AD DS (Active Directory Directory Services)

AD CS (Active Directory Certificate Services)

DNS (Domain Name System)

DHCP (Dynamic Host Configuration Protocol)

IPAM (IP Address Management)

RAID (redundant array of independent disks)

File Server

IIS (Internet Information Service)

EFS (Encrypted File System)

NLB (Network Load Balancing)

Active Directory Backup & Restore

(WDS) Windows Deployment Service

(WSUS) Windows Server Update Services

چکیده تحلیلی مباحث

تدوین: بابک آشفته یزدی

اسفند ۱۴..

1

I
- Active Directory Directory Services
- Network Infrastructure
- Application

II
- Workgroup (Decenteralized Management)

III
- LSD,Local SAM,ICS
- Authenticate,SMB,CIFS,NBT

IV
- Authentication,Authorization,Accounting
- NTLM

2

I
- SMB,FTP
- Whoami,hostname,Netstat -n

II
- Domain Base (Centeralized Management)
- Network,DSD,GSD

III
- TGT,Kerberos

IV
- Active Directory Directory Services

3

I
- AD DS , LDAP , AD CS , AD RMS , AD FS

II
- DDP (Domain Data Partition)
- NC (Naming Context)
- Domain , OU , Forest

III
- Forest Root Domain
- Trust (Oneway , Twoway)
- Trust (Transitive , None Transitive)

4

I
- CIP (Configuration Information Partition)
- Computer Name (FQDN , NetBIOS)
- Sysdm.cpl

II
- Name Space Structure
- Tree , Graph , Child

II
- SPOF (In service , In Structure)
- CIA (Confidentiality,Integrit ,Availability)

5

I
- Performance(Load Balancing Quick Access)

II
- Service Application (Stateful , Stateless)
- DNS(Query,Netmask ordering,load balance)

III
- Automatic Replication
- Push & Pull Replication
- KCC (Knowledge Consistency Cheker)
- Repadmin /kcc,ipconfig /displaydns

6

I
- Physical Site (Quick Access)
- Well Connection

II
- Intera Site , Inter Site
- Default-First-Site-Name
- User Interface , Management Tools
- SP (Schema Partition)
- Schema Extend

7

I
- ADP (AD Integrated Application)

II
- Replication Scope Per Partition
- Global Catalog
- GC Server

8

I
- Permission (Allow,Don't Allow,Deny)
- Type of Partition
- DC Install

II
- Service.msc,dismgmt.msc,control,sconfig
- Msconfig,winver,ncpa.cpl,ntdsutil
- DSRAM Password
- Forest & Domain Functional Level
- DFL & FFL

9

I
- Log Files (Transaction Log,Event Log)
- Sysvol Folder ,Convert.exe
- Attended & Unattended Install Script
- Transaction Commit , Auto Recovery

II
- Dnsmgmt.msc,dsa.msc,domain.msc
- Dssite.msc,dsac,adsiedit.msc
- Repadmin /kcc-syncall-replsum,dcdiag /q
- Adreplstatus,SCOM

10

I
- Domain Admin Group,Enterperise Group
- Schema Admin Group

II
- Join to DC (Online,Offline)

III
- Computer Account,Standard User Account
- Domain Users Group

III
- Join to domain Delegation Control
- Trust Relationship Error

11

I
- Rejoin ,lusrmgr.msc
- Disable & Reset Computer Account
- Account Operator Group
- Join to Domain from Command

II
- Active Directory Administration-Manage
- Snap-In , RSAT (Remote Server Admin)
- Compmgmt.msc,sysdm.cpl,gpedit.msc
- Gpmc.msc,ldp,ntdsutil,esentutl

12

I
- Snap-In AD Schema (schmmgmt.dll)
- User Mode , Author Mode
- UPN (User Principal Name) Suffix
- Change Password, Log on to,Log on Hours
- Group Policy

II
- Local Group Policy Object (Local GPO)
- None Local GPO (GP Object)
- Local GPO scenario

13

I
- GP Object Priority (Site,Domain,OU)
- Password Policy
- Rsop.msc,gpresult /H name.html

II
- Link to GP Object
- GP Object Scenario
- GPO Refresh-Update Interval
- Gpupdate /force,Specopsgpupdate
- Group Policy Update Policy

14

I
- Overal Group Policy Management View
- Open Migration Table Editor
- Block Inheritance
- Linked Enabled
- Report from Policy
- Gmmc.msc Connect to Specefic DC

15

I
- Conflict in common policy
- GPO Priority
- Revolution in Contradiction in Policy
- Policy Enforce
- Preferences Policy

II
- Administrative Templates
- .Adm & .Admx
- Policy Filter Option,Sysvol Bloat

16

I
- Policy Definition
- Local Store & Central Store

II
- Scripts (Startup-Shutdown)
- Scripts (Log on-Logoff)

III
- Default Domain & Domain ControllerPolicy
- Dcgpofix

IV
- GPO Container & Template Location
- Password Policy & Lockout Policy

17

I
- Password Policy & Lockout Policy on DC
- PSO (Password Setting Object)

II
- ADSI Edit PSC Container
- Dsget user

18

I
- User Account ...
- Local User Profile
- Temperory Profile
- Roaming User Profile

II
- Mandatory User Profile
- Super Mandatory User Profile
- %userprofile%,%username%,%windir%
- %programfiles%,.,..

19

I
- User profile (logon Script)
- Map Drive , Home Folder
- ABE (Access-Based Enumeration)
- Group , Object ,ACL

II
- Local Groups
- Permission & Rights in Groups
- Built in & None Built in Groups

20

I
- AD Groups
- Type (Security & Destribution)
- Scope (Domain local,Global,Universal)

II
- Netsted Groups

21
- I
  - Restricted Group Policy
- II
  - Run as Administrator
- III
  - ALP (Accounts member Local+Permission)
  - AGLP
  - AGP
  - AGDLP
  - AGUP , AGUDLP

22
- I
  - How to identify group membership
- II
  - Group Naming
- III
  - Shadow Group
  - Group Scope And Member
  - Active Directory Directory Services

23
- I
  - Snapshot
- II
  - Log on Cache
- III
  - OU (Active Directory Permission)
  - Create Container

24
- I
  - Computer Account
  - Net computer , Net user
  - FSMO (Flexible Single Master Options)
- II
  - DC Based on NT (old)
  - DC Based on AD After win 2000
  - Master & Multi Master Role
  - Forest Wide & Domain Wide Role

25
- I
  - Schema Master Role
  - Domain Name Master Role
  - RID (Relative ID) Master Role
  - Infrastructure Master Role
  - PDC Emulator Master Role
  - PDC Emulator Duties

26
- I
  - Optimizing the Placement of Operations Masters
- II
  - Identifying Operations Masters
  - Netdom Query FSMO
  - Dsquery Server
- III
  - Transferring Operations Master Roles
  - Seize Master Roles

27
- I
  - Seize Commands
- II
  - Seize Scenario
  - Temporary and permanent Seize Roles

28
- I
  - Two DC Role Sample
- II
  - Reasons for Demote Domain Controller
  - Inplaced Upgrade DC
  - Migration DC
  - Force demote(Removal) AD from Server
- III
  - Metadata Cleanup

29
- I
  - IFM (Install From Media)
- II
  - TGT (Ticket Garanting Ticket)
  - TGS (Ticket Garanting Service)
  - Trust First & Second Category
- III
  - Tree Root Trust , Parent-Child Trust
  - Shortcut Trust , External Trust
  - Forest Trust , Realm Trust

30
- I
  - External Trust Sample
  - One way -NoneTransitive-Manual
  - Domain Wide Authentication

31
- I
  - External Trust Sample
  - Two way -NoneTransitive-Manual
  - Selective Authentication

32
- I
  - AD Site
  - FRS(File Replication Service)
  - DFSR(Distributed File System Replication)
- II
  - Site Link
  - Site Link Transport Type
  - Site Link Cost

33
- I
  - Universal Group Membership Caching
- II
  - RODC (Read Only Domain Controller)
- III
  - FBS (Prefered Bridged Server)
- IV
  - LAPS (Local Administrator Password Solution)
  - Enable local administrator & Rename that
  - admpw.admx Policy

34
- I
  - Install LAPS.x64.msi on Domain Controller
  - Schema Extend-ms-Mcs-AdmPwd
  - Schema Extend-ms-Mcs-AdmPwdExpire
  - Set-AdmPwd ComputerSelf Permission
  - Set & Remove All-Extended Rights

35
- I
  - Publish LAPS.x64.msi Via GPO
  - Three way view LAPS
  - Reset LAPS
- II
  - MSA (Manage Service Account)

36
- I
  - Top 10 Most Important Group Policy for Preventing Security Breaches
  - Moderating Access to Control Panel
  - Control Access to Command Prompt
  - Important about Windows Update
  - Disallow Removable Medias USB,....
  - Prevent Windows LAN Manager Hash

37
- I
  - Top 10 Most Important Group Policy for Preventing Security Breaches
  - Restrict Software Installations
  - Disable Guest Account
  - Set Password And Lockout Policy Limits
  - Disable Anonymous SID Enumeration

38
- I
  - Policy CSE(Client Side Extention)
  - Pre GPO Filtering
- II
  - Enforced Policy
  - Block Inheritance
  - LoopBack Processing

39
- I
  - Pre GPO Slow Link Detection Policy
- II
  - GPO Filtering
  - Security Filtering (AD Permission)
- III
  - WMI Filtering (Dynamic Filtering)
  - Wmic Command
  - WMI Query Language (WQL)

40
- I
  - WMI Explorer
  - Item level Targeting & WMI GPO
- II
  - Folder Redirection Policy
  - Software Installation
- III
  - Computer Configuration Assign & Advance
  - User Configuration Assign & Publish
  - ZAP File Structure

41

I
- Software Restriction Policy

II
- AppLocker Policy
- GPO Planning

III
- Role Design
- Team Design

42

I
- RSoP(Resultant Set of Policy)
- RSoP Logging
- RSoP Planning
- Certificate

II
- CIA Triad , Confidentiality , Integrity
- CIA Triad , Encryption
- Two Way Encryption (Symetric,Asymetric)
- One Way Encryption

43

I
- Symetric & Asymetric Encryption
- Shared Key , Private Key ,Public Key
- Confidentiality + Authenticity

II
- PKI (Public Key Infrastructure)
- Asymetric + Symetric Algorithm
- Type of Symetric,Asymetric,Hash

44

I
- Hashing & Digest
- Confidentiality,No Integrity,No Authenticity
- No Confidentiality,No Integrity,Authenticity
- Confidentiality,Integrity,Authenticity
- Digital Signature (DS)

45

I
- Certification Authority (CA)
- Self Sign,Public CA,External CA,Private CA

II
- Request CA .pfx and .cert
- CA Authentication

III
- Certificate Trusted List (CTL)
- Certificate Revoke List (CRL)
- CRL Distribution Point (CDP)
- CRL Base , CRL Delta,Online Responder

46

I
- WildCard Certification
- Subject Alternate Name (SAN) Certificate

II
- DV SSL Domain Validated
- OV SSL Domain Validated
- EV SSL Domain Validated
- Certlm.msc , Certmgr.msc

47

I
- Certificate Chain
- Root CA , Intermediate CA , End Entity CA

II
- Enterprise CA
- Standalone CA
- Installing AD CS Server Role

48

I
- Create Certificate template (WS,Client)
- Group Policy for Automatic Enrollment
- CDP & AIA
- Certificate Hold , Certificate Publisher
- Request New Certificate No.1 & 2

49

I
- Request New Certificate No.3
- .cer & .pfx
- Name Resolution (DNS , Wins)

II
- NetBIOS , FQDN
- Ipconfig /displaydns , ipconfig /flushdns
- Hosts file
- Node Type (LMHOST – Wins – Broadcast)

50

I
- Dnsmgmt.msc , Dnscmd ,Getcommand
- Static & Dynamic DNS

II
- Forward Lookup Zone
- Newhost (A,AAAA)
- CNAME
- MX RECORD

51

I
- NSlookup
- Forward Lookup Zone

II
- New Delegation , Other New Record
- DNSSEC , General Status
- Type (Primary , Secondary)
- SOA , Name Server
- Zone Transfer (AXFR ,IXFR)

52

I
- DDNS In Network Without AD
- Hard Registration & Soft Registration

II
- Stale & Scavenging
- Update Record & Refresh Record

III
- SOA Tab (Serial ,Primary Server ,TTL)
- NS Record , MX Record , Glue Record

53

I
- WINS & WINS Lookup
- Forwarders

II
- LMHOST , WINS , Broadcast
- Cache Lookup
- Private Zone Secondary
- Conditional & Unconditional Forwarders

54

I
- Stub Zone
- Name Resolution Hierarchical
- Root Hint , Root Zone , Dot Zone
- Top Level DNS , Second Level DNS , Hosts
- Inverse Quary
- Recursive Quary
- Iterative Quary

55

I
- No RootHints & Forwarders
- Forwarders Without RootHints

II
- DNS Properties Advance
- Cache Poisioning

III
- Reverse Lookup Zone , PTR

IV
- GlobalName Zone
- SRV Record

56

I
- Auto Discovery (SRV Record)

II
- DNS + AD Integrated Zone
- Delegation Error
- Internal & External NameSpace

57

I
- ADP DNS Partition
- _Msdcs Zone
- Domain Scope Zone
- Forest Scope Zone

58

I
- SRV Record & Service Locator
- SCP AD Service
- Ipconfig /registerdns & Netlogon Service
- Secure only & Nosecure DDNS registaration
- Replication Sync Zones
- Security Tab
- Add a ADP Partition

59

I
- Configure DNS in Clients

II
- DHCP Server Broadcast Domain
- DHCP Discover
- DHCP Offer
- DHCP Request
- DHCP Ack + Options

60

I
- Destination Broadcast MAC
- Listen Ports 67,68 UDP
- Transaction ID
- Automatic Private IP Address (APIPA)
- Configure DHCP SRV
- Rogue DHCP SRV , Active & Authorize DHCP
- BootP SRV

61

I
- Display Statistics & Reservation

II
- Server,Scope,Reservation Options

III
- User Class ,DHCP Class ID
- DHCP Policies

IV
- Vendor Class & Predefined Options
- Disable NBT via DHCP

62

I
- DHCP Backup , mdb File
- Compact Database with jetpack
- Integrity DNS Server + DHCP Server

II
- DHCP Relay Agent
- Name Protection

63

I
- Name Protection & Credential user
- Reconcile

II
- DHCP HA (FailOver Clustering)
- DHCP HA (DHCP FailOver))

64

I
- Unicast Scope , Multicast Scope
- Super Scope , Multimode , Multinet

II
- Confilict Detection attempt
- Export , Import And Migrate a DHCP SRV
- DHCP Starvation

65

I
- IPAM (IP Address Management)

II
- RAID (redundant array of independent disks)
- JBOD(just a bunch of disks)
- Spand Volumes
- RAID Controller
- RAID 0

66

I
- RAID 1 , RAID 5

II
- Parity
- Hot Spare , Cool Spare

67

I
- RAID 6 , RAID 1+0

II
- RAID 1+0 , RAID 0+1

68

I
- DAS Storage
- File Level Access , Block Level Access
- NAS Storage
- SAN Storage

II
- Fiber Channel Adapter (FCA)
- Host Bus Adapter (HBA)
- LUN , WWN , WWID

69

I
- LUN Access

II
- Server Cluster
- Rule or Policies on Server Cluster
- Shared Folder & Shared Storage
- FT , load Balance , Performance , HeartBeat
- ISCSI , FC ,FCOE , ISCSI Initiator & Target

70

I
- SAN Storage (Owner & Passive)
- Active Node & Passive Node
- File SRV Implementation

II
- Enable access-based enumeration(ABE)
- Distributed File System (DFS) Replication
- Dynamic Access Control (DAC)
- AD RMS (Right Management Services)

71

I
- Administrative Share
- Fmgmt.msc
- Registry , Local Account Token Filter Policy
- Administrative Share From GPO

II
- Sharing Method
- Public Folder Share for All Users

72

I
- Organization Folder Share for OU

II
- Private folder for Users

73

I
- Enable ABE
- Disk Quota , Folder Quota
- Soft Quota , Hard Quota

II
- File or Folder Auditing
- Event Veiwer , Logs
- GPO (audit object access , object access)

74

I
- Limit User For Copy Specific File Type
- FSRM (File server resource manager)
- Soft Screen , Hard Screen

II
- Folder Quota

III
- Shadow Copy

75

I
- Dynamic Access Control(DAC)
- DLP (Data Leakage Prevention)
- (DRM) Digital Right Management
- AD RMS & Physically Right Management

II
- Distributed File System (DFS)
- DFS NameSpace & Replication
- FRS(File Replication Service)

76

I
- Definition NameSpace
- Standalone NameSpace
- Domain NameSpace
- Dfsmgmt.msc

77

I
- DFS Problems

II
- FTP SRV , Web SRV

III
- Default Document , Directory Browsing
- Static Content , Http Redirection
- WebDAV

IV
- Security Features ,Basic ,Digest ,IP Restrict
- Inetmgr.msc , iisreset

78

I
- wwwroot Folder & web.cfg
- OwnerShip GPO
- IUSR , Module , Handler Mapping

II
- Virtual Directory
- Http Redirect
- IP address and Domain Restriction

III
- differentiate between websites of a web SRV
- IP Base , Port Base

79

I
- HostName Base

II
- Application Pool

III
- IIS Backup
- Remote Management IIS

80

I
- FTP Service
- EFS (Encrypted File System)

II
- EFS NTFS Permission + Compress
- Symetric & Asymetric Compress
- EFS Certificate

81

I
- Recovery Agent
- GPO for Recover Agent

II
- Simultaneous use of multiple encrypted files

III
- (NLB) Network Load Balancing
- NLB & FailOver Cluster
- VIP , CAP , Stateless , Stateful

82

I
- Nlbmgr.msc
- Nlb , Wlbs
- Priority(unique host identifier)
- Unicast , Multicast , IGMP Multicast

II
- Rule in Server Cluster (IP,Port,Protocol)
- Single & Multiple Host + Afinity

83

I
- Load Weight

II
- Active Directory Backup
- Application Aware Backup
- Windows Server Backup , Wbadmin.msc
- VSS Backup
- Full ,Differential ,Increment & Daily Backup

84

I
- Restore Active Directory Backup
- Using DSRM
- Authorative Restore
- USN Database

85

I
- Increase USN For Objects

II
- (WDS) Windows Deployment Service
- Install Image
- Boot Image
- Win PE (Preinstallation Environment)
- Live Recovery

86

I
- Dism Command
- WDS & DHCP SRV in one Broadcast Domain
- WDS & DHCP SRV in Differ Broadcast Domain
- WDS & DHCP SRV on Same Server
- Wdmgm.msc

87

I
- Windows Server Update Services (WSUS)

II
- WSUS Planning
- Simple Deployment With Computer Groups
- Hierarchical WSUS
- Network Load Balancing
- Centralize Management
- Distributed Management

88

I
- Disconected WSUS SRV

II
- WSUS installation
- Wsus.msc
- WSUS Console Options

III
- Update Source and Proxy Servers
- Product & Classification
- Update File and Languages

89

I
- Synchronization Schedule
- Automatic Approvals
- Configure Automatic Updates

II
- Specify Interanet Service Location
- Enable Client Side Targeting
- Computers Option

90

I
- WSUS Import/Export
- Wsusutil.exe
- BITS (Backgroung Intelligent Transfer Service)

I

MCSA

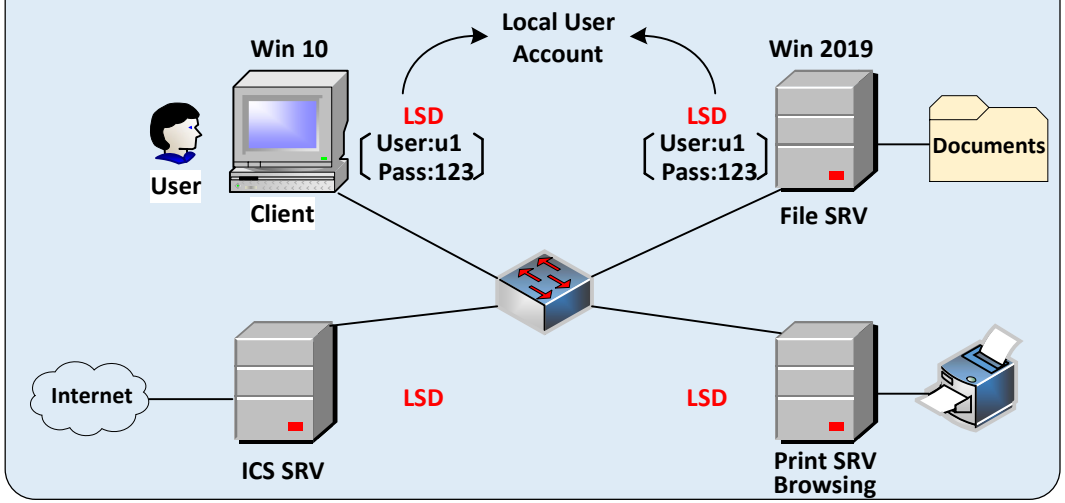
1. Active Directory Directory Services → Centralized management
   Network:
   1. Workgroup → Decenteralized management — مدیریت غیر متمرکز شبکه
   2. Active Directory → Centeralized management — ابزار مدیریت متمرکز شبکه
2. Network Infrastructure → A set of tools used to set up a network. (DNS server,DHCP server,IPAM,IPSEC,Windows Firewall,...) — مجموعه ابزارهایی که با استفاده از آنها شبکه راه اندازی شده است – زیر ساخت تبادل اطلاعات
3. Application → A set of tools for which the network is set up. (File SRV,Print SRV,WSUS,WDS,SCCM,...) — مجموعه ابزارهایی که به خاطر آنها شبکه راه اندازی شده است

SCCM:Microsoft System Center Configuration Manager
WSUS:Microsoft Windows Server Update Services
WDS:Microsoft Deployment Services

II

Network

1 Workgroup → Decenteralized management (Peer to Peer)



III

LSD : Local Security Database
Local SAM : Local Security Account Manager
LSD = Local SAM
ICS : Internet Connection Sharing

– از اتصال فیزیکی و لاجیکی بین ۲ تا n کامپیوتر شبکه بوجود می آید
– بر روی تمام ویندوز ها بصورت پیش فرض دیتا بیسی به نام LSD وجود دارد

– اگر کاربر نام کاربری و رمز عبور یکسان در کامپیوتر خود و دستگاه سروری که میخواهد از منابع آن استفاده کند داشته باشد فرایند احراز هویت در پس زمینه و بصورت نامحسوس انجام خواهد شد ، در غیر اینصورت کاربر نیاز به درج نام کاربری و رمز عبور معتبر جهت احراز هویت در سمت سرور خواهد داشت

Authenticate : فرایند احراز هویت " شناسایی " کاربر

Name Resolusion DNS SRV
- Name → IP
- IP → Name

– در این نوع شبکه برای استفاده از منابع سرورها باید بر روی کلیه سرورهای مرتبط User Account داشته باشیم

SMB : Server Message Block
CIFS : Common Internet File System

– جهت Hardening ، SMB V1 و NetBIOS در شبکه Disable میگردد

NBT : Net BT : NetBIOS over TCP/IP

– در شبکه Workgroup از متد NTLM استفاده میشود

IV


User

From Run or Browser Via SMB Protocol → Run → \\computer name \\IP address → From → Source Random port above 49000 Destination port 139,445 → Access → Shared Resources


SRV

Authenticated Methods (Protocol)
1 Workgroup → Windows New Technology LAN Manager AAA Protocol (NTLM) → Microsoft Base

(AAA)
- Authentication — provides a way of identifying a user — شناسایی کاربر
- Authorization — process determines whether the user has the authority to issue — مجوز سطح دسترسی کاربر
- Accounting — measures the resources a user consumes during access — حسابرسی کاربر

(AA) – شناسایی و مجوز سطح دسترسی لازم و ملزوم یکدیگرند و همیشه همراه با هم هستند

I

1 **SMB** — Server Message Block — **Ports : 139,445**

- فایل سرور و فولدر به اشتراک گذاشته شده و نهایتا راه اندازی سرویس فایل برای کاربران
- بیشتر جهت سرویس دادن به کاربران خاص در شبکه های سازمانی استفاده میشود
- احراز هویت کاربر از تمهیدات این سرویس میباشد، هرچند امکان عدم احراز هویت نیز میسر می باشد

2 **FTP** — File Transfer Protocol — **Ports : 20,21**

- راه اندازی سرور FTP و پیرو آن یک FTP Site و نهایتا راه اندازی سرویس فایل
- بیشتر جهت سرویس دادن به عموم بدون احراز هویت استفاده میشود

- اگر Log On به سرور بدون احراز هویت انجام شود به آن اتصال **Anonymous** گفته میشود

Whoami Run → Print host and user name

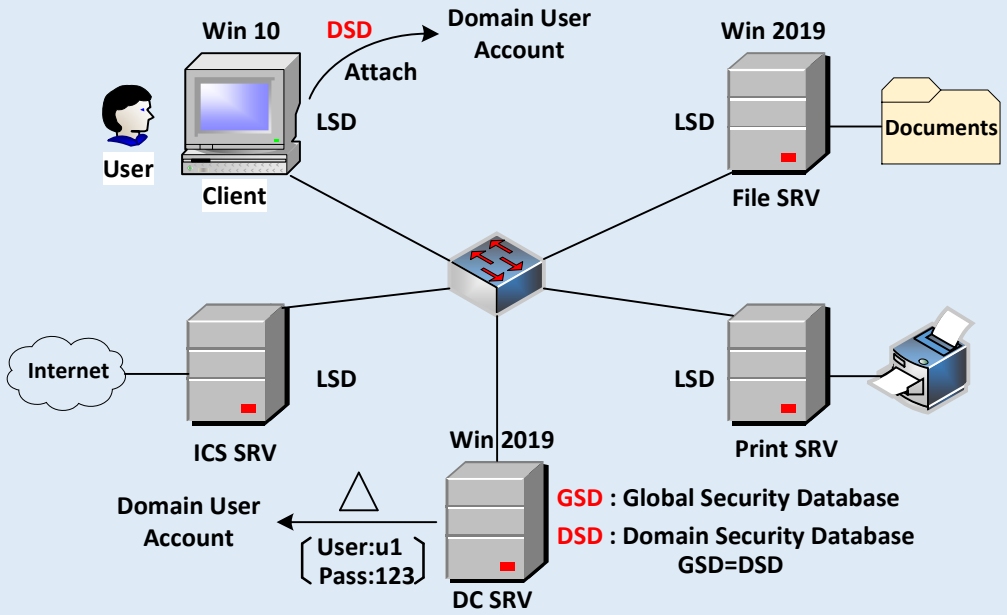
Whoami /user Run → Whoami + SID

Hostname Run → Print host name

Netstat -n Run → Print ip & port on stablished connection

II

2 **Domain Based** → **Centeralized management (Client / Server)**



- **Domain Model** شامل یک محدوده **Logical** از کاربران و کامپیوتر ها می باشد که بصورت **Logical** و **Physical** ذیل Policy های مشترک با هم در ارتباطند

III

- دامین کنترلر بعنوان یک سفت افزار فیزیکی و دامین بعنوان یک ماهیت مجازی لازم و ملزوم یکدیگر هستند
- نماد دامین کنترلر مثلث متوازی الاضلاع می باشد
- کلیه **User Account** های کاربران بصورت متمرکز در دامین کنترلر ساخته میشود
- جهت استفاده کامپیوتر ها از دامین باید سیستمها به دامین کنترلر Join شوند
- یکی از ارکان شبکه مبتنی بر دامین **DNS** می باشد و غالبا بر روی سرور **DC** قرار دارد

User

Name Resulation → کلاینت بر اساس نام دامین خود از DNS آدرس IP دامین کنترلر را استعلام میکند

Service Locator → سرور DNS آدرس IP دامین کنترلر را به کلاینت برمی گرداند

Kerberos

دامین کنترلر کاربر را احراز هویت می نماید و برای کاربر تیکت صادر می کند **TGT**

دسترسی به Domain "قلمرو" به مدت ۱۰ ساعت میسر می گردد

Port : 88

Authenticated Methods (Protocol)

Ticket-Granting Ticket (TGT)

2 **Domain Base** → **(AAA) Protocol Kerberos** → **Public Base**

- در شبکه **Domain Base** از هر دو پرتکل **NTLM , Kerberos** استفاده میشود

- فایل Services حاوی جدول پرتکل به همراه شماره پورت آن می باشد

C:\Windows\System32\drivers\etc\services

Run → **drivers** محل پوشه درایور

IV

Active Directory Directory Services → **AD DS** → **Software** → **Server Side Application** → **DC** → **Domain** → **Centralized management**

Directory

- مرز بین شبکه غیر متمرکز Workgroup و شبکه متمرکز Domain Base وجود یا عدم وجود Directory می باشد

1 **Directory=DSD**

2 **Directory is a hierarchical database for network objects**

Active Directory

- **AD** اسم محصول Directory Services مایکروسافت می باشد
- **AD** حالت پویا دارد و بدون دخالت ادمین نیز امکان تغییر اتوماتیک دارد

Directory Services

- مجوعه ای از سرویسها Services که منجر به ساخت Directory می شوند و امکان بهره برداری ازآن را میسر می کنند

3 ← Active Directory Directory Services → 2

Active Directory Directory Services

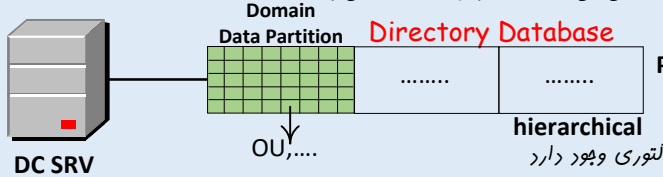
I

1. **Active Directory Domain Services (AD DS)**
2. **Active Directory Lightweight Directory Services (AD LDS) - LDAP**
   - is a Lightweight Directory Access Protocol (LDAP) directory service that provides data storage and retrieval support for directory-enabled applications, without the dependencies that are required for the Active Directory Domain Services (AD DS).
3. **Active Directory Certificate Services (AD CS)**
   - is a Microsoft product that performs public key infrastructure (PKI) functionality, supports personalities, and provides other security functionality
4. **Active Directory Rights Management Services (AD RMS)**
   - can be used to augment the security strategy for your organization by protecting documents using information rights management (IRM)
5. **Active Directory Federation Services (AD FS)**
   - provide users with single sign-on access to systems and applications located across organizational boundaries.

II

Domain Data Partition

- با راه اندازی **AD** امکان بهره برداری از نرم افزارهای مرتبط با این سرویس میسر میگردد مانند**Exchange Server**
- از سال ۲۰۰۸ به بعد Active Directory Directory Services بصورت یک پکیج ۵ محصوله عرضه می شود
- در راستای محقق نمودن هدف شبکه متمرکز **AD DS** شامل **Objects** و**Structures** می گردد
- اشیاء **Objects** بصورت دائم و مستمر *در حال تغییر* توسط ادمین می باشد ← (User Account),...
- ساختار**Structures** یکبار طراحی می گردد و غالبا *بدون تغییر* می باشد



- *چهار نوع* پارتیشن در دایرکتوری وجود دارد
- محل فایل دیتابیس دایرکتوری ← **C:\windows\system32\ntds.dit**

Ntds.dit = nt directory service . Directory file

III

AD Structures

1 Logical

1 Domain

- Domain Model – شامل یک محدوده Logical از کاربران و کامپیوتر ها می باشد که بصورت Logical و Physical ذیل **Policy** *های مشترک* با هم در ارتباطند که همین خط مشی های مشترک زمینه مدیریت متمرکز را فراهم می نماید
- عبارت DC داخل JPC.ir است صحیح نیست و DC برای JPC.ir میباشد صحیح است

2 OU (Organizational Unit)

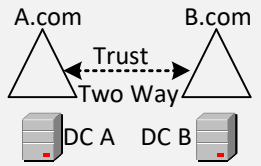
- جهت *ساماندهی و ایجاد نظم* در ذخیره سازی اطلاعات بر روی Domain Data Partition از**OU** استفاده می شود
- OU – به Folder در پارتیشن های هارد دیسک تشبیه می شود و Object ها در درون**OU**ها ساماندهی می گردد
- از**OU**بصورت تو در تو **(Nested)** میتوان استفاده نمود و به صورت سلسله مراتبی راهبری**OU**ها را به افراد مختلف **Delegate** نمود
- اینکه بر روی کامپیوترها چه نرم افزاری نصب باشد به Policy مرتبط است و میتوان از طریق Policy های هر OU بین آنها تمایز قائل شد
- بطور کلی برای طراحی OU از لوکیشن فیزیکی و Policy های مشترک استفاده نمیشود مثلا ۱۰ کاربر کنترل پنل نداشته باشند
- بطور کلی *ساختار سلسله مراتبی چارت سازمانی* شرکت ها به **OU** ها تخصیص داده می شود
- در بعضی از مستندات AD ازاعمال Policy به**OU**برای مخفی کردن Object هااشاره شده است
- یکی از کاربردهای**OU**اعمال Policy به آن جهت مدیریت بهینه متمرکز می باشد
- **OU** یک **Container** است که امکان اعمال Policy بر روی آن وجود دارد
- اگر یک User Account از یک OU به OU دیگر Move داده شود Policy های آن به همراه Manager آن عوض می شود

3 Forest (Trust)

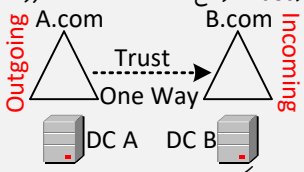
- **Trust** یک *ارتباط* **(Relation)** بین دو دامین است که باعث میشود تیکت صادر شده در یک دامین در دامین دیگر نیز اعتبار داشته باشد و بدینوسیله وسعت اعتبار تیکت بیشتر شود

انواع Trust

1 One way or Two way

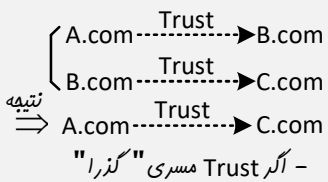


هر دو دامین به هم Trustدارند



تیکت صادر شده در A.com در B.com اعتبار ندارد ولی عکس آن درست است

2 Transitive or Non transitive



– اگر Trust مسری "گذرا" باشد رابطه بالا مورد قبول است درغیر اینصورت غیر

Domain Data Partition

– جهت ذخیره دیتای دامین استفاده میشود " هر آنچه به دامین مربوط است " و تعداد آن برابر باتعداد دامین های موجود در شبکه است

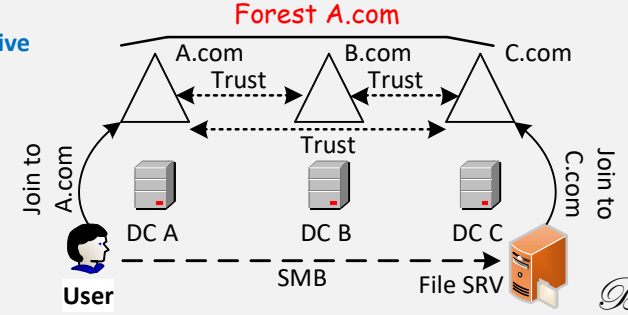
User Accout,Computer Account,Groups ,Policies.....

3 Automatic or Manual

- بین دامین های یک Forest بصورت اتوماتیک Trust دو طرفه وجود دارد ولی بین دامین های Forest های مختلف میتوان بصورت دستی Trust ایجاد کرد
- نام Forest همیشه برابر با نام اولین دامین **Forest Root Domain** می باشد
- Forest – در برگیرنده یک یا چند دامین می باشد که بین آنها یک " رابطه" Trust *دوطرفه* **Transitive** اتوماتیک وجود دارد

Forest ⟶ **Exist Automatic Two way Transitive between Domains**

- Forest – بزرگترین Structure اکتیودایرکتوری می باشد Forest معادل AD می باشد
- .... OU ⟶ .... ⟶ OU ⟶ Domain ⟶ Forest
- مرز Logical شبکهForest می باشد – نام شبکه دامین مدل مایکروسافتForest می باشد
- مفهومDirectory به Forest تعلق دارد

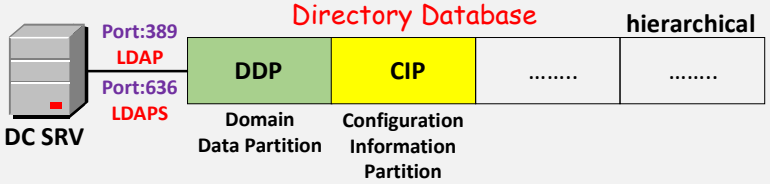


I Forest (CIP)

Configuration Information Partition

– جهت ذخیره ساختار **Forest** استفاده میشود " هر آنچه به Forest مربوط است "
و تعداد آن یک عدد در دایرکتوری می باشد

How many Domain ,Domain name , How many tree with root and parent and child name.....



Computer Name — On Windows:
1. **FQDN** (**DNS Name** / **Full Computer Name**) → Hostname.Suffixname (Flat نیست)
2. **NetBIOS** (**NetBIOS Name**)

Www.yahoo.com / Mail.yahoo.com → (www,mail) → اسم هاست داخل شبکه → (yahoo.com) → اسم شبکه

– **Flat** است و بخش بندی نمیشود، حداکثر ۱۵ کارکتر است و معمولا با حروف بزرگ نمایش داده میشود

– قاعدتا Hostname برابر NetBIOS Name است ، هرچند این امکان وجود دارد که متفاوت نام گزاری گردد که توصیه نمی شود

NetBIOS Name ← Hostname.Suffixname

– دسترسی سریع از طریق Run به System Properties ← **Sysdm.cpl** Run → System Properties

II AD Structures

1 Logical

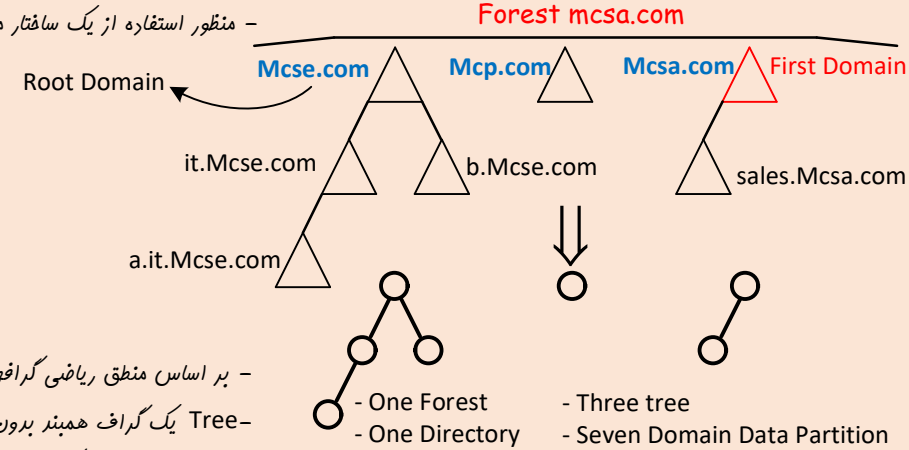
NameSpace Structure
ساختار نام گزاری

U1.test.com
U2.test.com
⋮

– منظور استفاده از یک ساختار منظم نام گزاری منطبق بر FQDN می باشد

4 Tree

Forest:mcsa.com →
- Mcse.com
  - it.Mcse.com
    - a.it.Mcse.com
  - b.Mcse.com
- Mcp.com
- Mcsa.com
  - sales.Mcsa.com



– اگر کسی ادمین Parent باشد ادمین Child آن نیست
– Policy های Parent ، Policy های Child آن نیست
– ارتباط Parent با Child ارتباط اسمی است پس اسم به ارث می برد و نه Policy

– بر اساس منطق ریاضی گرافها به این حالت Tree می گوییم
– Tree یک گراف همبند بدون لوپ می باشد
– در ترسیم Tree اگر بین دامین ها ارتباط اسمی وجود داشته باشد از خط اتصال بین دامین ها استفاده می کنیم

– از **Tree** جهت پیاده سازی **Name Space** استفاده میشود
– در واقع این **Tree** است که به ما اجازه ساخت یک **Child** در درون یک دامین را میدهد

- One Forest
- One Directory
- Three Root Domain
- Three tree
- Seven Domain Data Partition

.... OU → ....→ OU → Domain → Tree → Forest

III SPOF

2 Physical

SPOF

A single point of failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working

یک نقطه شکست واحد SPOF بخشی از یک سیستم است که در صورت خرابی، کل سیستم را از کار کردن باز می‌دارد

– مایکروسافت در روز دوم کاری هفته دوم هرماه آپدیت ارائه می نماید
– **SPOF** در هر حوزه ای امکان وقوع دارد و فقط از طریق تمهیدافزونگی **(Redundancy)** امکان برطرف نمودن مشکل میسر است

– با توجه به هزینه بسیار بالای برخی از افزونگی ها ارزش و عدد در دسترس پذیری **Availibility** سنجیده می شود

– در هر ۱۰۰ روز مجموعا ۲۴ ساعت معادل یکروز خارج از دسترس قابل قبول است → 99
– در هر ۱۰۰ روز مجموعا یک دهم روزخارج از دسترس قابل قبول است → 99.9
– در هر ۱۰۰ روز مجموعا یک هزارم روزخارج از دسترس قابل قبول است در این حالت حتما باید افزونگی را در نظر گرفت → 99.999

SPOF

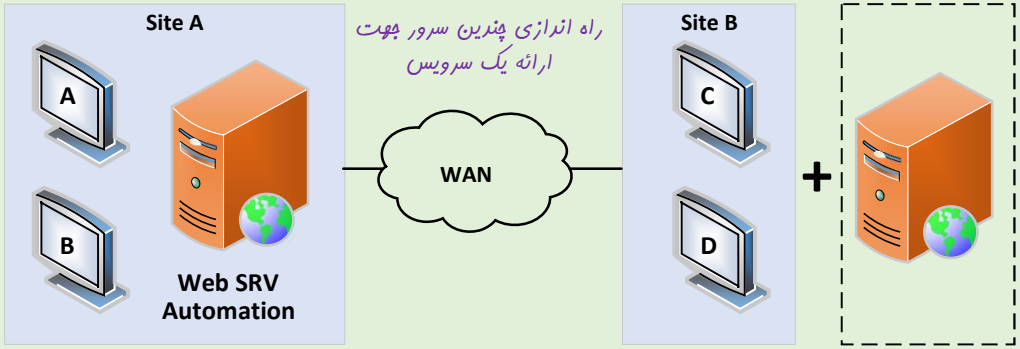
1. **SPOF In Service** در سرویس نرم افزاری
2. **SPOF In infrastructure** در زیرساخت تبادل اطلاعات

– راه اندازی چندین سرور جهت ارائه یک سرویس

1. – برطرف نمودن SPOF
2. – فراهم نمودن Fault Tolerance (FT)
3. – فراهم نمودن Availability (HA)
4. – افزایش Performance
5. – فراهم نمودن Load Balancing

مثلث امنیت

I Quick Access Performance



- در شکل روبه رو بعلت ضعیف بودن لینک ارتباطی بین دو سایت دسترسی کاربران سایت B برای استفاده از سرویس اتوماسیون در سایت A با مشکل کندی سرعت مواجه هستند که در اینحالت مجبور به اضافه نمودن یک سرور کمکی در سایت B هستیم تا در زمانهای مختلف این دو سرور با هم Replicate کنند و Sync گردند
- این حالت منجر به **Quick Access** می گردد که به نوعی افزایش **Performance** می باشد
  - **1 Performance** افزایش
    - **1** فراهم نمودن **Load Balancing**
    - **2** دسترسی سریع **Quick Access**
- همواره روش سرویس در یک سرور به Configuation و محتوی سرویس به Database مربوط میشود که در راه اندازی چندین سرور همزمان ، باید همه سرویس ها از این حیث شرایط یکسانی داشته باشند

II Stateful VS Stateless

1 Stateless

- سرویسی است که دیتا بیس ندارد
- در صورت وجود دیتابیس از درجه اهمیت بسیار پایینی نسبت به سرویس قراردارد
- دیتا بیس آن Read Only است
- تغییرات در دیتا بیس آن توسط افراد مشخص " ادمین " در ساعات مشخصی انجام میشود

Web SRV(IIS)
DNS SRV

- اگر سرویسی Stateless باشد میتوان Syncشدن سرورهای آن سرویس را بصورت Manualتوقع داشته باشیم

2 Stateful

Service Application Server side

- سرویسی است که مطمئنا دیتا بیس دارد
- دیتا بیس آن توسط کاربر در حال تغییر می باشد
- تغییرات دیتابیس بدون اطلاع ادمین انجام می شود

File SRV
Mail SRV
SQL SRV
AD SRV

- اگر سرویسی Stateful باشد میتوان Syncشدن سرورهای آن سرویس را بصورت Automatic توقع داشته باشیم
- اگر چندین سرور سرویس Stateful داشته باشند و بصورت Automatic هم نشود آنها را Sync نمود باید به نوعی صورت مسئله را عوض کنیم و مجموع کانفیگ و دیتابیس را از روی سرورها به یک محل متمرکزShared Folder یا Shared Storageانتقال دهیم

III

DNS Query → sales.Mcsa.com

Round Robin

First DNS Response	Second DNS Response	Third DNS Response
IP 1	IP 2	IP 3
IP 2	IP 3	IP 1
IP 3	IP 1	IP 2

- DNS موظف است همه Name Resolutionها را برگرداند
- با توجه به مورد بالا حالت Fault Telorance ساپورت می شود
- پیرو برگرداندن Round Robin آی پی ها ، حالت Load Balanceنیز ساپورت میشود
- با توجه به درخواست سرویس گیرنده DNS در صدر لیست نزدیکترینIP به Netid سرویس گیرنده را به صدر لیست انتقال می دهد

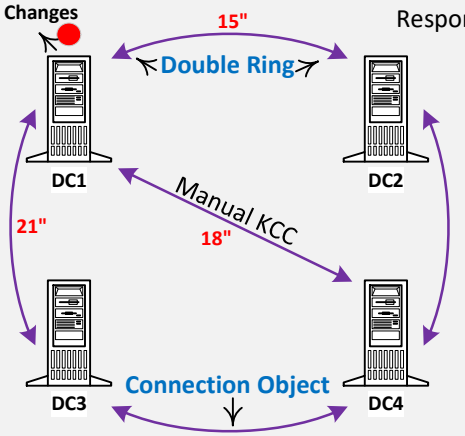
Dns Netmask Ordering

روش عمومی پیاده سازی سرویس ها بهره برداری از DNS

ipconfig /displaydns Run → List of dns query

Replication Topology

No Compress Replication



Repadmin /kcc → Force Update KCC

Automatic Replication

Connection object (User Account, Computer Accout,Group,.....)

