаунти •Създаване на Групи – по функции и по нива на сигурност •Създаване на групови политики •Прилагане на политиките към домейни, сайтове и организационни единици •Създаване на политики за разпространение на софтуера

Въпроси ?

Благодаря за вниманието !