Европейски съюз

ОПАК. Експерти в действие

Европейски социален фонд
Инвестиции в хората

Проект „Повишаване квалификацията на служителите от администрацията на централно ниво чрез усъвършенстване на знанията и практическите им умения за управление на софтуерни ИТ проекти в съответствие със съвременните методологии“, осъществяван с финансовата подкрепа на Оперативна програма „Административен капацитет” (ОПАК), съфинансирана от Европейския съюз, чрез Европейския социален фонд”, съгласно Договор № К13-22-1/05.03.2014 г.

НАРЪЧНИК

Дейност 6.

ОБУЧЕНИЕ ЗА СИСТЕМНИ АДМИНИСТРАТОРИ ЗА 58 СЛУЖИТЕЛИ НА ЦЕНТРАЛНАТА АДМИНИСТРАЦИЯ И ИЗДАВАНЕ НА СЕРТИФИКАТИ ЗА ПРОВЕДЕНОТО ОБУЧЕНИЕ

Изготвен в изпълнение на Договор № Д-37/11.12.2014 г.

между

МИНИСТЕРСТВО НА ТРАНСПОРТА, ИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ И СЪОБЩЕНИЯТА

и

„КОНСОРЦИУМ ИТ ОБУЧЕНИЯ 2015“ДЗЗД

New Horizons Computer Learning Centers

ciela

„КОНСОРЦИУМ ИТ ОБУЧЕНИЯ 2015“ ДЗЗД

София 1040, ж.к. Изток, бул. Драган Цанков 36, СТЦ Интерпред, блок А, ет.6; тел: 024210040; имейл: ittraining2015@newhorizons.bg;

Авторски колектив:

Александър Стефанов

Одобрил: Николай Пенев – ръководител на проекта

София, 2015 г.

Съдържание

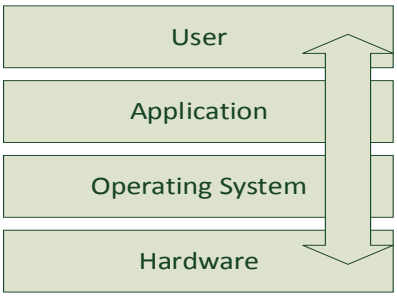
Въведение

Този наръчник е част от учебните материали по системно администриране за служители на централната администрация. Той има за цел да подпомогне обучителя и обучавания при подготовката му по системно администриране.
Наръчникът няма за цел да бъде книга по системно администриране, а в структуриран вид в допълнение на проведения обучителен курс да даде препратки към места в глобалната мрежа, където да получите по-задълбочени познания.
За по-задълбочени знания също така се препоръчват ръководствата на съответните производители.
Наръчникът се ползва както от обучаемите, така и от обучителите.

В наръчника се прави въведение в операционните системи и последователно надграждане на уменията за инсталиране, диагностика и поддръжка на операционните системи. Разгледани са и основните понятия в концепцията за облачните услуги.

Част I: Операционни системи.

1: Въведение в операционни системи (ОС):



Операционната система е софтуер, който управлява компютърния хардуер, софтуерните ресурси и осигурява среда за работа на компютърните програми (софтуерни приложения). Моделът на компютърна архитектура показва мястото на операционната система в него. Операционната система е компонентът, който осигурява връзката между потребителските действия и приложенията, и хардуерните компоненти, които трябва да изпълнят поставените от приложенията задачи.

Основните функции на операционните системи са:

- Управление на паметта – операционната система управлява оперативната памет, като заделя необходимата памет за всеки процес.
- Управление на процесора – операционната система управлява подаването на заявки към процесора. Тя синхронизира взаимодействието между процесор, памет, шина и входно-изходните устройства.
- Управление на прикачените устройства – всички прикачени устройства са изцяло под контрола на операционната система.
- Управление на файловата структура
- Контрол върху производителността на системата

- Контрол върху сигурността на системата
- Откриване и реакция при грешки
- Координация между потребители и софтуер
- Одит на събития

Типове операционни системи според принципа на работа:

- Batch operating systems - при този тип системи потребителят няма пряко взаимодействие с компютъра директно. Всеки потребител подготвя своята задача на off-line устройство и я предава на оператор, който сортира подобните задачи и ги подава към компютъра за изпълнение. Недостатъци: липса на взаимодействие между потребителя и изпълняваната от системата задача; процесорът често работи напразно (idle) тъй като механичните устройства са в пъти по-бавни от него; липса на приоритет при отделните задачи.
- Time-sharing operating systems - при този тип операционни системи множество задачи се изпълняват от процесора чрез превключване между тях, като всяка задача получава навременно изпълнение в реално време.
- Distributed operating System – този тип системи ползват множество разпределени процесори, за да обслужват множество потребители и приложения в реално време. Процесорите комуникират по между си чрез мрежа от високоскоростни комуникационни линии.
- Network operating Systems – те работят на специализиране сървъри, като основната им цел е предоставянето на достъп до споделени ресурси (file and print services) от множество потребители едновременно.
- Real Time operating Systems – системи, при които времето за отговор (времето за изпълнение на дадена задача) е оптимизирано и трябва да съответства на предварително зададен времеви интервал. Такъв тип операционни системи управляват индустриални контролни системи, оръжейни системи, роботи, системи за контрол на въздушния трафик и др.

Типове операционни системи според броя едновременно изпълнявани задачи:

- Single-tasking operating systems – операционни системи, при които само една единствена програма се изпълнява в даден момент.
- Multi-tasking operating systems - тип операционни системи, които дават възможност няколко програми да бъдат изпълнявани едновременно чрез превключване между тях. Те за известни още като Time-Sharing Operating Systems. Multi-tasking системите биват:

- pre-emptive – операционната система разпределя процесорното време на слотове (равни интервали), като заделя по един слот на всяка работеща програма.
- co-operative – операционната система разчита, че всеки ползващ ресурси процес ще даде време за достъп до компютърните ресурси и на останалите процеси.

- Multi-user systems – тип операционни системи, които позволяват няколко потребителя да достъпват компютърната система едновременно.

Типове операционни системи според броя процесори:

- Uniprocessor – single CPU
- Multiprocessor - multiple CPU, shared memory
- Distributed system – multiple CPU, no shared memory

Компоненти на операционните системи:

- Kernel (Ядро на операционната система) – осигурява базовото ниво на контрол върху всички хардуерни компоненти. Ядрото на операционната система е съвкупност от файлове и библиотеки, които управляват достъпа на приложенията до хардуера, например достъпа на отделните програми до оперативната памет.
- Execution Services – услуги, които способстват за изпълнението на отделните програми. Процесът по изпълнение на дадена програма извиква създаването на конкретен процес от ядрото на операционната система, което от своя страна заделя памет за конкретния процес и му дава достъп до компютърните ресурси.
- Процес- всяка програма, която е заредена в паметта, се изпълнява под формата на процес.
- Thread (нишка) – набор от инструкции и данни, които трябва да бъдат обработени от процесора. Когато даден процес иска да изпрати инструкции към процесора за обработка, този процес генерира нишка. Всяка програма, която е способна да изпълнява няколко различни задачи по едно и също време (визуализация на информация на дисплея; принтиране; взаимодействие с други програми), има възможността са генерира няколко различни потока от заявки (нишки) към процесора едновременно. Такъв тип програми (приложения) се наричат multithreaded приложения. Процесните нишки са начин да се подобри ефективността и бързодействието на дадена система чрез паралелизъм.
- Shell (обвивка) – командният интерпретатор, който изпълнява въведените от потребителя команди. Shell-а превежда разбираемите за потребителя

команди във формат, разбираем за компютърния хардуер. Понякога командният интерпретатор (shell) е част от ядрото на операционната система.

- Device drivers (драйвъри на устройства) – компютърен софтуер, позволяващ комуникацията и взаимодействието с даден хардуерен компонент.
- File system (файлова система) – осигурява подредбата, организацията и достъпа до информацията в информационните масиви (хард дискове, DVD-ROM, flash memory).
    - User Interface (потребителски интерфейс) – това е работната среда на потребителя, в която всяко негово действие се трансформира в команди към операционната система. Потребителският интерфейс може да бъде:
        - Graphical User Interface (GUI) – графична среда под формата на прозорци, графики и икони.
        - Command-Line Interface (CLI) – среда, където потребителя задава инструкции към операционната система под формата на команди.

Компоненти на операционните системи на база предлаганите услуги:

- Process Management – създаване, управление, синхронизация и прекратяване на процеси.
- Memory Management – управление на паметта; заделяне на памет за конкретен процес.
- I/O Device Management – управление на входно-изходните устройства и целият хардуер.
- File System – система за управление достъпа до дисковите устройства; създаване, прочитане, изтриване на файлове.
- Protection services – услуги, които управляват нивото на сигурност и реакцията при отделни събития.
- Network Management – управление на мрежовата комуникация.
- User Interface – средата, в която работи потребителя.

Файловите системи са неразделна част от всяка една операционна система. Файловите системи реализират следните функции:

- Позволяват на потребителя и софтуерните приложения да организират файловете в стройна директорийна структура
- Управляват процесите по създаване, прочитане, модификация и изтриване на файлове от даден информационен масив

- Управляват методите за достъп до дисковите масиви и сигурността на информацията в тях
- Комуникират с драйвърите на дисковите устройства
- Организират логическото разполагане на информацията по дисковите устройства, като данните се записват в т.н. клъстери (clusters), като един клъстер може да заема няколко физически сектора от дисковото устройство.

Организация на файловите системи (основни компоненти):

- Файл – най-малкият ресурс за съхраняване на информация върху даден информационен носител. Всеки файл има уникално име в рамките на дадена директория.
- Директория – контейнер, в който се съхраняват файловете; директорията е метод за организация на файловете.
- Метаданни – данни относно данните; например: информация за името, типа, големината на файла, както и типа на неговото разширение.
- Секюрити дескриптор – зона към файла, която отразява опциите, свързани със сигурността на този файл, например: NTFS permissions, indexing, compression, encryption.

Най-разпространените файлови системи днес са:

- File Allocation Table (FAT) файлова система – система за организация и достъп до информацията под формата на файлове. Съществуват три основни варианта на FAT файлова система:
  - FAT 12 – ползва 12 битова организация на таблицата за локация на файловете (FAT).
  - FAT 16 - ползва 16 битова организация на таблицата за локация на файловете (FAT).
  - FAT 32 - ползва 32 битова организация на таблицата за локация на файловете (FAT).

File Allocation Table (Таблица за локация на файловете) е последователен брой сектори, които отразяват лист със записи, като всеки запис дава информация за конкретен файл и неговото място в структурата на файловата система.

Информация относно FAT файловата система може да намерите на адрес: http://en.wikipedia.org/wiki/Design_of_the_FAT_file_system#FAT16

Информация относно сравнението между FAT16 и FAT32 файлови системи може да намерите на адрес: http://technet.microsoft.com/en-us/library/cc940351.aspx

- NT File System (NTFS): създадена от Microsoft, NTFS ползва Master File Table (MFT) и има максимален размер на дяла $2^{64}-1$ клъстера. Максималния размер на клъстера при NTFS файлова система е 64 kB. Основните функционалности на NTFS файловата система са:
  - Journaling – надеждно съхраняване на информацията с възможност за индексиране и улеснено търсене по ключови думи и атрибути.
  - Alternate data streams (ADS) – възможност за скриване на информация чрез ползването на алтернативни потоци за данни.
  - File compression – прозрачна за потребителя компресия и декомпресия на файлове.
  - Volume Shadow Copy – функционалност, позволяваща създаването на архивни копия (snapshots), отразяващи състоянието на даден файл към определен момент от време и връщане след време към тези архивни копия.
  - Encryption – криптиране на информацията на ниво файл или директория чрез ползване на Encrypting File System.
  - Quotas – възможност за ползване на дискови квоти, които ограничават потребителя при ползване на дисковото пространство.
  - Access Control Lists (ACL) – логически списъци, съдържащи секюрити идентификаторите на отделните потребители или групи от потребители, които могат да достъпват конкретен ресурс, както и техните права върху ресурса.
- Resilient File System (ReFS) – файлова система от нов тип, която се появява за първи път при Windows Server 2012 и основното ѝ предимство е устойчивост на откази. Тя е наследник на NTFS, като притежава редица новости, като:
  - Integrity – интегритета на данните е гарантиран чрез вградени механизми за проверка в реално време.
  - Availability – достъпността на информацията е гарантирана дори и при отказ на компютърната техника вследствие на отпадане на захранването.
  - Scalability – възможност за надграждане и работа с изключително големи обеми дискове.
  - Proactive Error Correction – следене за грешки в реално време и механизми за онлайн възстановяване.

Информация относно ReFS може да намерите на следният адрес: http://technet.microsoft.com/en-us/library/hh831724.aspx

Част II: Мрежова администрация.

1: Разбиране на мрежовата инфраструктура. Описание, терминология и избор на основните мрежови компоненти:

Стандартите в мрежовата инфраструктура се поддържат и развиват от IEEE – Institute of Electrical and Electronics Engineers – международна организация с нестопанска цел, която създава и внедрява норми и стандарти по отношение на комуникациите и технологиите, свързани с тях.

Най-широко използваните стандарти към момента са:

- IEEE 802.3 – стандарт за изграждане на компютърни мрежи, базирани на Ethernet технологии.
- IEEE 802.5 – Token ring мрежи, при които методът на достъп до средата се осъществява чрез т.н. маркер (token).
- IEEE 802.11 – Wireless локални мрежи, при които преносната среда е ефир (радио-вълни).
- IEEE 802.15 – Wireless PAN (personal area networks) мрежи, ползвани основно за комуникация между персонални устройства от типа PDA (Personal Digital Assistant). Пример за този стандарт са Bluetooth комуникациите.
- IEEE 802.16 – Broadband wireless мрежи. Тук се включват WiMAX технологиите.

Информация относно видовете мрежово стандарти и детайли относно тяхното внедряване може да бъде намерена на сайта на IEEE: http://www.ieee.org

Основни мрежови понятия и компоненти:

- Media (преносна среда) – средата, в която се осъществява комуникацията между отделните мрежови устройства.
- Data (данни) – потокът от данни по мрежата. Повече информация може да намерите на: http://www.unicode.org

- Node (възел, комуникационна точка, устройство) – всяко устройство, което има мрежови адаптер и може да комуникира.
- Client (клиент) – устройство или система, която ползва услугите, предлагани от т.н. сървъри.
- Server (сървър) - устройство или система, която предлага даден тип услуги в мрежата, например достъп до ресурси, място за съхранение на данни, централизирано принтиране, услуга за автоматично конфигуриране на мрежовите параметри на устройствата в дадена мрежа (DHCP server) и др.
- Peer (равнопоставен член на мрежата) – обикновено тези устройства или системи изпълняват ролята на клиенти и сървъри едновременно.
- Network adapter (NIC – network interface card) – мрежови адаптер (карта). Това в основният комуникационен компонент, чрез който се осъществява мрежовата комуникация. Всяко мрежово устройство притежава мрежов адаптер.
- Основни мрежови понятия и компоненти:
- Hub/switch/router – основни мрежови устройства.
- Bandwidth – това е параметър, който отразява капацитета или т.н. пропускливост на мрежовата среда. Измерва се в количество данни, преминали през комуникационната среда за единица време.
- Kilobits per second (Kbps)
- Megabits per second (Mbps)
- Gigabits per second (Gbps)
- Transport protocol – транспортният протокол е съвкупността от стандарти, правила, алгоритми, компоненти и методи, на база на които се осъществява комуникацията между отделните устройства в мрежата.

Мрежовата архитектура бива два типа според вида на преносната среда – жична и безжична:

Жична мрежова архитектура:

- Ethernet, Fast Ethernet, Gigabit Ethernet, PoE – Ethernet е основният и най-масово разпространен стандарт за мрежова комуникация. Като преносна среда се използват медни кабели от типа „усукана двойка“ или оптични влакна. Съществуват различни Ethernet стандарти, които поддържат различна скорост:
  - 10BASE-T - 10 Mbps
  - 100BASE-TX - 100 Mbps
  - 1000BASE-T - 1 Gbps (1000 Mbps)

- 10GBASE-T - 10 Gbps

- Token ring – мрежи, които имат кръгова топология и работят чрез употребата на маркер (token), който дава достъп до комуникационната среда на това устройство, което притежава маркера в момента.
- FDDI - (Fiber Distributed Data Interface) – маркер-базирана мрежова структура, която ползва оптични влакна за преносна среда.

Безжична мрежова архитектура – най-често ползваните технологии са:

- Wi-Fi;
- Infrared;
- Bluetooth;
- WiMax.

Компоненти на безжичната мрежа:

- Wi-Fi adapter (Безжичен мрежови адаптер) – адаптер, чрез който мрежовото устройство се свързва към безжичната мрежа.
- Access Point (Точка за достъп) – мрежово устройство, към което се свързват останалите клиенти на безжичната мрежа.
- SSID (Идентификатор на мрежата) – Service Set Identifier (SSID) е идентификаторът, който се излъчва от точката за достъп и който останалите безжични устройства прихващат с цел ориентиране.
- Infrastructure network (Инфраструктурна мрежа) – безжична мрежа, която осигурява централизиран входен портал за достъп на всички безжични мрежови клиенти.
- Ad-Hoc network (мрежа за директно свързване) – форма на свързване на безжични устройства, при която тези устройства се свързват директно по-между си без наличието на точка за достъп.

Протоколи и стандарти за безжичен достъп в разрешените за свободен достъп честотни ленти (Industrial, scientific and medical band - ISM):

- IEEE 802.11a: 54 Mbps in the 5.7 GHz ISM band
- IEEE 802.11b: 11 Mbps in the 2.4 GHz ISM band
- IEEE 802.11g: 54 Mbps in the 2.4 GHz ISM band
- IEEE 802.11n: 600 Mbps in the 2.4 GHz / 5 GHz GHz ISM band
- Infrared: 4 Mbps up to 3m
- Bluetooth: 24 Mbps up to 10m

Допълнителна информация за стандартите при безжичните мрежи може да бъде намерена на следните адреси:

- http://en.wikipedia.org/wiki/IEEE_802.11
- http://en.wikipedia.org/wiki/IEEE_802.11n-2009
- http://en.wikipedia.org/wiki/Infrared

Методи за контрол на достъпа до мрежовата среда – различаваме следните методи за контрол на достъпа до преносната среда:

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) – метод за контрол на достъпа до средата, който ползва принципа за откриване на колизии от отделните участници в мрежата. Всяко мрежово устройство, преди да изпрати пакет по мрежата, проверява (слуша) за сигнал, идващ от друг участник в мрежата. Ако такъв сигнал съществува към момента, то устройството изчаква определен интервал от време, преди да направи нов опит за предаване. Когато две устройства едновременно изпратят пакет по мрежата по едно и също време, се случва т.н. сблъсък (collision), който се регистрира от устройствата и те отново изчакват определен случаен интервал от време, преди да подновят процедурата по изпращане на пакети по мрежата.
- Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) - метод за контрол на достъпа до средата, подобен на CSMA/CD, при който всеки участник в мрежата предварително уведомява останалите чрез изпращането на специален уведомителен сигнал, наречен „advertisement". Всички мрежови устройства слушат непрекъснато за този сигнал и стартират предаването на своите данни едва тогава, когато не прихващат уведомителният сигнал.
- Token Passing – метод на предаване на данни, при който се ползва т.н. маркер (token), който дава право на притежателя на маркера да предава данни.
- Demand Priority - метод за контрол на предавателната среда, при който, за да може да предава данни по мрежата, всеки участник трябва да получи разрешителен сигнал от един централен концентратор, който управлява достъпа до предавателната среда.

Проблеми на физическата среда при безжични мрежи:

- attenuation – затихване на сигнала при отдалечаване от точката за достъп или при преминаването му през различни по плътност среди (вода, стени, стъкло). Всички прегради, които стоят на пътя на сигнала, абсорбират част от енергията му, което води до неговото отслабване и затихване.
- interference – интерференция – процес на отслабване или промяна на сигнала вследствие на наслагването му или под въздействието на други сигнали (вълни). Редица домакински и промишлени уреди могат да интерферират на безжичния сигнал, като по този начин го променят или отслабват.

Методи на защита на безжичните мрежи:

- криптиране – криптирането е най-надеждният метод за защита на данните, предавани по безжичен път.
- MAC филтриране – метод за ограничаване достъпа до дадена точка за достъп само от устройства с конкретни хардуерни адреси.
- скриване на SSID – метод за защита чрез спиране излъчването на идентификатора на безжичната мрежа.
- USB tokens – устройства, чието притежаване повишава автентикационните фактори на средата за достъп до безжичната мрежа.

Локални и глобални мрежи:

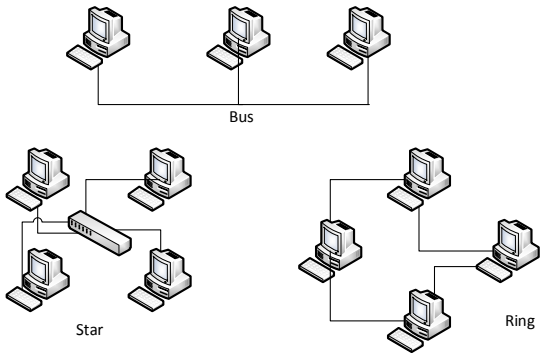
Локалната мрежа е най-разпространеният тип компютърна мрежа. Тя покрива конкретна физическа територия (етаж, офис, няколко сгради), като свързва по-между им всички мрежови устройства от тази територия. Основните компоненти на локалните мрежи са:

- Мрежови адаптер – част от мрежовото устройство, през която се осъществява мрежовата комуникация.
- Кабелна инфраструктура – тя включва всички видове кабели (медни, оптични), както и кабелни аксесоари, необходими за осъществяване на физическата свързаност между отделните устройства в даден мрежови сегмент.
- Hub (концентратор) – мрежови компонент, към който се включват всички останали устройства от дадена мрежа. Hub-а е сигнален повторител.
- Switch (превключвател) – мрежови компонент, подобен на концентратора, който работи на втори слой от седемслойният OSI модел и пренасочва пакетите на база MAC адреси.
- Termination point (терминираща точка) – точка, към която дадено устройство се закачва и така става част от локалната мрежа. Обикновено това са стенните или подови розетки.
- Wiring cabinet (апаратна станция/сървърно помещение) – това е помещение, в което се намира комуникационната техника.

Топология на локалните мрежи - Съществуват няколко типа мрежови топологии:

- Bus – топология, при която отделните мрежови устройства са свързани към един общ сегмент.

- Star - топология, при която отделните мрежови устройства са звездовидно свързани към hub или switch.
- Ring – топология, свързваща устройствата помежду им в кръг.
- Mesh – топология, която е смесица от всички останали топологии.
- Hybrid – този тип мрежова топология е комбинация от Bus и Star топологиите.



Комуникациите между отделни устройства в локална мрежа най-често се осъществяват на база Ethernet технологии. За да може да изпраща и приема пакети с данни, всяко мрежово устройство има т.н. хардуерен адрес, известен като Media Access Control (MAC) адрес. Този адрес е 48 битов, като е уникален в световен мащаб и това дава възможност на всеки две случайно избрани мрежови устройства, били те и от един и същ производител, да могат да комуникират успешно. Всеки генериран пакет в локалната мрежа притежава source и destination MAC адрес, което осигурява неговото успешно транспортиране по мрежата.

За повече информация: http://en.wikipedia.org/wiki/Ethernet_frame

Глобална мрежа - глобалната мрежа, наречена Wide Area Network, или WAN, е географски разпределена мрежа, която се състои от множество локални мрежи, обединени в една голяма мрежа. WAN мрежите могат да свързват както отделните LAN сегменти на територията на дадена компания (офис, отделни етажи или структурни звена, обособени като отделни мрежи), така и главният офис със отдалечени офис-клонове. Комуникационните линии, свързващи отделните доставчици на услуги (като интернет доставчици и др.), също се наричат WAN линии и те оформят една глобална мрежа.

Характеристики на глобалните мрежи:

- Скорост: глобалните мрежи са характерни с по-малка скорост в сравнение с локалните. LAN Ethernet мрежите поддържат до 10 Gbps, докато WAN линиите максимум до 150 Mbps.
- Латентност – при глобалните мрежи, забавянето по мрежата е по-голямо, което е обусловено от по-бавната скорост на линиите.
- Цена – глобалните комуникационни линии, които оформят глобалните мрежи, обикновено са скъпи и ненадеждни.

Физически компоненти на Глобалната мрежа:

- Bridge - наречен още „мост“, bridge-а обикновено свързва два отделни LAN сегмента, като препраща мрежовият трафик на базата на MAC адреси. Bridge-а може да бъде наречен още двупортов превключвател (switch), тъй като той препраща пакетите с данни от единият LAN сегмент към другият, вързан към него. Bridge-а подобно на switch-а, взема решение за препращането на даден пакет въз основа на т.н. mac-таблица (MAC Table).
- Router - Рутер (маршрутизатор). Рутерът е възлово мрежово устройство, което свързва различни типове мрежови сегменти и работи на трети слой (Мрежови слой) от седемслойният OSI модел. Рутерите поддържат различни протоколи за маршрутизиране и препращат мрежовите пакети на база на Internet Protocol (IP) информация.
- Leased line - Наета линия: наетата линия е комуникационен канал, който обикновено е собственост на телекомуникационна компания или държавна институция. Наетата линия се отдава под наем срещу такса за даден период на ползване и има определен капацитет.
- Backbone - Основен (гръбначен) високо-капацитетен комуникационен канал, който свързва няколко локални мрежи и осигурява надеждност и висока скорост на предаването на данни.

Съществуват различни методи на пакетиране на данните при глобалните мрежи. На база на тези методи и алгоритми са създадени редица общоприети OSI layer 2 протоколи и стандарти за свързване на локални мрежови сегменти. Най- широко използваните са:

- High-Level Data Link Control (HDLC) - За повече информация: http://en.wikipedia.org/wiki/High-Level_Data_Link_Control
- Point-to-Point Protocol (PPP) - За повече информация: http://en.wikipedia.org/wiki/Point-to-Point_Protocol
- X.25 - За повече информация: http://en.wikipedia.org/wiki/X.25
- Frame Relay - За повече информация: http://en.wikipedia.org/wiki/Frame_Relay

- Asynchronous Transfer Mode (ATM) - За повече информация: http://en.wikipedia.org/wiki/Asynchronous_Transfer_Mode
- Digital Subscriber Line (DSL) - За повече информация: http://en.wikipedia.org/wiki/Digital_subscriber_line
- Integrated Services Digital Network (ISDN) - Цифровите мрежи за интегрирани услуги са цифрови линии, които ползват съществуващите обществени телефонни линии за предаване на глас и данни. ISDN ползва 64 Kbps канали за пренос на информация като съществуват два типа ISDN архитектура:

  - Basic Rate Interface (BRI) – ползва два канала по 64 Kbps и пренася до 128 Kbps.

  - Primary Rate Interface (PRI) - ползва 32 канала по 64 Kbps и пренася до 1,536 Mbps.

  За повече информация относно ISDN може да ползвате следния линк: http://en.wikipedia.org/wiki/Integrated_Services_Digital_Network
- T-Carrier – стандартен метод за пакетиране на данни, които се използва предимно в Северна Америка. За повече информация относно T-Carrier стандарта: http://en.wikipedia.org/wiki/T-carrier
- E-Carrier – стандартен метод за пакетиране на данни, които се използва предимно в Европа. За повече информация относно E-Carrier стандарта: http://en.wikipedia.org/wiki/E-carrier

Свързване към Интернет: Определение на понятието Интернет:

Интернет е съвкупността от взаимосвързани мрежи, които покриват територията на земното кълбо в глобален мащаб. Интернет пространството е разпределено и достъпа до него се осъществява чрез свързване към мрежата на така наречените Интернет Доставчици (Internet Service Providers - ISP).

Определение на понятието Интранет:

- група от услуги, хоствани локално в мрежата
- частна структура
- услуги, базирани на принципите и технологиите на Интернет

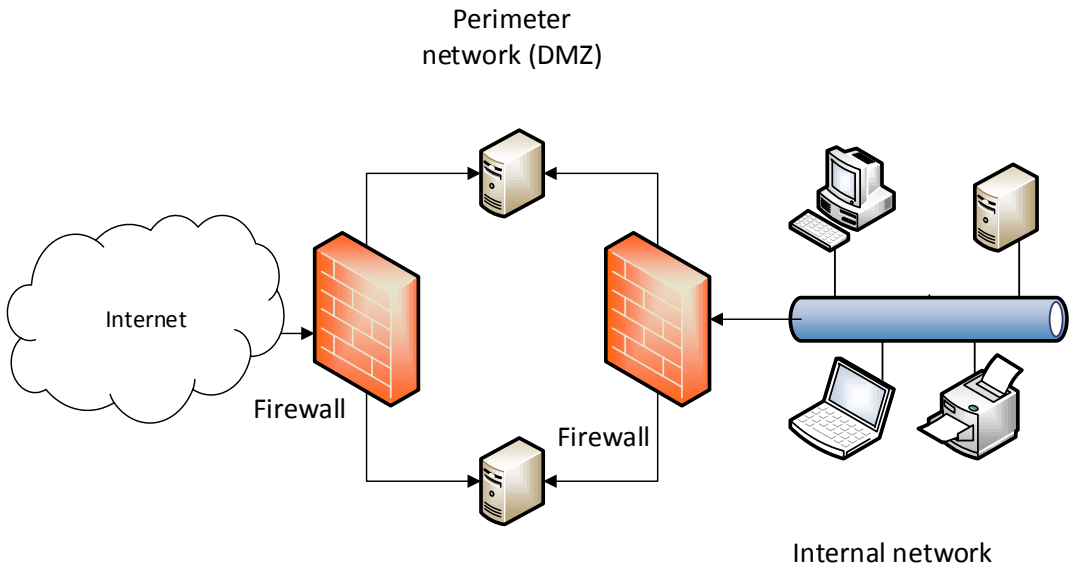
Определение на понятието Екстранет:

- предлага услуги, близки до Интранет
- част от вътрешната мрежа, която е достъпна за бизнес партньори от Интернет
- изисква допълнителни мерки и технологии за сигурност

Определение на понятието Firewall (Защитна стена) – защитната стена се използва като преграда между вътрешната за дадена организация мрежа и околният свят. Тя е съвкупност от хардуерни устройства, технологични решения и софтуерни компоненти, чиято цел е да пазят информационните активи и ресурси на дадена компания от неоторизиран външен достъп.

Firewall решенията могат да бъдат:

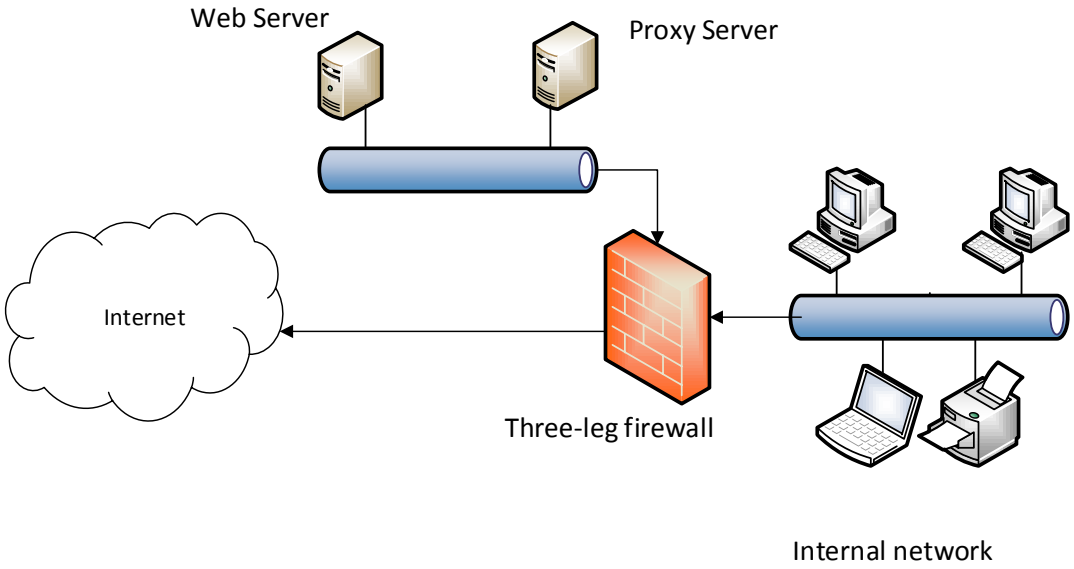
- хардуерни – ползват се специализирани хардуерни устройства, които поддържат сложна вътрешна логика за блокиране на достъпа до определени ресурси и услуги.
- софтуерни – представляват специализиран софтуер, който се инсталира върху сървърите и работните станции в мрежата.



Определение на понятието Proxy server (сървър-посредник) – proxy сървъра играе ролята на посредник между вътрешната за дадена организация мрежа и външното Интернет пространство. Той може да бъде:

- специално посветена за тази цел хардуерна конфигурация с инсталиран специфичен софтуер.
- firewall устройство с proxy функционалност.
- Съществуват два типа proxy сървъри:

- Proxy server (нормален, прав прокси сървър) – целта му е да филтрира достъпа на вътрешните клиенти до външни ресурси, и да кешира локално информация.
- Reverse proxy server (обратен прокси сървър) – пренасочва външни заявки към публикувани вътрешни ресурси и може да осъществява балансиране на товара и трафика.



Методи за отдалечен достъп до ресурси - понятието „отдалечен достъп“ включва всякакви форми на дистанционно достъпване на ресурси. Тук влизат следните категории:

- Достъп до ресурси в главният офис от компютри в отдалечен офис.
- Връзка между офиси, които се намират на големи разстояния един от друг или са географски разпределени.
- Форми на дистанционна работа, или т.н. Telecommuting (teleworking).
- VPN (виртуални частни мрежи) решения, които ползват като преносна среда незащитеното Интернет пространство.

Методите за отдалечен достъп до информация се базират на следните два модела:

- **AAA** модел:
  - Authorization – оторизация – процесът на предоставяне на опознавателна информация (credentials) на дадена система за контрол на достъпа до ресурси.
  - Authentication – автентикация – процесът на проверка за правилност, вярност и валидност на опознавателната информация.
  - Accounting and Auditing – мониторинг, контрол и одит относно достъпа и ползването на даден ресурс.
- **CIA** модел:
  - Confidentiality – конфиденциалност – процес, чиято цел е подсигуряването срещу неоторизиран достъп до сензитивна информация. Основният метод за постигане на конфиденциалност е криптиране.
  - Integrity – интегритет на данните – осигуряване цялостност на данните. Проверката за интегритет ни гарантира, че данните са непроменени и че не са неправомерно манипулирани.
  - Availability – достъпност – за постигане на достъпност се ползват методи като: RAID масиви, Disaster Recovery Sites, Load Balancing, Clustering и др.

Протоколи за имплементиране на AAA и CIA моделите:

- **Kerberos –** автентикационен протокол, който е основният механизъм на автентикация в среда на Активна Директория. Повече информация може да намерите на: http://en.wikipedia.org/wiki/Kerberos_(protocol)
- **RADIUS - Remote Authentication Dial In User Service** - комуникационен протокол, който осигурява автентикация, оторизация и акаунтинг в среда на отдалечен достъп до ресурси. Повече информация може да намерите на: http://en.wikipedia.org/wiki/RADIUS
- **TACACS - Terminal Access Controller Access-Control System** - комуникационен протокол, който контролира отдалечена автентикация и свързани с нея услуги по отношение на достъпа до мрежови устройства и ресурси. Повече информация може да намерите на: http://en.wikipedia.org/wiki/TACACS

- **LDAP - Lightweight Directory Access Protocol** - протокол за достъп до директорийни услуги. Повече информация може да намерите на: http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

Virtual Private Network (VPN) – виртуалните частни мрежи са съвременно понятие за отдалечен достъп до ресурси чрез използването на защитени виртуални канали (тунели) през незащитеното Интернет пространство. Съществуват два типа VPN имплементации:

- VPN for remote access – за отдалечен достъп до вътрешно-фирмени ресурси от отдалечени потребители.
- Site to site VPN – за изграждане на защитен комуникационен канал между отдалечени офиси или партньорски компании.

Основните протоколи, които се ползват при VPN решенията, са:

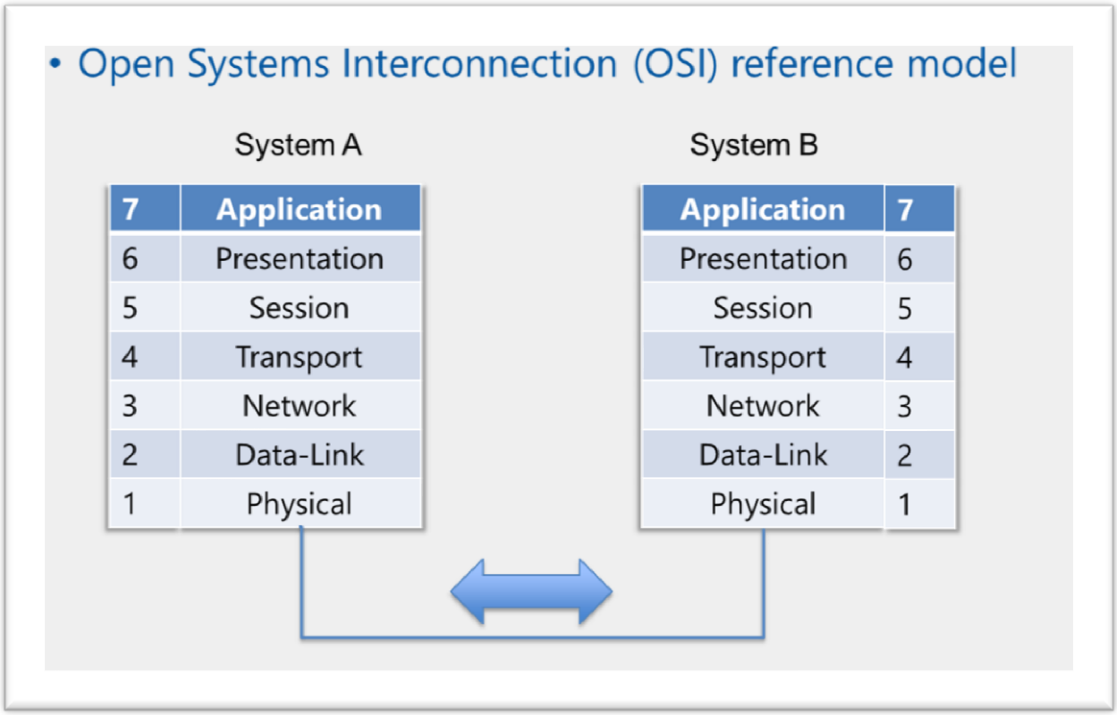
- Point-to-Point Tunneling Protocol (PPTP)
- Layer Two Tunneling Protocol (L2TP)
- Secure Socket Layer (SSL) tunneling protocol
- IP HTTPS
- IPsec

Други VPN решения:

- Direct Access – Microsoft решение за отдалечен достъп, което се нарича още “Always-On VPN”. Direct Access осигурява директна връзка на потребителите с ресурсите от тяхната корпоративна мрежа, независимо от местоположението на потребителя. Direct Access е метод за отдалечен достъп, който надеждно защитава мрежовия трафик и не изисква намеса от страна на потребителя.
- Network Access Protection (NAP) – протокол за контролиране достъпа до корпоративни ресурси от външни потребители на база т.н. „здравен статус“ на отдалечения потребителски компютър. Здравният статус на клиентския компютър се проверява на база health policy, което включва проверка на следните параметри:
  - инсталиран и обновен анти-вирусен софтуер.
  - пусната и конфигурирана защитна стена.
  - наличие на работещ софтуер за защита от зловреден код.
  - Windows Update настройки.

2: Свързване на мрежовите компоненти. Избор на мрежови устройства и технологии:

Open System Interconnection (OSI) мрежови модел: OSI модела е предложен от International Standard Organization (Международна Организация по Стандартизация) и е масово възприетият мрежови модел на комуникация. Той включва седем слоя, като всеки слой изпълнява определени функции и взаимодейства в останалите слоеве.



Характеристики на отделните слоеве в OSI модела:

- Physical layer (физически слой):
  - ✓ Управлява връзката с преносната среда
  - ✓ Управлява достъпа до средата
  - ✓ Предава данните под формата на електрически или оптични сигнали

- ✓ Интерпретира и конвертира сигналите в data-link frames
- ✓ Protocol data units (PDU) – формата на данните в конкретния слой се
- ✓ нарича Protocol data unit. PDU при физическия слой се нарича bits.

- Data-link layer (канален слой):
  - ✓ Управлява MAC адресната схема
  - ✓ Трансферира данните между устройствата
  - ✓ Енкапсулира (пакетира) пакетите информация от горните слоеве в т.н. “data-link frames” и ги предава на физическия слой за транспортиране
  - ✓ Вградена проверка за грешки в конкретният протокол
  - ✓ Protocol data units (PDU): frame.

- Network layer (Мрежови слой):
  - ✓ Имплементира логическа адресна схема за идентификация на хостовете в дадена мрежа
  - ✓ Рутира (маршрутизира) пакети на база протоколи за рутиране
  - ✓ Енкапсулира (пакетира) пакетите информация от горните слоеве в т.н. “packets” и ги предава на по-долните слоеве за транспортиране
  - ✓ Препредава пакетите от долните слоеве към т.н. „transport layer”
  - ✓ Protocol data units (PDU): packet (datagram)

- Transport layer (Транспортен слой):
  - ✓ Трансферира данните между приложения от различни хостове
  - ✓ Осигурява надеждна обмяна на данните като реализира проверки за грешки, корекции и следене на потока от информация между приложенията
  - ✓ Пакетира информацията, идваща от приложенията от по-горно ниво, като ги обвързва с конкретни TCP/UDP портове и ги предава на мрежовия слой
  - ✓ Препредава пакетите от долните слоеве към т.н. „session layer”
  - ✓ Protocol data units (PDU): segment

- Session layer (Сесиен слой):

✓ Осигурява, поддържа и прекратява сесиите между отделните приложения и хостове.

- Presentation layer (Представителен слой):

✓ Форматира и криптира данните с цел представянето им в определен формат.

- Application layer (Приложен слой):

✓ Генерира данните, които следва да бъдат предадени по мрежата

✓ Protocol data units (PDU): data (message)

Типове предавателна среда – предавателната среда е преносителят на информация, която се транспортира под формата на сигнали. Тези сигнали са различни в зависимост от типа технология.

✓ Коаксиален кабел – информацията се предава под формата на електрически сигнал.

✓ Кабел тип „усукана двойка“ – данните текат под формата на електрически сигнал между отделните проводници.

✓ Оптичен кабел – пакетите с данни се транспортират като електромагнитна (светлинна) вълна.

✓ Безжична среда (Wi-Fi) – ползват се радио вълни за кодиране и пренос на информация.

Разбиране на адаптери, концентратори и превключватели:

- Network Interface Card (NIC) – мрежови адаптер: Конвертира данните от протоколния стек в електрически (оптични) сигнали, които се транспортират през преносната среда. Всеки мрежови адаптер има уникален MAC адрес, който е генериран от производителя. Команди за проверка параметрите на мрежовия адаптер:

  - ipconfig /all;

  - arp –a

- Hub (концентратор):

✓ Многопортово устройство, към което се включват останалите участници в мрежата.

✓ Осигурява централна точка на свързване

✓ Служи за разширяване на мрежата и увеличаване броят на свързаните мрежови устройства

✓ Работи на физическия слой, като играе ролята на сигнален повторител

Повече информация относно мрежовият концентратор може да намерите на адрес: http://en.wikipedia.org/wiki/Ethernet_hub

- Switch (превключвател):

✓ Многопортово устройство, към което се включват останалите участници в мрежата, като осигурява централна точка на свързване

✓ Асоциира всеки свой порт с конкретен хардуерен адрес

✓ Работи стандартно на data-link слой-я, като препраща пакетите с данни на база MAC (хардуерни) адреси

✓ Превключватели с layer 3 и layer 4 функционалностти

Повече информация относно мрежовият превключвател може да намерите на адрес: http://en.wikipedia.org/wiki/Network_switch

- Router (рутер; маршрутизатор):

✓ Управлява мрежовия трафик като препраща пакетите на база “destination IP address”

✓ Поддържа различни рутиращи протоколи:

- RIP; IGRP; EIGRP; OSPF; IS-IS; BGP

✓ Взема рутинг-решения въз основа на информация от т.н. „рутинг-таблица“

✓ Работи на трети слой от седем-слойния OSI модел

✓ Свързва различни по тип мрежови сегменти

Повече информация относно мрежовият рутер може да намерите на адрес: http://en.wikipedia.org/wiki/Router_(computing)

Технология на рутирането - Рутирането е процес на препращане на мрежовите пакети на база информацията, записана в техните хедъри (заглавни части), а именно source и destination IP address. Рутерът взема решение относно препращането на всеки пакет, като прочита данните от полето destination IP address от хедъра на пакета, проверява своята routing таблица и съобразно информацията в нея препраща пакета към неговата дестинация.

Рутерите работят на базата на информация, която получават чрез предварително конфигурирани routing протоколи и обмяна на такава със съседните рутери. Съществуват различни routing протоколи, като най-общо се делят на две категории в зависимост от метода на определяне на routing направлението:

- Distance Vector routing protocols – при тази категория определяща е дистанцията до destination мрежата. Такъв тип протоколи са Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP).

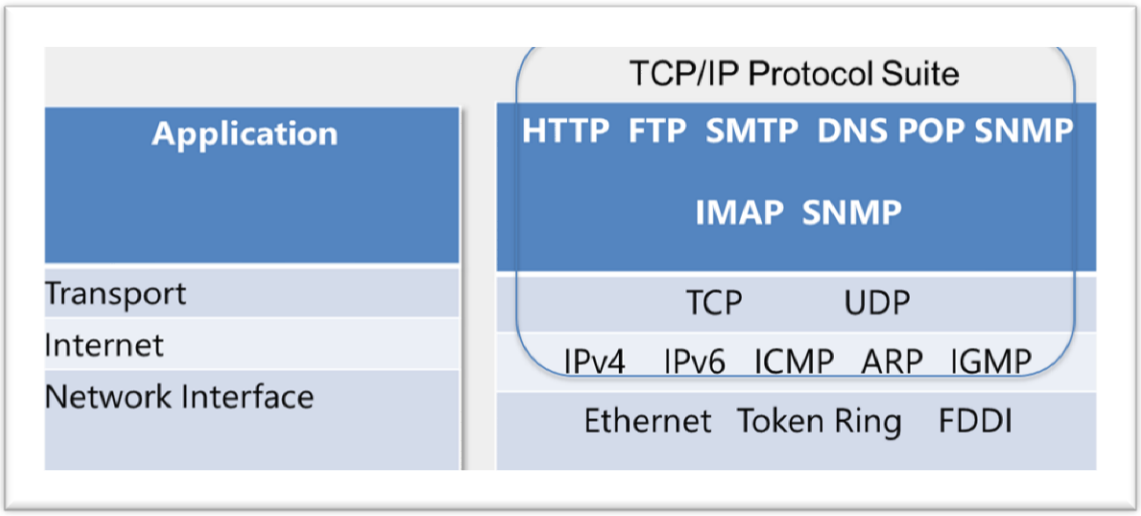
- Link-state routing protocols – определящо при тази категория протоколи е състоянието на връзката към съответния съседен рутер. Пример за такива протоколи са: Open Shortest Path First (OSPF) и Intermediate System to Intermediate System (IS-IS). Повече информация относно рутинг протоколите и рутирането може да намерите на адрес: http://en.wikipedia.org/wiki/Routing_protocol

3: Прилагане на TCP / IP. Описание на протоколи, услуги, TCP / IP пакети и прилагане на IPv4 в среда на Windows Server:

TCP/IP протоколен стек - TCP/IP протоколен стек наричаме съвкупността от мрежови протоколи, които работят на отделните нива (слоеве) и спомагат за цялостния процес на комуникация между два хоста по мрежата. Такива протоколи са:

- В приложният слой: HTTP; HTTPS; FTP; SMTP; DNS; POP3; IMAP4 и др.
- В транспортният слой: TCP; UDP.
- В мрежовият слой: IPv4; IPv6; ICMP; ARP; IGMP.