- به فرایند اتوماتیک **Sync** شدن سرویس های سرور ها **Replication** گفته میشود
- اگر یک سرور تغییرات را به سرور دیگر اعمال کند به آن **Push Replication** می گویند
- اگر یک سرور تغییرات رافود از سرور دیگر دریافت کند **Pull Replication** می گویند
- در حالت **Push** عموما وقتی تغییرات به حجم یا میزان مشخصی رسید **Replication** انجام میشود
- در حالت **Pull** در بازه های زمانی مشخصی **Replication** انجام میشود
- یک روش بدین شکل است که پیرو تغییرات یک سرور ، سرور دیگر را باخبر می کند **Notify** سپس سروری که notify را دریافت کرده با استفاده از حالت Pull تغییرات را دریافت میکند
- حالت ترکیبی Pull و Push نیز برای مطمئن شدن از Sync شدن حتمی تغییرات استفاده می شود
- در AD حالت تلفیقی **Pull+Notify** جهت Replication بین سرورها استفاده می شود **(Pull Notification Based)**

- پیرو تغییرات در **DC1** ، مجموع سرورهای Partnerآن **Notify** میشوند
- سرور ها حداکثر هر ۱۵ ثانیه یکبار بصورت اتوماتیک اگر تغییراتی بوجود آمده بود مبادرت به عمل **Notify** میکنند و با فواصل زمانی ۳ ثانیه Notify به دیگر سرورها فرستاده میشود تا همه سرور ها بصورت همزمان مبادرت به **Pull** کردن تغییرات نکنند
- **Connection Object** بصورت اتوماتیک توسط کامپوننتی به نام **KCC** ساخته می شود
- تغییرات در سطح **Attribute** تبادل می شود و چیز اضافه تری انتقال داده نمی شود

KCC (Knowledge Consistency Checker)

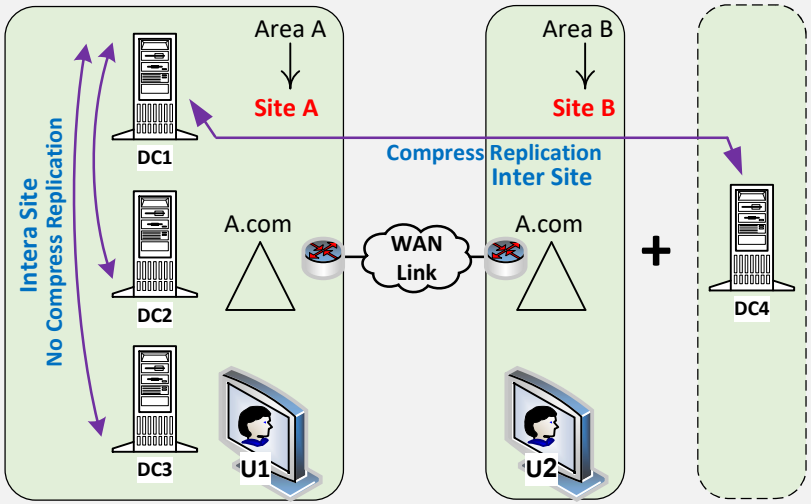
- **KCC** یکی از اجزاء ADمی باشد و وظیفه آن ساخت توپولوژی **Replication** می باشد
- Connection Object درصورت نیاز بصورت دستی نیز ساخته می شود
- KCC هر ۱۵ دقیقه یکبار Replication Topology را چک و در صورت نیاز **Update** میکند
- DC2 طبق توپولوژی میداند بین DC1 وDC4 ، کانکشن برقرار است بنابراین تغییرات را به DC4 Notify نمیکند

I

AD Structures

2 Physical Site

NetID in Site A is different from NetID in SiteB



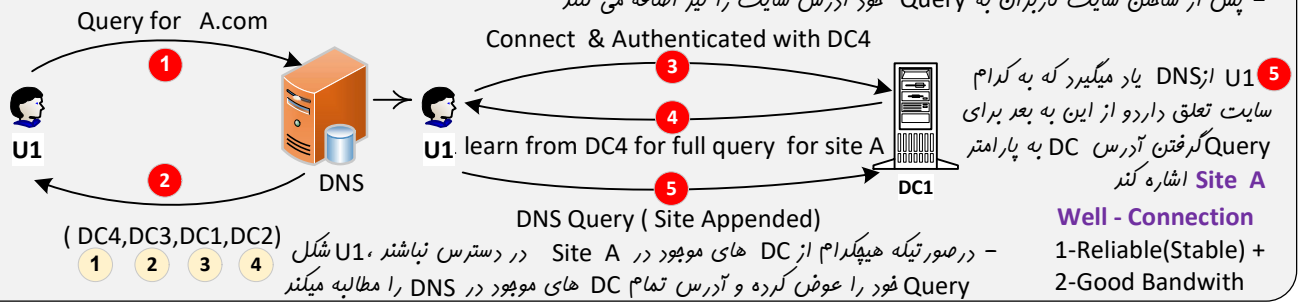
- در این سناریو کاربر مستقر در محل B از کند بودن دسترسی به دامین کنترلر که در محل A واقع شده است شکایت دارد در صورتیکه کاربران محل A از نظر سرعت دسترسی مشکلی ندارند و وقتی دامین کنترلهای محل A مانیتور میشوند سرعت و کارایی سرورها مطلوب می باشد

بروز یک مشکل

- جهت حل این مشکل تعداد یکعدد دامین کنترلر به محل B اضافه می نماییم **(Quick Access)**
- این امکان وجود دارد که بطور مثال DNS به کاربر **U1** طبق لیست خود در ابتدای آن لیست بصورت تصادفی **DC** موجود در محل **B** را اعلام کند
- حالت مطلوب اینست که اگر DC4 از دسترس خارج شده بود کلاینت U2 به DC های ناحیه A وصل شود و معکوس آن در مورد کلاینت U1 در ناحیه A

→ **Site**

- با ساختن Site در AD این امکان بوجود می آید که DNS در پاسخ Query کاربران هر سایت ، آدرس دامین کنترل های آن سایت را در اولویت قرار دهد
- پس از ساختن سایت کاربران به Query خود آدرس سایت را نیز اضافه می کنند



5 U1 از DNS یاد میگیرد که به کدام سایت تعلق دارد و از این به بعد برای Query گرفتن آدرس DC به پارامتر **Site A** اشاره کند

- درصورتیکه هیچکدام از DC های موجود در Site A در دسترس نباشند ، U1 شکل Query خود را عوض کرده و آدرس تمام DC های موجود در DNS را مطالبه میکند

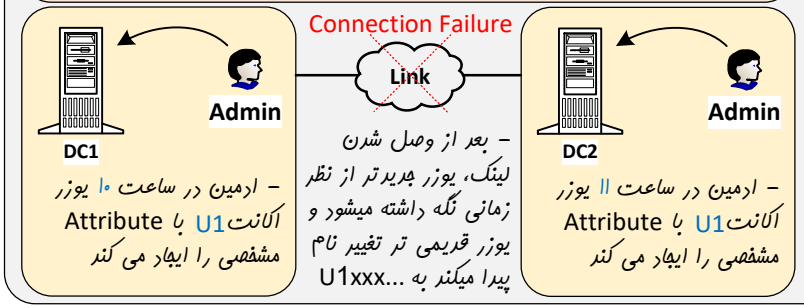
Well - Connection
1-Reliable(Stable) +
2-Good Bandwith

II

- در اینحالت DC1 و DC4 در بازهای زمانی مشخص بصورت **Pull** با هم ارتباط برقرار می کنند و برای هم Notification نمی فرستند
- در اینحالت هر ۳ ساعت یکبار ارتباط **Pull** برقرار می گردد که این زمان بر اساس ضریب **15n** از ۱۵ دقیقه تا ۷ روز قابل تغییر است
- اطلاعات بصورت **Compress** شده ارسال میگردد

Intera Site درون سایتی (2) ↓ **AD Replication** ↑ (1) **Inter Site** بین سایتی

- پیرو تغییرات در DC1 ، مجموع سرورهای Partner آن Notify میشوند
- سرور ها حداکثر هر ۱۵ ثانیه یکبار بصورت اتوماتیک اگر تغییراتی بوجود آمده بود مبادرت به عمل Notify میکنند و با فواصل زمانی ۳ ثانیه Notify به دیگر سرورها فرستاده میشود تا همه سرور ها بصورت همزمان مبادرت به Pull کردن تغییرات نکنند
- اطلاعات بصورت **Uncompress** ارسال میگردد
- این امکان وجود دارد که در حالت Inter Site با اعمال تنظیمات، Pull بصورت Notification Base و Compress نشده برقرار گردد



- ادمین در ساعت ۱۰ یوزر اکانت U1 با Attribute مشخصی را ایجاد می کند
- بعد از وصل شدن لینک، یوزر جدیدتر از نظر زمانی نگه داشته میشود و یوزر قدیمی تر تغییر نام پیدا میکند به U1xxx...
- ادمین در ساعت ۱۱ یوزر اکانت U1 با Attribute مشخصی را ایجاد می کند

- **Site** شامل یک یاچند DC میشود که بین آنها ارتباط خوب **Well - Connection** وجود دارد
- کاربرد سایت راه اندازی **Quick Access** است

- DC های مستقر در یک ساختمان ، در AD تشکیل یک Site مجزا را می دهند
- وقتی ارتباط بین DC ها از طریق LAN می باشدنیاز به ساختن Site مجزا نیست
- اگر ارتباط بین دو یا چند ساختمان از طریق LAN باشد و یا WAN از سرعت خیلی خوبی برخوردار باشد نیاز به ساخت Site نیست
- در ساختمانی که در آن DC وجود باید ترجیحا در AD ، Site ساخته شود
- با اضافه نمودن Site مشکل SPOF در ارتباط با DC مرتفع خواهد شد

Default-First-Site-Name
- این سایت بصورت پیش فرض در AD وجود دارد که میشود Rename نمود

User Interface

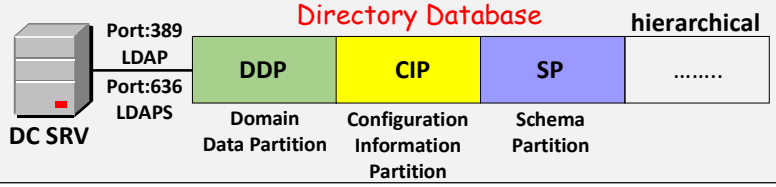
- از طریق رابط کاربری **(User Interface)** تعامل کاربر با دیتابیس بصورت کنترل شده فراهم می گردد
- دیتا بیس مجموعه ای از **Object (Table)** هاست که هر کدام شامل تعدادی **Attribute (Field)** می شود که از بدو طراحی مشخص می گردد

→ **Schema**

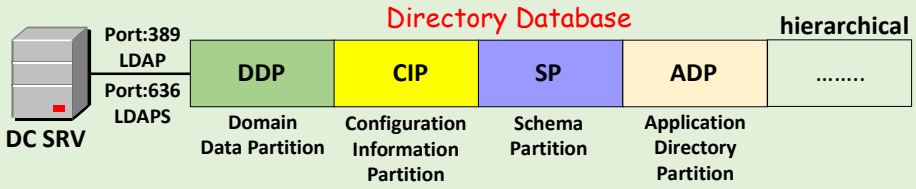
- اینکه از طریق رابط کاربری ، کاربر چه Object هایی با چه Attribute هایی میتواند ذخیره کند الگو یا مدل دیتابیس گفته میشود
- لیستی از Type Object ها و Attribute هایی است که به ازاء Object ها میتوان در دیتابیس ذخیره نمود

- به اضافه نمودن Object Class و Attribute به Schema اصطلاحا **Extend** کردن Schema میگویند
- با توجه به گسترش (Schema) باید (User Interface) نیز اصلاح شود
- ادمین بواسطه **User Interface** که به آن **Management Tools** نیز گفته میشود با **Directory** در تعامل می باشد

Directory Database

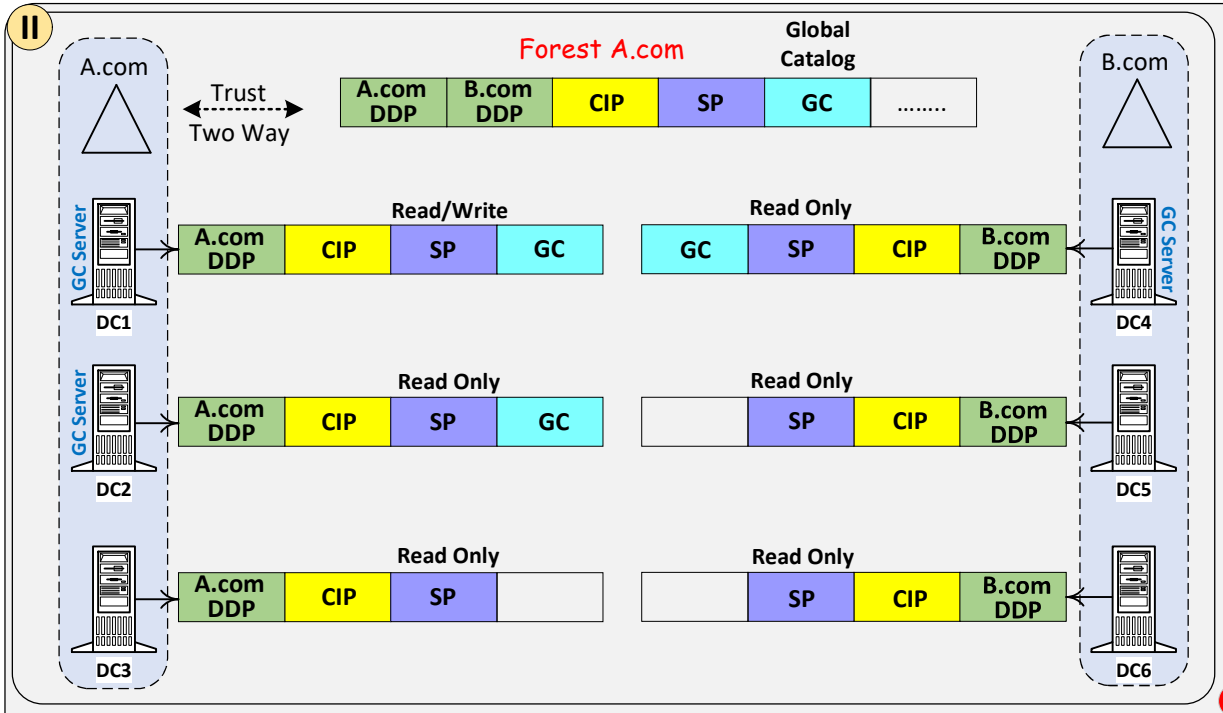


I AD Integrated Application



- AD Integrated Application نرم افزارهایی هستند که به AD وابسته هستند و بدون آن کار نمیکنند، این اپلیکیشن ها تمام یا بخشی از کانفیگ یا دیتای خود را در Directory ذخیره میکنند ، این اطلاعات ممکن است در DDP یا CIP ذخیره شود ولی یقینا در SP ذخیره نمیشود و ضمنا بر اساس نیاز خود میتواند پارتیشن به Directory برای ذخیره دیتای خود اضافه کند بطور مثال DNS
- این نرم افزارها ممکن است دیتا یا کانفیگی را در Directory ذخیره نکنند ولی به اطلاعات موجود در AD نیاز داشته باشند و با آن در تعامل باشند
- این نرم افزارها محدود به الگو Schema هست ذخیره دیتای خود هستند و در صورت نبود Object یا Attribute باید Schema توسط Setup نرم افزار Extend شود
- الگو گسترش یافته توسط نرم افزارهای وابسته به اکتیو دایرکتوری ، در صورت حذف نرم افزار از دیتابیس دایرکتوری حذف نمی شود

II

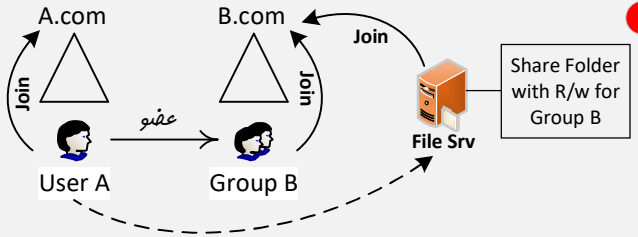


A Replication Scope Per Partition

Domain Data Partition	Replication Scope	Domain Wide
Configuration Information Partition	Replication Scope	Forest Wide
Schema Partition	Replication Scope	Forest Wide
GC	Replication Scope	Forest Wide

- فقط از طریق DC1 امکان Extend ، Schema وجود دارد و از طریق DC1 به الباقی DC ها Replicate می شود
- طبق شکل هیچکدام از DC ها کل دایرکتوری را ندارند و تجمیع DC ها شامل کل دایرکتوری میگردد ←
- اگر در کل دایرکتوری بخواهیم جستجو کنیم هیچکدام از DC ها شامل کل دایرکتوری نمی شود

B



- در اینحالت یک Object در A.com مرتبط به Object دیگر در B.com است
- در شکل بالا کاربر A از دامین A.com یک تیکت میگیرد که حاوی SID این کاربر می باشد ولی برای استفاده از فایل سرور نیاز به این دارد که Security SID Group هایی که این کاربر عضو آن است ثبت شده باشد ، مشکل این جاست که DC های دامین A.com از Object های دامین B.com بی خبر هستند ، برای رفع این مشکل باید پارتیشنی به دایرکتوری با نام Global Catalog اضافه شود این پارتیشن به کارگرفته میشود ولی بعنوان یک پارتیشن شمرده نمیشود ، این پارتیشن شامل همه Object ها به همراه Attribute های منتخب می شود
- رمز عبور در GC ذخیره نمیشود

C

- هر User Account یک Attribute دارد به نام SID و این صفت هویت اصلی User Account است و صرفا View دارد و قابل تغییر نیست
- در انتخاب Attribute های Object جهت ذخیره در GC میتوان تغییرات اعمال نمود
- به DC که حاوی پارتیشن GC باشد GC Server میگویند و میتوان بیش از یک GC Server در Forest داشت
- اگربخواهیم در کل دایرکتوری جستجو نمائیم باید از GC Server استفاده کنیم
- با مراجعه به GC ها DC در تیکتی که صادر میکنند SID کاربر و گروه هایی که کاربر عضو آن است را درج می نمایند
- بحث SPOF در ارتباط با GC نیز صادق است در ضمن GC در محدوده Forest Wide عمل میکند
- اگر GC Server Forest نداشته باشد به جزء ادمین Log on به Domain میسر نخواهد بود و نرم افزارهای وابسته به AD کار نخواهد کرد و Forest Down اتفاق خواهد افتاد
- هنگام صادر کردن تیکت توسط DC اگر GC Server موجود نباشد برای استعلام و ثبت گروه هایی که کاربر در آن عضو می باشد باید به یک GC Server مراجعه کند و اگر در Forest موجود نباشد عملا Forest Down اتفاق می افتد

I

User A —عضو→ Group B

- اگر کاربری بواسطه عضویت در گروه های مختلف به یک منبعی دسترسی داشته باشد و فقط در یک گروه دسترسی او به آن منبع گرفته شود ، دسترسی کاربر به آن منبع خاص لغو Override می شود
- به واسطه عضویت در یک گروه ، دسترسی های کاربر ممکن است بیشتر یا کمتر شود

Permission

1. **Allow** — دسترسی دادن
2. **Don't Allow** — دسترسی ندادن
3. **Deny** — دسترسی گرفتن

- هنگام صادر کردن تیکت توسط DC اگر GC Server موجود نباشد برای استعلام و ثبت گروه هایی که کاربر در آن عضو می باشد باید به یک GC Server مراجعه کند و اگر GC در Forest موجود نباشد عملا Forest Down اتفاق می افتد
- علت دیگر مراجعه به GC مشخص نمودن و مطمئن شدن از Deny Permission در کل گروه های موجود در Forest می باشد

Type Of Partition

1. **Active Directory Partition** → (DDP-SIP-SP) → Mandatory
2. **AD Integrated Partition** ← (ADP) ← Optional

II

1 Pre Configuration for DC

- به تنظیمات اولیه ویندوز اصطلاح زیر گفته میشود

OOBE (Out Of Box Experience)

1. Add Proper computer name
2. Configure Network Adapter
3. Disable ipv6 & Link-Layer Topology
4. Add 127.0.0.1 for dns server
5. Disable LMHOSTS lookup & NetBIOS over TCP from WINS Tab
6. Open add role and features on server manager

(Ready for Promotion)

- ابتدا باید رول اکتیو دایرکتوری فعال شود

7. Check mark Active Directory Domain Services and continue

- یک Utility کاربردی جهت Hardening ویندوز برنامه NARTAC SOFTWARE Best Practice می باشد که بعد از اجراء حالت IIS Crypto را انتخاب می کنیم

2 Deployment Configuration

1. Goto Server Manager Post Wizard for DC or type dcpromo from run
2. **New Forest** → A.com
3. New Domain { New Tree / New Child
4. New DC

3-1 Domain Controller option

1. Check Mark Domain Name System (DNS) Server
2. Forced Check Mark Global Catalog (GC)
3. No Check Mark Read Only Domain Controller (RODC)

- جهت تصحیح اشتباهات رخ داده شده در دامین کنترلر و برگرداندن دیتا به وضعیت قبلی استفاده میشود ، برای دامین اول امکان انتخاب ندارد

DC Install

- توصیه میشود که برای راه اندازی DC از یک ماشین فیزیکی و نصب بصورت Core Mode استفاده شود تا در صورت بروز مشکل در فضای ماشین های مجازی سرور موجود صدمه نبیند

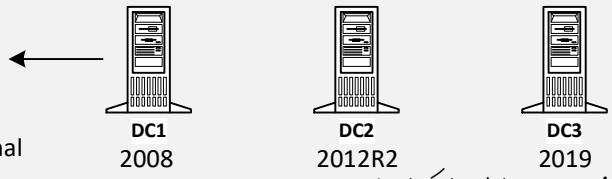
dcpromo → Run dc wizrd promotion	**cmd** → sconfig → Core mode server configuration	**ncpa.cpl** → Network configuration
Services.msc → System Services	**msconfig** → For safe mode AD repair (DRSM)	**ntdsutil** → Reset DSRM Password
Dismgmt.msc → Disk Management	**winver** → Display Win Version	**Servermanager** → SM Dashboard
Control → Control Panel		

- DC از 2008R2 به بعد Recycle bin وجود دارد که بصورت پیش فرض فعال نیست
- بعد از فعال سازی Recycle bin وقتی Object ای پاک میشود اصلا به مدت ۱۸۰ روز **Tomb Stone** میشود که امکان برگرداندن در این مدت را دارد

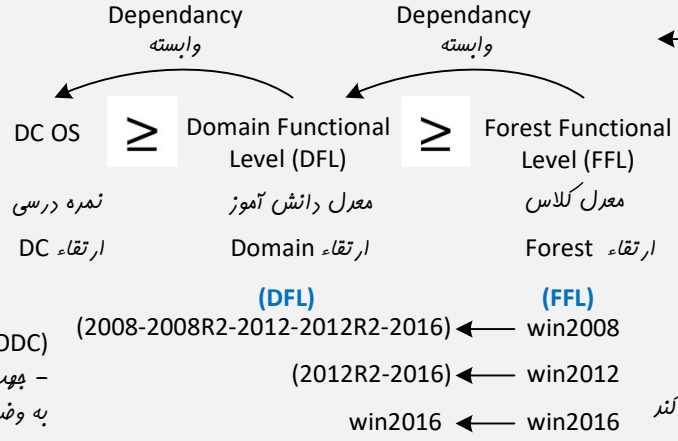
4 Type DSRM Password

- جهت برگرداندن بکاپ ابتدا باید سرویس اکتیو دایرکتوری رامتوقف کنیم تا فایل Ntds.dit از حالت قفل (in use) خارج شود در اینحالت امکان Compress و جابجایی فایل دایرکتوری مقدور است ولی همچنان نمیتوان بکاپ برگرداند بنابراین باید ویندوز را در حالت Safe Mode with network بالا آورد ، حال مشکل دیگر اینست که برنامه ای که با آن از DC بکاپ گرفته ایم در حالت Safe Mode کار نمیکند حال مایکروسافت حالتی از Safe Mode در AD را شامل میشود به نام Directory Services Restore mode (DSRM) که از ۲۰۰۸ به بعد بصورت Member Server (join to DC) کار می کند و چون پس از نصب DC محتویات LSD به DSD انتقال داده میشود باید بصورت دامینی وصل شویم ، لازم به ذکر است در DC های دوم به بعد LSD با محتویاتش پاک می شود و دایرکتوری به آن Replicate میشود - هر DC رمز **DSRM** خودش را دارد که موقع نصب DC مشخص می شود

3-2 Forest & Domain Functional Level



- بعلت ارتقاء DC ها در حال حاضر سیستم عامل ها یکسان نیستند
- بعلت وجود نرم افزار خاص در سمت کلاینت مجبور به داشتن سیستم عامل های متفاوت هستیم
- این امکان وجود ندارد که AD با نسخه پایین تر بر روی ویندوز بالاتر داشته باشیم
- مشخص کردن سطح عملیاتی در دامین و فعال نمودن عملیات های خاص تا سطح مشخص شده
- هر آنچه همه نسخه های مختلف ویندوز پشتیبانی میکنند بعنوان سطح عملیاتی در نظر گرفته می شود
- اگر تغییرات به دامین ربط پیدا کند باید دامین سطح عملیاتی مشخص شده را ساپورت کند
- اگر تغییرات به Forest ربط پیدا کند باید Forest سطح عملیاتی مشخص شده را ساپورت کند
- در صورت ارتقاء سرور های دامین امکان ارتقاء سطح عملیاتی وجود خواهد داشت



DC Install

4 DNS Option

1 No Check Mark Create DNS Deligation

– پیغام خطارا نادیده می گیریم

5 Additional Options

1 Type The Netbios domain name

– نام NetBIOS را تایپ نموده و سپس جستجو کرده و فرآیند نصب را ادامه می دهیم

6 Path

1 Database Folder: c:\windows\NTDS

– محتویات DC,LSD اول به DDP (Directory) که قرار است ساخته شود انتقال داده میشود

– محل قرارگیری فایل Ntds.dit پرسیده میشود

2 Log Files Folder: c:\windows\NTDS

– محل قرار گیری Transaction Log مشخص می گردد که مرتبط با یک دیتا بیس می باشد

Log Files

- **Event Log**
  - **Categories:** (Application Log, System Log, Security Log,Directory Service Log, DNS Log, File Replication Service Log)
  - **Type:** (information,Warning,Error,Success Audit security,Failure Audit Security)
- **Transaction Log**
  - Edb*.log 10 Mb The transaction log file
  - Edb.chk A checkpoint file
  - Resl.log The reserved transaction log files
  - andRes2.log

– به هر تراکنش جهت ثبت ، اصلاح یا حذف داده یک دیتابیس را Transaction Commit میگویند، و دیتا بیس از Log ها در جهت بازیابی اطلاعاتی که بصورت ناگهانی پیرو قطع برق یا ارتباط کاربر یا هر مورد دیگری اتفاق می افتد استفاده میکند تا اطلاعات را بازیابی کند یا به حالت قبل از تراکنش بر گرداند

– از Log ها برای بازیابی اطلاعات نیز استفاده میشود که اندازه حجمی و زمانی آن از زمان Full Backup تا زمان فعلی و جاری میباشد که به آن Auto Recovery میگویند

– درج دیتا توسط کاربر اول به Transaction Log انتقال داده میشود و بعد به دیتا بیس انتقال می یابد

– وقتی اطلاعات ابتدا به Transaction Log انتقال داده میشود نظم دقیقی که در موقع انتقال به دیتا بیس انتظار می رود را ندارد در صورتیکه محل این Log فایلها در یک دیسک مجزا از محل دیتابیس و با سرعت بالا در نظر گرفته شود باعث افزایش کارایی Performance میشود ، بدین صورت کاربر منتظر ارسال دیتا به دیتابیس نمیشود و با سرعت بالا اطلاعات به Transaction Log انتقال پیدا میکند

3 SYSVOL Folder: c:\windows\SYSVOL

– در حالت Domain Base مجموعه کلاینت ها بصورت Pull جهت گرفتن Policy های مشترک به DC مراجعه میکنند، Policy ها شبیه امرو نهی یا دستور تلقی میگردند

– Sysvol یک فولدر Share است که مجموع Policy های مشترک درون آن قرار دارند ، کاربران برای گرفتن Policy مرتبط به این فولدر مراجعه می کنند

– Directorty و Transaction Log را میتوان در درایوی با فرمت FAT32 ذخیره نمود ولی Sysvol الزاما باید حتما در پارتیشنی با فرمت NTFS ذخیره شود

Convert.exe → FAT to NTFS Convert
Convert d: /fs:NTFS

7 Review Options

1 View Script

– در صورتیکه بخواهیم بصورت Unattend نصب DC را در این سرور یا سرور دیگر ادامه دهیم Script را بصورت فایل متنی ذخیره نموده سپس پسوند آن را به ps1 تغییر میدهیم و از طریق Power Shell نصب DC را ادامه میدهیم

Install → **Attended** با حضور
Unattend بدون حضور → نیاز به → Answer File Script

```
Import-Module ADDDeployment
Install -ADDSForest
-CreateDnsDelegation:$false
-DatabasePath “C:\Windows\NTDS”
-DomainMode “Win2008”
-DomainName “A.com”
-DomainNetbiosName “A”
-ForestMode “Win2008”
-InstallDns:$true
-LogPath “C:\Windows\NTDS”
-NoRebootOnComplietion:$false
-SysvolPath “c:\Windows\sysvol”
-Force:$true
```

– جهت تغییر رمز ارتباط با Directory به جای LDAP(389) بصورت LDAPS(636) برقرار می گردد

– ساخت ۱۰۰ کاربر از طریق Command Prompt

Dnsmgmt.msc → DNS Manager

```
for /l %v in (1,1,100) do dsadd user cn=u%v,cn=users,dc=A,dc=com -pwd P@ssw0rd
```

– فولدر دوم sysvol و فولدر Scripts به اسم Netlogon بصورت Share در اختیار کاربران می باشد

C:\Windows\SYSVOL**sysvol**\A.com\
- Policies
- **Scripts** → Netlogon

DDP

Dsa.msc → Active Directory Users and Computers → Raise Domain Functional Level

CIP

Domain.msc → Active Directory Domains and Trusts → Raise Domain & Forest Level

CIP

Dssite.msc → Active Directory Site and Services → Enable **GC** from NTDS Setting

DDP+CIP

Dsac → Active Directory Administrative Center →
- Enable AD Recycle bin
- Raise Domain & Forest Level

– قابلیت Recycle bin از 2008R2 به DC اضافه شده و باید Functional Level حداقل 2008R2 باشد یا ارتقاء پیدا کند چون AD در حقیقت Forest AD محسوب میگردد

– در صورت افزایش Raise Domain & Forest Functional Level امکان کاهش آن وجود ندارد

DDP+CIP+SP+ADP

Adsiedit.msc → Extend ADSI Tools → Advanced ADSI Edit Tool

– اصطلاح Addational DC یا Secondary DC بی معنی است چون همه DC ها یک شرایط مشخص و ثابت دارند

– برای اضافه کردن DC دوم به فارست فرقی نمیکند ابتدا به DC اول Join شود و بعد Promote شود و یا مستقیما به فارست Promote شود نتیجه کار یکی است

– اگر ماشینی در حال حاضر عضو A.com باشد و بخواهیم بعنوان DC دوم به فارست B.com معرفی کنیم باز نیز فرقی نمیکند که حتما در ابتدا Disjoin شود و بعد به DC ها اضافه شود یا مستقیما بعنوان DC دوم Promote شود

– در زمان راه اندازی DC دوم از طریق شبکه بعد از پاک شدن LSD محتویات Directory و Sysvol از DC اول به DC جدید انتقال داده می شود در صورتیکه ارتباط بین دو DC از طریق WAN و ناپایدار باشد این انتقال را میتوان از طریق یک مدیا انجام داد Install From Media → (Export-Import)

Dssite.msc → Default-first-site → NTS settings → Automatic generated → R-Click → Replicate now → **Ok** ← تست Replication بین دو DC

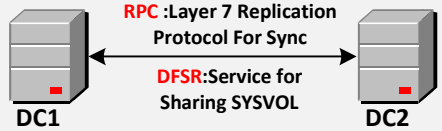
– فولدرهای Sysvol در دو DC وضعیت یکسان دارند و اضافه وپاک شدن یک Object در هر دو یکسان است

Repadmin /kcc → Force Connection object

Repadmin /syncall → Sync with all Partners

Repadmin /replsum → Replication Summary

Dcdiag /q → Only print error messages



– برای مانیتور کردن DC یکی از محصولات خوب Manage Engine می باشد ، محصول مایکروسافتی در این زمینه **ADREPLSTATUS** و سرویس مانیتور جامع تر به نام **SCOM** می باشد **(System Center Operation Manager)**

– برای Demote کردن DC از Server Manager بخش Manage/Remove Role and Features اقدام میکنیم پس از Demote شدن ماشین بصورت Join to Domain و اصلاحا Member Server بالا می آید

I

Domain Admins Group (admin Domain) → DDP

Enterprise Admins Group (admin Forest) → (Modify Forest) → CIP

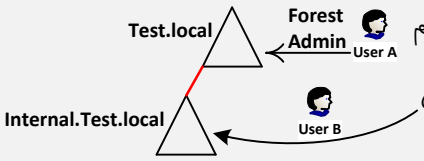
Schema Admins Group (admin Forest)

(Extend Schema) → SP

این دو گروه فقط در اولین دامین فارست وجود دارند

User A عضو → Administrators Group

اگر کسی عضو گروه Administrators باشد میتواند خود را عضو تمام گروه های موجود کند ، در اینحالت تمایز بین ادمین دامین و فارست وجود نخواهد داشت



میخواهیم کاربر B را ادمین دامین کنیم ونه فارست اگر فارست فقط یک دامین داشته باشد ، امکان تمایز بین ادمین دامین و فارست وجود ندارد

اگر کامپیوتر ها و کاربران Join به Child دامین باشند و شخص مورد نظر ادمین دامین Child باشد ، تمایز بین ادمین دامین و فارست ایجاد شده است

در این نوع طراحی چون Policy های دامین اصلی و Child از هم مجزا هستند ، تهدیدات امنیتی دامین بالاتر شامل دامین Child نمیشود

ضمنا با ایجاد چند Forest همانند Vlanning در طراحی شبکه میشود Zone بندی های مجزا داشت و ضریب امنیت را بالاتر برد

II

Join Clients to DC

- Offline → (From win 7 & 2008R2)
- Online

ملزومات Join آنلاین کلاینت به دامین

1. داشتن یک Local User Account عضو Local Administrators
2. داشتن نام FQDN دامین ← (Domain DNS Name)

برای Join کردن به دامین از اسم NetBIOS نیز میشود استفاده کرد که اشتباه می باشد ، چون در اینحالت از روش Broadcast استفاده میشود و به DNS مراجعه نمی گردد

3. داشتن Domain User Account

- بعد از Join کلاینت به دامین هم در سمت کلاینت تغییرات بوجود می آید و هم در سمت سرور دامین AD

Client ↓ Client

- تغییر Policy در کلاینت ، چون تحت تاثیر یکسری Policy مشترک قرار می گیرد
- تغییر نام کلاینت و اضافه شدن Suffix Name به Host Name
- تغییر در گروه ها و زمان کلاینت چون DC نقش NTP را بازی می کند
- قبل از Join کلاینت باید زمان و تاریخ با DC ، Sync باشد
- عمل Join به اعتبار Domain User Account انجام میشود

AD ↓ AD

- در AD ، Domain User Account ایجاد میگردد
- در AD ، Domain Computer Account ایجاد میگردد
- Computer Account در حین Join ساخته می شود

III

Computer Account

- Computer Name
- Password

- هنگام Join به دامین نام کامپیوتر و پسورد بصورت اتوماتیک و ساخته میشود و ارتباطی به ادمین ندارد و در حقیقت این پسورد است که ماهیت Computer Account را می سازد و پسورد آن بصورت اتوماتیک ۳۰ روز یکبار تغییر می کند
- پسورد User Account بصورت پیش فرض ۴۲ روز بعد باطل میشود

- قبل از جواب دادن به هر پنجره ای که از سمت دامین نام کاربری و رمز عبور را طلب میکند به سه سوال باید جواب داد

1. نام کاربری و رمز عبور را دقیقا چه رابطی میخواهد؟
2. نام کاربری و رمز عبور را دقیقا برای چی میخواهد؟
3. نام کاربری و رمز عبور حداقلی چیست؟

- بعضی اوقات نیاز به درج نام کاربری و رمز نیست و بر اساس الگوی دامین کنترلر این سوال پرسیده میشود

نکته مهم

- با یک Standard User Account نیز به تعداد ۱۰ بار میتوان Join به دامین نمود که میتوان به صفر تغییر داد

Active directory users and computer

View/advance features

R-click on Domain name

Properties/attribute editors

Ms-DS-MachineAccountQuata=0

IV

- پس از ساخت یک کاربر بصورت اتوماتیک کاربر عضو گروه Domain Users میشود
- این امکان وجود دارد که وظیفه Join to domain یا دیگر وظایف را از طریق Delegate Control به یک یا چند کاربر یا گروه تفضیص داد

Active directory users and computer

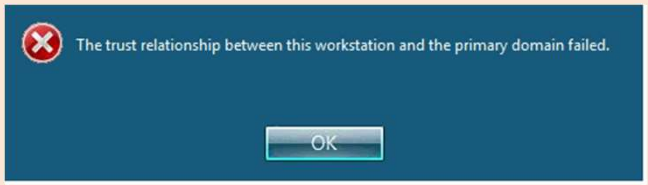
View/advance features

R-click on Domain name

Delegate Control

Join a Computer to a domain

رفع ایراد Trust Relationship



- یک روز 30 از بیش مثلا نمود Log on دامین به نتوان است ممکن مختلفی بدلایل Computer Account

1. میتوانیم کلاینت را Rejoin=Disjoin+join کنیم

- با administrtor\. بصورت Local لاگین کنیم بعد Disjoin و سپس join
- اگر با کاربری که قبلا Join کرده ایم Disjoin کنیم بدون Restart میتوان مجدد Join نمود در غیر اینصورت باید قبل Join مجدد Restart کنیم
- اگر با کاربر u1 قبلا Join کرده باشیم و بخواهیم Rejoin کنیم بدون حذف Computer Account میتوان مجددا به DC کلاینت را Join نمود ولی اگر بخواهیم با کاربر u2 کلاینت را Join کنیم در اینصورت باید قبل از Join مجدد Computer Account را از DC حذف کنیم

I

Rejoin ادامه

- فرض که کلاینت **A** با **u2** به دامین Join شده است
- فرض که کاربر **u1** عضو **Admin Local** است
- این کار را با دستور **Lusrmgr.msc** بصورت Run as administrator میتوان انجام داد

- در این مقطع نام و رمز کاربری را ویندوز میخواهد که بصورت اختیاری است ، چون سیستم میخواهد با قدرت نام کاربری که دریافت میکند Computer Account را Disable کند و در صورتیکه نام کاربری داده نشود **Computer Account** را **Disable** نمیکند فرض را بر این میگذاریم که نام کاربری را ندهیم

Delete PCA

- برای Join مجدد به مشکل Access is denied بر میخوریم چون Computer Account در مرحله قبل Disable نشده است
- در اینحالت اگر بخواهیم با کاربر u1 کلاینت را Join مجدد کنیم باید Computer Account را در DC پاک کنیم

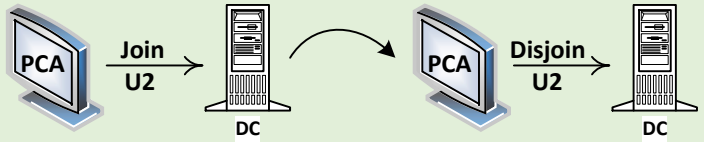
نکته مهم

- مجموع کانفیگ ها بر اساس SID در AD ثبت میشود پس اگر ما نام کامپیوتر را در DC پاک این کنیم عملا SID را برای همیشه از دست داده ایم و در مورد ماشین Exchange Server موضوع تبدیل به یک فاجعه خواهد شد این معضل در سمت سرور معنی پیدا میکند

2 - راه حل صحیح این است که **Computer Account** را **Reset** کنیم تا SID محفوظ بماند

Computer Account → Properties → Security → Advanced → Owner

- با روش بالا مشخص میشود صاحب کامپیوتر کیست که سیستم را Join کرده است



- در حالت بالا دیگر سیستم در موقع Disjoin نام کاربری نمیخواهد و نام کامپیوتر را نیز در DC به حالت Disable در می آورد چون خودش Join کرده و مجوز دارد
- پس بعنوان یک روش باید برای Join/Disjoin کردن کامپیوتر ها در AD از اکانتی استفاده کنیم که مجوز **Reset / Disable** کردن نام کامپیوتر را داشته باشد

- گروه **Account Operators** مجوز **Reset / Disable** کامپیوترها را دارد

II

- جهت اعطاء مجوز **Reset / Disable** از روش روبه رو استفاده میکنیم تا به یک کاربر یا گروه دسترسی کامل برای **Disjoin/join** را مهیا کنیم

روش Join کردن سیستم از طریق Command

- در این حالت فرق نمیکند از چه کامپیوتری در دامین استفاده شود DC or Client

Command | Client IP | Domain Name | Domain user | Domain user pass

netdom join 10.1.1.2 /domain:test.com /userd:u1 /passwordd:pass / user0:administrator /passwordo:pass /reboot:3

Admin Local | Admin Local Pass | Reboot after 3 "

Active directory users and computer
→ View/advance features
→ R-click on favorite Group
→ Properties
→ Add/Select a Principal
→ Descent computer objects
→ full control or enable, Read lockoutTime, and Write lockoutTime

Active Directory Administration / Management

جهت مدیریت اکتیو دایرکتوری به المانهای زیر نیاز می باشد

Permission or Rights or Both 1
- مجوز انجام کار مدیریتی

Management Tools(User Interface) 2
- ابزار های مدیریتی (GUI,CLI,Powershell ,Web UI,....)

Network Infrastructure 3
- زیرساخت تبادل اطلاعات

mmc(Microsoft Management Console) → **Snap-in** → **RSAT:Install Remote Server Administration Tools in None-server OS & Add Features on Servers OS**

جعبه ابزار — ابزار

mmc → **Add** → **Snap-in** → **Save** → **Name.msc**

- جعبه ابزار آماده، شامل یک یا چند ابزار
- قانون 8:3 کم و بیش در ویندوز رعایت میشود که شامل نام فایل حداکثر ۸ کاراکتر و پسوند آن شامل ۳ کاراکتر می باشد
- قبل از **Win/2008Vista** از جعبه ابزار **Adminpak.msi** استفاده میشد که ماجولار نبود و فقط شامل تعداد زیادی ابزار مجزا بود
- از ویندوز **Win/2008Vista** از ویژگی استفاده شد به نام **RSAT** که یک جعبه ابزار ماجولار میباشد که بصورت **Built-in** در سرورها موجود است

Traditional

DDP	**Dsa.msc** → Active Directory Users and Computers	→ Raise Domain Functional Level
CIP	**Domain.msc** → Active Directory Domains and Trusts	→ Raise Domain & Forest Level
CIP	**Dssite.msc** → Active Directory Site and Services	→ Enable **GC** from NTDS Setting
DDP+CIP	**Dsac** → Active Directory Administrative Center	→ Enable AD Recycle bin → Raise Domain & Forest Level
DDP+CIP+SP+ADP	**Adsiedit.msc** → Extend ADSI Tools	→ Advanced ADSI Edit Tool
DNS	**Dnsmgmt.msc** → DNS Manager	→ DNS Manager
GPO	**Gpmc.msc** → Group Policy Management	→ Group Policy Management
LDAP	**Ldp** → LDAP Modify	→ Change Special Attribute and view DDP,CIP,SP,ADP
	Ntdsutil , esentutl → Cmd Tools	→ Active directory (defrag , repair , dump , ...)

Gpedit.msc → Local GPO
sysdm.cpl → System Properties
Lusrmgr.msc → Local User and Groups
Compmgmt.msc → Computer Management

I

- جهت اضافه نمودن **Snap-in Active Directory shema** به mmc باید ابتدا فایل schmmgmt.dll را در سیستم رجیستر نمائیم **regsvr32 schmmgmt.dll**
- جهت تنوع در ابزارها ی گزارش گیری و کار با اکتیو دایرکتوری برای تعداد بالایی از کاربران بصورت همزمان از نرم افزارهای **3rd Party** استفاده میشود که یکی از نمونه های خوب آن نرم افزارهای شرکت **Manage Engine** می باشد **(AD Manager Plus)**
- Snap-inهایی که با پسوند **msc** توسط مایکروسافت ساخته شده است قابلیت ماجولار ندارد و بصورت مد **User mode** ساخته میشود و صرفا بصورت تک ابزاره قابل استفاده است
- Snap-inهایی که با پسوند **msc** توسط کاربر ساخته میشود بصورت پیش فرض با مد موالف **Author mode** ساخته میشود که قابلیت ماجولار دارد این امکان وجود دارد که **msc** که کاربر میسازد بصورت **User mode** ذخیره نمود

Default UPN suffix - DNS Domain Name

User Domain Logon Name

- u1@test.local → **UPN: User Principal Name**
- test\u1 → **NetBIOS name(pre windows)**

این امکان وجود دارد که UPN Suffix را از طریق Domain.msc تغییر دهیم و امنیت Logon کاربران را بالاتر ببریم

Active directory Domains & Trusts —R-Click→ Properties → **Add Alternative UPN Suffixes**

مدیریت UPN Suffixes را GC Servers انجام می دهد

- از طریق Alt+Ctrl+Del و سپس Change Password امکان عوض کردن هر کاری اعم از کاربر جاری و یا دیگر کاربران وجود دارد البته بشرط داشتن پسورد فعلی
- اگر کاربری یکسری فایل را از طریق EFS: Encrypt File System رمز کرده باشد و بعد Change Password اتفاق بیافتد مشکلی ایجاد نمیشود ولی اگر Reset Password انجام شود فایلهای رمز شده را دیگر نمیتواند بازیابی کند
- نامی که در AD Users and Computers دیده میشود صرفا یک لیبل نام است و ربطی به دیگر Attributeها اعم از ....Username, Account name, ندارد
- در ارتباط با Logon to در مشخصات Account کاربران نام NetBIOS Name درج می گردد
- در ارتباط با Logon Hours منظور زمانهایی است که کاربر میتواند Logon کند و بعد یا قبل از آن زمان ها همچنان به Logon ادامه دهد ، اگر بخواهیم این زمان های قبل یا بعد Logon را از کار بر بگیریم باید Policy مرتبط را تغییر دهیم

Policy → Network Security : Force logoff when logon hours expire

II

GP : Group Policy

A

- در هر Group Policy یک یا چند Policy وجود دارد

GP

1. **Local Group Policy object** —Local→ **Local GPO**
2. **None-Local Group Policy object** —AD→ **GP Object**

1 Local GPO

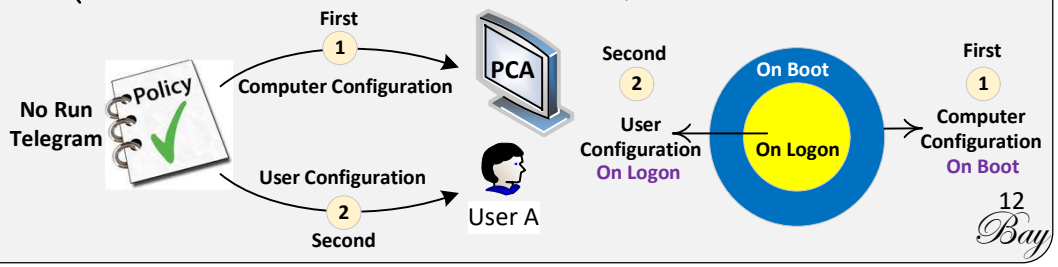
Gpedit.msc → Local GPO

- اعضای گروه Administrators امکان دیدن و ویرایش را دارند
- از دستورات **Whoami , whoami /groups** جهت فهمیدن نام کاربر و گروه های مرتبط با آن استفاده میکنیم
- Policy ها به دو گروه دسته بندی میشوند
- این پالیسی مستقل از اینکه چه کاربری به سیستم Logon کند اعمال میشود

Local GPO

1. **Computer Configuration**
2. **User Configuration**

- این پالیسی مربوط به کاربری است که به سیستم Logonمیکند



B

- تفاوت Computer Configuration و User Configuration در ترتیب پردازش آنهاست
- وقتی کامپیوتر بوت میشود و قبل از ورود به ویندوز Computer Configuration پردازش شده وبه سیستم اعمال میشود و بعد که کاربر به سیستم Logon نمود حال User Configuration پردازش شده و اعمال میشود سپس ویندوز در اختیارکاربر قرار می گیرد
- تعداد کمی پالیسی مشترک بین Computer Configuration و User Configuration وجود دارد حدود ۲۰ درصد
- در ارتباط با پالیسی های مشترک اگر تضادی پیش بیاید پالیسی Computer Configuration مورد قبول واقع میشود

سناریو تستی

- کلیه کاربران به Control Panel کنترل پنل دسترسی نداشته باشند

User Configuration → Administrative Template → Control Panel —Enable→ **Prohibit access to control panel and pc setting**

- کلیه کاربران به جزء کاربرانی که عضو گروه Administrators هستند به کنترل پنل دسترسی نداشته باشند

mmc → Add/remove Snap-in → Add Group policy object editor → Browse local computer → users → None-administrators

- بعد از ایجاد mmc خاص طبق مراحل سناریو اول Policy را فعال میکنیم

Rsop.msc → Resultant set of policy ← این ابزارنام و منبع پالیسی های اعمال شده بر روی کاربر را نشان میدهد

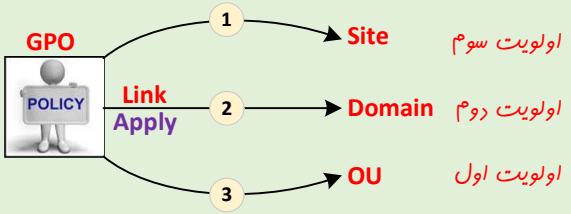
Secpol .msc → Security policy ← فقط بخش Security رانشان میدهد

I

2 GP Object

Gpmc.msc → Group Policy Management

– هر دامینی بصورت پیش فرض ۲ عدد GP Object دارد



Linked Policy ← Default Domain Policy

– لینکهای GPO به هر دو کامپیوتر و کاربر Apply میشود

Password Policy

– کامپیوترهای عضو دامین تحت تاثیر Default Domain Policy از سمت دامین قرار میگیرند

Default Domain Policy

Computer Configuration

→ Policies

→ Windows Setting

→ Security Setting

→ Account Policies

→ Password Policies

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Minimum password length audit
- Store passwords using reversible encryption
- Password must meet complexity requirements

Be at least Six characters in length

Contain characters from three of the following four categories:

1-English uppercase characters (A through Z)

2-English lowercase characters (a through z)

3-Base 10 digits (0 through 9)

4-Non-alphabetic characters (for example, !, $, #, %)

II

وقتی از gpedit.msc در یک سیستم غیر از دامین کنترلر استفاده کنیم پالیسیهایی که از سمت دامین پالیسی Force شده باشد فقط قدرت دیدن داریم ونه تصحیح

– اگر از mmc و نصب Snap-in دامین کنترلر استفاده کرده باشیم و مجوز مناسب نیز داشته باشیم امکان تغییر همه پالیسی ها میسر است

– از ابزار rsop.msc برای پیدا کردن منشاء GPO استفاده میکنیم – ابزار rsop را بدون پسوند از طریق cmd نیز میتوان اجرا نمود

– جهت رویت پالیسی های اعمال شده میتوان از دستور gpresult /H GPreport.html استفاده نمود که خروجی وب بیس همراه منشاء پالیسی در اختیار ما میگذارد

gpresult /H name.html → HTML Resultant set of policy

پالیسی ها از طریق لینک بر روی دامین ، سایت یا ou اعمال میشود و بدون لینک ، پالیسی کاربردی ندارد

Domain Controllers ← Link ← Default Domain Controller Policy

Test.local ← Link ← Default Domain Policy

سناریو تستی

– میخواهیم از طرف GPO این امکان را به کامپیوترهای دامین بدهیم که بدون رمز Blanked Pass به دامین وصل شوند

– وقتی Policy Setting را تعیین میدهیم حتی قبل از Ok نمودن تغییرات انجام شده است

Policy Setting ← 1 Not Defined 2 Defined 3 Enabled 4 Disabled

- Enforce password history=0
- Maximum password age=0
- Minimum password age=0
- Minimum password length=0
- Minimum password length audit=Not Defined
- Password must meet complexity requirements=Disabled

GPO Refresh/Update

– بر خلاف Local GP در GPO باید حتما طبق قواعدی Update اعمال بشود

– کلاینتها باید به دامین کنترلر مراجعه کنند و از طریق فولدر sysvol به پالیسی های مشترک دسترسی پیدا نموده و خود را Update کنند

– اساسا پالیسی ها همانند دستورالعمل میباشند و عملا به کلاینت ها دستور میدهند و نه اینکه کار خاصی برای کلاینتها انجام دهند

1 – کلاینتها هنگام بوت هم پالیسی های خود و هم با مراجعه به sysvol پالیسی های دامین را اعمال میکنند → Computer Configuration

2 – کلاینتها با Logon/Logoff به sysvol مراجعه نموده و فقط پالیسی های کاربر را اعمال میکنند → User Configuration

3 – کلاینتها در بازه های زمانی بین ۹۰ الی ۱۲۰ دقیقه به sysvol مراجعه نموده و مجموع تغییرات در پالیسی را اعمال میکند

User Configuration + Computer Configuration → 90"≤90"+(0-30)"≤120"

4 – دامین کنترلر ها هر ۵ دقیقه یکبار تغییرات پالیسی خود را اعمال میکنند User Configuration + Computer Configuration → 5"

5 – برای آپدیت لحظه ای در سمت کلاینتها بر روی هر کلاینت از دستور gpupdate /force استفاده میشود /force = Apply old and modify policies

نکته – gpedit.msc حالت Refresh ندارد و برای دیدن تغییرات باید حتما یکبار برنامه باز و بسته شود

6 – میتوان برای آپدیت لحظه ای از سمت غیر کلاینت برای تعداد زیادی کلاینت از نرم افزارهای 3rd Party استفاده نمود مانند specopsgpupdate

7 – از win2012 به بعد برای آپدیت لحظه ای از راه دور از طریق gpmc.msc قابلیتی به نام Group policy update اضافه شده که بر روی ou کار میکند

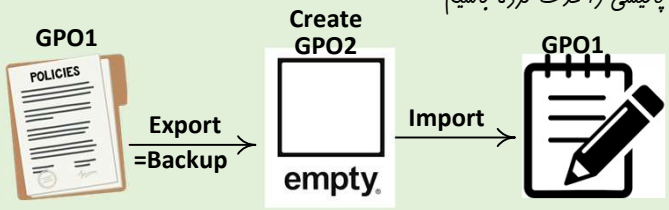
بدین صورت کامپیوترهایی که داخل آن ou قرار دارند Force میشوند تا ۱۰ دقیقه آپدیت شوند

I

Overal Group Policy Management View

- در ابزار gpmc.msc از طریق Group Policy Objects موجود در دامین از پالیسی ها بکاپ میگیریم و با کلیک سمت راست موس در دامین با استفاده از Manage Backups بکاپ ها را مدیریت میکنیم

- فرایند بازیابی از طریق Restore from Backup و با کلیک سمت راست ماوس بر روی پالیسی که قبلا بکاپ گرفته بودیم انجام میشود حتی اگر پالیسی را حذف کرده باشیم



- از طریق Import settings امکان درج یک پالیسی در یک پالیسی جدید وجود دارد ، از این حالت برای تغییر در یک پالیسی و اعمال آن در یک محیط جدید عمدتا استفاده میشود ، نکته اینکه اگر پالیسی بر روی محلی که Import میکنیم وجود داشته باشد پاک میشود و پالیسی جدید جایگزین میشود بدین معنی که حالت Append وجود ندارد

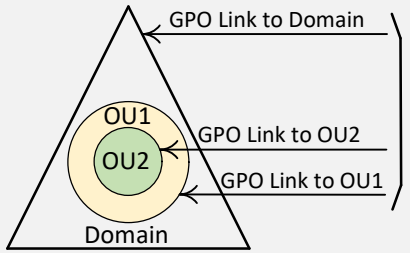
- با استفاده از Import در صورت حذف یک پالیسی میتوان حالت Restore راجهت برگرداندن بکاپ شبیه سازی نمود

Open migration table editor ←

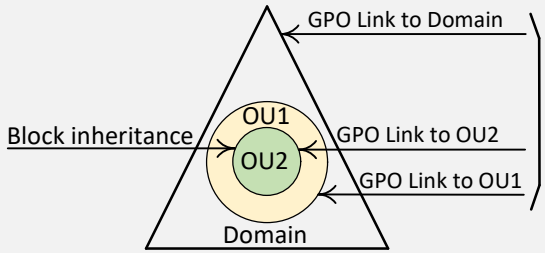
- اگر بخواهیم بطور مثال یک GPO را از یک فارست به فارست جدیدی انتقال دهیم با استفاده از Open migration table editor و انتخاب پالیسی مورد نظر جدولی از تغییراتی که باید قبل از انتقال بر روی پالیسی قبلی اعمال کنیم را بدست می آوریم

Block inheritance

- با استفاده از **Block inheritance** بر روی یک ou ارث بری از پالیسی بالا دست رامتوقف میکنیم ، در این حالت یک علامت تعجب آبی برروی ou ظاهر میشود



All GPO Policies Merged for Clients on OU2



Domain GPO + OU1 GPO Merged for OU1

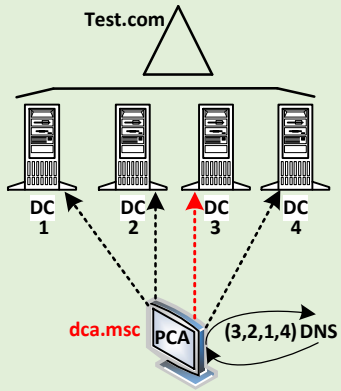
Only GPO Policy on OU2 Applied

- با گرفتن تیک از گزینه **Link Enabled** بر روی پالیسی لینک شده ، بصورت موقت اعمال پالیسی را متوقف می نماییم ، ضمن اینکه رنگ پالیسی لینک شده بصورت کم رنگ در می آید

- با انتخاب اصل یک پالیسی یا پالیسی لینک شده و سپس انتخاب Setting میتوانیم یک گزارش کامل با فرمت HTML از مجموعه پالیسی های اعمال شده بدست آورد

- در قسمت Starter GPOs تعدادی Template وجود دارد که موقع ساخت GPO میتوان از آن استفاده نمود و این امکان مهیا است که الگو سازی شخصی تولید کنیم

- با کلیک سمت راست بر روی یک پالیسی و انتخاب GPO Status میتوانیم Computer Configuration یا User Configuration و یا هر دو را Disable نمائیم



- مجموعه ابزارهایی که با دامین کنترلر کارمیکنند و نیاز به وصل شدن به یکی از آنها را دارند از طریق **DNS** و با ترتیبی که مشخص شده است با دامین کنترلر مربوطه ارتباط برقرار میکنندکه در این مثال دامین کنترلر ۳ بعنوان اولین دامین کنترلر از طریق **DNS** معرفی شده است

- در مورد ابزار gpmc.msc این موضوع کاملا متفاوت است و باید حتما به دامین کنترلر خاصی وصل شود و اگر آن دامین کنترلر در دسترس نباشد این ابزار وصل نمی گردد

I

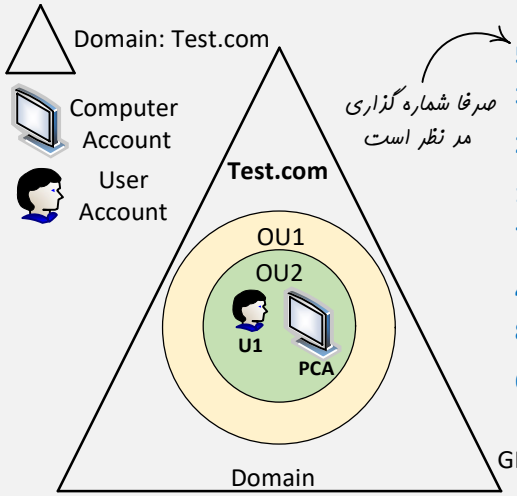
تضاد در پالیسی مشترک

1- داخل یک GPO اولویت Computer Configuration از User Configuration بالاتر است و اگر پالیسی مشترکی بین این دو وجود داشته باشد و عملا تجمیع Merge آن مقدور نباشد User Configuration باطل Override میشود

2- همه GPO های دامین اولویتشان از GPO محلی Local بیشتر است و در صورت بروز تضاد و ایجاد پالیسی مشترک ، پالیسی Local باطل Override میشود

3- GPO های اکتیو دایرکتوری از کمترین اولویت با Site سپس اولویت Domain و بالاترین اولویت OU می باشد

4- فرض OU $\xrightarrow{\text{3\# Link}}$ GPO سه پالیسی به OU لینک داده شده است ازبین این ها در صورت بروز تضاد اونیکه اولویت بالاتر دارد مقدم تر است ، با انتخاب OU و سپس Link Group policy objects ترتیب اولویت ها مشخص میشود



صرفا شماره گزاری مد نظر است

5 GPO
3 GPO
2 GPO
Link
Test.com
Apply C.C
Apply U.C

1 GPO
7 GPO
Link
OU1
Apply C.C
Apply U.C

4 GPO
8 GPO
6 GPO
Link
OU2
Apply C.C
Apply U.C

9 GP Local
Local
GP
Apply C.C
Apply U.C

C.C = Computer Configuration
U.C = User Configuration

- مجموع پالیسی ها با هم تجمیع میشود
- در صورت بروز تضاد اولویت بندی می گردد

Mereged

First Priority	4	OU2 Link Group policy objects Priority
Second Priority	8	
Third Priority	6	
Forth Priority	1	OU1 Link Group policy objects Priority
Fifth Priority	7	
Sixth Priority	5	Test.com Link Group policy objects Priority
Seventh Priority	3	
Eighth Priority	2	
Ninth Priority	9	Local Policy

Override

Override
(4,8,6,1,7,5,3,2,Local Policy)

انقلت در تضاد در پالیسی

1- فرض کنیم Administrator یک GPO5 به دامین لینک داده است و Admin OU2 به OU2 یک GPO4 دیگری لینک داده است و دچار تضاد شده ایم ، قاعدتا در این حالت اولویت با Admin OU2 می باشد، اگر بخواهیم بر اساس سلسله مراتب مدیریتی عمل کنیم و نگذاریم پالیسی GPO 4 برنده اولویت باشد باید پالیسی GPO5 را Enforce نماییم ، یعنی GPO5 به کل مجموعه اعمال میشود و به هیچ وجه Override نمیشود

Override
(5,4,8,6,1,7,3,2,Local Policy)

2- اگر برای OU2 ، Block Inheritance فعال شود فقط پالیسی هایی که به OU2 لینک داده شده به ترتیب اولویت فعال خواهند بود و دست آخر Local Policy

Override
(4,8,6,Local Policy)

3- اگر در مثال شماره ۲ برای GPO5 ، Enforce فعال شده باشد Block Inheritance در نظر گرفته نخواهد شد

Override
(5,4,8,6,Local Policy)

4- اگر ادمین دامین یک GPO را Enforce کند و ادمین پایین دست هم یک GPO دیگری را Enforce کند ، اولویت با ادمین دامین است یعنی تو این شرایط همیشه اولویت با ادمین بالادستی است

II

Preferences Policy

- اگر برای اعمال کانفیگ بر روی کامپیوتر ها یا کاربران GPO موجود باشد از آن استفاده میکنیم در عدم وجود پالیسی به Preferences در gpmc.msc مراجعه میکنیم
- در صورت عدم وجود پالیسی در Preferences باید از ابزارهای 3rd Party و فایلهایی با پسوند .adm Or .admx استفاده کنیم ، بطور مثال اگر بخواهیم برای Office / firefox پالیسی به Policy/ Administrative Templates اضافه کنیم
- Administrative Templates بیشترین پالیسی را در خود جا داده است و فقط در این محل امکان جستجو از طریق Filter Options وجود دارد
- برای پالیسی های Administrative Templates امکان تعریف Comments وجود دارد تا بعدا بر اساس آن امکان جستجو مهیا گردد ضمنا از طریق Administrative Templates امکان اضافه یاحذف نمون فایلهای adm. میسر است
- باید این نوع پسوند برای هر پالیسی بصورت مجزا به هر پالیسی اضافه شود که باعث افزونگی داده در Sysvol میشود که به این حالت اصطلاحا باعث متورم شدن Sysvol میشود (Sysvol Bloat) ← .adm
- زبان اضافه شدن پالیسی های این نوع پسوند تک زبانه است و برای زبان های مختلف باید بصورت مجزا این نوع پسوند اضافه شود
- این نوع پسوند یکبار برای همه پالیسی های مد نظر به Sysvol اضافه میشود میشود و برای مشکل چند زبانه بودن نیز فایلی در کنار این پسوند با پسوند .adml اضافه میگردد ← .admx

I

تغییر محل فایلهای Local Store به Central Store

Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer.

