Active Directory

Христо Вълчанов
Технически Университет - Варна

Предназначение на AD

- Active Directory Domain Services (AD DS) е директорийна услуга посредством която се организира динамичен и лесен достъп до разпределени мрежови ресурси.

Функции на AD

- Улеснява управлението на Windows мрежи с голям брой обекти. Управлението е чрез унифициран интерфейс.
- Консолидирана структура на домейни.
- Възможност за делегиране на административен контрол над ресурсите.
- Редуцира влиянието на пропускателната способност на мрежите.
- Опростено споделяне на ресурси.
- Интегрирана репликация и резервираност.
- Бързо откриване на ресурси.
- Ниска обща цена на администриране.

Компоненти на AD

- **Directory**. Самостоятелно хранилище на информация за потребителите и ресурсите в организацията.
- **Domain**. Колекция от обекти в директорията която формира област на управление. Домейните се именуват на базата на DNS.
- **Domain Controler (DC).** Услуга, съдържаща информация за сигурността и база от директорийни обекти за определен домейн. Отговаря за автентицирането на обектите в тяхната сфера на контрол.
- **Forest**. Най-големият логически контейнер в AD и включва всички домейни в неговия обхват, всички автоматично свързани заедно в транзитивно доверие. По този начин домейни от една част от гората автоматично се доверяват на всички останали домейни в нея.

Компоненти на AD

- **Organizational Unit (OU)**. Контейнер, съдържащ обекти. OU могат да се организират в йерархично дърво, съответстващо най-добре на структурата на конкретна организация.
- **Object**. Отделен компонент на директорията – потребител, група, споделена папка, принтер, контакт и дори OU.
- **Schema**. Схемата в AD е актуалната структура на базата данни. Различните типове информация, съхранена в AD се наричат атрибути. Схемата също поддържа стандартно множество от класове или типове обекти. Класът описва обект и асоциираните свойства, които се изискват за създаване на инстанция на обект.

Компоненти на AD

- **Site**. Колекция от компютри, които се географски отдалечено разположени и свързани с определени високоскоростни мрежови връзки.
- **Tree**. Колекция от домейни, започваща от единичен корен и разклоняваща се в периферни „дъщерни домейни”. Дърветата могат да се свържат в гора.
- **Trust**. В термините на AD е сигурен метод за комуникация между домейни, дървета и гори. Доверията позволяват потребителите в един домейн да се автентицират към други домейн контролери от друг домейн.

Групи в AD

- **Machine local groups.** Съдържа обекти, които принадлежат само на локалния компютър (или по-точно на обектите, съдържащи се в локалната за компютъра SAM база данни). Тези типове групи могат да имат за членове глобални групи, домейн локални групи от техния собствен домейн и универсални или глобални групи от техния собствен домейн или от други домейни на които се доверяват.

Групи в AD

- **Domain local groups**. Създават се само на домейн контролер. Могат да бъдат включени в машинни локални групи в същия домейн (процес, известен като влагане). Могат да съдържат глобални групи от домейн, който се доверява на текущия и други домейн локални групи от същия домейн. Използват се основно в огромни инфраструктури с множество домейни.

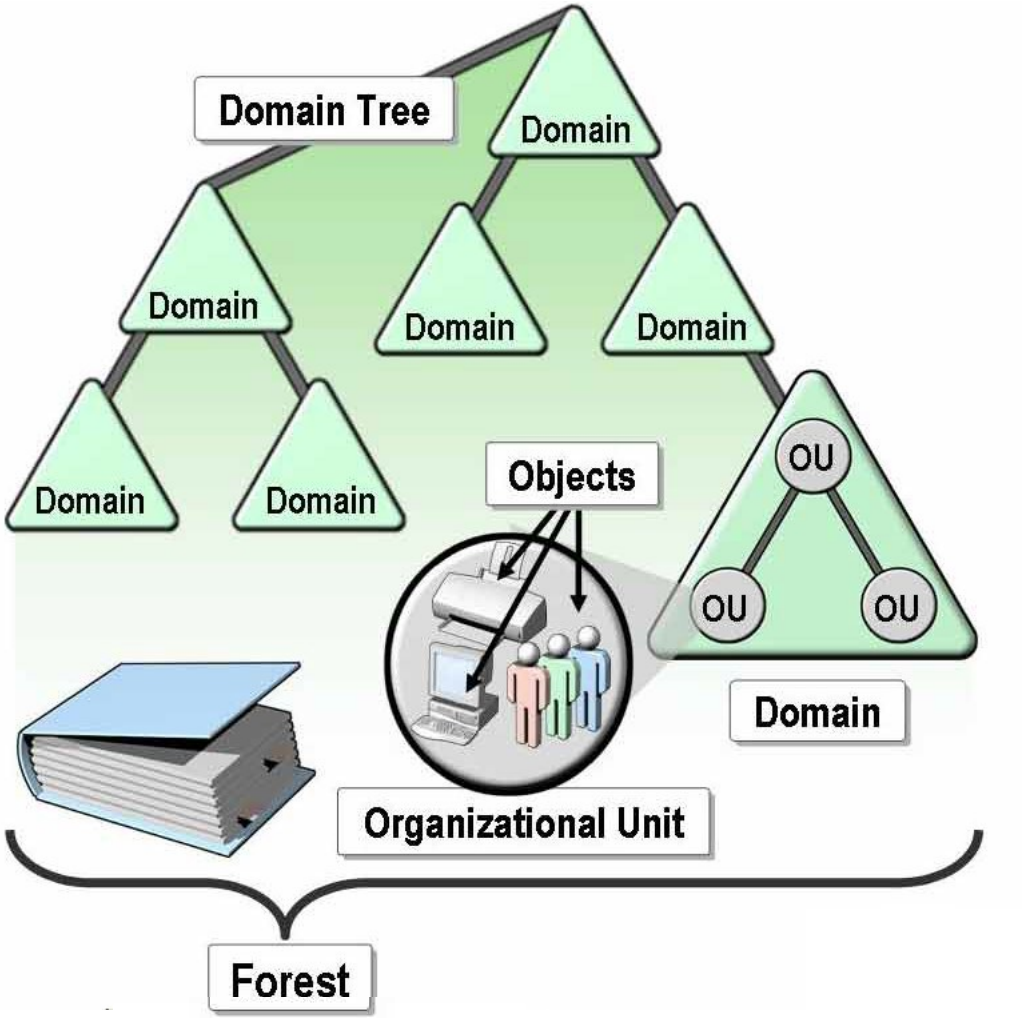
Групи в AD

- **Domain global groups**. Създават се само на домейн контролер. Могат да бъдат включени във всяка локална група на машина, която е член на текущия домейн или на доверен такъв. Могат също да бъдат влагани в други глобални групи, но всичките вложени домейн глобални групи трябва да са от същия домейн. Този тип групи са широко използван тип в домейните.