Повече информация можете да намерите на адрес: http://en.wikipedia.org/wiki/Internet_protocol_suite



Портовете са логически входно-изходни канали, през които преминават пакетираните данни от приложният слой. Всяко мрежово приложение или услуга ползва конкретен и уникален TCP/UDP порт. Протоколите, които управляват комуникацията на ниво „транспортен слой“, са два:

- Transmission Control Protocol (TCP) – сесийно-ориентиран протокол, който създава постоянен комуникационен канал между двата обменящи данни хоста, като осъществява контрол по отношение нивото на грешки, загуба на пакети, последователност при предаване и приемане на пакети, големина на приемащият буфер и т.н. TCP ползва редица собствени механизми за управление и поддържане надеждността на връзката между комуникиращите хостове и затова се нарича още „connection-oriented” протокол. Повече информация относно TCP може да намерите на адрес: http://en.wikipedia.org/wiki/Transmission_Control_Protocol

- User Datagram Protocol (UDP) – не-сесийно ориентиран протокол. За разлика от TCP, UDP не контролира потока от данни, няма вградени процедури за проверка на грешки при предаването и не следи за потвърждение от отсрещната страна за приемане на изпратените пакети. Повече информация относно UDP може да намерите на адрес: http://en.wikipedia.org/wiki/User_Datagram_Protocol

Sockets – логическо понятие, което представлява комбинация от IP адрес и съответен TCP/UDP порт. Пример: FTP (20, 21); SMTP (25); HTTP (80, 8080); SSL/TLS (443); POP3 (110); DNS (53). Повече информация относно Network Socket може да намерите на адрес: http://en.wikipedia.org/wiki/Network_socket

Характеристики на IPv4 адресите - IPv4 адресът прави всеки мрежови хост уникален в мрежата. IPv4 адресът е 32 битов, като се състои от мрежова част и хост част. Мрежовата маска определя границата между мрежовата част и хост частта. Съществуват два типа адреси според това дали те се рутират в Интернет:

- Частни адреси – те се използват за вътрешна комуникация между отделните мрежови устройства в дадена организация. Частните адреси не могат да се рутират извън границите на локалната мрежа (не се рутират в Интернет).

- Публични адреси – те се използват за комуникация между отделните компании и частни Интернет потребители. Този тип адреси се рутират в Интернет пространството и те се раздават под формата на обхвати на доставчиците на интернет услуги (Internet Service Providers - ISP). Интернет доставчиците от своя страна раздават конкретни диапазони от адреси на своите клиенти с цел комуникация в глобалната мрежа.

- Структура на IPv4 адрес:
  - ✓ 32 битов, като в двоичен вид се представя чрез степените на числото 2
  - ✓ Състои се от мрежова част и хост част
  - ✓ Мрежовата маска определя границата между мрежовата част и хост частта
  - ✓ Частни и Публични адреси

Network Class	Length in Network bits	Leading Bits	Range starts with	Range ends with	Exclusion	Default Mask	Private Range starts with	Private Range ends with
A	128	0	0.0.0.0	127.255.255.255	127.0.0.0	8	10.0.0.0	10.255.255.255
B	A+64	10	128.0.0.0	191.255.255.255	no	16	172.16.0.0	172.31.255.255
C	B+32	110	192.0.0.0	223.255.255.255	no	24	192.168.0.0	192.168.255.255

Конфигуриране на IPv4 адреси – съществуват два типа конфигуриране на IPv4 адресите:

- Ръчно конфигуриране – тези адреси се наричат статични и се поставят на устройства, които не са мобилни в мрежата и обикновено изпълняват важни инфраструктурни функции, например: рутери, превключватели, сървъри със

специална функционалност и др. При малки обеми на хостовете в даден мрежови сегмент е удобно да се ползват статични (ръчно конфигурирани) адреси, което води до простота и ефективност на така създадената инфраструктура.

- Автоматично конфигуриране – при този тип конфигуриране се използват технологии като Dynamic Host Configuration Protocol (DHCP) или Automatic Private IP Address Assignment (APIPA). Тези технологии дават възможност за автоматично конфигуриране на повечето мрежови параметри на даден хост, като независимо от неговата локация в мрежата, той винаги е достъпен и способен да комуникира мрежово.

Повече информация относно DHCP протокола може да намерите на адрес: http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

Полезни команди за проверка и отстраняване на проблеми относно IPv4 конфигурацията:

- Windows команди:
  - ✓ ipconfig
  - ✓ ping
  - ✓ tracert
  - ✓ pathping
- Windows PowerShell команди:
  - ✓ Get-NetIPConfiguration
  - ✓ Get-NetIPAddress
  - ✓ Test-Connection

Функционалностти на IPv6 адресната схема:

- Решава проблема с изчерпването на IPv4 адресното пространство.
- 128 битови адреси и съответно по-голямо адресно пространство.
- по ефективни протоколи за рутиране.
- вградени опции за сигурност чрез имплементация на IPsec
- липса на broadcast трафик
- възможност за самоконфигуриране на всеки мрежови хост

Автоматично конфигуриране на IPv6 устройства – съществуват два типа конфигуриране на устройства в среда на IPv6:

- ✓ Stateful – осъществява се с помощта на DHCPv6 сървър.
- ✓ Stateless – чрез комуникация с IPv6 router, който инструктира клиента каква конфигурация са ползва, или от къде и по какъв начин да получи своята IP конфигурация.

За повече информация, касаеща IPv6 мрежови протокол и типовете адресиране, моля посетете следният адрес: http://en.wikipedia.org/wiki/IPv6

Резолюция (конвертиране) на домейн имената - компютърните имена биват два вида:

- NetBIOS name – име във формат 15+1 символа, което се ползва при компютри в група от типа "workgroup" или относително малки мрежи без наличието на DNS услуга.

- Host Name – име, което може да достигне 255 символа и е част от т.н. Fully Qualified Domain Name (FQDN). Използва се в съвременните комуникации при наличието на сложни корпоративни мрежи или за достъп до Интернет ресурси. Съществуват няколко технологии и методи за резолюция на домейн имената. Това са:

- Domain Name System (DNS) инфраструктура – система за именоване на домейни, която дава възможност да се конвертират хост имената в IP адреси и обратно чрез изграждане на DNS инфраструктура, включваща DNS сървър(и), DNS зони, записи в зоните и заявки за резолюция на имената или IP адресите. Информация относно DNS услугите може да намерите на адрес: http://technet.microsoft.com/en-us/library/bb629410.aspx

- Link Local Multicast Name Resolution – метод за резолюция на имената, работещ на принципа на multicast съобщения между предварително самоконфигурирани IPv6 хостове. Повече информация може да бъде намерена на адрес: http://technet.microsoft.com/en-us/library/bb878128.aspx

- NetBIOS and WINS – система за конвертиране на имената, ползваща плоска структура и broadcast messaging, която е относително остаряла като технология и нефункционална при големи йерархични структури и комуникации в Интернет. NetBIOS over TCP/IP е остаряла технология, разчитаща на broadcast съобщения, която е неподходяща за комуникация между партньорски организации или Интернет. NetBIOS имената участват в Windows Internet Name Services (WINS) технологията за научаване на имената и IP адресите на мрежовите устройства. Повече информация на адрес: http://technet.microsoft.com/en-us/library/cc940063.aspx

- GlobalNames Zone – метод за разрешаване на т.н. прости (single-label names) имена. Single-label имената са статични имена на ресурси, които имат плоска структура не отговарят на DNS йерархичния модел. Обикновено такива имена се ползват за ресурси, които са относително статични и не променят често местоположението,

конфигурацията и името си. Пример за такъв тим ресурси в мрежата са файл-сървърите, принт-сървърите, интранет-порталите и др. С цел по-лесното им разпознаване в мрежата и лесното им запомняне от потребителите, обикновено администраторите на тези ресурси създават т.н. alias (псевдоними). Тези псевдоними всъщност са ръчно конфигурирани CNAME записи в DNS зоната, които отговарят на съответните A и PTR записи на дадените ресурси.

GlobalNames зоните са алтернатива на WINS функционалността в дадена мрежова инфраструктура. Употребата им е подходяща в ситуации, където няма инсталирана WINS роля и липсва интеграция между DNS и WINS.

GlobalNames зоната не е достъпна, докато GlobalNames zone поддръжката не е изрично разрешена чрез изпълнението на следната команда върху някой от авторитарните DNS сървъри в дадена мрежова среда:

dnscmd <ServerName> /config /enableglobalnamessupport 1

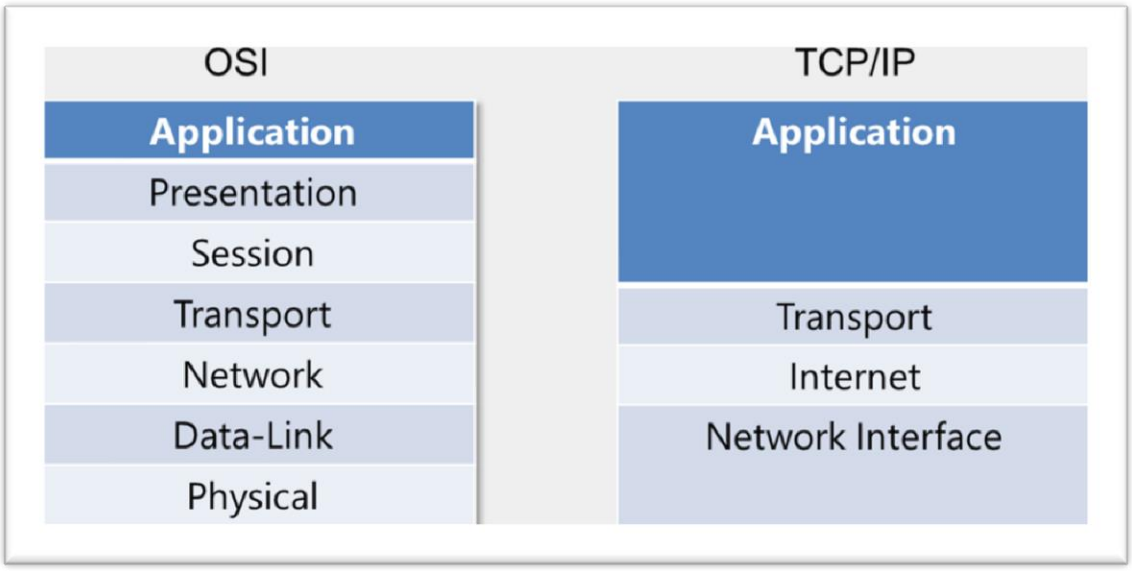
Повече информация относно GlobalNames зоните може да намерите на следният адрес: http://technet.microsoft.com/en-us/library/cc731744.aspx.

4: Прилагане на IPv4:

В контраст на седемслойният OSI модел, съществува и т.н. TCP/IP модел, който е алтернативно представяне на мрежовата комуникация и съдържа четири слоя:

1. Network Interface
2. Internet
3. Transport
4. Application

Повече информация може да получите на следният адрес: http://en.wikipedia.org/wiki/OSI_model



TCP/IP протоколи в приложния слой – в приложния слой работят редица протоколи, които отговарят за имплементирането на повечето съвременни мрежови услуги. Такива протоколи са: HTTP, HTTPS, DNS, DHCP, FTP, FTPS, SFTP, RDP, SMB, SMTP, SNMP, POP3, IMAP4.

IPv4 адресиране - IPv4 адресът се разделя логически на:

- ✓ Мрежова част (Network ID) – идентифицира мрежата
- ✓ Хост част (Host ID) – идентифицира хоста
- ✓ Мрежовата маска определя границата между мрежовата част и хост частта.

IP address	192	168	1	7
Subnet mask	255	255	255	0
Network ID	192	168	1	0
Host ID	0	0	0	7

IPv4 типове адреси - съществуват два типа адреси според това дали те се рутират в Интернет: публични и частни.

- Публични IPv4 адреси:
  - ✓ Те се използват за комуникация между отделните компании и частни Интернет потребители

- ✓ Те са уникални в глобален мащаб
- ✓ Могът да се рутират в Интернет пространството
- ✓ Назначават се от IANA/RIR

- Частни IPv4 адреси:
  - ✓ Не се рутират в Интернет пространството
  - ✓ Назначават се локално от организациите
  - ✓ Транслират се за достъпване на ресурси в Интернет
  - ✓ Диапазони частни мрежи:
    - 10.0.0.0/8
    - 172.16.0.0/12
    - 192.168.0.0/16

Представяне на IPv4 адреси – за представяне на IPv4 адресите се ползва т.н. Dotted-decimal notation метод, който се характеризира със следните особеностти:

- ✓ Базиран е на десетичната бройна система
- ✓ Мрежовите устройства ползват IP адресите в двоичен вид
- ✓ Представянето е базирано на степените на числото 2
- ✓ Кодиране на стойността в 8 бита
- ✓ Минималната стойност е 1
- ✓ Максималната стойност е 255

Пример за dotted-decimal notation представяне:

11111111.11111111.11111111.11111111

128+64+32+16+8+4+2+1=255

192	168	0	7
11000000	10101000	00000000	00000111

Network address: 192.168.0.0 Broadcast address: 192.168.0.255

Подмрежи и Supernetting:

- Subnetting (събнетиране) – разделяне на една мрежа на подмрежи с цел по-ефективно използване на адресното пространство. Осъществява се чрез преместването на стандартната събнет-маска.

Предимства на събнетирането:

- ✓ Ефективно използване на адресното пространство
- ✓ Сегментиране на мрежата и на мрежовия трафик
- ✓ Повишаване на сигурността при ползване на firewall
- ✓ Уплътняване на адресното пространство
- ✓ Информация относно събнетирането може да бъде намерена на адрес: http://en.wikipedia.org/wiki/IPv4_subnetting_reference

Пресмятане на броя на подмрежите (subnets) - ползва се формулата $2^{n,}$ където n е броя на битовете, с които отместваме мрежовата маска от нейната стандартна стойност за съответния клас мрежа.

Пресмятане на броя на хостовете (hosts) - ползва се формулата 2^n -2 , където n е броя на битовете, с които отместваме мрежовата маска от нейната стандартна стойност за съответния клас мрежа.

- Supernetting (обединяване на подмрежи) - комбиниране на няколко подмрежи в една голяма мрежа с цел по-ефективно рутиране. Подмрежите трябва да ползват последователни адреси.

Пример за обединяване на подмрежи:

Мрежа 192.168.2.0/24 11000000.10101000.00000010.00000000

Мрежа 192.168.3.0/24 11000000.10101000.00000011.00000000

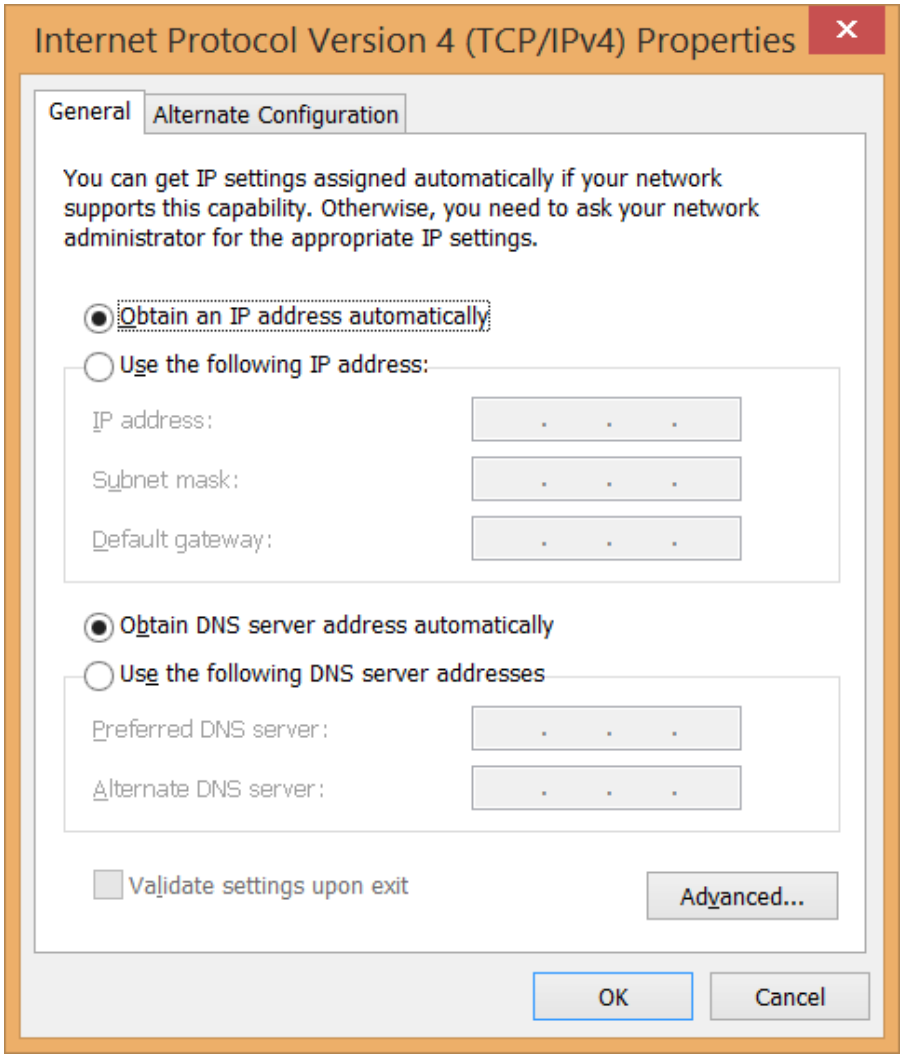
Обединена мрежа 192.168.2.0/23 11000000.10101000.00000010.00000000

Повече информация относно обединяването на мрежи (supernetting) може да бъде намерена на адрес: http://en.wikipedia.org/wiki/Supernetwork

Методи за конфигуриране на IPv4 адреси – съществуват два основни метода за конфигуриране на крайни устройства:

- ✓ Ръчно – през настройките на мрежовият адаптер
- ✓ Автоматично – DHCP протокол и инфраструктура

Методът на конфигуриране се настройва през опциите на мрежовия адаптер на клиентския компютър:



Инструменти и команди за отстраняване на IPv4 неизправностти – основните инструменти и команди, които се ползват, са следните:

- Ipconfig /all
- Ping
- Tracert
- Pathping
- Telnet
- Netstat
- Resource Monitor

- Windows Network Diagnostics
- Event Viewer
- Microsoft Message Analyzer - Microsoft Message Analyzer е протоколен анализатор, който може да прихваща мрежовият трафик и да го анализира. За да свалите Microsoft Message Analyzer, моля посетете следния адрес: http://go.microsoft.com/fwlink/?LinkID=331072

5: Прилагане на Dynamic Host Configuration Protocol (DHCP):

Dynamic Host Configuration Protocol (DHCP) е протокол за автоматично конфигуриране на мрежовите параметри на устройствата в дадена мрежа. DHCP протоколът се характеризира със следното:

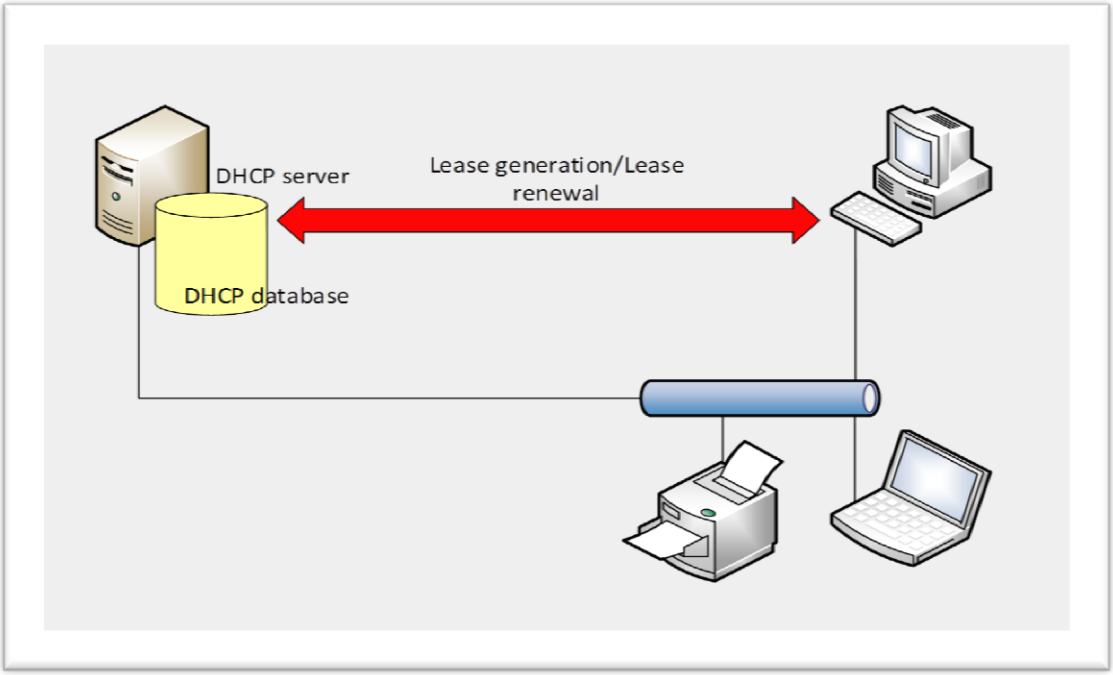
- ✓ Протокол за конфигуриране на динамични хостове
- ✓ DHCP редуцира сложността при конфигуриране на мрежовите устройства
- ✓ DHCP намалява административната работа и намалява възможността от грешки
- ✓ DHCP работи автоматично и елиминира възможността от конфликт на ниво IP адреси
- ✓ Конфигурацията на клиентите се подновява автоматично

Повече за DHCP протокола може да намерите на адрес: http://technet.microsoft.com/en-us/library/cc778368(v=WS.10).aspx

Как работи DHCP услугата:

- DHCP сървърът раздава последователно свободните адреси от даден обхват на базата на заявки от клиентите. Преди да раздаде даден адрес, DHCP сървърът проверява дали този адрес вече се ползва от някой мрежови хост като го ping-ва. Броят на ping съобщенията е параметър, който се настройва и се нарича Conflict Detection Attempt и Microsoft препоръчва стойност на този параметър, не по-голяма от 3. При стойност, по-голяма от 3, се наблюдава забавяне в раздаването на адреси на клиентите и като цяло се забавя DHCP услугата.

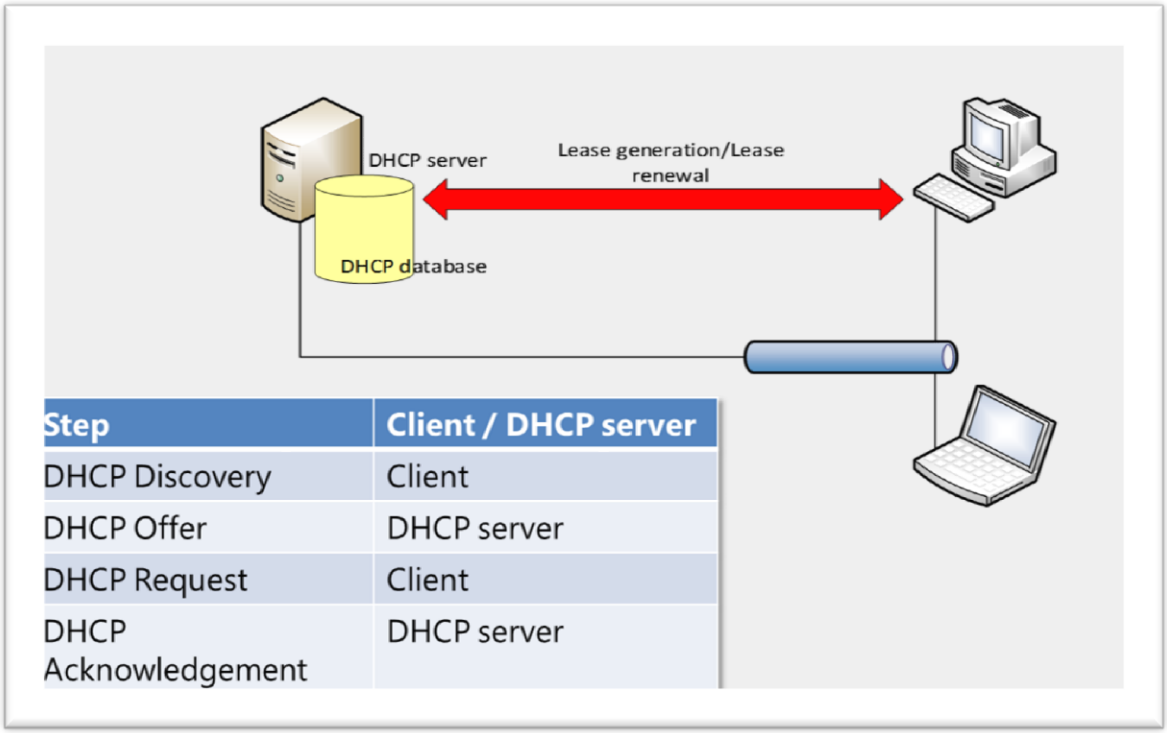
- DHCP сървърът записва вече раздадените адреси във вътрешна база данни, която отразява състоянието на всички DHCP обхвати и съответните раздадени адреси.



Етапи в комуникацията между DHCP клиенти и сървър:

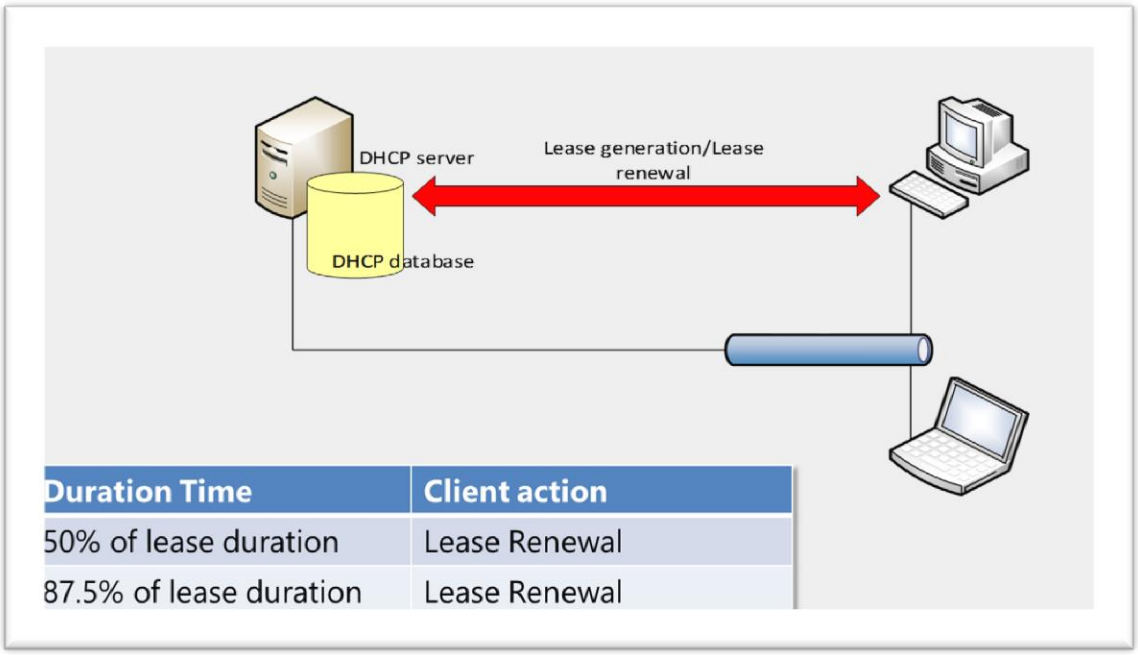
1. DHCP клиентът прави опит за откриване на DHCP сървър. За целта той изпраща DHCP Discovery съобщение по broadcast.
2. DHCP сървърът отговаря на клиентското съобщение, като отговаря на клиента с DHCP Offer.
3. DHCP клиента връща обратно към DHCP сървъра съобщение, с което иска да получи предложеният IP адрес. Това съобщение се нарича DHCP Request.
4. DHCP сървърът потвърждава адреса на клиента чрез т.н. DHCP Acknowledgement. Така раздаденият IP адрес се ползва от клиента „под наем“ за определен период от време.

За повече информация относно DHCP технологията при Windows Server 2012, моля посетете следният адрес: http://go.microsoft.com/fwlink/?LinkId=269709



Step	Client / DHCP server
DHCP Discovery	Client
DHCP Offer	DHCP server
DHCP Request	Client
DHCP Acknowledgement	DHCP server

Процес по подновяване на ползваните от DHCP клиентите адреси: На 50% от времето за ползване на дадената от DHCP сървъра мрежова конфигурация, клиентът прави опит за подновяване. Ако този опит е успешен, клиента продължава да ползва раздадените му мрежови настройки. Ако клиентът не успее да достъпи DHCP сървъра, той прави втори опит при изтичане на 87,5% от времето за ползване на дадения му адрес. Ако и тогава DHCP сървърът не е достъпен, клиента стартира процедурата по откриване на DHCP сървър в мрежата отначало.



Duration Time	Client action
50% of lease duration	Lease Renewal
87.5% of lease duration	Lease Renewal

Взаимодействие между DHCP и DNS - DHCP сървъра може да регистрира и динамично да подновява имената и IP адресите на клиентите. Това става благодарение на това, че DHCP може да ползва dynamic update protocol, чрез който да получава FQDN името на клиента и да го регистрира в съответните DNS зони на DNS сървъра. Освен това, може да бъдат конфигуриране т.н. DHCP политики, чрез които да контролираме регистрацията на имената на клиентските компютри на базата на предварителни критерии като: guest DNS suffix, disabling PTR registration и др.

DHCP Server Authorization - за да стартира DHCP server услугата, трябва DHCP сървъра да се оторизира. Процесът по DHCP оторизация включва регистрация на DHCP сървъра в Active Directory. Само оторизирани Microsoft DHCP сървъри могат да раздават адреси в среда на Microsoft Active Directory. Когато имаме неоторизиран DHCP сървър в мрежата (например Unix-based машина), единствения начин да предотвратим раздаването на адреси от тази машина е като я открием физически, спрем DHCP услугата й, или я изключим от мрежата.

Конфигуриране на DHCP обхвати - DHCP обхватите (scopes) са диапазони от адреси, предвидени за раздаване от сървъра. Тези диапазони отговарят на съответните IP мрежи или подмрежи и са предварително конфигуриране от администратора.

DHCP обхватите притежават следните параметри:

- ✓ Network ID – IP адресът на мрежата
- ✓ Lease duration – период за ползване на раздадените адреси
- ✓ Scope name – име на обхвата
- ✓ Subnet mask – маска на дадената мрежа
- ✓ IP address range – диапазон на раздаваните адреси
- ✓ Reservation – резервация на даден адрес на база MAC адрес
- ✓ Exclusion range – диапазон от адреси, изключени от раздаване

Конфигуриране на DHCP reservation (резервация): това е резервация на конкретен IP адрес за даден хост на база неговият MAC адрес. DHCP резервацията осигурява един и същ адрес на дадено мрежово устройство, като този адрес не може да бъде раздаден на друго такова.

Употреба на резервации:

- ✓ Принтери под DHCP
- ✓ Други устройства под DHCP, които искат постоянен IP адрес: Uninterruptable Power Supply (UPS); Digital Video Recording (DVR) устройства; компютри, достъпвани отдалечено през VPN канали

Конфигуриране на DHCP опции - DHCP опциите се прилагат на следните нива и при следната последователност:

- server
- scope
- class
- reservation

Съществуват множество опции за конфигуриране като най-използваните DHCP опции са:

- router (default gateway)
- DNS server
- Time server
- TFTP server

Управление на DHCP база данни - DHCP базата данни е динамична база, която съдържа информация за конфигурираните обхвати, резервации и раздадени адреси. Тя се намира в ***%systemroot%\System32\Dhcp folder*** и се архивира на всеки 60 минути. Желателно е да бъде архивирана ръчно на определен интервал от време, като за целта може да бъде ползват Windows Server Backup.

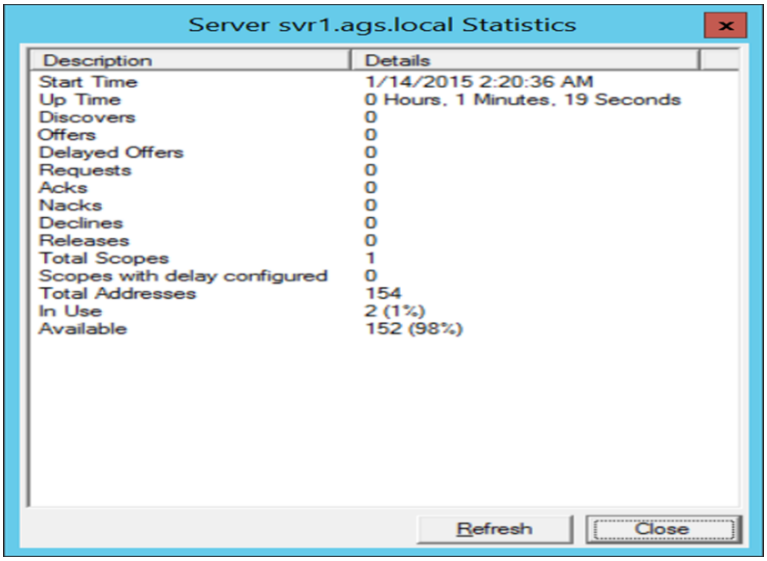
Процедурата по миграция на DHCP базата от един сървър на друг преминава през следните стъпки:

1. Архивиране на базата на стария сървър.
2. Спиране на DHCP услугата на стария сървър.
3. Копиране на архивното копие на DHCP базата на новия сървър.
4. Възстановяване на DHCP базата от архивното копие.
5. Стартиране на DHCP услугата на новия сървър.

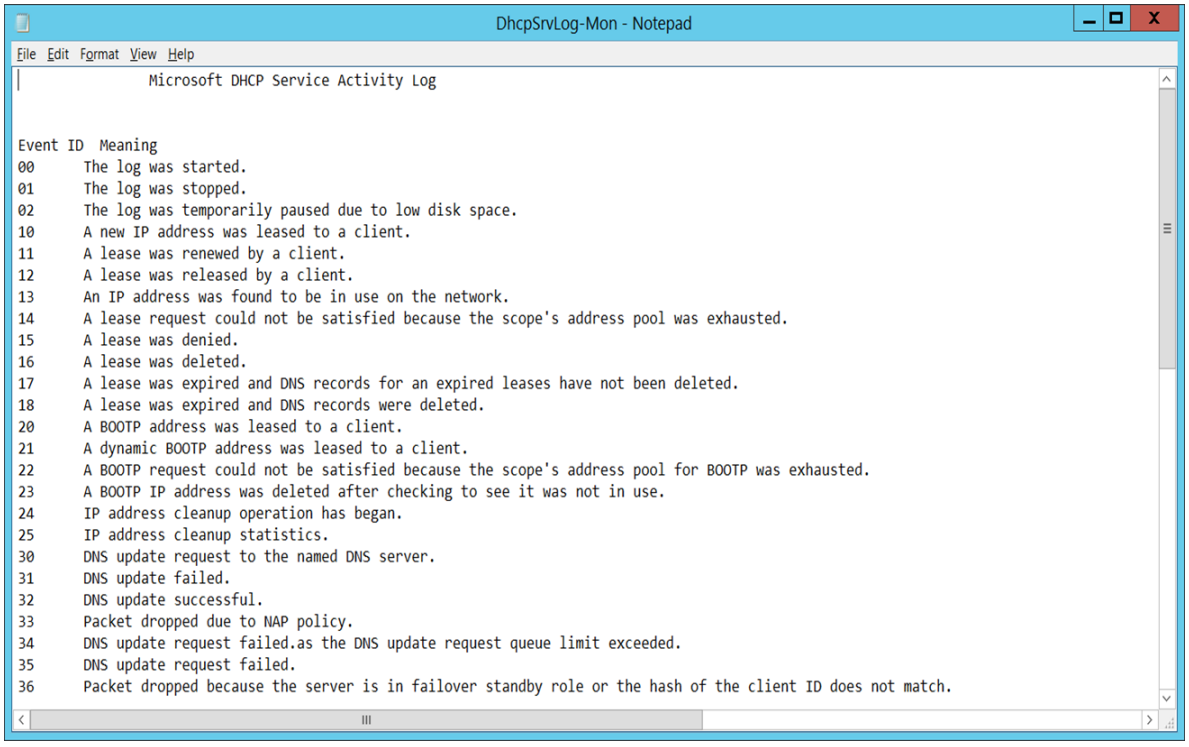
Блокиране достъпа на неоторизирани клиенти до DHCP услуги – подходящи са следните действия и технологии:

- Блокиране на физическият достъп до мрежата (жичен или безжичен) на неоторизирани клиенти
- Пускане на одит-функционалността на DHCP сървъра
- Регулярна проверка и анализ на одит логовете
- Ползване на 802.1X автентикация и базирани на нея технологии:
  - ✓ Network Admission Control (NAC)
  - ✓ Network Access Protection (NAP)

Статистика на DHCP услугите – DHCP статистиките дават възможност да се събира информация относно работното състояние и раздадените адреси от DHCP сървъра. Тези статистики се събират на ниво сървър или на ниво обхват.



Одит на DHCP услугите – DHCP сървърът автоматично генерира логинг-информация под формата на лог-файлове, които съдържат подробна информация относно активността на DHCP услугата. Тези лог-файлове са именовани съобразно конкретния ден от седмицата и се намират на следната локация: C:\Windows\System32\dhcp.



6: Внедряване на DNS: DNS пространството от имена (namespace) е йерархична структура за именоване, осигуряваща динамично конвертиране на имената на ресурсите към съответните техни IP адреси и обратно в локален или глобален мащаб. DNS протоколът е предпочитан метод за резолюция на имената от съвременните операционни системи. DNS имената са базирани на:

- ✓ Географски принцип – имената са разпределени на база държава или регион.
- ✓ Организационен принцип – разпределението на имената става на база функциите на дадена организация.

Основните компоненти при DNS резолюцията са:

- DNS сървър – съдържа информация относно имената на хостовете и техните IP адреси в зоната, за която даденият DNS сървър е отговорен.
- DNS зони – те отразяват конкретно адресно пространство (домейн) и съдържат A и PTR записи на хостовете от този домейн. DNS зоните биват:

- Forward lookup zone – права зона, чрез която се конвертират имената в IP адреси.

- Reverse lookup zone – обратна зона, чрез която се конвертират IP адресите в имена.

- DNS записи – биват:

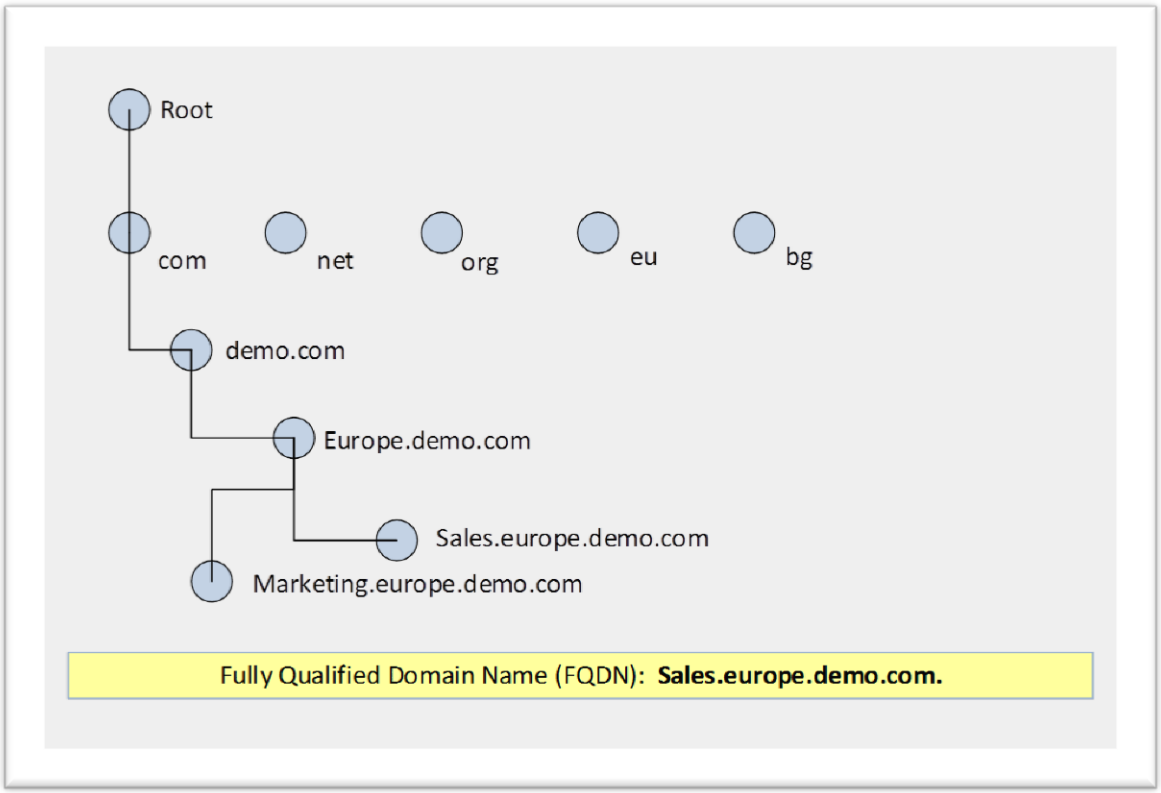
- A (прави – име към IP адрес);
- PTR (обратни - IP адрес към име)
- MX (Mail Exchanger – обозначава мейл сървъра в даден домейн)
- CNAME (alias - псевдоним)

- DNS заявки – заявките за резолюция на имената в IP адреси и обратно. Биват рекурсивни и итеративни.

Системата за именоване на домейни (DNS) има йерархична структура, като пълните имена на ресурсите се определят в зависимост от положението на дадения ресурс в йерархията. Най-високо е т.н. корен (главен домейн или root). Под него са top-level домейните (com; net; org; eu; bg), а под тях се намират реалните домейн имена на отделните организации. По този начин се образува т.н. Пълно име на мрежовият ресурс (Fully Qualified Domain Name - FQDN).

Допълнителни компоненти на DNS инфраструктурата:

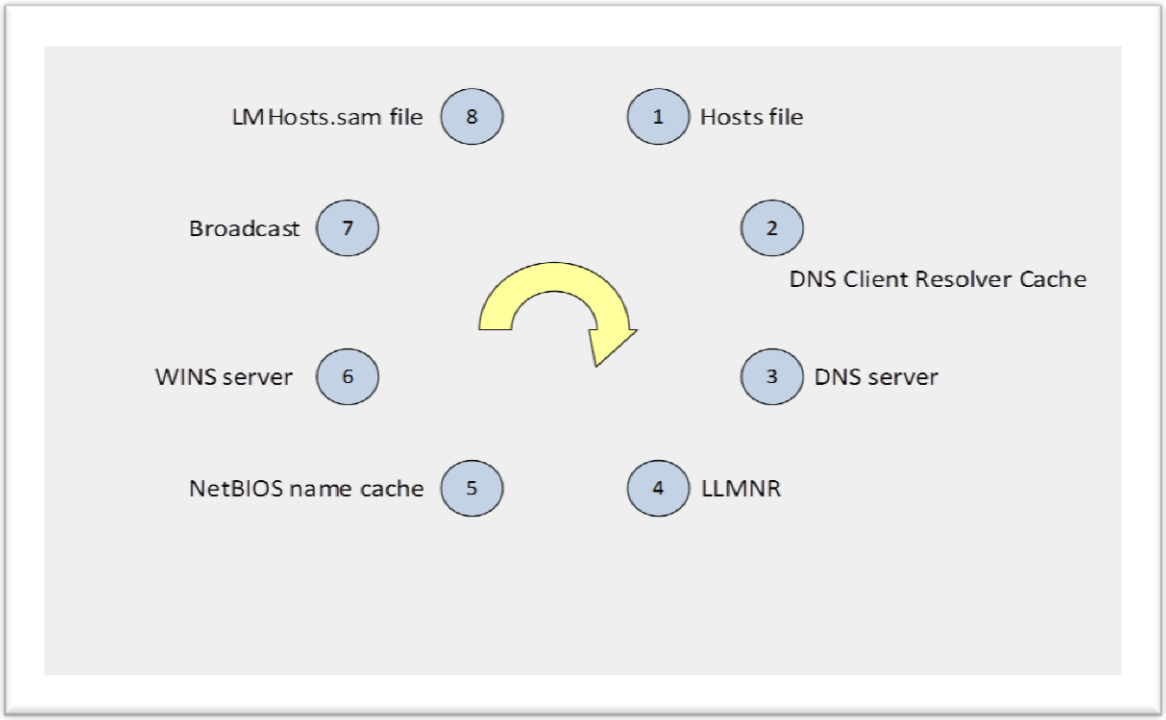
- DNS Client Resolver Cache (DNS resolver) – услуга, която работи в контекста на операционната система и трансформира имената в адреси и обратно. Освен това, DNS Client Resolver Cache-а играе ролята на буфер, в който се пазят вече известните за системата имена и техните съответни адреси.
- DNS Forwarder – процес на препредаване на заявките за резолюция от един хост (сървър) към друг.
- DNS Delegation – процес на прехвърляне на дейността по разкриване на имената или адресите към друг мрежови хост.



Процес на конвертиране на DNS имената от клиента – започва с прочитането на съдържанието на Hosts файла и зареждането му в т.н. DNS Client Resolver Cache. Когато дойде заявка за резолюция на име или адрес, проверката преминава през следните нива:

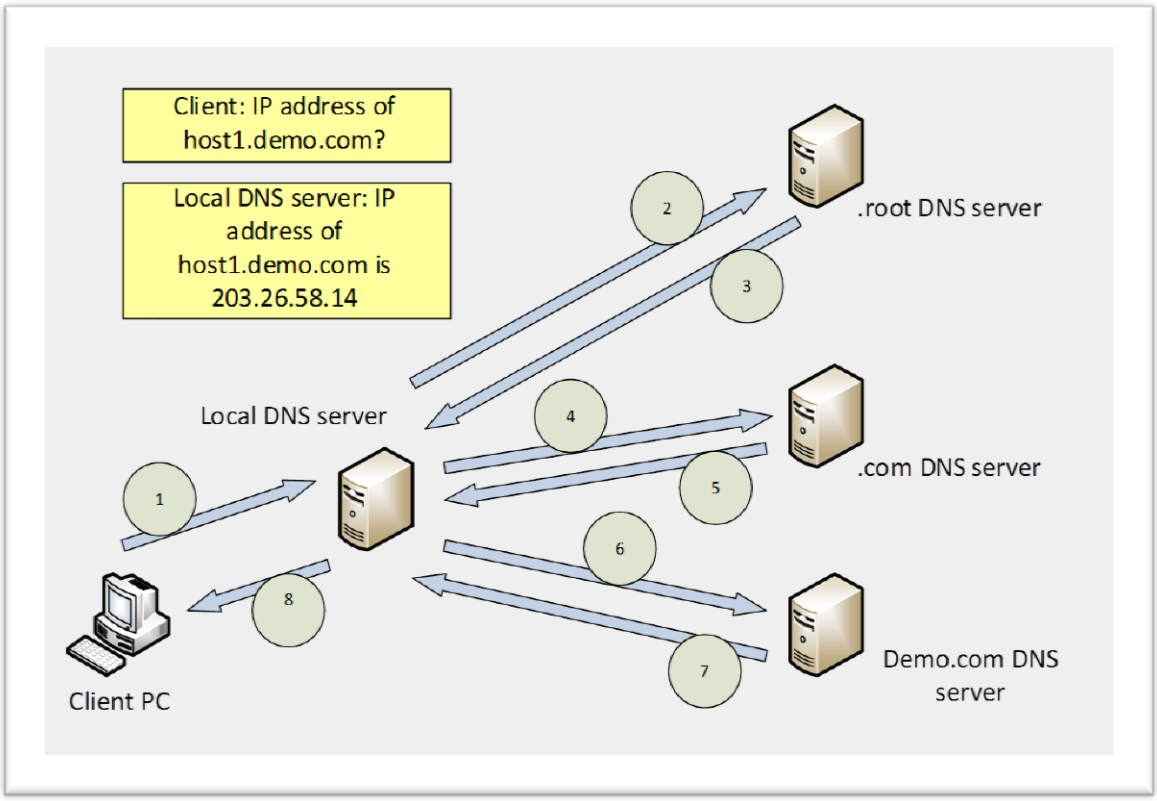
1. Прочитане съдържанието на Hosts файла и ако той не съдържа адекватна информация, се преминава на следващото ниво.

2. Проверка на DNS Client Resolver Cache-а. Ако той не съдържа нужната информация, се преминава на следващото ниво.
3. Заявка към конфигурираният DNS сървър. Ако той не съдържа адекватна информация в базата си, се преминава на следващото ниво.
4. Опит за резолюция чрез LLMNR. Ако този метод не върне адекватен отговор, се преминава на следващото ниво.
5. Опит за резолюция чрез NetBIOS client cache. Ако този метод не върне адекватен отговор, се преминава на следващото ниво.
6. Опит за резолюция чрез заявка към WINS сървър (ако има конфигуриран такъв). Ако този метод не върне адекватен отговор, се преминава на следващото ниво.
7. Опит за резолюция чрез Broadcast. Ако този метод не върне адекватен отговор, се преминава на следващото ниво.
8. Опит за резолюция чрез прочитане съдържанието на LMHosts.sam файла. Ако този метод не върне адекватен отговор, системата връща негативен отговор.