محل قرارگیری فایلهای Local در هردامین کنترلر ← C:\Windows\PolicyDefinitions بصورت پیش فرض دامین کنترلر به این محل برای فایلهای admx. مراجعه میکند ← در اینحالت باید هرadmx.را در تمامی محل های پیش فرض دامین کنترلرها کپی نمائیم

↓

Administrative Templates: Policy definitions (ADMX files) retrieved from the central store.

C:\Windows\PolicyDefinitions → Copy → C:\Windows\SYSVOL\sysvol\test.local\Policies

– برای اینکه دامین کنترلرها به یک محل مشترک برای admx. مراجعه کنند محل پیش فرض را تغییر میدهیم

برای اضافه نمودن فایلهایadmx.به Administrative Templates مجموعه فایلهای admx.و adml.را در زیر شاخه C:\Windows\SYSVOL\sysvol\test.local\Policies\PolicyDefinitions کپی میکنیم

II

Scripts

– در صورتیکه برای انجام کار خاصی پالیسی و admx. وجود نداشت از اسکریپت Command Base یا Powershell از Win7 یا 2008R2 به بالا استفاده میشود(.ps1 & .bat)

Default Domain Policy
- Computer Configuration
  - Policies
    - Windows Setting
      - Scripts (Startup /Shutdown)

Default Domain Policy
- User Configuration
  - Policies
    - Windows Setting
      - Scripts (Log on / Log off)

III

Default Domain Policies

– پیشنهاد مایکروسافت بر این است که تر جیحا برای پالیسی های خاص از دو پالیسی پیش فرض استفاده نشود بدین معنی که باید پالیسیها را دسته بندی کرد و در قالب یک GPO به کار گرفت ، ضمنا این دو پالیسی قابل پاک کردن نیست

GPO → detail → Unique ID

Default domain policy → {31B2F340-016D-11D2-945F-00C04FB984F9}

Default domain Controllers policy → {6AC1786C-016F-11D2-945F-00C04FB984F9}

dcgpofix

– این دستور دو پالیسی پیش فرض را به حالت اولیه برمیگرداند و در صورت عدم وجود آنها را می سازد

– در صورت پاک شدن سهوی Unique ID پالیسیهای پیش فرض باید Container آن را از طریق ابزار ADSI Edit پاک نمود و دستور dcgpofix را اجرا کرد

IV

GPO
- Container → Save → DDP = GPO Name → Location dsa.msc → Test.local/system/Policies
- Template → Save → Sysvol = Unique ID → Location → Sysvol

تشریح نام و محل قرار گیری GPO

Password Policy and Lockout Policy

Password Policies
- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Minimum password length audit
- Store passwords using reversible encryption
- Password must meet complexity requirements

Lockout Policy
- Account lockout duration ← رمز عبور چند بار اشتباه زده شود و سپس
- Account lockout threshold ← اکانت برای چه مدت قفل شود
- Reset account lockout counter after ← شمارنده بعد از چه مدت صفر شود ضمن اینکه هر ورود موفق این کانتر را صفر میکند

– اکانت Administrator هیچ وقت Lock نمیشود

– اصولا در یک سازمان کاربران بر اساس سطح دسترسی به منابعی که دارند دسته بندی میشوند و سپس از طریق Lockout Policy برای آنها محدودیتهای مختلفی اعمال می گردد

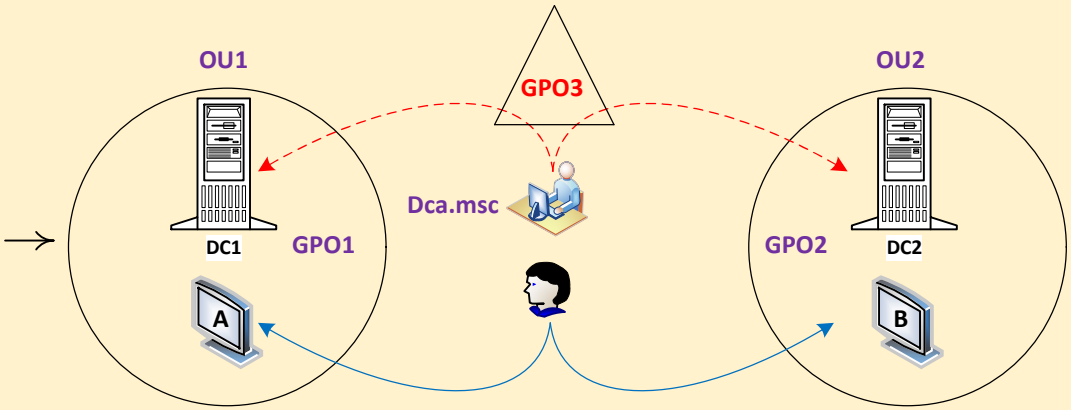
I

اعمال پالیسی بر اساس Computer Configuration جهت Set کردن Password Policy,Lockout Policy

GPO1 Link OU1
Computer Configuration

Lockout Policy: Account lockout duration=10

Password Policy: Minimum password length=3; Password must meet complexity requirements=no



OU2 Link GPO2
Computer Configuration

Account lockout duration=5 — Lockout Policy

Minimum password length=7; Password must meet complexity requirements=yes — Password Policy

- در ارتباط با کاربری که میخواهد به DC وصل شود وضعیت به گونه ای است که DNS او را به سمت DC1 یا DC2 هرایت خواهد کرد نکته مهم اینست که بعنوان یک قاعده DC1 یا DC2 از پالیسی OU خود تبعیت نمیکنند بلکه همواره از GPO هایی که به دامین نسبت داده شده اند پالیسی خود را دریافت میکنند و در مثال بالا DC1 و DC2 پالیسی های خود را با GPO3 هماهنگ خواهند نمود و پالیسی های OU ها برای دامین کنترلر ها Override خواهد شد
- با توجه به Password Policy و Lockout Policy وضعیت کامپیوترهای A و B بدین گونه خواهد بود که از پالیسی های OU مرتبط با خود تبعیت خواهند کرد

II

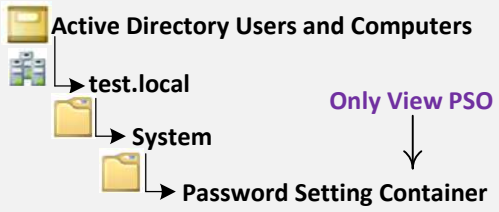
اعمال Password Policy,Lockout Policy بر اساس تفکیک کاربران PSO

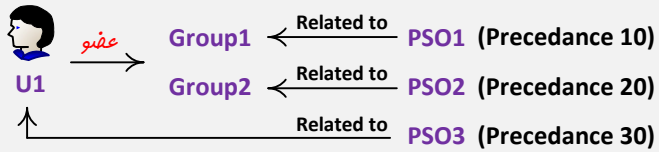
- همواره Attribute های User Account مقدم بر Policy هستند مثلا وقتی در User Account مشخص میکنیم پسورد هیچوقت منقضی نشود مقدم بر Policy است پس بر اساس توسعه Schema و اضافه شدن Attribute توسط نرم افزارهای 3rd party امکان تفکیک Password و Lockout در ویندوزهای قبل از 2008R2 میسر نبود

PSO (Password Settings Object)

PSO Related to Group or User

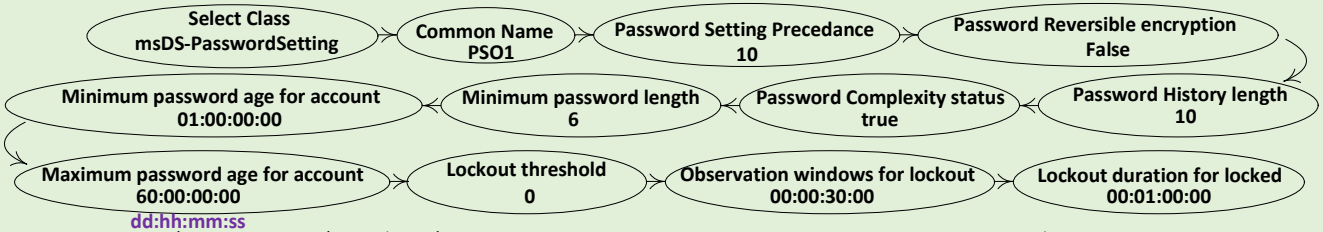
- بر اساس PSO ملزومات Password و Lockout مشخص شده و به User نسبت داده میشود
- اولویت PSO از Policy بالاتر است چون شبیه Attribute های کاربر می ماند و در صورت نبود یک PSO برای یک کاربر اولویت با پالیسی پیش فرض دامین خواهد بود
- یک روش ایده آل بدین شکل است که Password Policy و Lockout Policy را از طریق Default Domain Policy به دامین نسبت میدهیم و سپس گروه هایی برای تفکیک Password و Lockout بر اساس PSO ایجاد می کنیم





کاربر U1 تحت تاثیر PSO3 خواهد بود و در صورت عدم وجود PSO3 تحت تاثیر PSO1

1 برای ساخت PSO باید به کانتینر (Password Setting Container) PSC مراجعه کرد این مهم از طریق ADSI Edit در بخش DDP در دسترس است



-پس از ساخت PSO و گرفتن Properties از قسمت msDS-PSOAppliesTo برای مشخص کردن گروه و کاربران استفاده میکنیم

2 - روش دوم و بسیار راحت تر برای ساخت PSO استفاده از ابزار dsac می باشد
- با استفاده از فرمان زیر میتوان متوجه شد که آیا کاربر administrator تحت تاثیر PSO هست یا خیر و اگر هست کدام PSO

```
dsget user cn=administrator,cn=users,dc=test,dc=local -effectivepso
```

I

User Account ادامه

- هنگام تعریف Logon to برای کاربران باید دقت داشته باشیم به غیر از دستگاه کاربر مربوطه برخی کامپیوترهای سازمان ازقبیل Sharepoint,exchange,portal,Automation,..... نیز باید به کامپیوترها اضافه شوند
- Best Practice برای Lockout policy درج عدد ۱۰ برای هر سه Object مرتبط میباشد — Reset account lockout counter after=10 — Account lockout threshold=10 — Account lockout duration=10
- اگر Account lockout duration=0 باشد اکانت Lock می ماند تا ادمین آنرا Unlock نماید — اکانت administrator به هیچ عنوان Lock,delete,restrict,expire نمیشود
- Lockout policy در نگاه اول باعث افزایش امنیت میشود ولی این امکان وجود دارد که باعث کاهش امنیت نیز بشود بدین معنی که اگر کسی نام کاربری افراد مهم سازمان را به طریقی بدست آورد و با وارد کردن اشتباه رمز آن کاربر به دفعاتی که در policy تصریح شده است باعث قفل شدن اکانت شود که برای حل مدودی این مشکل از Logon to استفاده میشود ولی همچنان از طریق OWA مثلا exchange که به Logon to اضافه شده امکان خطر وجود دارد

II

User Profie

1 Local User Profile

- User profile شامل Data و Config اختصاصی یک کاربر میشود
- بار اولی که یک کاربر به سیستم وصل میشود محتویات C:\Users\Default در C:\Users\%userprofile% کپی میشود
- C:\Users\Public بخشی از User profile همه کاربران است — User profile = C:\Users\%userprofile% + C:\Users\Public
- بنابراین دسکتاپ یک کاربر برابر است با جمع دسکتاپ خودش به انضمام دسکتاپ موجود در C:\Users\Public\Desktop

%userprofile% → Current User profile
%username% → username
%programfiles% → Program files
%windir% → Windows folder
• → Current User profile
•• → All User profiles
•• → All User profiles

regedit → HKEY_CURRENT_USER → Current user config

2 Temprory profile

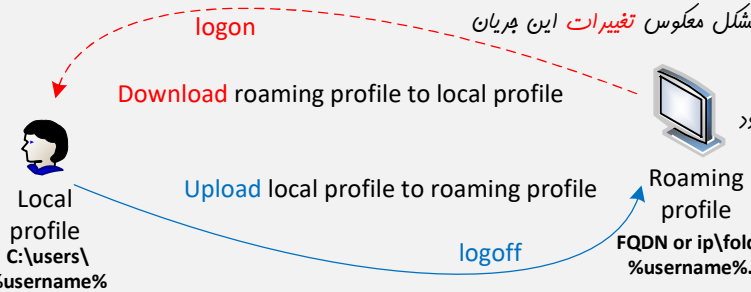
- اگر پروفایل کاربری که قبلا Logon کرده پاک شود وقتی مجددا Logon کند پروفایلش به حالت TEMP در می آید که اصطلاحا Temprory profile گفته میشود و تا موقعی که تمام اثرات پروفایل در رجیستری پاک نشود این وضعیت ادامه دارد
- کاربر Guest حالت Temprory profile دارد

مشکلات Local User Profile

- Local User profile در پارتیشن C: ساخته میشود و باعث افزایش حجم این درایو می گردد و میتواند باعث کندی ویندوز و عملکرد صحیح آن شود
- با پر شدن درایو C: و یا خرابی هارد عملا دیتای مهم کاربر که در پروفایلش ذخیره شده از دست می رود
- در صورت لاگین کاربر به سیستمهای مختلف امکان حفظ اطلاعات کاربر در پروفایلش میسر نخواهد بود
- امکان Backup گرفتن از Local User profile به سادگی میسر نمی باشد
- دچار عدم یکسان بودن پروفایلها در صورت لاگین کاربر در سیستم های مختلف خواهیم بود
- برای بهبود مشکل پروفایل کاربران میتوان محل ذخیره آن را به درایوی دیگر در همان سیستم و یا فایل سرور تغییر داد (Move Desktop profile location)

3 Roaming User Profile

- بدین معنی که با چرخش کاربر پای دستگاه های مختلف و لاگین به دستگاهها پروفایل آن از یک محل متمرکز و ثابت که عموما یک فولدر به اشتراک گذاشته شده فایل سرور میباشد فراخوانده شود
- برای استفاده از Roaming profile باید در قسمت Profile path پروفایل کاربران در AD users and computers آدرس محل ثابت را درج کنیم → Profile path = FQDN or ip\folder\%username%
- پس از تعریف Roaming profile و لاگین کاربر مربوطه به کامپیوتر خودش در سمتی که برای پروفایل کاربران در نظر گرفته شده است فولدری با نام کاربر و پسوند .v6 ایجاد خواهد شد FQDN or ip\folder\%username%.v6
- محل پروفایل Local در کامپیوتر کاربر همچنان حفظ میشود ، هنگام logon کاربر پروفایل Roaming به سمت پروفایل Local دانلود شده و موقع logoff بشکل معکوس تغییرات این جریان



- اگر دستگاه بدون logoff به دلیلی ریست شود مسلما مجموعه تغییرات به Roaming profile انتقال داده نمیشود → مشکلات
- در شروع و پایان کار اداری جریان بالای انتقال داده برای sync شدن وجود خواهد داشت و اگر پروفایلی سنگین باشد زمان زیادی برای هر کاربر تلف میشود

4 Mandatory User Profile

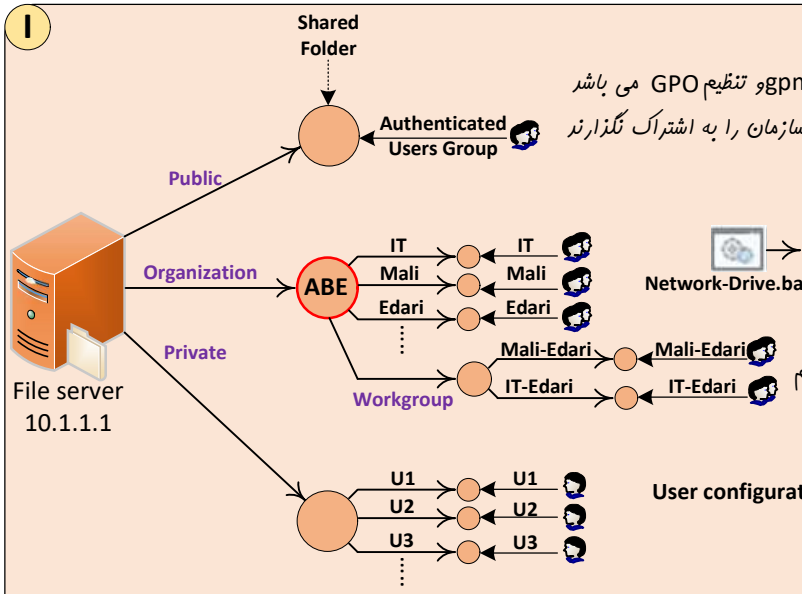
- یعنی به کاربر پروفایلی اختصاص دهیم تا کاربر نتواند در آن تغییری ایجاد کند و اگر در موقع logon امکان استفاده از پروفایل اجباری مقرور نباشد به حالت پیش فرض Local بر میگردد از این نوع پروفایل عمدتا در کیوسک ها Kiosk استفاده میشود در واقع تغییرات Temprory هستند

5 Super Mandatory User Profile

- همانند پروفایل اجباری میباشد با این شرط که اگر در موقع logon استفاده از پرو فایل اجباری مقرور نباشد ، کار بر نمیتواند به دستگاه لاگین نماید

I

User Profile (logon Script) - Map Drive



- استفاده از **Logon scripts** در پروفایل کاربران برابر با استفاده از **User configuration/windows settings/scripts/log on** از طریق gpmc.msc و تنظیم GPO می باشد
- فولدر Public برای استفاده عمومی در سازمان در نظر گرفته میشود و طبق زمانبندی خاصی پاک میشود و کاربران سازمان باید توجیه شوند که اطلاعات مهم سازمان را به اشتراک نگذارند
- ابتدا Share Permission و NTFS Permission را جهت دسترسی صحیح کاربران به منابع اختصاص داده شده تنظیم می نمائیم

1. Network-Drive.bat **Copy** → C:\Windows\SYSVOL\sysvol\test.local\scripts
   Logon scripts = Network-Drive.bat
2. راه حل دوم اسکریپت از طریق GPO میباشد **User configuration/windows settings/scripts/log on**

- برای اینکه کاربران فقط فولدرهایی که برایشان به اشتراک گذاشته شده را ببینند ازقابلیت **ABE** استفاده میکنیم و برای فعال کردن آن بدین شکل عمل میکنیم

Servermanager → **File and storage services** → **Shares** **Properties from Shared folders** → **Enable access-based enumeration(ABE)**

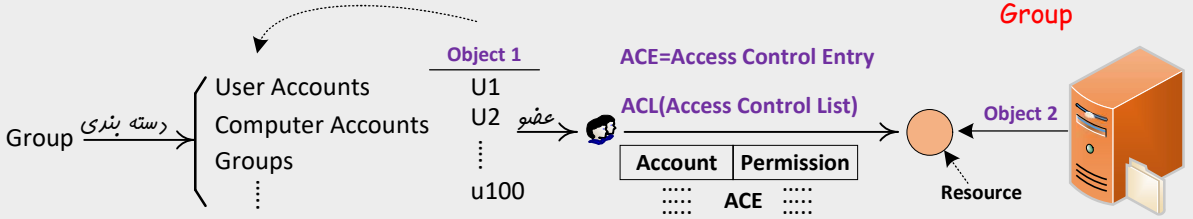
Drive Maps

- برای MAP کردن و تخصیص لیبل به فولدرهای MAP شده از gpmc.msc نیز میتوان استفاده نمود **User configuration/preferences/windows setting/Drive Maps**
- از پالیسی Drive Maps میتوان همانند اسکریپت نوشته شده بالا Create,Delete,update,Replace را میتوان اعمال نمود
- درصورت عدم وجود یک درایو ازقبل Update با Create عملکرد یکسانی دارند

Home Folder

- از قسمت User profile و Home folder امکان نسبت دادن یک درایو Private بصورت Local یاتحت شبکه برای هر کاربر بصورت مجزا میسر است و نکته مهم اینکه نیاز به تعیین سطح دسترسی نیز نیست و کاربر به فولدر شخصی خود دسترسی پیدا میکند هرچند این مهم از طریق اسکریپت نویسی نیز امکان پذیر است

II



Group

- به Object ی که میخواهیم نسبت به آن دسترسی برهیم **Resource** گفته میشود
- به Object ی که میخواهیم به آن دسترسی برهیم **Account** گفته میشود
- به Object1 دسترسی میدهیم نسبت به Object2
- در سمت **Resource** جدول **ACL** وجود دارد که مشخص میکند چه اکانتهایی چه دسترسی هایی دارند
- با یکبار ساخت Group امکان استفاده متعدد آن فراهم میشود و خاصیت ماجولار به آن می دهد
- با ساخت گروه و نسبت دادن آن به منابع وابستگی مراجعه مستقیم به منابع جهت افزایش دسترسی کاربران به منابع منتفی میشود
- با ساخت گروه امکان اطلاع رسانی بصورت گروهی فراهم میگردد
- کنترل سطح دسترسی و سریعتر و ساده شدن سطوح دسترسی

Local Groups

1. **Permission** – نسبت به منابع **Resource** استفاده میشود مثلا اگر کسی قرار است یک فایل را بخواند یا کپی کند باید نسبت به آن فایل Permission داشته باشد
2. **Rights** – نسبت به سیستم **System** استفاده میشود مثلا اگر کابر بخواهد سیستم را ریستارت کند یا زمان سیستم را عوض کند باید نسبت به سیستم Right داشته باشد
   Location → Computer configuration/windows settings/security setting/local policy,user right assignment

Built-in Groups

1. **System** – اعضاء این گروه را سیستم تعیین میکند و ادمین فقط قدرت **Right** دارد
   Everyone , Authenticated User , Anonymous Logon,.....
2. **Non-System** – اعضاء این گروه را سیستم تعیین میکند و ادمین قدرت **Right** و **Permission** دارد
   - هنگام اضافه کردن گروه در ACL اگر گروهی قسمت In folder آن خالی باشد نوع گروه **Built in system** است
   (Built-in system = security principals)

Non-Builtin Groups

- اعضاء این گروه راکاربر می سازد و قدرت **Right** و **Permission** دارد
  Tools : lusrmgr.msc / compmgmt.msc / ...

I

AD Groups

- گروه Power Users در LSD موجود است ولی در اکتیو دایرکتوری موجود نیست
- گروه در AD داخل DDP ذخیره میشود و در هنگام ساخت DC گروه های مرتبط با AD ساخته میشود
- کانتینر **Builtin** در AD users and computers اکثرا شامل گروه های ویندوزی میشوندو در هنگام نصب ویندوز ساخته میشوند و کانتینر **Users** منحصرا شامل گروههای AD میشوند که با **Promote** کردن **DC** ساخته شده اند

AD Groups

Type

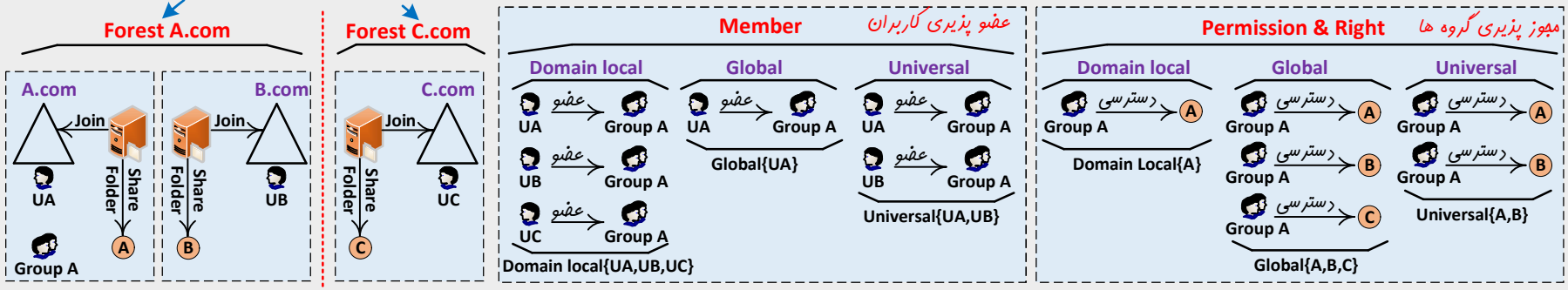
1. **Security**
   - Type گروه از Security به Distribution قابل عوض کردن میباشد و بالعکس
   - به این گروه نسبت به منابع میتوان **Right** و **Permission** داد و همچنین میتواند آدرس ایمیل داشته باشد بدین معنی اگر ایمیلی به این نوع گروه فرستاده شود به ایمیل باکس تمام اعضاء گروه فرستاده خواهد شد
   - این نوع گروه صرفا ایمیل آدرس دارد و چیزی به نام ایمیل باکس ندارد بنابراین اصطلاحا کاربران را **Mailbox Enable** میکنیم و خود گروه را **Mail Enable**
2. **Distribution**
   - به این گروه نسبت به منابع نمیتوان **Right** و **Permission** داد و فقط میتواند آدرس ایمیل داشته باشد و صرفا برای اطلاع رسانی استفاده میشود و نه مدیریت سطوح دسترسی

- موقعی که AD برای کاربران Ticket صادر میکند علاوه بر SID کاربران SID تمام گروه های Security که کاربر عضو آن هست نیز اضافه میشود ، این موضوع در صورت حجم بالای گروه های Security که کاربر عضو آن میباشد میتواند منجر به **Ticket Bloat** شود بنابراین اگر نیاز به سطوح دسترسی نیست بهتر است از گروه های Distribution استفاده شود که به تبع آن SID گروه درموقع صدور Ticket برای کاربران منظور نگردد
- گروه های Distribution در Exchange Server کاربرد زیادی دارند
- اگر گروه Security را به Distribution تغییر دهیم مجموعه Permission & Right از دست خواهد رفت

Scope

1. **Domain local**
2. **Global**
3. **Universal**

Permission & Right مجوز پذیری گروه ها

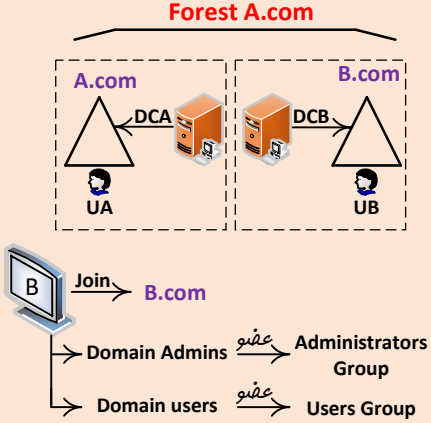


Member عضو پذیری کاربران

II

Nested Groups

میخواهیم UA بشود Administrator دامین B.com



- اسم Scope مترادف مجموعه مجوز پذیری کاربران آن می باشد
- برخی Scope ها قابلیت تبدیل پذیری نسبت به هم دیگر دارند ولی باید توجه داشت که در این تغییرات ممکن است محدوده عضو پذیری و مجوز پذیری آن تغییر کند که قبل از انجام این تبدیل باید انجام گردد
- میخواهیم UA را عضو Domain Admin دامین B.com نمائیم اما مشکل اینجاست که گروه مورد اشاره دارای Scope ، Global میباشد و گروه های Built-in را نمیتوان تغییر داد **Local**
- با توجه به اینکه Scope گروه **Administrators** ، Domain local است باعضو نمودن در این گروه کاربر ادمین DC های دامین B.com خواهد شد و نه کل دامین پس این مشکل بطور کامل حل نخواهد شد مگر اینکه این کاربر را عضو تمامی کامپیوترهای دامین B.com نمائیم که به این سادگی ها عملی نیست و ضمنا نمیتوان Nested Groups ساخت و یک گروه Domain local را که ساخته ایم عضو Domain Admin دامین B.com کنیم
- نهایتا از طریق **Restricted Groups Policy** باید کاربر UA را عضو گروه Administrators تمامی اعضاء دامین B.com پیاده سازی نمائیم

- G1 Global عضو G2 Universal ✓
- G1 Domain local عضو G2 Universal ✗
- G1 Universal عضو G2 Global ✗
- G2 G1
- G1 Global عضو G2 Global ✓
- G1 Global تبدیل G1 Domain Local ✗
  - نمیتوانیم این تبدیل را انجام دهیم
- G1 Domain Local تبدیل G1 Global ✓
- محدوده عضو پذیری و مجوز پذیری تغییر خواهد کرد

- G1 عضو G2
  - در اینحالت G1 مجوزهایش تغییر میکند چون مجوز های G2 را به ارث می برد و G2 اعضایش تغییر میکند چون اعضاء G1 به آن اضافه میشود
- G1 Domain local عضو G2 Global ✗
  - در اینحالت G1 نمیتوانند مجوزهای G2 را به ارث ببرد پس ممکن نیست
- G1 Global عضو G2 Domain local ✓
  - در اینحالت G1 میتوانند مجوزهای G2 را به ارث ببرد پس ممکن است
- G1 Universal عضو G2 Domain local ✓

I

Restricted Groups Policy

Default Domain Policy
Computer Configuration
Policies
Windows Setting
Security Setting
Restricted Groups

1 Restricted Groups — Add Groups: Administrators → Member of this groups (1) — Add Groups: Helpdesk

- این گروه کاربرد دوگانه دارد
- کاربران و یا گروه هایی که باید عضو گروه Administrators باشند را مشخص میکنیم ، در این حالت فقط Helpdesk عضو گروه Administrators خواهد بود البته بصورت پیش فرض کاربر Administrator را نیز اضافه میکند

2 Restricted Groups — Add Groups: Helpdesk → This group is member of (2) — Add Groups: Administrators

- کاربران و یا گروه های فعلی گروه Administrators حذف نمیشود بلکه گروه Helpdesk به گروه Administrators اضافه میشود

II

Run as administrator

- وقتی یک کاربر میسازیم بشکل پیش فرض عضو گروه **Domain Users** میشود
- با حالت Switch user این امکان وجود دارد که با کاربر سطح بالاتری به دستگاه Logon کنیم و بعد از اتمام کار مجددا Logoff نمائیم حسن کار اینست که تمام برنامه های باز کاربر بسته نخواهد شد
- برای اینکه یک برنامه را با مجوز Administrator استفاده کنیم روش **UAC(User Account Control)** بدین شکل است که بر روی فایل کلیک سمت راست کرده و Run as Administrator را اجرا میکنیم (1)
- برای اینکه یک برنامه را با مجوز Administrator استفاده کنیم روش گرافیکی آن بدین شکل است که کلید Shift را نگه داشته و همزمان بر روی فایل کلیک سمت راست کرده و Run as different user را اجرا میکنیم (2)
- روش سوم از طریق CMD است — مثال: runas /user:administrator notepad → Application — (3) runas /user:test\administrator "mmc gpedit.msc"
- میتوان CMD را بصورت runas باز کنیم /user:.\administrator cmd سپس در CMD که اولویت ادمین دارد هر دستوری را تایپ نمائیم ضمنا میتوانیم در قسمت Run نام دستور را تایپ نموده و سپس Ctrl+shift+Enter بزنیم
- در اینحالت یکبار که رمز ادمین را درج نمائیم برای دفعات آتی فایل اجرایی بدون درخواست رمز اجرا خواهد شد — runas/ savecred/ user:administrator" mmc gpedit.msc" → Save → A.bat
- این رمز در کنترل پنل Credential manager/windows manager ذخیره میشود که میتوانیم آن را پاک کنیم — از ساخت بچ فایل میتوان برای اجرای برنامه های خاص کاربران با اولویت ادمین استفاده نمود و کاربر را ادمین Local نکرد

III

ALP,AGLP,AGP,AGDLP,AGUP,AGUDLP

A=Account,L=Local group,G=Global group
DL=Domain local Group,U=Universal,P=Permission

- کاربرد گروه **Global** جهت دسته بندی **User Account** و **Computer Account** می باشد و برای دسته بندی گروه استفاده نمیشود بصورت پیش فرض گروه عضو Global میشود
- از **Domain local** اصولا برای دسته بندی گروه ها استفاده میشود
- AGP یک استراتژی در بهره برداری از گروه هاست که بصورت پیش فرض از آن استفاده میکنیم بدین معنی یوزر و کامپیوتر اکانت ها را عضو گروه گلوبال میکنیم و سپس برای آن مجوز تعیین میکنیم

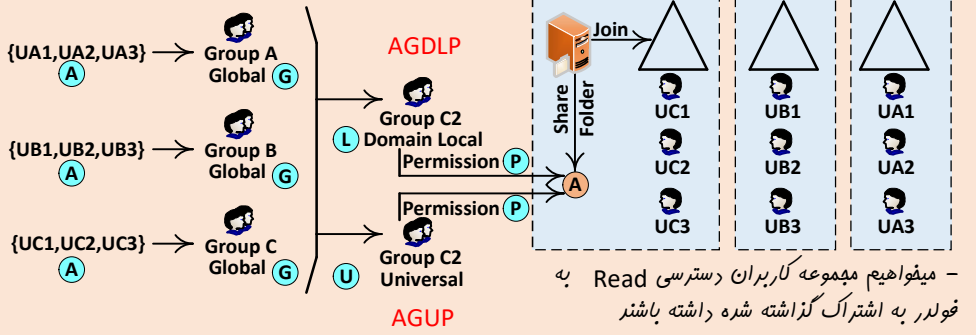
Group Strategy

A L P ---> Accounts member Local + Permission (Workgroup Network)
A G L P ---> Accounts member Global and Global Member Builtin Local+Permission
A G P --- > Accounts member Global +Permission
A G DL P ---> Accounts member Global and Global member Domain local and member of universal +Permission
A G U P --- > Account member Global and Global member Universal + Permission
A G U DL P --- > Accounts ,Global,Universal,Domain local + Permission

AGLP

HelpdesK Global —عضو→ Administrators Local Built-in
Domain Admins Global —عضو→ Administrators Local Built-in
Domain Users Global —عضو→ Domain Users Local Built-in

- بصورت پیش فرض وقتی گروه میسازیم از روش AGP استفاده میشود
- اگر نیاز نیست ترجیحا گروه AGDLP میسازیم چون AGUP باعث ایجاد Load بر روی GC Server ها میشود



- میخواهیم مجموعه کاربران دسترسی Read به فولدر به اشتراک گذاشته شده داشته باشند

I

G=Global
DL=Domain Local
UNI=Universal

روش تشخیص عضویت در گروه ها

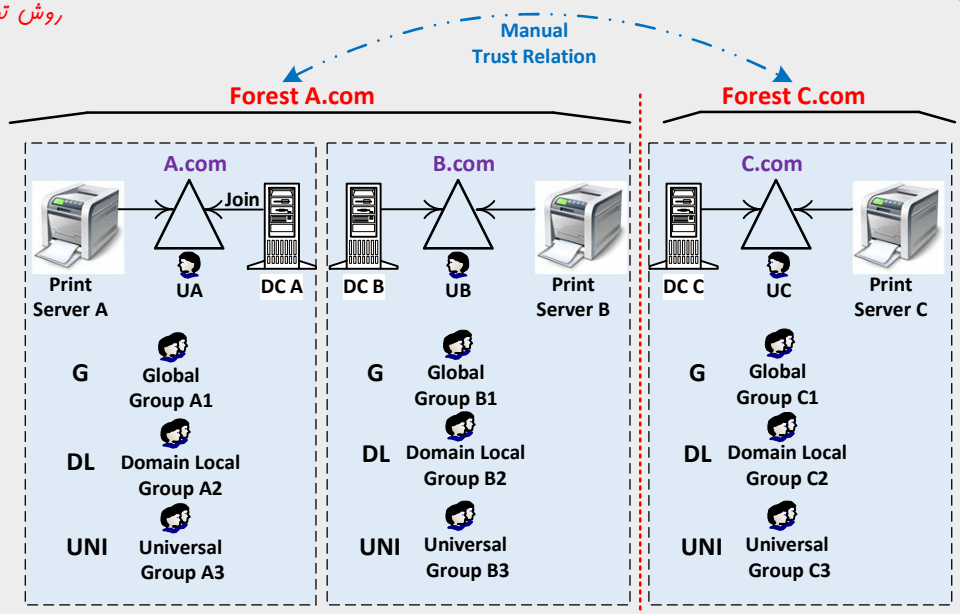
کاربرUAامکان عضویت در گروه های زیر رادارد

UA —عضو→ {G A1,DL A2,UNI A3,DL B2,UNI B3,DL C3}

– کاربرUAبواسطه عضویت در گروه هایی که اشاره شد امکان ارسال پرینت به هر سه پرینت سرور دارد چون گروه هایی که عضو آنها میباشد میتوانند عضو پرینت سرور باشد

– وقتی کاربرUAبهDC Aوصل میشود در تیکتی که برای او ساخته میشودSIDکاربر و SID مجموعه گروه های Security که عضو آنها است درج میشود حال DC A در DDP فود آدرس Global Securityکاربر UAرا دارد ولی گروه های Universal Securityرا باید ازGC Serverاستعلام نماید و دست آخر برای تشخیص گروه های Domain Local Security باید به Infra structure(FSMO) Master Role مراجعه کند که بعدا این موضوع در درس مطرح فواهد شد

– ساختن گروه های Universal Security باعث بالا رفتن Load ، GC Server ها فواهد شد



II

Group Naming

Global Group ← – باید بگونه ای این نوع گروه نام گزاری شود که مشخص شود چه کسانی عضو آن هستند
Sales,Marketing,executives,.....

Based on Members

Domain Local Group ← – باید بگونه ای این نوع گروه نام گزاری شود که مشخص شود چه دسترسی هایی دارد
Sales folder read,.....