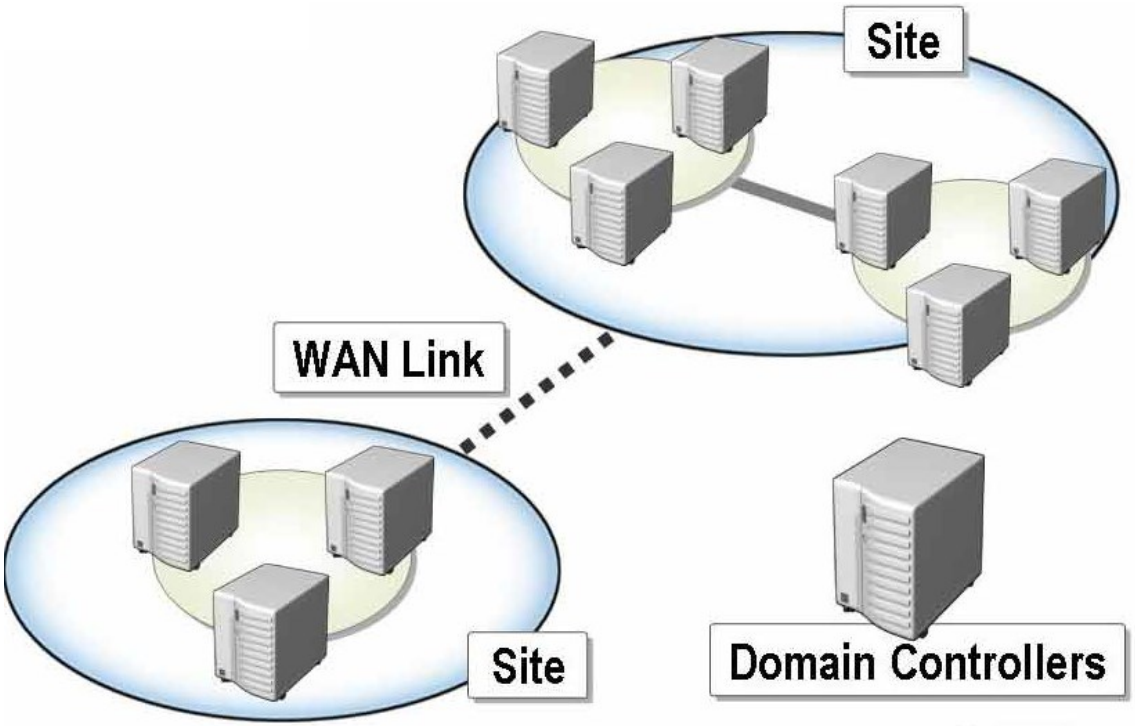
Групи в AD

- **Universal group**s. Съдържат глобални и универсални групи и тези вложени групи могат да бъдат от всеки домейн в AD гора.