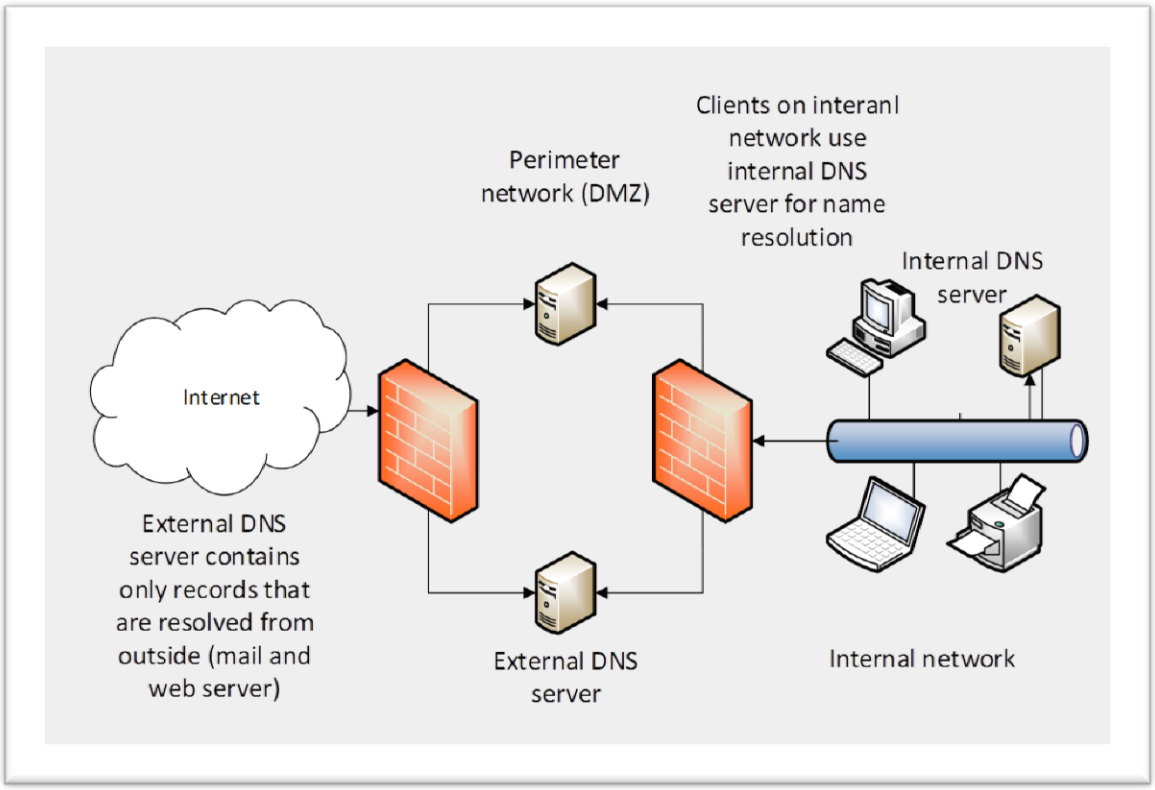


Процес на конвертиране на DNS имената в Интернет – процесът включва последователност от заявки, като се започне от root DNS сървъра и се премине последователно през т.н. top-level DNS сървъри, докато се стигне до авторитарният за даденото адресно пространство (домейн) сървър.

Отделните стъпки в процеса по конвертиране на имената в Интернет са отразени в следната графика:



Split-DNS - Split-DNS е инфраструктурно решение, при което процеса по преобразуване на имената е разпределен между 2 отделни DNS сървъра. Единият от тях се намира във вътрешната мрежа и обслужва всички DNS заявки от вътрешните клиенти, а другия се намира в периметър-мрежата и обслужва само и единствено външни за компанията клиенти. Разположения в DMZ мрежата DNS сървър съдържа записи само на тези ресурси, които са част от вътрешната мрежа и са публикувани навън за ползване от външни за компанията клиенти. Split-DNS моделът е отразен на следващата схема:



DNS queries (DNS заявки) – биват два типа:

- ✓ recursive queries – това са заявките, които се генерират от клиентите към техният конфигуриран DNS сървър.
- ✓ iterative queries – това са заявки, които даден DNS сървър генерира към останалите DNS сървъри.

Типове DNS сървъри:

- ✓ Authoritative (авторитарен; оторитативен) DNS сървър:

- отговаря и държи writable копие на дадена зона

- връща заявеният адрес или име, или връща авторитарен отговор „нямам информация“

- ✓ Non-authoritative (не- авторитарен) DNS сървър:

- проверява кеша; ползва forwarding; ползва root hints;

DNS Root Hints – функционалност, която ползва списък, съдържащ IP адресите на 13-те *Root DNS* сървъра в Интернет пространството. *Root Hints* се зареждат при инсталацията на *DNS* сървърната роля, като се копират от *cache.dns* файла. Ползват се, когато нямаме конфигурирано препращане (*forwarding*). Процесът на употреба на *Root Hints* от *DNS* сървъра наричаме DNS server recursion.

DNS Forwarding е процеса по препращане на заявката за резолюция към друг DNS сървър. DNS клиентите генерират заявки към конфигурирания DNS сървър. DNS сървърът ползва *forwarding*, когато е конфигурирано препращане (*forwarding*) и той не може да върне отговор на дадена DNS заявка на база информацията в базата си. DNS сървърът препраща заявките към друг DNS сървър (*Forwarder*).

DNS caching наричаме повторното извличане на информацията от вече обработени DNS заявки. DNS сървъра пази успешно резолираните DNS заявки в специален буфер, наречен кеш, като стандартното време за пазене на информация в кеша е 60 минути. Cache-only DNS server наричаме сървър, който няма конфигурирани зони.

Методи на инсталация на DNS сървърна роля:

- ✓ Server Manager
- ✓ Active Directory Domain Services Installation Wizard

Управление на DNS сървър – използват се следните инструменти:

- ✓ MMC console (DNS Manager snap-in)
- ✓ Server Manager
- ✓ DNS Manager console (dnsmgmt.msc)
- ✓ DNSCmd command-line tool
- ✓ Window PowerShell
- ✓ Remote Server Administration Tools (RSAT)

Типове DNS зони:

- Primary DNS zone – представлява редактируемо копие на конкретна DNS база.

- Secondary DNS zone – копие само за четене (read-only) на дадена DNS база.
- Stub DNS zone – копие на дадена зона, което съдържа само записи на авторитарните DNS сървъри за тази зона.
- Active Directory-Integrated DNS zone – зона, която се съхранява като част от базата на Active Directory и се репликира между домейн-контролерите в даден домейн. Позволява т.н. multi-master записване на информация в зоната. Основните характеристики на този тип зона са:

  ✓ Ползва AD DS репликация за уеднаквяване на зоновата информация между домейн контролерите

  ✓ Attribute-level replication

  ✓ Позволява secure dynamic updates

  ✓ Повишена сигурност

  ✓ Изискване за реализация: DNS ролята да е инсталирана на домейн контролер

  ✓ Възможност за делегиране на контрол върху дадена зона чрез модифициране на *access control list-a* на зоната

Информация относно Active Directory-Integrated DNS зоните може да намерите на следния адрес: https://technet.microsoft.com/en-us/library/cc772746(v=ws.10).aspx

7: Прилагане на IPv6:

Предимства и недостатъци на IPv6 протокола:

- Предимства:

✓ По-голямо адресно пространство в сравнение с IPv4

✓ Йерархична адресна и рутинг инфраструктура

✓ Автоматично конфигуриране: *stateful / stateless*

✓ Вградена поддръжка на *IPsec* и *QoS*

✓ Разширяемост (*scalability*)

✓ End-to-end communication (липса на методи за транслация като NAT)

- Недостатъци:

- ✓ По-трудна работа с 128 битови адреси
- ✓ Трудности при взаимно съществуване с IPv4

Разлики между IPv4 и IPv6 протоколи:

Feature	IPv4	IPv6
Fragmentation	Performed by routers and sending host	Performed by sending host
Address resolution	ARP via broadcast	Multicast Neighbor Solicitation messages
Manage multicast group membership	IGMP	Multicast listener discovery
Router discovery	ICMP Router Discovery	Router Solicitation/ Router Advertisements
DNS host record	A	AAAA
DNS reverse lookup zone	IN-ADDR.ARPA	IP6.ARPA
Minimum packet size	576 bytes	1280 bytes

Характеристика на IPv6 адресите:

- ✓ 128 битов формат
- ✓ Представяне и употреба в 16-тичен вид (*hex-based*)
- ✓ Възможност за премахване на нулеви стойности в началото на адреса
- ✓ Възможност за заместване на нулеви стойности в средата на адреса
- ✓ Възможност за заместване на последователни нулеви стойности в средата на адреса със символа ::

Пример за IPv6 адрес: **2001:1DB6:0000:2F4B:23AA:00FF:FE28:9B7A**

Сравнение на специалните адреси при IPv4 и IPv6:

Address Type	IPv4	IPv6
Unspecified	0.0.0.0	::
Loopback	127.0.0.1	::1
Broadcast	255.255.255.255	Multicast
Multicast	224.0.0.0/4	FF00::/8
Autoconfigured	APIPA (169.254.0.0/16)	FE80::/64

Видове IPv6 адреси:

- Global Unicast Addresses – имат следните характеристики:

  ✓ Рутират се в Интернет пространството
  ✓ Започват с 2 или 3 (2000::/3)
  ✓ Заделени 16 бита за събнетиране

Prefix (managed by IANA)	Prefix assigned to top-level ISP	Subnet bits for organizations	Client interface ID
48 bits		16 bits	64 bits

- Unique Local Addresses – имат следните характеристики:

  ✓ Еквивалент на частните IPv4 адреси
  ✓ Започват с FC или FD
  ✓ Заделени 16 бита за вътрешно-фирмено събнетиране

Prefix (11111110)	Organization ID	Bits for internal subnetting	Client interface ID
8 bits	40 bits	16 bits	64 bits

- Link Local Addresses – имат следните характеристики:

  ✓ Еквивалент на IPv4 APIPA адресите
  ✓ Започват с FE80::/8
  ✓ Автоматично се генерират от всички IPv6 хостове
  ✓ Притежават зонов идентификатор

Prefix FE80 (11111010)	Organization ID	Client interface ID
10 bits	54 bits	64 bits

Пример за Link Local Address: fe80::2b0:d0ff:fee9:4143%3

- Автоконфигуриране на IPv6 адресите - процесът по автоконфигуриране на IPv6 адресите от страна на мрежовите хостове преминава през следните стъпки:

  ✓ Генериране на *link-local address*

  ✓ Проверка за конфликти чрез *neighbor solicitation*

  ✓ Опит за намиране на рутер в мрежата чрез *router discovery*

  ✓ Заявка на префикс от рутера

  ✓ Добавяне на полученият префикс от клиента

  ✓ Опит за намиране на DHCP сървър при инструкция от страна на рутера

Технологии за взаимно съществуване на IPv4 и IPv6 адресни схеми:

- ✓ 6to4 tunneling
- ✓ ISATAP
- ✓ Teredo

За повече информация относно технологиите за взаимно съществуване и преминаване от IPv4 към IPv6 и обратно, моля посетете следния адрес: http://go.Microsoft.com/fwlink/?LinkID=112079&clcid=0x409

Част III: Администриране на работни станции и сървъри.

1: Внедряване на мрежова инфраструктура за файлове и услуги за данни:

- iSCSI – описание, компоненти и внедряване: iSCSI е мрежови протокол за достъп до SCSI-базирани устройства за съхраняване на данни, който пренася SCSI командите по IP мрежи.

Предимства на iSCSI:

✓ Ползва стандартна IP мрежа, което предполага липса на ограничение в разстоянието между предлагащата и ползващата iSCSI страна.

✓ Лесен за имплементация

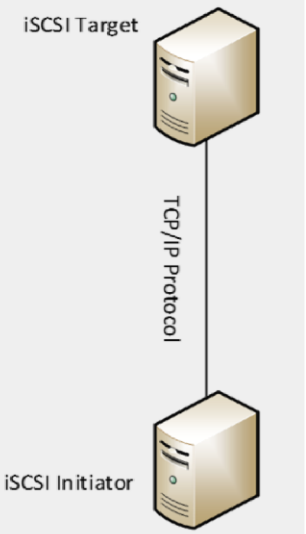
✓ Не изисква специален хардуер или окабеляване

- ✓ iSCSI работи на ниво LAN, WAN и Internet.
- ✓ Ползва TCP port 3260

Реализацията на iSCSI протокола се базира на следните компоненти:

- iSCSI Target – функционална роля на мрежовият хост, предлагащ iSCSI storage space.
- iSCSI Initiator – софтуерен компонент или хардуерен адаптер, позволяващ достъп до iSCSI Target дисковото пространство.
- iSCSI Qualified Name (IQN) – уникален идентификатор, който отразява връзката между iSCSI Target-а и iSCSI Initiator-а.

Component	Description
iSCSI Target	Run on storage and enable access to disks
iSCSI Initiator	Software component or adapter on server(client) that provides access to iSCSI target
iSCSI Qualified Name (IQN)	Globally unique identifier used to address initiators and targets on iSCSI network



Функционалности и внедряване на iSCSI:

iSCSI Target server	iSCSI initiator
Role service in Windows Server 2012	Runs as a service in the operating system
Features: - Network/diskless boot - Server application storage - Heterogeneous storage - Useful for lab environments	Installed by default in Windows 8 and Windows Server 2012 Features: - Authentication target/initiator (CHAP) - Query initiator for ID

Повече информация относно iSCSI възможностите на Windows Server 2012 може да получите на следния адрес: http://go.microsoft.com/fwlink/?LinkId=270038

За реализация на High Availability при iSCSI се използват следните два типа технологии:

- ✓ Multiple Connected Session (MCS) – позволява множество TCP/IP връзки от инициатора до таргета в рамките на една iSCSI сесия. Поддържа автоматичен *failover*.
- ✓ Multipath I/O (MPIO) – осигурява автоматичен failover при пропадане на мрежата само ако таргета и инициатора притежават множество мрежови адаптера (NIC).

За реализация на сигурност при iSCSI се използват следните протоколи:

- ✓ For authentication:

- One-way CHAP

- Mutual CHAP

- ✓ For encryption and data integrity:

- IPsec

Изисквания и добри практики при имплементиране на iSCSI:

- ✓ Бърза мрежова инфраструктура

- ✓ *High availability* на мрежовите ресурси
- ✓ Сигурност и защита на iSCSI устройствата за съхранение на данни
- ✓ Следване препоръките и добрите практики на производителя
- ✓ Комбиниран екип от специалисти от различни сфери при изграждане на iSCSI инфраструктурата

- Имплементиране на SMB 3.0 - Server Message Block (SMB) е протокол за осигуряване и достъп до споделени файлове (ресурси) в Windows Server 2012.

Функционалности на SMB 3.0:

- ✓ SMB transparent failover
- ✓ SMB scale out
- ✓ SMB multichannel
- ✓ SMB direct
- ✓ Performance optimization and encryption
- ✓ SMB operates over TCP port 445
- ✓ Enabled by default in W2K12 and specific Windows PowerShell cmdlets
- ✓ Hyper-V over SMB (SMB shared folder as storage for Hyper-V hosts)
- ✓ MS SQL Server over SMB (SMB shared folder can host SQL server database)

Внедряване на високопроизводителни мрежови функции – с цел повишена производителност и надеждност в среда на Windows Server 2012, е възможна употребата на следните технологични решения:

- Network Interface Card (NIC) Teaming – обединяване на няколко мрежови адаптера с цел увеличаване на мрежовия капацитет и постигане на *high availability* решение. Характеристики на NIC Teaming:
  - ✓ Increased throughput
  - ✓ Increased reliability
  - ✓ Network adapter load balancing
  - ✓ Конфигуриране – от Local Server Node in Server Manager

- Receive Segment Coalescing (RSC) - технология, при която централния процесор се разтоварва от обслужване на мрежовия трафик, като тези задачи се поемат от специален RSC-enabled мрежови адаптер, който комбинира входящите TCP пакети. Изисквания, ефекти и употреба на RSC решението:
  - ✓ Requirement for RSC-enabled network adapter
  - ✓ Performance improvement for received-side
  - ✓ Used in following scenarios: Hosted cloud environments; Input-intensive databases; File servers

Полезни Windows PowerShell команди за управление на RSC функционалността:

- ✓ Enable-NetAdapterRsc
- ✓ Disable-NetAdapterRsc
- ✓ Get-NetAdapter Rsc
- ✓ Set-NetAdapterRsc
- ✓ Set-NetOffloadGlobalSettings - ReceiveSegmentCoalescing

- Receive Side Scaling (RSS) – технология, при която мрежовия адаптер разпределя “kernel-mode” мрежовото натоварване между няколко процесорни ядра при компютри с “multi-core” процесори. Употреба на RSC решението:
  - ✓ Multi-core сървъри с голямо мрежово натоварване
  - ✓ Web и File сървъри
  - ✓ Load balancing of DirectAccess traffic
  - ✓ Network Load Balancing and Failover Clusters

Полезни *Windows PowerShell* команди за управление на *RSS* функционалността:

- ✓ Enable-NetAdapterRss
- ✓ Disable-NetAdapterRss
- ✓ Get-NetAdapter Rss
- ✓ Set-NetAdapterRss
- ✓ Set-NetOffloadGlobalSettings – ReceiveSideScaling

- SMB Direct – технология, която позволява RDMA-enabled мрежови адаптери да бъдат ползвани в среда на Windows Server 2012. Remote Direct Memory Access (RDMA)-capable NIC е мрежови адаптер, който работи на пълна скорост при минимална латентност и минимална употреба на централния процесор на даден сървър. Изисквания за ползване на SMB Direct:
  - ✓ Мрежови адаптери, които поддържат RDMA
  - ✓ Най-малко два сървъра под Windows Server 2012

  Употреба: Hyper-V over SMB; SQL over SMB

  Полезни *Windows PowerShell* команди за управление на *SMB Direct* функционалността:

  Enable-NetAdapterRdma <network_adapter_name>

  Disable-NetAdapterRdma <network_adapter_name>

- SMB Multichannel – технология, която позволява ползването на няколко мрежови адаптера едновременно за SMB 3.0 трафик. Изисквания:
  - ✓ Няколко мрежови адаптера
  - ✓ *RSS* или *RDMA-enabled* мрежови адаптери
  - ✓ Мрежови адаптери в *NIC-teaming*
  - ✓ Поддържани версии на операционни системи: Windows 8/8.1; Windows Server 2012/2012 R2

  Полезни *Windows PowerShell* команди за управление на *SMB Multichannel* функционалността:

  - ✓ To enable SMB server: Set-SmbServerConfiguration -EnableMultiChannel $true
  - ✓ To disable SMB server: Set-SmbServerConfiguration -DisableMultiChannel $true

2: Конфигуриране на Desktop Security:

Прилагане на централизирано решение за сигурността:

Audit Policies (одит политики) – одит политиките са незаменим елемент от цялостната политика по сигурност в дадена компания. Политиките по одит определят как се контролира достъпа до ресурси, какви събития да се

мониторират и при настъпването на какви действия или събития да се генерират логове.

- Audit strategy planning:

✓ Generation of a manageable volume of log messages

✓ Ability to view and analyze the generated audit log messages

- Windows 8 (Windows Server 2012) improvements:

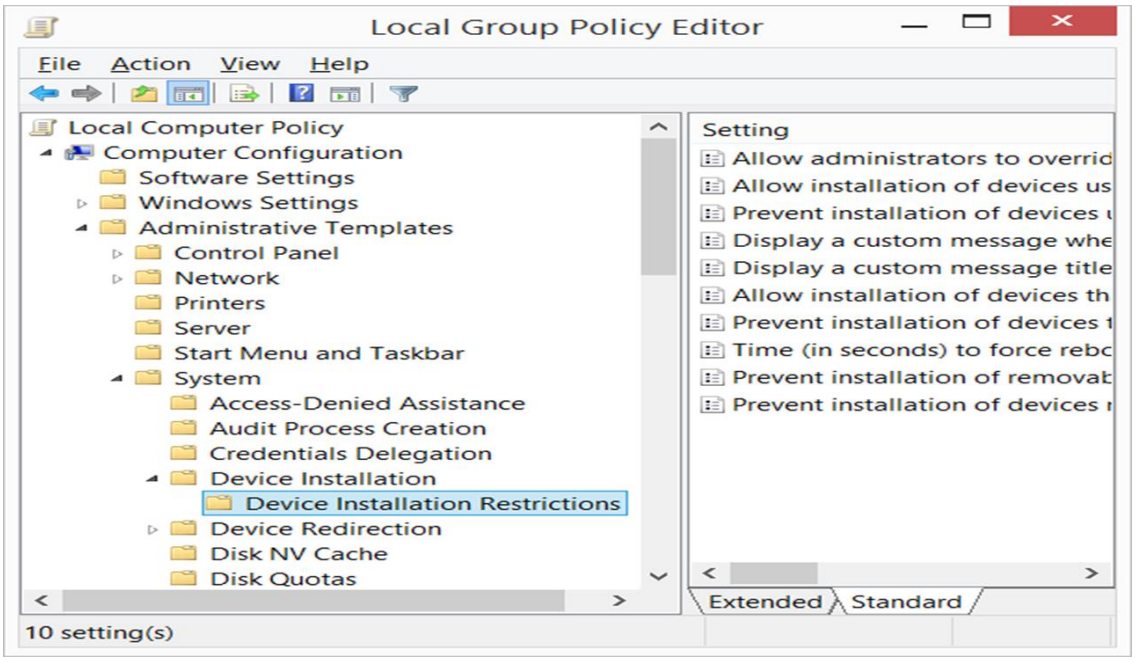
✓ Central management of audit policy through Group Policy

✓ Auditing of removable devices

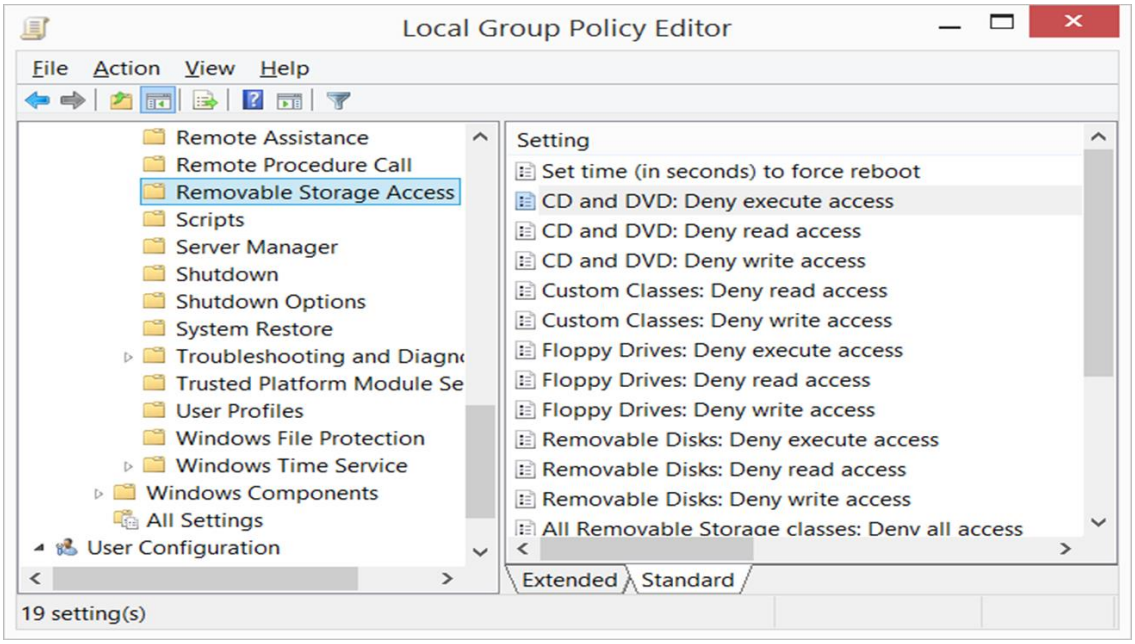
User Account Control - UAC е услуга, която предотвратява приложенията да добият административни права без знанието на потребителя. UAC предпазва компютърната система от автоматично инсталиране на зловреден софтуер и предупреждава потребителя когато той (или дадено приложение) се опитва да стартира процес, изискващ административни права. Без UAC функционалността и когато потребителя има административни права, всяко приложение, стартирано в контекста на потребителския акаунт, ще има административни права върху системата.

Device and Media Restriction Policy Settings – Group Policy настройки, касаещи контрол върху инсталирането на устройства. Намират се в Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions на Group Policy Editor конзолата.

Device Installation Group Policy Settings:



Removable Storage Access Group Policy Settings:



Планиране и изпълнение на BitLocker: BitLocker е функционалност, позволяваща побитово криптиране на дял или цял диск с цел предотвратяване на неоторизиран достъп до информацията на този диск

- Планиране употребата на BitLocker:

- ✓ На кои компютри ще се ползва?
- ✓ Ползване на BitLocker по време или след инсталация на операционната система?
- ✓ *Full-Volume* или *BitLocker On-Write Encryption*?
- ✓ BitLocker Mode? (BitLocker with TPM; BitLocker with TPM and PIN; BitLocker with USB device; BitLocker with TPM and USB device; Network Unlock)
- ✓ Информация относно BitLocker като технология може да намерите на адрес: https://technet.microsoft.com/en-us/library/hh831713.aspx

Предварителни изисквания при употреба на BitLocker:

- Системни изисквания:
  - ✓ Windows Vista or newer
  - ✓ Partition with minimum 1.5 GB NTFS formatted system drive, containing files necessary for decryption of system drive and to load OS
  - ✓ OS should be on NTFS partition
  - ✓ TPM support (or USB support)
- Изисквания по отношение на Active Directory:
  - ✓ Schema extensions to support BitLocker recovery password storage
  - ✓ GPO policy settings to manage BitLocker settings

Microsoft BitLocker Administration and Monitoring (MBAM) – приложение за наблюдение и управление на BitLocker в Enterprise среда. MBAM е част от Microsoft Desktop Optimization Pack (MDOP) и притежава следните функционалности:

- ✓ Allows you to manage and report on BitLocker usage in your enterprise network
- ✓ Client monitoring and reporting on status
- ✓ Centrally storing BitLocker drive recovery keys
- ✓ Managing TPM to provide a password file to bypass the PIN requirements when necessary
- ✓ MBAM 2.0 supports integration with Configuration Manager 2007 or Configuration Manager 2012

Планиране и внедряване на MBAM сървърна инфраструктура:

- MBAM изисквания:
  - ✓ Windows Server 2008 SP2 or newer
  - ✓ Microsoft SQL Server 2008 R2 or newer
  - ✓ Enterprise or Datacenter Editions
  - ✓ Internet Information Services (IIS)
  - ✓ SQL Server Reporting Services (SSRS)
  - ✓ Clients configured through Group Policy

Планиране и внедряване на MBAM клиентска инфраструктура:

- MBAM Client:
  - ✓ Requires .NET Framework 3.5.1
  - ✓ Can be installed before or after the computer is used by users
- Methods of deployment:
  - ✓ Manually
  - ✓ As part of Operating System image
  - ✓ Through Group Policy
  - ✓ As part of an Microsoft Deployment Toolkit (MDT) OS deployment
  - ✓ Through Configuration Manager

Планиране и изпълнение на EFS - Encrypting File Systems (EFS) е технология, която осигурява криптиране на информацията на ниво файл или директория. EFS осигурява онлайн защита на информацията само при работеща операционна система и ползва сертификати, като те могат да бъдат издадени от Certification Authority или самогенерирани от операционната система за конкретния потребител и с предназначение за EFS криптиране.

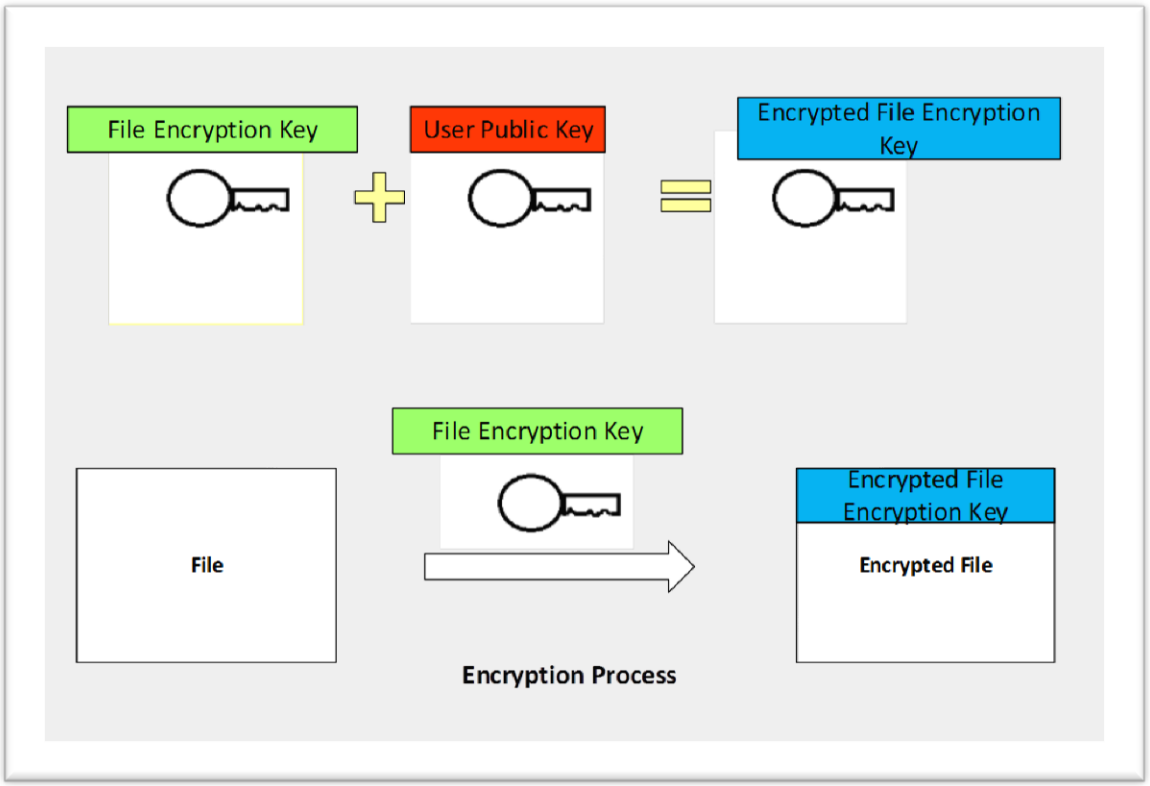
Повече информация относно EFS технологията може да намерите на адрес: https://technet.microsoft.com/en-us/library/cc962122.aspx

Предварителни изисквания за изпълнение на EFS:

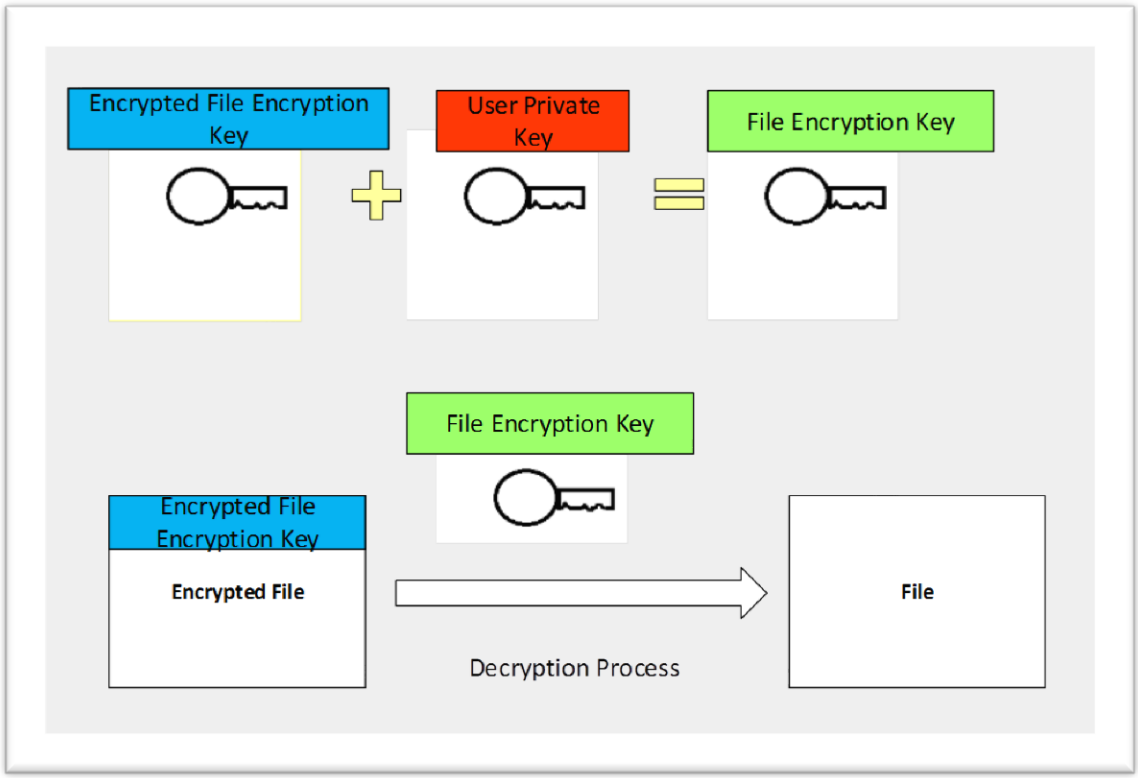
- ✓ Файлът или директорията трябва да са на NTFS форматиран дял
- ✓ Потребителят, криптиращ информацията, трябва да има *Modify* права

- ✓ Операционната система генерира в процеса на криптиране двойка ключове, като публичния се представя под формата на X.509 сертификат
- ✓ Трябва да е избран поне един *Data Recovery Agent*

Механизъм на действие на EFS криптирането:



Механизъм на действие на EFS криптирането:



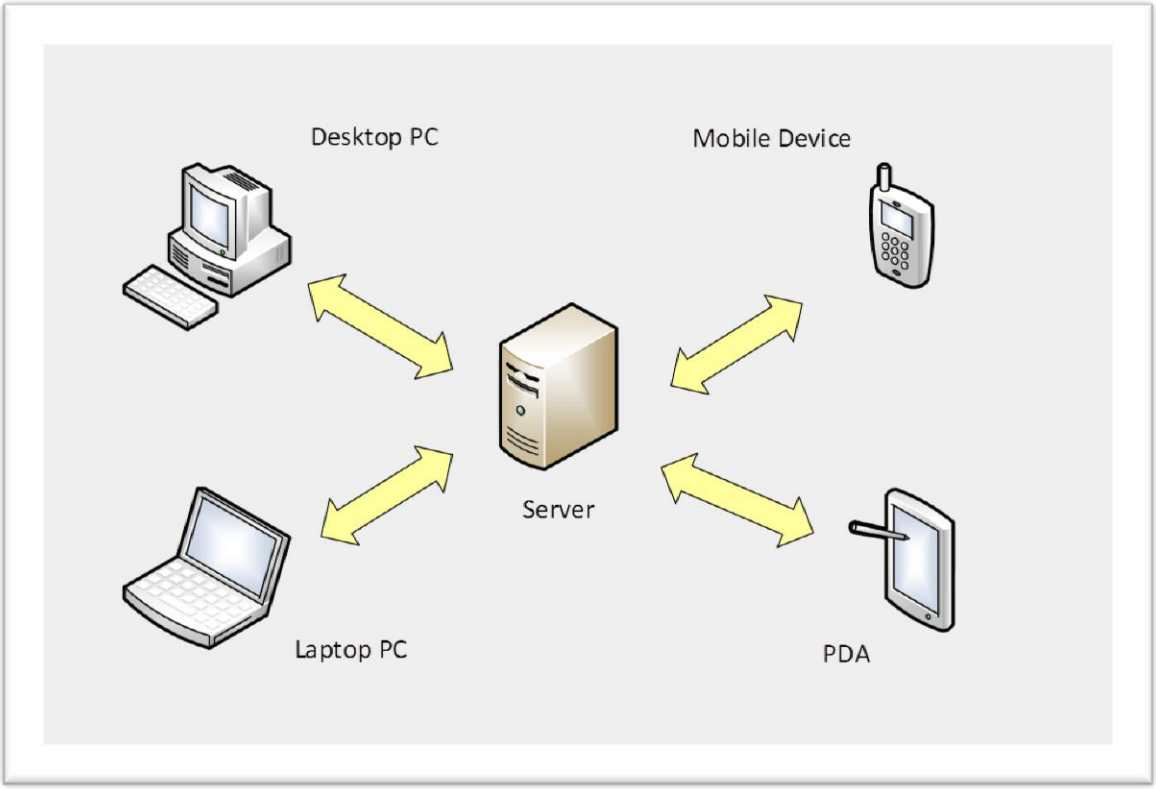
Планиране на EFS в Enterprise среда – EFS ограничава неоторизирания достъп до данни в ситуация на изгубена или откраднатa компютърна система.

- Планиране на EFS:
  - ✓ Кои файлове ще се защитават с EFS?
  - ✓ Кои потребителски акаунти ще бъдат *Data Recovery Agents*?
  - ✓ Кой е отговорен за процеса по възстановяване?
  - ✓ Кой инициира процедурата по възстановяване на данни?

3: Инсталиране и конфигуриране на Windows Server 2012:

Моделът „Клиент-Сървър“ е модел на комуникация, при който дадено устройство, наречено клиент, ползва услугите, предоставяни от друго устройство, наречено сървър.

- ✓ Сървър наричаме компютър или устройство, което осигурява услуги или ресурси в мрежата (място за съхранение на файлове; принтери; мейл-услуга).
- ✓ Клиент наричаме компютър или устройство, което ползва предоставяните от даден сървър услуги (ресурси).



Основни хардуерни компоненти на Windows Server:

- Процесор – основен компонент на компютърната техника, в основата на който стои аритметично логическо устройство, което изпълнява инструкции, генерирани от операционната система и приложенията с цел манипулиране на информация, записана в оперативната памет.
- Оперативна памет – пространство, в което се зареждат програмите като парчета код.

- Диск – дисковите устройства са място за съхраняване на информация. Съществуват различни типове дискове според типа среда за съхраняване и входно-изходните комуникационни интерфейси, например:

- дискове с магнитна повърхност за съхраняване на данните

- дискове от типа Solid State Drive, при които данните се съхраняват в EEPROM чипове от електронно независим тип.

Според типа на интерфейса, дисковете биват: IDE, ATA, SATA, SCSI, SAS и др.

- Мрежови адаптер – компонент, който осигурява мрежовата свързаност и възможността за комуникация с останалите устройства в компютърната мрежа.

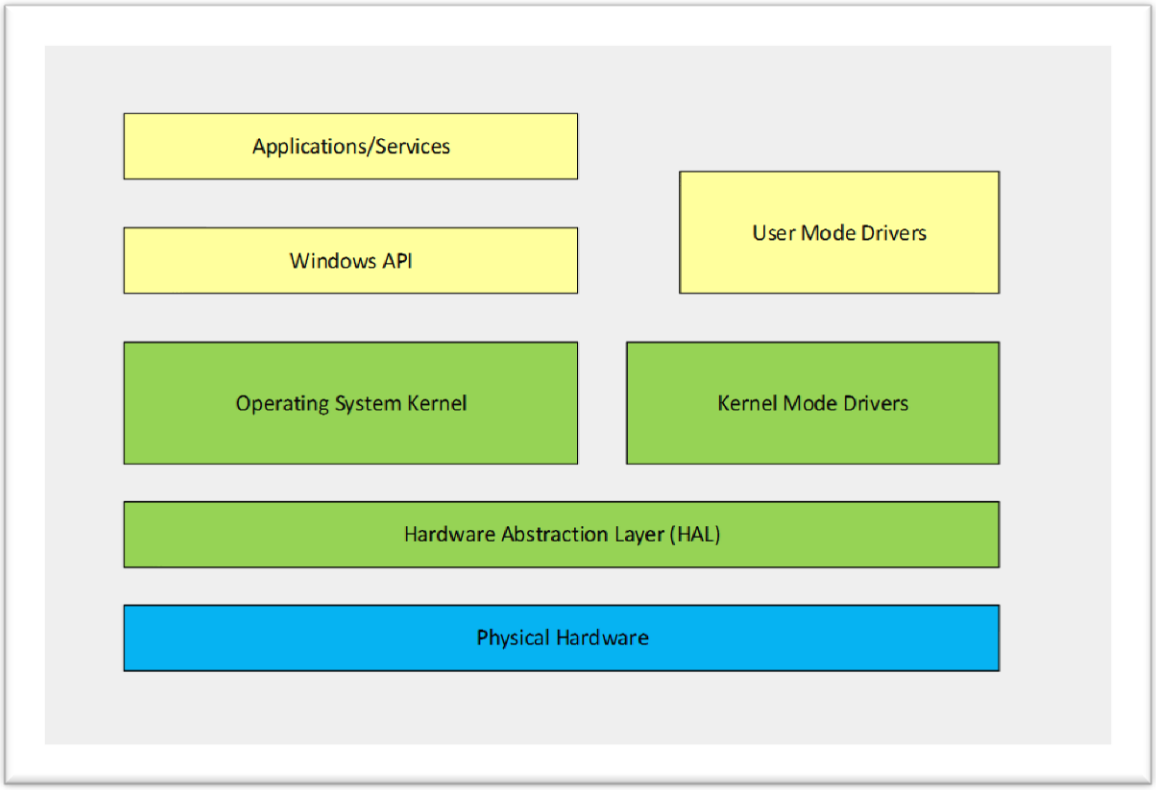
Спомагателни хардуерни компоненти на Windows Server:

- ✓ Motherboard (Дънна платка)
- ✓ Case with power supply unit (Кутия със захранващ модул)
- ✓ Fans (cooling system) (Вентилатори или специализирана система за охлаждане)
- ✓ Expansion devices (slots) (Разширителни слотове)
- ✓ Peripheral devices (Периферни устройства)
- ✓ Keyboard (Клавиатура)
- ✓ Mouse (Мишка)
- ✓ Monitor (Монитор)

Типове интерфейси за предаване на данни:

- Сериен интерфейс (serial bus) – данните се пакетират и се изпращат последователно през единичен канал. Примери за серийни интерфейси: serial port (COM port), SATA, SAS, USB, FireWire (IEEE1394), PCI,PCI express.
- Паралелен интерфейс (parallel bus) – данните се пакетират и се изпращат едновременно през няколко канала. Примери за паралелни интерфейси: LPT port, PATA, ISA, EISA, SCSI, Micro Channel, Parallel SCSI.

Софтуерна архитектура на Windows Server:



Основните версии при Windows Server 2012 са следните:

- Windows Server 2012 Standard Edition
- Windows Server 2012 Datacenter Edition
- Windows Server 2012 Foundation Edition
- Windows Server 2012 Essentials Edition

Съществуват и някои специфични версии, които имат конкретна функционалност:

- ✓ Microsoft Hyper-V Server 2012
- ✓ Windows Storage Server 2012

Методите за инсталация на Windows Server 2012 са следните:

- Инсталация от локален носител: Optical media; USB; ISO file; VHD
- Инсталация от споделена мрежова папка
- Методи за автоматична инсталация чрез ползването на Windows Deployment Services или MS System Center.

Методи на инсталация в зависимост от съществуването на инсталирана вече операционна система:

- Нова инсталация
- Подновяване – инсталиране на по-нова версия на операционната система върху вече съществуваща такава.
- Миграция – отказ от ползването на старата версия на операционната система и преминаване към по-нова такава.

Windows Server Core – версия на Windows Server 2012, при която липсва графичния потребителски интерфейс. По този начин операционната система е олекотена, което дава възможност за повишено бързодействие и намалена повърхност за атака.

За да инсталираме Windows Server Core, в процеса на инсталация трябва да изберем опцията *minimal Graphical User Interface (GUI) installation option.*

Ползи от употреба на Windows Server Core:

- ✓ Намалена употреба на ресурси
- ✓ Намалено обслужване
- ✓ Намалено администриране от потребителя
- ✓ Намалена повърхност за атаки
- ✓ Намален брой на обновяванията (Windows Updates)

Методи на администриране на Windows Server Core:

- ✓ Sconfig; netsh; Windows PowerShell
- ✓ Server Manager; Remote Server Administration Tools (RSAT)

Процесът на инсталация на Windows Server 2012 преминава в следната последователност:

- ✓ Сървърният хардуер трябва да отговаря на минималните изисквания за инсталация
- ✓ Стартирайте процеса по инсталация като стартирате **setup.exe**

- ✓ Потвърдете регионалните и езикови настройки
- ✓ Изберете **Install** или **Repair**, след което изберете версията на операционната система
- ✓ Приемете лицензионните споразумения
- ✓ Изберете типа на инсталация – **upgrade** или **custom**
- ✓ Изберете локацията на инсталиране и изчакайте процеса на инсталация да приключи
- ✓ Въведете администраторската парола

Процесът по след-инсталационно конфигуриране на Windows Server включва следните настройки:

- ✓ Активация на операционната система
- ✓ Установяване на времева зона
- ✓ Конфигуриране на компютърно име, домейн и мрежови настройки
- ✓ Добавяне на сървърни роли и функционалности
- ✓ Конфигуриране на *Windows Firewall* и *Remote Desktop*
- ✓ Мониторинг на основни събития
- ✓ Достъп до административните конзоли към всяка роля или функционалност

Стъпки в процеса на Windows Deployment Services Automatic Deployment:

- ✓ Изграждане на *Image file*
- ✓ Изграждане на *unattended answer file*
- ✓ Създаване на метод за разпространение на файловете за инсталация
- ✓ Стартиране на инсталацията от клиента

- Услуги (services) при Windows Server - услугата е стартиран изпълним файл, който работи в паметта и който изпълнява определена функция или предоставя дадена функционалност.