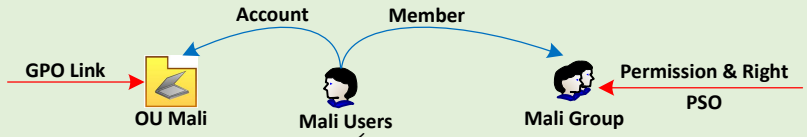
Based on Permission & Right

Group Scope and Members

GROUP SCOPE	MEMBERS FROM THE SAME DOMAIN	MEMBERS FROM ANOTHER DOMAIN IN THE SAME FOREST	MEMBERS FROM A TRUSTED EXTERNAL DOMAIN
Local	Users Computers Global groups Universal groups Domain local groups Local users defined on the same computer as the local group	Users Computers Global groups Universal groups	Users Computers Global groups
Domain Local	Users Computers Global groups Universal groups Domain local groups	Users Computers Global groups Universal groups	Users Computers Global groups
Universal	Users Computers Global groups Universal groups	Users Computers Global groups Universal groups	N/A
Global	Users Computers Global groups	N/A	N/A

III

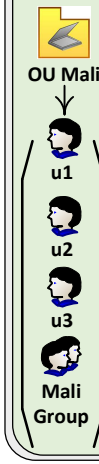
Shadow Group



– به OU نمیتوان مجوز دسترسی Permission & Right داد به این علت که OU ، SID ندارد و ضمنا PSOرا نیز نمیتوان به OUنسبت داد

– اگرOUبه نام مالی داشته باشیم میتوانیم اعضاء آن OUرا اصطلاحا بهShadow Group نسبت دهیم

– اگر کاربر فرضا ار مالی به اداری انتقال یابد هم گروه و هم OUآن باید به اداری انتقال یابد این کار را میتوان از طریق نوشتن یک بچ فایل انجام داد بدین صورت که فقط کاربران را درOUها جا به جا کنیم و بصورت اتوماتیک کاربران گروه های مرتبط جابه جا شوند



shadowgroup.bat

```
dsquery user ou=mali,dc=test,dc=local | dsmod group cn=mali,ou=mali,dc=test,dc=local -chmbr
```

"CN=u1,ou=mali,dc=test,dc=local"
"CN=u2,ou=mali,dc=test,dc=local"
"CN=u3,ou=mali,dc=test,dc=local"

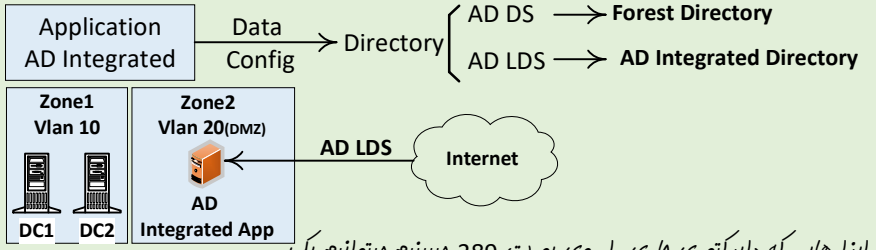
dsmod succeeded:cn=mali,ou=mali,dc=test,dc=local

– بعد از انجام این دستور مجموع کاربران OU Mali صرفا عضو گروه Mali فواهند بود و کاربران اضافی از گروه Mali حذف فواهند شد

– به بچ فایل الباقی OU ها را اضافه نموده و سپس در DC یک Task Scheduler اضافه میکنیم تا در زمان های مشخصی بروز شود

I — Snapshot

- چون AD یک اپلیکیشن Statefull می باشد امکان Restore کردن داده به آن معنی که در Snapshot ماشین های مجازی وجود دارد امکان پذیر نیست به این نکته باید توجه داشت که وقتی تغییری در AD یک DC ایجاد میکنیم آن تغییرات به الباقی DC ها Replicate میشود و وقتی آن DC را Restore میکنیم چون زمان آن عقب تر از الباقی DC ها میباشد مجموعه DC ها با زمان جدید Sync میشوند نهایتا به این موضوع باید توجه داشته باشیم که AD شامل تغییراتی میشود که ما در آن دخیل نیستیم که این برگرفته از Statefull بودن این اپلیکیشن است
- از اپلیکیشن های AD integrated نیز نمیتوان Snapshot گرفت چون تغییراتش در AD ثبت میشود و وابستگی شدیدی به آن دارد
- بنابراین Snapshot گرفتن از AD به این درد میخورد که ما میتوانیم متوجه شویم از زمان Snapshot گرفتن تا الان چه تغییراتی در AD بوجود آمده است و جنبه Documentation دارد ، به نوعی از دایرکتوری عکس میگیریم
- به کمک AD LDS(ADAM) میتوان هر تعداد Directory که بخواهیم بسازیم که Forest Directory نیست ، یعنی ریشه متمرکز ندارد و برای اپلیکیشن های AD integrated که این نوع نیاز را دارد ساخته میشود




```
C:\Windows\system32>ntdsutil
ntdsutil: snapshot
snapshot: ?
?                       - Show this help information
Activate Instance %s    - Set "NTDS" or a specific AD LDS instance as the active instance.
Create                  - Create a snapshot
Delete %s               - Delete snapshot with index or guid %s. Specify * to delete all snapshots
Help                    - Show this help information
List All                - List snapshots
List Mounted            - List mounted snapshots
Mount %s                - Mount snapshot with index or guid %s
Quit                    - Return to the prior menu
Unmount %s              - Unmount snapshot with index or guid %s. Specify * to unmount all mounted snapshots

snapshot:Activate Instance ntds
```

- با استفاده از همان ابزارهایی که دایرکتوری جاری را روی پورت 389 میبینیم میتوانیم یک دایرکتوری که قبلا از آن Snapshot گرفته ایم را ابتدا Mount کنیم و سپس با استفاده از ابزار دیگری بنام dsmain با پورت دلخواه ، نام Mount رابا ذکر محل Ntds.dit مشخص نموده و بعد از طریق Dsa.msc و Change Domain Controller آن را رویت میکنیم

بعنوان نمونه ⟵ `dsmain -dbpath c:\SNAP_202112081655_VOLUMEc$\windows\NTDS\ntds.dit ldapport 50000`

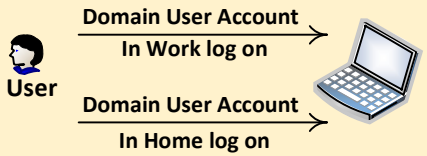
II — Log on Cache

Max Password age Default user account=42 day

Max Password age Default Computer account=30 day

Location ⟶ Computer configuration/windows settings/security setting/local policy /security options/inactive login number of previous logons

- وقتی کاربر Log on to DC میکند پروفایل او بر روی دیسک Cache میشود و او در منزل نیز میتواند با همان نام کاربری و رمز عبور در نبود دامین کنترلر به کار خود ادامه دهد و نیازی به Local User Account نیست
- اگر User Account کاربر Disable شود ، کاربر باقطع کردن کابل شبکه و شبیه سازی حالت منزل میتواند به شبکه وصل شود و از پروفایل خود استفاده کند، نکته اینجاست که از طریق پالیسی که Log on آخر کاربر ذخیره میشود که میتوان آن را به صفر تغییر داد ، دراین صورت کاربر فقط از طریق اتصال به دامین کنترلر میتواند به شبکه و پروفایل خود دسترسی داشته باشد

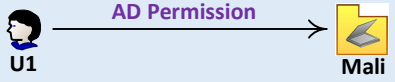


- میتوانیم پالیسی ذکر شده بالا را تغییر ندهیم و عدم اتصال کابل شبکه به کامپیوتر را یک Action تعریف کنیم و به آن Restart یا Shutdown را نسبت دهیم ، یعنی فقط با اتصال کابل شبکه و وجود دامین کنترلر بتواند وصل شود

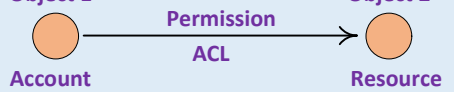
III — OU (AD Permission)

A

- برای مباحث Hardening میتوان به سایت https://www.cisecurity.org مراجعه نمود
- پیاده سازی چارت سازمانی توسط OU — **Organization Unit** ⟵ Create
- گروه هایی که به هیچ کدام از واحد های سازمانی تعلق ندارند یا بین چند واحد سازمانی مختلف مشترک هستند — **Groups** ⟵ Create — **Servers** ⟵ Create



- استفاده مستقیم از AD Permission بسیار سخت است چون تعداد موجودیهای دسترسی بسیار زیاد است و ضمنا تعداد زیادی از مجوز ها مفهوم نیستند ، پس استفاده مستقیم بدین شکل پیچیده و سخت است



- میخواهیم کاربر U1 فقط مدیریت User Account های مالی را داشته باشد؟

B

- بعلت پیچیدگی زیاد AD Permission برای منابع خاص مانند OU از Delegate Control Wizard استفاده میشود

Dsa.msc → Mali → Delegate Control → Add U1 → Cheked create,delete and manage user accounts

- با اینکار بصورت اتوماتیک Special permission ها برای کاربر تنظیم میگردد
- چه کسانی مجوز تغییر رمز Administrator را دارند؟
- اگر به Administrator security tab نگاه کنیم گروه Everyone امکان تغییر رمز را دارد ولی این شرط لازم است و کافی نیست ولی چون کاربران رمز فعلی را ندارند در نتیجه نمیتوانند رمز را عوض کنند پس گاهی اوقات به صرف داشتن مجوز، امکان انجام یک موضوعی میسر نیست
- میخواهیم یک OU را از دید یک کاربر مخفی کنیم؟

Dsa.msc → OU → Permission → Security Tab → Deny All Permission

Create Container

- با استفاده از ADSI Edit و انتخاب Container Object Class امکان ساخت Container در DDP وجود دارد

I — Computer Account

Use for Join to domain

- Sysdm.cpl → System Properties
- Cmd → Netdom join
- ncpa.cpl → Network Connection

redircmp ← هنگام Join کامپیوتر به دامین – Computer Account در محل جدید ذکر شده ذخیره میشود → **Redircmp ou=comp,dc=test.dc=local** → **Net computer \\com1 /add**

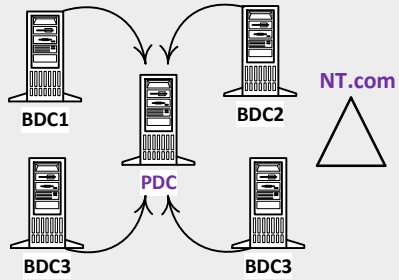
redirusr ← هنگام ساخت User Account در دامین در محل ذکر شده ذخیره میشود → **Redirusr ou=user,dc=test.dc=local** → **Net User \\u1 /add**

- امکان rename کردن Computer Account بصورت مستقیم مقدور نمی باشد
- امکان تغییر نام کامپیوتری که join به دامین است وجود ندارد مگر اینکه همزمان Computer Account آن در AD نیز تغییر کند
- **prestage** ← یعنی برای یک کامپیوتری در AD پیشاپیش Computer Account بسازیم تا در آینده بر اساس گروه یا کاربر دلخواهی که وارد میکنیم امکان join کردن آن به دامین مهیا شود از این روش برای ایجاد Server Cluster نیز استفاده میشود از کلاستر برای ایجاد یک سرور مجازی با یک نام و IP مشخص که توسط زنجیره ای از سرورها برای تامین یک سرویس خاص در نظر گرفته شده استفاده میشود
- یک نکته مهم اینکه نام Computer Account در محیط کامندی CMD به یک $ ختم میشود

II — FSMO

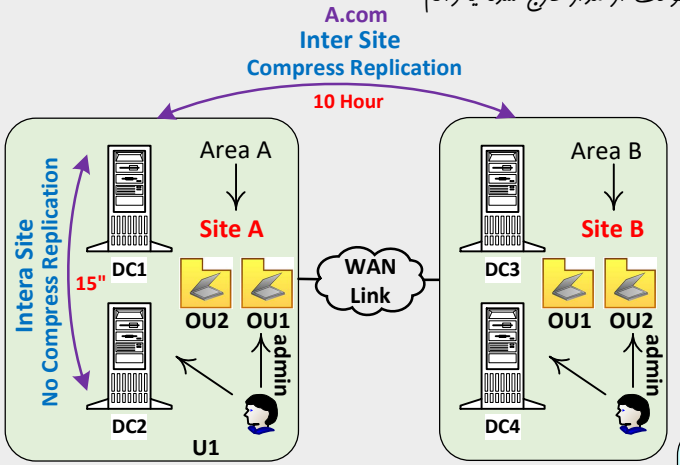
Flexible Single Master Operations (FSMOs)
Operations masters
Operations master roles
Single master roles
Operations tokens

DC Based on NT (old)

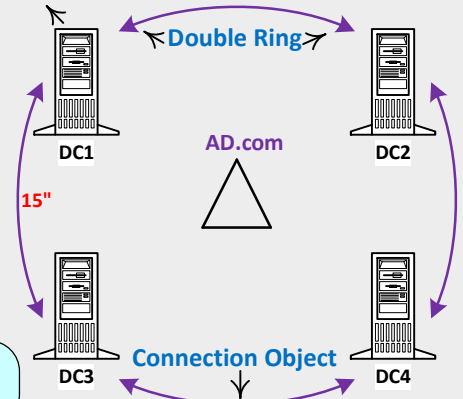


- در قبل از ویندوز ۲۰۰۰ میتوانستیم حداکثر یک عدد PDC و ۲۵ عدد BDC داشته باشیم که بصورت Hun & Spoke به PDC وصل بودند
- فقط یک Single Master Role وجود داشت که متعلق به PDC بود و به هر علتی اگر از مدار خارج میشد مواردی همچون Replication Join to domain,create computer Account, Change Password از دست میرفت و می بایست یکی از BDC ها را به PDC بصورت دستی ارتقاء میدادیم ، علت دستی ارتقاء دادن آن هم این بود که DC ها نمیدانستند PDC بصورت موقت از مدار خارج شده یا دائم

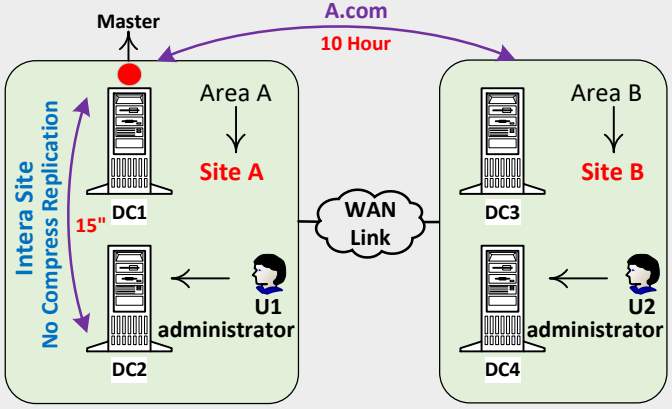
DC Based on AD After win 2000



- در این نوع شبکه ها همه DC هستند و بصورت **Multi Master Role** با هم کار میکنند
- فرض کاربر U1 ادمین OU1 باشد و به DC2 وصل شودو یک یوزر اکانت به نام ali در OU1 بسازد اگر فرض را براین بگذاریم که ۲ ساعت قبل Replication بین سایتی انجام شده باشد DC1 و DC2 هشت ساعت بعد متوجه این تغییر خواهند شد ، حال در بین این هشت ساعت اگر کاربر U2 به DC4 وصل شود و در OU2 یوزراکانتی به نام ali ایجاد کند ، حال در زمان Replication دو کاربر همنام خواهیم داشت



- برای رفع این مشکل دو ایده وجود خواهد داشت ، یکی اینکه از اساس جلوی این رخداد رابگیریم و دیگر اینکه بعد از بروز مشکل به داد آن برسیم ، برای حل این مشکل بطوری که اساسا این اتفاق رخ ندهد برای سایتهایمان یه رئیس Master تعیین میکنیم و همه دیگر DC ها برای انجام رول های مهم باید از آن اجازه بگیرند



- نکته مهم این که در شبکه AD ما Master نداریم بلکه Multi Master داریم و اگر فرضا مشکل ذکر شده بالا پیش آید در زمان Replication این مشکل بر اساس تقدم زمانی ، یک از کاربر ها را Rename خواهد کرد
- فرض که کاربر U1 به Dc2 وصل شده و Object1 را به Object Class Schema اضافه میکند و ضمنا ۲ ساعت نیز از زمان Replication قبلی گذشته است
- فرض که کاربر U2 به Dc4 وصل شده و Object1 را به Object Class Schema اضافه میکند و ضمنا تا زمان Replication چند ساعت باقی مانده است
- حال در زمان Replication تعداد ۲ عدد Object Class همنام داریم با توجه به اینکه توسعه Schema یکطرفه میباشد فقط یک راه حل داریم و آن هم تعیین یک رئیس Master در جهت ایجاد تغییر در Schema است و نه اینکه به دیگران اجازه این کار را بدهد و اگر به دلیلی Down شود این وظیفه را باید به یکی دیگر از DC ها سپرد در چنین وضعیتی DC که وظیفه تغییر رادارد یک نسخه Read & Write از اسکیما دارد و الباقی DC ها نسخه Read از اسکیما را دارند

AD DS contains five operations master roles. Two roles are performed for the entire forest: (Forest Wide)
1-Domain naming Master Role
2-Schema Master Role

Three roles are performed in each domain: (Domain Wide)
3-Relative identifier (RID) Master Role
4-Infrastructure Master Role
5-PDC Emulator Role

I

FSMO

– در تمامی مثالها وقتی صحبت از کاربر یا گروه میشود باید با دید انتزاعی به آن نگریست و مفهوم Object را در نظر آورد

1 Schema Master Role

– در کل Forest فقط یک DC این وظیفه را بعهده دارد و وظیفه آن تغییر در اسکیما می باشد و وجودش برای توسعه اسکیما ضروری است ، این DC یک نسخه Read & Write از اسکیما دارد و الباقی DCها نسخه Read از اسکیما را دارند

– وجود این رول برای **Forest Functional Level** ضروری است ، در نبود این رول اسکیما توسعه نمی یابد و چه بسا اپلیکیشن AD Integrated نصب نمیگردد

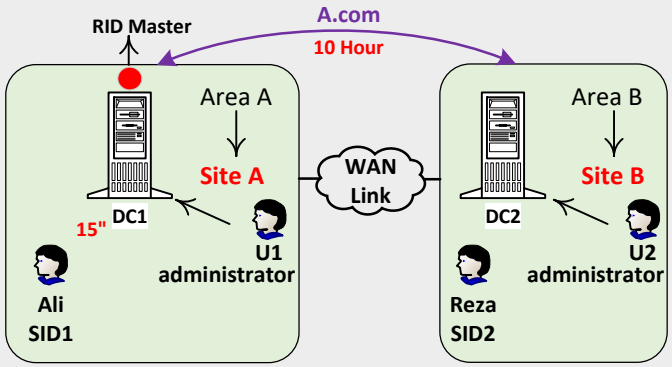
– برای توسعه اسکیما کاربر باید عضو گروه های **Enterprise admins & Schema admis** باشد پس وجود Schema Master Role شرط لازم برای توسعه اسکیما برای کاربر هست ولی کافی نیست

(Forest Wide)

2 Domain Name Master Role

– از این رول موقعی استفاده میشود که بخواهیم دامینی را به **Forest** اضافه یا حذف نمائیم و در حقیقت وظیفه اش مدیریت نام گزاری دامین های Forest است و به همین دلیل دو دامین همنام نمیتواند در Forest وجود داشته باشد

3 RID (Relative ID) Master Role



– کاربران (U1,U2) هر کدام User Account های (ali,reza) را با SID یکتایی که تولید میشوند در زمانهای مختلف قبل از اینکه Replication انجام گردد می سازند ، این امکان هرچند نادر ممکن است در مورد یکی شدن SID ها بوجود آید

– با توجه به اینکه SID یکتاست و امکان عوض شدن آن وجود ندارد در صورت یکی شدن ، به یک مشکل برطرف نشدنی برخواهیم خورد

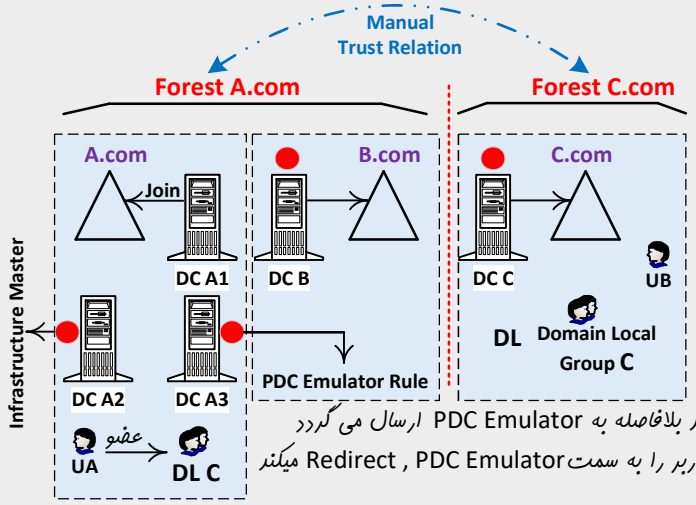
– با توجه به توضیحات بالا الگوی تولید **SID** وظیفه یک **DC** مشخص میشود که رول **RID Master Role** را دارد

– طبق این مثال روش کار بدین شکل است که DC2 به DC1 که رول RID Master را دارد مراجعه کرده و تعدادی SID دریافت کرده که در موقع لزوم از آنها استفاده میکند و قبل از اتمام SID ها مجددا برای دریافت SID به DC1 مراجعه می نماید

– نکته جالب اینکه DC1 فودش SID تولید نمیکند بلکه الگویی به دیگر DC ها ارائه میدهد تا توسط آن فودشان SID تولید کنند

– برایند این رول عدم تکراری SID در مجموعه Object های دامین فواهد بود و این رول به DHCP تشبیه میشود

4 Infrastructure Master Role



– وقتی کاربر UA به DCA1 وصل میشود در تیکتی که برای او ساخته میشود SID کاربر و SID مجموعه گروه های Security که عضو آنها است درج میشود حال در DCA1 فود DDP آدرس Global Security کاربر UA را دارد ولی گروه های Universal Security را باید از GC Server استعلام نماید و دست آخر برای تشفیص گروه های **Domain Local Security** باید به **Infrastructure Master Role** مراجعه کند

– اگر یک کاربر را از یک دامین عضو دامین لوکال فارست دیگری کنیم DC که وظیفه Infrastructure Master Role را دارد از این موضوع آگاه میشود و سپس این موضوع را به الباقی DCها فبر میدهد

– در واقع این رول یک وظیفه دوگانه دارد ، وظیفه اولش رصد کردن اتفاقاتی که برای هر **Object** در دامین می افتد و سپس وظیفه دومش اعلام کردن آن به دیگر دامین ها است در حقیقت تغییرات در دامین ها از طریق این رول Replicate می گردد

5 PDC Emulator Rule

1 **(Emulates a PDC for backward compatibility)** – NT4 در صورت وجود سرویس NT در شبکه نیاز به سروری است که نقش PDC را بازی کند

2 **(Participates in special password update handling for the domain)** – روش کار بدین شکل است که اگر پسورد کاربردر هر کدام از DCها تغییر کند بلافاصله به PDC Emulator ارسال می گردد

– حال اگر فرضا پسورد UA از طریق DCA1 تغییر کرده باشد و باهمان نام کاربری در DC C لاگین نمائیم چون این سرور از تغییرات آگاه نیست بطور اتوماتیک کاربر را به سمت PDC Emulator , Redirect میکند

3 **(Manages Group Policy updates within a domain)**

– اگر فرضا کاربر UA از طریق دستور Gpmc.msc بفواهد یک پالیسی را فعال کند ابتدا به سمت PDC Emulator , Redirect میشود و سپس تغییرات انجام میشود ، حال اگر کاربر UB نیز بفواهد پالیسی را تغییر دهد همین رفتار را فواهد داشت

– Group Policy Objects فقط روی PDC Emulator ایجاد ، تصحیح و تغییر میکند و بعد به دیگر DCها منتقل میشود

4 **Provides a master time source for the domain**

5 **Acts as the domain master browser** – کاربردی ندارد

– نکته اول اینکه افتلاف زمان در اجزاء دامین بر اساس پرتکل Kerberos حداکثر ۵ دقیقه می باشد ، در هر دامین یک PDC Emulator داریم که Master time همه کامپیوترهای موجود در آن دامین میشود حال طبق شکل بالا چون دامین A.com بعنوان Forest root domain در نظر گرفته میشود الباقی PDC Emulator های دامین های دیگر زمان فود را با آن Sync میکنند و در انتها Forest root domain نیز باید زمان فودش را با یک NTP server , Sync کند

(Domain Wide)

C:\Windows\system32>w32tm /query /status

I

Optimizing the Placement of Operations Masters

- اولین دامین کنترلر اولین دامین فارست تمامی Master Roles ها را در خود دارد و در صورت اضافه شدن دامین های دیگر میتوان تعدادی از این وظایف را به دیگر DC ها طبق قاعده زیر تفویض نمود
- بهتر است رولهای Forest Wide Master roles & GC Server روی یک DC و RID Master and PDC Emulator نیز بر روی یک DC دیگر باشد
- رول Infrastructure Master Role نباید بر روی DC باشد که GC Server است
- اگر در یک دامین همه DC ها GC Server هم باشند امکان داشتن Infrastructure Master Role نیست و البته نیازی هم به آن نیست چون اگر همه GC Server باشند همه از موضوع Infrastructure Master Role طی پروسه Replication باخبر خواهند بود پس بعنوان یک قاعده اگر در فارست DC داشتیم که GC Server نبود Infrastructure Master Role را به آن میسپاریم ولی اگر همه GC Server بودند نیازی به واگذاری Infrastructure Master Roleنیست

II

Identifying Operations Masters

Schema Master Role (1) — mmc → Snap-in Schema (Regsvr32 schmmgmt.dll) → Active directory Schema → R-Click → Operation master → View & Change Schema Master

Domain Name Master Role (2) — mmc → Snap-in Domain (Domain.msc) → Active directory Domain & Trusts → R-Click → Operation master → View & Change Domain Naming Operation Master

RID (Relative ID) Master Role (3)
Infrastructure Master Role (4)
PDC Emulator Rule (5)
— mmc → Snap-in Domain (Dsc.msc) → Active directory users and computers → R-Click → All Tasks → Operation master →
- RID Master Roles
- Infrastructure Master Role
- PDC Emulator

GCserver (0) — mmc → Snap-in Domain (Dssite.msc) → Active directory Site and services → R-Click → NTDS Setting → R-Click → Properties → Global Catalog

View All 5 Roles:
```
netdom query fsmo
```

```
dsquery server -site default-first-site-name -isgc
```
Site name

View GC Servers

- از دستورات **NTDSutil , DCDiag , NetDom** نیز برای رویت و انجام کارهای مختلف **FSMO** میتوان استفاده نمود

III

Transferring Operations Master Roles

- اگر بخواهیم به دلایلی مدتی یکی از DC هایی که Master Role دارد را خاموش کنیم و یا آن را آپگرید به دامین کنترلر بالاتری کنیم و یا ارتقاء Migration دهیم، Master Role را به DC دیگری تفویض میکنیم
- از طریق Snap-in هایی که رول ها را مشاهده کردیم میتوانیم با آن رولها را انتقال دهیم ضمن اینکه همواره استفاده از Command نیز میسر است
- فرض کنیم رول های Schema & PDC Emulator Rols را به DC دیگری واگذار کردیم و آن DC برای همیشه Down شده است در این شرایط باید از دستور Seize استفاده کنیم که از Command یا Powershell استفاده میکنیم
- در هنگامی که میخواهیم یک رول را Seize نمائیم ابتدا دستور بصورت اتوماتیک تلاش میکند عمل Transfer را انجام دهد و در صورت واقعا Down بودن DC که رول ها را بعهده داشته و اعلام Fail transfer نسبت به Seize اقدام میکند

I

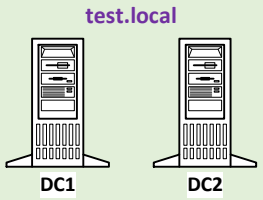
Seize Commands

```
C:\Windows\system32>ntdsutil
ntdsutil: roles
fsmo maintenance: ?
 ?                          - Show this help information
 Connections                - Connect to a specific AD DC/LDS instance
 Help                       - Show this help information
 Quit                       - Return to the prior menu
 Seize infrastructure master - Overwrite infrastructure role on connected server
 Seize naming master        - Overwrite Naming Master role on connected server
 Seize PDC                  - Overwrite PDC role on connected server
 Seize RID master           - Overwrite RID role on connected server
 Seize schema master        - Overwrite schema role on connected server
 Select operation target    - Select sites, servers, domains, roles and naming contexts
 Transfer infrastructure master - Make connected server the infrastructure master
 Transfer naming master     - Make connected server the naming master
 Transfer PDC               - Make connected server the PDC
 Transfer RID master        - Make connected server the RID master
 Transfer schema master     - Make connected server the schema master
fsmo maintenance:
```

II

Seize Scenario

- فرض کنیم رول های Schema & PDC Emulator Rols را به DC2 واگزار کردیم و برای همیشه Down شده است




```
C:\Windows\system32>netdom query fsmo
Schema master               DC2.test.local
Domain naming master        DC1.test.local
PDC                         DC2.test.local
RID pool manager            DC1.test.local
Infrastructure master       DC1.test.local
The command completed successfully.
```

```
C:\Windows\system32>ntdsutil
ntdsutil: roles
fsmo maintenance:  Connections
Server connections:Connect to server DC1.test.local
Binding to dc1.test.local
Connected to dc1.test.local using credentials of locally logged on user.
Server connections:quit
fsmo maintenance: Seize schema master
Attempting safe transfer of schema FSMO befor seizure.
fsmo maintenance:
```

```
fsmo maintenance: Seize PDC
Attempting safe transfer of schema FSMO befor seizure.
fsmo maintenance:
```

- حال اگر در مثال بالا DC2 مد نظر اگر به چرفه دامین برگردد نمیتوان همینطوری آن راوارد شبکه کرد بلکه باید ابتدا AD را از روی آن بصورت Force Removal پاک کرد و Metadata Cleanup انجام داد و مجددا یک DC جدید راه اندازی نمود

نکته مهم

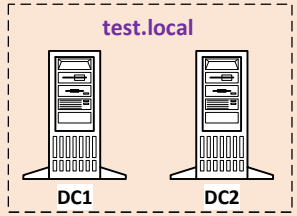
Temporary and permanent Seize Roles

- در مورد رولهای **1-Schema master Role** **2- RID Master Role** **3- Domain name operating master role** بعلت اینکه در لحظه به آنها نیاز نداریم و حیاتی نیستند میتوانیم صبر کنیم اما در مورد **4-PDC Emulator** و **5- Infrastructure Master Role** نمیتوان صبر نمود نکته اینکه در مورد سه مستر رول اول نباید موقتی Seize نمود و باید مطمئن شد که دیگر به چرفه دامین سرور مورد نظر بر نمی گردد ولی دو مستر رول آخر را میتوان موقتی Seize نمود چون امکان Transfer مجدد رول وجود دارد

- در صورت داشتن GC Server در DC نیاز به Infrastructure Master Role نیست و GC Server این وظیفه را بعهده میگیرد

- رول Infrastructure Master Role نباید بر روی DC باشد که GC Server است

I



Schema Master Role
Domain Name Master Role
RID (Relative ID) Master Role
Infrastructure Master Role
PDC Emulator Rule

– فرض کنیم یک فارست با یک دامین و دو دامین کنترلر موجود داریم ، در اینحالت چون رولی بین دامین کنترلر ها تغییر نکرده است هر ۵ رول بر روی Root Domain قرار خواهد داشت و هر دو دامین کنترلر بصورت پیش فرض GC Server نیز خواهند بود که باعث میشود رول Infrastructure Master Role بخاطر وجود GC Server از تغییرات مطلع نشود و به همین علت عملا این رول کارایی نخواهد داشت و طبق پروسه Replication هر دو دامین کنترلر از تغییرات مطلع خواهند شد

– ذکر این نکته مهم است که فعال کردن GC Server و Recycle bin نیاز به رول Infrastructure Master Role را مرتفع میسازد

– بنابراین در این حالتی که ذکر شده است نیازی به جابجا کردن مستر رول ها نیست مگر اینکه بخواهیم Migration انجام دهیم و اگر DC1 , Down شد با Seize کردن رول PDC Emulator Rule به DC2 بطور موقت و سریع مشکل حل خواهد شد و به دلایلی که گفته شد رول Infrastructure Master Role نیز عملا کارایی ندارد

II

دلایل Demote کردن دامین کنترلر

Migration
1 – ویندوز دچار خرابی شده باشد یعنی مشکل Replication داشته باشد (Sysvol Or Ntds.dit Don't Sync)
2 – Inplaced upgrade – یعنی ویندوز را با اجرای Setup نسخه بالاتر از روی وینوز فعلی به نسخه بالاتر آپگرید کنیم ، این روش بعلت خطاهای ناشناخته ای که ممکن است رخ دهد عموما توصیه نمیشود
Migration – Clean Install – بدین معنی که از ابتدا بصورت نصب را انجام دهیم

Migration

– در حال حاضر سقف Domain Functional level = Win2016 میباشد که نهایتا میتوان به آن ارتقاء داد ولی فود ویندوز در این وضعیت به Win2019 ارتقاء خواهد یافت

– ابتدا Promotion را روی ویندوز ۲۰۱۹ جلو میبریم در این وضعیت سه دامین کنترلر موجود خواهیم داشت سپس مجموعه مستر رول ها را به دامین کنترلر جدید انتقال میدهیم حال به مدت چند روز وضعیت دامین کنترل ها را از نظر کارائی و Replication رصد میکنیم و اگر مشکلی نبود آدرس DNS مجموعه کلاینت و سرورها را به سمت سرور جدید و DC2 تغییر میدهیم و باز نیز پس از تست چند روزه و عدم هر گونه مشکلی و لاگی که از DC1 , DNS گرفته ایم نشان نمیدهد که کلاینت یا سروری آدرسی مطالبه کرده باشدبعد از چند روز DC1 را از مدار خارج نموده و پس از تست های نهایی طی چند روز نام دامین کنترلر جدید را به نام DC1 تغییر میدهیم

– هر چند ما ماشین جدید را مستقیما تغییر نام میدهیم و اصولا هم مشکلی پیش نمی آید ولی پیشنهاد مایکروسافت اینست که از طریق دستور Netdom یک نام دوم که در اینجا DC1 است به سیستم بدهیم سپس نام دوم Secondry را به اول Primary تغییر دهیم و نهایتا نام دوم را پاک میکنیم و اینکار نیز به این علت است که با DNS تعارضی برای نام دامین کنترلر بوجود نیاید

– اگر به هر دلیلی دامین کنترلر DC1 قدیمی بدون پروسه Demote طبیعی پاک شود باید ابتدا Force Demote نمود و ضمنا اثرات Forest Metadata یا همان فهرست دامین کنترلر از رده خارج شده را از روی دامین کنترلر پاک کرد

(Metadata=catalog=data about data) ← مثل فهرست کتاب یا منوی غذا

Forest Metadata → Cleanup

– اگر با روش طبیعی Demote یک دامین کنترلر از چرخه دامین خارج شود بصورت Member Server بالا می آید و اگر Force Demote شود بصورت Standalone Server بالا می آید

– وقتی به دامین یک دامین کنترلر اضافه میشود هم بر روی دامین کنترلر جدید تغییرات بوجود می آید و هم بر روی کل دامین و Forest Metadata حال اگر کامپیوتر را به روش Force Demote بخواهیم پاک کنیم باید بدین شکل عمل نمود

1 Force demote(Removal) AD from Server 2 Metadata Cleanup – فرض که در شکل بالا فقط دو دامین کنترلر DC1,2 داریم و DC2 را بدون Demote پاک کرده ایم و میخواهیم Metadata Cleanup کنیم

III

Metadata Cleanup

```
C:\Windows\system32>ntdsutil
ntdsutil: Metadata cleanup
Metadata cleanup:Select operation target
Select operation target:Connections
server Connections:Connect to server dc1.test.local
Server Connection:quit
Select operation target:list sites
0 - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=local
Select operation target:select site 0
Select operation target:list domains
0 – DC=test,DC=local
Select operation target:select domain 0
Site - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=local
Domain - DC=test,DC=local
Select operation target:list servers in site
0 – CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=local
1 – CN=DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=local
Select operation target:select server 1
Site - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=local
Domain - DC=test,DC=local
Server - CN=DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=local
DSA Object – CN=NTDS setting ,CN=DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=local
DNS host name – DC2.test.local
Computer Object – CN=DC2,OU=Domain Controller,DC=test,DC=ir
Select operation target:quit
Metadata cleanup:Remove selected server
```

– در این مقطع اگر مستر رولی از DC2 پاک شده باشد آن رول Seize شده و به DC1 که الان به آن وصل شده ایم انتقال داده میشود

```
"CN=DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=local removed from dc1.test.local"
```

– جهت اطمینان کامل در انتهای کار بصورت چشمی نیز دامین ، سایت و DNS را چک میکنیم

I

Install From Media (IFM)

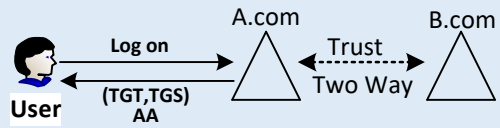
- هنگام راه اندازی دامین کنترلر دوم به بعد طی مراحل نصب ، اگر دامین دارای لینک شبکه WAN ضعیفی باشد این امکان وجود دارد که Directory و Sysvol و Registry به جای لینک شبکه از طریق یک مدیا به دامین کنترلر جدید انتقال داده شود

```
ntdsutil: ifm
Active Instance not set. To set an active instance use "Activate Instance ".
ntdsutil: Activate Instance ntds
ntdsutil: ifm
Ifm:create Sysvol full c:\ifm\sysvol-full
IFM media created successfully in c:\ifm\sysvol-full
```

II

TGT , TGS

- تیکتی که تضمین میکند که تیکت به مدت پیش فرض ۱۰ ساعت گرفته شود User SID + Security Groups SID ← (Authenticate) TGT (Ticket Garanting Ticket)
- بعد از TGT تیکت TGS مجوز استفاده از سرویس یک سرور را ارائه میکند مثلا مجوز سرویس فایل از یک فایل سرور ← (Authorize) TGS (Ticket Garanting Service)



- طبق مثال دامین کنترلر باید براند که مثلا فایل سرور سرویس فایل ارائه میدهد تا TGS را صادر کند ، یک Attribute در Computer Account وجود دارد به نام SPN (Service Principal Name) که مقادیر آن مشخص میکند که چه سرویس هایی ارائه میشود و در برخی موارد ممکن است در این قسمت سرویس مورد نظر برای ارائه سرویس مشخص نشده باشد و در این حالت از نظر دامین کنترلر آن کامپیوتر حاوی آن سرویس مد نظر نمی باشد ، برای اینکه متوجه شویم که مقادیر SPN یک کامپیوتری دارای نقص است یا خیر توسط یک سرویس مانیتورینگ مشخص میشود که بهترین نمونه آن SCOM (System Center Operation Manager) مایکروسافت می باشد

III

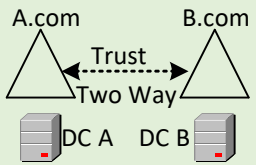
3 Forest (Trust)

- Trust یک ارتباط(Relation)بین دو دامین است که باعث میشود تیکت صادر شده در یک دامین در دامین دیگر نیز اعتبار داشته باشد و بدینوسیله وسعت اعتبارتیکت بیشتر شود

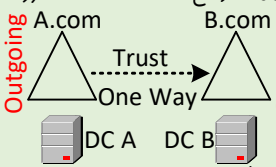
دسته بندی اول Trust

انواع Trust

1 One way or Two way

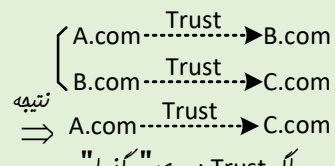


در یک فارست هر دو دامین به هم Trust دو طرفه دارند

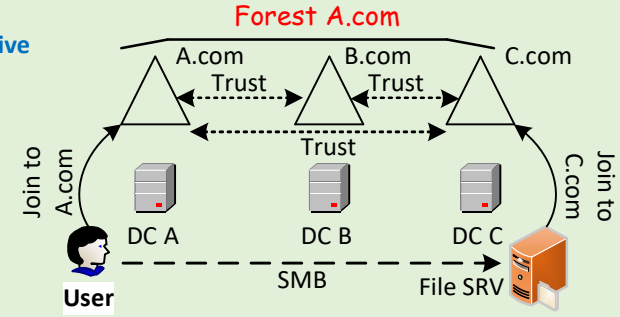


تیکت صادر شده در A.com در B.com اعتبار ندارد ولی عکس آن درست است

2 Transitive or Non transitive

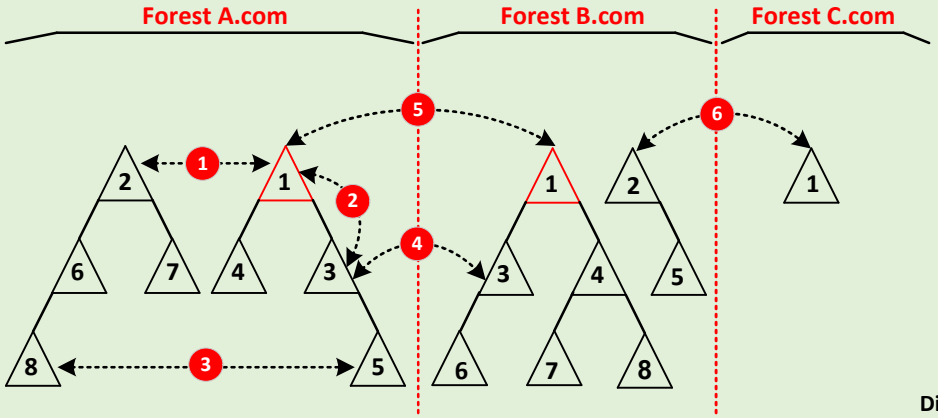


- اگر Trust مسری "گذرا" باشد رابطه بالا مورد قبول است درغیر اینصورت غیر



دسته بندی دوم Trust

- برای این نوع دسته بندی این سوالها مطرح میگردد ۱- این تراست بین کدام دو دامین واقع شده است؟ ۲- تراست یکطرفه است یا دوطرفه ؟ ۳- تراست گذرا است یا غیر گذرا ؟ ۴- تراست بصورت اتوماتیک است یا دستی تنظیم میشود؟



Tree root trust 1
Between Forest Root Domain and New Root Tree in Same Forest
Two way -Transitive-Automatic

Parent-child trust 2
Between Parent Domain and Child in Same Tree Forest
Two way -Transitive-Automatic

Shortcut Trust 3
Between two Domain from different tree in Same Forest
One way or Two way -NoneTransitive-Manual

- بصورت معمول نیز تراست Transitive وجود دارد فقط بر روی دامین Load میگذارد و برای کم کردن Logical فاصله بین دامین ها و افزایش Performance در دامین هایی که Tree های عمیق دارند استفاده میشود

External Trust 4
Between Two Domain in Different Forest
One way or Two way -NoneTransitive-Manual
Password trust Change Every 7 Days

- اگر ۷ روز ارتباط قطع شود تراست باید مجدد برقرار شود

Forest Trust 5
Between Two Forest Root Domain in Different Forest
One way or Two way -Transitive-Manual
Password trust Change Every 7 Days

- بجای برقراری ۴۶ تراست اکسترنال میتوان یک تراست بین Forest Root Domain ها برقرار کرد

Realm Trust 6
Between a Microsoft Directory and None Microsoft Directory If support Authentication Kerberos V5 Ex. OLDAP
One way or Two way -Transitive or None Transitive-Manual

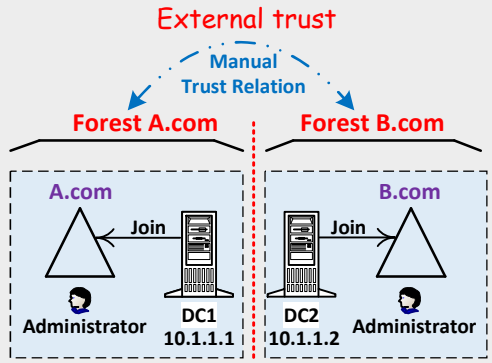
I

Ping From DC1

```
C:\Users\Administrator>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:
Reply from 10.1.1.2: bytes=32 time<1ms TTL=128
```

Browse from DC1

- در ابتدای کار و قبل از اینکه تراستی بین دو فارست برقرار شود از هر کامپیوتر دامینی که کامپیوتر دیگر را Browse میکنیم نیاز به نام کاربری و رمز عبور خواهیم داشت



- با توجه به شرایط موجود دو نوع تراست میتوان ایجاد کرد (External trust & Forest trust)
- در هنگام ایجاد تراست عموما هر ادمینی تراست سمت خودش را می سازد مگر اینکه رمز ادمین سمت مقابل را داشته باشد

External trust

A.com <---------- B.com

One way -NoneTransitive-Manual

میخواهیم کاربری که در سمت **A.com** تیکت برای او صادر میشود تیکتش در سمت **B.com** نیز اعتبار داشته باشد

A.com

1 Ping → 10.1.1.2 → Ok

2 Dnsmgmt.msc → Conditional forwarder → New conditional forwarder → DNS Domain → B.com → IP Address → 10.1.1.2

ابتدا باید یک رکورد در DNS برای سمت مقابل ایجاد کنیم

3 Domain.msc → R-Click Mouse → A.com(properties) → Tab trust → New trust → Insert name → B.com → External trust → One-way:incoming → This domain only → Both this domain and specified domain → Trust password → wxyz → Finish

- اگر رمز دامین سمت مقابل را داشته باشیم از اینحالت استفاده میکنیم تا تمام مراحل سمت مقابل اتوماتیک انجام شود

B.com

1 Ping → 10.1.1.1 → Ok

2 Dnsmgmt.msc → Conditional forwarder → New conditional forwarder → DNS Domain → A.com → IP Address → 10.1.1.1

ابتدا باید یک رکورد در DNS برای سمت مقابل ایجاد کنیم

3 Domain.msc → R-Click Mouse → B.com(properties) → Tab trust → New trust → Insert name → A.com → External trust → One-way:outgoing → This domain only → Both this domain and specified domain → Domain wide authentication → Trust password → wxyz → Finish

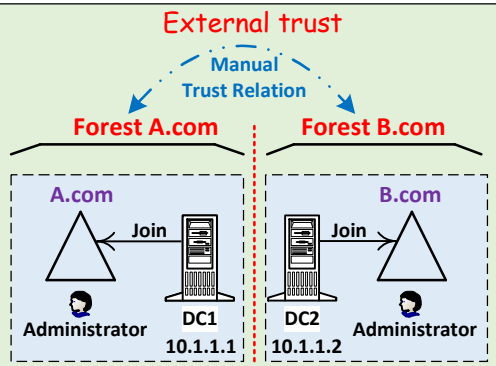
- اگر رمز دامین سمت مقابل را داشته باشیم از اینحالت استفاده میکنیم تا تمام مراحل سمت مقابل اتوماتیک انجام شود

Domain wide authentication – با توجه به اینکه B.com به A.com تراست کرده است در این حالت کاربری که در A.com Authenticate میشوند همه کامپیوترهایش به تمام منابع B.com دسترسی خواهد داشت

Selective authentication – با توجه به اینکه B.com به A.com تراست کرده است در این حالت فقط بخشی از منابعی که برخی کامپیوترهای کاربران A.com اجازه دسترسی به آن را دارند ، مشخص میکنیم

- بعد از اتمام کار و برقراری External trust حال کاربران دامین A.com وقتی عمل Browse را انجام میدهند بدون درج نام کاربری و رمز به تمام منابع B.com دسترسی خواهند داشت و بصورت معکوس نیاز به نام کاربری و رمز عبور خواهد بود
- در قسمت Both this domain and specified domain اگر تراست هر دو طرف را همزمان برقرار کنیم نیاز به Trust password نخواهد بود وبصورت اتوماتیک برقرار خواهد شد
- این امکان وجود دارد که یک تراست One way را به یک تراست Two way Convert نمود و مجددا از نوع تراست را نساخت

I



میخواهیم کاربری که در سمت **A.com** تیکت برای او صادر میشود تیکتش در سمت **B.com** نیز اعتبار داشته باشد و بلعکس بصورت **Selective authentication**

1. **Ping** → **Ok** (10.1.1.2)

2. ابتدا باید یک رکورد در DNS برای سمت مقابل ایجاد کنیم: **Dnsmgmt.msc** → **Conditional forwarder** → **New conditional forwarder** → **DNS Domain** (B.com) → **IP Address** (10.1.1.2)

3. **Domain.msc** → **R-Click Mouse** (A.com(properties)) → **Tab trust** (New trust) → **Insert name** (B.com) → **External trust** → **Two Way** → **This domain only** / **Both this domain and specified domain** → **Selective authentication** → **Trust password** (wxyz) → **Finish**

1. **Ping** → **Ok** (10.1.1.1)

2. ابتدا باید یک رکورد در DNS برای سمت مقابل ایجاد کنیم: **Dnsmgmt.msc** → **Conditional forwarder** → **New conditional forwarder** → **DNS Domain** (A.com) → **IP Address** (10.1.1.1)

3. **Domain.msc** → **R-Click Mouse** (B.com(properties)) → **Tab trust** (New trust) → **Insert name** (A.com) → **External trust** → **Two Way** → **This domain only** / **Both this domain and specified domain** → **Selective authentication** → **Trust password** (wxyz) → **Finish**

در این مقطع از کاربران User Account خواسته نمیشود چون به هم تراست دارند ولی نمیتوانند همدیگر را Browse نمایند چون حالت Selective authentication دارد و هنوز تنظیم نشده است و کاربران Authenticate User محسوب نمیشوند

حال باید مشخص کنیم بطور مثال چه کاربرانی از **A.com** بر روی چه کامپیوترهایی از **B.com** حالت **Authenticate User** داشته باشند و با این کار محدوده تراست را کوچک میکنیم

Administrator A.com → Authenticate User (بطور مثال) → **DC2** 10.1.1.2

Dsa.msc → **On B.com** (Active view/advance) → **Tab Domain controller** (DC2(properties)) → **Tab Security** (Add user administaror from A.com / Athenticate with a user on A.com) → **Administrator (A\Administrator)** (Select Allow to authenticate)

باید درمرحله Security نام کاربر و رمز عبور را از سمت مقابل دریافت کنیم

Administrator B.com → Authenticate User (بطور مثال) → **DC1** 10.1.1.1

Dsa.msc → **On A.com** (Active view/advance) → **Tab Domain controller** (DC1(properties)) → **Tab Security** (Add user administaror from A.com / Athenticate with a user on A.com) → **Administrator (B\Administrator)** (Select Allow to authenticate)

با توجه به مرحله قبل در قسمت Authenticate , Security میباشد

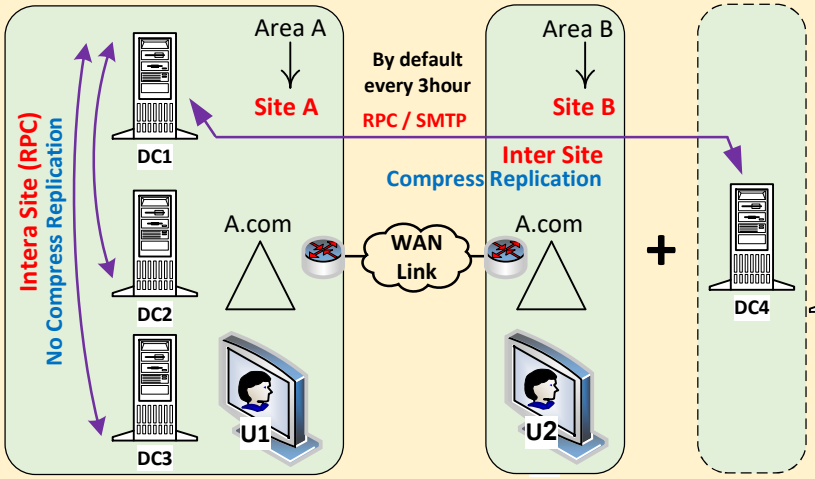
31- حالت Forest Trust نیز همانند External Trust میباشد با این تفاوت که حالت Transitive دارد و میتواند Forest Wide یا Selective authentication باشد بنابراین وسیعترین حالت تراست حالت Forest Wide میباشد

- حالت Selective authentication شبیه ساختار Hardware Firewall می ماند ، یعنی محدودیت کامل برقرار میشود تا زمانیکه Authenticate User را برقرار کنیم

I

Physical Site

NetID in Site A is different from NetID in SiteB



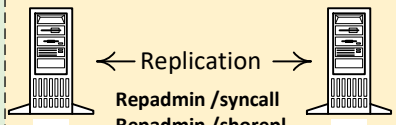
AD Site

– علت اضافه شدن یک سایت دو علت اصلی میتواند داشته باشد اول اینکه لینک بین دو ساختمان که از نظر جغرافیایی جدا از هم هستند ضعیف می باشد و ناچار به ایجاد یک Quick Access در سایت جدید برای کاربران هستیم و دوم اینکه لینک بین ساختمانها خوب است و کاربران نیز شکایتی ندارند در این مرحله ممکن است برای رفع SPOF در سایت اول یک سایت جدید همراه با دامین کنترلر ایجاد میکنیم و اساسا ساختار مایکروسافت بدین شکل است که در هر ساختمانی که یک دامین کنترلر اضافه میشود باید یک سایت تشکیل شود

FRS(File Replication Service)Old
DFSR(Distributed File System Replication)New

– وقتی Replication انجام میشود دو ماهیت Ntds.dit و Sysvol باهم Sync میگردد

– FRS سرویسی است که دو تغییرات دو فولدر Share شده را باهم Sync میکند



Repadmin /syncall
Repadmin /shorepl
Repadmin /replsummary
dcdiag
ADREPLSTATUS (App)

– در صورت ساختن یک فایل در Dc1 , Sysvol باید در Dc2 , Sysvol نیز آن را مشاهده نمود

– پرتکلی که برای Sync شدن Replication استفاده میشود RPC(Remote Procedure Call) می باشد

– پرتکل RPC ازدو Session برای Replication استفاده میکند

Primary Session on port 135 & Second Session on Random port

RPC Client → RPC Server

– مجموعه Snap-in در ارتباطات اکتیو دایرکتوری از این پرتکل در لایه اپلیکیشن استفاده میکند

– سه عنصر Site Name , DCs , Subnet حتما در یک سایت وجود دارند

– وقتی فقط یک سایت وجود دارد Default-First-Side-Name نمی بایست Subnet برای آن تعیین نمود ، ولی برای بیش از یک سایت باید به دقت Subnetها مشخص شوند

II

Site Link

– Site Link مربوط به مشخص کردن جزئیات ارتباط Inter Site میباشد و بعنوان دستورالعمل Replication شناخته میشود ، بعنوان مثال هفت روز هفته هر سه ساعت یکبار به صورت فشرده Replication بین دو سایت برقرار شود

Default

Schedule — Replicate Every

n*15,Default 180" 15"-7day

– Site Link نیاز به نام گذاری دارد که معمولا از نام سایت ها استفاده میکنیم مثلا Site A-SiteB یا Site A-SiteB-Site C

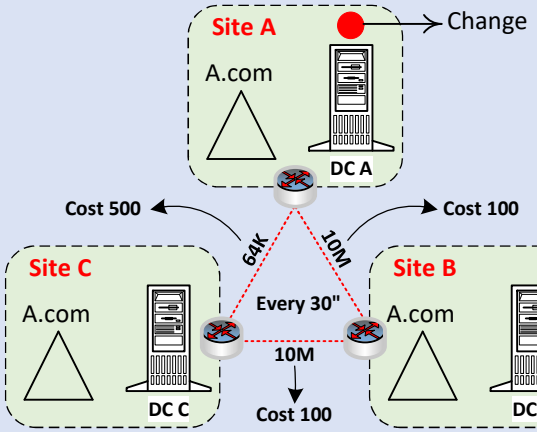
Site Link Transport Type

– منظور همان پرتکل لایه Application برای فرایند Replication میباشد نکته اینجاست که وقتی از پرتکل RPC استفاده میکنیم در کنسول Dssite.msc با نام IP شناخته میشود پرتکل SMTP تقریبا هیچ وقت استفاده نمیشود و مربوط به مواقعی است که لینک بین دو سایت اصلا قابل اعتماد نباشد Non-Reliable یا بعضی اوقات برقرار نباشد برای تبادل تغییرات اکتیو دایرکتوری از آن استفاده میشود

– دو نکته در ارتباط با پرتکل SMTP وجود دارد یکی اینکه تغییرات DDP با این پرتکل Replicate نمیشود پس DCهایی که قرار است با این پرتکل در دو طرف سایت باهم Sync شوند نباید در یک دامین باشند و نکته دوم اینکه این پرتکل برای تبادل اطلاعات پرتکل ایمنی نیست و برای برقرار کردن امنیت آن نیاز به Certificate خواهیم داشت SMTPS

– در مورد اینکه بزرگترین پارتیشن دایرکتوری کدام است نمیتوان نظر دقیقی ارائه کرد ولی پرواضح است که حجم تغییرات DDP در دایرکتوری از الباقی پارتیشن ها بیشتر است

– در اغلب طراحی ها یک فارست و یک دامین و به تعداد پراکندگی جغرافیایی ساختمانها سایت تعریف میشود و برای افزایش دامین باید حتما دلیل منطقی وجود داشته باشد



Site Link Cost

1 Site Link ← SiteA-SiteB-SiteC فقط یک سایت لینک بدون Cost

– اگر DC A تغییر کند DC B به DC A سر زمان مشخص مراجعه نموده و از طریق لینک فیزیکی AB تغییرات را میگیرد

– اگر DC A تغییر کند DC C به DC A سر زمان مشخص مراجعه نموده و از طریق لینک فیزیکی AB-BC تغییرات را میگیرد

– نکته اینجاست که برای تبادل تغییرات در DC B و DC C از لینک فیزیکی AB دو بار استفاده میشود

2 Site Link ← SiteA-SiteB SiteB-SiteC دو سایت لینک بدون Cost

– میتوان تبادل را به شکلی انجام داد که تغییرات DC A ابتدا به DC B منتقل شده و سپس DC C از طریق DC B مبادرت به دریافت تغییرات کند در اینصورت از لینک فیزیکی AB یکبار استفاده خواهد شد و DC A , DC C بعلت نداشتن سایت لینک اقدامی برای دریافت تغییرات از هم دیگر نمیکنند

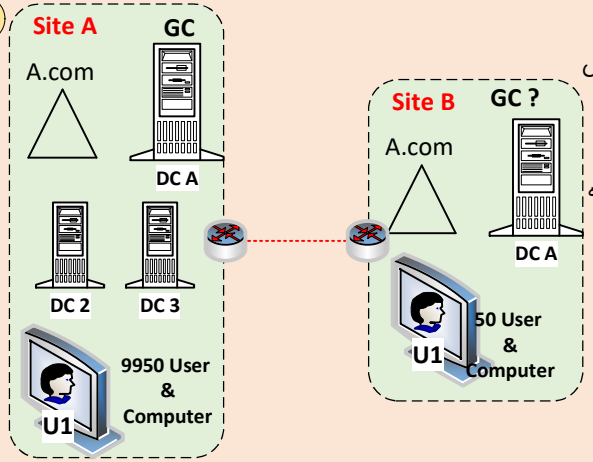
– در اینحالت اگر روتر B از مدار خارج شود کلا Replication قطع خواهد شد چون روتر B , SPOF شده است

3 Site Link SiteA-SiteC SiteB-SiteC SiteA-SiteB سه سایت لینک با Cost

– در اینحالت از SiteA-SiteC استفاده نخواهد شد مگر اینکه روتر B از دسترس خارج شده و ارتباط سایت B قطع شود

نکته
– اگر بین دو سایت سه لینک فیزیکی مختلف توسط روتر برقرار باشد به سایت لینک هیچ ارتباطی پیدا نمیکند و اینکه از چه لینکی اطلاعات عبور کند وظیفه روتر است
– اگر بین دو سایت یک لینک فیزیکی با سه سایت لینک برقرار باشد هر سه سایت لینک حتما استفاده خواهد شد حتی اگر Overlap داشته باشد

I GC Server (Universal Group Membership Caching)



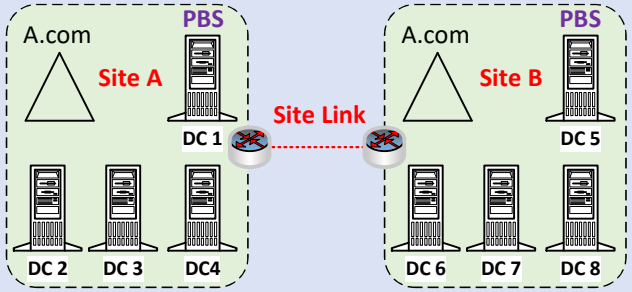
- عمدتا در حال حاضر طراحی بر اساس Per Site انجام میگردد ، برای GC Server بر اساس سایت تصمیم گیری میکنیم که در هر سایت آیا GC Server داشته باشیم و چند تا حال اگر یک فارست و یک دامین و دو سایت داشته باشیم که در سایت A سه دامین کنترلر و در سایت B یک دامین کنترلر وجود داشته باشد اگر فرضا در سایت A تعداد ۹۹۵۰ کاربر وجود داشته باشد و در سایت B تعداد ۵۰ کاربر وجود داشته باشد طبق قاعده طراحی موارد زیر را در نظر میگیریم
- اگر در سایت B , GC Server نداشته باشیم کاربران این سایت برای Log on کردن وقتی به DC مراجعه میکنند چون DC موجود GC Server نیست نمیتواند عضویت کاربر در گروه های Universal را تشخیص دهد به سایت A که GC Server دارد مراجعه میکند و یک ترافیک بر روی لینک دو سایت گذاشته خواهد شد ولی اگر B , DC GC Server باشد این ترافیک حذف میشود ولی ترافیک Replication بین GC Server ها به لینک بین دو سایت اضافه میشود
- حال با توجه به تعداد کاربر بالای سایت A اگر کاربران سایت B در هنگام Log on به سایت A برای ارتباط با GC Server مراجعه کنند بهتر از تبادل ترافیک GC Server Replication خواهد بود
- یک نکته مهم اینکه اگر لینک بین دو سایت قطع شود دیگر کاربران سایت B نمیتوانند به DC موجود در سایت Log on کنند در این شرایط قابلیتی وجود دارد به نام **Universal Group Membership Caching** که باعث میشود وقتی DC B به DC A برای سوال درمورد گروه های Universal مراجعه میکند جواب را Cache میکند و هر از چند گاهی نیز آن را به روز میکند

II RODC (Read Only Domain Controller)

1. – در RODC دایرکتوری بصورت فقط خواندنی می باشد و نمیتوان مستقیما در دایرکتوری تغییر ایجاد کرد بنابراین تغییرات در DC ایجاد میشود و به RODC , Replicate میگردد
2. – Password هیچ اکانتی به RODC , Replicate نمیگردد به غیر از کامپیوتر اکانت خود RODC و یک یوزر اکانت ارتباطی اکتیو دایرکتوری ها ، ولی با **PRP (Password Replication Policy)** میتوان این قاعده را برای برخی اکانتها تغییر داد
3. – Replication بین DC و RODC یکطرفه می باشد DC ⟶ RODC

- بنا براین در محلی که نتوان از نظر فیزیکی امنیت سرور DC را تضمین نمود از RODC استفاده میشود و در هر سایتی یک RODC بیشتر نمیتوان گذاشت
- اگر کاربری برای Log on به RODC مراجعه کند این سرور چون حاوی رمزها نیست برای استعلام پسورد به یک DC مراجعه خواهد نمود در ضمن DC به RODC و بالعکس Convert نمیشود

III (PBS) Preferred Bridged Server



- در هر سایت بصورت اتوماتیک یک نماینده برای Replication انتخاب میشود مثلا در سایت A , DC1 و در سایت B , DC5 انتخاب میشود
- موقعی که موعد Replication میرسد فقط نماینده ها با هم Replicate را انجام میدهند
- به این روش اصطلاحا **(PBS) Preferred Bridged Server** میگویند

IV LAPS (Local Administrator Password Solution)

- تمام کامپیوترهای موجود در دامین دارای یک Local User Account به نام Administrator هستند که بصورت پیش بر روی کلاینتها Disable و بر روی سرورها Enable میباشد

1 Enable Local Administrator & Rename that

Gpmc.msc → Computer Configuration → Windows Setting → Security Setting → Local Policies → Security Options → **Accounts:Administrator Account Status** / **Accounts:Rename Administrator Account**

فرض که Administrator را فعال نموده و به testadmin تغییر نام داد ه ایم

- LAPS پسورد Administrator داده شده را ریست نمیکند بلکه آن رابه یک رمز Random عوض میکند بنابراین رمز هر کامپیوتر با ماشین دیگر متمایز است
- در این روش امکان بروز رسانی رمز عبور نیست و علت آن اینست که در ویندوزهای سرور قدیمی از طریق پالیسی میشد تغییر رمز داد و همین طور که میدانیم از دو بخش پالیسی بخش کانتینر DDP ذخیره میشود و Template در Sysvol ذخیره میشود و چون همه رمزها در Sysvol ذخیره میشود و تمام کاربران نیز به آن دسترسی Read دارند به یک مشکل امنیتی برمی خوردیم هر چند که رمزها بصورت Clear Text در Sysvol ذخیره نمیشد

2 Copy AdmPwd.admx & AdmPwd.adml in PolicyDefinitions
Add LAPS to Computer Configuration/Administrative Templates

LAPS (Local Administrator Password Solution)

3 Install LAPS.x64.msi on the Domain Server

- نرم افزار LAPS را بر روی DC یا یک سرور عضو دامین نصب میکنیم

4 Schema Extend

ms-Mcs-AdmPwd – Stores the password in clear text
ms-Mcs-AdmPwdExpirationTime – Stores the time to reset the password

- برای توسعه اسکیما باید حتما نام کاربری که با آن به یک سیستم وصل شده ایم عضو گروه **Administrators,Schema Admins** باشد این دو Attribute به Computer Account اضافه میشود
- باید Permission تعریف کرد تا هر کسی دسترسی خواندن این دو Attribute را نداشته باشد

```
PS C:\Users\Administrator> Import-Module AdmPwd.PS
PS C:\Users\Administrator> Update-AdmPwdADSchema

Operation             DistinguishedName                                                Status
---------             -----------------                                                ------
AddSchemaAttribute    cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=t...  Success
AddSchemaAttribute    cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=test,DC=local       Success
ModifySchemaClass     cn=computer,CN=Schema,CN=Configuration,DC=test,DC=local           Success
```

- برای روی PowerShell دستورات توسعه اسکیما را اجرا میکنیم که باید حداقل نسخه ۲ به بالا باشد

5 Set-AdmPwdComputerSelfPermission

In the next step we will grant computers the ability to update their password attribute using the Set-AdmPwdComputerSelfPermission command.
This is required so the machine can update the password and expiration timestamp of its own managed local Administrator password.