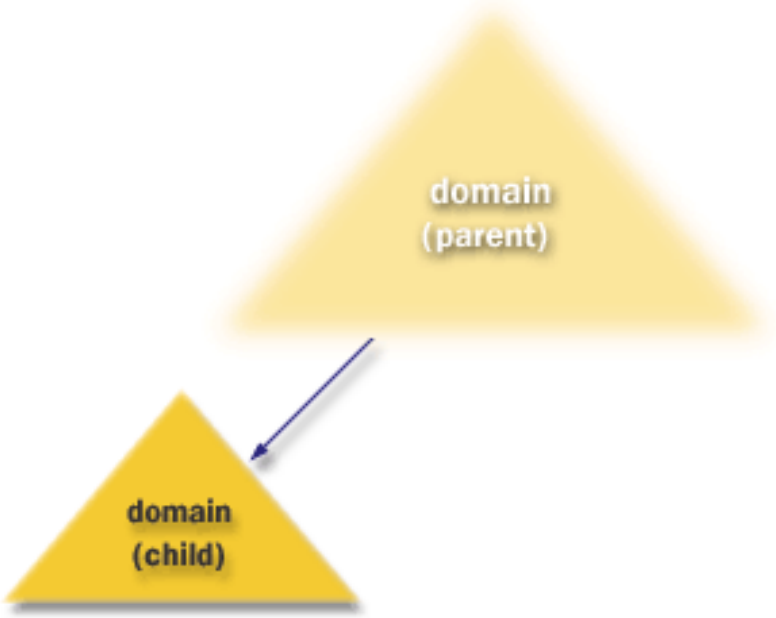
Логическа структура на AD



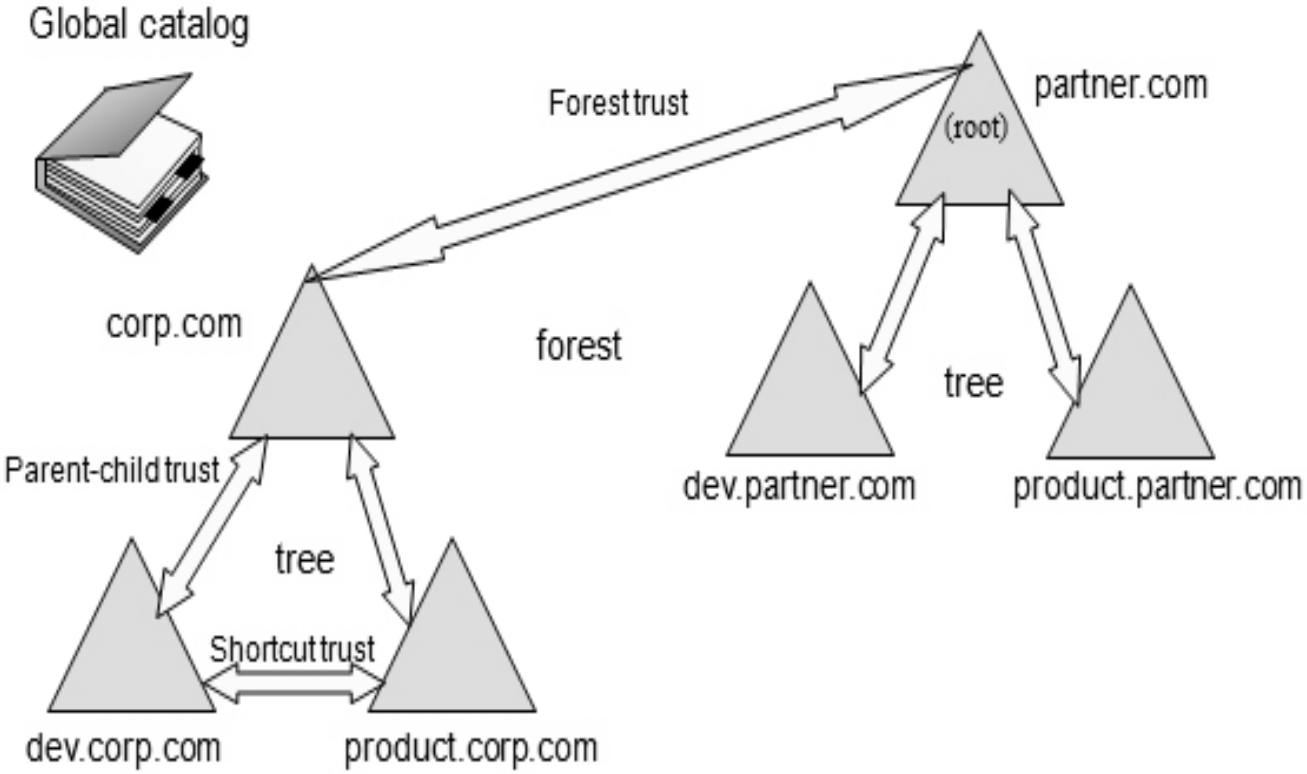
Физическа структура на AD



Отношения между домейни



Отношения на доверие

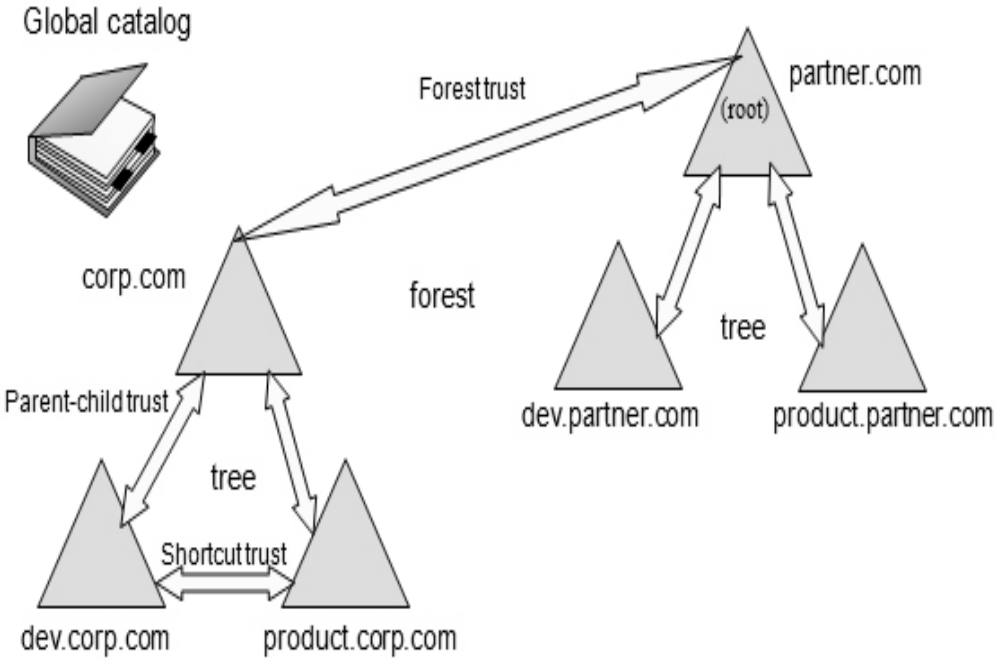


Отношения на доверие

- Ако не са конфигурирани отношения на доверие, домейнът е ограничен при достъпа до ресурси единствено в рамките на организацията.
- Отношенията на доверие са необходими за достъп до ресурси извън собствения домейн.
- Доверието е връзка за автентициране между два домейна, чрез която принципалите могат да бъдат оторизирани за достъп до ресурси в други домейни.

Видове доверие

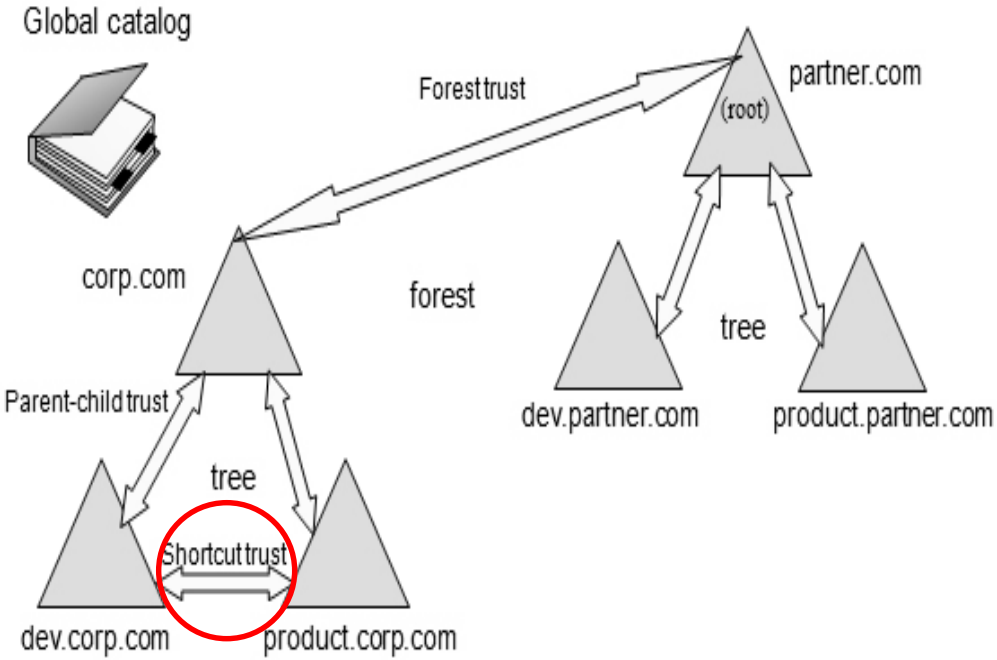
- **Transitive Two-Way**. Всички домейни в гората поддържат транзитивно двупосочно отношение на доверие с всеки друг домейн в гората:



Ако има доверие между *dev.partner.com* и *partner.com* и между *product.partner.com* и *partner.com*, то съществува отношение на доверие между *dev.partner.com* и *product.partner.com* .

Видове доверие

- **Shortcut trusts**. Този тип доверие се създава между домейни, които не са в наследствена връзка. Прилагат се в случаите, когато често се осъществява достъп до ресурси между домейни, които са отдалечено свързани в дървото или гората.