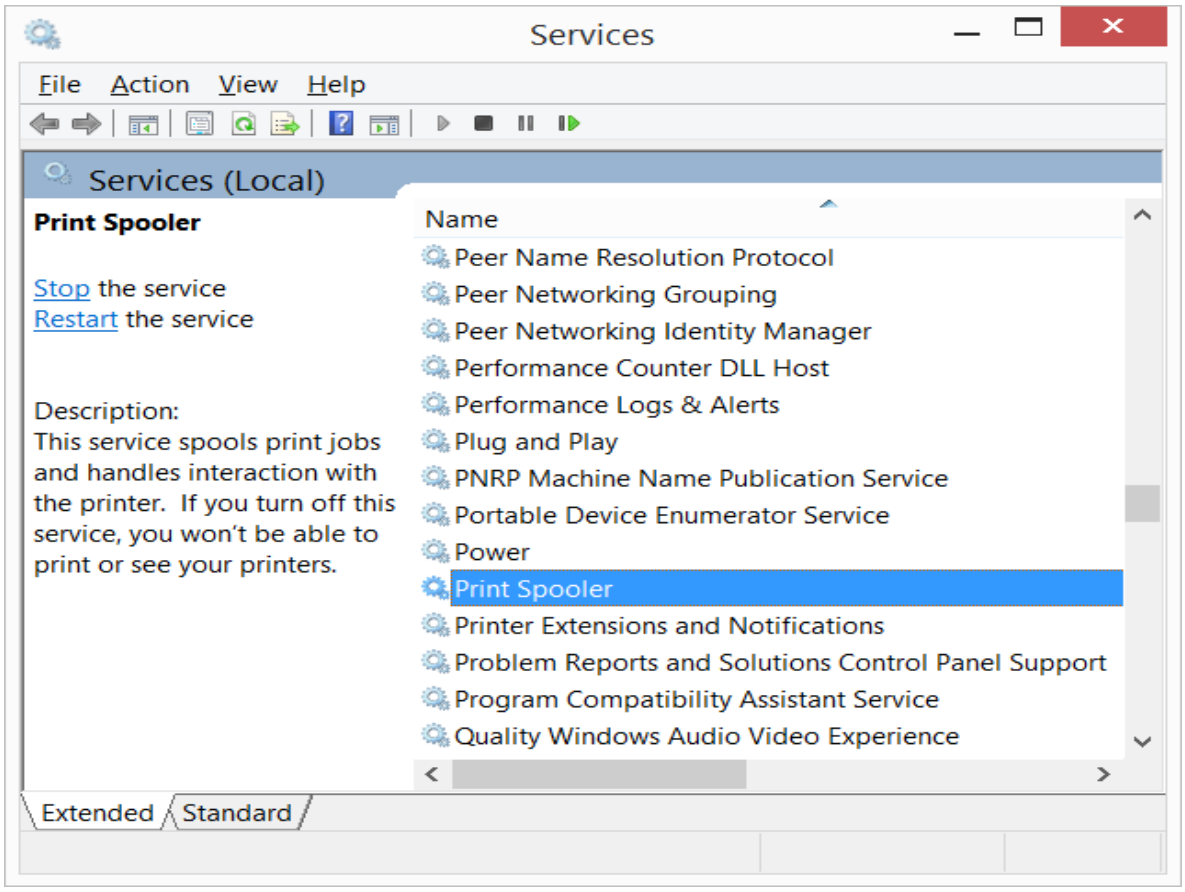
Примери за услуги:

- ✓ Print Spooler
- ✓ Task Scheduler
- ✓ Windows Time

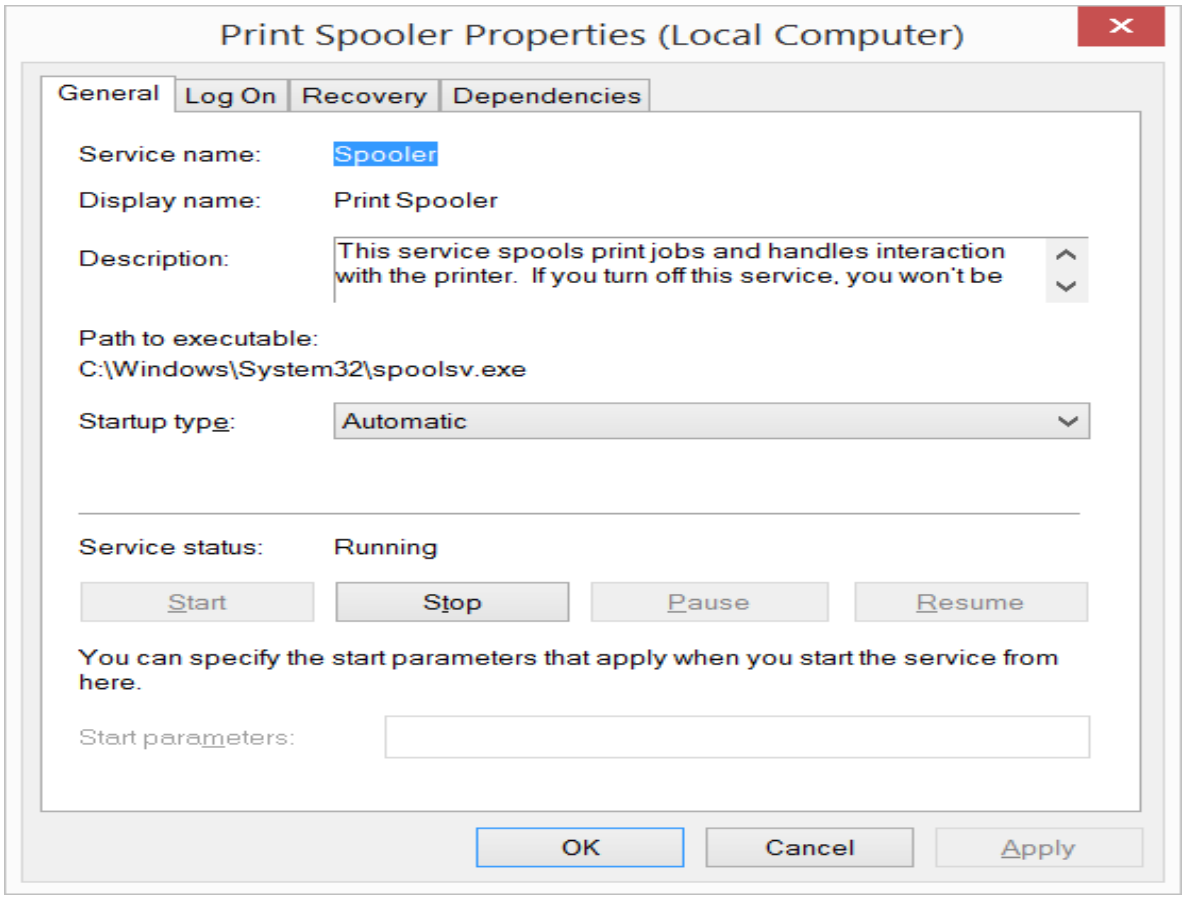
Типове услуги според метода на стартиране:

- ✓ Automatic (Automatic Delay)
- ✓ Manual
- ✓ Disabled

Конзола за управление на услугите в Windows Server:



Конфигуриране на услуга:



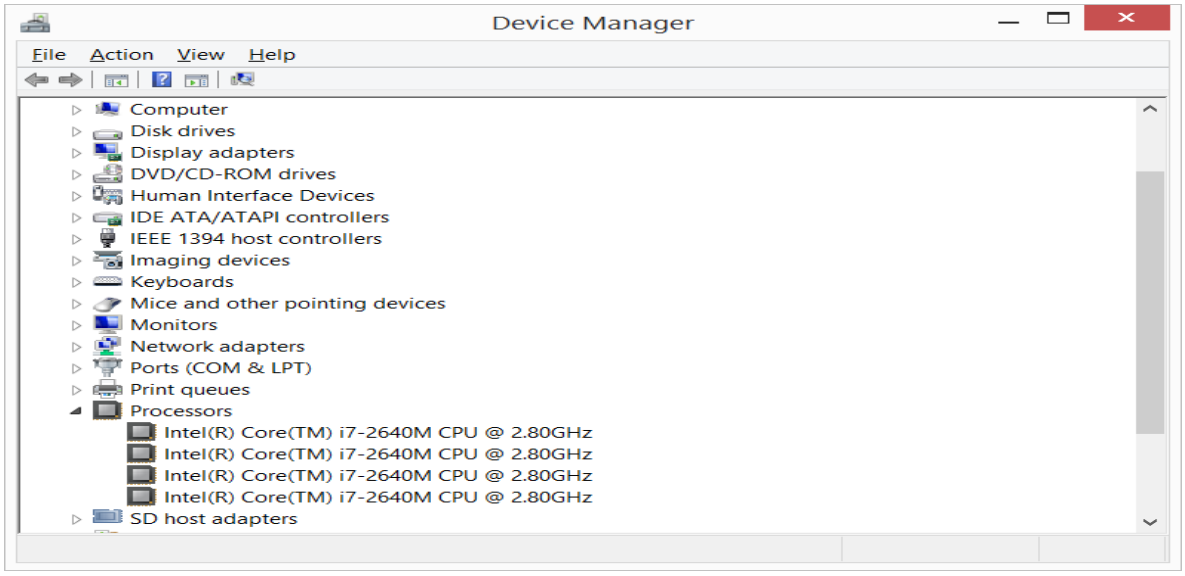
Конфигуриране на устройства и драйвъри на устройства:

- Хардуерно устройство (device) – хардуерен компонент, който изпълнява специфична функция и е инсталиран или прикачен към компютърната система. Хардуерни настройки на устройствата:
  - ✓ DMA channel
  - ✓ IRQ line
  - ✓ Memory range

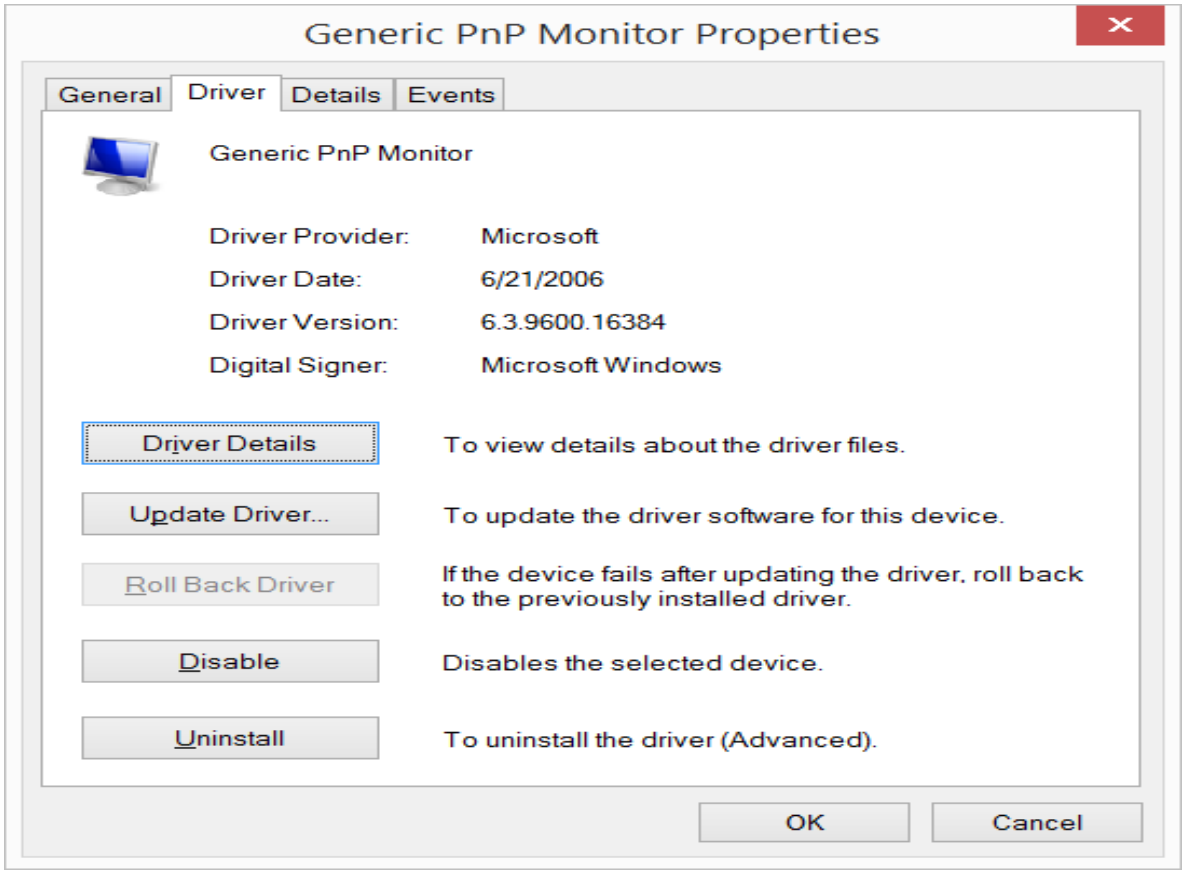
- ✓ I/O range

Plug and Play-enabled devices – позволяват автоматично конфигуриране от страна на операционната система по отношение на тези устройства.

Драйвър на устройство (device driver) – малка софтуерна програма, позволяваща на операционната система и хардуерните компоненти да комуникират с конкретното хардуерно устройство. Управлението на хардуерните устройства и техните драйвъри става през *Device Manager* конзолата.



Конфигуриране на драйвър на устройство:



4: Инсталиране на Storage в Windows Server. Технологии за съхранение на данни и конфигуриране на съхранението в Windows Server среда:

Технологии за съхранение на данни:

- Direct-Attached Storage (DAS) - това е категория, която обхваща всякакъв тип дискови устройства за съхранение на данни, които са прикачени локално към компютърната система.

Типове Direct-Attached Storage (DAS) според техния интерфейс:

- ✓ Enhances Integrated Drive Electronics (EIDE)
- ✓ Serial Advanced Technology Attachments (SATA)
- ✓ Small Computer System Interface (SCSI)
- ✓ Serial-attached SCSI (SAS)
- ✓ Solid-State Drive (SSD)

DAS характеристики:

- ✓ Лесен за конфигуриране
- ✓ Евтино решение за съхраняване на данни
- ✓ Бавно и нецентрализирано решение

- Network-Attached Storage (NAS) – устройство за съхранение на данни, което е самостоятелно, има мрежови адаптер, чрез който се свързва в мрежата, и се достъпва мрежово като споделен ресурс

NAS предимства:

- ✓ Относително евтино решение
- ✓ Лесно за конфигуриране (Web interface)

NAS недостатъци:

- ✓ Относително бавен достъп в сравнение с SAN
- ✓ Неподходящо решение за големи и сложни инфраструктури

- Storage Area Network (SAN) – специализирана високоскоростна мрежа, която свързва компютърни хостове към високопроизводителни системи за съхранение на данни. SAN може да бъде базирана на *Fibre Channel* или *iSCSI*. Fibre Channel пренася SCSI командите по кабели тип „усукана двойка“ или оптични влакна. Повече информация относно Fibre Channel технологиите може да намерите на следния адрес: http://www.fibrechannel.org/

SAN предимства:

- ✓ Централизирано място за съхраняване на данните
- ✓ Бърз достъп
- ✓ Висока степен на защита от отказ

SAN недостатъци:

- ✓ Висока цена на инфраструктурата
- ✓ Изискване за специализирани умения за конфигуриране и поддръжка

Управление на дискове и томове:

Partition Table – таблица, която отразява организацията на конкретно дисково устройство и размерите на неговите логически дялове (partitions)

Типове Partition Tables:

- ✓ Master Boot Record (MBR):

- големина на дяла до 2TB
- до четири главни дяла (primary partitions)
- не позволява запис на информация между няколко диска (striping or mirroring)

✓ GUID Partition Table (GPT):

- големина на дяла над 2TB
- до 128 дяла
- поддържа запис на информация между няколко диска едновременно (RAID)

Базови и Динамични дискове:

- Базови дискове – те могат да включват primary partitions, extended partitions или логически дискове.

✓ Primary partition наричаме дял, който функционира като физически диск и може да съдържа операционна система.

✓ Extended partition е дял, върху който могат да бъдат създадени няколко логически диска (logical drives).

✓ Logical drive наричаме диск, който е създаден в рамките на даден extended partition.

- Динамични дискове – представляват съвкупност от дискове, които оформят една обща логическа единица, с която оперира операционната система. Динамичните дискове могат да включват simple, spanned, striped, mirrored and RAID-5 volumes.
- Виртуални дискове – представляват файлове, които операционната система разглежда и манипулира като отделни физически дискови дялове. Съвременните операционни системи имат възможност да стартират от виртуални дискове (Boot from VHD).

Windows Server 2012 ползва два типа виртуални дискове:

✓ .vhd (Virtual Hard Drive) – с големина на диска до 2 TB.

✓ .vhdx (Virtual Hard Drive Extensible) – с големина на диска до 62 TB.

Типове VHD дискове:

✓ Dynamically expanding VHD – характеризират се с много ефективно използване на дисковото пространство

✓ Fixed-size VHD

- ✓ Differencing VHD – схема на организация, при която промените се отразяват на differencing диска, а base диска стои непроменен

Mount Point – препратка, сочеща към локация от диска, позволяваща операционната система да достъпва дадения ресурс директно.

Употреба на *mount points*:

- ✓ При необходимост от дисково пространство без да променяме структурата на директориите (*folders*)
- ✓ Липса на свободни букви за обозначаване на дялове (*drive letters*)

Link (връзка) – файл, който съдържа препратка към друг файл или директория (папка). Съществуват два типа връзки:

- ✓ Symbolic file link
- ✓ Symbolic directory link

Дискови квоти (storage quotas) – метод за лимитиране използването на дисково пространство, който ползва нотификация за достигнат предварително зададен праг.

Квота нотификациите могат да стартират допълнителни действия като:

- ✓ Изпращане на мейл нотификации
- ✓ Запис на събитие в *Event Viewer*
- ✓ Стартиране на команда или скрипт
- ✓ Генериране на отчет (*report*) относно

Устойчивост на откази – Windows Server 2012 поддържа следните технологии за устойчивост на откази:

- Storage Space: функционалност, която позволява да добавяме всякакви по размер или тип дискове към Storage Pool-а и така да създаваме надеждни виртуални дискове, които се управляват като единично пространство за съхраняване на информация (Storage Space).

Ползи от изграждането на Storage Space :

- ✓ Redundancy
- ✓ Thin provisioning

Полезни команди:

- ✓ Get-StoragePool
- ✓ Resize-SpacesVolume

- Redundant Array of Independent Disks (RAID) - комбинация от няколко физически диска в един логически с цел увеличаване на бързодействието и осигуряване на излишък от ресурси.

Най-използвани RAID нива:

- ✓ RAID 0 (striping)
- ✓ RAID 1 (mirroring)
- ✓ RAID 5 (striping with parity)
- ✓ RAID 10 (mirroring of striped drives)

Повече информация относно RAID технологиите може да бъде намерена на адрес: http://en.wikipedia.org/wiki/RAID

Част IV: Управление на услуги - Active Directory, DNS, DHCP и други.

1: Сървърни роли в Windows Server – Windows Server 2012 предлага няколко типа услуги и функционалности, които могат да бъдат добавени от менюто Manage на Server Manager конзолата. Тези функционалности биват няколко категории:

- Сървърна роля (server role) – описва основна сървърна функционалност. Основните роли при Windows Server 2012 са 17 на брой и те са описани в следващата таблица:

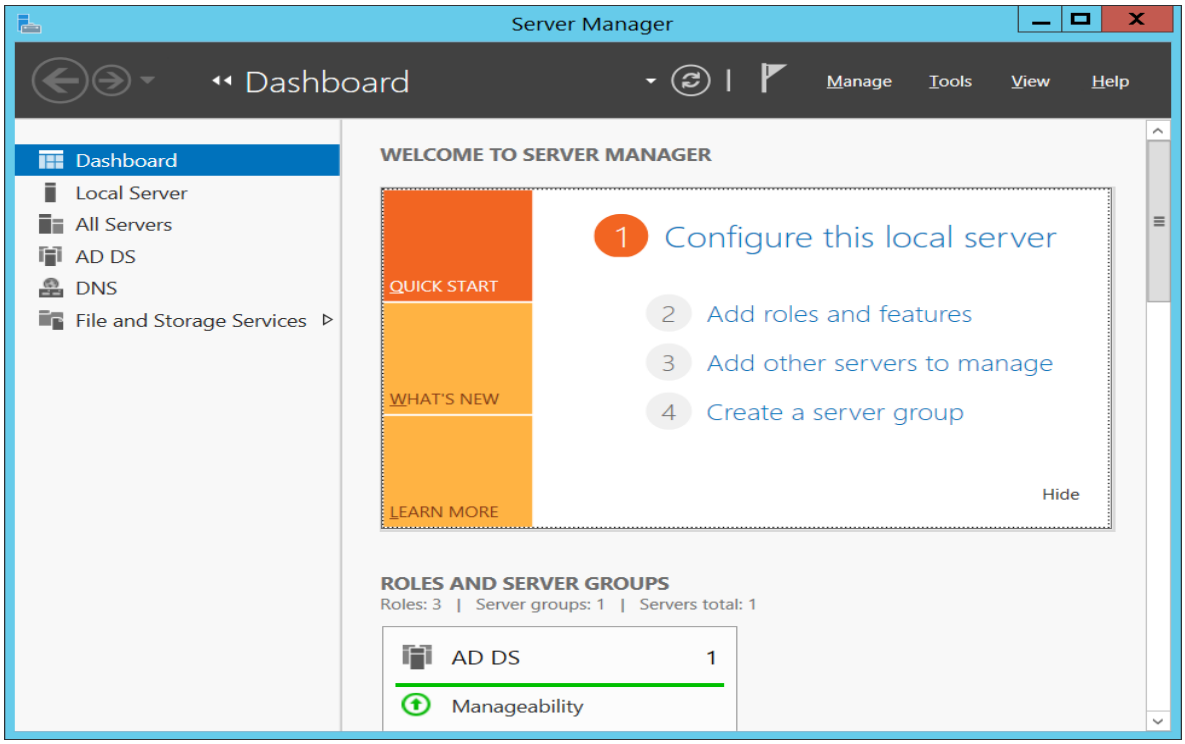
Сървърни роли в Windows Server 2012

- Допълнителни функционалности (features) – компоненти, които играят спомагателна роля по отношение на конкретна сървърна роля и обикновено не доставят услуги директно на клиентите.
  - ✓ Примери: Windows Server Backup; failover clustering
  - ✓ Features on Demand
- Ролеви услуги (role services) – те отразяват различни ролеви функционалности и могат да бъдат инсталирани и активирани отделно.

Основно място за добавяне и премахване на роли, функционалности и ролеви услуги в Windows Server 2012 е Server Manager конзолата. Тази конзола е основен инструмент на системния администратор и дава възможност за управление и мониторинг на даден сървър (или група от сървъри).

Употреба на Server Manager:

- ✓ Добавяне и премахване на роли и функционалности
- ✓ Управление на няколко сървъра в мрежата от едно централизирано място
- ✓ Управление и мониторинг на статуса на даден сървър
- ✓ Достъп до конзолите и инструментите за управление на различните сървърни функционалности (DNS; DHCP; ADDS; AD Certificate Services и др.)



Инсталиране на сървъри със специфични роли – Windows Server 2012 предлага добавяне на специфични сървърни роли, като всяка от тях активира допълнителни услуги, които могат да бъдат ползвани от потребители и приложения в дадена инфраструктура. Характеристиките на тези специфични роли, както и техните параметри, са описани както следва:

- File Server (файлов сървър) – осигурява съхранение и достъп до информация, организирана под формата на файлове и директории.

Употреба на файловият сървър:

✓ Осигурява място за съхранение на потребителските файлове

✓ Позволява споделяне на информацията между различни потребители

✓ Контролира нивото на достъп до съхраняваната информация

✓ Осигурява backup и restore на файловете с данни

- Print Server – осигурява централизирано решение за печат, при което принтерите са инсталирани на един централен сървър, като така са достъпни от всеки мрежови хост и натоварването относно подготовката на документи за печат се поема от принт-сървъра.

Ползи от Print Server решението:

- ✓ Единно място за контрол статуса на всички принтери
- ✓ Разтоварване на клиентските компютри
- ✓ Възможност за реализиране на решения за непрекъсваемост и достъпност чрез използване на *clustering* технологии

- Application Server – компютър със инсталирана сървърна операционна система, върху който се изпълняват специфични мрежово-ориентирани приложения.

Приложение на Application сървърите:

- ✓ Client-server приложения
- ✓ Web-based приложения

- Web Server (Internet Information Services - IIS) – компютър, който има директен достъп до Интернет или конкретен корпоративен Интранет, и осигурява достъп до следното съдържание:

- ✓ Static content
- ✓ Web-based applications
- ✓ Streaming content

Изисквания при инсталиране на Web Server (IIS):

- ✓ Web Server
- ✓ FTP Server
- ✓ IIS Hostable Web Core
- ✓ Management Tools

Информация относно Web Server ролята може да бъде намерена на адрес: http://en.wikipedia.org/wiki/Internet_Information_Services

- Remote Access Server – компютър, който осигурява отдалечен достъп до корпоративни ресурси на потребители или системи, които се намират извън корпоративната мрежа на дадена компания.

Примери и технологии за отдалечен достъп:

- ✓ DirectAccess
- ✓ VPN
- ✓ Network Policy Server

- ✓ Network Access Protection (NAP)
- ✓ Remote Access Dial-In User Service (RADIUS)

Microsoft сървърните операционни системи, както и сървърните роли и услуги, предлагани от тях, могат да бъдат управлявани отдалечено от клиентски компютърни системи. За целта на клиентите трябва да бъде инсталиран т.н. Remote Server Administration Tools (RSAT). RSAT е комплект от приложения, даващи възможност за отдалечено управление на Windows - базирани сървъри от компютър с инсталирана клиентска операционна система.

Специфики при RSAT версиите:

- ✓ Windows Server 2008/2008R2 могат да се управляват само от Windows 7 клиент с инсталиран RSAT.
- ✓ Windows Servers 2012/2012 R2 могат да се управляват само от Windows 8 клиент с инсталиран RSAT.

- Hyper-V Role – Windows Server 2012 роля, позволяваща създаването и управлението на виртуални инстанции (машини) с различни операционни системи и приложения върху тях. Hyper-V ролята дава възможност за виртуализиране на цялостна инфраструктура, като осигурява надеждност, бързодействие и изолиране на отделните ресурси и услуги.

Изисквания за имплементиране на Hyper-V:

- ✓ процесори с x64 архитектура и хардуерна виртуализация
- ✓ Data Execution Prevention (DEP)
- ✓ Технологии, осигуряващи излишък от ресурси по отношение на дисково пространство, мрежови адаптери, процесорна мощ и оперативна памет.

Hyper-V е основа за редица Microsoft технологии за виртуализация:

- ✓ Server Virtualization
- ✓ Desktop Virtualization
- ✓ Remote Desktop Services and Virtual Desktop Infrastructure
- ✓ Application Virtualization
- ✓ User-state Virtualization
- ✓ Integration with System Center family products for scalability and efficiency

Съображения при избора на сървърни роли – водещият принцип при избора и реализацията на сървърни роли е базиран на собствеността върху ресурсите и отговорността относно тяхната поддръжка. Различаваме три типа инфраструктурни решения, при които имаме напълно различен модел на собственост и поддръжка на инфраструктурните системи:

- On-Premise услуга– тип ресурс, който е собственост на дадена организация и е изцяло под нейн контрол и поддръжка.

Употреба на On-Premise ресурси:

- ✓ Infrastructure services
- ✓ Shared files and printers
- ✓ Hosted applications
- ✓ Systems for Network access
- ✓ Application updates and operating systems deployment

- Cloud Services (облачни услуги) – модел на отдалечено осигуряване на инфраструктурни системи и услуги на компании с цел намаляване или елиминиране на локално ползваната собствена инфраструктура и разходите за нейното управление.

Категории облачни услуги:

- ✓ Infrastructure as a Service (IaaS)
- ✓ Platform as a Service (PaaS)
- ✓ Software as a Service (Paas)

- Hybrid Services (хибридни услуги) – при този модел, част от инфраструктурата се намира в организацията и е под нейн контрол и поддръжка, а друга част е изнесена в облака под формата на облачни услуги.

2: Въведение в директорийните услуги (Active Directory Domain Services – AD DS):

Общ преглед на директорийните услуги, реализиране в среда на Windows Server 2012:

Определение на понятието „Директорийни услуги“ - директорийните услуги представляват метод на управление достъпа до ресурси в дадена организация, който се базира на следните физически и логически компоненти:

- ✓ Логически компоненти: Domain; Domain trees; Schema; Partitions; Forests; Sites; OUs; Containers
- ✓ Физически компоненти: Domain controllers; Data stores; Global catalog servers; RODCs

Microsoft имплементацията на директорийни услуги се нарича Active Directory (Активна Директория) и се реализира чрез добавяне на сървърната роля, наречена Active Directory Domain Services (AD DS) при Windows Server 2012.

Технологии и инфраструктурни решения, подпомагащи AD DS: Domain Name System (DNS); Dynamic Host Configuration Protocol (DHCP); Group Policy.

Основни понятия при Active Directory (Активна Директория):

- AD DS Domain – контекстна среда, в която се създават и съществуват всички потребителски, компютърни акаунти и групи, които отразяват физическите обекти в дадена организация.

  Характеристики на домейн средата:

  ✓ Изисква поне един домейн-контролер

  ✓ Всички домейн-контролери притежават редактируемо копие на базата-данни на домейна

  ✓ Домейнът е репликационна граница

  ✓ Домейнът е административен център за конфигуриране и управление на обекти

  ✓ Домейнът осигурява защитен достъп до ресурсите като автентикира и контролира потребителите или приложенията

  ✓ Домейнът се създава с промотирането на първия домейн-контролер

  ✓ Домейнът е:

  - Административна граница
  - Репликационна граница
  - Автентикационна граница

- Организационни единици (Organizational Units - OUs) – организационните единици са обекти от контейнерен тип, които се използват за групиране на

обекти в даден домейн. Обикновено организационните единици са отражение на структурата на дадена компания. Организационните единици създават йерархична структура в домейна, която е базирана на:

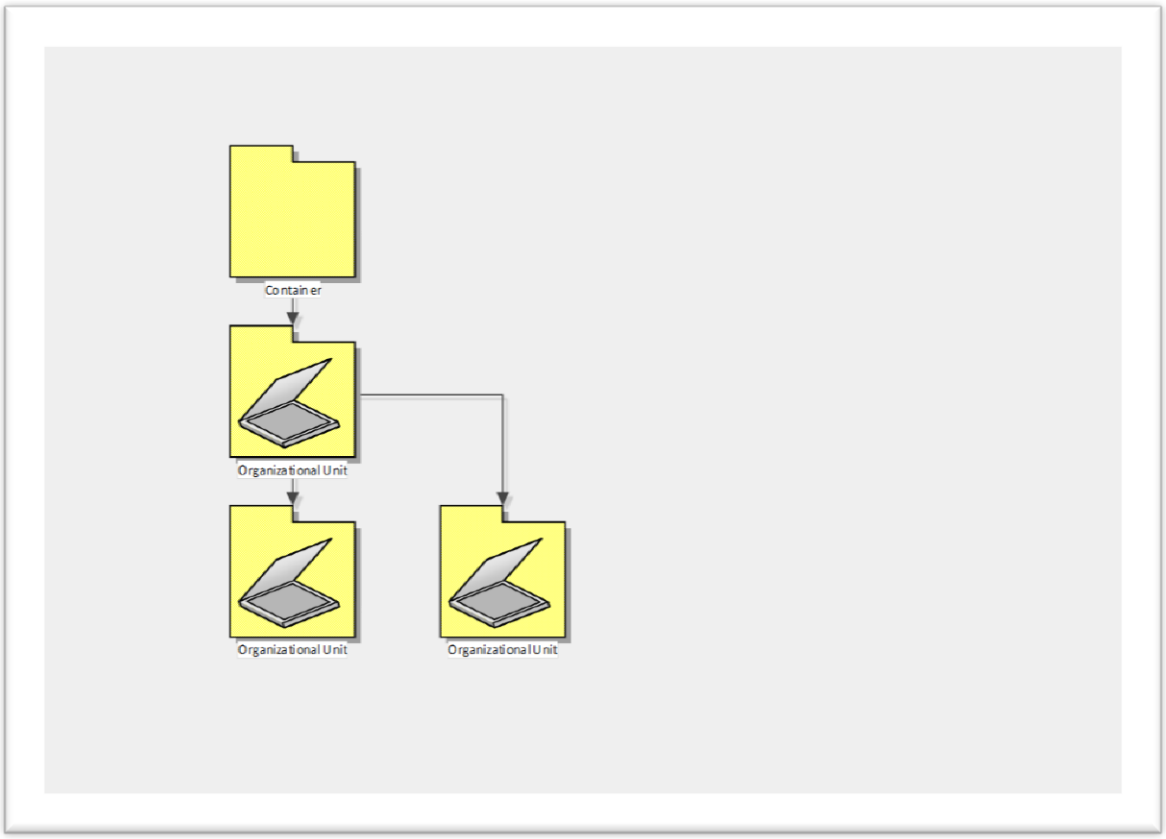
- географски принцип
- подразделения в компанията (организацията)
- ресурси
- изисквания за управление и контрол

Употреба на организационни единици (OUs):

- ✓ Конфигуриране на обекти чрез създаване и активиране на *Group Policy Objects (GPOs)*
- ✓ Делегиране на административни права

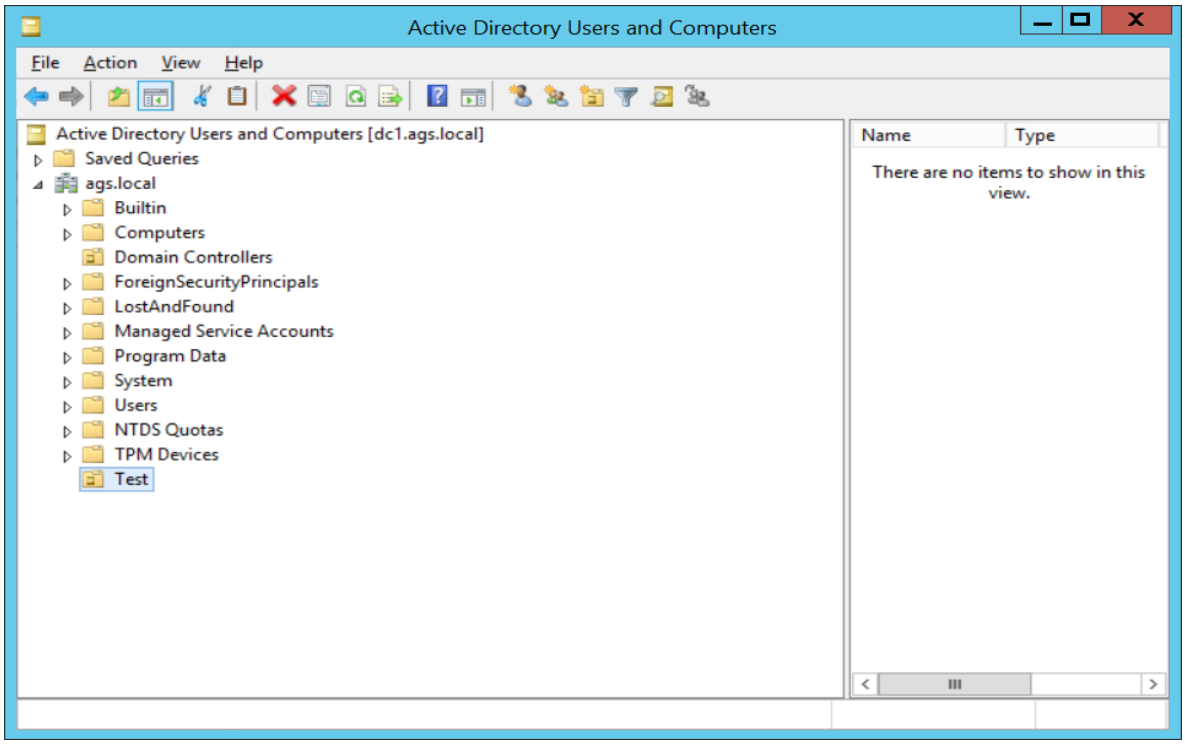
Визуализация на контейнери и организационни единици:

- ✓ Организационни единици – представени са като папка с книга върху нея
- ✓ Контейнери – представени са като празна папка



Разлика между контейнери и организационни единици – основната разлика е във възможността да се прилагат групови политики. Системните администратори в дадена компания могат да прилагат групови политики, като закачват създадените Group Policy обекти към предварително създадените организационни единици. Върху контейнерите не може директно да се закачват Group Policy обекти. Ако искаме да приложим определени политики върху контейнерите в активна директория, то трябва да отразим съответните промени в т.н. Default Domain Policy.

Следващата снимка от екран показва структурата на Active Directory, като обектите, визуализирани с празни папки са контейнери, а тези, визуализиране като папка с книга върху нея са организационни единици.



- AD DS Tree (дърво) – съвкупност от един или няколко домейна, които споделят граничещо именно пространство (name space). При дърветата имаме логическо йерархично групиране на домейни, което се създава чрез връзка (*relationship*) между отделните домейни и йерархично подреждане на домейн имената (*DNS namespace*).

- AD DS Forest (гора) – съвкупност от няколко дървета (trees) в дадена домейн структура, които споделят обща схема и глобален каталог. Първият домейн, създаден в дадена гора, се нарича forest root domain.

Характеристики на AD DS Forest:

✓ Replication Boundary for the configuration and schema partitions in the AD DS database.

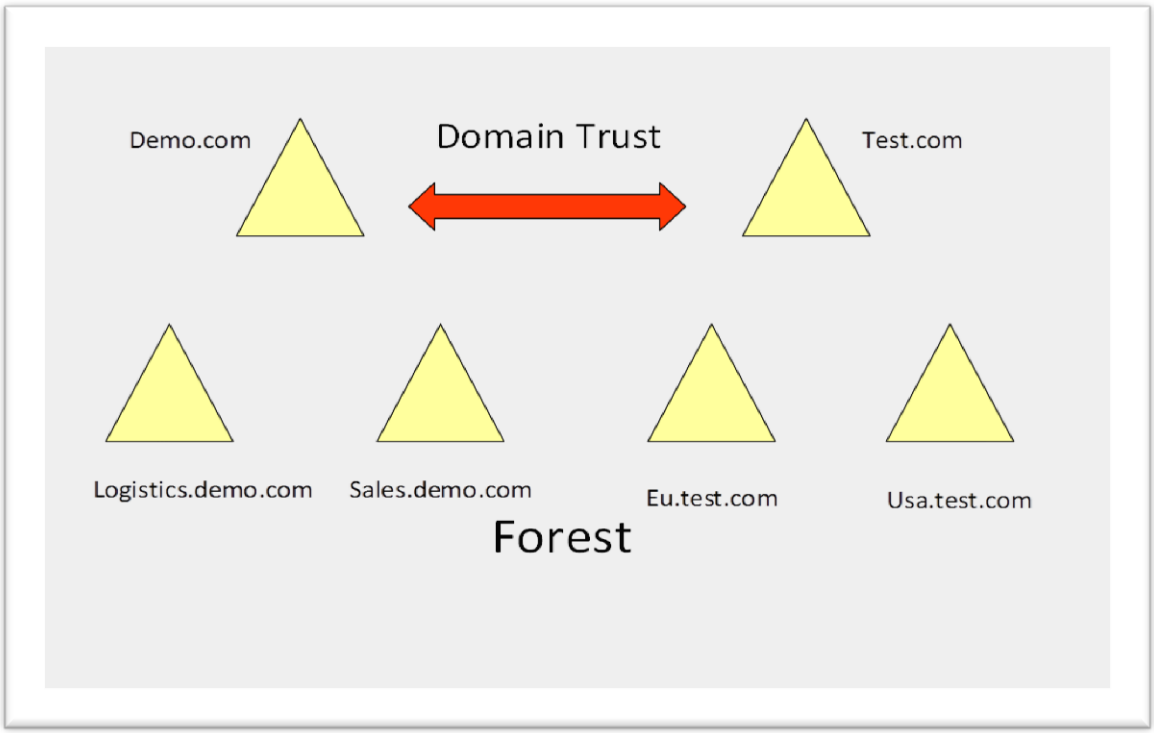
✓ Най-високото ниво в AD DS йерархията

✓ AD DS гората е граница по отношение на сигурността (*security boundary*)

✓ Стандартно при имплементация на AD DS се изгражда една гора

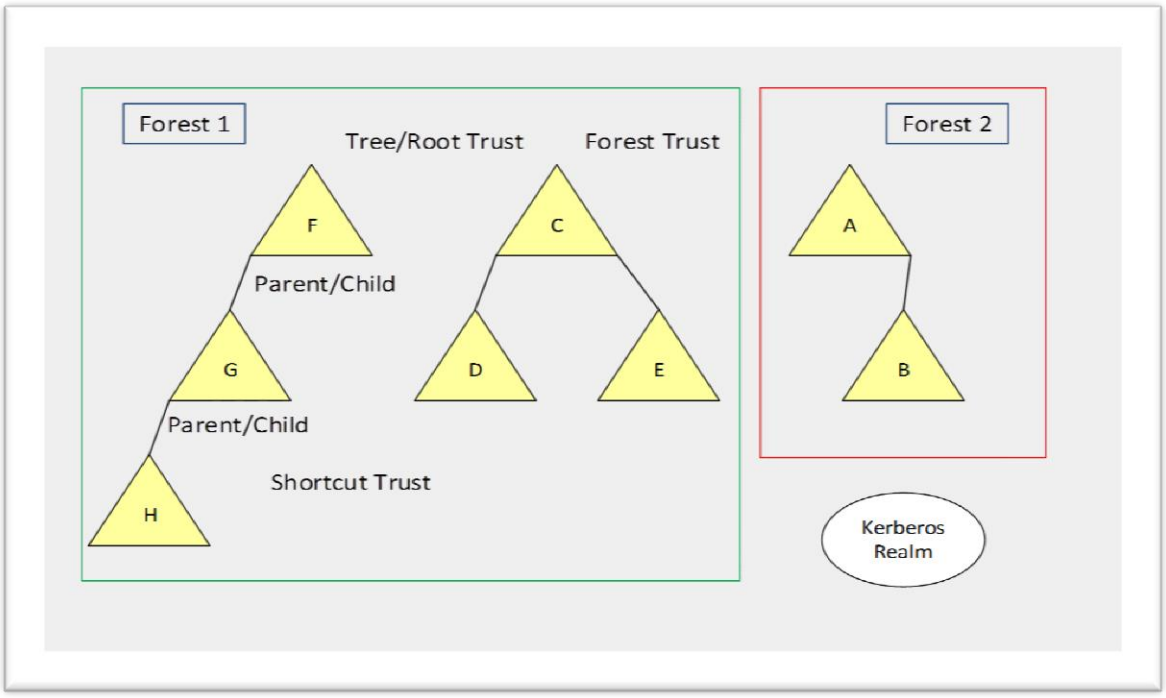
✓ Forest-wide operations master roles:

- Domain naming master
- Schema master



- Trust Relationship е форма на логическа връзка между домейни, която дава възможност за взаимно достъпване на ресурси между домейните. Съществуват различни форми на trust relationship:

✓ Forest trust
✓ Parent/Child trust
✓ Shortcut trust
✓ External trust
✓ Realm trust



- AD DS Schema – схемата, по която са създадени и организирани класовете обекти и техните атрибути в AD DS. AD DS schema е гръбнака на активната директория.

Примери за класове обекти:

- Users
- Computers
- Organizational Units

Примери за атрибути на обектите:

- User name
- Password
- Member
- DNS Hostname

- Домейн-контролер (Domain Controller) – сървър, на който е инсталирана Active Directory Domain Services (AD DS) ролята и който притежава редактируемо копие на базата на активната директория (Ntds.dit) и папката SYSVOL. Домейн контролерът е роля, която има следните функции:

✓ Осигурява и контролира процесите по автентикация и оторизация
✓ Участва в процеса по репликация на базата на активната директория и *GPO* обектите
✓ Изпълнява функцията на *Global Catalog*
✓ Осигурява *multi-master* модел на администриране на *Active Directory*

Характеристики на домейн-контролерите:

✓ Промотиране на домейн-контролер (обявяването му като носител на базата на активната директория и делегирането му на контрол относно достъпа до ресурси)
✓ Осъществяване на процеса по автентикация чрез *Kerberos authentication service* и *KDC services*
✓ Достъпност на *AD DS* услугата чрез промотирането на поне два домейн-контролера
✓ High Availability
✓ Disaster Recovery of AD DS
✓ RODC
✓ BitLocker

- Read-Only Domain Controller – има следните функции и характеристики:

✓ Притежава *read-only* копие на базата на активната директория

✓ Не инициира репликации, а само приема реплицирани промени в активната директория

✓ Осигурява високо ниво на сигурност по отношение автентикация и достъп до ресурси в офис-клонове и периметър мрежи с относително ниска физическа защита

✓ Не може да е носител на *FISMO* роля

✓ Не може да изпълнява ролята на репликационен сървър

- Глобален Каталог (Global Catalog) – функционалност на домейн-контролера, която се характеризира със следното:

✓ Глобалният каталог съдържа пълно копие на всички обекти и техните атрибути от домейна, в който той функционира, и частично копие на обектите на всички домейни и съвкупност от дървета (гори), на който неговият домейн вярва.

✓ Отговаря на заявките за намиране на конкретен обект или обекти на ниво forest

- Flexible In-line Single Master Operation (FISMO) Roles - роли на ниво домейн или гора, които са уникални и се изпълняват от конкретни домейн-контролери.
  ✓ Forest-wide roles:

- Domain naming master – носителят на тази роля отговаря за именоването на новосъздадените домейни.

- Schema master – всички промени по схемата на Active Directory могат да бъдат реализирани само върху schema master домейн контролера

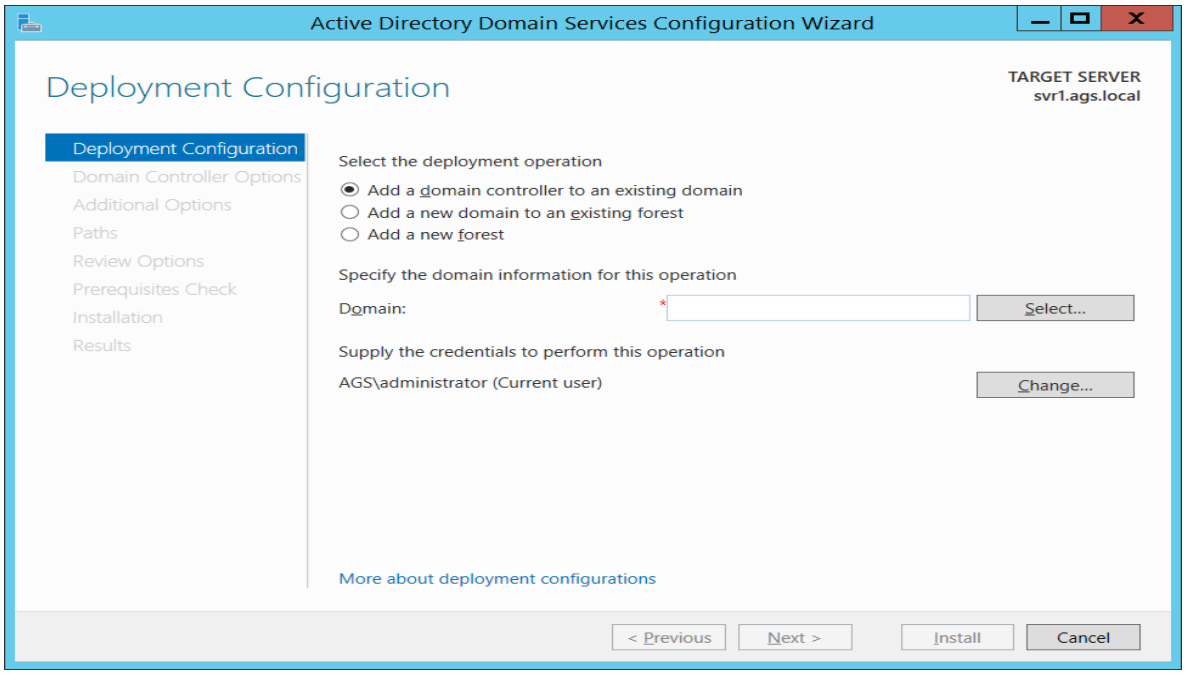
  ✓ Domain-wide roles:

- PDC Emulator – носителят на тази роля отговаря за синхронизиране на времето в целия домейн, предизвиква т.н. Urgent replication при събития, касаещи компютърни или потребителски акаунти и е локация по подразбиране за промени в Group Policy.

- RID master – тази роля е свързана с разпределянето на RID pools.

- Infrastructure master – роля, свързана с обновяването членството на универсалните групи в мулти-домейн среда.

- Инсталиране на домейн-контролер – инсталацията и промотирането на домейн контролер в среда на Windows Server 2012 се осъществява от Server Manager конзолата.



- Инсталиране на домейн-контролер върху Server Core – съществуват два метода:

  ✓ Метод 1: Използване на *Server Manager* на предварително инсталиран *Windows Server 2012 with Graphical User Interface (GUI)* за свързване към *Server Core* машината:

  1. Инсталиране на *AD DS* роля

  2. Промотиране на машината като домейн-контролер от *AD DS Configuration Wizard*

  ✓ Метод 2: Използване на *Windows PowerShell* локално, или отдалечено през *WinRM*:

  1. Инсталиране на *AD DS* с командата:

  Install-WindowsFeature AD-Domain-Services

  2. Промотиране на домейн-контролера с командата:

  Install-ADDSDomainController

- Upgrade на домейн-контролер – възможните опции са:

✓ In-place upgrade from Windows Server 2008 to Windows Server 2012:

- Ползи: Всички инсталирани приложения и файлове остават непроменени по време на процеса на *Upgrade*

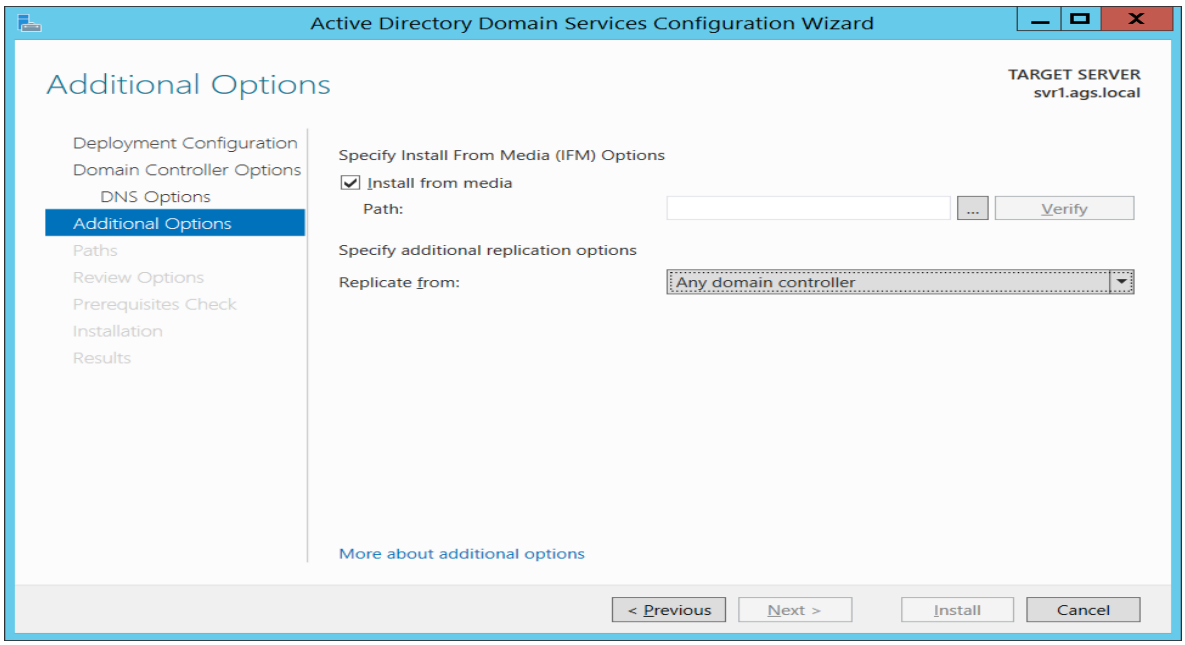
- Недостатъци: Могат да останат стари и повредени файлове и динамично-свързани библиотеки

✓ Introducing a new Windows Server 2012 server into the domain and promoting it to a domain controller

- Ползи: Новият сървър няма стари файлове по дисковото пространство

- Недостатъци: Допълнителна работа по мигриране на файлове и настройки

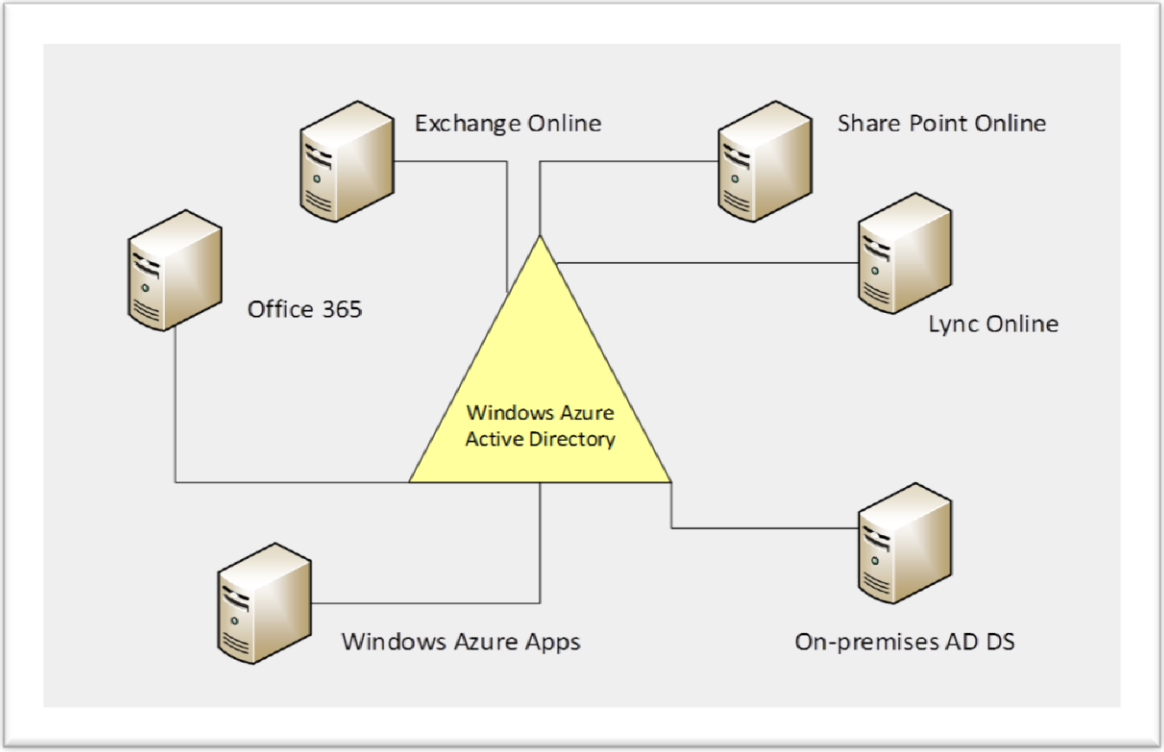
- Инсталиране на домейн-контролер чрез използването на опцията “Install from Media”



Реализиране на Активна Директория в среда на Windows Azure – Windows Azure е cloud-базираната среда за реализация на облачни услуги на Microsoft. Съществуват няколко типа изнесени облачни услуги, които са алтернатива на същите услуги, но реализирани в частна среда.