Set-AdmPwdComputerSelfPermission- OrgUnit <name of the OU to delegate permissions>

```
PS C:\Users\Administrator> Set-AdmPwdComputerSelfPermission -OrgUnit "Test Policy"

Name         DistinguishedName                Status
----         -----------------                ------
Test Policy  OU=Test Policy,DC=Test,DC=local  Delegated
```

- به کامپیوترهای داخل OU اجازه میدهیم که رمز Administrtor شان را عوض کنند

6 Removing Or Add All Extended Rights & View User or Groups Password Access Rights

– To restrict the ability to view the password to specific users and groups you need to remove "All extended rights" from users and groups that are not allowed to read the value of attribute ms-Mcs-AdmPwd

1. Open **ADSIEdit**
2. Right Click on the OU that contains the computer accounts that you are installing this solution on and select Properties.
3. Click the **Security tab**.
4. Click Advanced.
5. Select the Group(s) or User(s) that you don't want to be able to read the password and then click Edit.
6. **Uncheck All extended rights**.

OR

Set-AdmPwdReadPasswordPermission -OrgUnit <name of the OU to delegate permissions> -AllowedPrincipals <users or groups>

Set-AdmPwdReadPasswordPermission -OrgUnit "test policy" -AllowedPrincipals helpdesk

- اجازه دیدن رمز Administrtor را به کاربران یا گروه های مجاز میدهیم و از کاربران یا گروه های غیر مجاز سلب میکنیم

To quickly find which security principals have extended rights to the OU

```
Find-AdmPwdExtendedRights -Identity "Test Policy" | fl
ObjectDN :OU=Test Policy,DC=test,dc=local
ExtendedRightHolder: {NT AUTHORITY\SYSTEM,TEST\Domain Admins,TEST\Helpdesk
```

I

LAPS (Local Administrator Password Solution)

7 Publish LAPS.x64.msi Via GPO On Destination Clients

Copy LAPS.x64.msi to \\test.local\SYSVOL\test.local\scripts

Gpmc.msc → Computer Configuration → Software Setting → Software Installation (New Package) → Select UNC Path LAPS.x64.msi and Assign (UNC Path: \\test.local\SYSVOL\test.local\scripts)

Gpmc.msc → Computer Configuration → Administrative Templates → LAPS

1	Password Seeting	Password Complexity	Default: Large letters + small letters + numbers + special
		Password Length	Default: 14 characters
		Password Age	Default: 30 days
2	Name of Administrator account to Manage	Administrator account name	testadmin in my Example
3	Don't allow Password expireation time longer than required by policy	When such expiration is detected, password is changed immediately and password expiration is set according to policy	Not Configure
4	Enable Local Admin Password Mnagement		Enable LAPS

8 3 way to view Local Administrator Password Clients

1. From LAPS UI Application
2. From Power shell Get-AdmPwdPassword <Client NetBIOS Name>
3. From ClientComputerAccount/Attribute Editor/ → ms-Mcs-AdmPwd And ms-Mcs-AdmPwdExpiretion Time

9 Reset Local administrator Password

1. From Power shell Reset-AdmPwdPassword <Client NetBIOS Name>
2. Restart the client (after restart client's password is Changed)

II

MSA (Manage Service Account)

- برای اینکه به یک سرویس مانند SQL یک User Account اکانت نسبت دهیم از SPA استفاده میکنیم و از این سرویس عمدتا برای ارتباط بین دستگاه های سفت افزاری یا سرویس های نرم افزاری با دامین استفاده میشود البته بشرط سازگار بودن
- این سرویس از یک جنبه مانند User Account می باشد ولی از بابت اینکه بصورت اتوماتیک رمزش عوض میشود شبیه Computer Account می باشد و از طریق Powershell ساخته میشود
- بعد از ساخته شدن SPA از طریق Manage Service Accounts در AD Users And Computers قابل دسترس است

On DC

1. Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10) → چون EffectiveTime بصورت پیش فرض ۱۰ ساعت بعد کلید را تولید میکند بدین شکل در لحظه کلید تولید میشود
2. Repadmin /syncall & Repadmin /Replsum → جهت Sync شدن کلیدها بین دامین کنترلرهای مختلف
3. New-ADServiceAccount -Name MSA-SCCM-SQL -DNSHostName MSA-SCCM-SQL.Domaint.com -PrincipalsAllowedToRetrieveManagedPassword sccm-sql$

MSA-SCCM-SQL: Service Account Name
MSA-SCCM-SQL.Domaint.com: Service Account FQDN Name
sccm-sql$: نام کامپیوتری که میخواهد از این سرویس استفاده کند

On SQL Server SCCM-SQL

1. Install Powershell For AD DS → Install Active directory module fo windows Powershell (Select Server role Features)
2. Install-ADServiceAccount MSA-SCCM-SQL
3. Test-ADServiceAccount MSA-SCCM-SQL → Return True

- حال از طریق Services.msc سرویس مد نظر را به از طریق Logon tab به Service Account Name نسبت میدهیم
  Mark This account on Logon tab and insert domain\MSA-SCCM-SQL$ و قسمت رمز را نیز خالی میگذاریم
- باید حتما سرویس با این نوع اکانت سازگار باشد بطور مثال در موقع نصب SQL میتوان از این نوع اکانت استفاده نمود

Top 10 Most Important Group Policy Settings for Preventing Security Breaches

Moderating Access to Control Panel

Setting limits on a computers' Control Panel creates a safer business environment. Through Control Panel, you can control all aspects of your computer. So, by moderating who has access to the computer, you can keep data and other resources safe. Perform the following steps:

1

Gpmc.msc → User Configuration → Administrative Templates → Control Panel → **Prohibit access to Control Panel and PC settings**

Prevent Windows from Storing LAN Manager Hash

Windows generates and stores user account passwords in "hashes." Windows generates both a LAN Manager hash (LM hash) and a Windows NT hash (NT hash) of passwords. It stores them in the local Security Accounts Manager (SAM) database or Active Directory. The LM hash is weak and prone to hacking. Therefore, you should prevent Windows from storing an LM hash of your passwords. Perform the following steps to do so:

2

Gpmc.msc → Computer Configuration → Windows Setting → Security Setting → Local Policies → Security Options → **Network security: Do not store LAN Manager hash value on next password change**

Control Access to Command Prompt

Command Prompts can be used to run commands that give high-level access to users and evade other restrictions on the system. So, to ensure system resources' security, it's wise to disable Command Prompt. After you have disabled Command Prompt and someone tries to open a command window, the system will display a message stating that some settings are preventing this action. Perform the following steps:

3

Gpmc.msc → User Configuration → Administrative Templates → System → **Prevent access to the command prompt**

Important about Windows Update

Forced system restarts are common. For example, you may face a situation where you were working on your computer and Windows displays a message stating that your system needs to restart because of a security update. In many cases, if you fail to notice the message or take some time to respond, the computer restarts automatically, and you lose important, unsaved work. To disable forced restart through GPO, perform the following steps:

4

Gpmc.msc → Computer Configuration → Administrative Templates → Windows Component → Windows Update →

Configure Automatic Update
Specify intranet microsoft update service location
No auto-restart with logged on users for scheduled automatic updates installations
Automatic update detection frequently
Turn off upgrade to last version of windows through windows update
Allow none administrators to receive update notification
Turn on recommended update from automatic update

Disallow Removable Media Drives, DVDs, CDs, and Floppy Drives

Removable media drives are very prone to infection, and they may also contain a virus or malware. If a user plugs an infected drive to a network computer, it can affect the entire network. Similarly, DVDs, CDs and Floppy Drives are prone to infection. It is therefore best to disable all these drives entirely. Perform the following steps to do so:

5

Gpmc.msc → User Configuration → Administrative Templates → System → Removable Storage Access →

CD and DVD Deny Read/Write Access
Custom Classes Read/Write Access
Removable Disk Read/Write Access
All removable storage classess :deny All Classes
WPD Devices Read/Write Access

Top 10 Most Important Group Policy Settings for Preventing Security Breaches

Restrict Software Installations

When you give users the freedom to install software, they may install unwanted apps that compromise your system. System admins will usually have to routinely do maintenance and cleaning of such systems. To be on the safe side, it's advisable to prevent software installations through Group Policy:

6

Gpmc.msc → Computer Configuration → Administrative Templates → Windows Component → Windows Installer → **Prohibit User Install**

Disable Guest Account

Through a Guest Account, users can get access to sensitive data. Such accounts grant access to a Windows computer and do not require a password. Enabling this account means anyone can misuse and abuse access to your systems. Thankfully, these accounts are disabled by default. It's best to check that this is the case in your IT environment as, if this account is enabled in your domain, disabling it will prevent people from abusing access:

7

Gpmc.msc → Computer Configuration → Windows Setting → Security Setting → Local Policies → Security Options → **Accounts: Guest Account Status**

Set Password And Lockout Policy Limits

Set the minimum password length to higher limits. For example, for elevated accounts, passwords should be set to at least 15 characters, and for regular accounts at least 12 characters. Setting a lower value for minimum password length creates unnecessary risk. The default setting is "zero" characters, so you will have to specify a number:

If you set the password expiration age to a lengthy period of time, users will not have to change it very frequently, which means it's more likely a password could get stolen. Shorter password expiration periods are always preferred. Windows' default maximum password age is set to 42 days

8

9

Gpmc.msc → Computer Configuration → Windows Setting → Security Setting → Account Policies → Password Policies → Password:
- **Enforce password history**
- **Maximum password age**
- **Minimum password age**
- **Minimum password length**
- **Minimum password length audit**
- **Password must meet complexity requirements**

Lockout:
- **Account lockout duration**
- **Account lockout threshold**
- **Reset account lockout counter after**

Disable Anonymous SID Enumeration

Active Directory assigns a unique number to all security objects in Active Directory; including Users, Groups and others, called Security Identifiers (SID) numbers. In older Windows versions, users could query the SIDs to identify important users and groups. This provision can be exploited by hackers to get unauthorized access to data. By default, this setting is disabled, ensure that it remains that way. Perform the following steps:

Gpmc.msc → Computer Configuration → Windows Setting → Security Setting → Local Policies → Security Options → **Network Access: Do not allow anonymous enumeration of SAM accounts and shares**

10

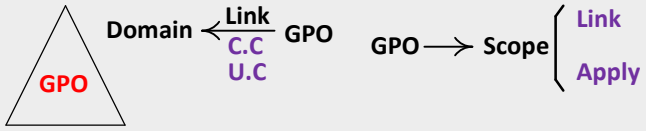
I

Policy

- اگر یک پالیسی نتواند بدرستی کار کند و بخشی از اجزای آن اشتباه کانفیگ شده باشد میتواند باعث کند شدن کامپیوتر ها در موقع بوت ویندوز شود
- برای اینکه یک کلاینت متوجه یک پالیسی شود باید در سمت کلاینت Client Side Extention (CSE) آن پالیسی را داشته باشیم بدین معنی که کلاینت باید از طریق CSE آن پالیسی متوجه دستور ارسال شده از طریق پالیسی بشود
- مجموعه پالیسی هایی که در قسمت Preferences وجود دارند قبلا در ویندوز قبل از ۲۰۰۸ توسط شرکت های 3rd Party بصورت Script در GPO اجرا میشدند
- برای اینکه یک اسکریپت در قسمت Preferences فقط یکبار برای هر کلاینت انجام شود پس از تنظیمات پالیسی در تب Common گزینه Apply Once and don't reapply را فعال میکنیم
- در قسمت Computer Configuration/windows Setting/security setting/System Services تنظیمات مربوط به سرویس های ویندوز میباشد
- اگر برای تنظیم یک پالیسی خط چین قرمز در زیر آن بود باید با زدن کلید F5 به خط ممتد سبز آن را تبدیل کنیم تا پالیسی اعمال شود بطور مثال User Configuration/Preferences/control panel/Internet setting/Home page

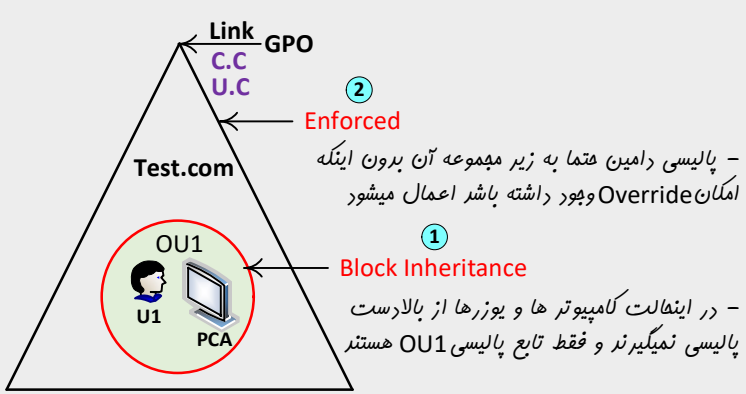
II

Pre GPO Filtering

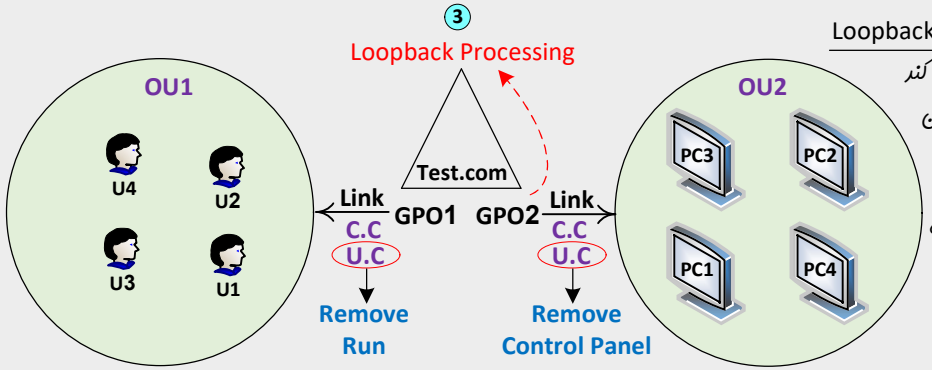


- در حالت معمول Link , Scope = Apply , Scope است حال میتوان Link , Scope را بزرگتر از Apply , Scope کرد

Link Scope (> or =) Apply Scope



- پالیسی دامین هتما به زیر مجموعه آن بدون اینکه امکان Override وجود داشته باشد اعمال میشود
- در اینحالت کامپیوتر ها و یوزرها از بالادست پالیسی نمیگیرند و فقط تابع پالیسی OU1 هستند



حالت اول بدون اعمال Loopback Processing

- اگر U1 از دستگاه PC1 به دامین Log on کند
- U1 فارغ از اینکه از چه کامپیوتری به دامین وصل شود Run نخواهد داشت
- U1 مطمئنا Control Panel خواهد داشت چون کاربر متعلق به OU2 نیست و در Link , Scope نیست

- Loopback Processing دارای دو حالت Merge Mode و Replace Mode میباشد

حالت دوم با اعمال پالیسی Loopback Processing

Merge Mode

- این پالیسی دربخش Computer Configuration قرار دارد و روش کار آن بدین شکل است که در یک مرحله فارغ از اینکه چه کاربری ممکن است به آن متصل شود حال چه بشکل دامینی یا به شکل Local هر دو Computer Configuration و User Configuration را یکجا Apply میکند و تمایزی بین کاربری که ممکن است به آن وصل شود قائل نمیشود بنابراین در اینحالت اگر کاربر U1 به کامپیوتر PC1 وصل شود نه کنترل پنل دارد و نه Run menu در واقع تفاوتی بین C.C و U.C در OU2 قائل نمیشود و OU1 , U.C با OU2 , U.C حالت Merge پیدا میکند ضمنا قابل ذکر است که اگر تضادی بین OU2 , U.C که این پالیسی در آن فعال شده و OU1 , U.C پیش بیاید اولویت با OU2 , U.C است

حالت دوم با اعمال پالیسی Loopback Processing

Replace Mode

- عملکرد این حالت با حالت Merge یکسان است به جز اینکه OU2 , U.C جایگزین OU1 , U.C یا به تعبیر دیگر Replace میشود

Gpmc.msc → Computer Configuration → Administrative Templates → System → Group Policy → Configure User Group Policy Loopback Processing Mode

Other Useful Policies for Policy:
- Turn off Background refresh of group policy
- Set group policy refresh of group policy
- Configure logon script delay
- Set group policy refresh interval for domain controller

I

Pre GPO Filtering

4 Slow Link Detection

- فرض بر اینکه از طریق پالیسی Software Installation مبادرت به نصب نرم افزارPDF Reader از طریق C.C نموده ایم حال اگر پهنای باند کامپیوتری که از طریق شبکه میخواهد پالیسی را دریافت کند پایین باشد میتوانیم این پالیسی را در شرایطی که پهنای باند پایین باشد فیلتر نمائیم و پیش فرض آن بدین شکل میباشد که پهنای باند برابر یا کمتر از 500K راکه Detect نموده ضعیف تلقی کرده و از اعمال یکسری پالیسی از جمله Software Installation صرف نظر میکند

- برای تعیین عدد لینک ضعیف باید GPO مورد نظر را Edit نمائیم

Gpmc.msc → Computer Configuration → Administrative Templates → System → Group Policy → Configure Group Policy Slow link detection

- این پالیسی تا ویندوز ۲۰۰۳ از پرتکل ICMP با استفاده از RTT (Round Trip Time=TTL in ms) برای تشخیص تخمینی پهنای باند استفاده میکرد و در ویندوزهای بالاتر از روش NLA (Network Location Awareness) استفاده میکند که یک قابلیت لایه ۳ OSI Network میباشد و با نام Network Location Awareness یک سرویس در ویندوز فعال می باشد نکته اینکه DHCP Client از این سرویس نیز استفاده میکند

II

GPO Filtering

- در مورد GPO Filtering دو تکنیک وجود دارد

1 Security Filtering ← AD Permission

2 WMI Filtering ← Dynamic Filtering

1 Security Filtering (AD Permission)

- کامپیوتر ها و کاربران برای دسترسی به GPO باید AD Permission داشته باشند که شامل ویژگی Read و Apply GP(Group Policy) می باشد در نتیجه با فیلترکردن Apply GP امکان اعمال پالیسی فیلتر میشود
- وقتی یک GPO ساخته میشود بصورت پیش فرض فقط گروه Authenticated Users است که دسترسی Read و Apply GP را به GPO دارد
- وقتی بر روی یک GPO کلیک مینمائیم در سمت راست از طریق تب Delegation به Security Setting آن GPO دسترسی خواهیم داشت و اگر Apply GP را Unmark کنیم حتی اگر پالیسی را لینک دهیم اعمال نخواهد شد
- با Apply GP , unmark از Authenticated Users و Mark کردن Read و Apply GP برای کاربران و گروه های خاص در GP اولین نوع فیلترینگ مبتنی بر AD Permission انجام میگردد
  - 1 مجموع پالیسی ها به هیچ کسی اعمال نشود و برفی مستثنی شوند
  - 2 مجموع پالیسی ها به همه اعمال شود و برفی مستثنی شوند
- با Deny کردن Apply GP برای گروه یا کاربران خاص و نگه داشتن حالت پیش فرض Read و Apply GP برای Authenticated Users نوع دوم فیلترینگ مبتنی بر AD Permission انجام میگردد
- برای Security Filtering بر روی یک GPO وقتی بر روی آن کلیک میکنیم در پنل سمت راست بخش Security Filtering داریم که از آن استفاده نمیکنیم چون بصورت کامل فیلترها را نشان نمیدهد بلکه از Delegation استفاده میشود

III

2 WMI Filtering(Dynamic Filtering)

- فرض کنیم که یک پالیسی داریم که میخواهیم به فقط تمام ویندوزهای ۷ اعمال شود راه حل اول اینست که از روش Security Filtering استفاده کرده و یک گروه بسازیم که شامل کامپیوترهایی باشد که ویندوز ۷ دارند و دسترسی Apply GP را از گروه Authenticated Users بگیریم و دسترسی Read و Apply GP را به گروه مد نظر بدهیم ، را حل دوم استفاده از WMI Filtering میباشد که بصورت پویا و دینامیکی کامپیوترهای ویندوز ۷ را مشخص میکند
- Windows Management Instrumentation (WMI) در ویندوز کاربردهای زیادی دارد از جمله مانیتورینگ و پالیسی فیلترینگ ، WMI شامل تعداد بسیار زیادی متغییر Variable می باشد اگر بتوانیم از مقادیر متغییر ها مطلع شویم عملا مانیتورینگ را انجام داده ایم و اگر بتوانیم مقادیر متغیر ها را تغییر دهیم مدیریت را لحاظ کرده ایم ، با زدن دستور wmic در Powershell,CMD میتوانیم اطلاعات WMI ها را بدست آوریم بطور مثال wmic:root\cli>memorychip
- زبان WMI Query Language (WQL) مربوط به استخراج داده از دیتابیس WMI میباشد و کاملا شبیه SQL Query میباشد

```
select * from Win32_OperatingSystem WHERE Version LIKE "10.%" AND (ProductType = "2" or ProductType = "3" )
select * from Win32_OperatingSystem WHERE Version like "6.3%" AND ProductType="1" AND OSArchitecture = "32-bit"
Select * from Win32_Processor where AddressWidth = "64"
select Version from Win32_OperatingSystem WHERE Version like “10.0.17134” AND ProductType=”1”
SELECT Model FROM Win32_ComputerSystem WHERE Model = “VMWare Virtual Platform”
Select * from WIN32_ComputerSystem where TotalPhysicalMemory >= 1073741824
```

```
Windows versions:
Windows Server 2016 and Windows 10 — 10.%
Windows Server 2012 R2 and Windows 8.1 — 6.3%
Windows Server 2012 and Windows 8 — 6.2%
Windows Server 2008 R2 and Windows 7 — 6.1%
Windows Server 2008 and Windows Vista — 6.0%
Windows Server 2003 — 5.2%
Windows XP — 5.1%
Windows 2000 — 5.0%
```

```
ProductType=1 – any desktop Windows edition;
ProductType=2 – Active Directory domain controller;
ProductType=3 – Windows Server.
```

I

- برای فعال کردن WMI Filtering بر روی یک GPO بدین شکل عمل میکنیم
- ابتدا WMI مورد نظر را تعریف میکنیم و بعد به پالیس مورد نظر از قسمت WMI Filtering نام WMI را به پالیسی نسبت میدهیم

Gpmc.msc → Domains → Test.local → WMI Filters → New → Insert name and add query

- جهت تست WQL میتوان از نرم افزار WMI explorer استفاده نمود ، همچنین از طریق Powershell یا CMD نیز امکان تست WQL میسر است

https://www.ks-soft.net/hostmon.eng/wmi/index.htm → Wmiexplorer

- امکان استفاده از WMI Filtering در پالیسی هایی که فقط در قسمت Preferences هستند تسهیل شده است بدین صورت که در تب Common این پالیسی ها گزینه ای به نام Item-Level Targeting اضافه شده که همان WMI Filtering میباشد وتعدادی از مهمترین WQL ها بصورت گرافیکی در آن لیست شده است ، ضمن اینکه با انتخاب WMI Query میتوانیم WQL دلخواه خود را درج نمائیم

II

Folder Redirection

Documents
Desktop
Downloads
⋮
→ Redirect → File server

- بطور پیش فرض Desktop در سیستم ها در آدرس C:\users\%users%\desktop قرار دارد حال میتوانیم این فولدر را Redirect به مکانی دیگر بکنیم
- این امکان همانطور که دروس پیشین به آن اشاره شد بصورت Locally امکان پذیر است ولی میتوان از طریق پالیسی نیز این مهم را میسر نمود بنابراین میتوان از طریق پالیسی به محل های متغییر کاربران را Redirect نمود
- از طریق پالیسی فیلترینگ میتوان فقط فولدرهای برخی کاربران را Redirect نمود
- در داخل فولدر به اشتراک گذاشته شده Desktop برای هر کاربر یک desktop\%users%\desktop میسازد و محتویات قبلی را به محل جدید انتقال می دهد

Gpmc.msc → Policies → Windows Setting → Folder Redirection → Desktop Properties → Setting Basic → Target Path (fileserver\desktop)

III

Software Installation

Computer Configuration (Assign)

Read Permission

Installation .msi & .mst File → PCs

SDP(Session Description Protocol)

Modification استفاده کنیم به تب Advance

MSI (Microsofte installer)
MST (Microsofte Transform)

- زمانی که از این ویژگی از طریق Computer Configuration استفاده میکنیم دو حالت Assign و Advance داریم و تفاوت آن در این است که اگر از حالت Advance دسترسی خواهیم داشت و میتوانیم فایلهای .mst را اضافه کنیم که حاوی Configuration options جهت سفارشی نصب کردن فایل .msi می باشد
- رفتار نصب یک فایل msi. میتواند از طریق یک یاچند فایل mst. تغییر پیدا کند
- در هنگام Remove کردن یک فایل msi. از Software Installation باید دقت کنیم که دوحالت داریم که بصورت پیش فرض فایل نصب شده را از سیستم ها پاک میکند و حالت دوم که با نرم افزارهای نصب شده بر روی سیستم ها کاری ندارد
- فایل msi. باید ساختار مناسب برای نصب اپلیکیشن از طریق Software Installation را داشته باشد پس به صرف داشتن پسوند msi. هر فایلی قابل نصب از طریق Software Installation نیست

User Configuration (Assign)

- در این حالت پالیسی به غیر از فایلهای msi. میتوان از فایلهای متنی zero-hour auto purge (ZAP) نیز استفاده نمود حال از حالت Assign یا Published و Advance استفاده نمود

Assign(msi) / Publish(msi , zap)

- در حالت Assign وقتی فایل msi. نصب میشود حالت ظاهر سازی دارد یعنی ما برنامه را میبینیم ولی عملا نصب نشده است و در دو حالت نصب میشود اول اینکه روی فایلی که مرتبط با آن برنامه هست کلیک کنیم و دوم اینکه از طریق Program & features\install a program fron the network در لیست نصب اپلیکیشن قرار میگیرد در بعضی مواقع ممکن است فایل msi. با توجه به ویژگی آن نصب نیز شره باشد

User Configuration (Publish)

- در حالت Publish هم برای msi. و هم برای exe. نیز استفاده میشود ولی برای فایلهای exe. باید از روی این فایلها یک فایل متنی بسازیم و پسوند آن فایل را به exe. تغییر میدهیم
- در حالت Publish برای کاربران ظاهر سازی نیز نمیشود ولی میتوان اپلیکیشن را از طریق Program & features\install a program fron the network نصب نمود
- نصب اپلیکیشن برای هر دو حالت Publish و Assign مرتبط با کاربری است که دسترسی و مجوزلازم برای نصب را داشته باشد
- بصورت معمول نیاز به بخش [ext] نیست و از طریق کنترل پنل میتوان فایل exe. را نصب نمود ولی اگر این بخش به فایل zap. اضافه شود باعث میگردد تا اگر در ویندوز بر روی فایلی با این پسوند ها کلیک شد برنامه نصب گردد

ZAP File Structure

```
[Application]
FriendlyName = "Microsoft Excel 97"
SetupCommand = \\servername\sharename\Excel 97\setup.exe
DisplayVersion = 20
Publisher = Microsoft
URL = http://www.microsoft.com/office
```

```
[ext]
XLS=
XLA=
XLB=
XLC=
XLM=
XLV=
XLW=
```

I — Software Restriction

- از این پالیسی در هر دو حالت Whitelist و Blacklist میتوان استفاده نمود و برای اینکه اپلیکیشنهای خاصی بر روی سیستم اجرا شوند یا نشوند استفاده میشود نکته اینکه این پالیسی فقط بر روی فایلهای اجرائی کار میکند
- این پالیسی هم در Computer Configuration و هم در User Configuration وجود دارد

پالیسی براساس اینکه چه کاربری به آن وصل میشود
Gpmc.msc → Software Configuration → Windows Setting → Security Setting → Software restriction

پالیسی برروی کامپیوتر فارغ از اینکه چه کاربری به آن وصل میشود
Gpmc.msc → Computer Configuration → Windows Setting → Security Setting → Software restriction

1 — Security levels
- Disallow ← هیچ فایل اجرائی اجرا نشود
- Basic User ← فقط برنامه هایی که نیاز به مجوز administrator ندارند اجرا میشوند
- Unrestricted ← همه فایلهای اجرائی اجرا شوند

+

2 — Additional rules
- New certificate rule
- New Hash Rule ← - در اینحالت بر اساس محتوای فایل تصمیم گیری میشود و اگوی فایل را برای محدودیت مد نظر قرار میدهد ولی مثلا اگر نسخه یک فایل عوض شود محتوی عوض شده و این پالیسی از کار می افتد
- New network zone rule
- New Path Rule ← - اگر مسیر بدهیم فقط برنامه های اجرائی در مسیر ذکر شده محدود میشوند و اگر برنامه ها به مسیر دیگری انتقال داده شود پالیسی از کار می افتد

- در صورت وجود تعارض بین New Hash Rule و New Path Rule اولویت با New Hash Rule میباشد

II — AppLocker

- شکل توسعه یافته Software Restriction پالیسی AppLocker میباشد که از ویندوز ۲۰۰۸ و ۷ به بعد کار میکند
- در AppLocker مشکل Hash Rule را نداریم و عملا هیچ نسخه ای از برنامه اشاره شده فعال نخواهد بود
- AppLocker در صورتی کار میکند که سرویس Application Identity بر روی کامپیوتر هایی که پالیسی را دریافت میکنند فعال باشد بنابراین از فعال بودن این سرویس قبل از اعمال AppLocker باید مطمئن شویم

Gpmc.msc → Computer Configuration → Preferences → Services → Application Identity

Gpmc.msc → Computer Configuration → Windows Setting → Security Setting → Application Control →
- Script rule
- Package app rules
- Executable Rule
- Windows Installer Rule

- اصولا به جای این پالیسی از DLP یا End Point Protection استفاده میشود و نکته اینکه بر روی سیستمها با کمی تاخیر نتیجه پالیسی نمایان می گردد

III — GPO Planning

Default Domain Policy

Default Domain Controller Policy

- نکته اول در طراحی پالیسی اینست که به دو پالیسی پیش فرض که در سیستم وجود دارد کاری نداریم و فقط برخی پالیسی های خاص را که برای کل دامین عمومیت دارد را بر روی آنها اعمال میکنیم
- همانطور که همه پالیسی را در دل یک GPO تعریف نمیکنیم به ازای هر پالیسی هم یک GPO تعریف نمیکنیم بلکه پالیسی ها را دسته بندی کرده و به GPO نسبت میدهیم دسته بندی پالیسی ها بر اساس یک وجه مشترک انجام میشود مثلا بر اساس این هدف که تنظیمات یک مرورگر وب انجام شود ، تعدادی پالیسی بصورت مشترک به یک GPO نسبت داده میشود که این نوع طراحی Role Design نامیده میشود ممکن است مجموعه پالیسی غیر مرتبط به هم را از طریق یک GPO بطور مثال به OU یک واحد سازمانی نسبت دهیم به اینحالت Team Design میگویند مثلا پالیسی منشیهای سازمان یا لپ تاپ های سازمان
- لینک دادن یک پالیسی آخرین کاری است که بعد از تعریف پالیسی و کانفیگ آن و فیلترینگ پالیسی انجام میشود

I

RSoP (Resultant Set of Policy)

- دارای دو مد میباشد یکی مد Tshoot میباشد که با بررسی منشاء پالیسی صحت عملکرد پالیسی را مشخص میکنیم که از طریق تایپ دستور RSOP در محیط CMD یا RSOP.msc در Run بدست می آید
- یکی از روشهای متداول RSOP استفاده از Dsa.msc در AD میباشد بدین شکل که با کلیک بر روی نام کاربر یا نام کامپیوتر و سپس All Task\RSoP (logging) پالیسی های اعمال شده و منشاء آن مشخص میشود
- وقتی RSOP ساخته شد از طریق R-click\properties\Precedence یا Source GPO میتوانیم منشاء پالیسی را ببینیم
- برای بدست آوردن RSOP باید حتما یک کاربری قبلا به آن سیستم لاگین کرده باشد
- میتوان RSOP Snap-in را نیز به یک کنسول اضافه نمود
- مد Modeling Planning برای موقعی استفاده میشود که فرضا اگر کاربر را از یک گروه یا OU در آوریم و عضو گروه یا OU دیگری کنیم شرایط پالیسی به چه شکل خواهد شد در اینحالت میتوانیم وضعیت یک کاربر را در ارتباط با گروه یا OU های متفاوت در دامین بسنجیم و برایند پالیسی ها را ببینیم در ارتباط با تغییرات گروه چون Permission تغییر میکند عملکرد پالیسی تحت الشعاع قرار میگیرد All Task\RSoP (Planning)
- در مد Planning میتوان مجموعه اجزاء دخیل در پالیسی را بصورت متغییر و کلی مشخص نمود و بصورت تنظیم مجموعه اگر ها استفاده میشود بطور مثال اگر کاربری در دامین یا گروه یا OU مشخصی به یک کامپیوتر یا مجموعه کامپیوترهای موجود در یک گروه یا OU مشخص وصل شود چه پالیسی خواهد داشت

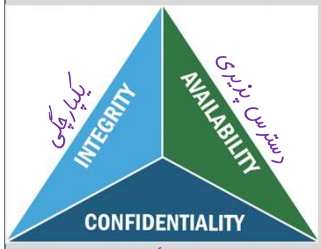
II

مدل مثلث امنیت

CIA Triad Security → Authentication → Server Authentication → Certificate

پس هرجا بحث امنیت باشد بحث Certificate نیز هست

Certificate گواهینامه الکترونیکی



Integrity

- Integrity یعنی مطمئن باشیم فایلی که دانلود کرده ایم همان فایلی است که در فایل سرور موجود بوده است و بین راه هیچگونه تغییری در آن صورت نپذیرفته است

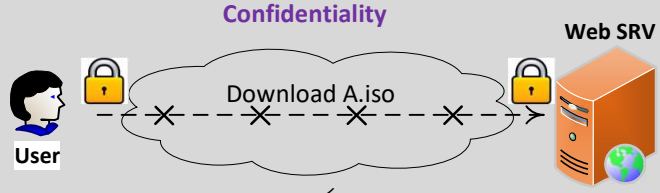
A

Availibility

- اگر مصداق مثلث امنیت را یک وب سایت یا ایمیل سرور بگذاریم یعنی یک سرویس
- با توجه به هزینه بسیار بالای برخی از افزونگی ها ارزش و عدد در دسترس پذیری Availibility سنجیده می شود
- در هر ۱۰۰ روز مجموعا ۲۴ ساعت معادل یکروز خارج از دسترس قابل قبول است → 99
- در هر ۱۰۰ روز مجموعا یک دهم روزخارج از دسترس قابل قبول است → 99.9
- در هر ۱۰۰ روز مجموعا یک هزارم روزخارج از دسترس قابل قبول است در این حالت حتما باید افزونگی را در نظر گرفت → 99.999
- مواردی ازقبیل DDOS , SPOF باعث میشود Availibility کاهش پیدا کند

B

Confidentiality



- Confidentiality یعنی مطمئن باشیم که تبادل اطلاعات بصورت محرمانه انجام میگیرد و کسی در بین مسیر امکان بازگشایی اطلاعات رمز شده را ندارد و فقط اطلاعات را دست به دست میکند

Encryption

- به دانش تولید الگوریتم های رمز نگاری Cryptography گفته میشود و به انجام عمل رمز نگاری Encryption گفته میشود
- محرمانگی با رمزنگاری پیاده سازی میشود و شامل اجزاء Component زیر میباشد

① Cleartext , Plain text + ② Key + ③ Function (Algorithm) f(x) → ④ Cipher Text

① Cipher Text + ② Key + ③ Function (Algorithm) $f^{-1}(x)$ → ④ Plain text

محرمانگی

- همانطور که مشخص است در محرمانگی دو فاکتور تابع ریاضی و کلید نقش دارند که کلید نقش برجسته و پررنگتری بین این دو دارد چون تابع ریاضی در دسترس همگان میباشد و این کلید است که محرمانگی را به همراه می آورد

Encryption

① Two Way Encryption (Encrypt ⟷ Decryption)

- امکان رمزبرداری وجود دارد و برگشت پذیر است

① Symetric (Common key or Secret Key)

- متقارن در کلید یعنی همان کلیدی که برای رمز نگاری استفاده میشود برای رمزبرداری نیز استفاده میشود

② Asymetric (Private Key & Public Key=Key Pair)

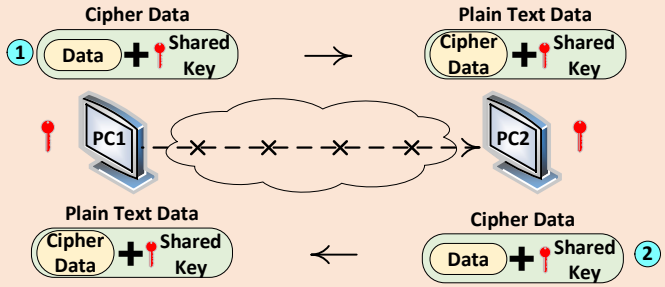
- نامتقارن در کلید یعنی دارای یک جفت کلید خصوصی و عمومی هستیم که مکمل همدیگرند بدین معنی که با هر کدام از کلیدها رمزنگاری شود با کلید دیگر رمز برداری میشود و قاعده کار بدین شکل است که کاربر کلید خصوصی را به هیچ عنوان از خود جدا نمیکند و صرفا کلید عمومی را برای همگان به اشتراک میگذارد حال اگر بخواهد بصورت رمز شده اطلاعاتی را برای کاربر مقابل بفرستد با کلید عمومی کاربر طرف مقابل اطلاعات را رمز میکند و در سمت دیگر آن کاربر با کلید خصوصیش اطلاعات را رمز برداری میکند و بالعکس

② One Way Encryption (Hashing)

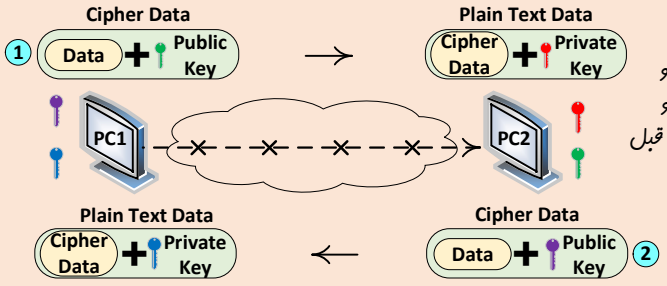
- امکان رمزبرداری وجود ندارد و برگشت پذیر نیست

I

Symetric Encryption

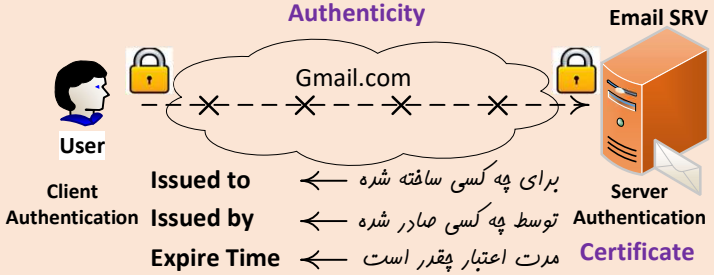


Asymetric Encryption



- در اینحالت اگر در وسط راه کسی کلیدهای عمومی خودش را با ترفندی به دو طرف ارتباط معرفی کند میتواند مهرمانگی را از بین برده و خودش را جایگزین دو طرف ارتباط نماید پس فقط رمزنگاری فاقی مهرمانگی به ارمغان نمی آورد بلکه قبل از آن نیازمند احراز هویتAuthenticity هستیم
- Authenticity در درون Confidentiality قرار دارد

Authenticity



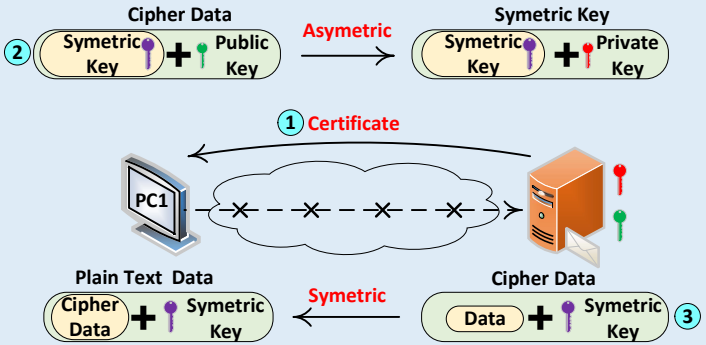
- Client Authentication یعنی کلاینت خودش را به سرور بشناساند و Server Authentication یعنی سرور خودش را به کلاینت بشناساند و در این ارتباط لایه ۷ ابتدا سرور خودش را به کلاینت میشناساند و معمولا کلاینت اگر نیاز باشد با نام کاربری و رمز عبور خودش را به سرور میشناساند
- در مورد شناساندن سرور به کلاینت میتواند Computer Account مورد استفاده قرار بگیرد که مصرف داخلی دارد و در شبکه دامین مرل استفاده میشود و همچنین کاربر نیز با User Account خودش را به سرور میشناساند و این تعاملات از طریق Kerberos انجام میشود
- بعضی اوقات ارتباط بین اجزاء مختلف از طریق Preshared Key انجام میشود
- روشی که همواره و تحت هر شرایطی میتواند استفاده شود Certificateمی باشد

II

PKI (Public Key Infrastructure)

- به فرایندی گفته میشود که باعث تولید و توزیع و مدیریت کلید خصوصی و عمومی میشود بدون اینکه امکان سو استفاده از کلید عمومی میسر باشد و بخشی از موضوع مدیریت به بکاپ گیری و ابطال Revoke کلید بر میگردد
- اگر کامپیوتری ابتدا Certificate را برای شناساندن خود به کامپیوتر دیگر و جهت احراز هویت ارسال کند و سپس در فاز بعدی کلید عمومی را ارسال کند باز نیز این نکته وجود دارد که در بین راه افرادی کلید عمومی را عوض نمایند و خود را بجای کامپیوتر فرستنده جا بزنند پس باید ارسال Certificate و کلید عمومی در قالب یک فاز ارسال شود نهایتا این موضوع برین شکل حل میشود که همراه با **Certificate** و در درون آن کلید عمومی نیز مبادله میشود
- در تب Details مجموعه اطلاعات مرتبط با Certificate از جمله کلید عمومی نیز وجود دارد
- هزینه استفاده از الگوریتمهای Asymetric بسیار بالا میباشد بدین معنی که مصرفCPU بالایی دارند و برق زیادی مصرف میکنند و برای تبادل اطلاعات استفاده نمیشود و به جای آن از الگوریتم symetric استفاده میشود

Asymetric+Symetric



Some examples of symmetric encryption algorithms include:
AES (Advanced Encryption Standard)128,256bit
DES (Data Encryption Standard)56bit,3DES-168bit
IDEA (International Data Encryption Algorithm)
TLS/SSL protocol
Blowfish (Drop-in replacement for DES or IDEA)
RC4 (Rivest Cipher 4)
RC5 (Rivest Cipher 5)
RC6 (Rivest Cipher 6)

Examples of asymmetric encryption include:
Rivest Shamir Adleman (RSA)
the Digital Signature Standard (DSS),
which incorporates the Digital Signature Algorithm (DSA)
Elliptical Curve Cryptography (ECC)
the Diffie-Hellman exchange method
TLS/SSL protocol

Examples of Hash encryption include:
SHA 0,1(160bit),2(256,384,512bit)
MD5
HAVAL
RIPEMD320
Gost
Whirlpool
CRC

I

1) If $F(x)=y \not\Rightarrow F^{-1}(y)=x$ تابع برگشت ناپذیر است

2) If $F(1bit)=128bit \Rightarrow F(1TB)=128bit$ حجم دیتای خروجی همواره ثابت است

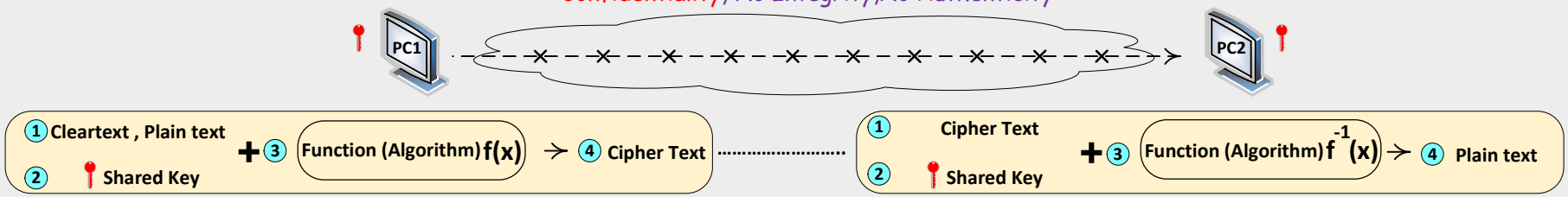
3) If $F(a)=c \ \& \ F(b)=c \Rightarrow a=b$

One Way Encryption (Hashing)