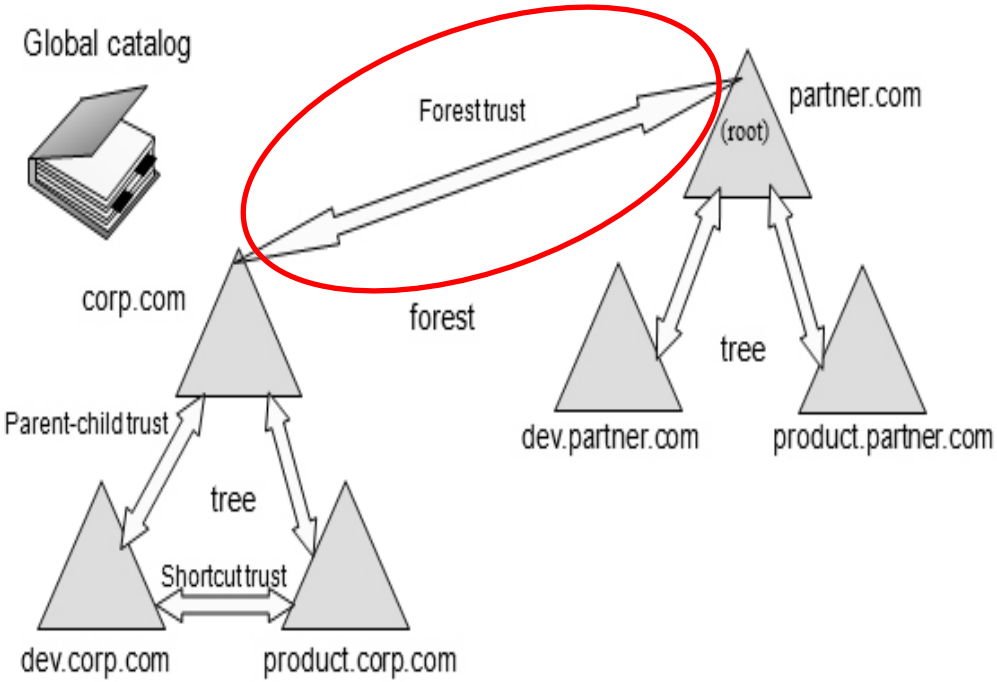


Отношенията на доверие от този тип не са транзитивни.

Видове доверие

- **Forest trust**. Това е двупосочно транзитивно отношение на доверие между две отделни гори.

Тези отношения не са транзитивни към други гори.



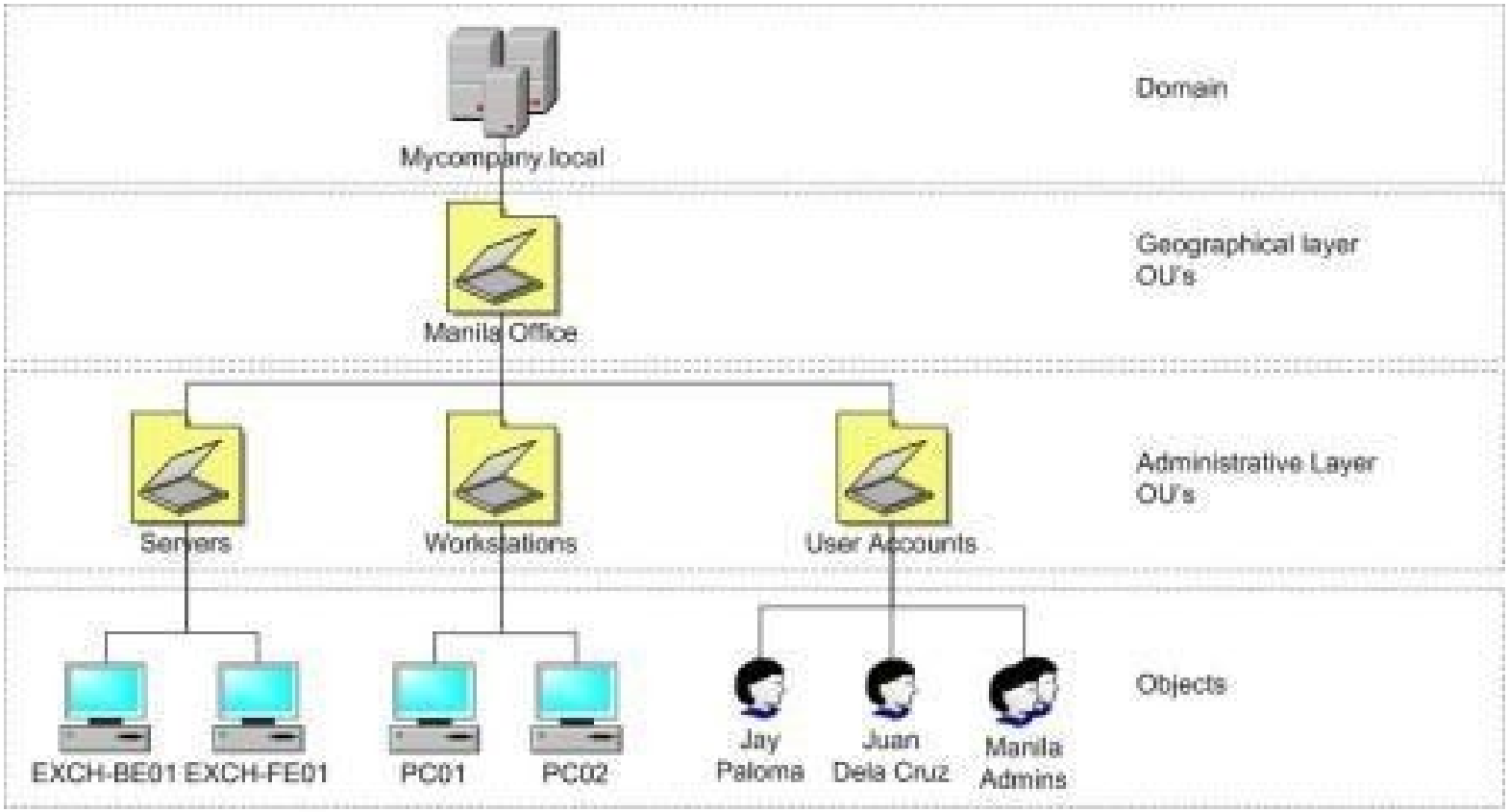
Глобален каталог

- Представлява подмножество на всички домейни в гората.
- ГК съдържа списък на всички домейни в гората и списък на всички обекти в тези домейни, но само подмножество на атрибутите за всеки обект.
- Редуцирането на обема информация по този начин позволява бързо откриване на коректния домейн за потребителя, което от своя страна ускорява процеса на автентикация.
- ГК съдържа и името на всяка глобална група за всеки домейн и името и пълния списък на членове на всяка универсална група в гората.