Най-известните Microsoft облачни услуги са:

- Windows Azure Active Directory
- Office 365
- Exchange Online
- Share Point Online
- Lync Online



Особеностти при Windows Azure имплементациите:

- ✓ Windows Server 2012 е „cloud and virtualization-ready“
- ✓ Rollback промени и възможност за връщане към предишни състояния на дадена виртуална среда
- ✓ Лимит на ресурси
- ✓ Времевата синхронизация на виртуалните машини

- ✓ Single point of failure (Централно място за отказ на дадена услуга)
- ✓ Потребителят не знае къде географски се намира неговата информация в облака
- ✓ На потребителя не може да се гарантира липсата на неоторизиран достъп до неговите ресурси

- Новости при Windows Server 2012 Active Directory:

  ✓ Лесно откриване в случай на домейн-контролер, който е възстановен от *snapshot rollback*

  ✓ Инсталиране и конфигуриране на клонирани виртуални машини

  ✓ Употреба на *Windows PowerShell* скриптове за автоматизация на инсталацията

  ✓ Строг контрол върху достъпа до ресурси

  ✓ Възстановяване на изтрити директорийни обекти от *AD DS Recycle Bin*

  ✓ Употреба и управление на т.н. „*RID pool*”

  ✓ Dynamic Access control – метод на контрол на достъпа до ресурси, който ползва не само потребителско име и парола, но и редица други атрибути на потребителските акаунти

- Новости при Windows Server 2012 R2 Active Directory:

  ✓ Workplace Join – позволява регистрирането на частни потребителски устройства в домейна

  ✓ Web Application Proxy – дава възможност за публикуване на приложения от домейна в Интернет

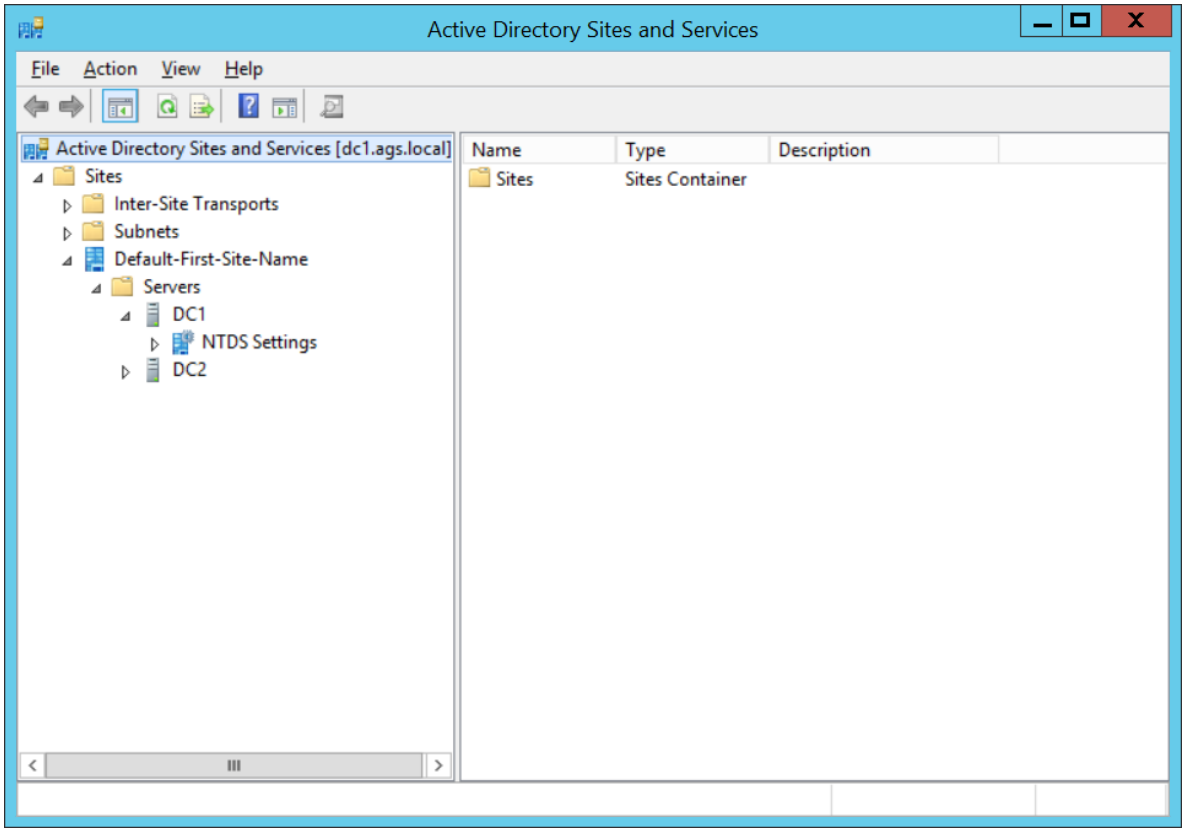
  ✓ Multi-factor Access Control – позволява генерирането на твърдения (*claims*) за даден обект на база различни негови атрибути

  ✓ Multi-factor Authentication – създава условия за внедряване на многофакторна автентикация

3: Изграждане на активна директория (AD DS):

- AD DS Sites – сайтовете са използват за логическо представяне на физическата мрежа.
- Site Links – логически връзки, които отразяват физическата свързаност между отделните сайтове.

- AD DS Replication – репликацията е процес на уеднаквяване на Active Directory данните между отделните сайтове и съответните домейн-контролери в тях.
- AD DS сайтовете и връзките между тях се управляват през специална административна конзола, наречена AD Sites and Services.



- DNS интеграция в AD DS:

  ✓ DNS се инсталира като част от процеса по инсталация на първия домейн контролер в даден домейн

  ✓ Интеграцията между DNS и AD DS е препоръчителна и необходима по отношение на т.н. “secure dynamic updates”

  ✓ Необходимост от употребата на няколко DNS сървъра с цел непрекъсваемост на услугата и разпределение на DNS трафика

  ✓ Процесът по намиране на домейн-контролерите от компютрите в домейна се осъществява с помощта на SRV записите, поддържани от DNS сървъра

Инструменти за администриране на Активна Директория чрез използването на Windows PowerShell:

- Active Directory Administrative Center Windows PowerShell History Viewer:
  - ✓ Показва *GUI* командите в *Windows PowerShell* формат
  - ✓ Позволява автоматизация на ежедневните административни задачи
- AD DS Configuration Wizard – позволява експортиране на инсталационните настройки за последваща употреба или преглед
- AD DS Module for PowerShell:
  - ✓ повече от 10 команди за *Install/Uninstall*
  - ✓ повече от 50 команди за администриране на *AD DS*

Основни обекти в Active Directory:

- Потребителски акаунт (user account) – обект в *Active Directory*, който отразява реален потребител в дадена организация.

Атрибути на потребителски акаунт – те съдържат информация за конкретния потребител, например: потребителско име, парола, адрес, телефон, звено, в което потребителя работи и др.

Потребителският акаунт позволява ползване на дадена система от даден потребител. Чрез контролиране статуса на акаунта, ние контролираме достъпа на потребителя до *Active Directory* средата .

- Група (group account) – колекция от потребителски акаунти, компютърни акаунти, контакти или други групи, която дава възможност за управление на тези акаунти като едно цяло.

Видове групи според целта на употреба:

- ✓ Security – ползват се за контрол на достъпа до ресурси. Могат да притежават различни права върху даден ресурс. Могат да се ползват за мейл дистрибуция.
- ✓ Distribution – ползват се за мейл-услуги и не могат да се ползват за контрол на достъпа до ресурси.

Видове групи според периметъра им на действие:

- ✓ Domain local
- ✓ Global
- ✓ Universal

Обхвати на групите – обхвата и членството на отделните видове групи е отразен в следната таблица:

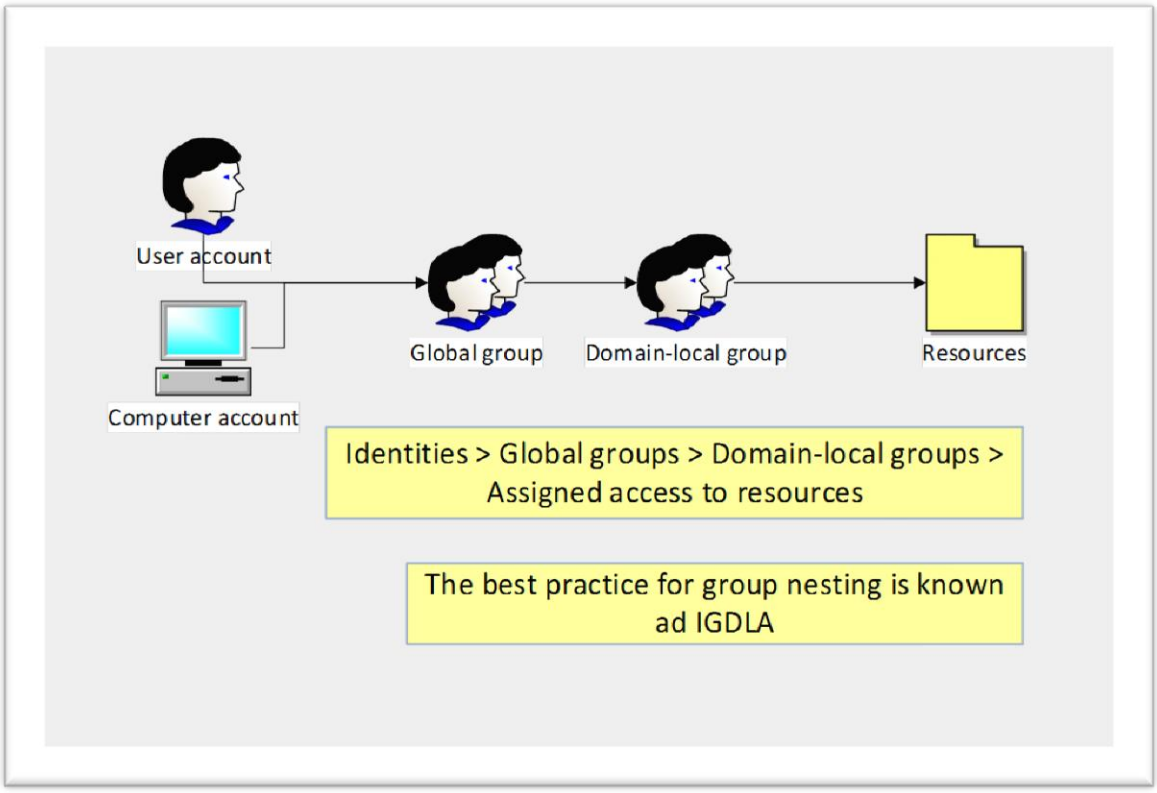
Group Scope	Member from same domain	Members from domain in same forest	Members from trusted domain	Can be assigned permission to resources
Local	U, C, GG, DLG, UG, local users	U, C, GG, UG	U, C, GG	On the local computer only
Domain-local	U, C, GG, DLG, UG	U, C, GG, UG	U, C, GG	Anywhere in the domain
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

Group Nesting – процес по добавянето на група в група. Така дадена група става член на групата, в която е добавена.

Стратегия при Group Nesting в големи организации: Accounts>Global>Universal>Domain Local>Permissions

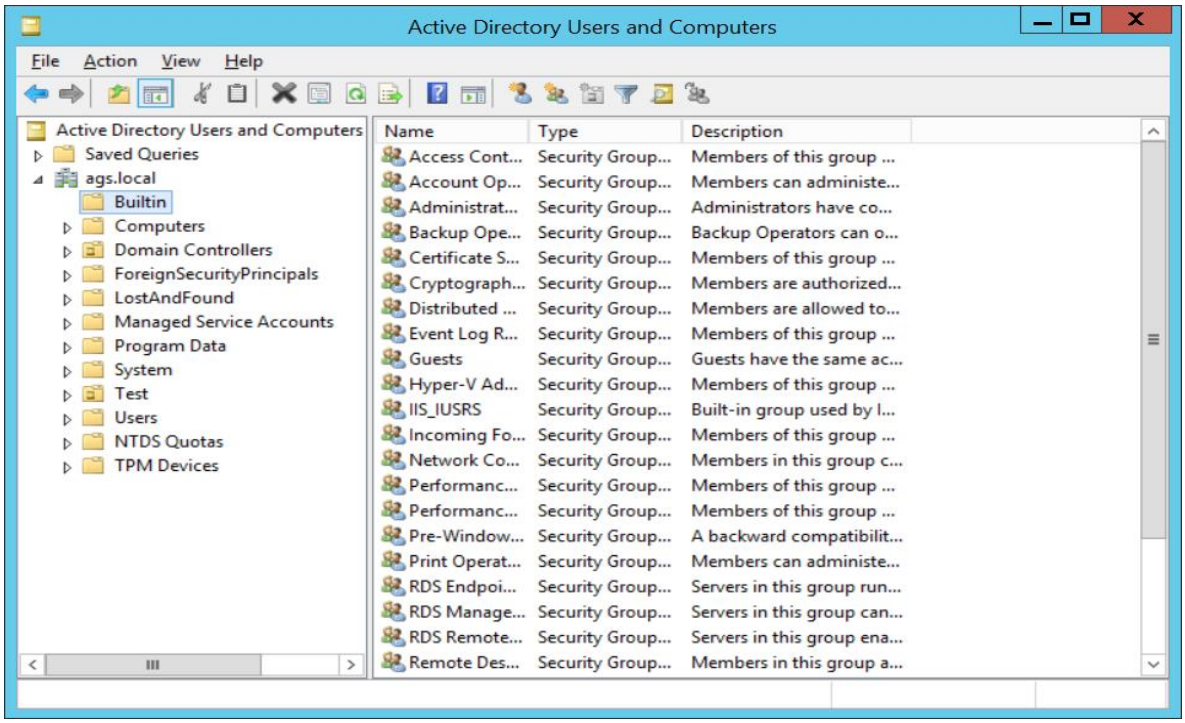
Добри практики при управлението на групи - при управлението на групи е желателно ползването на модела IGDLA (Accounts>Global>Domain Local>Permissions), при който потребителските или компютърни акаунти стават членове на глобални групи, глобалните групи стават членове на домейн-локални групи и назначаваме достъп до ресурсите на база домейн-локални групи.



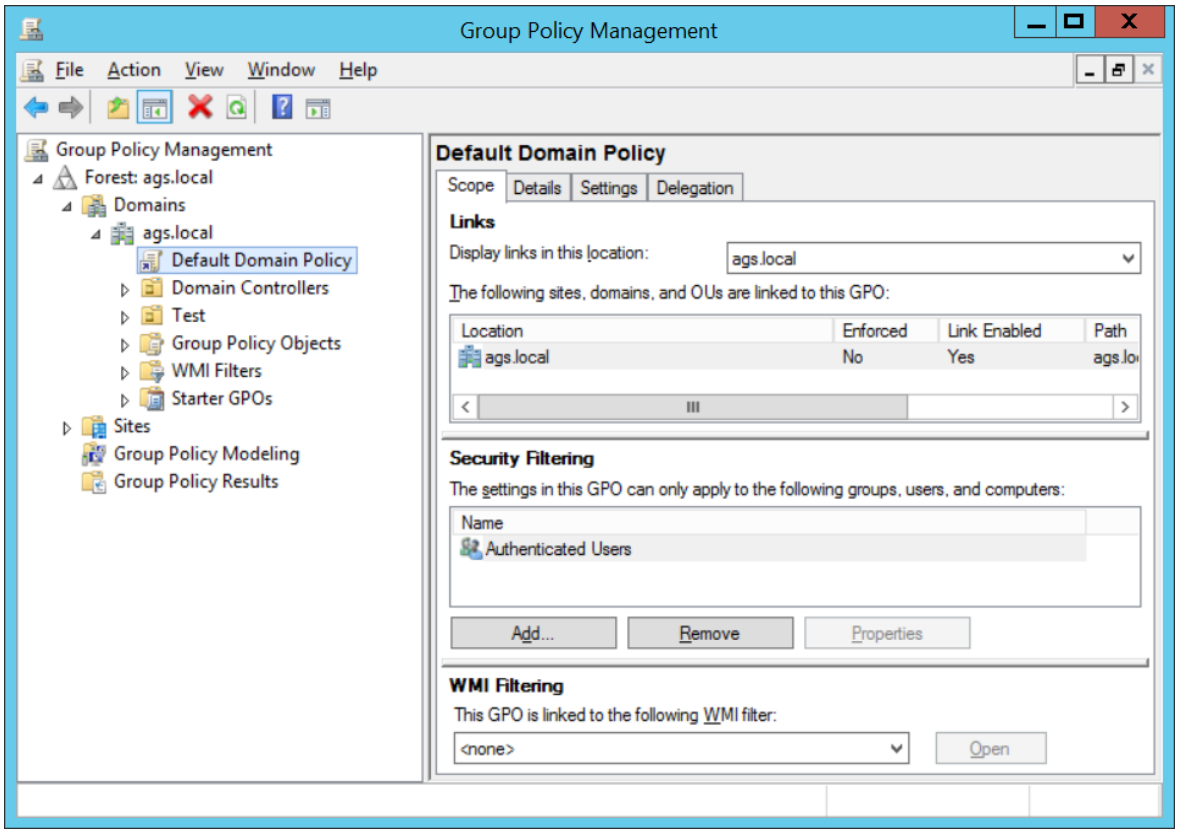
Default Build-in groups (Групи по подразбиране) – това са групи, които са предварително създадени в процеса на инсталиране на Active Directory и се ползват наготово с цел улеснено администриране. Тези групи са:

- ✓ Enterprise Admins
- ✓ Domain Admins
- ✓ Administrators
- ✓ Server Operators
- ✓ Account Operators
- ✓ Backup Operators
- ✓ Print Operators

Съществуват и т.н. „специални групи“, като членството в тези групи се контролира от операционната система. Такива групи са Anonymous Logon; Interactive; Everyone; Authenticated Users; Creator Owner.



- Компютърни акаунти (computer accounts) – обекти в *Active Directory*, които отразяват компютрите, членове на конкретния домейн. Всеки компютър в домейна притежава компютърен акаунт с уникално име и *Security Identifier (SID).*
- Добри практики при управлението на акаунти в Active Directory:
  - ✓ Не позволявайте споделянето на акаунти между потребителите
  - ✓ Планиране на *naming convention* за именоване на акаунтите
  - ✓ Използвайте вградените групи където е възможно
  - ✓ Реализирайте *Group Nesting* за по-голяма ефективност
  - ✓ Избягвайте даването на права директно на потребители вместо на групи
  - ✓ Ограничете броя на потребителите, които могат да създават акаунти в домейна
  - ✓ Въвеждайте *Managed By* и *Location* полетата на акаунтите
- Групова политика (Group Policy) – технология, която позволява автоматизирано управление и контрол на големи групи обекти в Active Directory. Създаването и управлението на Group Policy обекти става през Group Policy Management конзолата:



Компоненти на Group Policy:

- ✓ Group Policy settings
- ✓ Group Policy objects

Типове Group Policy Objects:

- ✓ Local GPOs
- ✓ Domain-based GPOs

Ред на прилагане на груповите политики: Local Policy>Site Policy>Domain Policy>OUs Policy

Прилагане на групови политики върху сървъри и клиентски компютри:

- При стартиране на компютъра:
  - ✓ Прилагане на компютърни политики
  - ✓ Стартиране на *Startup scripts*
  - ✓ Подновяване на компютърните политики на всеки 90 минути

- При логване на потребителя:
  - ✓ Прилагане на потребителските политики
  - ✓ Стартиране на *Logon scripts*
  - ✓ Подновяване на потребителските политики на всеки 90 минути
- Полезна команда за обновяване на груповите политики: gpupdate /force

- Group Policy Preferences – преференциите са категория настройки в Group Policy Editor конзолата, които:
  - ✓ Разширяват функционалността на груповите политики
  - ✓ Намаляват необходимостта от *Logon scripts*

Group Policy Preferences включват настройки в следните категории:

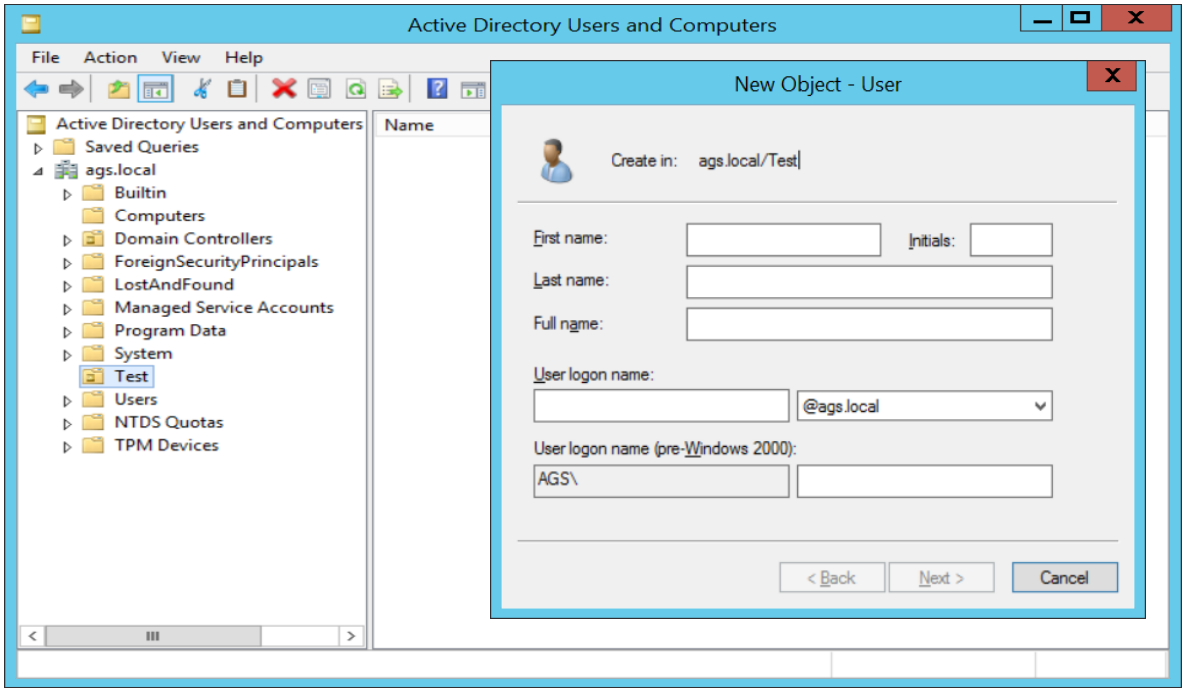
- ✓ Map network drives
- ✓ Configure desktop shortcuts
- ✓ Set environment variables
- ✓ Map printers
- ✓ Set power options

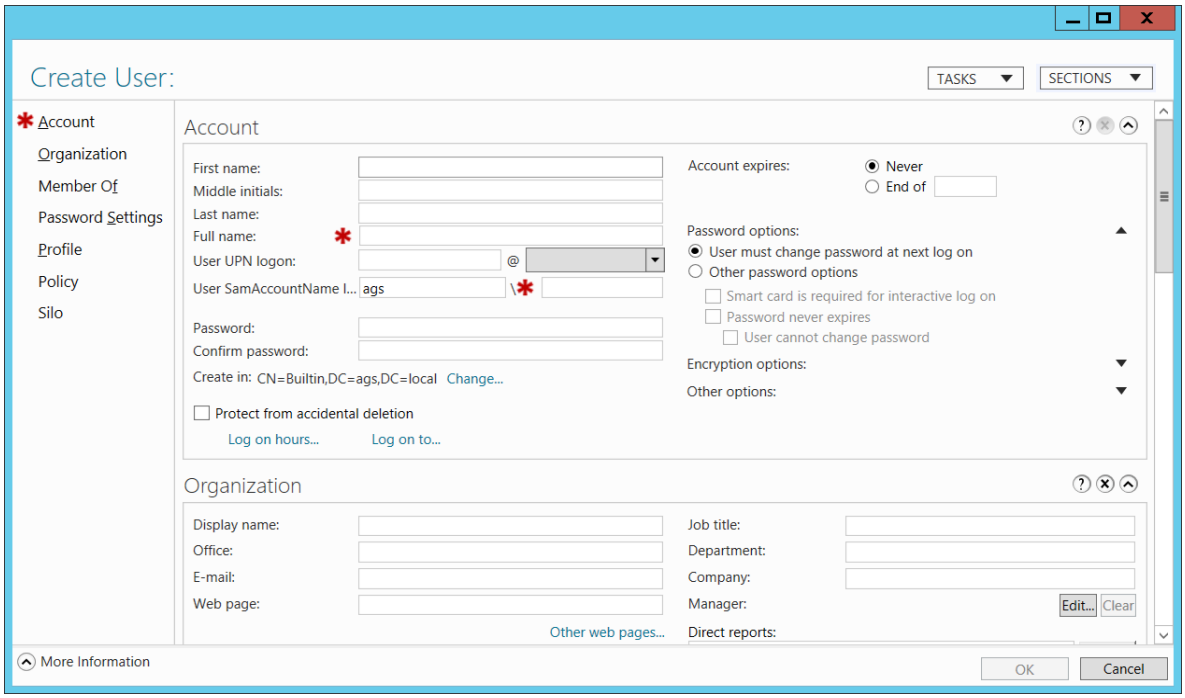
4: Управление на обекти в AD DS:

Инструменти за администриране на AD DS:

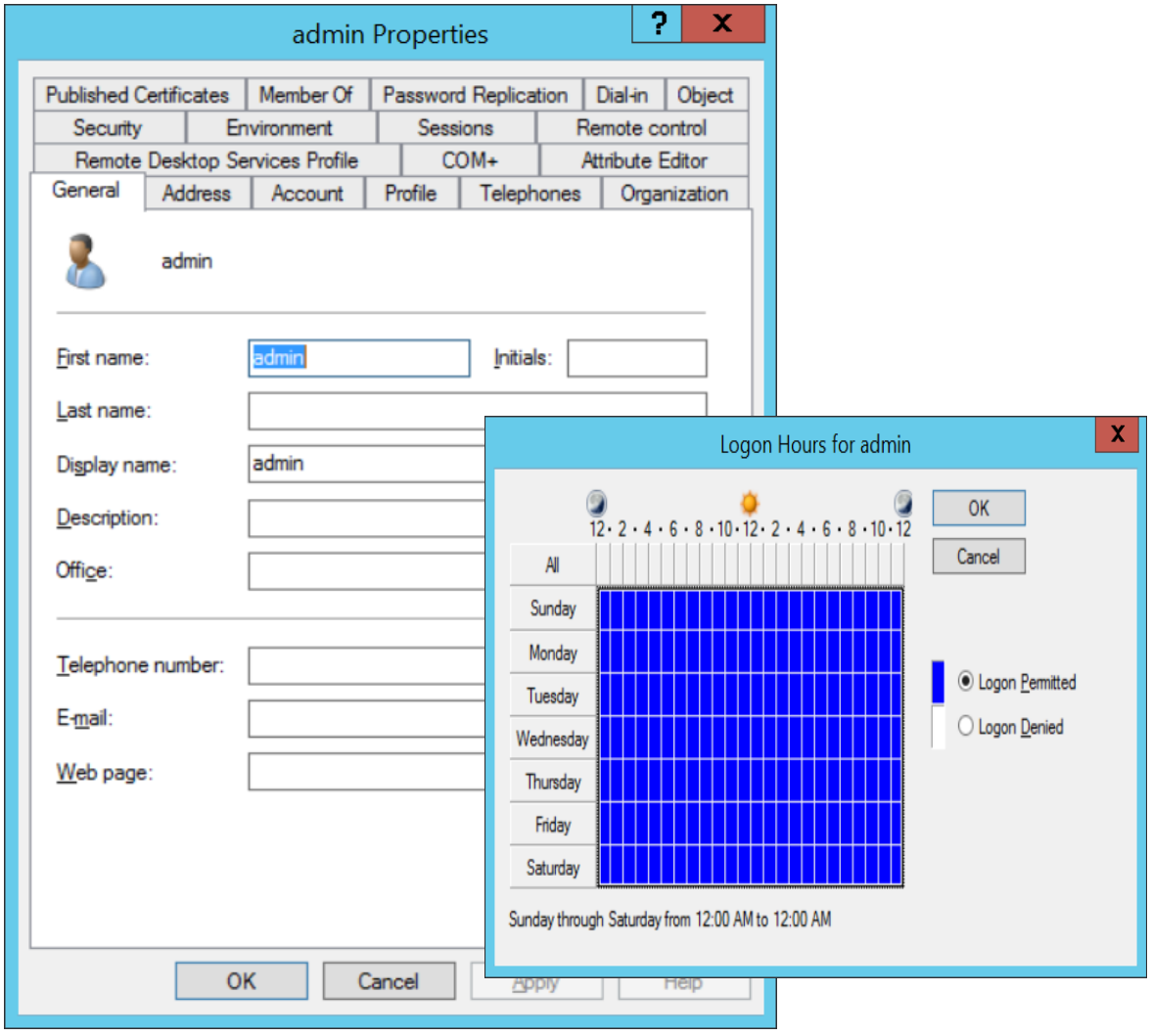
- Инструменти за администриране на обекти в Active Directory, ползващи графичен интерфейс:
  - ✓ Active Directory Administration snap-in
  - ✓ Active Directory Users and Computer
  - ✓ Active Directory Administrative Center
- Command-line инструменти за администрация:
  - ✓ Active Directory Module in Windows PowerShell
  - ✓ Directory Services tools: dsadd; dsget; dsmod; dsmove; dsquery; dsrm

- Създаване на потребителски акаунти - създаването на потребителски акаунти в Active Directory може да се изпълнява през Active Directory Users and Computers или през Active Directory Administrative Center.

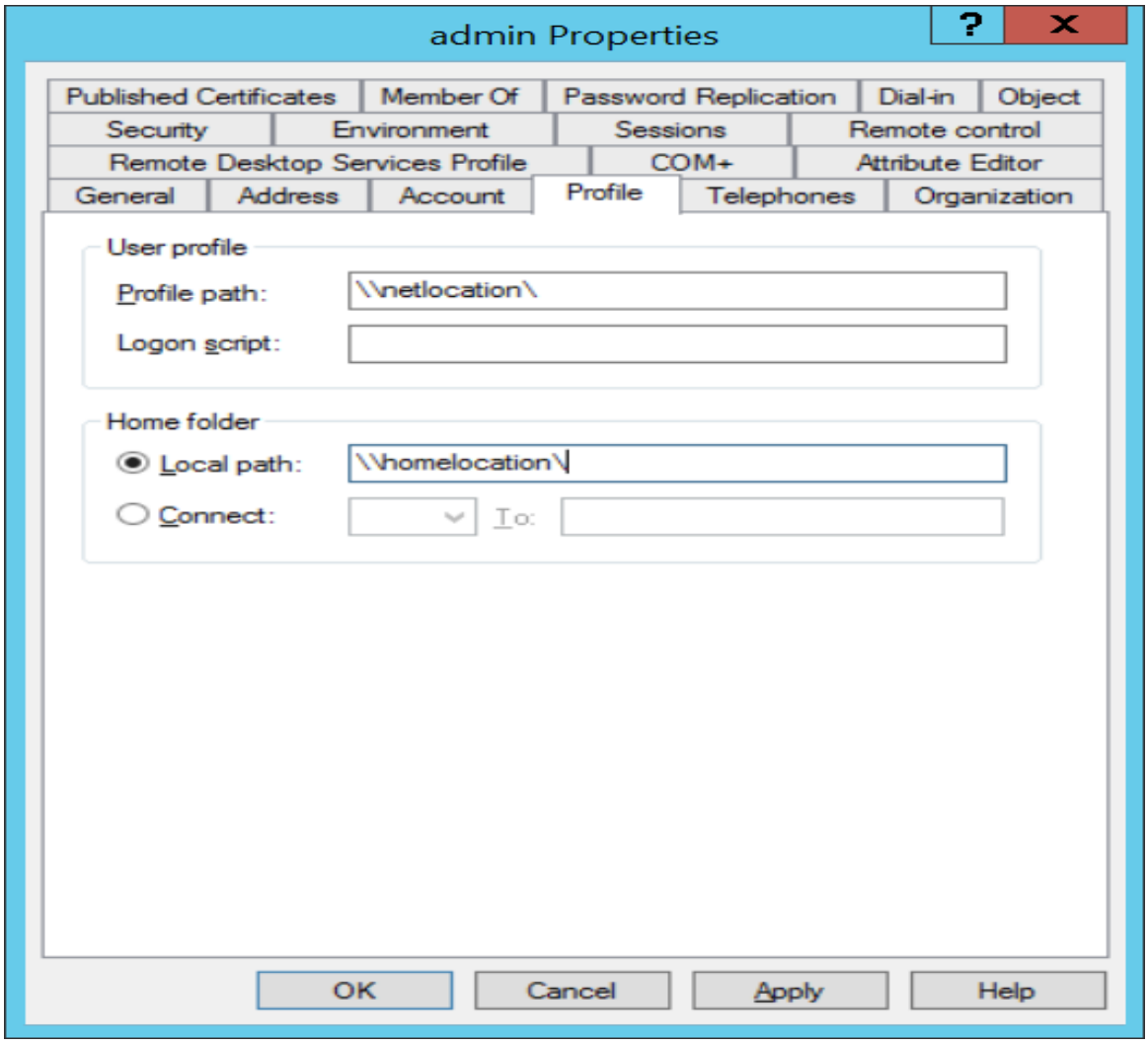




Конфигурирането на атрибутите на потребителските акаунти се осъществява от Properties на самия акаунт.

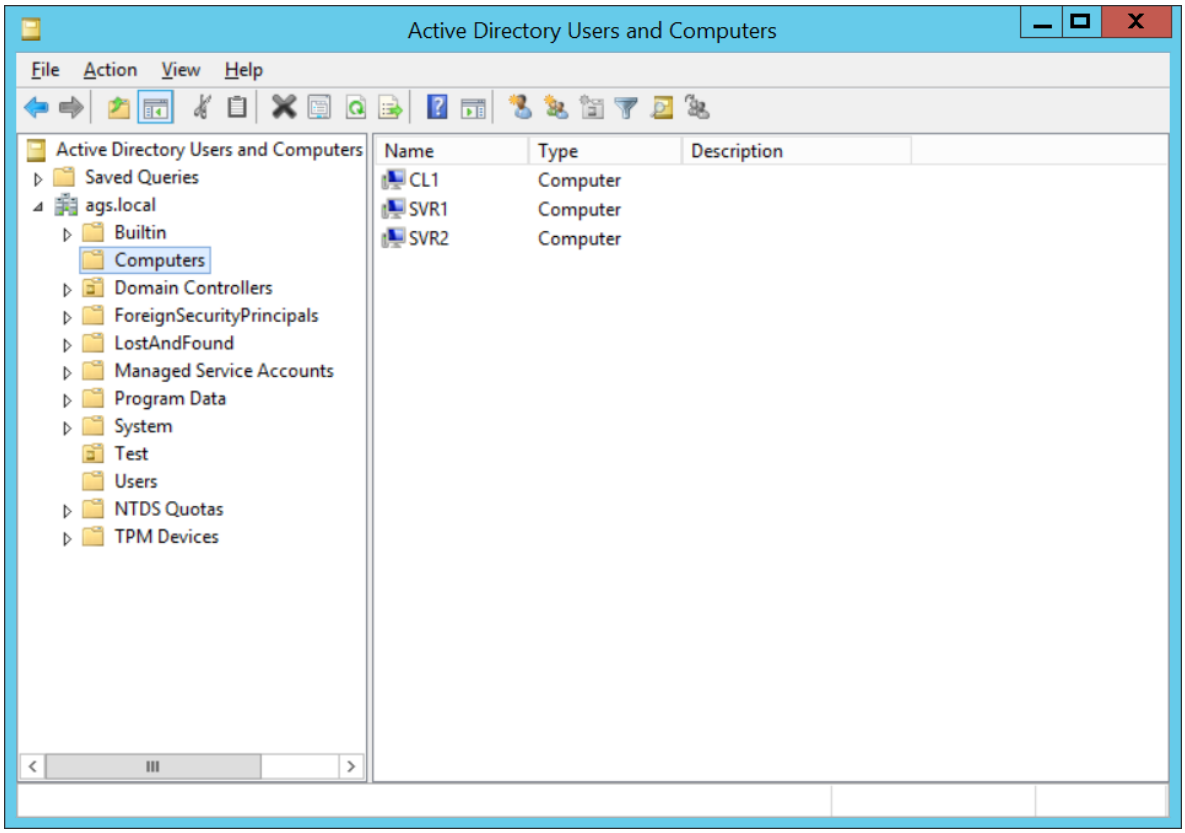


Част от атрибутите на даден акаунт е и местоположението на потребителския профил. Той може да бъде съхраняван на мрежова локация или на клиентския компютър на потребителя.

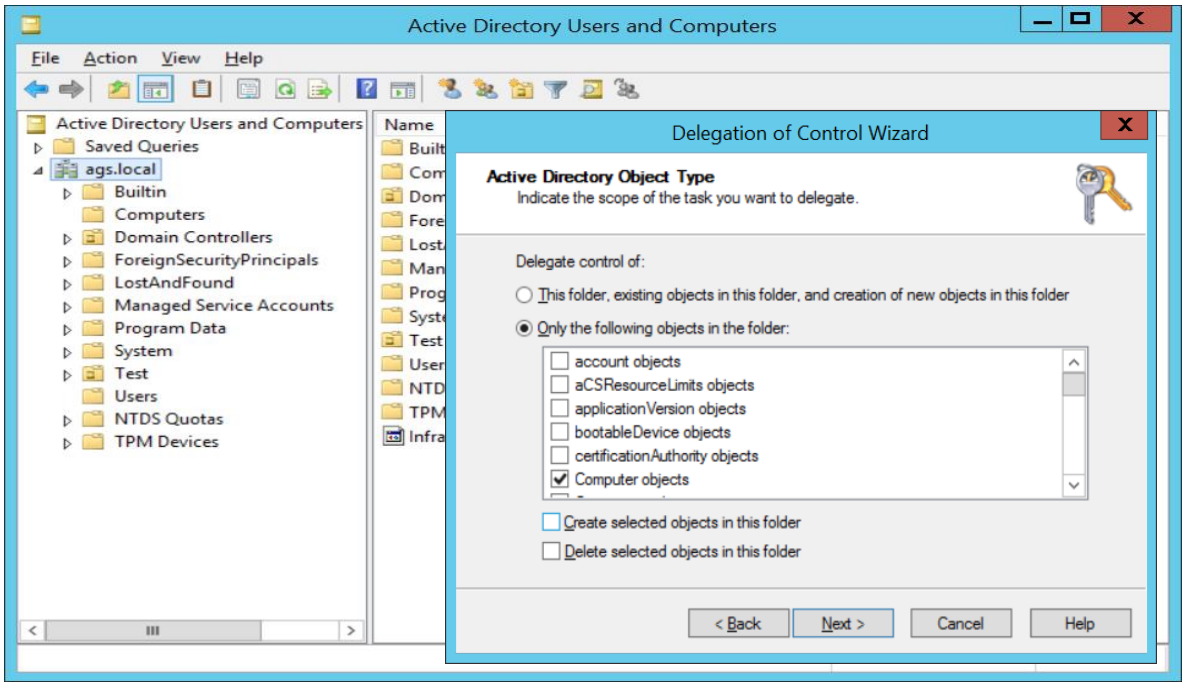


- Управление на компютърни акаунти - добра практика при компютърните акаунти е създаване на организационни единици, отговарящи на типа компютърна архитектура:
  - ✓ Servers
  - ✓ Client computers
  - ✓ Разделяне на компютърните акаунти в отделни организационни единици се прави с цел лесно администриране и имплементиране на Group Policy.

При създаване на компютърни акаунти в Active Directory, по подразбиране те са разположени в контейнера Computers.



Чрез използването на Delegation of Control Wizard, ние можем да делегираме права за създаване на акаунти на група от потребители, като по този начин прехвърлим тази дейност от домейн администраторите към отделно звено, което ще създава акаунтите в домейна.



- Offline Domain Join – метод за присъединяване на компютри в домейна когато те не могат да достъпят домейн контролер. Процедурата включва 2 етапа:

✓ Създаване на файл за последващо присъединяване към домейна:

djoin.exe /Provision /Domain <DomainName> /Machine <MachineName> /SaveFile <filepath>

✓ Импорт на предварително създадения файл:

djoin.exe /requestODJ /LoadFile <filepath> /WindowsPath <path to the Windows directory of the offline image>

Всеки компютърен акаунт в даден домейн има парола, която се подменя регулярно от домейн контролера. Тази подмяна става автоматично през интервал от време, който се настройва на ниво домейн. По този начин се установява т.н. Secure channel между компютъра и домейн контролера. Ако компютърът се преинсталира или се възстанови от архив, или не присъства в мрежата на домейна повече от конфигурирания интервал на автоматична смяна на паролата, то този компютър изпада от домейн средата и secure channel-а между него и домейн контролера се чупи.

- Атрибути на компютърните акаунти:

✓ sAMAccountName – името на компютърния акаунт в домейна

✓ Всеки компютърен акаунт има парола, която се подменя регулярно от домейн контролера

- NetLogon service – услуга, която ползвайки името и паролата на дадения компютърен акаунт, го логва в домейна и така установява т.н. ”secure channel” между компютъра и домейн контролера.
- Събития, при които се чупи т.н. „secure channel”: преинсталиране на компютър; връщане от архив или snapshot; отсъствие на компютъра от домейн средата за дълго време.
- Възможностти за нулиране (*resetting*) на *secure channel-a* между даден компютър и домейн контролера:

✓ Изваждане и наново добавяне на компютъра към домейна

✓ Нулиране на компютърния акаунт (*computer account resetting*)

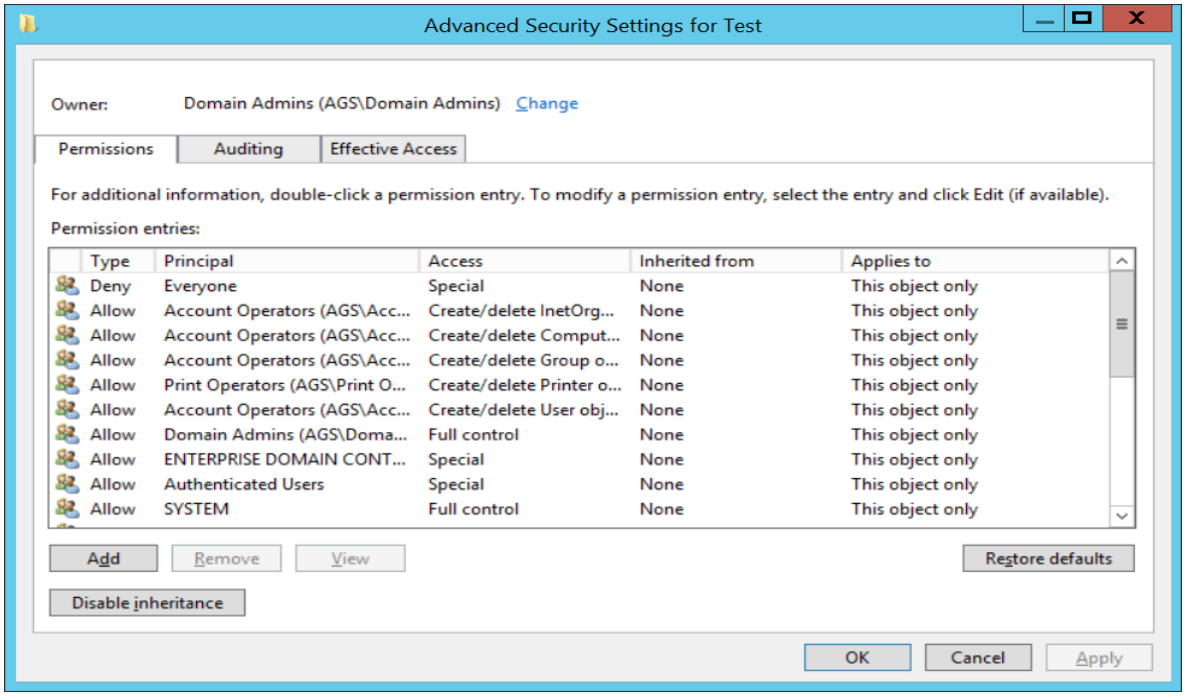
- AD DS поддържа концепцията „Bring Your Own Device“ (BYOD) чрез Workplace Join функционалността. Workplace Join има следните характеристики:

✓ *Workplace Join* създава *AD DS* обект, който отговаря на потребителското устройство

✓ Поддръжка на *iOS* устройства

✓ Планирана поддръжка на *Android* устройства

- Права върху обектите в Active Directory – правата върху обектите в Активна Директория се контролират през Advanced Security Settings на конкретния обект.