- در Hashing فقط الگوریتم یا همان تابع ریاضی را داریم و کلیدی استفاده نمیشود قابل ذکر است که الگوریتم Hashing باید سه قابلیت داشته باشد
- به خروجی Hashing اصطلاحا **Digest** گفته میشود از این الگوریتم جهت **Integrity** استفاده میشود

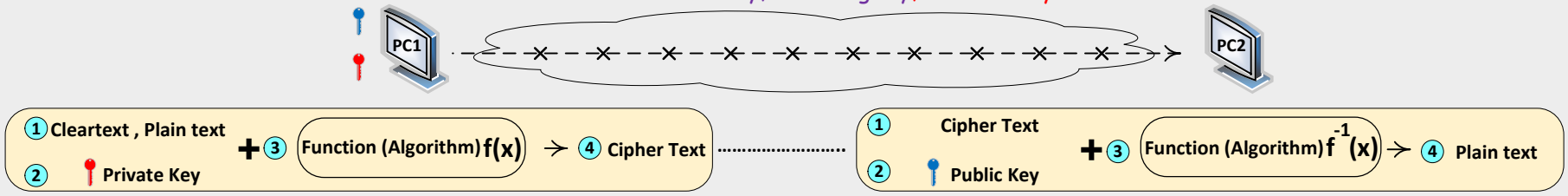
- فرض که کاربر میخواهد یک فایل ISO از سایت دانلود کند جهت اطمینان از اینکه فایلی که دانلود میشود حتما همان فایلی است که در سایت به اشتراک گذاشته شده است بدین روش عمل میشود ابتدا وب سرور فایل ISO را از طریق یک الگوریتم Hashing مثلا Sha1 مقدار Digest آن را محاسبه کرده و در کنار دانلود فایل آن را نیز ارائه میدهد سپس دریافت کننده با استفاده از همان الگوریتم اگر به Digest برابر با سایت برسد مطمئن خواهد بود که فایل در طول مسیر عوض نشده است و یکپارچگی حفظ شده است

Confidentiality, No Integrity,No Authenticity



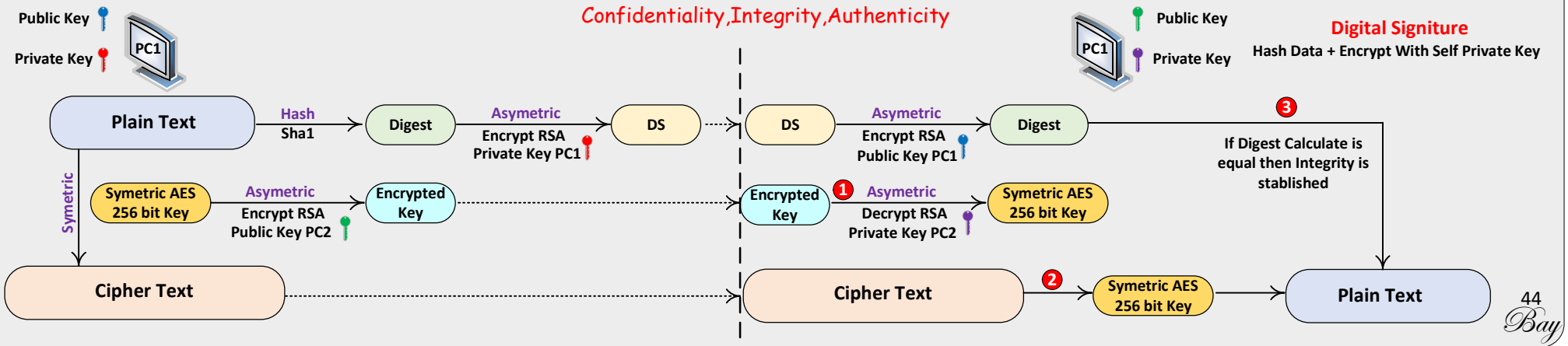
- وقتی نمیتوان محتوی فایل را خواند دلیل بر این نمیشود که در آن نمیشود تغییری ایجاد کرد پس دو موضوع Confidentiality و Integrity مستقل از هم هستند

No Confidentiality, No Integrity,Authenticity



- چون با کلید خصوصی PC1 رمز شده اگر دیتای رمز شده در مسیر توسط دیگران رمزگشایی شود حداقل مطمئن هستند که دیتا مربوط به PC1 میباشد

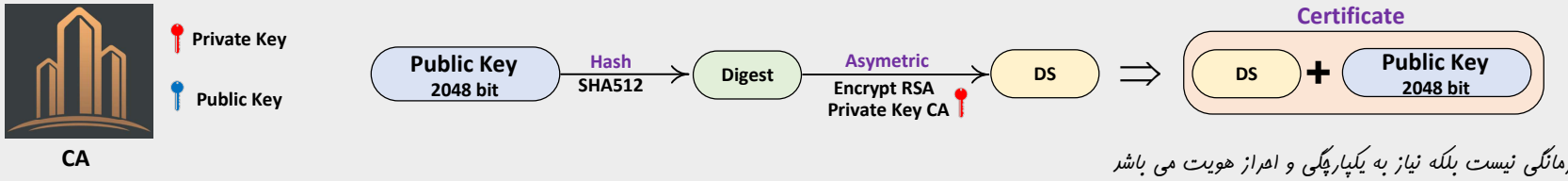
Confidentiality,Integrity,Authenticity



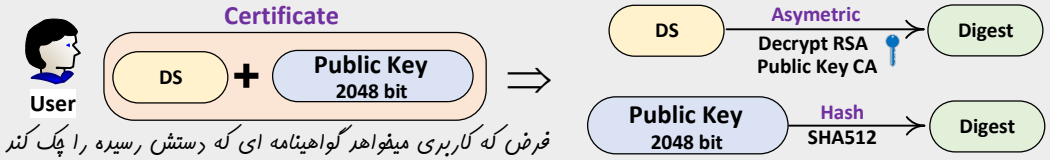
I

Certification Authority (CA)

- یک شبکه میتواند دارای مرکز صدور گواهینامه الکترونیکی باشد Certification Authority (CA)
- بعد از اینکه کلید عمومی و خصوصی توسط یک اپلیکیشنی یا زیرساختی ساخته شد برای ارائه کلید عمومی به عموم باید در قالب یک Certificate ارائه گردد بنابراین کلید عمومی به یک CA ارائه شده و Certificate دریافت میگردد
- اگر کلید عمومی با یک الگوریتمی توسط CA , Hash گردد و سپس با کلید خصوصی CA رمز گردد DS آن کلید عمومی به دست می آید و نهایتا در قالب یک Certificate ارائه میگردد



- در تبادل Certificate نیاز به محرمانگی نیست بلکه نیاز به یکپارچگی و احراز هویت می باشد



فرض که کاربری میخواهد گواهینامه ای که دستش رسیده را چک کند

- اگر مقدار Digest برابر باشد به Certificate اعتماد خواهد کرد

- Self Sign Certificate بدین معنی است که خودش برای خود گواهینامه صادر کرده است و نشانه آن هم اینست که Issued by و Issued to با هم برابر است البته ممکن است که برابر نیز نباشد
- گواهینامه میتواند از یک CA گرفته شود حال در این شرایط دوحالت داریم یا Public CA است که به آن External CA نیز گفته میشود و یا Private CA میباشد که به آن Internal CA نیز گفته میشود
- تفاوت Certificate بصورت Private CA یا Public CA در محدوده اعتبار آن می باشد که داخلی باشد یا همه آن را قبول داشته باشند و اعتبار جهانی داشته باشد

II

پروسه دریافت CA

- این پروسه دارای سه گام میباشد اول باید یک درخواست Request بسازیم و بعد از موافقت با درخواست ، دریافت آن میباشد در مرحله دوم باید گواهینامه در جای مناسب نصب یا کانفیگ شود (Install or Import) ودر مرحله آخر باید مشخص شود تا به کاربرانی که نیاز به گواهینامه دارند کدام یک از گواهینامه ها را برای آن کار خاص ارائه کند (Binding)
- گواهینامه الکترونیکی ممکن است به فایل باشد با پسوند .pfx که علاوه بر کلید عمومی حاوی کلید خصوصی نیز هست که جهت محافظت از آن حتما شامل پسورد است ولی وقتی سرور بخواهد گواهینامه را ارائه دهد یک فایل با پسوند .cer را برمیگرداند که دیگر شامل کلید خصوصی نیست

III

CA Authentication مراحل

- یک مقداری از اعتبار یک گواهینامه به صادر کننده آن مربوط میشود پس کلاینت اول باید ببیند کجا گواهینامه را صادر کرده Issued by و آیا به صادر کننده آن اعتماد Trust دارد؟

1. **Certificate Trust List (CTL)** – حاوی لیستی از CA ها میباشد که به آنها اعتماد داریم به طور مثال ویندوز یک چنین لیستی را در درون خود دارد و همه اپلیکیشنهای کلاینتی و سروری از CTL آن ویندوز استفاده میکنند ولی اپلیکیشنهای غیر ویندوزی ممکن است از CTL ویندوز استفاده کنند یا خودشان CTL داشته باشند بطور مثال فایرفاکس CTL خود را دارد
   - از طریق Snap-in Certificate و اضافه نمودن Computer Account میتوان در فولدر Trust Root Certification Authority لیست CTL های ویندوز را مشاهده کرد
2. – سپس در یافت کننده گواهینامه اعتبار زمانی آن گواهینامه را چک میکند
3. – در مرحله بعد چک میکند آیا گواهینامه متعلق به همان جایی است که ادعا میکند Issued to
4. – یک گواهینامه میتواند قبل از اینکه اعتبار آن به پایان برسد به دلایل فنی یا حقوقی یا سیاسی باطل Revoke شود قابل ذکر است که یک CA لیست گواهینامه های باطل شده را (CRL) با دانلود آن از CA به روز میکند

Certificate Revoke List (CRL) – کلاینت جهت دانلود لیست (CRL) به گواهینامه مراجعه کرده و از طریق آدرس CRL Destribution Point (CDP) که درون گواهینامه موجود است این لیست را دانلود و به روز میکند

- یک CRL Base داریم که حاوی لیست کل گواهینامه های باطل شده است که مثلا ماهیانه یکبار آپدیت میشود و یک CRL Delta داریم که تغییرات را هفتگی آپدیت میکند وممکن است بر اساس تنظیمات CA شامل CRL Delta نباشد و فقط CRL Base را انجام دهد

Online Responder

- در روش بهینه تر برای CRL یک Online Responder راه اندازی میشود که وظیفه آن دانلود کردن لیست CRL میباشد بطوریکه الباقی سیستم ها از Online Responder سوال خود را در مورد لیست CRL می پرسند و قاعدتا این سرویس بر روی یک ماشین دیگری غیر از CA راه اندازی میشود تا بر روی آن بار اضافی نیاندازد و پرتکلی که کلاینتها برای سوال پرسیدن استفاده میکنند Online Certificate Status Protocol (OCSP) میباشد

I

- اگر به جای نام DNS یک سایت از آدرس IP استفاده کنیم به احتمال بالا خطای گواهینامه دریافت میکنیم هر چند بر اساس سیاست آن سایت میتوان بصورت Unsecure کار را ادامه داد

WildCard Certificate

- یعنی قبل از نام دامین امکان استفاده از هر نامی وجود داشته باشد مانند

*.test.com ⟶ Mail.test.com Oa.test.com Portal.test.com www.test.com .....

Subject Alternate Name (or SAN) certificate
Unified Communications Certificate (UCC)

- اگر بیش از یک دامین در اینترنت برای منظورهای مختلف ثبت شده باشد چون در آن اسامی متعدد آمده است باید SAN Certificate اخذ نمود

Subject Alternate Name

Issued by:faratarhgroup.com ⟶ DNS Name=faratarhgroup.com
DNS Name=www.faratarhgroup.com
DNS Name=mail.faratarhgroup.com
DNS Name=autodiscover.fts.ir
DNS Name=mail.fts.ir

II

DV,OV,EV Certificate

EV SSL Extended Validated

هویت حقوقی درخواست کننده گواهی به طور کامل تایید می گردد، این تاییدیه در در نوار سبز رنگی در کنار آدرس سایت در مرورگر نمایش داده می شود که موجب جلب اعتماد هرچه بیشتر کاربران به سایت می گردد این گواهینامه تنها برای شرکتها ، سازمانهای دولتی ، بانکها ، وزارتخانه ها و به طور کل اشخاص حقوقی صادر می گردد و درخواست کننده باید مدارک کامل ثبتی و قانونی و هویتی خود را به صورت ترجمه شده ارسال نماید به دلیل وجود مراحل مختلف تایید هویت و همچنین نمایش نوار سبز رنگ تایید، این نوع گواهی دارای هزینه صدور بالایی می باشد و همچنین بالاترین میزان کسب اعتماد برای سایت را به همراه خواهد داشت

OV SSL Organization Validated

هویت حقوقی درخواست کننده گواهی به طور کامل تایید می گردد به این صورت که این گواهینامه تنها برای شرکتها ، سازمانهای دولتی ، بانکها ، وزارتخانه ها و به طور کل اشخاص حقوقی صادر می گردد و درخواست کننده باید مدارک کامل ثبتی و قانونی و هویتی خود را ارسال نماید به دلیل وجود مراحل مختلف تایید هویت این نوع گواهی دارای هزینه صدور بالایی می باشند اما به همان میزان نیز دارای اعتبار بالایی می باشند

DV SSL Domain Validated

تنها هویت مالک دامنه از طریق ایمیل بررسی و تایید می گردد و هیچ مرحله بررسی و تایید هویت دیگری ندارد به دلیل کم بودن مراحل تایید هویت این گواهینامه هزینه صدور آن بسیار پایین می باشد اما به همان میزان نیز اعتبار ان پایین می باشد این نوع گواهی مناسب برای فروشگاه ها و وب سایت های کوچک و متوسط می باشد

- از طریق Snap-in میتوان به Certificate دسترسی داشت که شامل سه بخش میباشد اول گواهینامه های های کاربر ، دوم گواهینامه های کامپیوتری که متصل هستیم و سوم گواهینامه های سرویس که قرار است رویت و مدیریت شوند بنابر این هر کاربری فقط به گواهینامه های خودش دسترسی دارد ولی اگر کاربر عضو گروه Administrator آن ماشین باشد به غیر از گواهینامه خودش امکان مدیریت گواهینامه های آن ماشین و سرو یس ها را نیز دارا می باشد

- اگر به غیر از کلید عمومی ، کلید خصوصی نیز بر روی کامپیوتر موجود باشد یک علامت کلید بر روی آیکون گواهینامه ظاهر میشود ضمن اینکه اگر بر روی گواهینامه دو با کلیک کنیم پیغامی با مضمون وجود کلید خصوصی همرا با یک کلید در تب General درج میشود

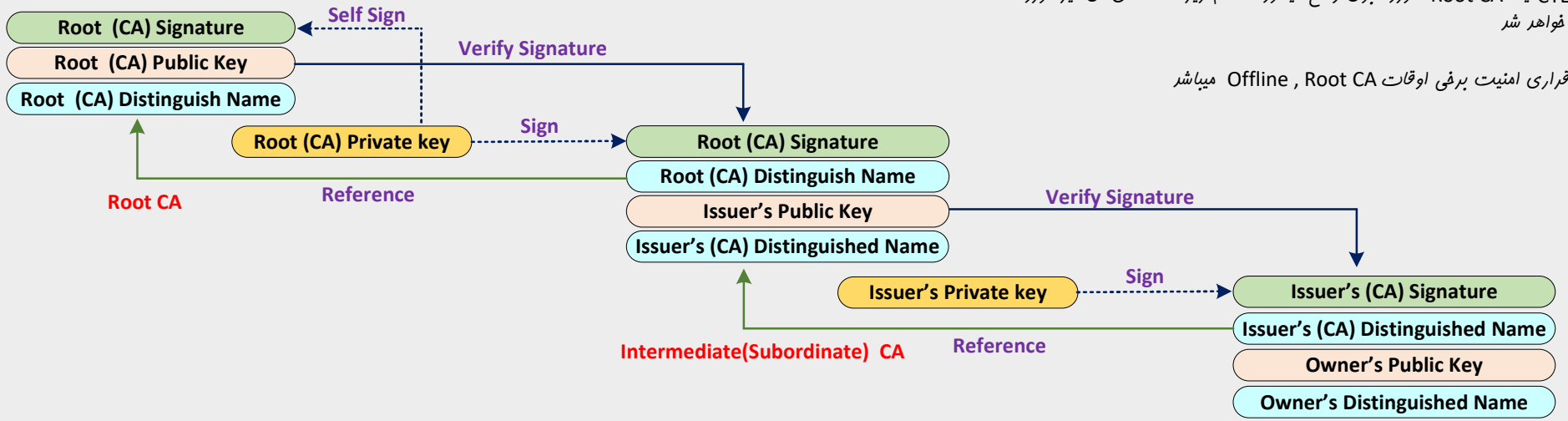
Certmgr.msc ⟶ Manage User Certificate
Certlm.msc ⟶ Manage Computer (Local Machine) Certificate

- در ارتباط با Hardening ویندوز برنامه IISCrypto.exe عملکرد مناسبی دارد و باعث میگردد تا پرتکل های قدیمی رمز نگاری و Hashing را بدون دستکاری رجیستری Disable کنیم

I

Certificate Chain

- وقتی در CTL یک Root CA مورد قبول واقع میشود ، تمام زیر شاخه های آن نیز مورد قبول واقع خواهد شد
- جهت برقراری امنیت برخی اوقات Root CA , Offline میباشد



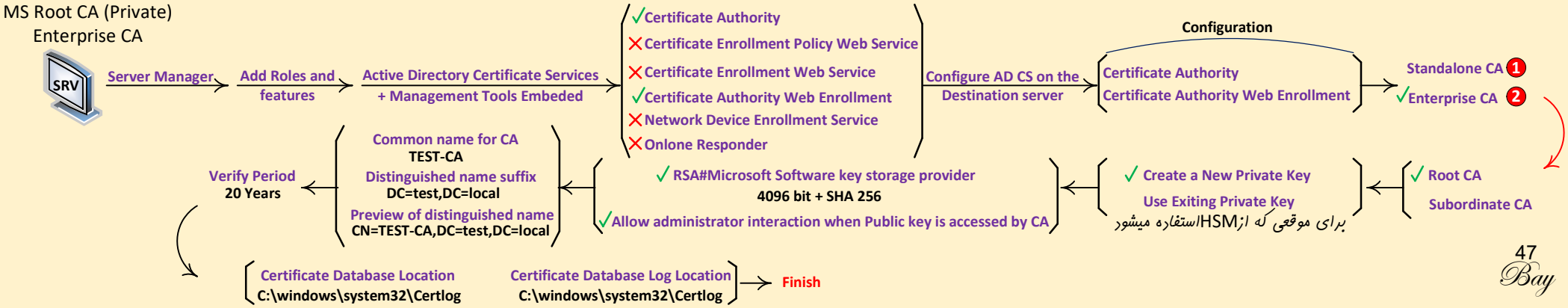
- طبق یک قانون نانوشته عموما زمان اعتبار Root CA را ۲۰ سال در نظر میگیرند
- Root CA اول به خودش به صورت Self Sign گواهینامه میدهد و بعد به لایه زیر دستی خودش و بعد از آن تقریبا کار دیگری ندارد و میتواند در حالتی خاص جهت حفظ امنیت خاموش شود
- Intermediate CA اعتبار یا همان گواهینامه خود را از Root CA میگیرند و سپس به لایه های پایینتر میتوانند گواهینامه اختصاص دهند

II

Enterprise CA , Standalone CA

- برای راه اندازی CA در مایکروسافت دونوع CA امکان پذیر است ، **Standalone CA** و **Enterprise CA** ، عمدتا در سازمان ها Enterprise CA راه اندازی میشود
- **Standalone CA** – چه شبکه دامین مدل و چه Workgroup امکان راه اندازی را دارد
- **Enterprise CA** – اصلیترین شرایطش اینست که کامپیوتر Join to domain باشد و کسی که آن را راه اندازی میکند حتما ادمین فارست باشد یا عضو Enterprise Admin فقط در این حالت Certificate Templates فعال است
- نام کامپیوتر و دامین و Rejoin بعد از راه اندازی CA نمیتواند تغییر کند
- ۵ آیتم آخر باعث تنوع در سرویس گرفتن از CA میشود

Installing the AD CS Server Role



I

Create Certificate Template for Workstation and Client Authentication:

certsrv.msc → Certification Authority

Control Panel → Administrative Tools → Certification Authority ⇒ Certificate Templates → Right click then Manage: → Workstation Authentication → right click then select Duplicate Template: → General Tab →

Template Display Name
Client-Server Authentication
Validity Period
2 Years
✓ Publish Certificate in Active Directory
✓ Don't auto reenrol if duplicate certificate

Open Control Panel then go to Administrative Tools -> Certification Authority:

Security Tab ← add Domain Computers Check the boxes for Read and Autoenroll: ← Extention ← On the Extensions tab click Application Policies then Edit: ← Add -> Server Authentication then Ok: ← Subject Name ← click the DNS name box to add the DNS name to the SAN of the certificate. Click Apply and Ok: ← Certificate Templates ← New -> Certificate Template to Issue Client-Server Authentication

- اینطور نیست که بعد از راه اندازی Root CA هر کس درخواست گواهینامه کرد Root CA با آن موافقت کند ، طبیعتا کسی که درخواست Request میدهد باید AA (Authenticate,Authorized) شود ، به نوعی درخواست ها فیلتر میشود

- اگر Standalone CA داشته باشیم همه درخواست ها اول در حالت Pending قرار میگیرد و سپس توسط ادمین با درخواست ها موافقت یا مخالفت میشود
- اگر Enterprise CA داشته باشیم فیلترینگ در مرحله درخواست عملیاتی میشود یعنی فقط کسانی میتوانند درخواست بدهند که میتوانند درخواست داشته باشند این مهم بر اساس Certificate Template انجام میگردد

Configure Group Policy for Automatic Certificate Enrollment:

Gpmc.msc → Computer Configuration → Windows Setting → Security Setting → Public Key Policies →

Certificate Service Client – Certificate Enrollment Policy → Enable → Active Directory Enrollment Policy

Certificate Service Client –Auto Enrollment → Enable →
- Renew ,Update Pending,remove revoked Certificates
- Update certificates that use certificate templates

- مجموعه رفتارهایی که نمیخواهیم توسط Certificate Templates مد نظر قرار بگیرد و از طریق آن گواهینامه صادر شود را میتوانیم از Certificate Templates پاک نمائیم
- مجموعه Certificate Templates در قسمت CIP Partition ذخیره شده اند adsiedit.msc → Services → Public key Services → Certificate Templates

- بعد از راه اندازی CA باید حتما CDP را تنظیم نمود ضمنا میتوان به غیر از آدرس LDAP آدرس HTTP را نیز برای کلاینتها Publish نمود

- از طریق Sertsrv.msc میتوان بکاپ ، بازیابی ، Start/Stop سرویس CA و تجدید سرویس را انجام داد و با Properties گرفتن از CA و ورود به تب Extention میتوان تنظیمات AIA(Authority Information Access) CDP (CRL Distribution Point) را انجام داد

✓ Include in the AIA Extension of issued Certificates (Http)
✓ Include in the CDP Extension of issued Certificates (Http) & ✓ Push CRLs to this location (c:\windows\system32\certsrv\certenroll\....

CDP: – آدرسی است که از طریق آن CRL دانلود میشود
AIA: – آدرسی است که از طریق آن گواهینامه CA دانلود میشود

- وقتی از طریق certsrv.msc\Revoked Certifications عمل Revoke رانجام میدهیم فقط اگر از حالت Certificate Hold برای Revoke استفاده کرده باشیم قابلیت Unrevoke امکان پذیر است
- وقتی یک Root/subordinate CA راه اندازی میکنیم Computer Account آن عضو گروه Cert Publisher خواهد شد تا امکان Publish Certificate میسر گردد
- بر روی Certificate Templates پیش فرض نمیتوان تغییراتی ایجاد کرد لذا باید از Duplicate Template استفاده کرد و اگر بخواهیم امکان انتقال کلید خصوصی را نیز مهیا کنیم باید از تب Request Handling حالت Allow private key to export را فعال کنیم
- جهت درخواست گواهینامه میتوان از راه کارهای مختلفی استفاده نمود ، یک از آنها استفاده از ① Certlm.msc\personal\certificates بر روی سیستم لوکال یا استفاده از کنسول وب مرتبط با CA میباشد Request new certificate →
② Https://<server-CA>/sertsrv

I

1. Inetmgr.msc\Server Certificate

3 – یک روش دیگر استفاده از کنسول IIS و بخش Server Certificates میباشد که میتوان گواهینامه را Import یا Request نمود این روش بیشترین مورد استفاده را دارد Inetmgr.msc

2. Action Tab → Import / Create Certificate Request → Distiguished Name Properties → CSP Crptographic Service Provider → Create txt File Name

– در این حالت درخواست گواهینامه کامل شده است ، حال دو راه جهت ادامه کار میتوان انجام داد

– راه اول مراجعه به CA میباشد: Root CA → Certsrv.msc → R-Click on CA All Task → Submit new request

– راه دوم مراجعه به Web CA میباشد: Web CA/Certsrv → Request a Certificate → Submit a certificate request → Insert Content of txt file → Download .cer Certificate

3.

– بعد از دانلود فایل .cer مجدد به کنسول IIS\Certificate مراجعه کرده و از قسمت Complete Certificate Request فایل را ارجاع داده و نهایتا منجر به درج فایل در IIS خواهد شد

– اصولا روش کار برای وب سرور های خارج از سازمان بدین شکل است که ما ابتدا درخواست گواهینامه را در IIS خود کامل کرده و فایل .txt که حاوی فقط کلید عمومی میباشد را به مرکزCA تحویل میدهیم سپس آن مرکز با ترکیب کلید عمومی ما وDS کلید عمومی که تحویل شده است گواهینامه را صادر کرده .cer و تحویل می نماید ، این موضوع برای دیگر سرویس های سازمان از قبیل Exchange, Skype,.... نیز به همین شکل میباشد نکته مهم اینکه هر جا در خواست صادر میشود همانجا نیز باید کامل شود حال با ترکیب کلید عمومی و خصوصی یک pfx. ساخته میشود که میتوان در صورت نیاز از طریق Exportبه جای درست آن انتقال داد و استفاده کرد

II

Name Resolution (DNS , WINS)

Node:
- Physicall address(MAC) → User for next hop addressing
- Logical Address (IP) → User for End to End Addressing
- Computer Name → User for User Friendly
  - NetBIOS Name → 1 segment,Max 15 Char,without . → (WINS)
  - FQDN → Hierarchical,with . ,Host name+Suffix Name → (DNS)

→ Name Resolution: Name ⟷ Translate ⟷ IP address

Domain Name System (DNS)

Windows Internet Name Service (WINS)

– DNS به غیر از Name Resolution وظیفه Service Locator را نیز بعهده دارد که شامل مواردی همچون پیداکردن آدرس دامین کنترلر و ایمیل سرور و غیره نیز میشود

DNS Client: www.google.com / IP ?

1. – مقایسه میکند که آیا نام داده شده نام خودش است؟ \\mycomputername
2. – بهره برداری از فایل متنی Host File که قبل از فرایند DNS انجام میشود C:\Windows\System32\drivers\etc\hosts
3. – بهره برداری از DNS Client Cache
   – در فرآیندName Resolution جواب های گرفته شده Cashe میگردد و کسی که جواب میدهد زمان نگهداری TTL این Cashe را مشخص میکند
   – Cashing شامل Reverse Cashe نیز میشود یعنی از IP به Name
   – پس از اتمام زمان TTL , DNS آدرس را از Cashe پاک میکند ولی مواردی که در Host Fileوجود دارند TTL آنها هیچوقت کم نمیشود
   – در صورت بروز تضاد بین DNS Cashe و Host File اولویت Host File بالاتر است
4. – بهره برداری از DNS SRV بر اساس تنظیمات DNS Client

– اگر از DNS SRV سوال پرسیده شود و جوابی دریافت نگردد روال Name Resolution به شکل زیر ادامه پیدا میکند

1. – بهره برداری از فایل متنی LMHOST
2. – سوال پرسیدن از WINS
3. – Broadcast

– ترتیب بهره برداری از سه آیتم ذکر شده بستگی به مقدار Node Type دارد اطلاعات بیشتر را از طریق جستجو Wins node type در اینترنت میتوان بدست آورد

Ipconfig /displaydns
google.com
Ipconfig /Flushdns
Delete Cashe

```
----------------------------------------
Record Name . . . . . : google.com
Record Type . . . . . : 1
Time To Live  . . . . : 181   → Second
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 172.217.169.238
```

```
C:\Users\ashofteh>ipconfig /all
Windows IP Configuration
   Host Name . . . . . . . . . . . . : Admin-PC
   Primary Dns Suffix  . . . . . . . : tmgic.local
   Node Type . . . . . . . . . . . . : Hybrid
```

I

- پرتکل DNS بر روی پورت Udp 53 جهت Name Resolution کار میکند و از پورت Tcp 53 جهت Zone Transfer استفاده میشود
- در DNS وقتی صحبت از **Authority** میشود بصورت انتزاعی مفهوم صلاحیت مد نظر میباشد بنابراین وقتی سئوالی میشود اگر نسبت به آن سوال صلاحیت داشته باشد ملزم به پاسخگویی است
- بطور مثال DNS ,test.local نسبت به سوالات test.local دارای Authority میباشد و علت آن اینست که دیتابیس test.local برروی DNS SRV موجود است و به این دیتابیس **Zone** و به اطلاعات ثبت شده در آن **Record** گفته میشود
- رکوردهای داخل دیتا بیس یا همان Zone میتواند **Static** ثبت شود و یا **Dynamic (DDNS)** ثبت شود لازم به ذکر است که نوع دیتابیس بصورت متنی **TXT** میباشد
- در بالاترین سطح دو نوع Zone داریم که شامل تنوع رکورد میباشد

Zone
- Forward Lookup Zone —منتج→ IP address
- Reverse Lookup Zone —منتج→ FQDN

قاعدتا تعداد رفعاتی که ازForwatd استفاده میشود خیلی بیشتر از Reverse میباشد

Dnsmgmt.msc —Run→ **Dns Management**

منسوخ شده

dnscmd —Cmd→ **Dns Management**

Get-Command -Module DnsServer —Powershell→ **Dns Management**

II

Forward Lookup Zone (R-Click)

- DNS SRV که Zone ندارد اصطلاحا به آن **Caching Only SRV** میگویند و عملا مجموعه سوالات (Query) را در صورت عدم وجود در Cache به DNSهای دیگر Forward نموده و جوابی که دریافت خواهد نمود را Cashe کرده و اعلام خواهد کرد
- ISP ها عموما از Cache SRV استفاده میکنند چون قرار نیست میزبان (Hosting) کلاینتها باشند
- Zone بصورت داینامیکی ساخته نمیشود و باید بصورت دستی یا اتوماتیک ساخته شود ضمنا وقتی Zone میسازیم فایل آن در **C:\Windows\System32\dns** ساخته میشود و وقتی یک Zone را پاک میکنیم فایل قبلی پاک نمیشود
- جهت بررسی عملکرد موردی DNS از **nslookup** استفاده میشود و همه اسامی DNS آفرش به . ختم میشود

Forward Lookup Zone\zone —R-Click→ New Host(A or AAAA) → **A=IPv4 , AAAA=IPv6**
- میتوان با اسم یکسان و IP متفاوت رکورد ثبت نمود که جهت Round Robin استفاده میشود
- میتوان با IP یکسان و بااسم متفاوت رکورد ثبت نمود بطور مثال در یک شبکه ایمیل سرور با اسامی متفاوت شناخته شود **Pop3.test.local imap.test.local mail.test.local**

New Host(A) → **MBX1.test.local (1.1.1.1)**

CNAME → **Mail.test.local (MBX1.test.local)**

CNAME → **Auto.test.local (MBX1.test.local)**

- با این کار دو اسم مستعار **(Alias)** برای یک هاست رکورد MBX1.test.local ساخته ایم

(CNAME)

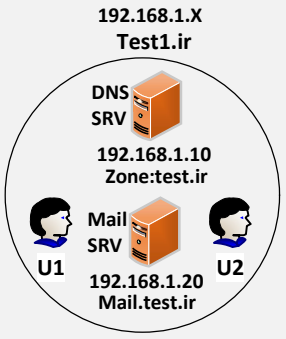
- میتوان یک IP اصلی برای یک ماهیت در نظر گرفت و اسامی مستعار دیگری به آن نسبت داد
- سرویس DNS وقتی استارت میشود از طریق رجیستری متوجه میشود که چه Zoneهایی دارد و سپس به تناظر آن به محل دیتا فایلها مراجعه کرده و آنها را در رم بارگذاری میکندسپس از طریق فایل موجود در رم پاسخ ها را ارجاع میدهد واگر تغییرات جدیدی در کنسول مدیریتی ایجاد شود در واقع در رم ایجاد شده است و سیستم طبق توالی زمانی کوتاه و مشخصی تغییرات را در فایلهای مد نظر ذخیره میکند **Update Server Data File**

Ram Data —Update Server Data File→ **Data File** **Data File** —Reload→ **Ram Data**

- اگر تغییرات را در فایلهای Zone ثبت کنیم برای بروز رسانی در حافظه از گزینه **Reload** استفاده میشود

Domain
- AD Domain —Policy→ DC
- DNS Domain —Suffix Name→ DNS SRV

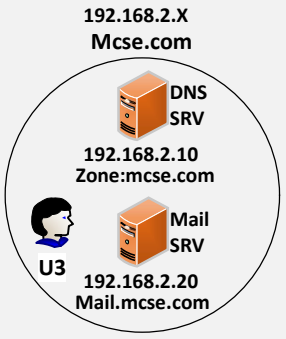
- فرض که دوشبکه داریم که هر دو ایمیل سرور دارند و با هم تبادل ایمیل می پردازند ، با علم به این موضوع که وقتی صحبت از DNS Domain میشود منظور محدوده مشترک Suffix Name مد نظر میباشد



U1@test.ir —Email→ **U2@test.ir**
U1@test.ir —A Record→ **Resolve mail.test.ir from DNS**
U1@test.ir → **Send mail to u2@test.ir**

U1@test.ir —Email→ **U3@mcse.com**
U1@test.ir —A Record→ **Resolve mail.test.ir from DNS**
Mail.test.ir —Query→ **Resolve mail.mcse.com from DNS**
DNS —Query MX Record and obtain IP Email→ **Chain of Dns to mail.Mcse.com**
Mail.test.ir —Send SMTP→ **Send u1 mail to u3 based of Mcse Email SRV's IP and port 25**

MX Record



- در DNS در یک رکورد مشخص میگردد که ایمیل سرور چه اسمی دارد=**MX Record**
در یک رکورد دیگر IP مرتبط با اسم ایمیل مشخص میگردد=A Record

MX Record —Output→ **Name of Email Server**
A Record —Output→ **IP of Email Server**
+ → **Email SRV's IP for output DNS**

- جهت تبادل ایمیل بین ایمیل سرور داخلی سازمان و ایمیل سرور خارج از سازمان نیازمند ساخت MX Record در DNS سازمان هستیم

I

nslookup

```
C:\Users\test>nslookup
Default Server:  dns.test.local
Address:  192.168.11.20

> server 8.8.8.8
Default Server:  dns.google
Address:  8.8.8.8

> set type=mx
> bmi.ir
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
bmi.ir  MX preference = 10, mail exchanger = mail.bmi.ir
> set type=a

> mail.bmi.ir
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    mail.bmi.ir
Address:  89.235.64.89
```

– اگر یک سازمان دو جای مختلف Provider ایمیل سرور داشته باشد از طریق تنظیم عدد Mx Preference در هنگام ساختن MX Record میتواند آنکه عدد پایینتر داشته باشد را بعنوان ایمیل سرور اصلی به دیگران معرفی کند

II

Forward Lookup Zone (R-Click Continue..)

– اگر بر روی Zone ی که در Forward Lookup Zone ساخته ایم R-Click کنیم از حالت New Delegation جهت تفویض بخشی از جواب سوالهای DNS به سرور دیگر استفاده میشود

– اگر بر روی Zone ی که در Forward Lookup Zone ساخته ایم R-Click کنیم از حالت Other New Record جهت به کارگیری انواع دیگری از رکوردها با توجه نوع اپلیکیشنی که استفاده میکنیم به DNS اضافه میکنیم

– از DNSSEC برای Query گرفتن از DNS استفاده میشود بطوریکه مطمئن شویم پاسفی که دست به دست دریافت کرده ایم حتما از یک SOA معتبر بوده و بین راه توسط DNSهای دیگر تغییری نکرده است تا زمان نگارش این مبحث برای حوزه ir , DNSSEC بعلت عدم ساپورت قابل پیاده سازی نیست

– وقتی یک Zone راپاک میکنیم از ریجستری که همان کانفیگ میباشد حذف میشود ولی دیتا فایل آن در مسیر ذکر شده پاک نمیشود

– از Export List جهت استخراج رکوردهای یک Zone بر روی یک فایل متنی استفاده میشود

Forward Lookup Zone Without AD (Properties)

– اگرDNS بصورت Cache Only Server کانفیگ شده باشد چونZoneو دیتا بیس نداردStatelessمیباشد و اگر هم Zone داشته باشد ولی دیتابیسDynamic نباشد باز نیزStateless است و درصورتDynamic بودن Stateful است

General 1
- Status 1 – جهت Start/Pause نمودن عملکرد یک Zone استفاده میگردد ، وقتی که عملکرد به Pause تغییر میکند تغییر میکند Pause به Zone
- Type 2
  - Primary 1 – در اینجا منظور صرفا دامین DNS است ولی این نکته حائز اهمیت است که دامین AD ملزم به داشتن دامین DNS میباشد
  - Secondary 2 – جهت برطرف نمودن SPOF در شبکه،DNSدوم را ایجاد میکنیم – Zoneها طی پروسه Zone Transfer از طریق پورت Tcp 53طبق یک فرایند یکطرفه با هم Sync میشوند

Domain Test.local —سرویس میگیرد از→ Zone Test.local —قرار دارد در→ DNS SRV

– Zone Primary حالت Read/Write وZone Secondry حالت Read Only دارد

– Zone Secondry تغییرات را ازZone Primary یا به عبارتی Master Name SRV بصورت Pull میگیرد ، این اتفاق به سه صورت امکان پذیر است

SOA
Zone Transfer
Name Server

1 – بصورت دستی با Properties گرفتن از Zone Secondry و انتخاب Transfer from Master

– پس از کانفیگ Zone Secondry جهتZone Transfer باید درZone Primary ازقسمت Allow Zone Transfer Zone Secondry , IP address را درج نمائیم تا اجازه Zone Transfer داده شود ضمنا Notify نیز در همین تب فعال میشود

– در Zone Transfer فقط رکورد انتقال میابد و نه کانفیگ مگر اینکه کانفیگ داخل یک رکورد قرار گرفته باشد بنابراین جدول زمانبندیZone Transfer داخل رکورد SOA قرار میگیرد

2 – طی بازه های زمانی مشخص ، بطور پیش فرض ۱۵ دقیقه

3 – میشود به Master Name SRV گفت که وقتی تغییر کرد تغییر را Notify نماید

Zone Transfer
- 1 All Zone Transfer (AXFR) – یعنی هر بار کل رکوردهای یک Zone , Transfer شوند
- 2 Increment Zone Transfer(IXFR) – یعنی بعد از بار اول که کل Zone , Transferمیشود دفعات بعد فقط تغییرات Transfer میشوند

Zone Primary —Transfer Zone→ Zone Secondry

Zone Secondry —Transfer Zone→ Zone Secondry

Zone Secondry —No Transfer Zone→ Primary Secondry

I — DDNS in private network Without AD(Host record & PTR)

- نکته اول اینکه DDNS باید بر روی هر دو Dns Client & Dns SRV ساپورت شود
- نمیتوان کانفیگی نمود که Dns Client سوالهایش را از یک Dns SRV پرسد و رکوردهایش را در یک Dns SRV دیگر بصورت داینامیکی ثبت کند
- Dns Client باید Suffix Name مناسب داشته باشد یعنی برابر با Dns SRV Suffix name باشد
- اگر نخواهیم فرضا یک کامپیوتر رکوردهایش بصورت دینامیکی ثبت شود و یا یک کامپیوتر دو کانکشن داشته باشد و بخواهیم اسم سیستم با یکی از IP ها رجیستر شود بدین معنی که Per Connection باشد تنظیمات شبکه کلاینت بدین شکل باشد

Network Connection → TCP/IP V4 → Properties → Advanced → DNS →
✓ Register this connection's addresses in dns
Use this Connection's Dns suffix in dns registration

- نکته بعدی اینکه DDNS باید بر روی Zone ی که میخواهیم در Dns SRV فعال باشد Zone Name\General\Dynamic Update → Nonesecure and secure
- درصورت انجام موارد بالا کلاینت در موقع ریستارت ویندوز یا سرویسهای DNS client , DHCP Client مبادرت به درج رکورد بصورت داینامیکی خواهد کرد به اینحالت Hard Registration میگویند
- اگر بخواهیم Soft Registration را انجام دهیم باید در قسمت کامند کلاینت این دستور را درج نمائیم Ipconfig /registerdns

II — Stale & Scavenging

- اگر IP یک کلاینت عوض شود Host Record آن سریعا در سرور DNS تغییر میکند ولی اگر نام کلاینت تغییر کند در زمان ریستارت ویندوز رکورد آن تغییر خواهد کرد ضمنا در هر دو حالت رکورد Update Record میشود ولی هر موقع Time Stamp آپدیت شود اصطلاحا Refresh Record میشود
- زمانیکه DDNS بصورت Unsecure برقرار باشد پروسه Authentication برقرار نخواهد شد و واقعا مطمئن نیستیم که رکوردی که ذخیره میشود واقعا همان چیزی باشد که ادعا میشود

Time Stamp DDNS records Register → 1400/10/30-11AM
→ تا هفت روز تایم استمپ تغییر نمیکند ، و نیاز به Refresh ندارد — No refresh Interval=7day
+ تا هفت روز تایم استمپ باید آپدیت شود ، و نیاز به Refresh شدن دارد → refresh Interval=7day

اگر رکورد در هفت روز دوم آپدیت نشود حداقل ۱۴ روز از عدم تغییر تایم استمپ گذشته است و اصطلاحا رکورد Stale میشود باید Scavenging از تب General فعال شده باشد

- وقتی رکورد Stale میشود DNS برای پاسخگویی از آن استفاده نمیکند

1 – اگر بعد از Stale شدن رکورد به مسیر <DNS name>\Scavenge stale resource records مراجعه کنیم میتوانیم بصورت دستی فایلهای Stale شده را پاک کنیم

2 – روش بعدی تنظیم اتوماتیک میباشد که بعد از تعداد روز منظور شده بصورت اتوماتیک رکوردهای Stale شده را پاک میکند

+ هفت روز اضافه تر برای پاک کردن اتوماتیک رکورد ، با این تنظیم پس از ۲۱ روز رکوردهای Stale شده پاک میشوند
Dns SRV/Advance /delete automatic scavenging of stale records7=day

III — Forward Lookup Zone Without AD (Properties)

- مجموعه کانفیگهایی که اینجا انجام میشود درقالب یک رکورد SOA در کنار الباقی رکوردهای یک Transfer , Zone میگردد Zone Name → Properties → SOA

Start Of Authority (SOA) 3

1 **Serial Number** – بعنوان یک شمارنده افزایشی ، هر رکوردی که ایجاد یا ویرایش یا پاک شود در رکورد SOA سریال یک عدد افزایش پیدا میکند و از افزایش دستی آن جهت تست فرآیند Zone Transfer بین دو DNS استفاده میشود

2 **Primary Server** – نشاندهنده Primary FQDN بر روی یک Zone مشخص میباشد

3 **Responsible Person** – نشاندهنده ایمیل آدرس شخص مسئول آن Zone میباشد نکته اینکه از • به جای @ استفاده میشود علت آن اینستکه @ در DNS معنای خاصی دارد Hostmaster.test.local →

@ نشان دهنده Same As Parent Folder میباشد در DNS

@ A 10.1.1.1 or @ MX mail.test.local → @=test.local

4 **Minimum (default) TTL** – برای رکوردهای استاتیک پیش فرض TTL یک ساعت میباشد و برای رکوردهای داینامیک ۲۰ دقیقه ، TTL و بخشی از Option های DNS با فعال نمودن View\advance در دسترس میباشند

Name servers 4

- از MX Record جهت مشخص نمودن ایمیل سرور و از NS Record جهت مشخص نمودن DNS Server استفاده میشود
- شامل FQDN , DNS SRV ها میشود در این شرایط نیاز به یک A رکورد برای DNS SRV میباشد ، به A رکورد DNS SRV اصطلاحا Glue Record میگویند ، اگر FQDN را مناسب Zone انتخاب کنیم بصورت اتوماتیک A Record نیز ساخته میشود

```
PS C:\Windows\system32> nslookup
Default Server: server.test.local
Address:  192.168.11.20
> set q=ns
> bmi.ir
Server:  server.test.local
Address:  192.168.11.20

Non-authoritative answer:
bmi.ir  nameserver = ns2.bmi.ir
bmi.ir  nameserver = ns1.bmi.ir

ns2.bmi.ir      internet address = 89.235.64.66
ns1.bmi.ir      internet address = 89.235.64.65
```

Forward Lookup Zone Without AD (Properties) WINS

I

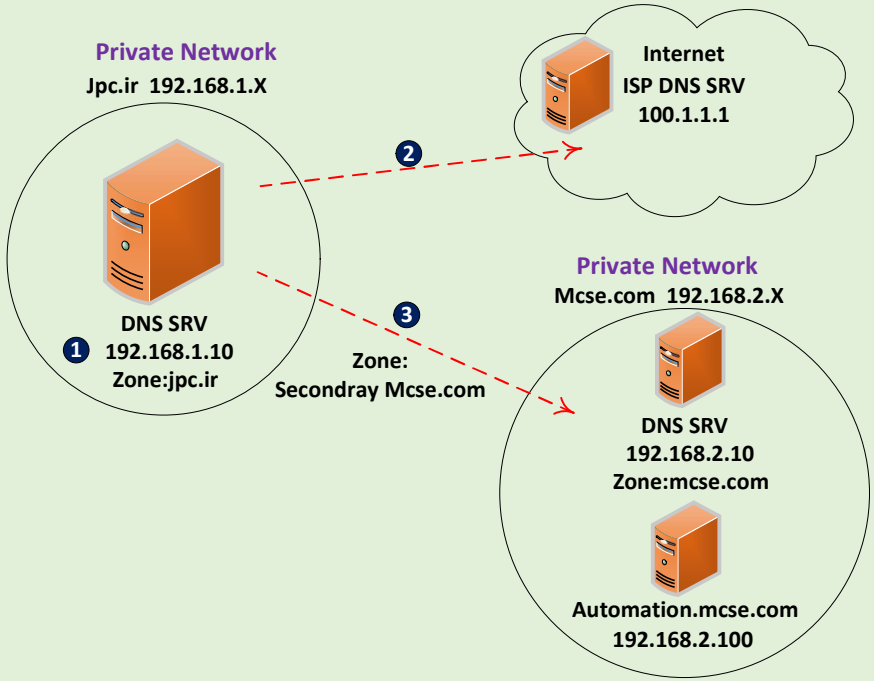
FQDN → IP? → DNS SRV

NetBIOS Name → IP? → WINS SRV

WINS 5

- جهت Name Resolution اسامی **Netbios** ی استفاده میشود و در حال حاضر کاربردی ندارد ضمنا در WINS حالت Reverse IP (PTR) نداریم
- اگر از DNS SRV سوالی پرسیده شود و نداند درصورت فعال بودن WINS قبل از پاسخ به کلاینت بخش Host Name سوال که عموما NetBIOS Name میباشد را با WINS مورد تعامل قرار خواهد داد
- همانند رکورد SOA که قابلیت انتقال کانفیگ را نیز دارا میباشد در WINS رکورد **WINS Lookup** را داریم
- ویندوز از طریق پرتکل NetBIOS over TCP/IP = NBT که یک اینترفیس بین لایه اپلیکیشن و ترانسپورت در مدل TCP/IP میباشد عمل سازگاری NetBIOS با TCP/IP را به سرانجام میرساند

II



DNS Server **Properties** → **Forwarders**

Forwarders ← 1 ISP های DNS SRV 2 DNS SRV های مغایرات 3 International های DNS SRV

- جهت پیدا کردن بهترین فورواردر از دستور Ping 8.8.8.8 -n 10 استفاده میکنیم و هر کدام Average پایینتری داشت در لیست فورواردرها در صدر لیست قرار میدهیم
- اگر DNS نسبت به یک سوال Authority نداشته باشد و سوال مربوط به یک ماهیت Private داخلی باشد تکلیف چیست؟

1 Quary 1: mail.jpc.ir → Ip ? DNS – نسبت به این سوال Authority دارد

- اگر از DNS SRV سوال پرسیده شود و جوابی دریافت نگردد روال Name Resolution به شکل زیر ادامه پیدا میکند

1 – بهره برداری از فایل متنی LMHOST
2 – سوال پرسیدن از WINS
3 Broadcast

– ترتیب بهره برداری از سه آیتم ذکر شده بستگی به مقدار Node Type دارد اطلاعات بیشتر را از طریق جستجو Wins node type در اینترنت میتوان بدست آورد

2 Quary 2:www.google.com → Ip ?

- اگر DNS نسبت به یک سوال Authority نداشته باشد و در واقع سوال مرتبط با Zone های داخلی نباشد از DNS SRV Cache استفاده خواهد نمود که نتیجه پرسش از DNS های خارجی میباشد ، این Cashe در صورت تیک خوردن View/Advnace در DNS قسمت **Cached Lookups** قرار دارد ، حال اگر در Cashe موجود نباشد DNS به DNS SRV های خارجی سوال را فورووارد میکند

3 Quary 3:Automation.mcse.com → Ip ?

- اگر تنظیمات برای Zone:mcse.com انجام نشود این سوال فورووارد میشود و اگر هم جوابی برگردد یک IP Public خواهد بود که پاسخ صحیحی نیست چون ما به دنبال یک IP Private هستیم

برای این پاسخ سه راه حل وجود دارد

1 – راه حل اول اینست که بر روی سرور DNS SRV یک **Zone Private Secondary** نسبت به Mcse.com بسازیم سپس Master Name Server تعیین میکنیم و بدین شکل Zone Transfer برقرار میشود

– در این راه حل باید در هر دو طرف بر روی فایروال پورت Tcp 53 جهت Zone Transfer باز باشد و تنظیماتش نیز انجام شده باشد ضمنا صورت جواب دادن به صرفه نیست چون هر ۱۵ دقیقه یکبار که آپدیت میشود تمام رکوردهای را باید به Secondry Zone انتقال دهد و اگر تعداد رکوردها بالا باشد عملا هزینه زیادی در بر خواهد داشت

2 – راه حل دوم استفاده از **Conditional Forwarder** میباشد که شامل مجموعه ای از شرط ها است

– در اینحالت ساختار متوجه تغییر IP Conditional Forwarder نمیشود و بصورت دستی باید تغییر را درج نمود

– در Zone Transfer , Conditional Forwarder انجام نمیشود

Conditional Forwarder

If Quary is about Mcse.com → **Forward** → 192.168.2.10

If Quary is about Test.com → **Forward** → .....