AD схема

- Дефиниция на атрибути и класове, които могат да се създават в гора.
- Включва множество от правила, определящи типа и формата на данните.
- Дефинира два типа компоненти:
  - Обекти – единица за съхраняване на данни.
  - Атрибути – описание на обект. Може да се дефинира отделно от обект.

Organizational units



AD и DNS

- AD е тясно свързана с DNS.
- Имена на домейни в AD са DNS имена.
- Зоновите файлове на DNS могат да се съхраняват в AD.
- За откриване на домейн контролерите се използва специален ресурсен запис в DNS – SRV.

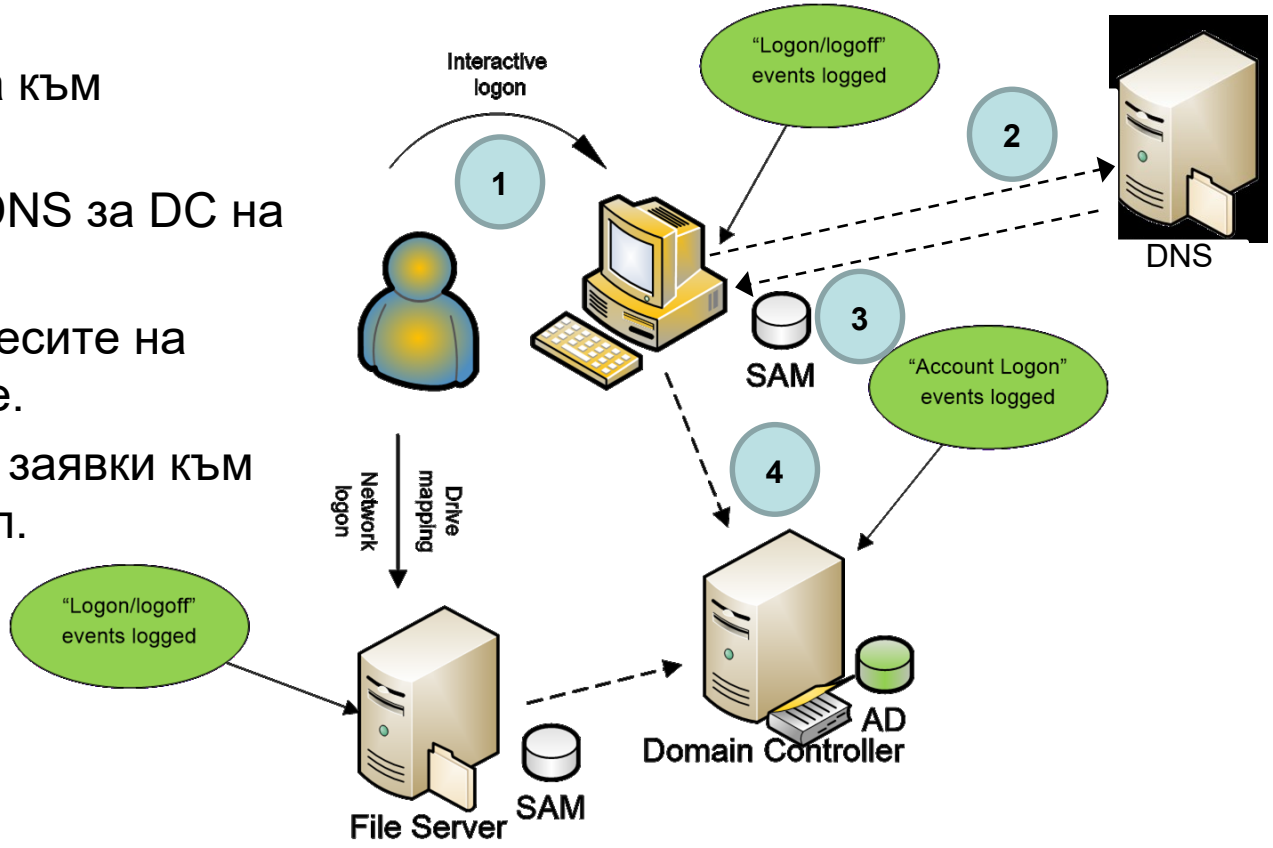
_ldap._tcp.Corp.com. 600 IN SVR 0 100 389 DC.Corp.com

Ресурсен запис SRV

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. 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

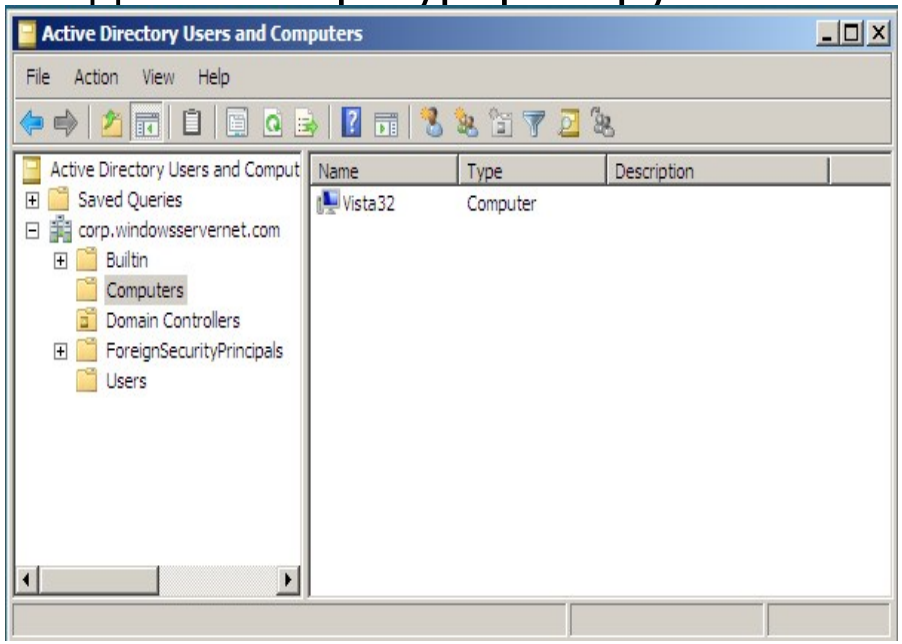
Процес на логване на потребител в домейн

1. Изпраща се заявка към *netlogon* процеса.
2. Netlogon запитва DNS за DC на изисквания домейн.
3. DNS връща IP адресите на домейн контролерите.
4. Клиентът изпраща заявки към DC по LDAP протокол.