- Крайни (ефективни) AD DS права върху обекти:

  ✓ Те се акумулират

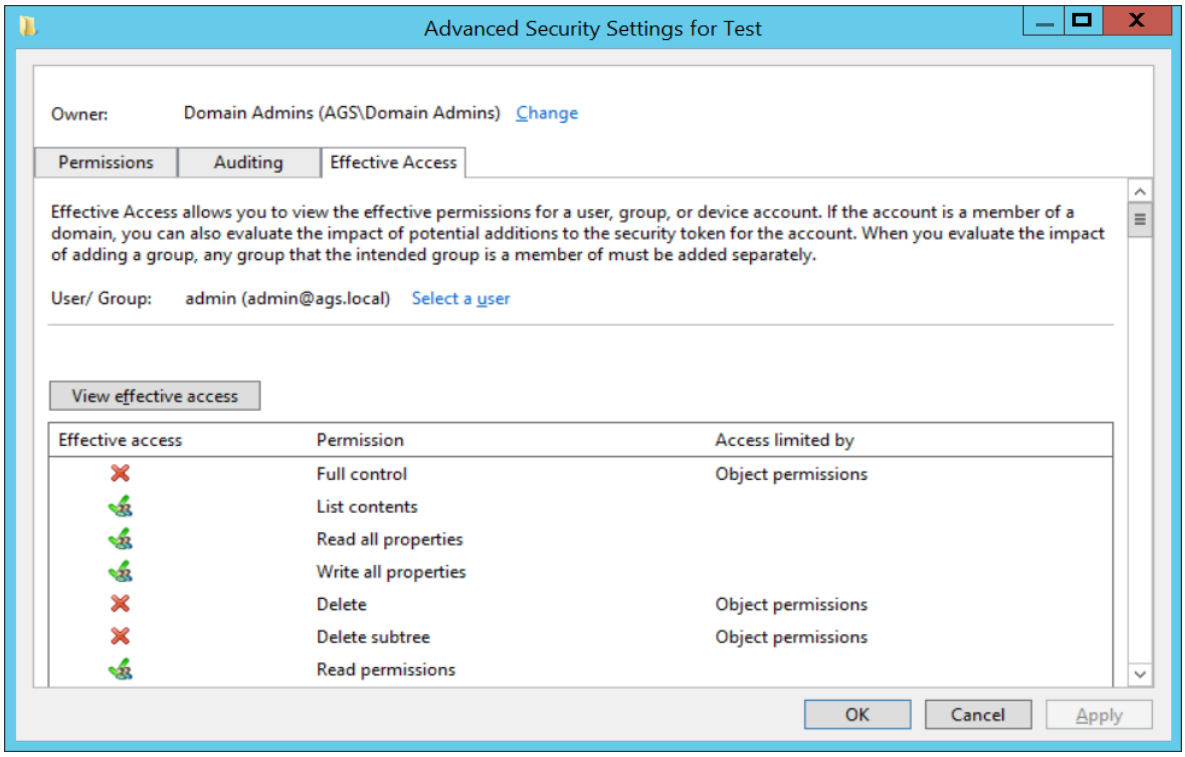
  ✓ Забранителните права (*Deny permissions*) имат предимство над разрешителните (*Allow permissions*)

  ✓ Добра практика е да се разрешават права върху ресурсите на групи, а не на единични потребители

- Преглед на ефективните права:

  ✓ Effective permissions Tab of security descriptor

  ✓ Manual analysis



Изграждане на файлов и принт-сървъри:

Сигурност на файлове и папки: Сигурността на потребителските файлове и папки се базира на строг контрол на достъпа до тези ресурси. Обикновено информацията на потребителя се съхранява локално и на файлов сървър, където правата за достъп се контролират от собственика на информацията с помощта на системния администратор. Основните моменти относно сигурността на потребителските данни са насочени в следните направления:

- **Права върху файлове и папки (File and Folder Permissions):**

  ✓ Те контролират достъпа до файлове и папки, намиращи се на NTFS или ReFS форматирани дискове.

- ✓ Конфигурират се върху файлове или папки.
- ✓ Могат да бъдат позволителни (Allow) или забранителни (Deny).
- ✓ Наследяват се (from parent folder to child folder).

Правата върху файлове и папки се конфигурират през т.н. Security Descriptor, който може да бъде достъпен, като върху съответната папка се кликне с десен бутон и се избере Properties, след това таб-а Security.

Типове права върху ресурсите:

- ✓ Стандартни (Standard Permissions) – те отразяват основните активности, позволени върху даден обект.
- ✓ Разширени (Advances Permissions) – те отразяват всички активности в детайли, които са позволени върху даден обект.

При конфликт на правата, предимство имат:

- ✓ Изключително наложените забранителни права (Explicitly assigned Deny)
- ✓ Изключително наложените разрешителни права (Explicitly assigned Allow)
- ✓ Наследените забранителни права (Inherited Deny)
- ✓ Наследените разрешителни права (Inherited Allow)

- **Права върху споделени файлове и папки (File and Shared Folder Permissions)** – споделянето на ресурсите осигурява достъпа до тях от множество потребители дистанционно по мрежата. За да контролираме достъпа до споделените ресурси, ние ползваме т.н. Shared Folder Permissions, които се прилагат само върху папки, достъпвани отдалечено.
  - ✓ Скриване на споделените папки –скриването на отдалечените папки се осъществява с добавяне на символа $ в края на името на споделената папка.
  - ✓ Достъпване на споделена папка – ползва се Universal Naming Convention (UNC) path:

  Примери за достъпване на споделени и скрити споделени папки:

  \\SRV1.demo.com\sales (стандартна папка)

  \\SRV1.demo.com\sales$ (скрита папка)

- **Административни споделени папки (Administrative Shares)** – скрити папки, които осигуряват достъп на администратора до всеки дял на диска, както и до специални системни папки:

  Примери: C$; D$; E$; Admin$

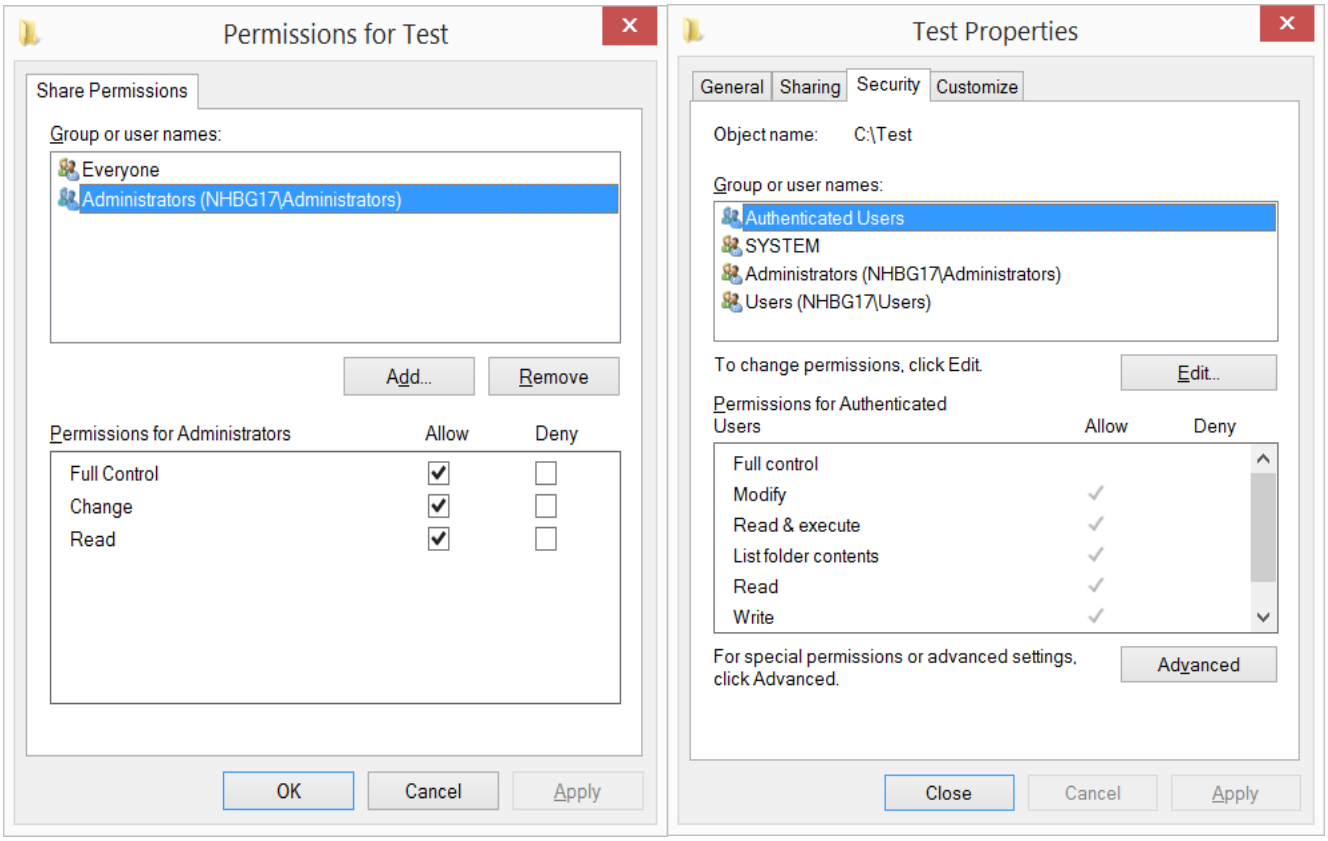
Достъпване на административни споделени папки:

\\svr1.demo.com\C$

\\svr1.demo.com\D$

\\svr1.demo.com\Admin$

Следните прозорци демонстрират възможностите за конфигуриране на Shared Permissions и Security (NTFS) permissions за конкретна потребителска папка:



- **Наследяване на права (Permissions Inheritance)** – наследяването е механизъм, който дава възможност за управление достъпа до споделени ресурси без изрично конфигуриране на права върху тях. Правата се наследяват по подразбиране (parent/child relationship) и така се реализира автоматизация в процеса на конфигуриране на правата върху ресурсите. Ако искаме да дефинираме експлицитни права на дадено ниво (ресурс), е необходимо да спрем наследяването, за да може да зададем конкретни права върху папката или файла.
- **Блокиране на наследяването (Block Inheritance)**:
  - ✓ Блокирането може да се приложи на ниво файл или папка
  - ✓ Можем да блокираме наследяването с цел да наложим нови права върху "child" обектите или да премахнем наследените вече права
- **Ефективни права (Effective Permissions)** – ефективните права се получават при комбинирането на NTFS permissions и Shared permissions върху дадена папка на база най-рестриктивните такива.

  Пример за ефективни права:

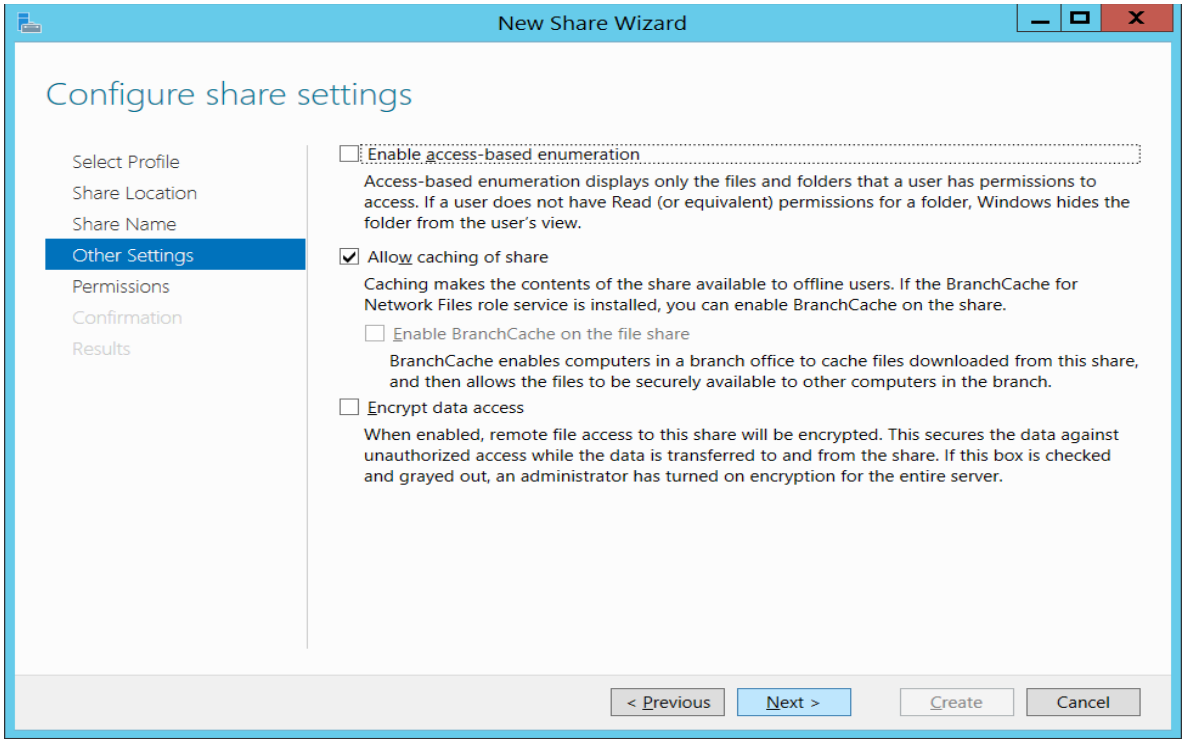
User name	NTFS permissions	Share permissions	Effective permissions
User 1	Write	Read	Read
User 2	Modify	Full Control	Modify

- **Access-Based Enumeration** е функционалност, позволяваща визуализация само на тези споделени ресурси, върху които потребителя има права. Така ако даден потребител има права върху даден ресурс, той ще може да го вижда в Windows Explorer. Ако потребителят няма права върху ресурса, то този ресурс няма да е видим за този потребител.

Access-Based Enumeration характеристики:

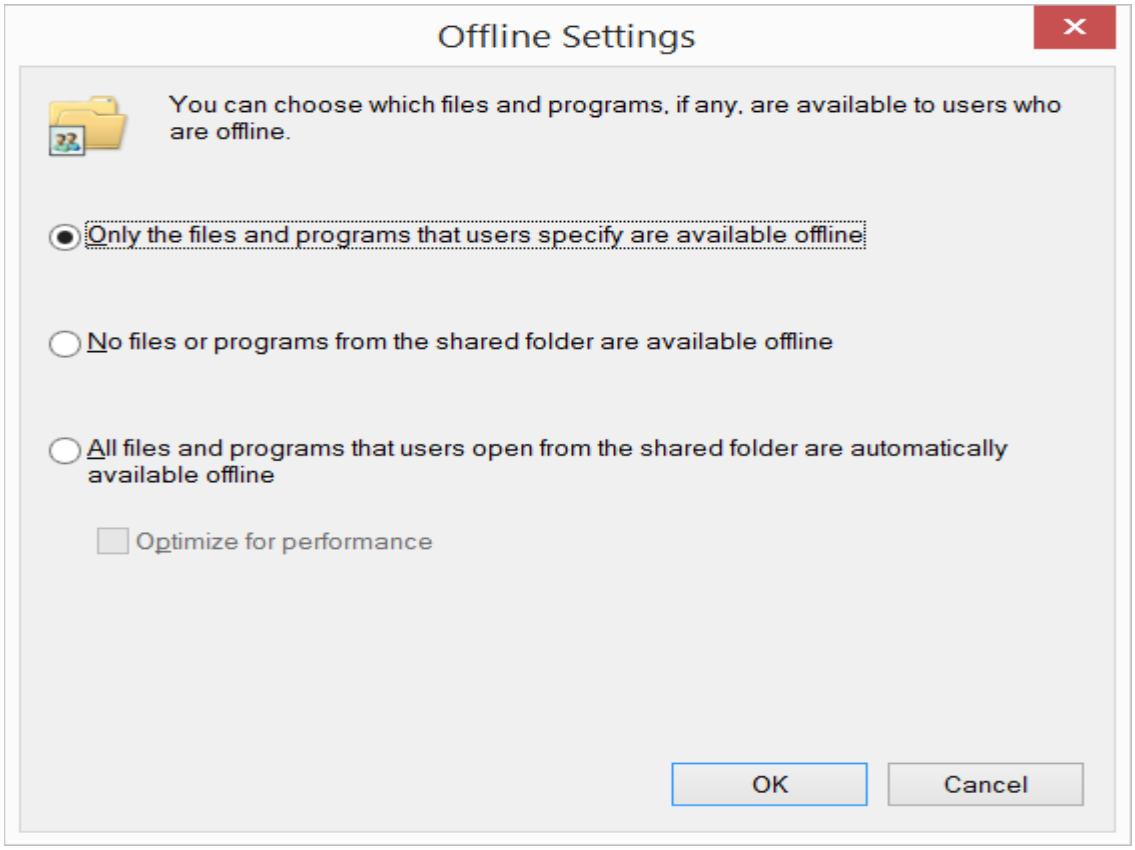
- ✓ Вградена функционалност в Windows Server 2012
- ✓ Достъпен за споделени папки
- ✓ Конфигурира се на база споделена папка
- ✓ Конфигурира се през Server Manager

Access-Based Enumeration функционалността се конфигурира през Server Manager конзолата през Share settings:



- **Offline Files** - Offline Files е функционалност, която позволява на клиентския компютър да кешира файлове локално за offline ползване когато не е свързан в мрежата и няма достъп до мрежовия ресурс. По този начин на клиентския компютър остава локално копие на offline файловете, които могат да се ползват от потребителя, докато той няма мрежова връзка с ресурса. Когато потребителя отново се включи в мрежата, протича процес на синхронизация между offline и online файловете, като така информацията се уеднаквява.

Следващият екран показва възможностите за настройка относно Offline Files функционалността.



- **Shadow Copies** - Shadow Copies е технология, позволяваща възстановяване на файлове от копия на техни предишни версии.

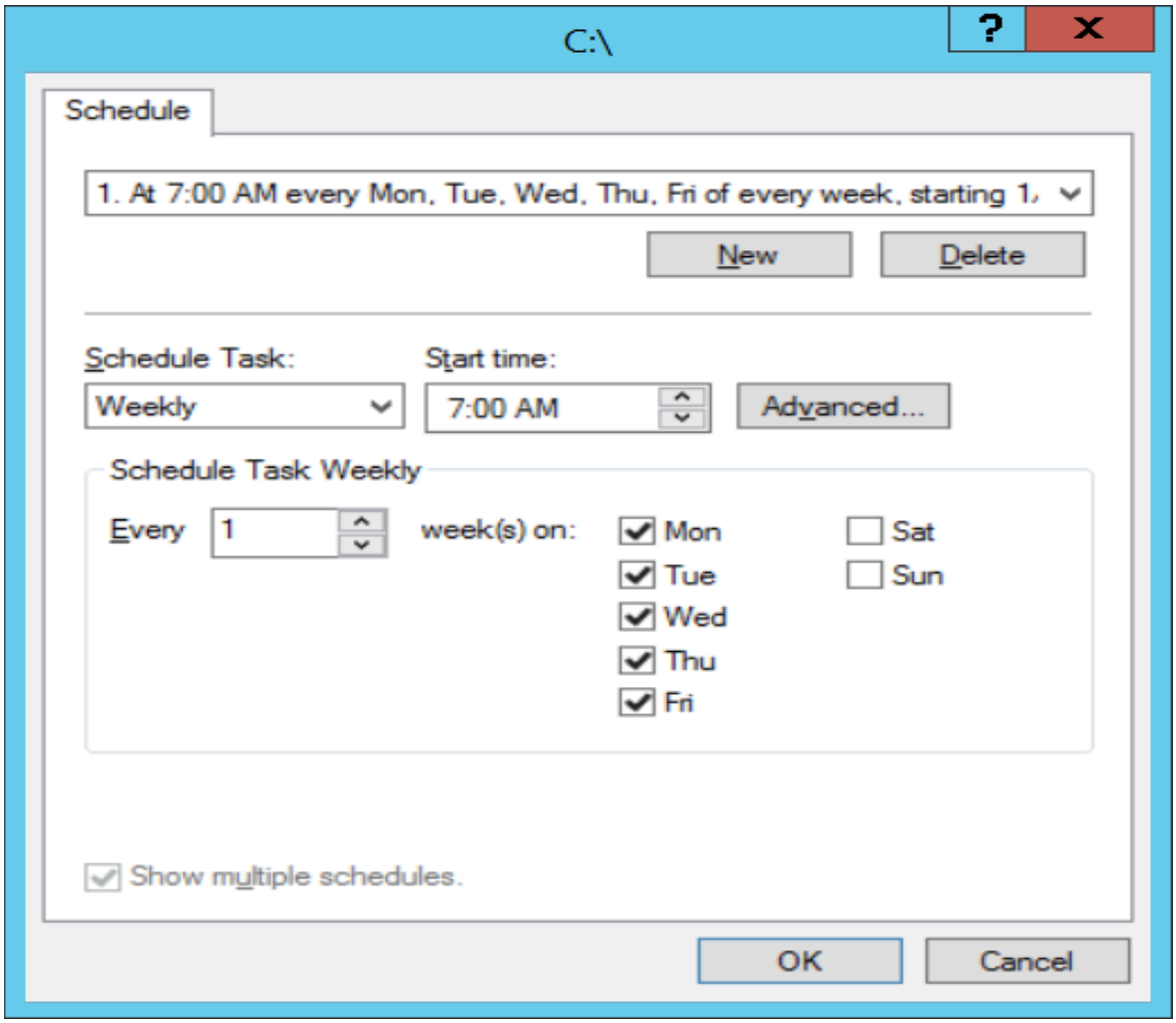
Характеристики на Shadow Copies технологията:

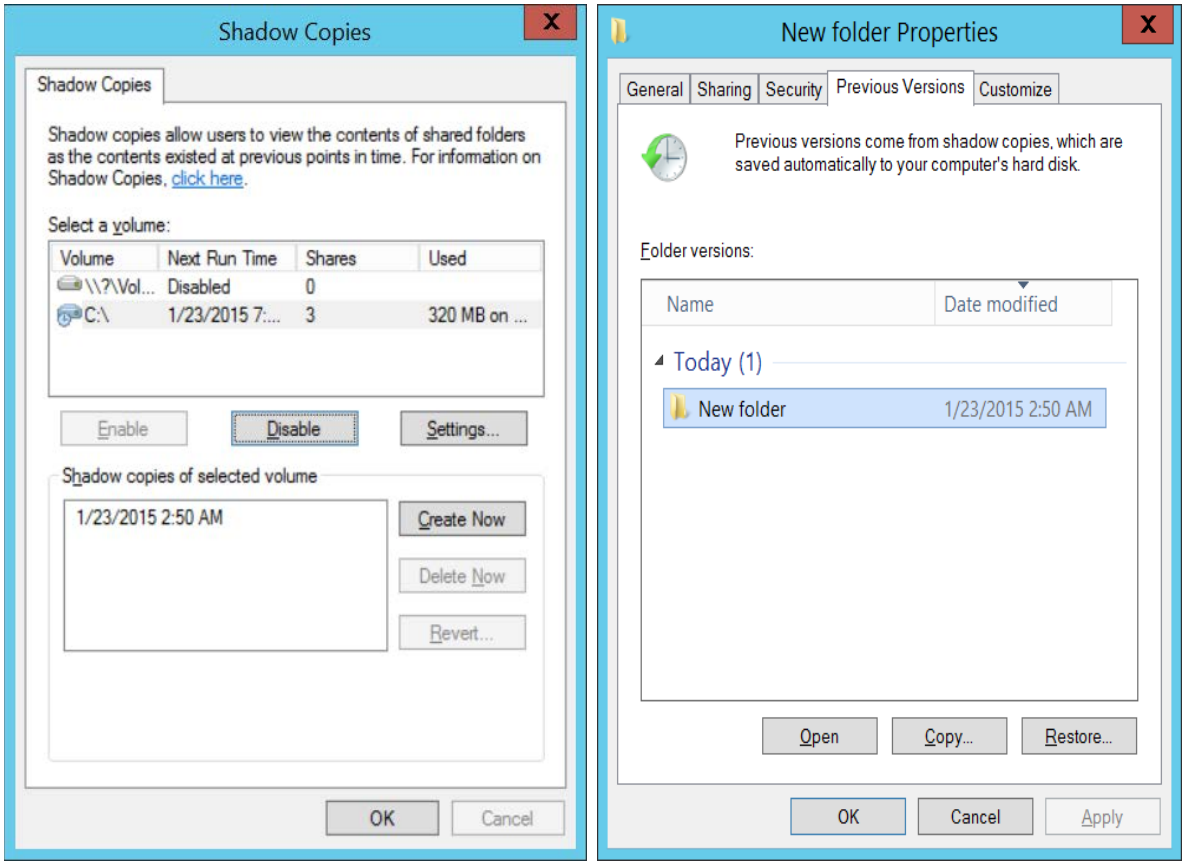
- ✓ Конфигурира се на ниво дисков дял
- ✓ Позволява достъп до предишни версии на файлове
- ✓ Базирана е на следенето на промените по диска
- ✓ Ползва допълнително дисково пространство, което е заделено на същия дял на диска
- ✓ Когато диска е пълен, старите копия на файловете се изтриват
- ✓ Не е технология, която напълно изключва архивирането на информация (backup)
- ✓ Не е подходяща технология за възстановяване на бази-данни

- ✓ Предишните версии на файловете са достъпни през менюто Previous Versions, което се появява при кликване с десен бутон на мишката върху конкретния файл (споделена папка)

Планиране употребата на Shadow Copies – след като бъде активирана, Shadow Copies функционалността може да бъде конфигурирана така, че създаването на регулярни копия на споделените папки или файлове да се случва на базата на предварително създаден график. Така създаването на архивни копия ще се изпълнява в контекста на преконфигуриран Schedule Task, което напълно автоматизира процеса и разтоварва администратора от допълнителни backup процедури.

Следните екрани показват детайли относно създаването на график за стартиране на Shadow Copies график (Shadow Copies schedule), както и възможностите за възстановяване на данни чрез Shadow Copies:





• **Work Folders Role Service** е функционалност, която позволява на потребителите да синхронизират корпоративни данни между ползваните от тях устройства и корпоративния файлов сървър. Когато потребител промени файл от Work Folders от някое устройство, тази промяна се репликира на корпоративния файлов сървър. Процесът по репликация ползва SSL port 443, което гарантира сигурен трансфер на данните.

Характеристики на Work Folders:

- ✓ New role service of the File and Storage Services Role in Windows Server 2012 R2
- ✓ Достъпът до файловете в Work Folders е URL-базиран (достъп от всякъде)

- ✓ Наличие на различни имена на файлове в зависимост от устройството, на което са модифицирани:

Document1_name_of_pc

Document1_name_of_tablet

Ползи от употребата на Work Folders:

- ✓ Достъпът до файловете става както от домейн устройства, така и от устройства извън домейна
- ✓ Осигурява offline достъп до работните папки
- ✓ Криптиране на данните
- ✓ Синхронизира файловете на потребителите

Ограничения в употребата на Work Folders:

- ✓ Работи само при Windows Server 2012 R2 и Windows 8.1
- ✓ Не позволява селектирана синхронизация на файлове
- ✓ Не позволява синхронизиране на няколко споделени папки едновременно

Изисквания и компоненти на работните папки (Work Folders):

- Софтуерни изисквания:

- ✓ Windows Server 2012 R2 file server with NTFS or ReFS
- ✓ Windows 8.1 client with NTFS or ReFS
- ✓ SSL certificates

- Сървърни компоненти:

- ✓ Work Folders role service
- ✓ File Server role service
- ✓ Web Server role
- ✓ IIS Management Console/Hostable Web Core role service

- Клиентски компоненти:

- ✓ Manual deployment through Control Panel
- ✓ Automatic deployment through Group Policy, Configuration Manager or Intune

Конфигуриране на работни папки - Процесът по конфигуриране на работни папки преминава през два етапа:

- Сървърна конфигурация:

✓ Инсталиране на Work Folders role service

✓ Създаване на споделена папка

✓ Инсталиране на сървърен сертификат със същият subject name като Work Folders URL

- Клиентска конфигурация:

✓ При ръчно конфигуриране, потребителят въвежда своя и-мейл адрес

✓ При автоматично конфигуриране се ползва Group Policy

Конфигуриране на мрежови принтери:

Характеристика на мрежовият принтер: Мрежовият принтер е печатащо устройство, което има мрежови интерфейс и получава заявките за печат по мрежата. По този начин мрежовия принтер може да бъде ползван от множество клиентски компютри едновременно, без да се налага споделянето му на конкретен компютър. Особено подходящо решение е реализацията на принт-сървър чрез добавянето на Print Server ролята на даден сървър в среда на Windows Server 2012. По този начин се реализира централизирана локация за предоставяне на услуги по печатане на документи от крайните потребители, както и лесен метод за мониторинг и управление на състоянието на всички устройства за печат, добавени на дадения принт-сървър.

Ползи от употребата на мрежови принтери:

✓ Централизирано управление чрез Print Management Console

✓ Улеснено откриване на проблеми

✓ Намалени общи разходи при процеса на принтиране на документи

✓ Лесно откриване на мрежовите принтери чрез публикуването им в Active Directory

Недостатъци при мрежовите принтери и Print server ролята:

✓ Single Point of Failure: Принт-сървърът може да се окаже критична точка във вашата printing услуга, което налага ползването на clustering технологии

✓ Процесът по печат е зависим от състоянието на мрежовата инфраструктура

Enhanced Point and Print е технология, ползваща “v4 driver model” принт драйвъри с цел осигуряване на улеснено управление на принтиращите устройства и техните драйвъри в дадена компания.

Характеристики на Enhanced Point and Print:

- ✓ Принт-сървърите не се налага да съхраняват клиентски принтер драйвъри
- ✓ Принтер драйвърите са изолирани по между си и така не позволяват конфликт на имената на драйвър файловете
- ✓ Един драйвър може да поддържа няколко типа устройства
- ✓ Драйвър пакетите са с малък размер и се инсталират бързо
- ✓ Принтер драйвърите и принтерския потребителски интерфейс могът да се дистрибутират независимо един от друг

Настройки на сигурността на мрежовите принтери – сигурността на мрежовите принтери се базира на тените настройки, които биват два типа:

- Стандартни настройки относно процеса на принтиране на документи - дават възможност на всеки потребител да може да:
- ✓ Принтира (Print)
- ✓ Управлява собствените си документи за печат (Manage documents)
- Допълнителни настройки – при тях потребителя може да:
- ✓ Принтира (Print)
- ✓ Управлява принтера като устройство (Manage printer)
- ✓ Управлява документите за печат на дадения принтер (Manage documents)

Printer Pooling е технология, която позволява комбинирането на няколко физически принтера в един логически. Printer Pooling повишава надеждността на процеса по принтиране на документи и дава възможност за добавяне на нови устройства с цел намаляване натоварването на всеки принтер.

Изисквания за реализация на Print Pooling:

- ✓ Всички принтери трябва да ползват един и същ драйвър
- ✓ Всички принтери трябва да са в една и съща физическа локация

Branch Office Direct Printing е функционалност, която дава възможност клиентските компютри в офис-клона да печатат директно на мрежовите принтери, които са споделени на принт-сървъра. Windows клиентите получават информация за принтерите, разположени в офис-клона от принт-сървъра, но изпращат заявките за печат директно към принтерите. По този начин заявките за печат не пътуват по мрежата до централния принт-сървър и после обратно до принтерите в офис-клона, а се насочват от клиентските компютри директно към принтерите в офис-клона.

Предимства на Branch Office Direct Printing:

- Редуциране на мрежовия WAN трафик

- Заявките за печат се кешират на клиентските компютри в офис-клона

Конфигуриране на Branch Office Direct Printing през Windows PowerShell:

Set-Printer -name "<Printer Name Here>" -ComputerName <Print Server Name Here> -RenderingMode BranchOffice

Методи за инсталиране принтери на клиентите – използват се три основни метода за инсталация на принтери на клиентските компютри:

- ✓ Group Policy Preferences
- ✓ GPO created by Print Management
- ✓ Manual installation

Прилагане на групови политики (Group Policy):

Компоненти на груповите политики – технологията за реализиране на групови политики се базира на два компонента:

Настройки на груповите политики (Group Policy settings):

- ✓ Включват специфични конфигурационни настройки
- ✓ Прилагат се на компютър или потребител

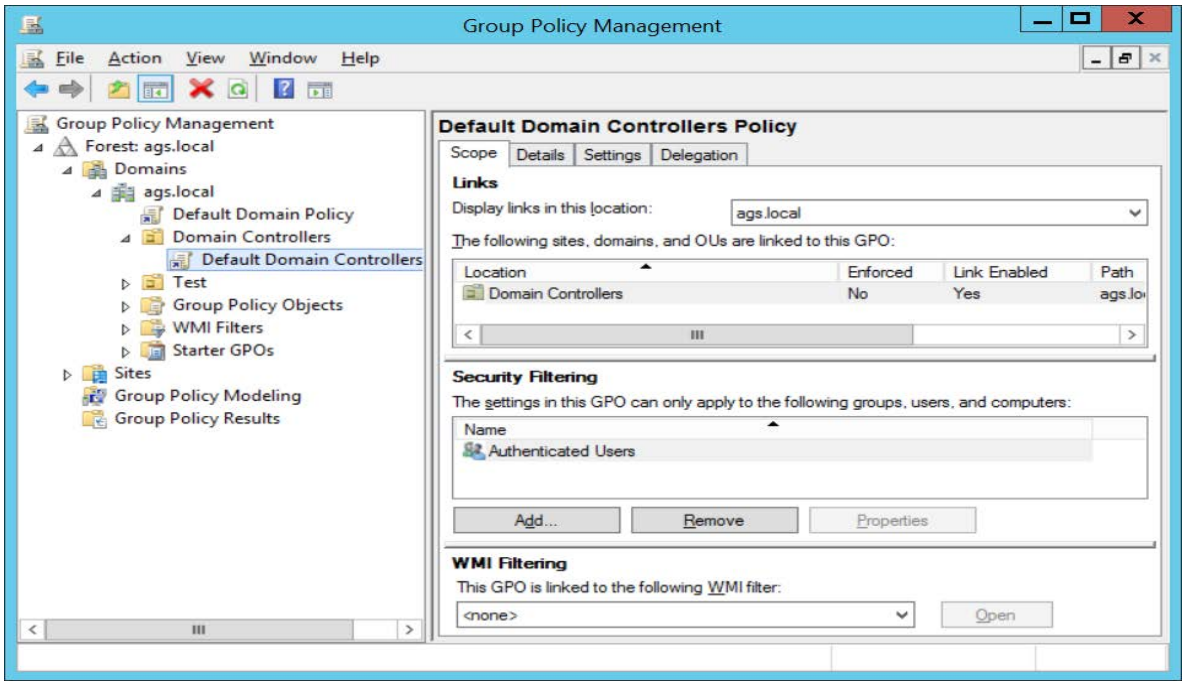
Обект на груповите политики (Group Policy Object - GPO):

- ✓ GPO е обект от контейнерен тип, който се съхранява в Active Directory
- ✓ Представлява колекция от Group Policy настройки
- ✓ Прилага се на ниво компютър, потребител или и на двете нива

Всеки Group Policy Object се състои от два компонента:

- Group Policy Container, който се съхранява в AD DS като обект и осигурява информация за отделните версии на GPO
- Group Policy Template, който се съхранява се в споделената папка SYSVOL и осигурява настройките на груповите политики

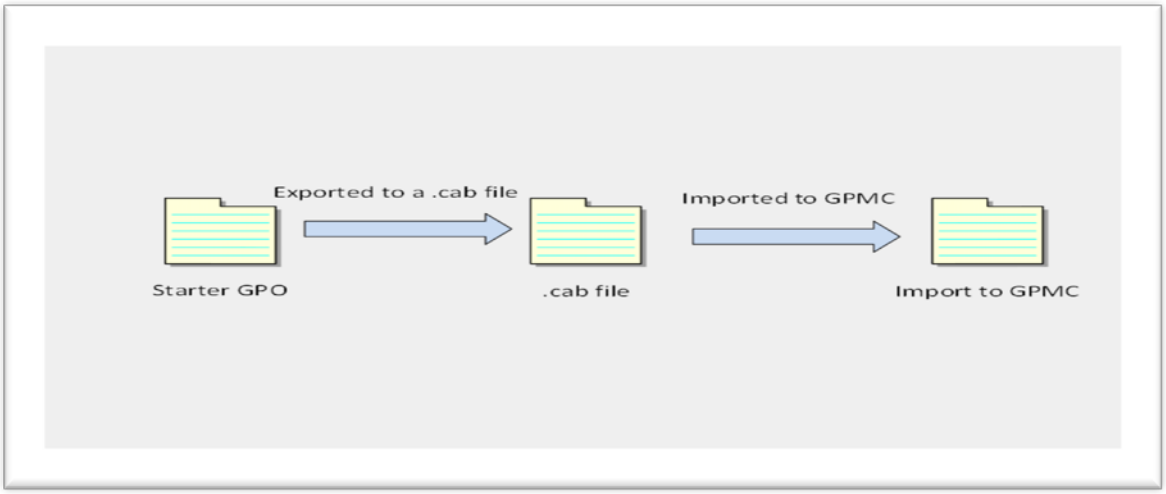
Основният инструмент за конфигуриране и контрол на груповите политики, който се ползва от системния администратор, е Group Policy Management конзолата. Group Policy Management Console е инструмент за създаване, управление и прилагане на групови политики на отделни нива в йерархията на дадена домейн среда.



Starter GPO – Group Policy обект, който е преконфигуриран от администратора и може да бъде ползван като готов шаблон за създаване на нови Group Policy обекти.

Характеристики на Starter GPO:

- ✓ Съдържа преконфигурирани настройки на Administrative Templates, които се ползват като основа за създаване на нови GPO
- ✓ Могат да се експортират в .cab файлове
- ✓ Могат да бъдат импортирани в GPMC



Делегиране управлението на GPOs е метод, който позволява разпределяне на административния товар относно управлението на Group Policy инфраструктурата, като дава възможност тази дейност да се изпълнява от лица извън групата на Domain Admins или Enterprise Admins.

Задачи, които могат да бъдат делегирани:

- ✓ Създаване на GPOs включително Starter GPOs
- ✓ Редактиране на GPOs
- ✓ Управление на Group Policy връзки на съответните нива: site/domain/OU
- ✓ Изпълнение на Group Policy Modeling и Group Policy Results
- ✓ Създаване на WMI филтри

GPO Links:

- ✓ Ние доставяме настройки на даден обект като закачваме GPO към контейнера, в който е разположен този обект
- ✓ Забраняването на връзката (link disabling) премахва настройките от контейнера
- ✓ Изтриването на връзката (link deletion) не изтрива конкретния GPO
- ✓ Не можем да закачваме GPOs към следните контейнери: Users; Groups; Computers; System containers. Ако искаме да приложим настройки, които да засегнат тези контейнери, то тези настройки трябва да бъдат отразени в Default Domain Policy.

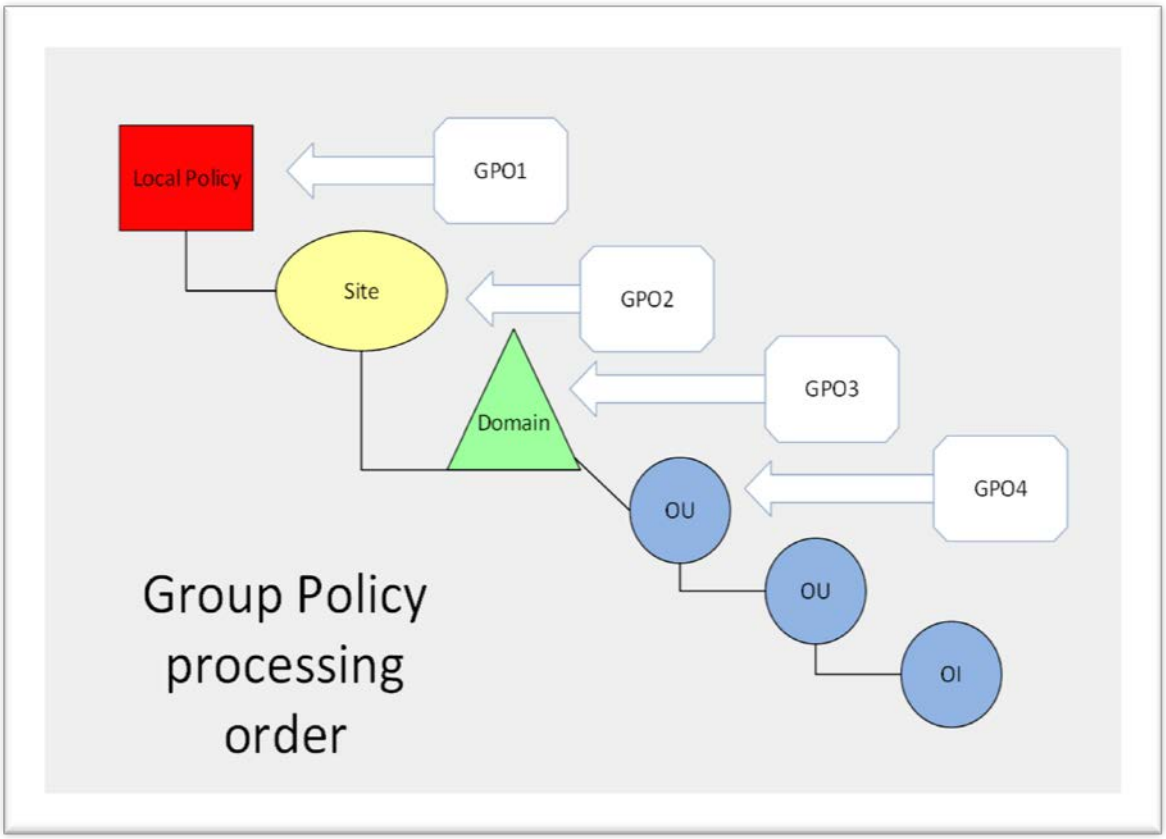
Прилагане на GPOs:

- ✓ Компютърните настройки се прилагат при стартиране на компютъра
- ✓ Потребителските настройки се прилагат при логване на потребителя
- ✓ Подновяване на политиките – параметър, който се настройва
- ✓ Настройките по сигурността (Security Settings) се подновяват на всеки 16 часа задължително
- ✓ Команди за подновяване на политиките: gpupdate /force; Invoke-Gpupdate
- ✓ Remote Policy Refresh feature – опция, достъпна при Windows Server 2012 и Windows 8 за отдалечено обновяване на политиките на клиентите през GPMC.

Ред на прилагане на GPOs съобразно мястото на обектите в Active Directory – груповите политики се прилагат в следната последователност, като всяко следващо ниво има предимство пред предишното при конфликтни настройки:

- Local Policy
- Policy from Site level

- Policy from Domain level
- Policy from Organizational Unit (and every child OU)



В среда на Active Directory винаги съществуват две политики по подразбиране, наречени **Default GPOs**. Това са:

✓ Default Domain Policy - определя акаунт политиките на ниво домейн, а именно:

- Password policies
- Account lockout policies
- Kerberos protocol policies

✓ Default Domain Controller Policy – прилага се на домейн-контролерите и определя техните настройки:

- Auditing policies
- User rights on domain controllers

GPO Security Filtering е технология за филтриране прилагането на дадена политика върху определени обекти. Осъществява се с помощта на следните методи:

- Използване на Group Policy permissions:

✓ Всяко GPO има ACL

✓ По подразбиране, групата Authenticated Users има Read and Allow Apply Group Policy права

- Използване на глобални или универсални групи за контрол върху прилагането на дадено GPO
- Използване на Windows Management Instrumentation (WMI) филтри. Актуална информация относно употребата на WMI филтри може да бъде получена на следния адрес: https://technet.microsoft.com/en-us/library/cc779036%28v=ws.10%29.aspx

Административни шаблони (Administrative Templates) – административните шаблони са средство за контрол на операционната система и потребителската работна среда. Те определят как изглеждат конкретните настройки в груповите политики и как тези настройки са групирани в Group Policy Management Editor конзолата. Състоят се от два компонента:

✓ .admx file – файл, който съдържа group policy registry настройките и е езиково неутрален. Промяната в настройките на административните шаблони променя съответния параметър в Windows Registry.

✓ .adml file – съдържа конкретна езикова информация, която дава възможност за визуализиране на group policy настройките на съответния език.

Administrative Templates section for computers	Administrative Templates section for users
Control Panel	Control Panel
Network	Desktop
Printers	Network
Server	Shared Folders
Start Menu and Taskbar	Start Menu and Taskbar
System	System
Windows components	Windows components

Съществуват два типа категории настройки в Group Policy:

- Managed policy settings (Policies):

- ✓ Потребителският интерфейс е заключен и потребителя не може да прави промени по настройките
- ✓ Промените се отразяват в един от четирите резервни registry ключа
- ✓ Възможността за промени и потребителският интерфейс се отключват когато компютъра (потребителя) е извън обхвата на дадения GPO
- • Unmanaged policy settings (Preferences):
- ✓ Потребителският интерфейс не е заключен
- ✓ Промените са постоянни (те „татуират“ Windows Registry)
- ✓ Промените в настройките остават валидни дори когато компютъра (потребителя) е извън обхвата на дадения GPO

Процедура по разширяване обхвата на административните шаблони:

- ✓ Създаване на нови административни шаблони или сваляне на вече съществуващи такива от сайта на производителя
- ✓ Добавяне (import) на шаблоните към GPO така, че те да са достъпни за ползване
- ✓ Конфигуриране на конкретните настройки
- ✓ Активиране на GPO

Central Store е папка, осигуряваща централизирано съхраняване на административните Group Policy шаблони. Тази папка притежава следните характеристики:

- ✓ Централно място за съхраняване на ADMX и ADML файловете
- ✓ Разположен е в папката SYSVOL
- ✓ Трябва да се създаде ръчно
- ✓ Автоматично се открива от Windows операционните системи
- ✓ Group Policy Management Editor се закачва автоматично към central store локацията на PDC emulator домейн контролера в даден домейн.
- ✓ Репликира се между домейн-контролерите
- ✓ Представлява папка, която носи името PolicyDefinitions и се намира в следната локация:

C:\Windows\SYSVOL\sysvol\{Domain Name}\Policies\

- ✓ Копиране на съдържанието на папката C:\Windows\PolicyDefinitions в новосъздадения central store

Повече информация относно функциите и създаването на central store може да намерите на адрес: https://msdn.microsoft.com/en-us/library/bb530196.aspx

Управление на потребителския работен плот (User Desktops) чрез групови политики

Възможностите за управление и унифициране на потребителския работен плот са базирани на имплементирането на следните технологични решения:

Пренасочване на папки (Folder Redirection) е функционалност, позволяваща конкретни потребителски папки, които се намират на даден файлов сървър, да се визуализират пред потребителя като локални ресурси на ползвания от него компютър. Пренасочването на папки всъщност е преместване на ресурсите от потребителския профил на даден сървър и визуализиране на тези ресурси като локални за потребителя.

Папки, които могат да бъдат пренасочвани:

- ✓ Desktop
- ✓ Start Menu
- ✓ Documents
- ✓ Pictures
- ✓ AppData\Roaming
- ✓ Contacts
- ✓ Downloads
- ✓ Favorites
- ✓ Music
- ✓ Videos

Опции при конфигурирането на Folder Redirection:

- ✓ Basic Folder Redirection – ползва се, когато всички потребители запазват своите файлове в една и съща локация
- ✓ Advanced Folder Redirection – ползва се, когато достъпа до ресурсите на файл-сървъра е базиран на групово членство
- "Follow the Documents folder" option – дава възможност определени папки да станат подпапки на Documents

Target folder location – опции:

- ✓ Redirect to the users` home directory (Documents folder only) – пренасочване на папка в home директорията на даден потребител
- ✓ Create folder for each user under the root path – създаване на папка за всеки потребител в началото на дисковия дял
- ✓ Redirect to the following location – пренасочване към конкретна локация, която може да се посочи
- ✓ Redirect to the local user profile location – пренасочване в локалния потребителски профил

Групови политики при прилагане на скриптове - скриптовете са последователност от логически свързани команди и параметри, които изпълняват дадена задача или автоматизират конкретен процес.

Примери за употреба на скриптове: Изчистване на временни папки; изчистване на "page file"; прикачване на мрежови ресурси и др.

Прилагане на скриптове чрез групови политики:

- ✓ На ниво компютри:

- Startup scripts – този тип скриптове се изпълняват при стартиране на компютърната система.

- Shutdown scripts - този тип скриптове се изпълняват при гасене на компютърната система.

- ✓ На ниво потребители:

- Logon scripts - този тип скриптове се изпълняват при логване на потребителя.

- Logoff scripts - този тип скриптове се изпълняват при отписване на потребителя от системата.

Управление на софтуер чрез групови политики – технологията за ползване на групови политики дава възможност за инсталиране и преинсталиране на софтуер на територията на даден домейн. Процесът по управление на софтуер чрез Group Policy е базиран на технологията **Windows Installer.** Windows Installer позволява автоматизиране на процеса по инсталиране, преинсталиране, подновяване и премахване на софтуер с помощта на групови политики.

- Компоненти на Windows Installer:

- ✓ Windows Installer service:

- напълно автоматизира процеса по инсталация и конфигуриране на софтуер

- модифицира или поправя съществуваща софтуерна инсталация

✓ Windows Installer Package:

- съдържа информация относно инсталирането и деинсталирането на дадено приложение

- файл с разширение „.msi”

- референция към локация на инсталиране

Съществуват два типа методи за инсталация на софтуер:

- Назначаване на софтуер (Assigning software) – можем да назначаваме софтуер на ниво компютър и на ниво потребител.
  - ✓ Назначаване на софтуер на ниво компютър – при този вариант, софтуерът се инсталира при следващото рестартиране на компютърната система. Така инсталирания софтуер ще бъде достъпен за всички потребители на този компютър.
  - ✓ Назначаване на софтуер на ниво потребител – при този вариант, софтуерът се рекламира в старт менюто на потребителя. Инсталацията се стартира когато потребителя кликне двойно върху иконата на рекламирания софтуер или когато стартира файл, чието разширение е асоциирано със този софтуер.
- Публикуване на софтуер (Publishing software) – при публикуването на софтуер, той се появява под формата на бутон за пряк достъп (shortcut) в графата Programs and Features на Control Panel. Процесът по инсталация стартира с кликване върху иконата на публикувания софтуер или когато потребителя стартира файл, чието разширение е асоциирано със този софтуер.
  - ✓ Не може да се публикува софтуер на ниво компютър!!!

Управление на софтуерни подновявания (Software Updates) чрез групови политики: съществуват два типа софтуерни подновявания:

- Optional Upgrade – при този тип, потребителят решава дали и кога да направи подновяването.
- Selective Upgrade – администраторът подбира конкретни потребители, оформяйки ги в групи, на които ще бъде подновена версията на софтуера, предвиден за подновяване.

Част V: Инструменти за системна администрация и отстраняване на проблеми.