Unconditional Forwarder

Else → **Forward** → ..... **Internet Forwarder**

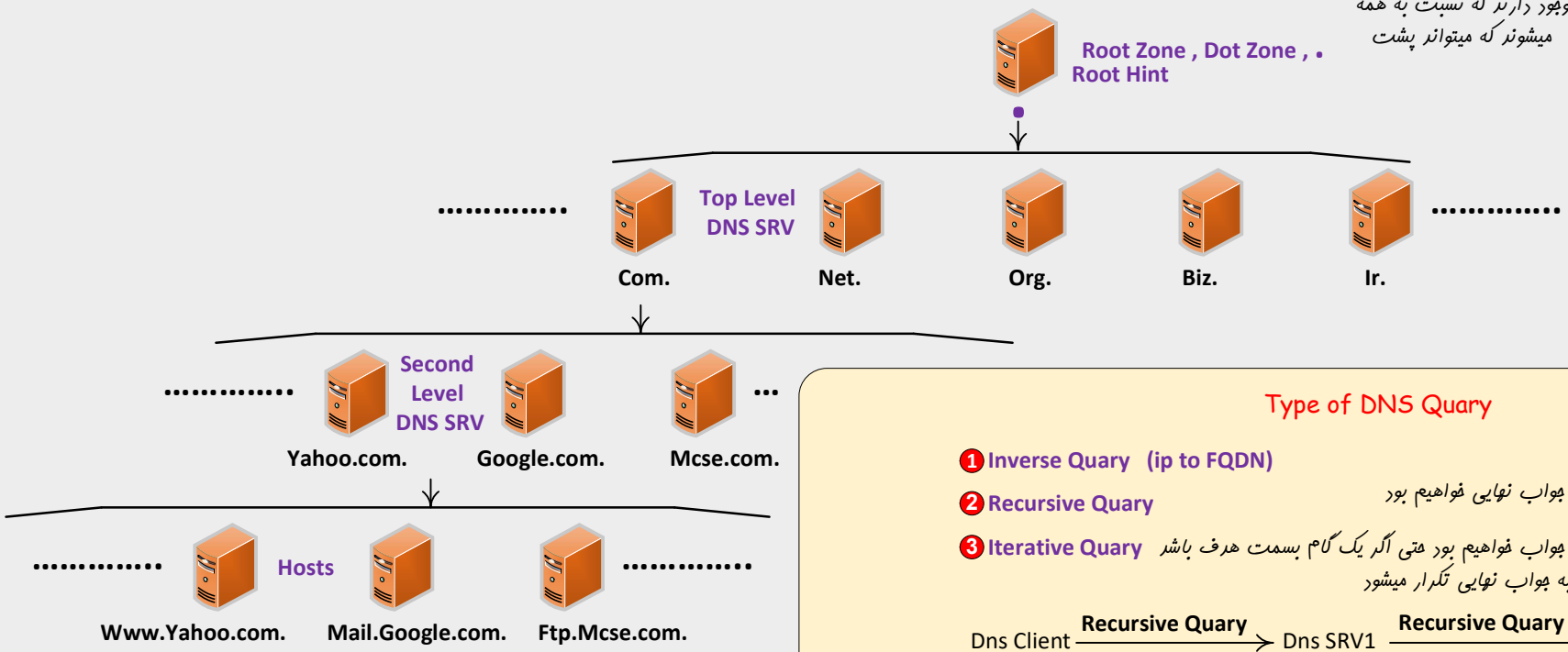
I

3- راه حل سوم استفاده **Stub Zone** میباشد که راه حل هوشمندانه تری میباشد و روش کار بطور مثال بدین شکل است که ما Zone:mcse.com را بصورت Stub Zone بر روی DNS SRV میسازیم و شبیه Secondary Zone باید Master Name SRV تعریف کنیم تا Zone Transfer انجام شود ولی فرق آن با Secondary Zone در این هست که فقط سه نوع رکورد **SOA Record,Glue Record,NS Record** را آپدیت میکند بنابراین از این سه رکورد متوجه DNS SRV ها میشود و سوالها را به سمت آن فوروارد میکند ضمنا بصورت اتوماتیک از طریق Zone Transfer متوجه تغییر DNS SRVها میشود ولی از آنها هیچگاه بعنوان Master Name SRV استفاده نمیکند

- در این روش برخلاف Secondary Zone نیاز به کانفیگ خاصی در قسمت Master Zone برای شناساندن آن بعنوان همکار نیست
- Stub Zone برخلاف Primary Zone وSecondary Zoneبر روی Zone حالت Authority ندارد بلکه صرفا آدرس آن را برای فوروارد میداند

ساختار سلسله مراتبی Name Resolution

- در راس ساختار سلسله مراتبی DNS SRV وجود دارند که نسبت به همه سوالها Authority دارند و شامل ۱۳ عدد IP میشوند که میتواند پشت آنها n عددDNS SRV باشد



Type of DNS Quary

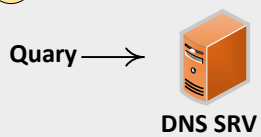
1. **Inverse Quary (ip to FQDN)**
2. **Recursive Quary**
   - سوال پرسیده شده و منتظر جواب نهایی خواهیم بود
3. **Iterative Quary**
   - سوال پرسیده شده و منتظر جواب خواهیم بود حتی اگر یک گام بسمت هرف باشد و همین وضعیت تا رسیدن به جواب نهایی تکرار میشود

Dns Client —**Recursive Quary**→ Dns SRV1 —**Recursive Quary**→ Dns SRV2 .....

- اگر در این تسلسل به Dns SRVبرسیم که برای پاسخ یا فورواردر ندارد و یا جوابی از فورواردر ها دریافت نکند به سراغ Root Hint خواهد رفت این مراجعه آخر به Root Hint را Iterative Quary میگویند چون مطمئن نیست که حتما پاسخ نهایی را بیابد چونRoot Hint به سرور بر اساس سوال آی پی های Top Level DNS SRVمرتبط را باز میگرداند و باز نیز این سوال با فرضا ir.بصورت Iterative Quary ادامه میبابد تا به جواب برسیم

- در صورتیکه مجموعه DNS های Root Hint را از روی سرور پاک کنیم با دادن یک آی پی معتبر Public مانند 8.8.8.8 و زدن دکمه Copy from server میتوان مجددا آن را احیاء نمود
- فایل Root Hint در محل \Windows\System32\dns\CACHE.DNS قرار دارد ضمنا یک نسخه اورژینال نیز در \Windows\System32\dns\samples وجود دارد
- وقتیDns SRVبه یک دامین برای دادن پاسخ Authorityداشته باشد میتواند این وظیفه را به سرور دیگری تفویض Delegate کند البته باید به اسمی اشاره کنیم که NS & Glue recordمناسبی داشته باشد

I



1 – آیا نسبت به سوال Authority جهت پاسخ دارد؟ Primary Zone

2 – بررسی DNS SRV Cache

3 – Forwarding
- Conditional Forwarding
- Stub Zone
- Conditional Forwarding
- Unconditional Forwarding (international Forwarders)

4 – Root Hint

No RootHints & Forwarders

– اگر بخواهیم Dns SRV که نسبت به یک Authority , zone دارد در صورت عدم یافتن جواب عملیات جستجو را ادامه ندهد و به سراغ فورواردرها و Root Hint نرود دو راه داریم

1 – در قسمت Zone مد نظر یک New Zone بصورت Root Hint ایجاد کنیم اینکار با ساختن یک Zone بصورت نقطه • میسر میباشد

2 – در بخش Properties\Advance در تام Dns SRV گزینه Disable Recursion را فعال کنیم

Forwarders Without RootHints

– اگر بخواهیم Dns SRV که نسبت به یک Authority , zone دارد در صورت عدم یافتن جواب عملیات جستجو را از طریق فورواردرها ادامه دهد ولی سراغ Root Hint نرود تنظیم زیر را انجام میدهیم

– در بخش Properties\Forwarders تیک را ازگزینه مربوطه بر میداریم ✕ Use RootHint if no forwarders Are Available

II

DNS SRV\Properties\Advance

DNS SRV Properties\ Advance →

✕ **Disable Recursion (also Disable Forwarders)**
– اگر بخواهیم Dns SRV که نسبت به یک Authority , zone دارد در صورت عدم یافتن جواب عملیات جستجو را از طریق فورواردرها ادامه دهد ولی سراغ Root Hint نرود تنظیم زیر را انجام میدهیم

✕ **Enable BIND Secondaries**
– جهت سازگاری با نسخه های قدیمی BIND DNS linux SRV که فقط حالت AXFR : Full Zone Transfer را ساپورت میکنند استفاده میشود

✕ **Fail on load if bad zone data**
– اگر در ساختار فایل Zone Data اطلاعات اشتباهی درج شده باشد آن را نادیده میگیرد و قسمت های صحیح را اجرا میکند

✓ **Enable Round robin**
– اگر چند آی پی با یک نام در Zone تعریف شده باشد جهت پاسخ بین آنها بوابها پرفش ایجاد میکند

✓ **Enable netmask ordering**
– با توجه به آی پی درخواست کننده آی پی هایی که به کلاینت نزدیکترند با مقایسه بیشترین بیت هم شکل به صدر لیست انتقال داده میشوند مانند بحث Quick Access
– این موضوع در اینترنت همیشه هم صحیح عمل نمیکند چون ممکن است آی پی نزدیکتر در یک محیط جغرافیایی خیلی دورتر از درخواست کننده باشد

✓ **Secure cache against pollution**
– DNS SRV Cache میتواند آلوده به یکسری اطلاعات غلط Fake شود روش کار بدین شکل است که اطلاعاتی که بر اساس زمان اعلام شده فرضا یک ساعت Cache شده است طی این مدت اجازه تغییر نخواهد داشت بدین شکل Cache Poisoning اتفاق نخواهد افتاد

III

Reverse Lookup Zone (PTR)

– تعداد ۳ عدد Reverse Lookup Zone بصورت پیش فرض ساخته میشود ←

– بعضی اوقات بر روی پالیسی که در فایروال یا وب سرور و یا غیره تنظیم میشود که با نام FQDN خاصی قاعده یا قانونی انجام گردد ، اگر با آی پی ، مراجعه ای با موارد اشاره شده انجام شود در این مواقع نیازمند PTR برای بدست آوردن نام هستیم

0.in-addr.arpa → NS & SOA of DNS SRV
127.in-addr.arpa → NS & SOA of DNS SRV + PTR 127.0.0.1
255.in-addr.arpa → NS & SOA of DNS SRV

Network 192.168.1.0 — PTR → **1.168.192.in-addr.arpa** In-add=inverse address

IV

Globalnames zone

– اگر یک Zone با نام GlobalNames بسازیم و در آن فرضا A record www را تعریف نماییم اولویت آن از A record www تمامی Zone های دیگر بالاتر میباشد و DNS همواره آن را در پاسخ بر میگرداند از این روش میتوان از تعریف یک A record مشترک برای تمامی Zone ها به جای تعریف در تک تک Zone میتوان بهره برد البته این قابلیت را باید از طریق کامند dnscmd یا پاورشل فعال نمود

```
Dnscmd /config /?
Dnscmd /config /EnableGlobalNamesSupport 1
Dnscmd /info /EnableGlobalNamesSupport
```

SRV Record

– به این رکورد Service Location نیز گفته میشود و برای مشخص نمودن لوکیشن ارائه سرویس مشخص میشود از هیث آی پی و پورت بنابراین مواردی همچون مشخص نمودن سرویس ..... , skype , outlook , DC از این نوع رکورد استفاده میشود که به فرآیند Auto Discover منجر میگردد ، این روش در DNS میباشد مشابه همین روش را در AD با نام Service Connection Point (SCP) داریم

I

SRV Record

```
> set q=srv
> _autodiscover._tcp.parskhodro.ir
Non-authoritative answer:
_autodiscover._tcp.parskhodro.ir      SRV service location:
        priority      = 0
        weight        = 100
        port          = 443
        svr hostname  = autodiscover.parskhodro.ir
autodiscover.parskhodro.ir     internet address = 217.11.24.235
autodiscover.parskhodro.ir     internet address = 185.175.77.75
```

- طبق این اطلاعت سرویس Auto Discover بر روی آی پی ها و پورت ذکر شده جهت تشخیص Exchange توسط Outlook استفاده میشود

II

DNS+AD Integrated Zone

- AD Integrated Zone یک Type Zone جدید نیست و بدین معنی است که بر خلاف مطالب گذشته که مجموعه دیتای استاتیک و دینامیک Zoneها بر روی یک فایل متنی ذخیره میشد اینبار بر روی دایرکتوری Ntds.dit ذخیره میشود
- از AD Integrated Zone به شرطی میتوان استفاده نمود که DNS SRV بر روی DC SRV راه اندازی شده باشد
- Secondary Zone نمیتواند AD Integrated Zone باشد ولی Primary,Stub,Forward,Reverse Zone میتوانند باشند

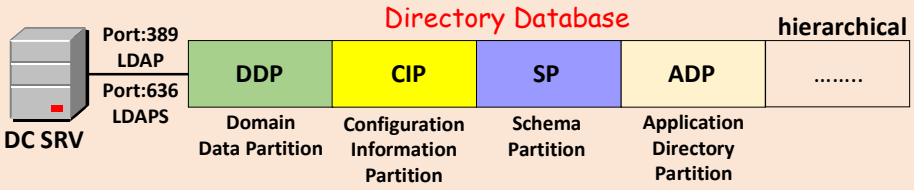
ساختار نامگذاری داخلی با خارجی میتواند یکسان یا متفاوت باشد

ساختار نامگذاری **NameSpace**
- **Internal** ساختار نامگذاری داخل شبکه — **AD Domain** → Jpc.local
- **External** ساختار نامگذاری ازدید بیرون از شبکه — **Internet Domain** → Jpc.ir

- فرض کنیم دامنه Jpc.ir را در اینترنت ثبت میکنیم حال نیاز به یک DNS SRV جهت پاسخگویی به سوالات Jpc.ir در حوزه اینترنت را داریم ، در اغلب مواقع این سرویس بصورت رایگان بر روی هاستینگ بیرونی وجود دارد حال DNS SRV Jpc.ir باید .ir DNS SRVرا در جریان تغییرات بگذارد تا براند وظیفه پاسخگویی به سوالات Jpc.irبه کدام DNS SRV محول شده است این کار بصورت تکنیکی با Delegationانجام میگیرد یعنی سرور .ir نسبت به سوالهای .ir Authority دارد ولی پاسخگویی به Jpc.ir را واگذار کرده است به سرورDNS Jpc.ir

- میدانیم AD Domain وابسته به سرور DNS میباشد که میتواند همراه با آن در شبکه محلی متولد شود و همنام با نام AD یک Zone با همان نام را نیز میسازد و وقتی در زمان نصب AD به Delegation Error برمیخوریم علت آن اینست که میخواهد به سرور .ir وجود فرضا Jpc.ir را اعلام کند و نمیتواند و چون عمدتا قرار نیست این اتفاق بیافتد از این مرحله عبور میکنیم حال اگر ما یک Child Domain به Jpc.irاضافه کنیم چون ادمین فارست دارد یک دامین اضافه میکند میتواند پروسه Delegation را انجام دهد و بعبارت دیگر Child Domain به دامین Jpc.ir دسترسی دارد و در اینحالت پیغام خطایی دریافت نمیشود

- این امکان وجود دارد که اطلاعات فرضا Zone Jpc.ir را در DDP ذخیره کنیم ولی به دلایل مشخصی این کار را نمیکنیم و مطلوب ما نیست در ادامه به تشریح این موضوع می پردازیم

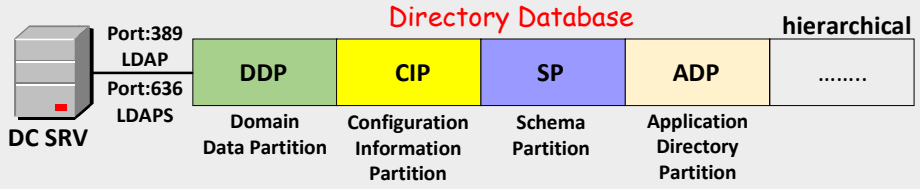


فرض **Forest A.com**
- **Domain A.com** (DC1+DNS),(DC2+DNS),DC3
- **Domain B.com** (DC4+DNS),(DC5+DNS),DC6

ADP DNS Partition

– این امکان وجود دارد که اطلاعات فرضا Zone Jpc.ir را در DDP ذخیره کنیم ولی به دلایل مشخصی این کار را نمیکنیم و مطلوب ما نیست در ادامه به تشریح این موضوع می پردازیم از ویندوز ۲۰۰۰ به قبل در DDP ذخیره میشده است

فرض
Forest A.com [Domain A.com (DC1+DNS),(DC2+DNS),DC3 — Domain B.com (DC4+DNS),(DC5+DNS),DC6]



1

– اگر فرض را بر این بگذاریم که اطلاعات Zone A.com در DDP A.com ذخیره شود و اطلاعات Zone B.com در DDP B.com ذخیره شود Scope Replication مطلوب ما نخواهد بود

– DDP A.com بین DC های دامین Replicate,A.com میشود چه DNS SRV باشند چه نباشند

– DDP B.com بین DC های دامین Replicate.B.com میشود چه DNS SRV باشند چه نباشند

– DC3,DC6 نیازی به این Replicate ندارند چون DNS SRV نیستند ولی بصورت اضافه انجام میشود

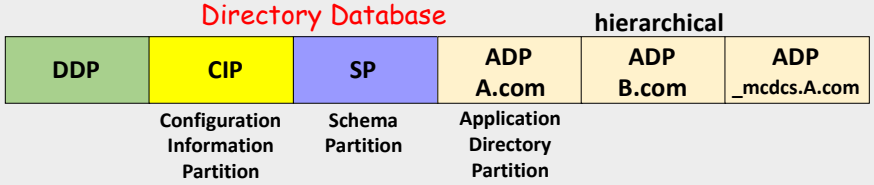
2

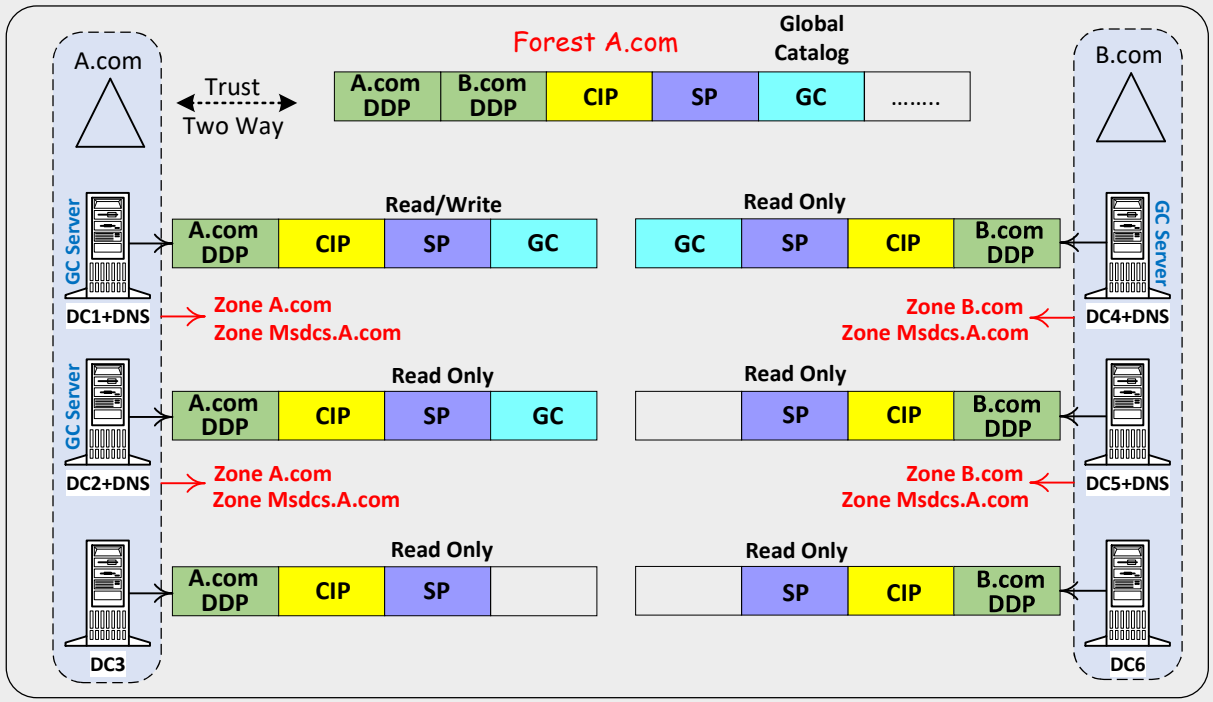
– میدانیم DC4 , DNS SRV دامین B.com و همچنین DNS SRV فارست A.com نیز میباشد بنابراین DC4 , DNS SRV و DC1 , DNS SRV ازهیث فارست A.com با هم همکارهستند و جهت پاسگویی به سوالات فارست A.com نیاز به _Msdcs.A.com خواهند داشت

– اگر _Msdcs.A.com در DDP A.com ذخیره شود در آنصورت به DC3 بصورت اضافی منتقل شده و به DC4,DC5 که باید منتقل شود انتقال داده نمیشود

– اگر _Msdcs.A.com در DDP B.com ذخیره شود در آنصورت به DC6 بصورت اضافی منتقل شده و به DC1,DC2 که باید منتقل شود انتقال داده نمیشود

این مشکل بدین صورت حل خواهد شد



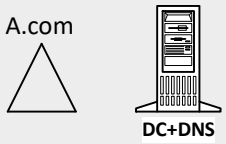


– در ADP A.com اطلاعات Zone A.com در آن ذخیره شده و بین DC+DNS Domain A.com تبادل Replicate میشود ⟵ (DC1,DC2)

– در ADP B.com اطلاعات Zone B.com در آن ذخیره شده و بین DC+DNS Domain B.com تبادل Replicate میشود ⟵ (DC4,DC5)

– در DDP _Msdcs.A.com اطلاعات Zone _Msdcs.A.com در آن ذخیره شده و بین DC+DNS Forest A.com تبادل Replicate میشود ⟵ (DC1,DC2,DC4,DC5)

بنابراین اگر یک دامین بعلاوه DNS راه اندازی کنیم مجموع Zone ها بدین شکل خواهد بود



A.com → Cheked Second Radio button when install **(Domain Scope)**

_msdcs.A.com → Cheked First Radio button when install **(Forest Scope)**

– این تغییرات اگر DNS همراه DC نصب شود ایجاد میشود ولی اگر از قبل Zone داشته باشیم محتویات DNS تغییر نمیکند و باید Zone را پاک نموده و از نو تعریف کنیم

I

- تعدادی از رکوردهایی که داخل یک Zone ثبت میشوند مربوط به **SRV Record/Service locator** میباشند و تعدادی از آن اعم از LDAP Server,Kerberos Server,GC Server,... مرتبط با DC میباشند و تنوع در زمینه رکوردهای غیرDC نیز وجود دارد مانند Skype record,Exchange Record,Time Server,...

- میدانیم کلاینت سرویس سرورش را بطور اتوماتیک به دو شکل میتواند پیدا کند یا از طریق **SCP AD** یا از طریق **SRV Record** نکته اینکه SRV Record ها بصورت اتوماتیک ساخته میشود ، جهت بحث ثبت اتوماتیک باید در تنظیمات شبکه DNS SRV آدرس DNS را بر روی 127.0.0.1 تنظیم کنیم تا برای ثبت اتوماتیک به خودش مراجعه کند

- میدانیم کامند Ipconfig /registerdns بر روی کلاینت و سرور باعث ثبت اتوماتیک A Record & PTR Record میشود ولی برای SRV Record از سرویس **Netlogon** استفاده میشود و باید ریستارت شود

- در تب General درحالت Secure only فقط کامپیوترهایی که Join to DC هستند میتوانند بصورت اتوماتیک رکورد ثبت کنند وفقط همان کامپیوتر میتواند رکورد داینامیک را تصحیح کند و برای الباقی فقط خواندنی میباشد

- در تب General درحالت None Secure and Secure همه کامپیوترهای میتوانند رکورد داینامیک ثبت کنند ولی آنهایی که Join to DC نیستند بصورت Non Secure میباشد

- در تب General درحالت None کلا داینامیک رکورد غیر فعال میباشد

- در AD integrated Zone اگر فرضا دو عدد DC+DNS با Primary Zone داشته باشیم چون هر دو متعلق به دایرکتوری هستند پیرو قاعده Replication ناگزیر همراه با آپدیت دایرکتوری Zone ها با هم Sync میشوند

مزایای AD Integrated Zone نسبت به Standard Zone

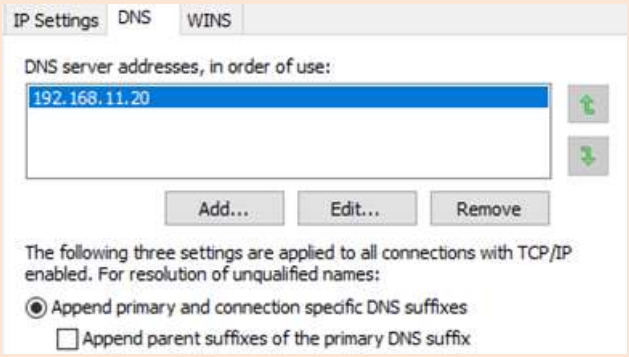
1 -مزیت امنیت (Security Tab) 2 -مزیت امنیت (Security Only On General Tab) 3 – فرایند Replication نسبت به Zone Transfer ایمن تر است 4 – ذخیره شدن Zone در دایرکتوری به جای فایل متنی

اضافه و پاک نمودن پارتیشن ADP با نام part1 به مجموعه پارتیشنهای دامین Jpc.local بر روی سرور Jpc-server.Jpc.local

```
partition management:create NC part1,dc=jpc,dc=local jpc-server.jpc.local
partition management:list
Found 6 Naming Context(s)
0 - CN=Configuration,DC=jpc,DC=local
1 - DC=jpc,DC=local
2 - CN=Schema,CN=Configuration,DC=jpc,DC=local
3 - DC=ForestDnsZones,DC=jpc,DC=local
4 - DC=DomainDnsZones,DC=jpc,DC=local
5 – DC=part1,DC=jpc,DC=local
partition management:delete NC  part1,dc=jpc,dc=local
partition management: list
Found 5 Naming Context(s)
0 - CN=Configuration,DC=jpc,DC=local
1 - DC=jpc,DC=local
2 - CN=Schema,CN=Configuration,DC=jpc,DC=local
3 - DC=ForestDnsZones,DC=jpc,DC=local
4 - DC=DomainDnsZones,DC=jpc,DC=local
```

```
C:\Users\Administrator>ntdsutil
ntdsutil: partition management
partition management: connections
server connections: connect to server jpc-server
Binding to jpc-server ...
Connected to tmgic-server using credentials of locally logged on user.
server connections: quit
partition management: list
Note: Directory partition names with International/Unicode characters
will only
display correctly if appropriate fonts and language support are loaded
Found 5 Naming Context(s)
0 - CN=Configuration,DC=jpc,DC=local
1 - DC=jpc,DC=local
2 - CN=Schema,CN=Configuration,DC=jpc,DC=local
3 - DC=ForestDnsZones,DC=jpc,DC=local
4 - DC=DomainDnsZones,DC=jpc,DC=local
```

I



تنظیمات DNS در سمت DNS Client

- مجموعه DNS SRV هایی که باید توسط کلاینت استفاده شوند به ترتیب میتوان اضافه نمود ⟵ **DNS Server Addresses , in order of use**

- باید مشخص کنیم جستجوی Parent تا کجا ادامه پیدا کند وگرنه آیتم ❷ کارنخواهد کرد و این موضوع از طریق تنظیم پالیسی بر روی DC مشخص خواهد شد

\\Filesrv. ⟶ Ip ?
\\Filesrv.ir ⟶ Ip ?
\\Filesrv.jpc.ir ⟶ Ip ?

Gpmc.msc ⟵ **Computer Configuration** ⟵ **Administrative Templates** ⟵ **Network** ⟵ **DNS Client**

Primary DNS suffix develoution level=3

\\Filesrv.club.jpc.ir
3 2 1

\\Filesrv.club.jpc.ir ⟶ Ip ?

\\Filesrv ⟵ **DNS**

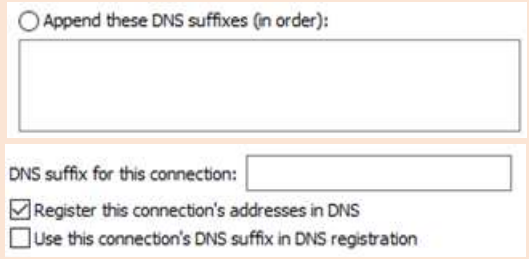
Club.jpc.ir ⟶ **Append parent suffixes of the primary DNS suffix** ❷

- اگر نام یک کلاینت را وارد کنیم در صورت عدم جواب از Primary Suffix ویندوز با اضافه نمودن نام Parent Suffix سعی میکند IP را برگرداند

\\Filesrv.sales.club.jpc.ir ⟶ Ip ?

Sales.Club.jpc.ir ⟶ **Append primary and connection specific DNS suffixes** ❶

- اگر نام یک کلاینت را وارد کنیم ویندوز با اضافه نمودن نام Primary Suffix سعی میکند IP را برگرداند



⟵ ❸ **Append these DNS Suffixes (in order)**

- میتوان به جای اضافه نمودن پالیسی و استفاده از حالت ❷ از چک مارک روبه رو و مشخص نمودن اولویت Suffix ها استفاده نمود

❹ **Register this connection's address in DNS** ⟶ - کانکشن کلاینت را به صورت داینامیکی در DNS درج مینماید

❺ **Use this connection's DNS suffix in DNS registration** ⟶ DNS Suffix For this connection: **Test.com**

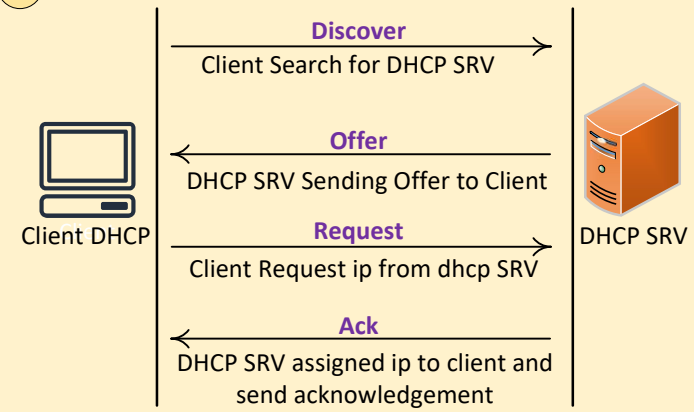
- کانکشن کلاینت را در Zone Test.com نیز بصورت داینامیکی درج مینماید

- از طریق ریستارت ویندوز کلاینت یا کامند Ipconfig /registerdns عمل داینامیکی درج نام کلاینت و IP آن در DNS انجام میپذیرد

II

DHCP Server

- در شروع این مبحث فرض بر اینست که کلاینت ها و سرور در یک Broadcast Domain قرار دارند و DHCP Client با Broadcast سعی میکند DHCP SRV را پیداکند به این موضوع DHCP Discover میگویند



DHCP SRV (223.1.2.5)

DHCP Discover	DHCP Offer	DHCP Request	DHCP Ack + Options
Src:0.0.0.0,68 dest:255.255.255,67 yiaddr:0.0.0.0 transaction ID:654	Src:231.1.2.5,67 dest:255.255.255,68 yiaddr:223.1.2.4 transaction ID:654 DHCP SRV ID:223.1.2.5 lifetime:3600 secs	Src:0.0.0.0,68 dest:255.255.255,67 yiaddr:223.1.2.4 transaction ID:654 DHCP SRV ID:223.1.2.5 lifetime:3600 secs	Src:223.1.2.5,67 dest:255.255.255,68 yiaddr:223.1.2.4 transaction ID:654 DHCP SRV ID:223.1.2.5 lifetime:3600 secs

Time ⟶

I

- بعلت اینکه در ابتدای کار سمت کلاینت فاقد IP میباشد مراحل اخذ IP از DHCP SRV بصورت Broadcast انجام میشود
- دلیل ۴ مرحله ای اخذ IP به این علت است که ممکن است در شبکه بیش از یک DHCP SRV وجود داشته باشد ضمنا کلاینت به DHCP Offer ی که زودتر دریافت کرده باشد DHCP Request میدهد و باعث میگردد تا سرور براند که آیا IP ی که Offer داده است مورد استفاده یکی از کلاینتها قرار خواهد گرفت یا خیر
- در بسته های تبادلی Destination Broadcast MAC برابر ۱۲ تا F میباشد ، در ضمن DHCP SRV بر روی پورت **Listen , 67 UDP** مینماید و DHCP Client با پورت **68 UDP** ارتباط برقرار میکند
- DHCP Client از یک آدرس لایه اپلیکیشنی به نام **Transaction ID** برای احراز هویت خود به DHCP SRV در هنگام تبادل بسته ها استفاده میکند
- اگر DHCP Client طی چند بار تلاش موفق به پیدا کردن DHCP SRV نشود به خود یک IP در رنج **169.254.x.y** میدهد که به آن اصطلاحا **Automatic Private IP Addressing (APIPA)** میگویند
- اگر کانکشن شبکه کلاینت را Disable/Enable کنیم یا کابل شبکه را قطع و وصل نمائیم و یا از طریق کامند دستور Ipconfig /renew را تایپ کنیم باعث میشود DHCP Discover مجددا انجام شود
- برای راه اندازی DHCP SRV ابتدا رول آن را از طریق Server Manager راه اندازی کرده و سپس آن را تنظیم مینمائیم — Dhcpmgmt.msc Run→ Dhcp Configuration
- قدم دوم در راه اندازی DHCP SRV بعد از نصب رول راه اندازی **Scope** میباشد تا امکان **DHCP Offer** برای سرور مهیا شود Scope شامل Address Pool or Range میشود
- به ازای هر Vlan ی که در آن DHCP Client وجود دارد در DHCP SRV باید یک Scope ساخته شود
- روش علمی و صحیح مشخص نمودن رنج بدین شکل است که مجموع IP های یک شبکه را مشخص کنیم و سپس رنج IP ی که نمیخواهیم به کلاینت ها داده شود Exclude نمائیم

- اصولا یک فضای ۱۰ درصدی از اول و آخر آدرس شبکه Exclude میشود
  Network IP Start:192.168.12.1 End:192.168.12.254 → Exclude IP Start:192.168.12.1 End:192.168.12.9
- اگر بیش از یک DHCP SRV داشته باشیم جهت تقدم و تاخر در Offer دادن از این گزینه میزان انتظار و بعد Offer استفاده میشود
  Subnet delay in mili second=0 →
- بعد از ساخت Scope یک فلش قرمز بر روی Scope وجود دارد چون هنوز عملیاتی نشده است و باید با کلیک سمت راست بر روی Scope آن را **Active** نمود تا فلش قرمز از روی Scope برداشته شود
- در این مقطع همچنان DHCP SRV بعلت فلش قرمز بر روی IPV4 یا IPV6 فعال نیست این موضوع علت امنیتی دارد چون ممکن است یک DHCP SRV بصورت Fake در شبکه وجود داشته باشد که اصطلاحا به آن **Rogue DHCP SRV** میگویند
- مایکروسافت برای حل حدودی این مشکل بدین شکل عمل میکند که اگر DHCP SRV مایکروسافتی و **Join to domain** باشد برای سرویس دادن باید **Authorize** شود و از برای اینکار مجوز بگیرد
- برای Authorize نمودن بر روی نام DHCP SRV کلیک سمت راست نموده و گزینه Authorize را انتخاب مینمائیم بعد از انجام اینکار چک مارک بر روی IPV4 و IPV6 به حالت سبز رنگ در می آید
- اگر یک سرور غیر مایکروسافتی DHCP SRV به کار گرفته شود بحث امنیتی Authorize منتفی خواهد بود پس موضوع Authorize نمودن DHCP SRV بیشتر جنبه مدیریتی دارد تا امنیتی
- برای حل مشکلات امنیتی اصولا در لایه های پایینتر باید مشکل را حل نمود بطور مثال در زیرساخت تبادل اطلاعات مانند فایروال ، سوئیچ و روتر مشکل را حل و فصل نمود
- به غیر از DHCP SRV سرورهای دیگری از قبیل SCCM DP , WDS ,... نیز ممکن است از طریق پنل DHCP SRV امکان Authorize شدن را پیدا کنند — DHCP → Manage Authorize Servers
- DHCP SRV از Scope ی به Offer , DHCP Client میدهد که با Primary ip address سرور یکی باشد
- اگر DHCP Client براند که DHCP SRV , IP پیست در صورت درخواست مجدد برای IP دیگر Discover نمیکند بلکه Request میدهد بدین معنی که Unicast عمل میکند و نه Broadcast
- قبل از DHCP SRV پرتکلی وجود دارد به نام **BootP SRV** که همچنان امکان برقراری این پرتکل وجود دارد — DHCP SRV → DHCP Client BootP SRV → BootP Client
- DHCP SRV بصورت پیش فرض به BootP Client سرویس نمیدهد ولی میتوان با Properties گرفتن از Scope و رفتن به گزینه Advanced بین حالتهای DHCP , BOOTP,Both سوئیچ نمود

I

R-Click On DHCP SRV

IPV4/Display Statistics → (start time,uptime,discovers,offers,request,acks,nacks,total scope,total address,inuse % ,available %)

IPV4/Scope/Reservation → – جهت رزرو Dynamic IP برای دستگاهها براساس MAC Address استفاده میشود

– با اجرای کامند Ipconfig /release بر روی کلاینت IP از قسمت Address releases DHCP SRV حذف شده و با اجرای کامند Ipconfig /renew بر روی کلاینت IP از سمت DHCP SRV به کلاینت واگزار میشود

– اگر DHCP SRV به یک کلاینت IP ی را واگزار کند در صورت خالی بودن همان IP و درخواست مجدد کلاینت همان IP را به کلاینت واگزار مینماید در غیر اینصورت اولین IP آزاد Scope را تخصیص میدهد

II

Options

– DHCP SRV به غیر از واگذاری IP این امکان را دارد تا مقادیر متنوعی از Option های مختلف را نیز در اختیار کلاینت قرار دهد

– Option ها حاوی نام و کد مربوطه میباشند مانند 003 Router,006 DNS servers,015 DNS Domain Name,042 NTP Servers,150 TFTP Servers

– سه جا میتوان Option تعریف نمود

1. Servers
   – هر کس از DHCP SRV درخواست IP کند Option های تعریف شده به درخواست کننده واگزار میشود
2. Scope Option
   – هر کس از Scope درخواست IP کند Option های تعریف شده به درخواست کننده واگزار میشود
3. Reservation Option
   – هر کس از Reservation , IP بگیرد Option های تعریف شده به درخواست کننده واگزار میشود

– در صورت تعارض اولویت از ۳ به ۱ میباشد و در صورت عدم تعارض جمع این سه در نظر گرفته میشود

3 → 2 → 1

III

ارائه متفاوت Options به برخی از کلاینتها بر اساس User Class

– کانکشن کارت شبکه DHCP Client حاوی یکسری Properties میباشد که یکی از آنها DHCP Class ID نام دارد و این ویژگی اگر IP استاتیک تعریف شده باشد کاربردی ندارد پس زمانی کاربرد پیدا میکند که تنظیمات شبکه کلاینت بر روی اتوماتیک تعریف شده باشد به کمک پارامتر ذکر شده میتوان کلاینتها را دسته بندی نمود و بر اساس این دسته بندی ها به آنها Option های مختلف اختصاص داد ضمنا DHCP Class ID حالت متنی Case Sensitive دارد

```
ipconfig/showclassid    Displays all the dhcp class IDs allowed for adapter.
ipconfig/setclassid     Modifies the dhcp class id.
ipconfig/showclassid6   Displays all the IPv6 DHCP class IDs allowed for adapter.
ipconfig/setclassid6    Modifies the IPv6 DHCP class id.
```

```
ipconfig /setclassid Ethernet test
Windows IP Configuration
Successfully set the DHCPv4 class id for adapter Ethernet
```

```
ipconfig /setclassid Ethernet
Remove Class Id
```

```
ipconfig /showclassid Ethernet
Ipconfig /all
View class id
```

– برای اعمال Option های مختلف به دسته بندیهای مختلف از Policies در سطح سرور یا Reservation استفاده میشود

– ابتدا باید معادل Client Class ID در سرور Define User Classes را بسازیم

– سپس پالیسی مربوطه را تعریف مینمائیم

– پالیسی بر اساس معیارهایی غیر از DHCP Class ID نیز امکان تعریف دارد

– اگر پالیسی های متعدد داشته باشیم ترتیب آنها را میتوانیم با بالا و پایین قراردادن پالیسی ها اولویت بندی کنیم

IPV4 —R-Click→ Define User Classes —Add→ test

IPV4/Scope/Policies —Add→ Policy Name —Add→ Criteria: User Classes / Operator:Equal / Value:test —Define Options→ Finish

IV

ارائه متفاوت Options به برخی از کلاینتها بر اساس Vendor Class

– از Vendor Class در بخش Advanced با کلیک سمت راست بر روی Option در سطوح مختلف مورد اشاره در بالا استفاده میشود ولی همانند User Class این مورد نیز باید بصورت خاص تعریف شود

– حال بعد از تعریف Vendor Class باید آپشنهای آن را نیز تعریف کنیم

– جهت تعریف دقیق باید به مستندات مرتبط مراجعه نمود بعلت اینکه درج فیلدها باید بر اساس مشخصات دقیق فنی صورت پذیرد

IPV4 —R-Click→ Define Vendor Classes —Add→ Linux

IPV4 —R-Click→ Define predefined options —Add→

تنظیم DHCP بطوریکه بر روی کلاینتها NetBIOS over TCP وضعیت Disable پیدا کنند

IPV4/server options —R-Click→ Configure options... —Advanced→ Microsoft options —Check Mark→ 001 Microsoft Disable netbios option —Data Entry→

0x0 = Default
0x1 = Enable NetBIOS Over TCP/IP
✓ 0x2 = Disable NetBIOS Over TCP/IP

I — DHCP Backup & Compact Database With Jetpack

- DHCP کلا هاوی یک فایل دیتا میباشد و همانند DNS نیست که به ازای هر Zone یک دیتا فایل داشته باشد قابل ذکر است که دیتا بیس DHCP,WINS از نوع Access میباشد — System32/dhcp/dhcp.mdb
- DHCP هر یکساعت یکبار بصورت اتوماتیک بکاپ گرفته میشود هرچند امکان بکاپ دستی نیز وجود دارد — DHCP Server Name R-Click → Backup
- امکان تغییر بکاپ اتوماتیک از طریق رجیستری وجود دارد — HKLM\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters
- در صورتی که فایل دیتای DHCP بزرگتر از 30MB شده باشد نیاز به Compact خواهد داشت و برای اینکار از ابزاری به نام Jetpack استفاده میشود

1. DHCP Server Name R-Click → All task → Stop
2. Cd system32\dhcp Run → jetpack dhcp.mdb temp.mdb
3. DHCP Server Name R-Click → All task → Start

Batch File

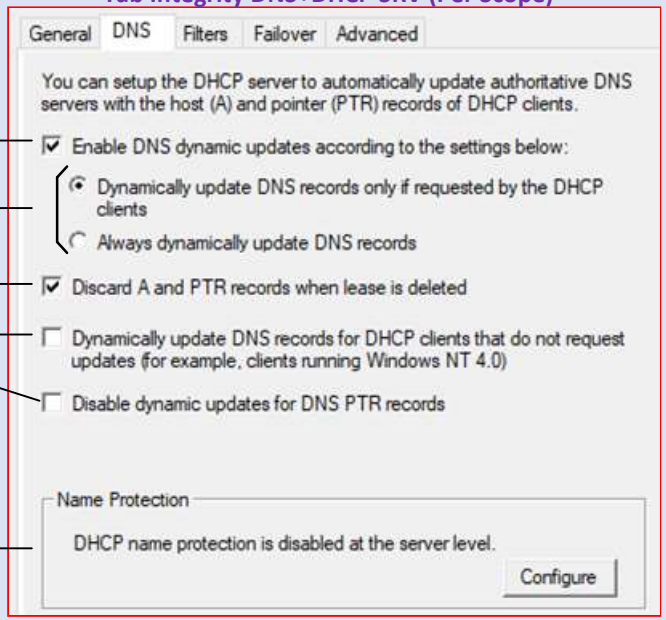
```
cd %SYSTEMROOT%\SYSTEM32\DHCP
NET STOP DHCPSERVER
jetpack Dhcp.mdb Tmp.mdb
NET start DHCPSERVER
```

- جهت ایجاد فایل Jetpack باید از طریق Server Manager رول Wins Server نصب شده باشد

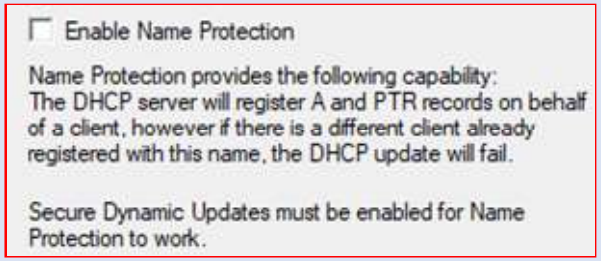
II — Integrity DNS Server + DHCP Server

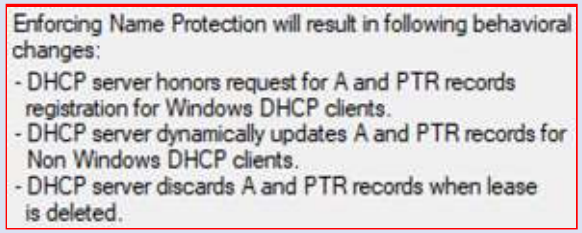
- وقتی صحبت از AD Integrated DNS میشود یعنی DDNS آن بصورت Secure Only میباشد — DC+DNS Zone:test.local → AD Integrated → DDNS → Secure Only
- وقتی DHCP Client از DHCP SRV آی پی میگیرد نوبت رجیستر کردن رکوردهایش(Host Record(A+PTR در DNS میشود
- اگر از **DHCP Relay Agent** در شبکه استفاده شود بدین شکل خواهد بود که DHCP Client از طریق Broadcast به Relay Agent میرسد و این سرویس با Unicast به سراغ DHCP SRV خواهد رفت و Relay نقش میانجی را بازی خواهد کرد
- DHCP Client هم خودش مستقلا میتواند Host Record را در DNS ثبت کند و هم میتواند از طریق DHCP SRV اقدام به انجام اینکار کند
- Win NT,IOS,Android نمیتوانند خودشان رکوردهایشان را در DNS ثبت کنند بدین معنی که DDNS ساپورت نیستند

Tab Integrity DNS+DHCP SRV (Per Scope)



- با برداشتن این Mark دیگر DHCP SRV دخالتی برای ثبت رکورد در DNS ندارد و در صورت Mark بقیه گزینه ها نحوه دخالت را مشخص میکنند
- مربوط به کلاینتهایی است که DDNS را ساپورت میکنند و در حالت اول تصمیم برای ثبت رکورد در DNS به کلاینت واگذار میشود و در حالت دوم در هر حالتی ثبت رکورد در DNS به DHCP SRV واگذار خواهد شد
- برای کلاینتهایی که دوره اختصاص آی پی آنها گذشته است Host Record آنها از DNS حذف شود
- برای کلاینتهایی که نمیتوانند خودشان ثبت رکورد در DNS انجام دهند با زدن این Mark سرور DHCP مبادرت به انجام این کار می نماید
- حالت ثبت رکورد PTR در DNS برای کلاینتها از طریق DHCP SRV غیر فعال میباشد





- **Name Protection** باعث غیر فعال شدن همه گزینه ها به جز گزینه اول میشود و شرط آن اینست که DDNS بصورت Secure only باشد و دیگر اینکه اگر رکوردی از قبل ثبت شده باشد DHCP SRV نمیتواند مجدد رکورد را ثبت نماید

I

- وقتی Name Protection فعال میشود یک مشکل امنیتی بوجود می اید و آن هم اینست که امکان ثبت رکورد فیک توسط کلاینت در DNS SRV فراهم میگردد و البته این موضوع باتوجه به امکان ثبت Black List در DNS تا حدود زیادی جلوی ثبت رکوردهایی به طور مثال Mail,www,... را میگیرد


DHCP SRV1
192.168.1.1-127


Client DHCP


DHCP SRV2
192.168.1.128-254

- فرض میکنیم بعد از Discover کردن توسط کلاینت Offer DHCP SRV1 زودتر به کلاینت رسیده باشد و کلاینت آی پی **192.168.1.100** را گرفته و بواسطه Name Protection Host Record در DNS ثبت شده باشد حال اگر سروری که آی پی داده خاموش شود فرض آی پی **192.168.1.200** را کلاینت میگیرد ولی اینبار نمیتواند به علت عملکرد Name Protection آن را در DNS ثبت نماید چون مالک آی پی DHCP SRV1 میباشد
- برای حل این مشکل میتوان یک یوزر در AD ثبت نمود و از طریق **IPV4/advanced/credentials** آن را به هر دو سرور معرفی نمود و با این شرایط مالک برای ثبت رکورد در سرورهای DHCP نام یوزری است که ثبت کرده ایم و نه نام کامپیوتر اکانت DHCP SRV

- در کل استفاده از Name Protection به شرط به کارگیری Credential User توصیه میشود
- جهت بررسی عملکرد DHCP SRV و کانفیگ آن نیاز به یک اپلیکیشن در حوزه Service Monitoring مانند Scom داریم

Reconcile

- مواردی ارقبیل Scope در کانفیگ ذفیره میشود و مجموعه اطلاعات مرتبط به آن که به مرور اضافه میشود در دیتا فایل ذفیره میگردد اگر بین این دو تضادی پیش بیاید مثلا Scope یا دیتا پاک شود به نوعی بین این دو نیاز به دوستی و صلح است

Scope R-Click → Reconsile

IPV4 R-Click → Reconsile All Scopes

- اگر پیغام Database is Consistent برگردانده شود یعنی تضادی پیدا نشده است

II

DHCP HA

- DHCP در حالت Stateful کار میکند و کاربر در تغییرات دخیل نمیباشد
- برای پیاده سازی **DHCP HA** چندین روش وجود دارد

1 روش اول Split Scopes

- در روش اول تاتقسیم رنج آی پی بین DHCP SRV ها امکان تکراری شدن را از سرورها سلب میکنیم ، در صورتیکه تعداد کلاینتها بیش از 50% کل آی پی ها باشد اگر یکی از سرورها از دور خارج شود سرور دیگر جوابگو نمیباشد


DHCP SRV1
Scope1:192.168.1.1-254
Exclude(1-127)


DHCP SRV2
Scope1:192.168.1.1-254
Exclude(128-254)

- فرض کنیم که کلاینت A از DHCP SRV2 آی پی 192.168.1.200 را دریافت نموده و بعد از آن سرور DHCP SRV2 Down شده است حال وقتی کلاینت A به سرور DHCP SRV1 مراجعه میکند چون در Exclude آن این آی پی موجود است سرور DHCP SRV1 بجای Ack با Nack پاسخ کلاینت را میدهد و باعث میشود کلاینت همچنان با همان آی پی به کار خود ادامه دهد

- از ایرادات این روش این است که باید بر روی همه سرورها تقسیم بندی درصدی و دقیق که با هم Overlap نشوند انجام داد و برای هر تغییری در Scope,option باید به همه سرورها مراجعه نمود و در عمل مدیریت غیر متمرکز است
- برای اینکه بفهمیم که هر کدام از سرورها چه آی پی به کلاینت ها اختصاص داده اند محل متمرکزی وجود ندارد و به هر کدام باید مستقلا مراجعه نمود
- در مجموع **Monitoring** و **Management** غیر متمرکز میباشد
- از ویندوز 2008R2 به بعد پیاده سازی این روش راحت تر انجام میگیرد بطوری که روی سرور اول Scope را میسازیم و با R-Click بر روی آن امکان Advance\Splite Scope را داریم ولی این فقط برای بار اول است واگر تغییری در Scope ها صورت پذیرد بر روی همه سرورها بصورت جداگانه باید اعمال گردد

2 روش دوم Failover Clustering

- میتوانیم از Feature Failover Clustering ویندوز استفاده کنیم بدین معنی که چندین DHCP SRV را داخل یک Faileover Clustering قرار دهیم این کار ممکن است ولی مطلوب نیست چون پیچیدگی آن بالا است

3 روش سوم DHCP Failover

- از ویندوز 2012 به بعد قابلیتی بعنوان DHCP Failover اضافه شد که از همین روش نیز اصولا استفاده میشود
- در این روش به ازای هر Scope دو عدد DHCP SRV میتوان راه اندازی نمود و این دو سرور در مورد آی پی ها باهم تعامل دارند
- ابتدا باید Scope ها بر روی یکی از سرورها ساخته شود و بعد DHCP Failover بر روی یکی از مد های **Load Balance, Hot standby** را برقرار نمود