Управление на потребители и групи

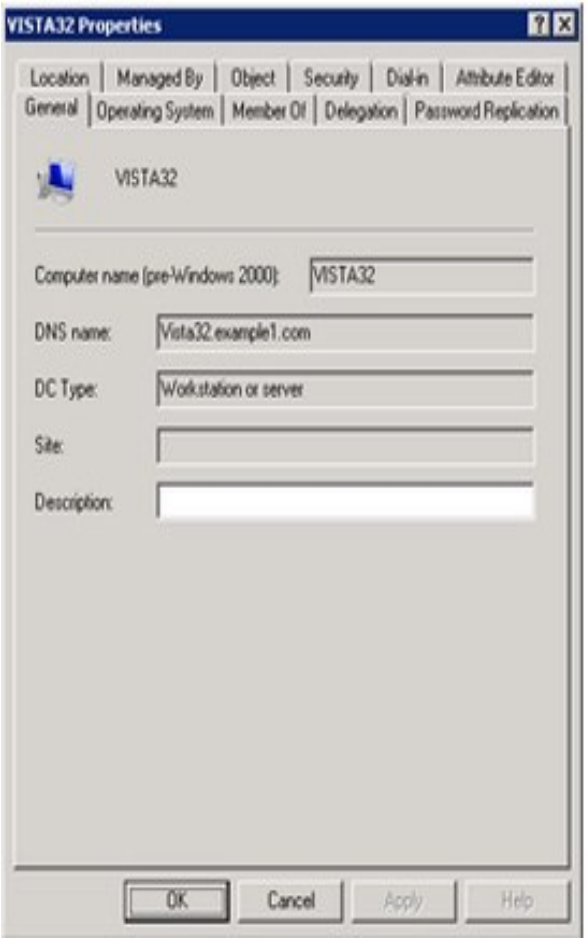
- **Active Directory Users and Computers (ADUC).**
- Позволява да се създават, променят и изтриват потребителски акаунти; да се менажират групи и техните членове и да се конфигурират групови политики.

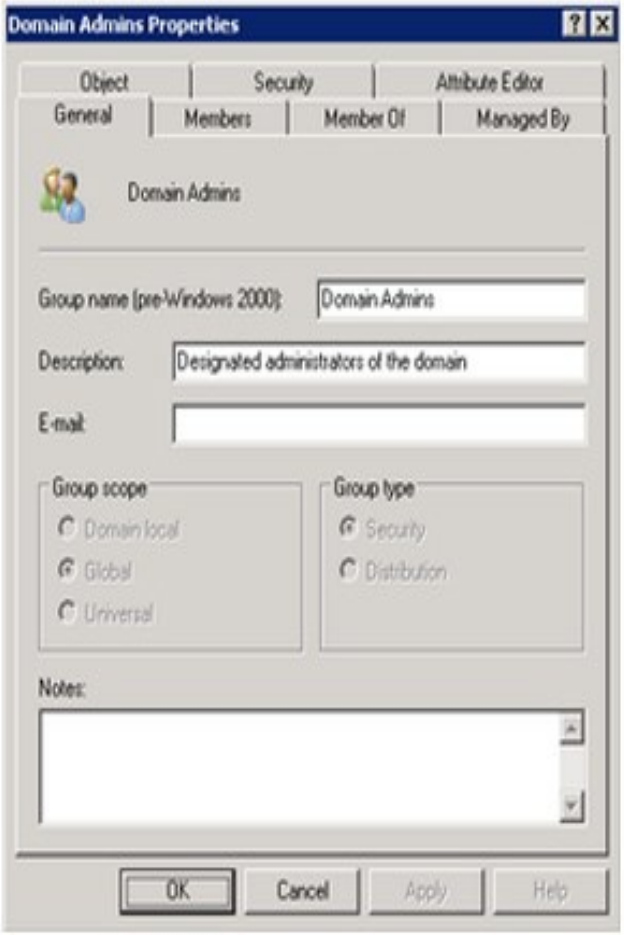


Обекти

- **Обект компютър** - Обектът компютър описва компютри, които имат определени права в мрежата – домейн контролери, сървъри или работни станции. Домейн контролерите са в отделен контейнер Domain Controlers, докато сървърите и работните станции – в Computers.
- **Обект група** - Съществуват два основни типа групови обекти. Първият е *security*. Той позволява управление на правата на достъп за множество обекти. Вторият е *distribution*. Използва се за групово изпращане на е-мейли.
- **Обект потребител** - Представя актуалните потребители в системата.

Атрибути на обекти





Създаване на потребители и групи

Изисквания към имената:

- Имената трябва да са уникални в домейна (за потребител в домейн) или в машината (за локален потребител)
- Да имат максимално 20 символа
- Да не съдържат следните символи: „ / \ [ ] : ; | = , + * ? < >
- Да не съдържат само празни позиции или само точки

Използване на LDAP за създаване на потребители

- LDAP (Lightweight Directory Access Protocol) е основен протокол за достъп и модифициране на съдържанието на AD DS.
- Администраторът може да използва команди, базирани на този протокол, чрез които да се автоматизира процеса на създаване на потребители и групи.
- Всеки обект се представя чрез специален LDAP идентификатор (Distinguished Name).

Използване на LDAP за създаване на потребители

<u>Пример:</u>

Потребител *Fred Flintstone*, който да бъде в контейнер *BRusers* в домейна *bedrock.local*.

LDAP име:

cn=“Fred Flintstone”, cn=BRusers, dc=bedrock, dc=local

Използване на LDAP за създаване на потребители

<u>Пример 2:</u>

Потребител *Barney Rubble* от контейнера *Tech*, съдържащ се в контейнера *Cave* на домейна *enterprise.com.*

LDAP име:

cn=”Barney Rubble”, cn=Tech, cn=Cave, dc=enterprise, dc=com

Потребителско име на принципал

User Principal Name (UPN) - в контекста на LDAP се използва за идентифициране на потребител в директорията.

Ако потребителското име е *fflinstone*, то UPN е:

fflintstone@bedrock.local

Администриране чрез команди

Задаването на атрибути в LDAP може да се направи посредством командата **dsadd**. Това позволява използването на скриптове за автоматизиране на създаването и менажирането на потребителски акаунти, групи, OU и др.

Добавяне на компютър

Нека има компютър с име *JH-WXP-DSK*, който да бъде добавен към OU *Admin*, и се автентицира като домейн администраторки акаунт:

dsadd computer CN=JH-WSP-DSK, OU=Admin,
DC=bedrock, DC=local –u administrator –p

Опцията **–p** ще изведе съобщение за въвеждане на парола.