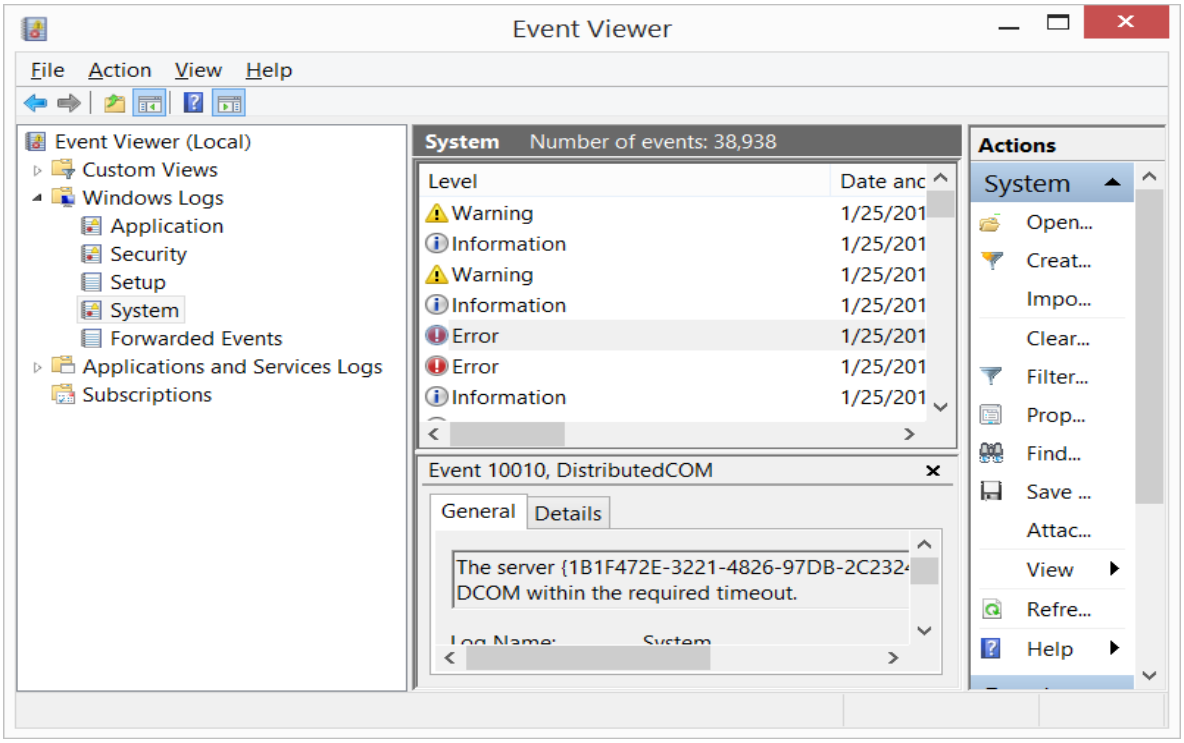
Мониторинг на производителността на сървъри

Наблюдението на работното състояние и производителността на сървърите, както и анализа на случилите се събития назад във времето, се базира на няколко типа технологии, които позволяват мониторинг върху дадена система. До голяма степен, получаването на информация относно даден сървър зависи от способността на инсталираната върху него операционна система да прихваща събития и да ги отразява под формата на логове с цел по-нататъшното им преглеждане от администратора. Колкото повече събития регистрира дадена операционна система, толкова по успешна и желана от администраторите е тя.

Мониторинга на производителността на сървърите в дадена мрежа включва следните дейности**:**

- **Запис на събития (Event Logging) -** Event Logging е процес на записване на системни събития, касаещи операционната система, приложенията и всички услуги, работещи на даден компютър. Колкото повече събития записва дадена операционна система под формата на логове, толкова повече полезна информация е налице за администраторите, поддържащи тази система.
- **Event Viewer** – административна конзола за визуализиране и анализ на записите на системните събития в среда на Windows Server 2012. Стартирането на тази конзола става от следната локация: Control Panel\Administrative Tools\Event Viewer. Всички записани събития се съхраняват в: %SystemRoot%\System32\Winevt\Logs\ folder.

Event Viewer конзолата дава възможност за преглед на отделните категории логове и записаните в тях събития, както и генериране на справки за конкретни събития на база техния тип или EventID.



- **Windows Logs** – събитията, регистрирани от операционната система, се записват в три основни категории логове:

✓ Application Log – съдържа събития относно приложенията

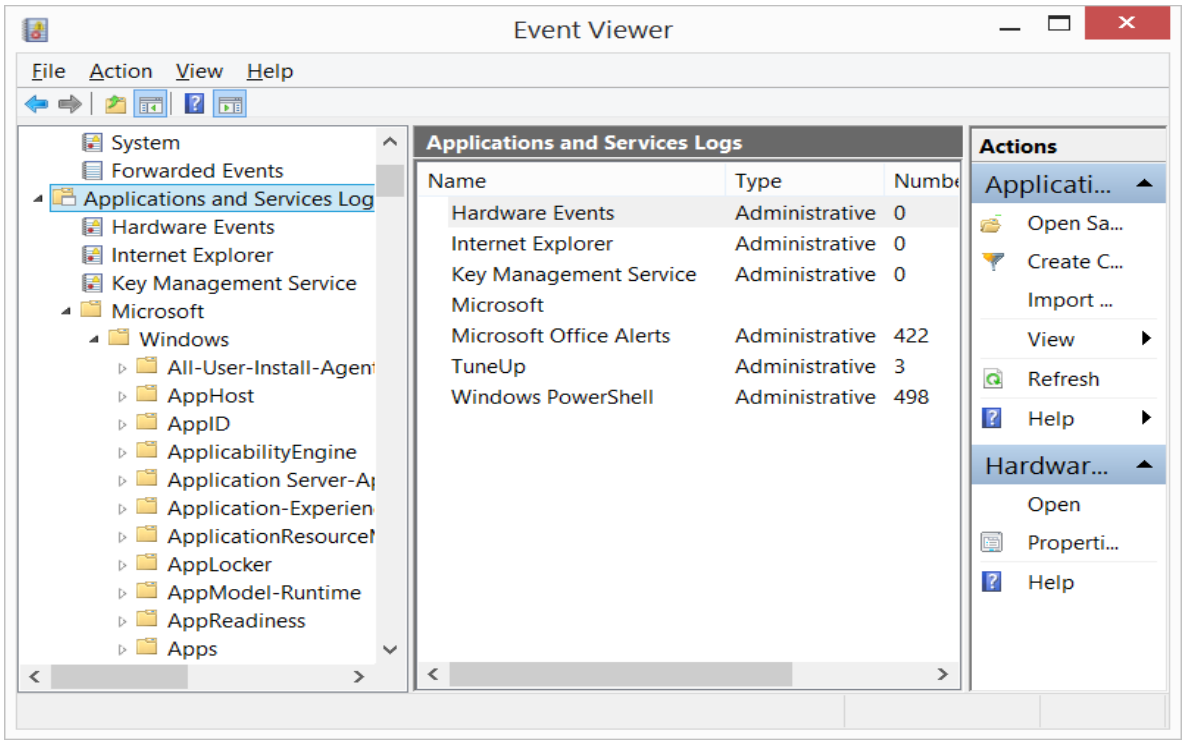
✓ System Log – съдържа системни събития

✓ Security Log – съдържа събития, касаещи сигурността на системата

Полезни Windows PowerShell команди, свързани със записа на събития (Event Logging):

- Get-EventLog
- Show-EventLog
- Write-Eventlog.

Windows Server 2012 (Windows 8) имат възможност за логване на допълнителни събития, отнасящи се до хардуерните компоненти, Internet Explorer и всички роли и функционалности на операционната система. Тези събития са събрани в отделна категория, наречена Applications and Services Logs, като в нея имаме разпределение на събитията съобразно функционалността, която те отразяват.



Типове събития и формат на данните - събитията, генерирани и записани от операционната система, биват следните типове:

- ✓ Information events – това са събития, които имат чисто информативен характер.
- ✓ Error events – това са събития, които отразяват настъпили грешки в конкретна функционалност или услуга. На тези събития администраторът трябва да отреагира веднага, защото те могат да са признак за предстоящо спиране или неработоспособност на системата.
- ✓ Warning events – това са предупредителни събития, които имат за цел да насочат вниманието на администратора към евентуален бъдещ проблем.

Security Log events classification – събитията, касаещи сигурността на системата, отразяват успешните или неуспешни опити за достъп до ресурси:

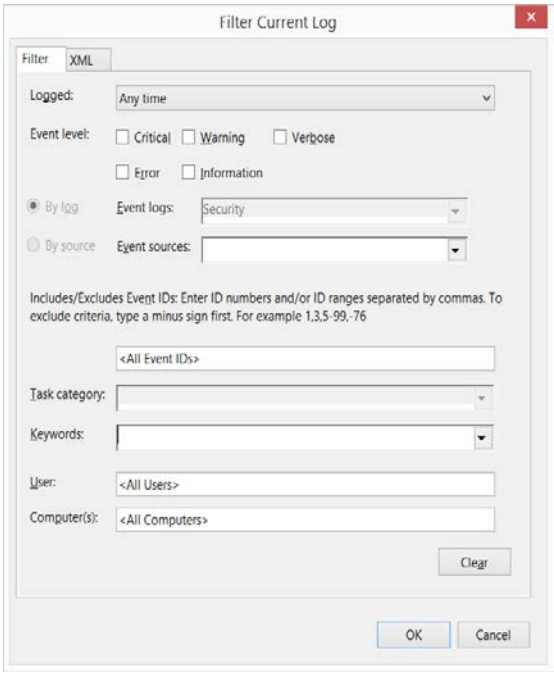
- ✓ Audit Success
- ✓ Audit Failure

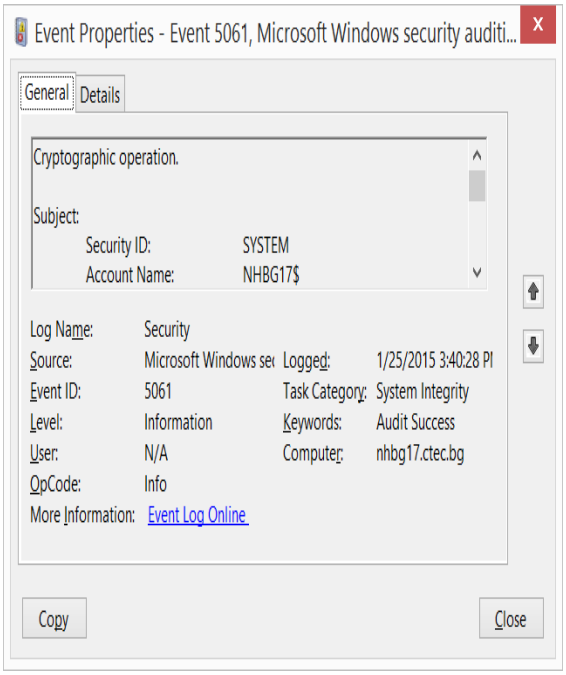
General and Details Tab in Event Viewer – дава допълнителна информация относно:

- ✓ Log Name from which the event came
- ✓ Event ID
- ✓ Component that generated event

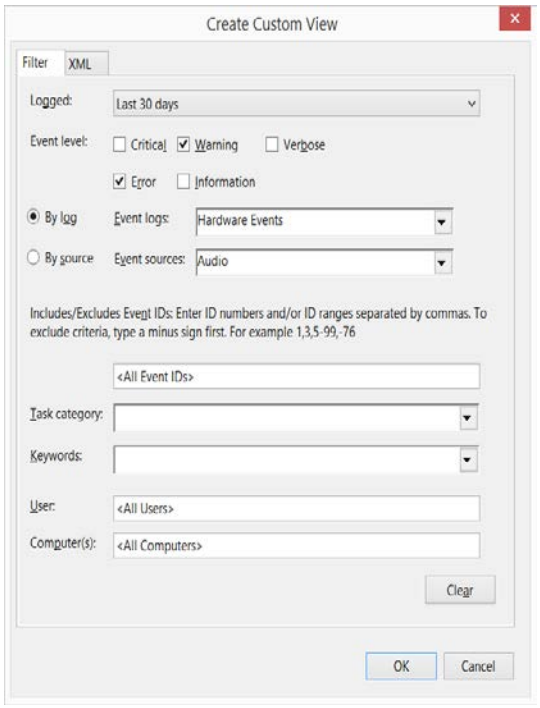
- ✓ Time of event logging
- ✓ User/Computer account on which the event was logged

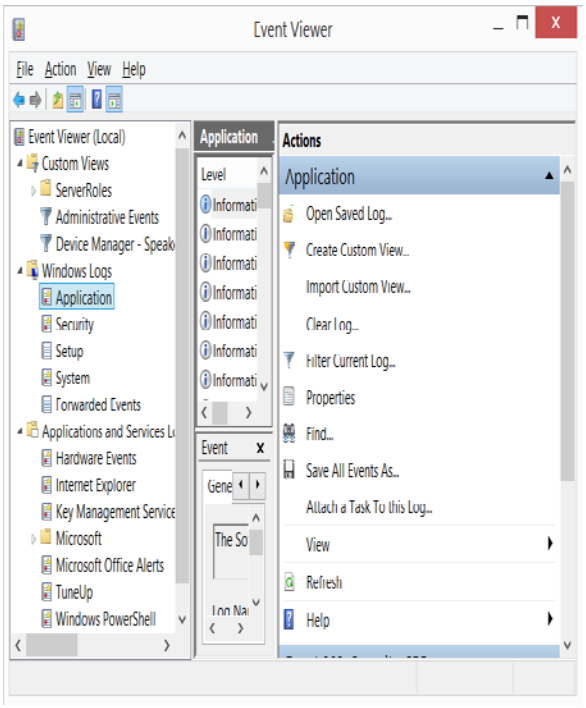
Следващите екрани демонстрират търсенето на конкретни събития през Event Viewer конзолата чрез прилагане на филтри, както и информация относно конкретно събитие, включваща Event ID, Logon Name, Source (източник на събитието), User, Category и др.





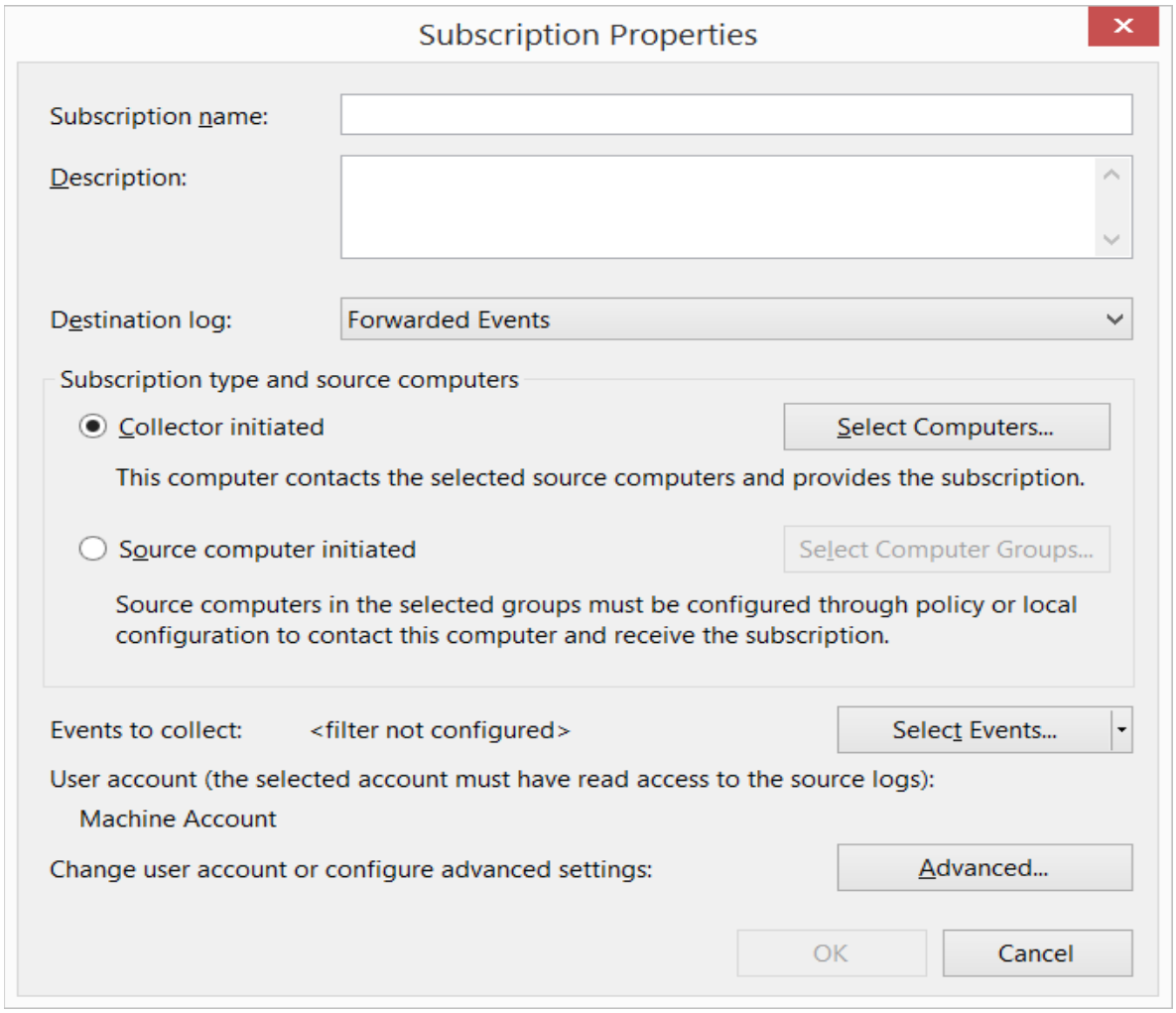
През Event Viewer конзолата можем да филтрираме записаните от системата събития, като можем да избираме категории събития, EventID, тип на логовете, потребител, компютър. Освен това, можем да експортираме филтрираните събития с цел по-късното им разглеждане чрез импортиране на друга система. Възможно е конфигуриране на задача (task) или изпълнение на script при запис на събитие с конкретен EventID.





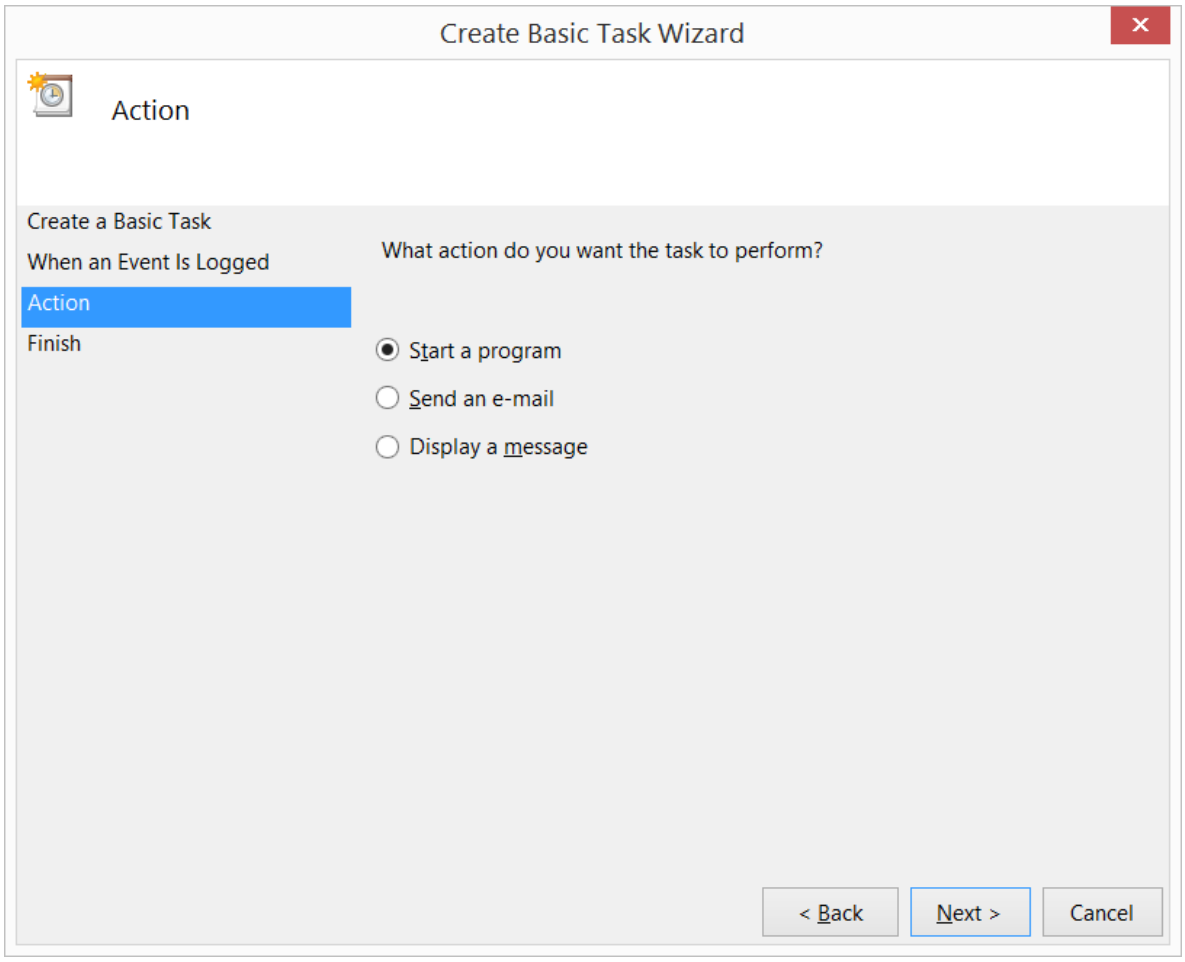
Event Logging Subscription (Абонирано отдалечено събиране на логовете) - Windows Server 2012 ни дава възможност да събираме събития от отдалечени машини и да ги съхраняваме на едно централно място с цел елиминиране на неоторизиран достъп и изтриване на логовете от даден потребител с повишени права върху дадена система. Тази функционалност се нарича Events Subscription, като генерираните събития се съхраняват на защитен сървър. Процесът по събирането и препращането на събитията може да бъде иницииран както от Collector сървъра, така и от клиентите.

Следният екран демонстрира възможностите на Subscription функционалността на Windows Server 2012.



Event Viewer Tasks - Event Viewer конзолата има вградена функционалност за изпълнение на конкретно действие при настъпване на дадено събитие. Типовете действия биват:

- Стартиране на програма
- Изпращане на мейл
- Визуализация на системно съобщение



- **Наблюдение на производителността (Performance Monitoring)**

Тесни места в производителността на Windows Server 2012 (Performance Bottlenecks) - получават се когато дадена система не може да обслужи заявка за достъп до ресурс или услуга в оптимално време. Обикновено заниженатa производителност е причинена от конкретен хардуерен компонент или е следствие на неоптимална конфигурация на системата и работещите на нея приложения или предлагани услуги.

Стратегии за откриване тесните места на дадена система:

- ✓ Добавяне на ресурси или надграждане (upgrade)
- ✓ Балансиране на товара между няколко сървъра
- ✓ Изпълнение на ресурсоемки приложения в ненатоварени периоди (нощем или в извън-работно време)
- ✓ Конфигуриране и настройка на системата с цел оптимална работа

Процес по наблюдение на производителността – включва използването на различни методи и инструменти за наблюдение, като те се разделят на две категории съобразно момента на наблюдаване на производителността на системата:

- Real Time Monitoring – те показват натовареността на системата в реално време. Такива са: Performance monitoring, Service Level Agreements (SLAs)
- Historical Monitoring – наблюдение на системата пост-фактум, т.е. анализ на вече случили се събития. Примери за такъв тип методи и инструменти са: Event Viewer, Performance Monitor.

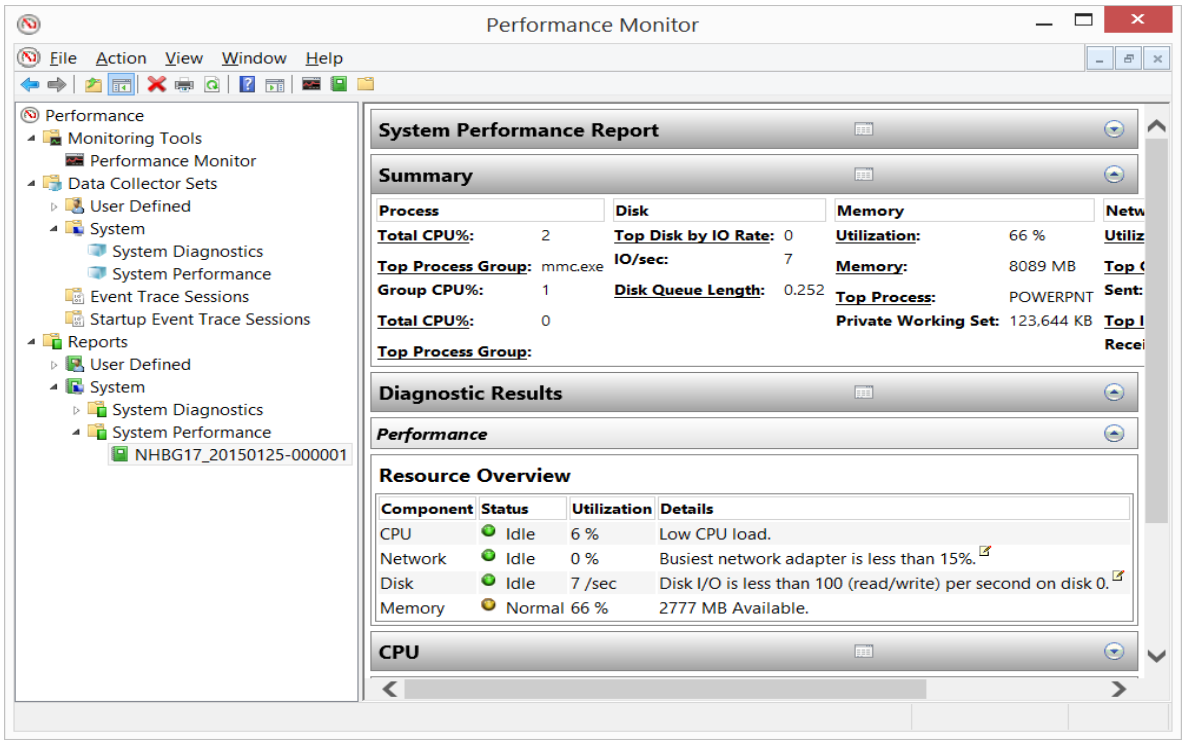
Наблюдението на производителността на всякакъв тип компютърни архитектури се базира на следене на стойностите на отделни параметри, наречени броячи на производителността (Performance Counters). Тези броячи ни дават информация относно стойността на отделни параметри на дадена система и нейното натоварване. Основните броячи, които дават базова информация и които се ползват най-често, са:

- Processor counters:
✓ Processor\% Processor Time
✓ Processor\Interrupts/sec
✓ System\Processor Queue Length
- Memory counters:
✓ Memory\Pages/sec
- Disk counters:
✓ Physical Disk\% Disk time
✓ Physical Disk\Average Disk Queue Length

Желателно е да следим основните броячи, касаещи работата на компютърната система като цяло. Добра практика е стойностите на тези броячи при нормална натовареност на системата да не надхвърлят 80 процента от максималната си стойност. Ако основните броячи надхвърлят този праг, следователно трябва да се помисли за добавяне на компютърна мощ (upgrade) или оптимизиране на системата.

Добра практика е използването на т.н. Data Collector Sets. Това са данни, на базата на които можем да правим анализ и статистика на параметрите и бързодействието на дадена система. Те съдържат следните типове данни:

✓ Performance counters
✓ Event trace data
✓ System configuration information



Конфигуриране и отстраняване на проблеми с DNS (Domain Name System):

Опции на DNS сървъра (DNS Server options) – DNS сървърът притежава редица опции, които могат да бъдат конфигуриране с цел оптимизиране работата на DNS услугата и повишаване на сигурността на системата.

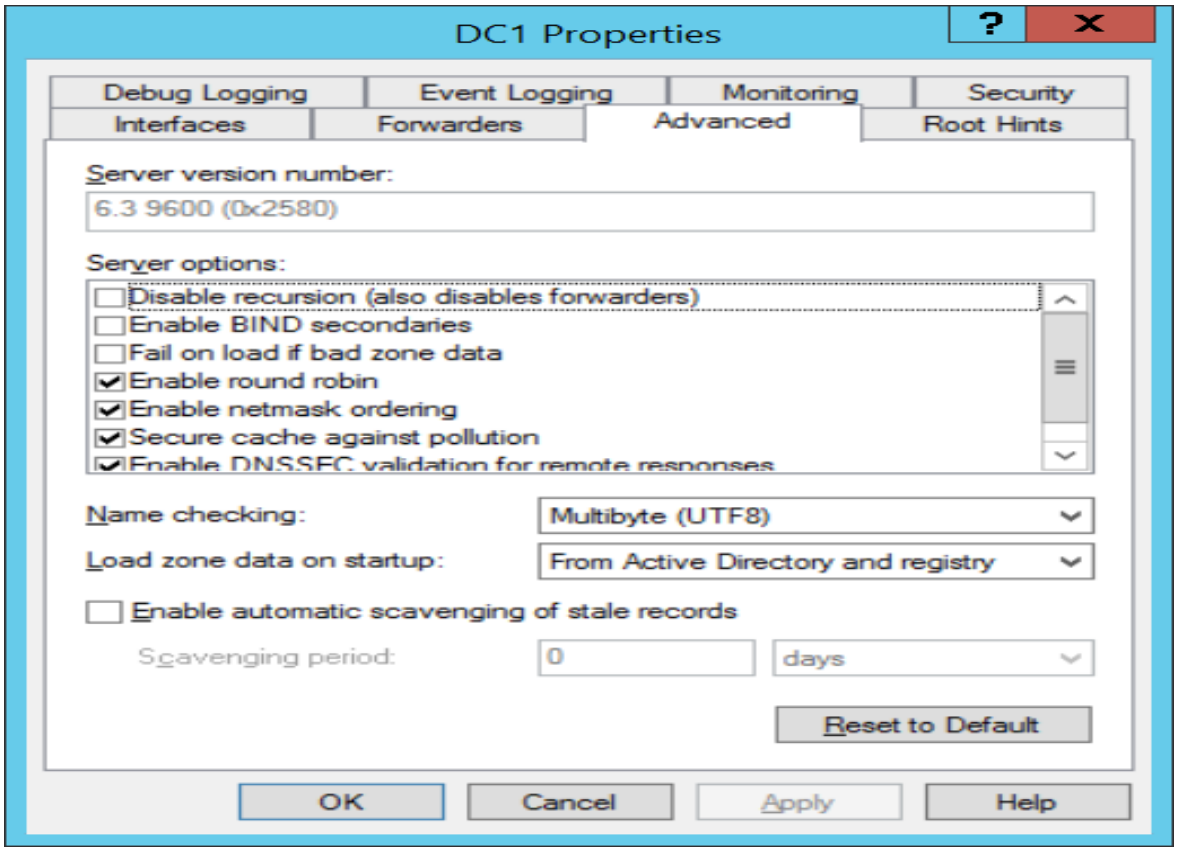
По известните опции на ниво DNS сървър са следните:

- Enable Round Robin – това е функционалност, която е пусната по подразбиране и осигурява балансиране на натовареността на система, която включва повече от един хост. Пример за такива системи са Web сървърите, при които Web услугата се предоставя от няколко сървъра, които са в Network Load Balancing (NLB) конфигурация, като всеки сървър има различен IP адрес и всяка Web заявка се поема от различен сървър.

При Round Robin, DNS сървъра притежава няколко прави (A) записа за конкретен ресурс, като всички записи имат едно и също име (hostname) и различни IP адреси. Така при последователни заявки DNS сървърът всеки път връща различни IP адреси, които водят към различни сървъри и така се реализира NLB функционалност на ниво DNS.

- DNS SEC (DNS Security Validation) – представлява функционалност, която реализира цифрово подписване на всеки един запис от базата данни на DNS сървъра. По този начин се валидират отговорите, върнати от DNS сървъра и се гарантира тяхната автентичност.
- Enable automatic scavenging of stale records – тази функционалност позволява автоматично премахване на всички стари и неактуални записи от базата на DNS сървъра. Възможността за такова изчистване на старите записи е базирана на т.н. параметри на ресурсните записи. Ресурсните записи притежават параметри, които се използват от DNS сървъра с цел поддържане на актуална информация относно записите в дадена DNS зона. Най-важният от тези параметри е Time To Live (TTL). Това е параметър, който показва колко време конкретния DNS запис ще бъде валиден, след което трябва да бъде подновен от клиента. Действията, които могат да бъдат предприети от DNS сървъра, са следните:
  - ✓ Aging (остаряване на записите) – когато периода на валидност на даден запис изтече и той не бъде подновен от клиента.
  - ✓ Scavenging (премахване на стари записи) – процес на автоматично премахване на стари записи от базата на даден DNS сървър.

Следният екран демонстрира възможните опции, касаещи DNS сървъра:



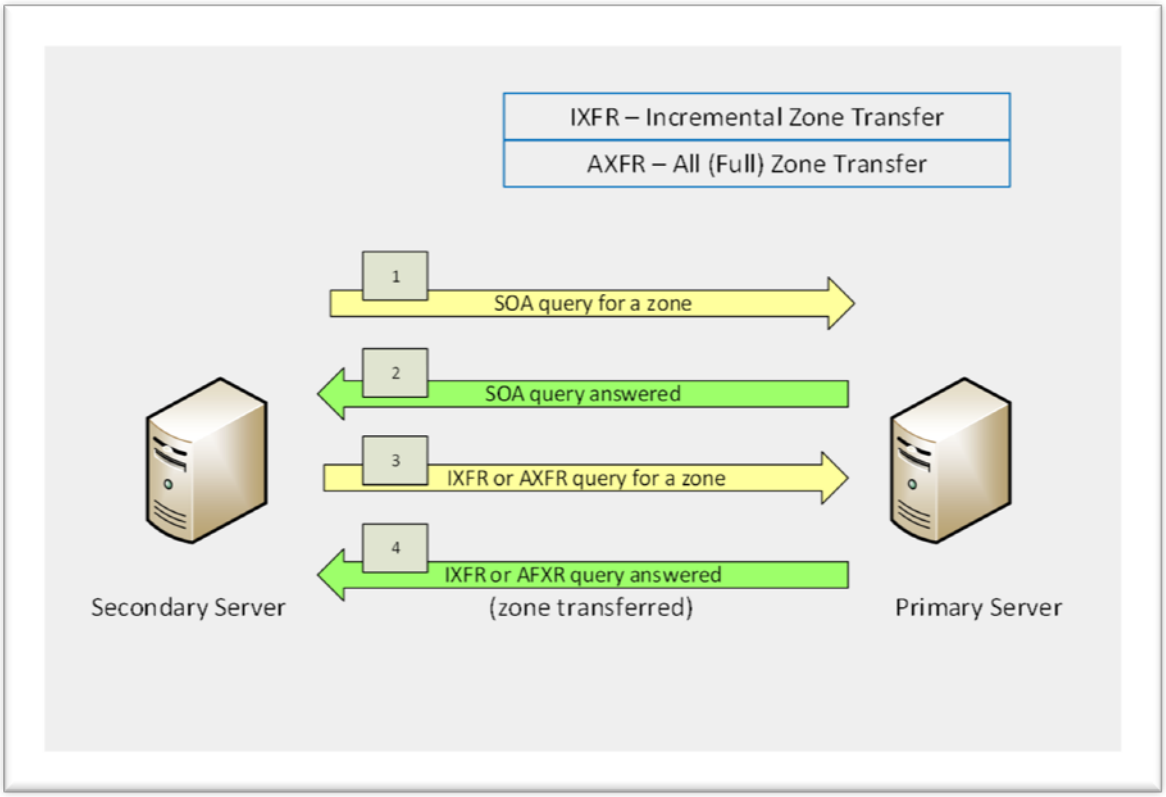
DNS зонов трансфер (DNS Zone Transfer) – един от основните моменти, които изискват внимание от страна на системния администратор и могат да доведат до проблеми, е свързан с трансфера на зонова информация между отделни DNS сървъри. DNS зоновият трансфер е синхронизация на DNS зона между DNS сървъри с цел оеднаквяване на зоновата информация. Протича под формата на четири стъпки, като са възможни два типа трансфер на данните от зоната: инкрементален и пълен.

Процесът по трансфер на зонова информация преминава през четири стъпки, като е възможно да трансферираме цялата зона или само инкрементални промени в нея.

С цел повишаване сигурността при зоновия трансфер е желателно да бъдат реализирани следните добри практики:

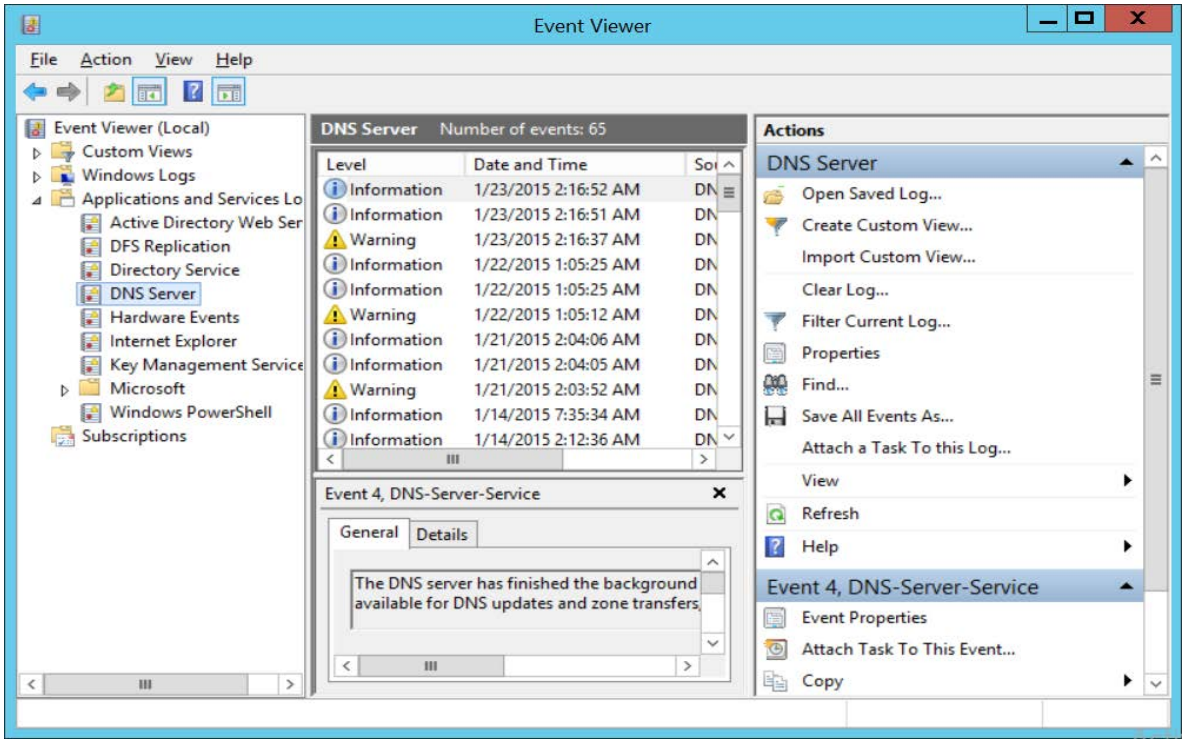
- ✓ Ограничаване на зоновия трансфер само до определени сървъри
- ✓ Криптиране на zone transfer трафика
- ✓ Ползване на Active Directory-integrated zones

Следната схема демонстрира отделните стъпки при трансфера на DNS зона между два сървъра.



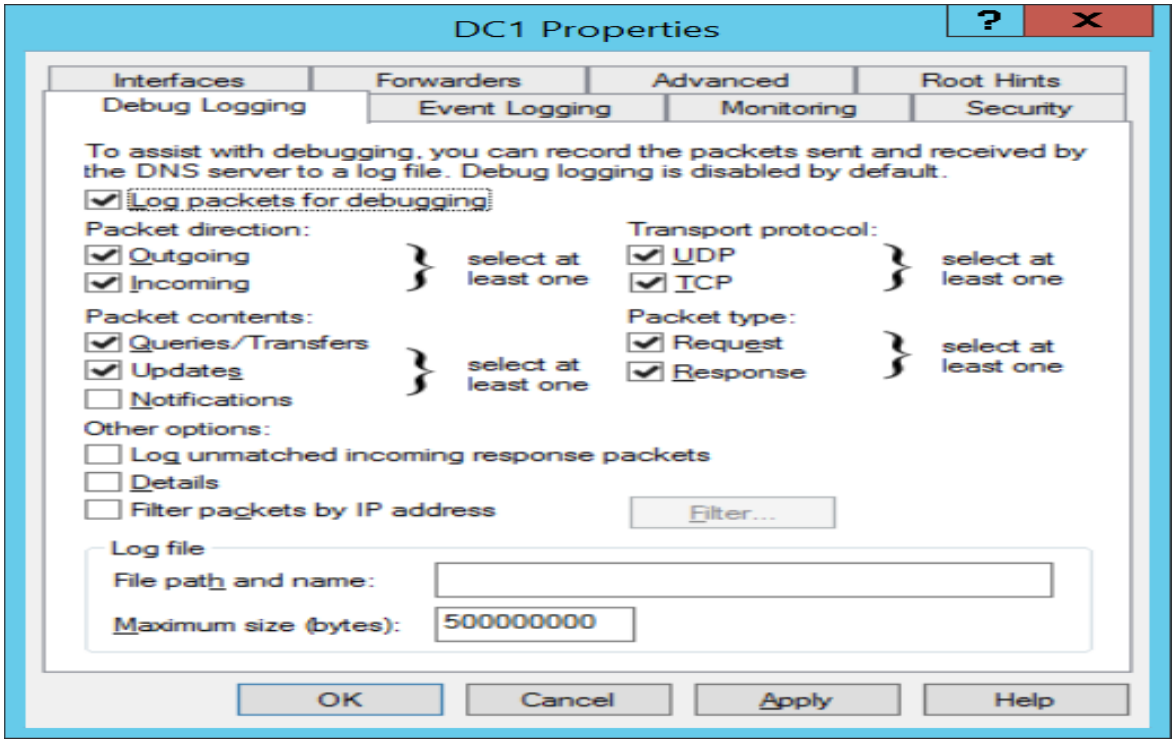
Мониторинг на DNS сървър – наблюдението на състоянието на DNS сървъра включва няколко типа мониторинг:

- Мониторинг на DNS сървър чрез DNS Event Log - в Event Viewer има специална категория, наречена DNS Server, която съдържа само записи на събития, касаещи активността на DNS сървъра.



- Мониторинг на DNS сървър чрез Debug Logging - DNS сървърът, реализиран в среда на Windows Server 2012, дава възможност да бъде конфигурирано подробно логване на всички пакети, получени или изпратени от DNS сървъра, с цел детайлно наблюдение на активността на самата DNS сървърна роля. Тази функционалност се нарича DNS Debug Logging. Тя е спряна по подразбиране и води до увеличена консумация на ресурсите на машината, на която е инсталирана DNS ролята.

Следният екран демонстрира възможностите на DNS Debug Logging.



- **Мониторинг на DNS сървър чрез Windows PowerShell -** Windows Server 2012 дава възможност за допълнителен мониторинг на DNS функционалността чрез употребата на Windows PowerShell команди за DNS конфигуриране, управление и отстраняване на проблеми. По-долу са посочени няколко примерни команди:
  - ✓ Get-DnsServerStatistics parameters:
  - ✓ ZoneQueryStatistics
  - ✓ ZoneTransferStatistics
  - ✓ ZoneUpdateStatistics
  - ✓

Windows Server 2012 притежава и възможност за активиране и управление на DNS Sec функционалността през Windows PowerShell. Инструкции относно управлението на DNSSec през Windows PowerShell може да намерите на следния адрес: http://blogs.technet.com/b/wsnetdoc/archive/2014/03/26/dnssec-on-windows-server.aspx

Поддръжка на AD DS

Дейностите по поддръжка на Активна Директория са разнообразни и засягат различни аспекти. Основните от тях са разпределени в следните категории:

- **Инсталиране на виртуализиран домейн-контролер –** виртуализираният домейн-контролер е виртуално копие на хардуерен такъв. Виртуалният домейн-контролер не се различава по функционалност и възможности от един реален домейн-контролер, инсталиран върху специфична хардуерна конфигурация и в среда на Windows Server 2012. Основните характеристики на виртуализирания домейн-контролер са следните:

  ✓ Scalability (Възможност за добавяне на нови ресурси и за разширяване на системата)

  ✓ Независимост от хардуера

  ✓ По-бързо възстановяване при повреди или проблеми в сравнение с хардуерен домейн-контролер

  ✓ Windows Server 2012 Hyper-V е напълно подходяща среда за виртуализиране на домейн инфраструктура

  ✓ Time synchronization (синхронизиране на времето между host и guest машините)

  ✓ Single point of failure – при проблем или отпадане на хардуерната host машина отпадат всички guest виртуални машини.

Употреба на checkpoints при виртуализиран домейн-контролер и проблеми, свързани с AD DS Replication процеса:

✓ Промените в Active Directory се правят на ниво атрибут на даден обект, не на ниво обект.

✓ Всеки домейн-контролер отразява промените в атрибутите на обектите, като генерира т.н. Update Sequence Numbers (USNs).

✓ Възстановяването от checkpoint води до изтриване на USNs.

✓ Checkpoints са полезни за тестови среди или среди за разработване, но употребата им в среда на Активна Директория може да доведе до повреда на нейната база данни.

Изисквания за безопасна виртуализация на домейн-контролери:

- ✓ Hypervisor-ът да поддържа Virtual Machine Generation Identifier, като например Windows Server 2012 Hyper-V.
- ✓ Виртуализираните домейн-контролери да бъдат с операционна система Windows Server 2012 или Windows Server 2012 R2.
- ✓ Virtual Machine Generation Identifier (VMGI) – параметър, който позволява на виртуализирания домейн-контролер да разбере дали е възстановен от checkpoint. При всяко връщане от checkpoint, на виртуализирания домейн-контролер му се генерира нов VMGI.
- ✓ Host машината поставя VMGI като параметър в BIOS-а на виртуализирания домейн-контролер, който от своя страна в последствие съхранява идентификатора в AD DS базата.
- ✓ Виртуализираният домейн-контролер проверява VMGI всеки път при стартиране и преди всяка заявка за запис или корекция на AD DS базата. Ако VMGI от базата и от BIOS-а имат различни стойностти, то домейн-контролера разбира, че е възстановен от checkpoint и взема предпазни мерки с цел избягване на повреди по базата на AD DS.

Предпазни мерки от страна на виртуализираните домейн-контролери при възстановяване от checkpoint (snapshot) - когато домейн-контролерът разбере, че е възстановен от checkpoint, той предприема предпазни мерки с цел избягване на повреди по базата на AD DS. Тези предпазни мерки включват следните действия:

- ✓ Отмяна на локалния RID pool.
- ✓ Назначаване на нов Invocation ID на базата на домейн-контролера, като по този начин той се представя като нов за домейна и предизвиква репликация от останалите домейн-контролери към него.

Клониране на домейн-контролер – клонирането е процес, при който ние създаваме идентично копие на даден домейн-контролер, което копие може да бъде ползвано в последствие за инсталиране на нов домейн-контролер в среда на Активна Директория.

Причини за клониране на домейн-контролери:

- ✓ Бързо дистрибутиране на нови домейн-контролери
- ✓ Употреба на инфраструктури от типа „Private Cloud”
- ✓ Стратегии за бързо възстановяване при отпадане на работещ домейн-контролер

Етапи в процеса на клониране на домейн-контролер:

- ✓ Добавяне на домейн-контролера в Cloneable Domain Controllers group

- ✓ Проверка за съвместимост на приложенията и услугите
- ✓ Създаване на DCCloneConfig.xml файл
- ✓ Експортиране на домейн-контролера
- ✓ Създаване на нови домейн-контролери чрез импортиране на предварително експортирания домейн-контролер

Добри практики при виртуализацията на домейн-контролери:

- Недопускане на „single point of failure“
- Всички компютри да ползват общ и надежден източник на времева синхронизация
- Употреба на технология за виртуализация, ползваща Virtual Machine Generation Identifier параметър
- Избягване употребата на точки за възстановяване (checkpoint or snapshots)
- Употреба на техниките за клониране на домейн-контролери
- Употреба на конвенция за имената на компютрите в домейна, позволяваща клониране на домейн-контролери

- **Инсталиране на Read-Only Domain Controller (RODC) –** RODC е тип домейн-контролер, който съдържа read-only копие на базата данни на активната директория и се ползва в незащитени среди, където вероятността този домейн-контролер да бъде компроментиран е голяма.

Употреба на Read-Only Domain Controller (RODC): RODC осигурява следните функции, като едновременно с това създава защитена среда за автентикиране и оторизиране на домейн потребители и елиминира рисковете от компроментиране на базата на активната директория в случай на кражба на RODC:

- ✓ RODC Credential caching - Credential caching се управлява от Password Replication Policies. Password Replication Policies определят кои потребителски и компютърни акаунти ще могат да ползват RODC и съответно съдържат allowed и denied list, базирани на следните групи:

- Allowed RODC Password Replication Group – само членовете на тази група могат да се логват на RODC контролера.