Добавяне на потребител

Нека се добави потребител *brubble* (Barney Rubble) с е-мейл адрес *brubble@enterprise.com* с начална парола „*changeme*” към OU *Tech*, който да бъде член на групата *Caveman*:

dsadd user cn=brubble, ou=tech, dc=enterprise, dc=com
–upn brubble@enterprise.com –fn Barney –ln Rubble
–display “Barney Rubble”–password changeme
–email brubble@enterprise.com
-memberof cn=caveman, ou=tech, dc=enterprise, dc=com

Добавяне на OU

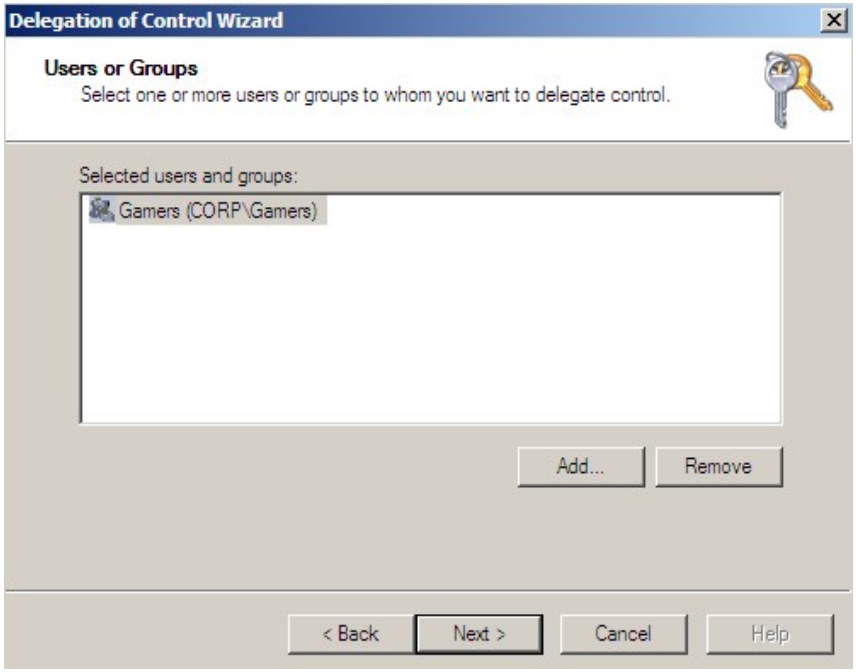
Нека се добави OU с име *Support* към домейна *bedrock.local*:

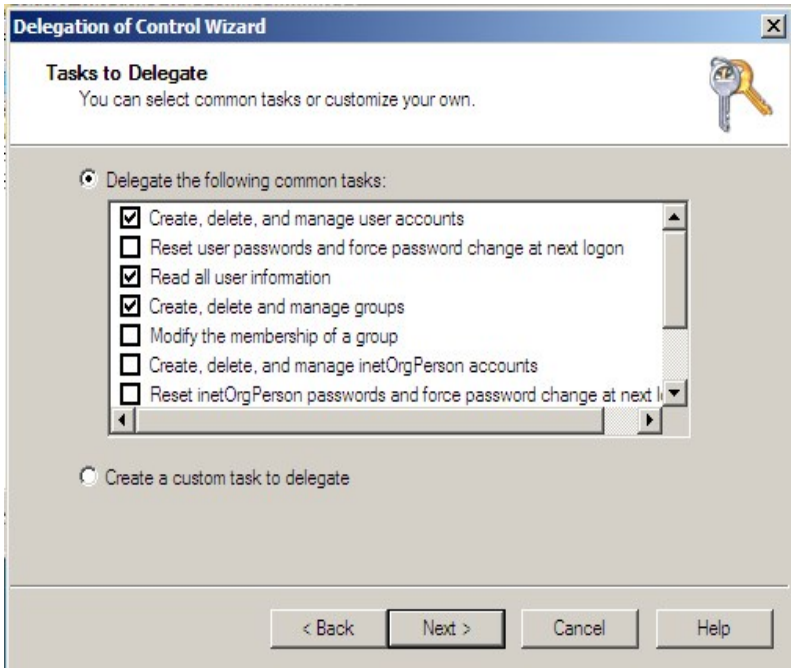
dsadd ou cn=support, dc=bedrock, dc=local

Делегиране на права

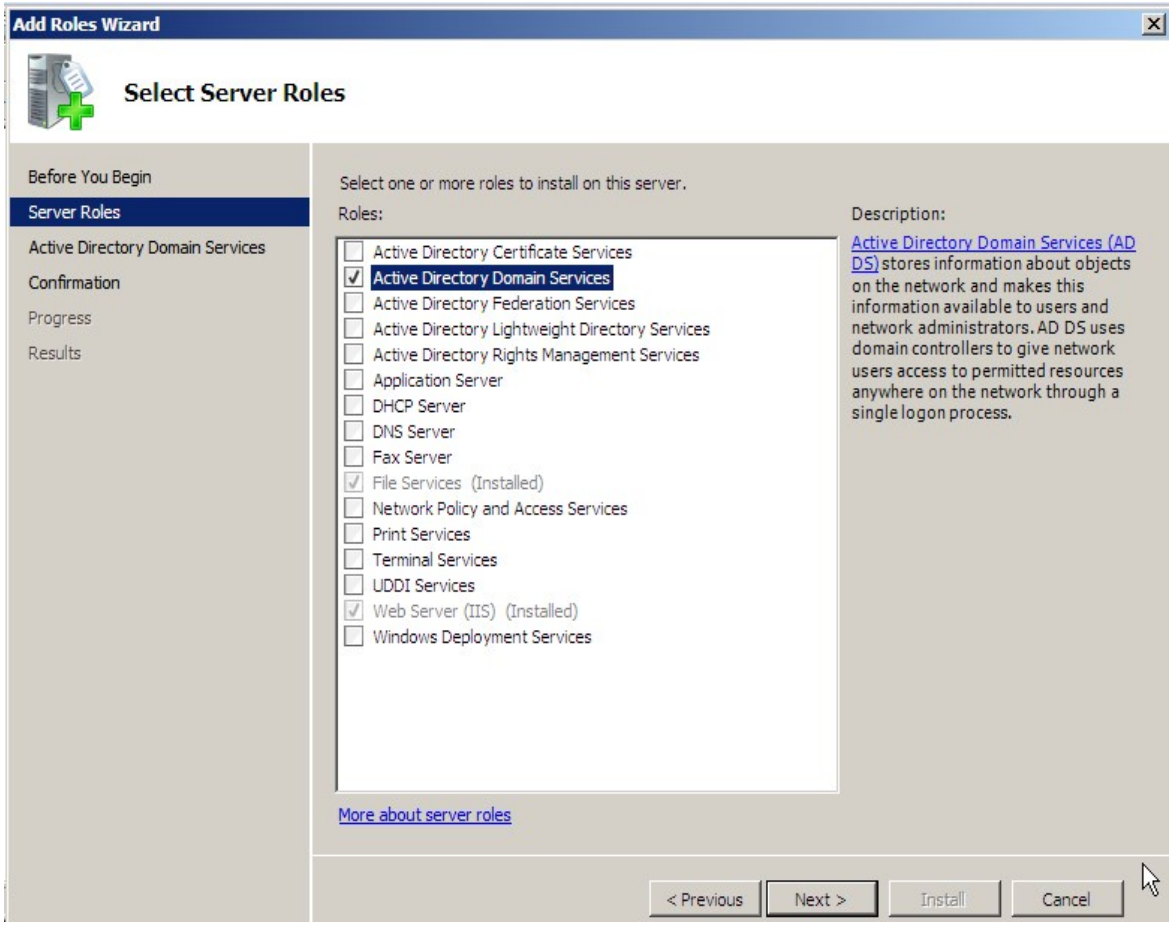
- Една от новите функционалности на AD DS е възможността да се дават на други потребители частични административни права за контрол на подмножество на директорията – процес. Например, могат да се дадат права на определен служител в организацията да ресетира паролите на другите служители. Процесът на делегиране се улеснява от помощник.

Делегиране на права





Инсталиране на роля Active Directory Domain Services



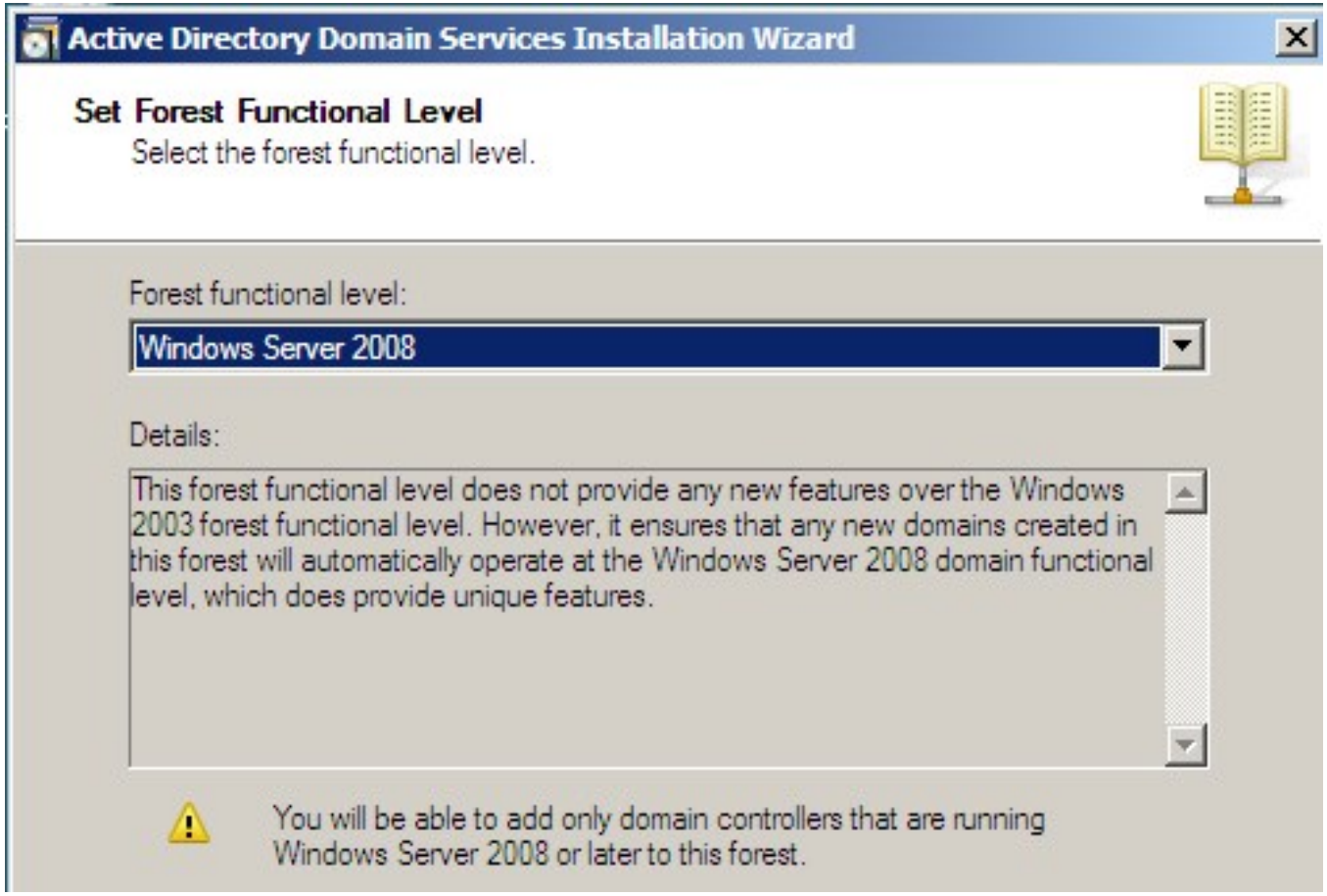
Инсталиране на възможности на ролята

Конфигуриране на DC

Първият домейн в AD DS има специално значение. Първо, процесът на инсталиране на нов домейн автоматично добавя първия домейн контролер в този домейн. Второ, този нов домейн става корен на цялата гора, което означава, че той има специално предназначение по отношение на останалите домейни в нея.

За стартиране на този процес, на машината, която ще бъде първия домейн контролер, се стартира системната програма **Start -> Run-> dcpromo.exe**. Стартира се помощник за инсталиране, който напътства целия процес.

Ниво на съвместимост



Ниво на съвместимост

- **Windows 2000 forest functional level**. Този режим поддържа всички типове домейн контролери (NT, 2000, 2003, 2008), като поддържа само 5000 члена в индивидуална група.
- **Windows Server 2003 forest functional level**. Поддържа NT и 2000 домейн контролери, но дава възможност за по ефикасна репликация на AD и транзитивно доверие между гори.
- **Windows Server 2008 forest functional level**. Този режим не добавя нови особености в сравнение с предния, но позволява новите домейни в гората да оперират в ниво Windows Server 2008, което от своя страна притежава нови функционалности.

Въпроси?