- Denied RODC Password Replication Group – на членовете на тази група е изрично забранена възможността за логване на RODC контролера.

Добра практика: Да не се кешират имена и пароли (credentials) на домейн административни акаунти.

- ✓ Разделяне на административните роли относно RODC.

✓ Възможност за реализация на Read-only DNS.

Етапи при създаването на RODC:

✓ Проверка за несъществуване на компютърен акаунт в домейна, отговарящ на RODC

✓ Предварително създаване на RODC акаунт в AD DS в контейнера Domain Controllers

✓ Стартиране на AD DS Installation Wizard върху новия RODC

Особеностти при локалното администриране на RODC:

- Делегиране управлението на RODC на локални администратори
- Промотиране на един потребител за администратор на RODC
- Кеширане на информация за логване само на делегираните администратори на RODC
- Конфигуриране на управлението на RODC чрез следните методи:

✓ Managed By tab of RODC account

✓ dsmgmt

✓ ntdsutil

- **Администриране на AD DS – основните инструменти за администриране на Активна Директория от страна на системните администратори са следните:**
  - **Active Directory Administration Snap-ins –** най-често използваните snap-in функционалности, които могат да бъдат добавени към Microsoft Management Console (MMC) и които се ползват за ежедневна употреба от администраторите, са следните:

✓ Active Directory Users and Computers

✓ Active Directory Sites and Services

✓ Active Directory Domains and Trusts

✓ Active Directory Schema

Добра практика е домейн ресурсите да се управляват от клиентски компютър с инсталирана клиентска операционна система, като за да управлява домейн средата, администраторът трябва да инсталира съответния Remote Server Administration Tools (RSAT). RSAT е конкретен за съответната клиентска операционна система и може да бъде свален от следната локация: https://www.microsoft.com/en-

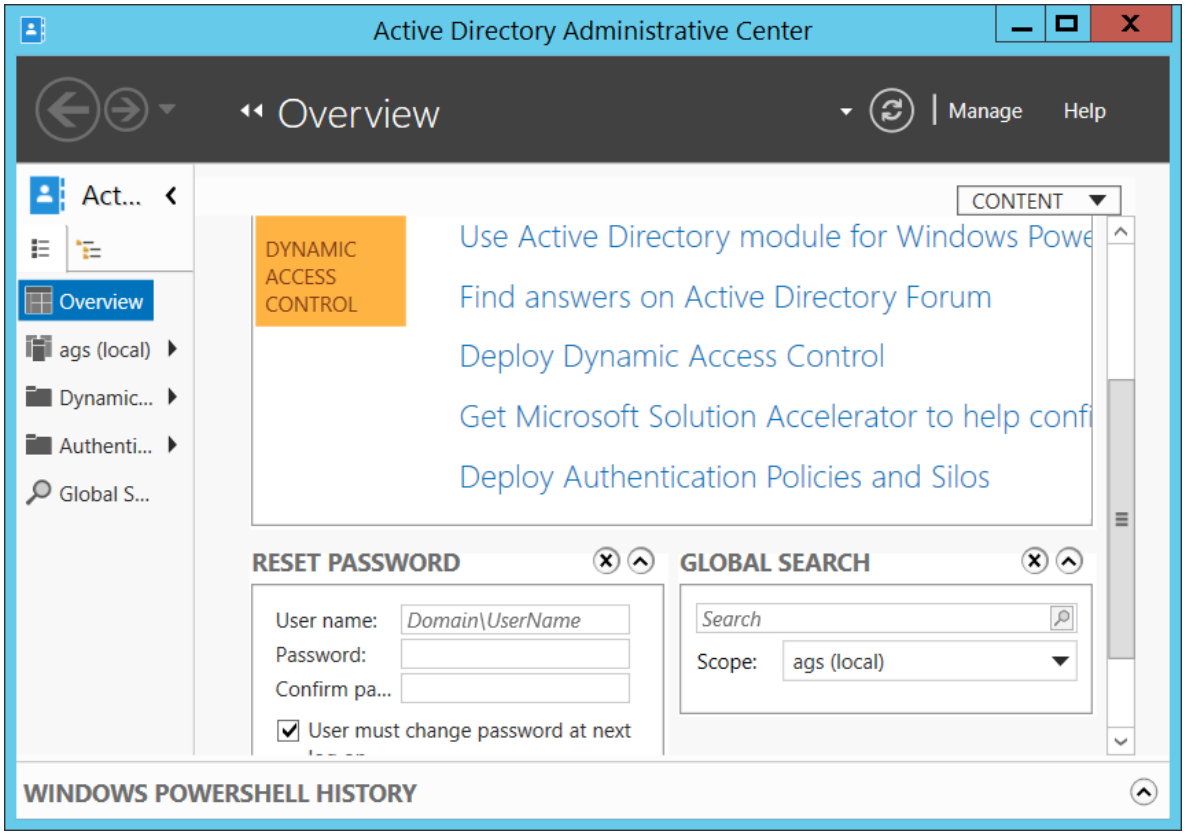
us/search/Results.aspx?q=remote%20server%20administration%20tool&form=DLC

- **Active Directory Administrative Center** е задачно-ориентирана конзола за управление на домейн среда и нейните обекти. Тя е базирана на Windows PowerShell команди и скриптове, които се изпълняват на заден план скрито от потребителя. Основните новости в Active Directory Administrative Center при Windows Server 2012 са:

✓ AD Recycle Bin

✓ Fine Grained Password Policy

✓ Windows PowerShell History Viewer



- **Ntdsutil** е инструмент, който е основно средство за управление на задачи, свързани с базата на активната директория и разполага със следните функционалности:

  - Управлява и контролира FISMO ролите

- Поддържа AD DS базата чрез:
- ✓ Offline defragmentation
- ✓ Create and mount snapshots
- ✓ Move database files
- Поддържа домейн-контролер метаданните
- Нулира Directory Services Restore Mode password

- **Active Directory module for Windows PowerShell -** осигурява управлението на AD DS в следните области:
  - ✓ User and computer management
  - ✓ Group management
  - ✓ OU and Password policy management
  - ✓ Searching and modifying objects in AD DS
  - ✓ Forest and domain management
  - ✓ Domain controller and FISMO roles management
  - ✓ Managed service account management
  - ✓ Site replication
  - ✓ Central access and claim management
- **AD DS Backup and Recovery**:

  AD DS backup – най-често ползваните типове backup при домейн-контролери са:

  ✓ System state backup – архивно копие на системното състояние на домейн-контролера.

  ✓ Full backup – копие на целия системен диск (или на целия домейн-контролер).

  AD DS restore:

  ✓ Non-authoritative restore – процес на възстановяване на домейн-контролер, при който той се репликира от останалите работещи домейн-контролери в домейна.

  ✓ Authoritative restore – дава възможност за възстановяване на изтрити обекти.

- ✓ Full server restore (performed in Windows RE) – процес на възстановяване на целия сървър, върху който е инсталирана домейн-контролер функционалността (AD DS role).

- **Управление на базата на AD DS –** базата данни, в която Active Directory съхранява всички домейн обекти и техните атрибути е от типа Windows Internal Database. Този тип бази ползват транзакшън ловове за вкарване на информация в базата и имат вграден механизъм за защита и недопускане на грешки.

Windows Server 2012 дава възможност AD DS ролята да бъде инсталирана и тя да работи като услуга в операционната система. По този начин AD DS може да бъде стартирана и спирана от Services административната конзола.

Състояния на AD DS:

- ✓ AD DS started
- ✓ AD DS stopped
- ✓ Directory Services Restore Mode (DSRM)

Windows Server 2012 ползва snapshots като моментни снимки на състоянието на базата на активната директория. AD DS Snapshots представляват копия на моментното състояние на базата на Active Directory към конкретен момент. Windows Server 2012 ни дава следните възможностти в употребата на AD DS Snapshots:

- Създаване на AD DS snapshot и монтаж на този snapshot към уникален порт с помощта на Ntdsutil командата
- Зареждане на snapshot: Десен бутон върху AD Users and Computers и избиране на Connect to Domain Controller, след което въвеждаме serverFQDN:port
- Преглед на snapshot в read-only режим без възможност за възстановяване на данни от този snapshot
- Възможност за възстановяване на конкретен snapshot

AD Recycle Bin е функционалност, която при Windows Server 2012 може да се ползва през Active Directory Administrative Center и има графичен интерфейс (за разлика от Windows Server 2008, където ползването на AD Recycle Bin става през Command Line Interface). AD Recycle Bin осигурява следните функционалности:

- ✓ Осигурява възможност за възстановяване на изтрити директорийни обекти без спиране на AD DS.
- ✓ За възстановяването на изтрити обекти се ползва Windows PowerShell или Active Directory Administrative Center

Част VI: Модел на сигурност.

Осигуряване на сигурност в Windows сървъри

Сигурността в среда на Windows Server 2012 е насочена в следните направления:

- **Общ преглед на сигурността в Windows –** в концепцията на Майкрософт за сигурност на операционните системи е залегнало общоприетото понятие AAA модел. **AAA модела** е модел за контрол на достъпа до ресурси, който включва три компонента:

✓ Authentication (автентикация) – процесът на проверка на user/computer credentials за правилност.

✓ Authorization (оторизация) – процесът по оторизиране (разрешаване достъпа до ресурси).

✓ Accounting and Auditing – мониторинг, контрол и одит върху активността на даден потребител (процес) относно даден ресурс.

Технологии и функционалности за реализиране на сигурност при Windows Server 2012:

- **User Account Control (UAC)** е услуга, която предотвратява възможността приложенията да добият административни права без знанието на потребителя.

✓ UAC предпазва компютърната система от автоматично инсталиране на зловреден софтуер.

✓ UAC предупреждава потребителя когато той (или дадено приложение) се опитва да стартира процес, изискващ административни права.

✓ Без UAC и когато потребителя има административни права, всяко приложение, стартирано в контекста на потребителския акаунт, ще има административни права върху системата.

- **Методи за контрол върху файлове и папки** - основните методи за контрол върху файлове и папки са базирани на следните технологии:

  - File and folder permissions:

  ✓ Достъпни са при NTFS и ReFS

  ✓ Определят правата при локален достъп до ресурсите

  ✓ Винаги се прилагат

- Shared folder permissions:

✓ Достъпни са при FAT32, NTFS и ReFS

✓ Определят правата върху ресурсите при достъпването им по мрежата

- Effective permissions (Ефективни права при отдалечен достъп до ресурси)

✓ Комбинацията от File/Folder Permissions и Share Permissions, като най-рестриктивните права имат предимство

- Dynamic Access Control:

✓ Базиран е на file, folder and share permissions

✓ Ползва централни политики (central policies), които са условни и са изградени на база атрибути на обектите и твърдения (claims)

- **Account Policies** наричаме политиките, конфигурирани и ползвани с цел повишаване сигурността на потребителските акаунти. Те спомагат за намаляване вероятността от неоторизиран достъп до системи и ресурси, като се прилагат редица техники и конфигурационни параметри. Основните параметри, които засягат сигурната употреба на потребителските акаунти, са следните:

- Password policies:

✓ Complex Password

✓ Enforce password history

✓ Maximum password age

✓ Minimum password age

✓ Minimum password length

✓ Store password using reversible encryption

- Account Lockout policies:

✓ Lockout threshold

✓ Lockout duration

✓ Reset account lockout after

- **Fine-Grained Password Policies** е функционалност, която позволява прилагането на различни password и account lockout политики по отношение на индивидуални потребители или глобални секюрити групи в даден домейн.

- Компоненти на Fine-Grained Password Policies:

- ✓ Password Settings Container
- ✓ Password Settings objects
- Характеристики на Fine-Grained Password Policies:
- Прилагат се на ниво потребител или глобална секюрити група
- Не могат да се прилагат на ниво огранизационна единица (Organizational Unit – OU)
- Имат предимство пред домейн политиката (Default Domain Policy)
- Може да бъдат конфигурирани няколко Password Policies в един домейн
- Конфигурират се през Active Directory Administrative Center или Windows PowerShell

- **Auditing** е процес на следене активността на потребителите и операционната система и записване на генерираните събития в специален файл, наречен log file. Освен стандартните настройки, касаещи базово одитиране на логването и достъпа до ресурси, в Windows Server 2012 съществува възможност за одит на повече категории събития чрез т.н. **Advanced Auditing Options** (success/failure):

  - ✓ Account Logon
  - ✓ Account Management
  - ✓ Detailed Tracking
  - ✓ DS Access
  - ✓ Logon/Logoff
  - ✓ Object Access
  - ✓ Object Change
  - ✓ Privilege Usage
  - ✓ System
  - ✓ Global Object Access Auditing
  - ✓ **Auditing is not enable by default**

- **Digital Certificate (Цифров Сертификат)** – цифровите сертификати са в основата на редица технологии за сигурност. Основните характеристики на цифровите сертификати са следните:

  - ✓ Основен компонент на Public Key Infrastructure (PKI)

- ✓ Ползва асиметрично криптиране
- ✓ Сертификатът е метод за разпространение на публичния ключ
- ✓ Сертификатът обвързва публичния ключ с обекта, който е притежател на съответния частен ключ

Цифровият сертификат съдържа следната информация:

- ✓ Информация за собственика на сертификата
- ✓ Публичният ключ на собственика на сертификата
- ✓ Информация за издателя на цифровия сертификат
- ✓ Дата на издаване и на изтичане на сертификата
- ✓ Сериен номер
- ✓ Цифров подпис на издателя

Повече информация относно цифровите сертификати може да намерите на следния адрес: http://en.wikipedia.org/wiki/Public_key_certificate

- **Контрол на достъпа (Access Control)** – контролът на достъпа до ресурси в среда на Windows Server 2012 се осъществява на базата на Discretionary access control листове. Всеки ресурс притежава такъв лист, които съдържа множество записи, наречени access control entries (ACEs). Основните характеристики на DAC листовете (списъци) и Access Control записите са следните:

- Discretionary access control list (DACL):
- ✓ Съдържа Access Control Entries (ACEs)
- ✓ Контролира изцяло достъпа до съответния ресурс, като определя кой security principle какви права притежава
- ✓ DACL е функционалност на NTFS/ReFS
- Access Control Entry (ACE):
- ✓ Единичен запис, който разрешава или забранява конкретен вид достъп на специфичен потребител, група или компютърен акаунт до конкретен ресурс

Съществуват стандартни и разширени права, които могат да бъдат давани на потребителите (компютърните акаунти или процесите) за достъп до ресурси в NTFS или ReFS файлови системи. Разширените права дават възможност за много по-детайлно контролиране на активността на даден субект (потребител, процес, компютър) върху конкретен обект. Правата са основен елемент на контрола на достъпа до ресурсите и се конфигурират през т.н. секюрити дескриптор на даден ресурс, който от своя стра-

на може да бъде достъпен, като се кликне с десен бутон върху ресурса и се избере Properties и след това Security.

Standard Permissions	Advanced Permissions
• Full Control • Modify • Read & Execute • List Folder Contents • Read • Write • Special Permissions	• Full Control • Traverse Folder/Execute File • List Folder/Read Data • Read Attributes • Read Extended Attributes • Create Files/Write Data • Create Folders/Append Data • Write Attributes • Write Extended Attributes • Delete Subfolders and Files • Delete • Read Permissions • Change Permissions • Take Ownership • Syncronize

- **Одит на файлове и папки** – одитът на файлове и папки доставя следните функционалности:

  ✓ Дава информация за достъпа до файлове и папки, както и кой модифицира информацията

  ✓ Осигурява отчетност (reporting) относно използването на даден ресурс

  • Компоненти на успешния одит:

  ✓ Инструкция към конкретния сървър кои сфери на операционната система да бъдат одитирани. Осъществява се през Group Policy

  ✓ Разрешаване на одитиране на ниво security descriptor на конкретния ресурс

  • Мониторинг на одит събития:

  ✓ Събитията се записват в Windows Security Log

  ✓ Могат да бъдат разглеждани с Event Viewer

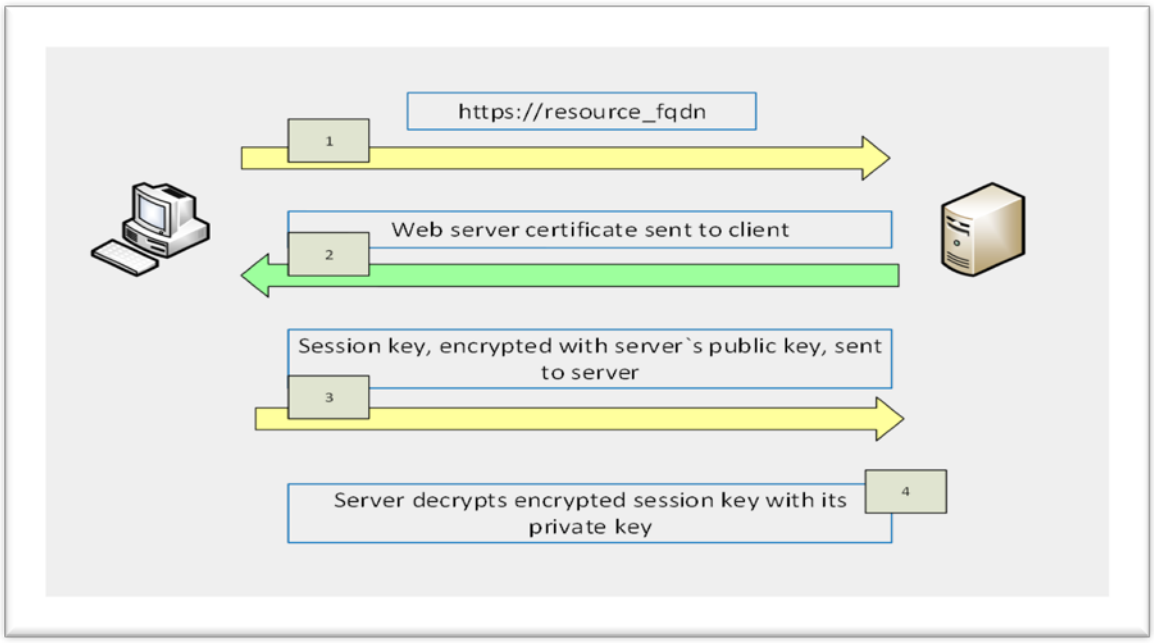
- **Dynamic Access Control – DAC** е технология, която притежава следните характеристики:

- ✓ Допълнителен слой от защитни техники, който се разполага над NTFS правата за контрол на достъпа до конкретен ресурс
- ✓ Ползва централни политики (central policies), които са условни и са изградени на база атрибути на обектите и твърдения (claims)
- ✓ Контролът над ресурсите е силно гранулиран и е на ниво атрибути: Full Time employee; location; department; manager; names
- ✓ Конфигурира се през Active Directory Administrative Center

Подробна информация относно Dynamic Access Control може да намерите на адрес: https://technet.microsoft.com/en-us/library/dn408191.aspx

- **Прилагане на криптиране –** криптирането на информацията е с цел конфиденциалност и е залегнало в следните направления и технологии**:**
- **Приложение на сертификатите в процеса на криптиране –** цифровите сертификати са метод за разпространение на единия от двойката математически обвързани ключове, които се използват от всеки участник в процеса на комуникация. Пример за употребата на сертификати е Hypertext Transfer Protocol Secure (HTTPS) протокола. Той ползва Secure Sockets Layer (SSL)/Transport Layer Security (TLS) като основен протокол и е базиран на комбинация от асиметрично и симетрично криптиране.

Следният пример демонстрира установяването на HTTPS сесия между уеб бразър и уеб сървър:



- **Encrypting File System (EFS):** Характеристики на Encrypting File System (EFS):
  - ✓ Технология за криптиране на файлове и папки
  - ✓ Поддържана само от NTFS дялове
  - ✓ Позволява прозрачно криптиране и декриптиране
  - ✓ Ползва комбинация от симетрично и асиметрично криптиране
  - ✓ EFS ползва AES 256 bit symmetric encryption by default
  - ✓ EFS е разрешена като функционалност по подразбиране
  - ✓ Може да бъде забранена през Group Policy
  - ✓ EFS криптиран файл, преместен в FAT или ReFS, престава да бъде криптиран
- **BitLocker** е функционалност, която реализира криптиране на данните върху даден диск. Основните възможности на BitLocker са:
  - ✓ Осигурява надеждно криптиране на данните и проверка за интегритет на процеса по стартиране на операционната система
  - ✓ Инсталира се като Windows Server 2012 Feature от Server Manager
  - ✓ Конфигурира се през Group Policy
  - ✓ BitLocker To Go – позволява криптиране на преносими устройства

Информация относно имплементирането на BitLocker може да намерите на следните адреси:

http://en.wikipedia.org/wiki/BitLocker
https://technet.microsoft.com/en-us/library/cc766295(v=ws.10).aspx

Част VII: Нови възможности и предизвикателства за работа от тип "работа в облак".

Прилагане на сървърна виртуализация с Hyper-V:

- **Характеристики на сървърната виртуализация:**

✓ По-ефективно използване на хардуерните ресурси

✓ Изолация на приложения и услуги

✓ Разпределяне на натоварването

✓ Прозрачна за потребителя

✓ Guest виртуалните машини могат да ползват различни операционни системи

✓ Улеснен процес по инсталация на сървъри чрез:

- Шаблони за виртуални машини (Virtual machines templates) – достъпни през System Center 2012 Virtual Machine Manager (VMM)
- App-Controller virtual machine self-service portal – портал, през който потребителя може да заяви виртуална машина, генерирана на база предварително създадени шаблони

Сървърната виртуализация при Windows Server 2012 позволява следните типове виртуализирани услуги**:**

Виртуализация на работен плот (Desktop Virtualization) – включва следните технологии:

✓ Client (Local) Hyper-V

- достъпно при Windows 8/8.1

- не поддържа миграция на виртуални машини (Virtual Machine Migration)

- позволява публикуване на приложения, инсталирани на guest виртуалната машина, в старт менюто на Host машината

- позволява виртуализация на стари операционни системи

✓ Virtual Desktop Infrastructure (VDI):

- потребителите се логват на виртуални машини през Remote Desktop Protocol, като всеки потребител разполага със собствена работна среда

- изисква инсталацията на Remote Desktop Service

- изисква инсталацията на Remote Desktop Virtualization Host role service

  ✓ RemoteFX – функционалност, позволяваща на guest виртуалните машини да ползват висококачествено видео през host видео адаптера

- необходимо е хост видео адаптера да поддържа DirectX 9.0c като мимимум

- изискване за поддръжка на host CPU Second Level Address Translation (SLAT)

Виртуализация на приложения (App-V) – технологиите за виртуализация на приложения се характеризират със следните функционалности:

- ✓ Приложенията не са инсталирани перманентно на виртуалните машини
- ✓ Приложенията се разпространяват от сървъра на клиента когато клиента пожелае да ползва дадено приложение
- ✓ App-V е част от Microsoft Desktop Optimization Pack
- ✓ Изолация на отделните приложения едно от друго
- ✓ Възможност за ползване на приложения в portable формат, които не изискват инсталация
- ✓ Приложенията може да следват потребителя от компютър на компютър
- ✓ User Experience Virtualization (UE-V) – възможност за виртуализиране на цялостната работна среда на потребителя
- ✓ Операционната система и приложенията следват потребителите между няколко компютъра

Презентационна виртуализация (Presentation Virtualization) – включва следните технологии:

- ✓ Remote Desktop Services – технология за отдалечен достъп до компютърни системи
- ✓ Поддръжка на приложения през RemoteApp функционалност
- ✓ Отдалечен достъп през RD Gateway (входна точка за отдалечен достъп)

Разлики между Desktop Virtualization и Presentation Virtualization:

- Desktop Virtualization:
- ✓ Всеки потребител има своя виртуална машина, върху която работи

- ✓ Потребителският работен плот и приложенията се намират на виртуалната машина на потребителя

- Presentation Virtualization:

- ✓ Всеки потребител се логва в отделна сесия на host сървъра
- ✓ Потребителският работен плот и приложенията се намират на host машината

Windows Azure е cloud-базирана платформа, осигуряваща среда за виртуални машини и приложения. Windows Azure осигурява Platform as a Service (PaaS) и Infrastructure as a Service (IaaS) услуги и поддържа различни типове програмни езици, инструменти и платформи.

Характеристики на Windows Azure:

- ✓ Възможност за автоматична промяна на капацитета на ползваните виртуални ресурси
- ✓ Предлагане на Web хостинг
- ✓ Предлагане на хостинг на готови продукционни среди
- ✓ Хостване на виртуални машини
- ✓ Хостване на бази данни

Повече информация относно Windows Azure може да намерите на следния адрес: http://en.wikipedia.org/wiki/Microsoft_Azure

Характеристики на Hyper-V:

- ✓ Hardware virtualization роля при Windows Server 2012
- ✓ Осигурява директен достъп на виртуалните машини до хардуерните ресурси на host машината чрез т.н. hypervisor layer

Методи за употреба на Hyper-V:

- ✓ Hyper-V роля в Windows Server 2012/2012 R2
- ✓ Microsoft Hyper-V Server 2012 Edition

Хардуерни изисквания при използване на Hyper-V:

- Характеристики на процесора:

- ✓ x64 platform with Hardware Assisted Virtualization and Data Execution Prevention (DEP)
- ✓ CPU capacity

- Памет – минимум 4 GB
- Производителност на дисковите масиви
- Капацитет на мрежовите интерфейси чрез използване на няколко мрежови адаптера

Хардуерни компоненти на виртуалните машини:

- **Симулирани основни хардуерни компоненти:**

✓ BIOS
✓ Memory
✓ Processor
✓ IDE Controller 0 and 1
✓ SCSI Controller
✓ Synthetic Network Adapter
✓ Serial Ports (COM1 and COM2)
✓ Diskette drive

- **Допълнителни хардуерни компоненти**:

✓ SCSI Controller (up to 4)
✓ Network Adapter
✓ Legacy Network Adapter
✓ Fibre Channel Adapter
✓ RemoteFX 3D video adapter

Характеристики на Виртуалните машини 2-ро поколение - виртуалните машини 2-ро поколение се различават от 1-во поколение по:

✓ Премахване на емулирани устройства
✓ UEFI firmware (вместо BIOS) с функции secure boot, boot from SCSI controller и PXE boot
✓ По-бърз процес на стартиране и инсталация на операционната система
✓ Съвместимост с Generation 1 виртуални машини
✓ Поддръжка на следните guest операционни системи:

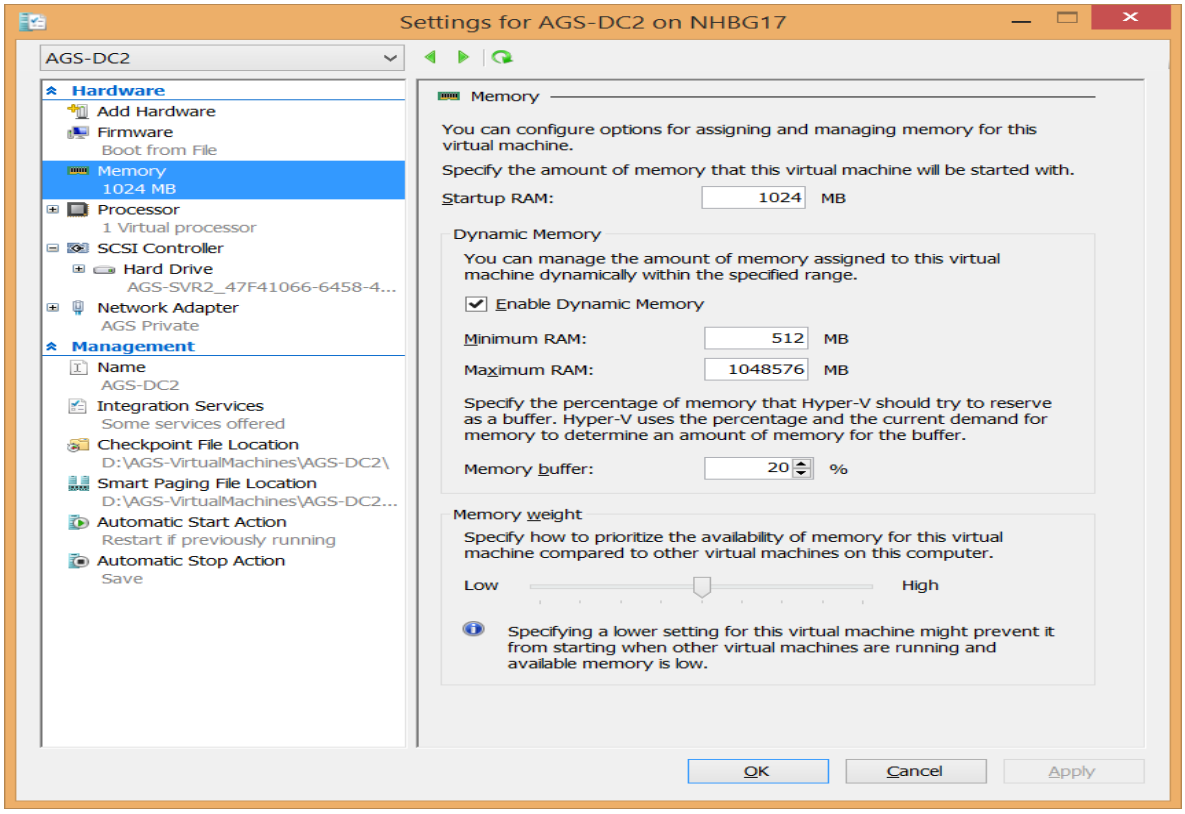
- Windows Server 2012/R2
- Windows 8/8.1 64 bit versions

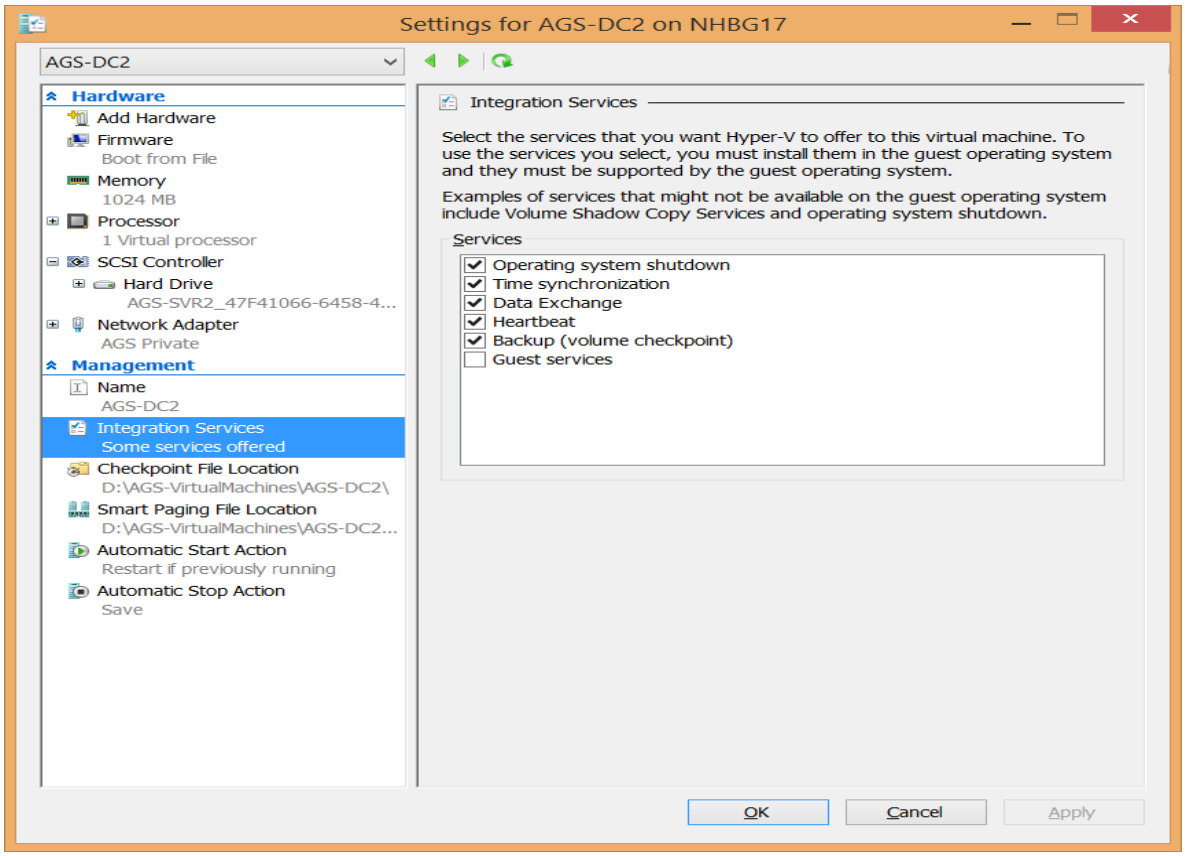
Динамична памет (Dynamic Memory) - Hyper-V средата за виртуализация в Windows Server 2012 дава възможност за конфигуриране и ползване на т.н. динамична памет (dynamic memory). При активиране на тази опция, Hyper-V автоматично ще управлява и разпределя оперативната памет на host машината между guest виртуалните машини според тяхното натоварване и според наличните ресурси на host машината.

Virtual Machines Integration Services е функционалност, която позволява интеграция на различни типове услуги между host и guest машините. Такива типове услуги могат да бъдат:

- Operating system shutdown – автоматично гасене или рестартиране на guest виртуалните машини при гасене или рестартиране на host машината.
- Time Synchronization – синхронизация на времето между host и guest машините.
- Data Exchange – обмяна на данни между host и guest машините.
- Heartbeat – сигнален интерфейс между host и guest машините.

Следните два екрана демонстрират възможностите за настройка на динамична памет и интегрирани услуги при Hyper-V:





Hyper-V Resource Metering е функционалност, която дава информация за ресурсите, ползвани от Hyper-V функционалността. Основните Hyper-V Resource Metering параметри са:

- ✓ Average CPU use
- ✓ Average physical memory use:

- Mimimum memory use

- Maximum memory use

- ✓ Maximum disk space allocation
- ✓ Incoming network traffic for a network adapter
- ✓ Outgoing network traffic for a network adapter

Hyper-V Resource Metering функционалността може да бъде ползвана само през Windows PowerShell.

Новости при Windows Server 2012 R2 Hyper-V:

- Споделен виртуален хард диск
- Автоматично активиране на виртуалните машини
- Подобрена сесийна комуникация по отношение на няколко виртуални машини

- Storage quality of service (качество на услугите относно употребата на дисковото пространство на host машината)
- Улеснен процес по създаване на виртуални машини

Подобрения при Windows Server 2012 R2 Hyper-V:

- Улеснена промяна на размера на виртуалните дискове
- Live migration (Миграция на работеща виртуална машина)
- Failover Clustering
- Integration Services (интегрирани услуги, позволяващи комуникация между host машината и guest виртуалните машини)
- Export of VM (експорт на виртуални машини)
- Replica of VM (реплика на виртуална машина, изнесена на друг хост)
- Вграден поддръжка на повечето Linux дистрибуции

Употреба на Hyper-V Checkpoints – checkpoint (snapshot) наричаме файл, който отразява състоянието на дадена виртуална машина в конкретен момент от време. Употребата на checkpoints функционалността ни позволява да върнем дадена виртуална машина към предишно стабилно състояние в даден момент от време. Създаването на checkpoints през Hyper-V Manager-а позволява на даден потребител да създава произволен брой снимки на моментното състояние на виртуалната машина, които след време да се ползват като алтернатива на архивни копия, към които машината лесно може да бъде върната. Основните характеристики на checkpoints са следните:

- Checkpoints не са решение, което замества архивирането на състоянието и информацията на дадена машина (backup solution).
- В предишните версии на Windows Server, checkpoints се наричат snapshots.
- Когато създаваме checkpoint, Hyper-V записва състоянието на виртуалната машина в differencing диска на машината.
- Когато върнем дадена виртуална машина от checkpoint, тя се връща в състоянието, в което е била в момента на създаване на checkpoint-та.
- Можем да експортираме виртуалните машини с техните checkpoints.

Управление на виртуални мрежи - Hyper-V емулира възможностите и поведението на реален мрежови превключвател (switch) чрез т.н. виртуален мрежови превключвател.

Типове виртуални превключватели:

- ✓ External – позволява комуникация между виртуалните машини, host машината и Интернет пространството.

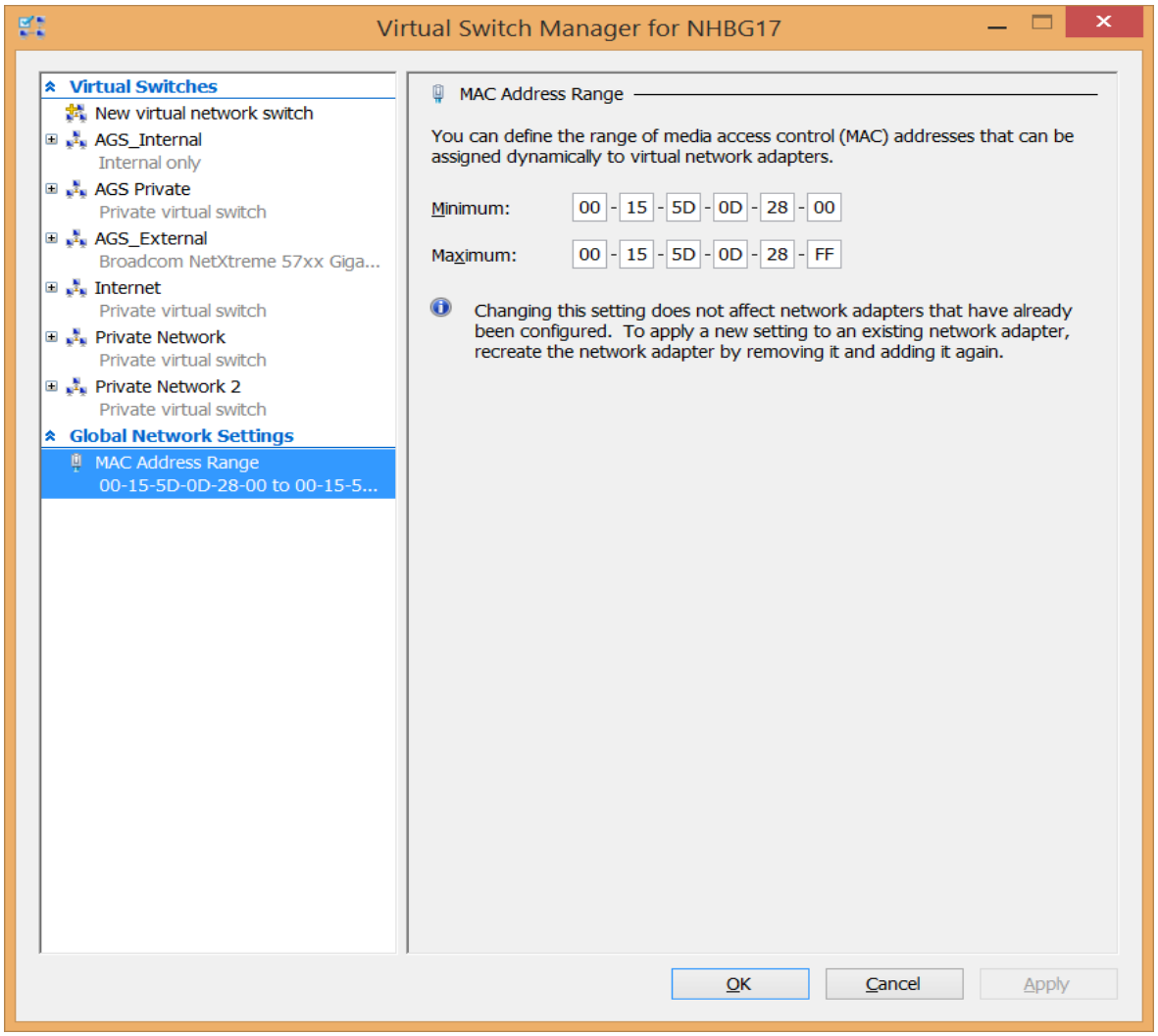
- ✓ Internal – позволява комуникация както между виртуалните машини, така и между тях и host машината.
- ✓ Private – позволява комуникация само между виртуалните машини.

Virtual Switch Extensions позволяват използването на third-party vendors виртуални превключватели, които са виртуални копия на техни реални хардуерни устройства.

Виртуални локални мрежи (Virtual Local Area Networks - VLANs) в среда на Hyper-V се характеризират със следните възможности:

- Логически разделят мрежовия трафик, които преминава през дадено физическо устройство, наречено превключвател (switch).
- VLANs се ползват за изолиране и защита на мрежовия трафик ползвайки 802.1q протокол.
- За да ползваме виртуални частни мрежи, виртуалният превключвател трябва да поддържа и да е конфигуриран за VLAN tagging.
- За да препращаме пакети между различни виртуални частни мрежи ни е необходимо устройство, работещо на трети слой от OSI модела (layer 3 switch или router).

Управление на MAC адресите на виртуалните машини: Hyper-V позволява да управляваме диапазона от MAC адреси, които ще ползват нашите виртуални машини. Тази функционалност и нейните настройки може да бъде управлявана през Virtual Switch Manager менюто на Hyper-V Manager конзолата в среда на Windows Server 2012.



Въведение в Cloud модела:

Предимства и недостатъци на Cloud модела: Cloud моделът е модел за изграждане на инфраструктури от типа „работа в облака“.

- Предимства на Cloud модела:

  ✓ Възможност за изграждане на виртуализирани центрове за данни (virtualized datacenters)

  ✓ Намаляване на оперативните разходи

  ✓ Уплътняване на ресурси (набор от виртуални машини върху един реален физически сървър)

✓ Устойчивост на откази, резервираност на системи и услуги, възможност за разширяване

- Недостатъци на Cloud модела:

✓ Липса на точна информация относно местонахождението на потребителските данни

✓ Липса на гаранция срещу неоторизиран достъп до лични данни

Типове и характеристики на облачните услуги:

- Публичен Cloud:

✓ Ползване на инфраструктура и услуги, които са изнесени в центъра за данни на Cloud доставчика

✓ Намалени оперативни разходи

✓ Намален контрол върху изнесената в Cloud инфраструктура

✓ Липса на гаранция за сигурност на данните при multi-tenant услуги

- Частен Cloud:

✓ Частният Cloud е собственост на дадена организация

✓ Инфраструктурата на частния Cloud се управлява и поддържа от административен и технически персонал на компанията

✓ Пълен контрол от страна на компанията-собственик върху инфраструктурата и услугите, предлагани от частния Cloud

- Хибриден Cloud:

✓ Комбинация от публичен и частен Cloud

✓ Възможност за едновременен контрол върху собствената инфраструктура и възползване от предимствата на публичната такава

Модели на Cloud услугите (Cloud service models):

- Software as a Service (SaaS):

✓ Доставя бизнес процеси и приложения

✓ Минимално конфигуриране и цена, базирана на ползваните услуги

- Platform as a Service (PaaS):

✓ Доставя готова платформа за имплементиране на приложения и услуги

✓ Възможност за улеснено разрастване на приложенията

- Infrastructure as a Service:

- ✓ Доставя готова хардуерна инфраструктура – сървъри, дисково пространство, мрежови решения
- ✓ Служи за база на SaaS и PaaS
- ✓ Цена на услугата, изцяло базирана на ползваните ресурси

Компоненти на System Center 2012 R2 и тяхната употреба в хибридния Cloud модел:

- ✓ App Controller – използва се за управление на услуги при хибридния cloud модел
- ✓ Service Manager – предлага управление на процеси с помощта на Self-Service Portal позволяващ на потребителите да си заявят услуги през уеб браузър
- ✓ Virtual Machine Manager (VMM) – осигурява платформа за управление на виртуални машини и услуги при private Cloud
- ✓ Orchestrator - осигурява методи за автоматизация на IT процесите
- ✓ Operations Manager – предлага мониторинг на производителността и достъпността на услугите
- ✓ Data Protection Manager (DPM) – осигурява защита и възстановяване на данните при Windows базирани сървъри
- ✓ Configuration Manager – използва се за разпространение на софтуер и за хардуерна и софтуерна инвентаризация при Windows базирани платформи.

Основни бизнес изисквания при внедряването на частен Cloud:

- Competitive advantage – постигане на напредък с внедряването на услуги от типа private Cloud
- Scalability – възможност за надграждане
- Reduced costs – редуциране и оптимизация на разходи за поддръжка на дадено технологично решение

Идентифициране на услугите и тяхната приложимост при частен Cloud:

- Идентифициране на услугите:
  - ✓ Местоположение на данните
  - ✓ Изисквания към компютърните ресурси
  - ✓ Изисквания по отношение на софтуера и операционните системи
  - ✓ Изисквания за пропускливост на мрежовата среда

- Приложимост на услугите:
  - ✓ Дали услугата отговаря на изискванията и е готова за имплементиране в частен Cloud
  - ✓ Изисквания за регулярен и доказано работещ backup
  - ✓ Дали процесът по миграция е успешно тестван в пред-продукционна среда
  - ✓ Съществува ли документиран и тестван метод за връщане на направените промени

Основни изисквания при преминаване към публичен Cloud:

- Security – сигурността е основно изискване към облачните услуги. Основните аспекти относно сигурността на данните в облака са следните:
  - ✓ Липса на информация относно физическото местоположение на данните.
  - ✓ Липса на сигурност относно това кой оперира с данните на клиента и гаранция срещу неоторизиран достъп до тях и кражба на ноу-хау.
- Service Level Agreements (SLA) – писмена форма на договорни отношения между две или повече страни, които засягат поддържане на конкретно ниво на дадена услуга.
- Cost – цената за преминаване и ползване на облачни услуги трябва да бъде сметната в дългосрочен план.
- Support – поддръжката на инфраструктурата при публичните облачни услуги се поема от доставчика на тези услуги и тази поддръжка е включена в таксата, която клиентите на облачни услуги плащат за ползване на предоставената им услуга.
- Technology – обновяването на технологиите, ползвани при облачните услуги, се осъществява от доставчика на тези услуги. Той се грижи всички инфраструктурни системи да бъдат регулярно обновявани и защитени.

Мониторинг на състоянието и производителността на частен Cloud: основните параметри за мониторинг на състоянието и производителността на услуги от типа „частен облак“ са:

- Състояние на операционната система
- Състояние на бази данни
- Достъп до Web сайтове и Web услуги
- Натоварване на хардуера
- Състояние на мрежата

- Състояние на конкретни приложения

Компоненти на System Center Operations Manager за мониторинг:

- Operations Manager Data Warehouse – позволява подробна хардуерна инвентаризация на конкретни машини
- Operations Manager Reporting features – възможност за генериране на подробни отчети на база предварителни заявки от страна на администратора

Основни индикатори за състоянието на Cloud услугите:

- Performance (производителност) – следенето на производителността на предлаганите облачни услуги е задължение на доставчика на тези услуги.
- Time (време) – своевременната реакция при отпадания на услуги или рискови събития трябва да бъде гарантирана от доставчика на облачни услуги.
- Quality (качество) – качеството на предлаганите услуги е основен параметър при реализиране на облачни решения.
- Cost (цена) – цената трябва да бъде правилно пресметната, като задължително условие е да бъде направена оценка на риска и тази оценка да бъде взета под внимание при вземането на решения относно миграция към облачни услуги.
- Risk (риск) – оценката на риска и неговия анализ са основен индикатор за даден тип облачна услуга.
- Profitability (възможност за генериране на печалба) – индикатор, показващ ефективността от облачните решения за определен период от време.

Изисквания при използването на System Center 2012 R2 за мониторинг на Cloud услугите:

- Интеграция между Operations Manager и Virtual Machine Manager
- Импортиране на Windows Azure Management Pack
- Импортиране на Operating System and Application Management Packs
- Импортиране на VMM Fabric Dashboard Management Pack

Списък с полезни препратки

1. **https://technet.microsoft.com/en-us/ Основен портал на Майкрософт, където детайлно е разгледана всяка тяхна технология. Включва много детайли относно инсталиране, конфигурация и поддръжка на всички Майкрософт продукти и технологични решения.**
2. **https://msdn.microsoft.com/bg-bg Дата порталът на Майкрософт, насочен към специалисти по програмиране и писане на скриптове.**
3. **http://azure.microsoft.com/en-gb/ Сайт с последните новости и детайли относно платформата за предоставяне на Cloud-базирани решения от Майкрософт.**
4. **https://en.wikipedia.org/wiki/Main_Page Уикипедия – световна онлайн библиотека.**
5. **http://www.iso.org/iso/home.html Сайт на Международната Организация по Стандартизация.**
6. **https://www.sans.org/ Портал за новостите в областта на информационната сигурност, закони, регулации и стандарти.**
7. **http://www.nist.gov/ National Institute of Standards and Technology – включва препоръчителни стандарти относно изграждането на всякакъв тип информационни системи.**
8. **https://learningnetwork.cisco.com/welcome Официална learning - платформа на Cisco с възможност за изучаване на огромно количество мрежови технологии.**
9. **http://www.tomshardware.com/ Сайт, посветен на хардуерните компоненти, които се ползват в съвременната компютърна техника.**