DHCP SRV1
Scope1:192.168.1.1-254


DHCP SRV2
Scope1:192.168.1.1-254

DHCP Server Name\IPV4 R-Click → Configure Failover

I

- DHCP Failover فقط شامل Scope ها میشود و برای Option ها باید بصورت مستقل برای هر سرور اقدام نمود پس حالت بهینه بدین شکل است که ابتدا Option ها بر روی هر دو سرور بصورت یکسان پیاده سازی شود و بعد بر روی یکی از سرورها Scope را تعریف نموده و بعد از آن DHCP Failover را راه اندازی نمائیم در هر صورت بعد از راه اندازی نیز باید حتما Option ها بصورت مستقل تعریف شود

- وقتی یک تغییری بر روی Scope یکی از سرورها انجام میدهیم باید بر روی همان سرور از طریق Scope\Replicate Scope تغییرات را بین دو سرور Sync نمود

- برای استفاده از Hot Standby باید پورت TCP 647 بین دو سرور باز باشد

Unicast Scope , SuperScope , MulicastScope

Unicast Scope

- Scope هایی که تا الان تعریف شده است Unicast Scope میباشد

Multicast Scope

- امکان تعریف Multicast Scope در مایکروسافت وجود دارد

DHCP Server Name\IPV4 → R-Click → New multicast Scope **Valid Range (224.0.0.0 – 239.255.255.255)**

Super Scope

- Super Scope از یک یا چند Scope درست میشود بنابراین یک Scope یا به هیچ Super Scope ی تعلق ندارد و یا نهایتا عضو یک Super Scope میباشد

- میدانیم در شبکه وقتی میخواهیم فرضا DC ها را از 2019 به 2022 ارتقاء دهیم ابتدا یک DC جدید 2022 راه اندازی میکنیم و پس از انتقال رولها به سرور جدید و مدتی کار کردن سر ورهای قدیمی بطور موقت خاموش شده و پس از مدتی بطور کامل حذف میشود

- فرض کنیم یک Scope بدین شکل داشته باشیم 192.168.1.1-254 که برای Vlan خاصی به تعداد 50 کلاینت مد نظر قرار گرفته بود حال طی مرور زمان تعداد کلاینتها به 500 رسیده است در این شرایط یک علامت تعجب آبی رنگ به نشانه بروز یک مشکل بر روی Scope درج میشود جهت تبدیل این Scope به Scope بزرگتر بدون Down Time فرضا یک Scope دیگر به شکل 172.16.X.X میسازیم برای کلاینتهایی که به آنها آی پی نرسیده و APIPA شده اند حال هر دو رنج را در یک Super Scope قرار میدهیم تا سرور بتواند به هر دو رنج پاسخ دهد سپس همه آی پی های رنج اول را Exclude میکنیم تا همه از رنج دوم آی پی بگیرند پس از مدتی رنج اول را از Super Scope پاک میکنیم در واقع Super Scope یک فرایند Migration از یک Scope کوچک به یک Scope بزرگتر میباشد

DHCP SRV1
Scope1:192.168.1.1-254 → Scope2:172.16.1.1-172.16.3.254
Exclude(1-254)

Superscope : superscope

- چون کل رنج را در Scope1 بصورت Exclude درآورده ایم از Scope2 به کلاینتها آی پی میدهد فقط ذکر این نکته مهم است چون رنج Scope1 را در سرور داریم این امکان فراهم میشود که از Scope2 کلاینتها آی پی بگیرند و در نهایت پس از اتمام کار ابتدا Super Scope را پاک میکنیم ولی باعث نمیشود Scope ها پاک شوند و نهایتا Scope1 را پاک میکنیم

- کامپیوتری که بیش از یک کارت شبکه داشته باشد به آن **Multihomed** گفته میشود

- Broadcast Domain ی که داخل آن چند Netid باشد **Multinet** گفته میشود یعنی یک سگمنت و یک Broadcast Domain داریم با Netid های مختلف

II

Export, import and migrate a DHCP server

MIgration

DHCP SRV1 Win2019 → **Export** → **Import** → DHCP SRV1 Win2022

CMD

```
netsh dhcp server export C:\dhcp.txt all
netsh dhcp server import c:\dhcp.txt all
```

Power Shell

```
Export-DhcpServer
Import-DhcpServer
```

Confilict Detection Attempts

DHCP Server Name\IPV4 → R-Click → Advanced\Confilict Detection Attempts

- یک کلاینت وقتی به هر طریقی استاتیک یا داینامیک آی پی میگیرد تا وقتی مطمئن نشود که کس دیگری از آن استفاده نمیکند حق استفاده از آی پی را ندارد

- اینکه یک آی پی در شبکه با دیگر آی پی ها Conflict ندارد توسط پرتکل ARP انجام میشود

- کلاینت اگر آی پی از سرور بگیرد و پس از تست متوجه شود در شبکه کانفلیکت دارد موضوع را به سرور اطلاع میدهد و سرور آن آی پی را Bad Address درج مینماید و یک آی پی دیگری به کلاینت میدهد و سرور خودش تلاشی برای پیدا کردن کانفلیکت انجام نمیدهد که حالت پیش فرض است حال اگر عدد Confilict Detection Attempts را مثلا برابر با ۲ قرار دهیم از این به بعد سرور قبل از اینکه یک آی پی را در اختیار کلاینت قرار دهد به تعداد ۲ بار تلاش میکند تا کانفلیکتی در شبکه پیدا نکند و بعد به کلاینت Offer میدهد این تعداد حداکثر میتواند ۵ بار در نظر گرفته شود

- Attack ی در DHCP SRV وجود دارد به نام **DHCP Starvation** که باعث میشود کلاینت قربانی کل آی پی ها را به سرور کانفلیکت اعلام کند و نهایتا کل Scope از طرف سرور به حالت Bad Address در آید بنابراین تنظیم Detection Attempts جلوی این حمله را بطور کامل نمیگیرد چون بعد از چند بار امکان حمله وجود دارد ضمنا با تغییر MAC نیز میتوان همین حمله را بوجود آورد

I

- یکی از Use Case های استفاده از Detection Attempts میتواند این باشد که یک DHCP SRV خراب شده باشد و سرور جدیدی با همان شرایط Scope قبلی بالا آورده باشیم با توجه به زمان Leased سرور قبلی مسلما به Conflict IP برخورد خواهیم کرد حال میتوانیم Detection Attempts=2 قرار دهیم و بعد از دو سه روز Bad Address ها را پاک نموده و مجددا Detection Attempts را به عدد صفر تغییر دهیم

IPAM (IP Address Management)

- در Server Virtualization(Hyperv- ESXI) از منابع استفاده حداکثری میشود ولی این استفاده بهینه نیست و برای بهینه شدن باید به مفاهیم Container(Docker) پردافت
- اگر بخواهیم برانیم که یک آی پی در حال حاضر روی چه دستگاهی ست شده است اگر استاتیک باشد عموما از روی فایل اکسلی که تهیه میشود مشخص میگردد و اگر داینامیک باشد از روی DHCP SRV حال اگر بخواهیم یک آی پی فرضا ۱۰ ماه قبل بر روی چه دستگاهی بوده است نقش IPAM معلوم میگردد چون در اینحالت History نیز بر روی ثبت IP ها داریم
- اینکه History آی پی ها را داشته باشیم یکی از علتهایش موارد مرتبط با جرم شناسی Forensic میباشد بدین معنی که به شبکه حمله ای شده است و میخواهیم منشاء آن مشکل امنیتی را بدست آوریم
- میتوان DHCP SRV ها را داخل IPAM آورد و از طریق آن آی پی ها مدیریت نمود وآی پی رزرو نمود یا Option تخصیص داد و همچنین DNS SRV ها را و برخی سرویس های دیگر
- از IPAM مایکروسافت خیلی استقبال نشده است چون امکان گزارش گیری دقیق وجود ندارد بنابرای عمدتا از غیر مایکروسافتی استفاده میشود مانند Solarwind IPAM و میتوان از Open Source لینوکسی نیز بهره برد
- IPAM مایکروسافت داخل Features ها قرار دارد و از آن طریق نصب میگردد و IPAM راه اندازی پیچیده ای دارد و خروجی غیر جذاب

II

RAID (redundant array of independent disks)

System → Subsytem → CPU, RAM, ✓Disk, NIC

- به منابعی که برای ذخیره کردن اطلاعات استفاده میشود Storage میگویند و با توجه به اهمیت دیتا از بین اجزای سیستم Storage از همه مهم تر است
- اصولا یک فضایی در اختیار OS قرار میگیرد که توسط فایل سیستم OS آن فضا فرمت شده و مورد استفاده قرار میگیرد
- Storage میتواند بخشی از یک دیسک باشد یا اجتماعی از چندین دیسک

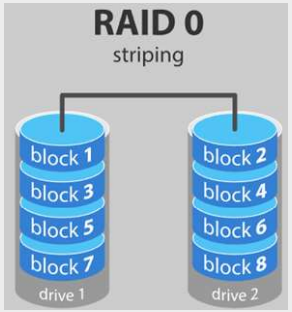
RAID (redundant array of independent disks)=Disk Group+Rule or Policy

- Raid مجموعه از دیسکها است که طبق یک قاعده مشخص با هم جهت ذخیره دیتا همکاری میکنند نحوه همکاری میتواند باعث تحمل خرابی FT و کارایی IOPS (input/output per second) یا فراهم کردن فضای بزرگتری برای ذخیره اطلاعات شود Raid با ید حداقل FT یا IOPS یا هر دو را در اختیار ما بگذارد و اگر فقط به ما افزایش دیسک دهد و نه دو پارامتر دیگر به آن دیگر Raid نمیگوییم بلکه از آن بعنوان JBOD(just a bunch of disks) یاد میگردد و اسم مایکروسافتی آن که بصورت نرم افزاری برقرار میگردد Spaned Volumes گفته میشود

RAID

RAID 0 – striping
RAID 1 – mirroring
RAID 5 – striping with parity
RAID 6 – striping with double parity
RAID 10 – combining mirroring and striping

- Raid میتواند Hardware یا Software پیاده سازی گردد در حالت سخت افزاری یک Raid Controller جهت برقراری Raid وجود خواهد داشت
- در حالت Raid سخت افزاری باید الزاما همه دیسکها از یک نوع باشند (IDE,SCSI,SATA,SAS,...) ولی در حالت نرم افزاری چنین محدودیتی وجود ندارد و حتی میتوان بخشی از دیسک را استفاده نمود که دلیل بر بسیار انعطاف پذیر بودن است ولی قدرتمندی و استحکام سخت افزاری را ندارد



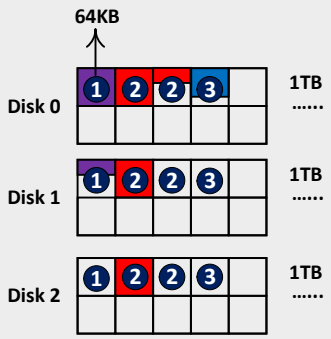
In a RAID 0 system data are split up into blocks that get written across all the drives in the array. By using multiple disks (at least 2) Untill 32 at the same time, this offers superior I/O performance. This performance can be enhanced further by using multiple controllers, ideally one controller per disk

Advantages of RAID 0

RAID 0 offers great performance, both in read and write operations. There is no overhead caused by parity controls. All storage capacity is used, there is no overhead.The technology is easy to implement.

Disadvantages of RAID 0

RAID 0 is not fault-tolerant. If one drive fails, all data in the RAID 0 array are lost. It should not be used for mission-critical systems.



- اگر بلوک N ام از دیسک 0 برای ذخیره کردن یک فایل استفاده شود بلوک N ام از همه دیسکهای Raid 0 برای آن فایل استفاده خواهد شد

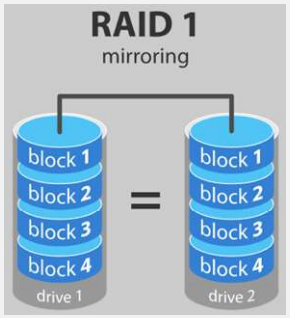
1 1.txt=100KB
2 2.txt=200KB
3 3.txt=50KB

- در این مثال سرعت خواندن و نوشتن سه برابر بیشتر از استفاده از یک هارد خواهد شد
- از این نوع Raid برای اطلاعات کم اهمیت تر مانند Page File,cache استفاده میشود، در واقع اصل این نوع دیتا جای دیگری قرار دارد و برای دسترسی سریعتر از این روش استفاده میکنیم

Data → ✓Temporary Data, Data, OS

- این Raid میتواند با الباقی Raid های پایه ای ترکیب شود

I



Data are stored twice by writing them to both the data drive (or set of data drives) and a mirror drive (or set of drives). If a drive fails, the controller uses either the data drive or the mirror drive for data recovery and continuous operation. You need at least 2 drives for a RAID 1 array.

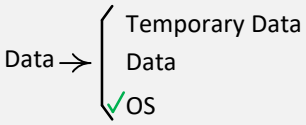
Advantages of RAID 1

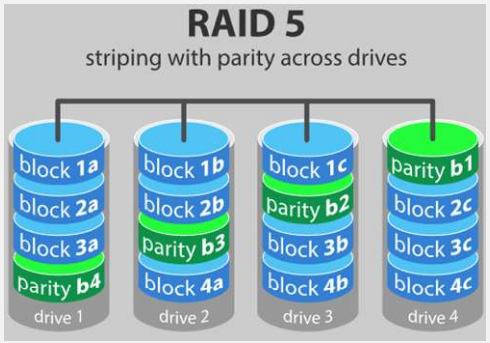
RAID1 offers excellent read speed and a write-speed that is comparable to that of a single drive .In case a drive fails, data do not have to be rebuild, they just have to be copied to the replacement drive. RAID 1 is a very simple technology.

Disadvantages of RAID 1

The main disadvantage is that the effective storage capacity is only half of the total drive capacity because all data get written twice .Software RAID 1 solutions do not always allow a hot swap of a failed drive. That means the failed drive can only be replaced after powering down the computer it is attached to. For servers that are used simultaneously by many people, this may not be acceptable. Such systems typically use hardware controllers that do support hot swapping.

- در اینحالت دیتا بیت به بیت در هر دو درایو ذفیره میشود
- تاثیری در افزایش Performance ندارد ولی مایکروسافت مدعی است که در حالت نرم افزاری بطور همزمان از هر دو دیسک اطلاعات خوانده میشود ، در این وضعیت با افزایش Performance در خواندن اطلاعات مواجه خواهیم بود
- مسلما تحمل خرابی یک دیسک در اینحالت وجود دارد ولی هزینه آن بالا است بدین معنی که فرضا دو دیسک ۸ ترابایتی به کار گرفته میشود ولی به اندازه یک دیسک ظرفیت ذفیره سازی وجود دارد
- از این روش عموما برای ذفیره سازی سیستم عامل با استفاده از ۲ عدد دیسک ظرفیت پایین استفاده میشود





RAID 5 is the most common secure RAID level. It requires at least 3 drives but can work with up to 16. Data blocks are striped across the drives and on one drive a parity checksum of all the block data is written. The parity data are not written to a fixed drive, they are spread across all drives, as the drawing below shows. Using the parity data, the computer can recalculate the data of one of the other data blocks, should those data no longer be available. That means a RAID 5 array can withstand a single drive failure without losing data or access to data. Although RAID 5 can be achieved in software, a hardware controller is recommended. Often extra cache memory is used on these controllers to improve the write performance.

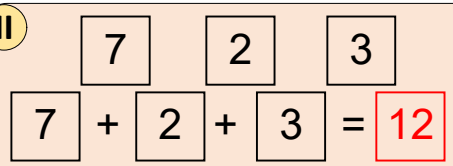
Advantages of RAID 5

Read data transactions are very fast while write data transactions are somewhat slower(due to the parity that has to be calculated .)If a drive fails, you still have access to all data, even while the failed drive is being replaced and the storage controller rebuilds the data on the new drive.

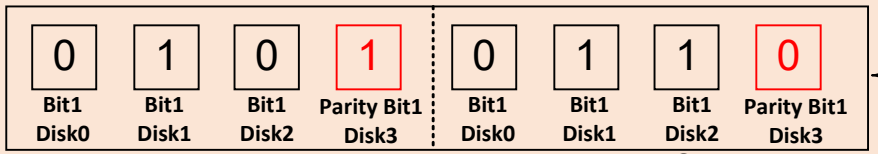
Disadvantages of RAID 5

Drive failures have an effect on throughput ,although this is still acceptable .This is complex technology. If one of the disks in an array using 4TB disks fails and is replaced, restoring the data (the rebuild time) may take a day or longer, depending on the load on the array and the speed of the controller. If another disk goes bad during that time, data are lost forever.

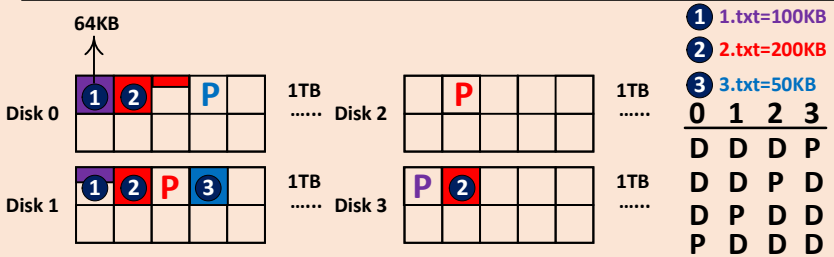
II



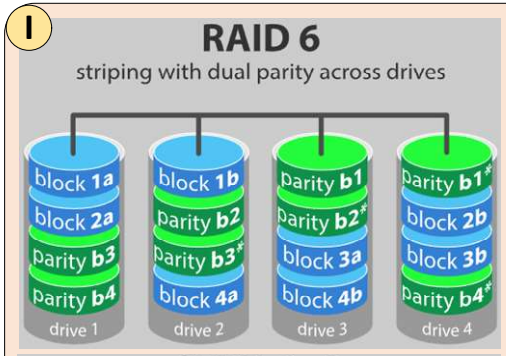
- میتوان گفت RAID 5=RAID 0 + Parity البته این صرفا تشبیه است
- فرض کنیم بر روی سه عدد کاغذ یادداشت کوچک ۳ عدد را درج نموده ایم و میخواهیم کاری کنیم که اگر یکی از این کاغذها از دست رفت عددی که بر روی آن درج شده از بین نرود چه زغاک ،ارمی ایجاد میکنیم که جمع جبری سه کاغذ دیگر است که Parity نامیده میشود حال اگر کاغذ عدد ۷ از بین برود با کاغذ چهارم امکان بدست آوردن آن عدد میسر خواهد بود

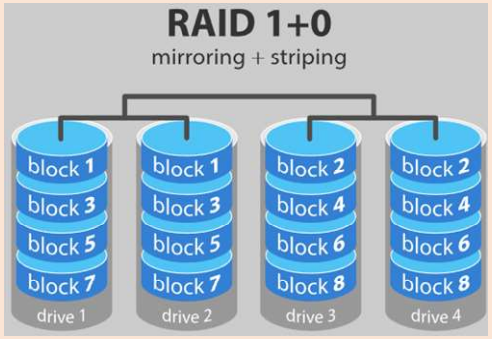


- فرض بر اینکه Parity Bit بر این اساس کار کند که تعداد زوج ها یک شود بدین صورت دو مثال از بیت یک دیسک ها آورده شده است
- نوشتن اطلاعات به علت محاسبه Parity باعث کمی کندی سرعت در نوشتن میشود
- در صورت خرابی یکی از هارد دیسکها سرعت نوشتن با توجه به محاسبه Parity باعث کندی محسوسی میشود
- Parity باعث میشود FT برست آید البته باهزینه خیلی کمتر از Raid 1 ولی با تحمل خرابی برابر با Raid 1 که یک هارد خواهد بود
- Parity برروی هارد دیسک ها به نوبت میچرخد و باعث میشود که به هارد فشار وارد نشود
- اگر بلوک N ام از دیسک 0 برای ذخیره کردن یک فایل استفاده شود بلوک N ام از همه دیسکهای Raid5 برای آن فایل استفاده خواهد شد
- اگر در Raid5 دو عدد هارد خراب شود کل دیتا از بین خواهد رفت جهت حل این مشکل یک دیسک Hot Spare تعریف میکنند که حالت Stand By دارد و در صورت خراب شدن هارد اول بصورت بر فط جایگزین خواهد شد که این حالت سفت افزاری است و در این حالت اگر نیاز به دخالت انسانی باشد به آن Cool Spare میگویند



I





RAID 6 is like RAID 5, but the parity data are written to two drives. That means it requires at least 4 drives and can withstand 2 drives dying simultaneously. The chances that two drives break down at exactly the same moment are of course very small. However, if a drive in a RAID 5 systems dies and is replaced by a new drive, it takes hours or even more than a day to rebuild the swapped drive. If another drive dies during that time, you still lose all of your data. With RAID 6, the RAID array will even survive that second failure.

Advantages of RAID 6

Like with RAID ,5 read data transactions are very fast .If two drives fail, you still have access to all data, even while the failed drives are being replaced. So RAID 6 is more secure than RAID 5.

Disadvantages of RAID 6

Write data transactions are slower than RAID 5 due to the additional parity data that have to be calculated. In one report I read the write performance was 20% lower.

Drive failures have an effect on throughput ,although this is still acceptable .This is complex technology. Rebuilding an array in which one drive failed can take a long time.

It is possible to combine the advantages (and disadvantages) of RAID 0 and RAID 1 in one single system. This is a nested or hybrid RAID configuration. It provides security by mirroring all data on secondary drives while using striping across each set of drives to speed up data transfers.

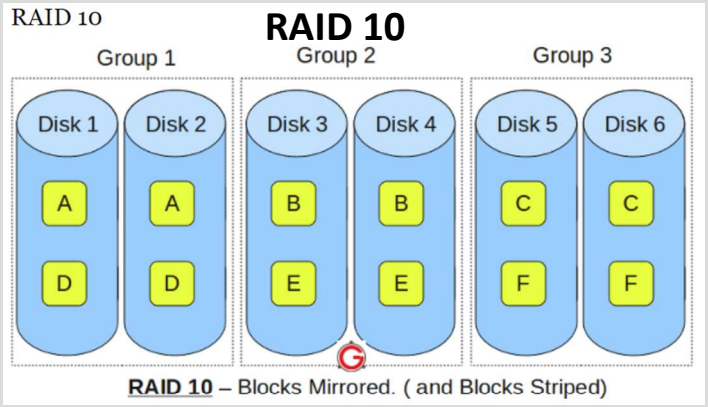
Advantages of RAID 10

If something goes wrong with one of the disks in a RAID 10 configuration, the rebuild time is very fast since all that is needed is copying all the data from the surviving mirror to a new drive. This can take as little as 30 minutes for drives of 1 TB.

Disadvantages of RAID 10

Half of the storage capacity goes to mirroring, so compared to large RAID 5 or RAID 6 arrays, this is an expensive way to have redundancy.

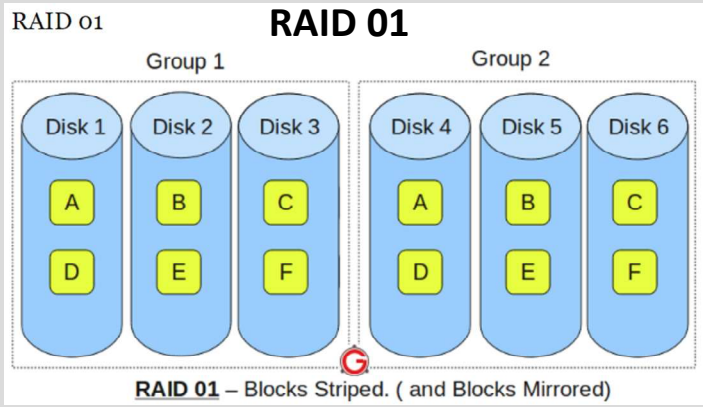
II



RAID 10 is also called as RAID 1+0

It is also called as "stripe of mirrors"

It requires minimum of 4 disks To understand this better, group the disks in pair of two (for mirror). For example, if you have a total of 6 disks in RAID 10, there will be three groups–Group 1, Group 2, Group 3 as shown in the above diagram. Within the group, the data is mirrored. In the above example, Disk 1 and Disk 2 belongs to Group 1. The data on Disk 1 will be exactly same as the data on Disk 2. So, block A written on Disk 1 will be mirroed on Disk 2. Block B written on Disk 3 will be mirrored on Disk 4. Across the group, the data is striped. i.e Block A is written to Group 1, Block B is written to Group 2, Block C is written to Group 3. This is why it is called "stripe of mirrors". i.e the disks within the group are mirrored. But, the groups themselves are striped.



RAID 01 is also called as RAID 0+1

It is also called as "mirror of stripes"

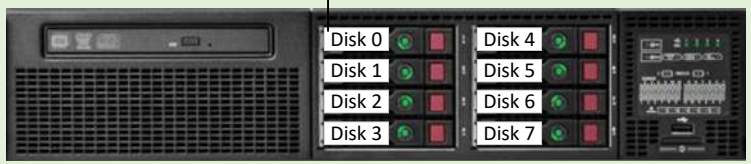
It requires minimum of 3 disks. But in most cases this will be implemented as minimum of 4 disks. To understand this better, create two groups. For example, if you have total of 6 disks, create two groups with 3 disks each as shown below. In the above example, Group 1 has 3 disks and Group 2 has 3 disks. Within the group, the data is striped. i.e In the Group 1 which contains three disks, the 1st block will be written to 1st disk, 2nd block to 2nd disk, and the 3rd block to 3rd disk. So, block A is written to Disk 1, block B to Disk 2, block C to Disk 3. Across the group, the data is mirrored. i.e The Group 1 and Group 2 will look exactly the same. i.e Disk 1 is mirrored to Disk 4, Disk 2 to Disk 5, Disk 3 to Disk 6. This is why it is called "mirror of stripes". i.e the disks within the groups are striped. But, the groups are mirrored.

I

Storage (DAS)

Storage → 1 Direct-attached storage (DAS) / 2 Network-attached storage (NAS) / 3 Storage Area Network (SAN)

- به منابعی که برای ذخیره کردن اطلاعات استفاده میشود Storage میگویند
- DAS مستقیما به سیستم وصل ، شناسایی و قابل استفاده Connect,detect,usable میشود
- دسترسی به Storage به دوشکل اتفاق می افتد 1 File Level Access 2 Block Level Access
- در DAS چون سیستم عامل مستقیما به آن متصل است و Storage را کنترل میکند بدین معنی که فایل سیستم را بر روی Storage میسازد ، دسترسی از نوع Block Level میباشد



{Disk0,1,2,3,4,5,6,7}=Srorage Pool or Storage Space

{Disk6,7}=Hot Spare

{Disk0,1,2,3,4,5}=RAID 5 = 5TB

- چون سیستم عامل مستقیما فضای ذخیره سازی را فرمت کرده و کنترل میکند بنابراین دسترسی از نوع Block Level میباشد
- اصولا فایل سیستم در اختیار هر کسی باشد دسترسی آن به فضای ذخیره سازی Block Level میباشد

← Enclosure

- در صورت نیاز به فضای بیشتر از Enclosure استفاده میکنیم بطوریکه عموما این دستگاه از طریق یک رابط فیزیکی مانند کابل SAS به کنترلر SAS سرور متصل شده و یک Storage Pool بزرگ در اختیار ما میگذارد
- فضای ذخیره سازی در DAS را میتوان برای دیگر کامپیوترها از طریق تکنیکهای مختلفی همچون Share folder,ISCSI,SMB,NFS در شبکه به اشتراک گذاشت ، در اینحالت نحوه دسترسی کلاینتها به DAS بصورت File Level میباشد
- مفهوم File Level دسترسی غیر مستقیم به فضای ذخیره سازی میباشد در اینحالت دستور از طریق کلاینت به دستگاهی که از طریق سیستم عامل دسترسی مستقیم Block Level دارد ارسال شده و توسط آن دستگاه بر روی فضای ذخیره سازی اجرا میشود

Storage (NAS)

- فضای ذخیره سازی سفت افزاری که بصورت کامپکت شده حاوی سیستم عامل سفارشی شده و اینترفیس های شبکه ای باشد و امکان اتصال مستقیم به سوئیچ برای آن مهیا شده باشد را NAS میگوئیم

II

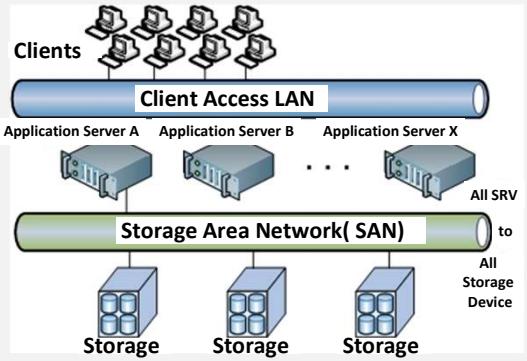
Storage (SAN)

- وقتی از یک زیر ساخت تبادل اطلاعات بر پایه اترنت جهت دسترسی کلاینتها و سرورها به فضای ذخیره سازی استفاده میکنیم ممکن است از لحاظ امنیتی و کارائی جهت کلاینتها مقبول باشد ولی برای سرورها ممکن است مورد قبول نباشد چون سرور ممکن است با استفاده از فضای ذخیره سازی سرویسی ارائه برهد و در زمان پیک کاری باعث کاهش چشمگیر عملکرد سرور شود در این حالت شبکه سرورها با Storage از الباقی شبکه توسط SAN مجزا میشود
- SAN یک شبکه است جهت دسترسی سرور ها به فضای ذخیره سازی و شبکه ای مستقل با امنیت و کارائی بالا ، در این شبکه سرورها با Storage و Storage با Storage در ارتباط میباشد
- جهت بدست آوردن بالاترین کارائی در شبکه SAN از Fiber Channel(FC) به جای Ethernet استفاده میشود و FC تکنولوژی میباشد که بواسطه آن تجهیزات و ارتباطات SAN ساخته میشود
- به کارت شبکه ای که در تجهیزات SAN مورد استفاده قرار میگیرد host bus adapter (HBA) گفته میشود

host bus adapter (HBA) → Fiber Channel Adapter(FCA)

SAN Switch

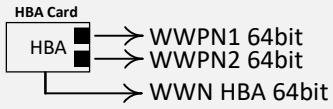
SAN Storage



- بعد از اینکه SAN Storage را فرضا با RAID 5 پیکره بندی کردیم میتوانیم فضای برست آمده را به logical unit number (LUN) های مختلفی تقسیم بندی کنیم
- در DAS به فضایی که برای ذخیره کردن اطلاعات فرمت میشود Volume گفته ودر SAN از آن بعنوان LUN یاد میگردد

(HBA) → (FCA) → World Wide Name (WWN) / World Wide Identifier (WWID)

- WWN یک آدرس ۶۴ بیتی است که متعلق به هر پورت و فود HBA میباشد



68

Bay

I

- از طریق SAN یک LUN را میتوانیم به چندین سیستم اختصاص دهیم
- از طریق SAN ارتباط سیستم ها Block Level خواهد بود

Storage → 1 (DAS) → Block Level Access
Storage → 2 (NAS) → File Level Access (Shared Folder)
Storage → 3 (SAN) → Block Level Access (Shared Storage)

- فرض کنیم ۶ هارد یک ترابایتی را RAID 5 کرده ایم و بدین شکل LUN ساخته ایم

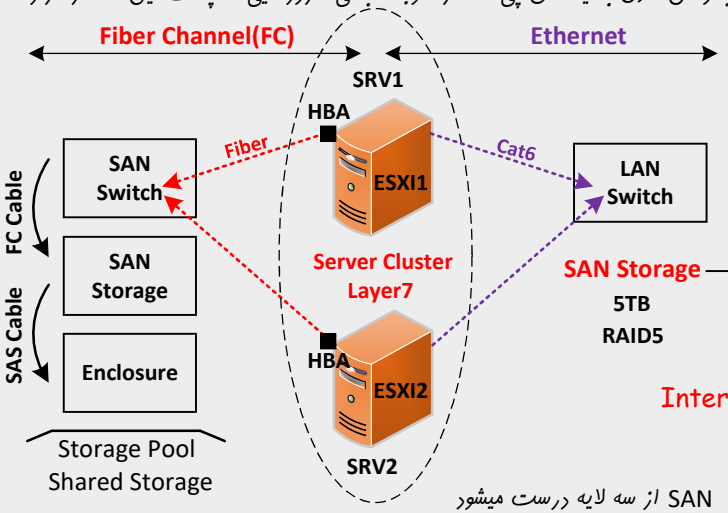
Storage (5TB RAID5)
- LUN1 → 2TB → Present WWPN → SRV1 & SRV2
- LUN2 → 2TB → SRV1 & SRV2
- LUN3 → 1TB → SRV1 & SRV2

II

Server Cluster

RAID → (Disk Groups) Or (Disk Array) + { Rule Or Policy} → Data
Server Cluster → (SRV Groups) Or (SRV Array) + { Rule Or Policy} → Service

- به گروهی از سرورها که مطابق یک قاعده و قانون مشخص جهت ارائه یک سرویس با یکدیگر همکاری دارند سرور کلاستر گویند
- این گروه از سرورها باید رفتارشان در قبال سرویس Config و محتوی سرویس DataBase باید باهم Sync باشند ، این را میدانیم که اگر قرار باشد سرویسی با هم بصورت دستی سینک شود باید سرویس ذاتا Stateless باشد حال اگر سرویس Stateful باشد و ضمنا روش اتوماتیکی برای سینک شدن وجود نداشته باشد و اینکه امکان دستی نیز بعلت Stateful بودن وجود نخواهد داشت لاجرم باید صورت مسئله پاک شود ، اگر کل دیتا بیس و کانفیگ عملا یکجا قرار داشته باشد بصورت اتوماتیک اطلاعات Sync میشود
- اینکه اطلاعات بصورت Shared Folder یا Shared Storage در یکجا قرار بگیرد بستگی به سرویس دارد که با کدام یک از دو روش سازگاری داشته باشد ، بطور مثال IIS حالت Shared Folder را میپذیرد ولی Exchange نیاز به Block Level Access دارد یا بطور مثال ESXI در حالت Member of Cluster نیاز به Shared Storage دارد
- برای استفاده از کلاستر سرور به غیر از مواردی همچون FT,Load balanced,Performance,.... یک دلیل مهم دیگر هم دارد و آن اینست که کلاینت با وصل شدن به یک آی پی کلاستر متوجه الباقی سرورهایی که پشت این کلاستر قرار دارند و با هم همکاری میکنند نمیشود و فقط جهت دریافت سرویس یک سرور را می بیند و دچار تعدد سرور نمیگردد
- وقتی یک سرویس در کلاستر از طریق Server Side ارائه میگردد تمام سرورها از خارج شدن و بازگشت مجدد سرور های همکار مطلع میشوند و کار را در شرایط مختلف بین خود تقسیم مینمایند
- بین سرورهای داخل کلاستر سیگنالی تبادل میشود به نام Heartbeat که بواسطه آن سرورها از وجود یا عدم وجود همدیگر مطلع میشوند



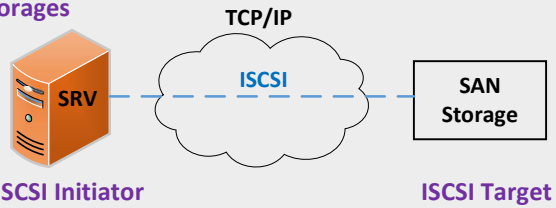
SAN Storage → 5TB RAID5
- LUN1 → 2TB → Present WWPN → SRV1 & SRV2
- LUN2 → 2TB → SRV1 & SRV2
- LUN3 → 1TB → SRV1 & SRV2

SAN Storage ↔ Shared Storage ↔ SRV Cluster (ESXI 1 / ESXI 2)
- DRS → DPM
- HA → FT
- VSAN → SDS

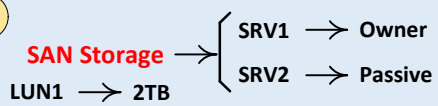
Internet Small Computer Systems Interface (ISCSI)

- در گذشته دیوایس های SCSI از طریق کابل SCSI و با استفاده از پرتکل SCSI و اجرای دستورات مرتبط با این پرتکل با یکدیگر ارتباط برقرار میکردند
- استفاده از پرتکل SCSI مربوط به ارتباطات مرتبط با DAS میباشد
- امکان استفاده از دستورالعمل های SCSI در شبکه TCP/IP از طریق پرتکل ISCSI میسر میشود بدین گونه که دستورالعملهای SCSI درون بسته های Encapsulate,IP میگردد و از طریق شبکه TCP/IP دستورات به دیوایس مورد نظر بصورت لایه ۳ انتقال پیدا میکند
- در حالت FCOE روش کار بدین گونه است که دستورات FC را درون بسته های Encapsulate,Ethernet میکنیم بصورت لایه ۲
- از ویندوز ۲۰۰۸ به بعد ISCSI Initiator بصورت نرم افزاری درون سیستم عامل وجود دارد و از ویندوز ۲۰۱۲ به بعد ISCSI Target نیز Software Define شده است
- SAN از سه لایه درست میشود

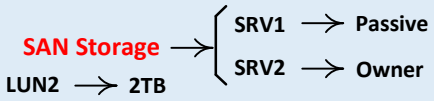
SAN Storage
1. Servers to Storages
2. Storage Networking → FC (Fiber Channel) / ISCSI (Internet Small Computer System Interface) / FCOE (Fiber Channel Over Ethernet)
3. Storages



I

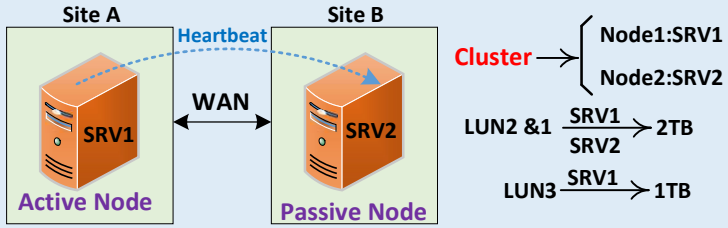


– فرض کنیم که دو سرور را در یک کلاستر به شکل **FailOver** قرار داده ایم و به هر دو یک LUN را نسبت داده ایم
– سرور ۱ اگر برای مدت مشخصی Heartbeat به سرور ۲ نفرستد Failover رخ داده و سرور ۲ بصورت اکتیو در آمده و جایگزین سرور ۱ میگردد



– بعد از راه اندازی هر دو LUN به نوعی ترکیب ۲ سری Active/Passive خواهیم داشت در حقیقت کار به دو Instance تقسیم شده است و در مورد کار شماره ۱ یک سرور اکتیو و دیگری پسیو است و در مورد کار شماره ۲ بالعکس

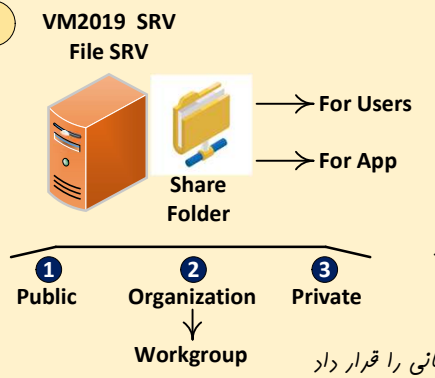
– در طراحی بالا میتوان یک سرور سوم را بصورت Stand by در مدار قرار داد تا درصورت Fail شدن دو سرور دیگر جایگزین آنها گردد و ذکر این نکته مهم است که باید حداکثر بار هر سرور کمتر از ۵۰ درصد باشد تا Failover و جایگزینی میسر گردد



– فرض کنیم سرور ۲ برای مدت مشخصی Heartbeat دریافت نکرده است در اینحالت واقعا مشخص نیست که سرور یک از مدار خارج شده است یا لینک WAN قطع شده است ، یک LUN3 در سایت A درست میشود که به آن Witness نیز میگویند ، یک از وظایف آن ذخیره Cluster Config میباشد
– LUN3 به غیر از نام شاهد Witness به آن هر نصاب quorum نیز میگویند و به این علت درست میشود که در حالت کلاستر Active Node از بین اکثریت یا همان هر نصاب مشخص میشود
– اگر لینک WAN قطع شده باشد و LUN3 در Site A قرارگرفته باشد در آن سایت دو LUN فعال داریم که مجموع Shared Storage و LUN3 میباشد و در سایت دیگر ۱ عدد بنابراین سرور ۱ فعال میماند و سرور ۲ حق اکتیو شدن ندارد
– اگر سرور ۱ Fail شده باشد سرور ۲ و LUN3 با یکدیگر در ارتباطند و هر نصاب ۲ را خواهند داشت و در این شرایط سرور ۲ اکتیو خواهد شد
– بنابراین LUN3 بعنوان **Quorum Cluster** دو وظیفه دارد یکی ذخیره سازی کانفیگ کلاستر و دوم مشخص نمودن اکثریت یا همان هر نصاب معمولا یک LUN با ظرفیت پایین برین منظور به کار گرفته میشود
– ویندوز دو Feature وجود دارد که با آنها میتوان کلاستر ساخت **NLB & Failover Cluster**

Cluster IP Address : VIP
Cluster Computer Account (in The Active Directory) : CAP
NLB (Network Load Balancing) Cluster (L4), Stateless , IIS , Web Server ; Host Support ---> 32 ;No Application Aware;no Share Storage
Failover Cluster (L7), Stateful , Hyper-V Server , File Server , SQL Server , Exchange Server , ... ; Node Support ---> 64; Application Aware ; Shared Storage needed

II



File SRV Implementation

– اصولا در طراحی ، فایل سروری که کاربران از آن استفاده میکنند متفاوت از فایل سروری می باشد که اپلیکیشنها از آن استفاده میکنند

1 – فولدری به نام Public برای همه کاربران با دسترسی R&W یا Modify ساخته میشود که موقع Log On برای کاربران با ایده موقتی بودن Map شده و بصورت دوره ای پاک میشود

2 – فولدری با نام هر واحد سازمانی ساخته شده و در اختیار هر واحد قرار میگیرد ولی مشکل این روش اینست که ممکن است تعداد فولدرهای سازمانی خیلی زیاد شود بنابراین یک فولدر با نام سازمان ساخته شده و الباقی فولدرهای سازمانی داخل آن ساخته میشود و هر کارمند دسترسی به فولدر همان واحد خواهد داشت ، این حالت نیز مطلوب نیست چون باز نیز از نظر بصری فولدر های زیادی توسط کاربران رویت میشود بنابراین با تکنیک Enable access-based enumeration(ABE) و فعال نمودن آن فولدرهایی که کاربران به آنها دسترسی ندارند دیده نمیشود

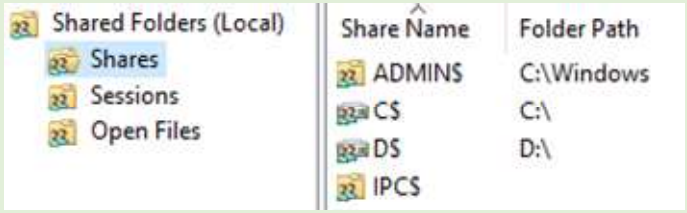
3 – مرحله بعدی ساخت Shared Folder بصورت Private میباشد که قاعدتا Home Folder شامل این موضوع میشود

– برای واحد های سازمانی که کار مشترک دارند میتوان طبق روش مرحله ۲ یک فولدر مربع به نام Workgroup در کنار دیگر فولدرهای سازمانی ایجاد کرد و داخل آن فولدر های مشترک سازمانی را قرار داد
– این سه مرحله میتواند از طریق GPO با فیلترینگ کاربر ادمین به دامین یا OU سازمان لینک داده شود
– مشکلی که در این مقطع وجود دارد اینست که فایل سرور SPOF میباشد به همین دلیل یک فایل سرور دیگر با همان کانفیگ فایل سرور اول ایجاد میکنیم ، حال نیازمند مکانیزمی هستیم که تغییرات را Sync کند این مکانیزم در مایکروسافت با **Distributed File System (DFS) Replication** برقرار میگردد و میتواند بصورت دو طرفه برقرار گردد
– در فایل سرور مکانیزم های دیگری همچون **Dynamic Access Control (DAC)** وجود دارد که در کنار Shared Permision و NTFS Permision بعنوان یک ابزار داینامیکی کنترل سطح دسترسی با استفاده از Rule برقراری میسر میگردد یا **AD RMS (Right Management Services)** که با آن DLP پیاده سازی میگردد ، بطور مثال کاربر بتواند یک فایل را بخواند ولی نتواند پرینت بگیرد یا به فلش درایو انتقال دهد

I

Administrative Share

fsmgmt.msc → Run → Shared Foldaer



net view \\computername /all

Admin$ — Remote admin (this is the %SystemRoot% directory)
IPC$ — Remote IPC (used in named pipes)
C$ — Default Drive Share

- با File level access امکان شیرینگ وجود ندارد و باید حتما از طریق Block level access این مهم انجام پذیرد

Disable/Enable Administrative Share from registry

In order to Disable Windows10 from publishing administrative shares In Win10

reg add HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\
parameters /f /v AutoShareWks /t REG_DWORD /d 0

In order to Enable Windows10 from publishing administrative shares In Win10

reg add HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\
parameters /f /v AutoShareWks /t REG_DWORD /d 1

AutoShareWks (for desktop versions of Windows) or AutoShareServer (for Windows Server)

fter a reboot, administrative shares will not be created. In this case, the tools for remote computer manage, including psexec, will stop working.

Disable/Enable Administrative Share from registry via LocalAccountTokenFilterPolicy

reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v "LocalAccountTokenFilterPolicy" /t REG_DWORD /d 1 /f

Disable/Enable Administrative Share from GPO (drive letter only without Admin$)

Action:Delete

Gpmc.msc → Computer Configuration → Preferences → Network Share → New Network Share
- Delete all regular share
- delete all hidden non-administrative shares
- ✓delete All administrative drive-letter share

II

Sharing Method

- در NTFS Permission مجوزهایی که از بالا دست به ارث رسیده اند امکان حذف شدن ندارند و فقط مجوز هایی که به ACL آن فولدر یا فایل مستقیما اضافه شده اند امکان حذف دارند ، میتوان از طریق گزینه Advanced در NTFS Permission و استفاده از Disable inheritance ارث بری را متوقف کرد ، در اینحالت با دو گزینه تبدیل مجوزهای به ارث برده شده به مستقیم و حذف مجوزهای به ارث برده شده مواجه خواهیم شد در مثال های آتی تبدیل مجوز را مد نظر قرار میدهیم

Public Folder Share for All Users

Disable inheritance ← Public\

Shared permission

- Full Control
- ✓ Change
- ✓ Read

NTFS permission (security tab)

- System
- Local administrator
- ✓ Full Control
- ✓ Modify
- ✓ Read & Execute
- ✓ List Folder contents
- ✓ Read
- ✓ Write
- Special Permissions

→ Security tab/advanced → Add → Select a Principal → Domain Users or users Group

Folder

- Type:Allow
- Applies to :This folder only
- ✓ Read & Execute
- ✓ List Folder contents
- ✓ Read
- ✓ Write

Content of Folder

- Type:Allow
- Applies to :Sub Folder and files only
- ✓ Read & Execute
- ✓ List Folder contents
- ✓ Read
- ✓ Write
- ✓ modify

I

Organization Folder Share for Organization Units

Disable inheritance ← Organization \

Shared permission

- Full Control
- ✓ Change
- ✓ Read

System
Local administrator

- ✓ Full Control
- ✓ Modify
- ✓ Read & Execute
- ✓ List Folder contents
- ✓ Read
- ✓ Write

Special Permissions

→ Security tab/advanced → Add → Select a Principal → Domain Users or users Group

NTFS permission (security tab)

Folder

- Type:Allow
- Applies to :This folder only
- ✓ Read & Execute
- ✓ Read
- ✓ List Folder contents

Disable inheritance ← Organization \IT

Security tab/advanced → Add → Select a Principal → IT Group

Folder

- Type:Allow
- Applies to :This folder only
- ✓ Read & Execute
- ✓ Read
- ✓ List Folder contents
- ✓ Write

Content of Folder

- Type:Allow
- Applies to :Sub Folder and files only
- ✓ Read & Execute
- ✓ Read
- ✓ modify
- ✓ List Folder contents
- ✓ Write

II

Private folder for Users

Disable inheritance ← HomeFolders\

Shared permission

- Full Control
- ✓ Change
- ✓ Read

System
Local administrator

- ✓ Full Control
- ✓ Modify
- ✓ Read & Execute
- ✓ List Folder contents
- ✓ Read
- ✓ Write

Special Permissions

→ Security tab/advanced → Add → Select a Principal → Domain Users or users Group

NTFS permission (security tab)

Folder

- Type:Allow
- Applies to :This folder only
- ✓ Read & Execute
- ✓ Read
- ✓ List Folder contents
- ✓ Write

Content of Folder

- Type:Allow
- Applies to :Sub Folder and files only
- ✓ Read & Execute
- ✓ Read
- ✓ modify
- ✓ List Folder contents
- ✓ Write

Domain Users or users Group → Properties from AD Users & Computers → Profile tab

- ✓ Home folder
- ✓ Connect: H: \\file SRV\Home Folders\%username% → Automatically Create users folder on the HomeFolders

Gpmc.msc → User Configuration → Preferences → Drive Maps

Action:Update or Create

- ✓ Reconnect
- ✓ Location: File SRV\Public
- ✓ Label as: Temperory
- ✓ Use: T

Action:Update or Create

- ✓ Reconnect
- ✓ Location: File SRV\Organization
- ✓ Label as: Organization
- ✓ Use: O

Action:Update or Create

- ✓ Reconnect
- ✓ Location: File SRV\HomeFolders\%username%
- ✓ Label as: Private
- ✓ Use: H

I

Enable ABE

Servermanager → File & Storage services → Shares → (C:\Public / C:\organization / C:\HomeFolders) → Setting → ✓Enable Access-Based Enumeration

Disk Quota

Quota

Server Side OS ← مرتبط با ← Folder Quota — Disk Quota → مرتبط با → NTFS FS

- با برقراری Quota چون سقف استفاده از منبع ذخیره سازی محدود میگردد کاربر عملا مجبور است جهت کسب فضای مناسب فایلهای قدیمی یا کم اهمیت خود را پالایش نماید
- Quotaدر دو حالت قابل استفاده میشود اول حالت **Soft Quota**که برای مانیتورینگ استفاده میشود بدین معنی که موجب عدم محدودیت دسترسی به فضای ذخیره سازی نمیشود و برای تحلیل آماری مورد استفاده قرار میگیرد
- حالت دوم **Hard Quota**نام دارد که به منظور محدودیت در فضای ذخیره سازی مورد استفاده قرار میگیرد
- Quotaبر اساس محاسبه حجم مالک Owner فایل یا فولدر محاسبه خود را انجام میدهد
- با نسبت دادن دو پارامتر سطح اخطار و محدودیت فضای دیسک به Quota میتوان گزارش آماری را مفهومی تر نمود نکته اینکه از بعد از تعیین این دو پارامتر وضعیت جدید شروع میشود و عطف به قبل از آن نمیگردد و برای اینکه این گزارش در مورد فضای مورد استفاده کاربران قبل از ایجاد وضعیت جدید همین شرایط صدق کند باید از مجموعه کاربران در گزارش Properties , Quata Entries گرفته و همین محدودیت جدید را به آنها نیز اعمال نمود
- بعد از اعمال Quota میتوانیم از طریق Quata Entries برای برخی از کاربران استثنا قائل شویم و محدودیت فضای ذخیره سازی آن کاربران را تغییر دهیم و حتی بدون محدودیت بگذاریم و اگر کاربری وجود نداشت میتوانیم آن را اضافه نمائیم

C:\ → Properties → Quota → (✓ Enable quata management → Soft Quota / ✓ Deny disk space to users exceeding quata limit → Hard Quota)

II

File Or Folder Auditing

- برای اینکه مشخص شود بر روی فایل یا فولدر چه عملی توسط چه کاربری انجام شده است بطور مثال پاک شدن یا تصحیح شدن و بتاسطه آن گزارش تهیه نمائیم دو راه کار وجود دارد
- از طریق **Event viewer** و پیمایش Windows log/Security ولی ذکر این نکته مهم است که بصورت پیش فرض ویندوز اینگونه رخداد ها ثبت نمیشود و باید مشخص کنیم که این حساسیت بر روی کدام فولدر یا فایل وجود دارد

1- از طریق GPO میتوانیم مشخص کنیم که دسترسی به فایل ، فولدر یا پرینتر حسابرسی Auditشود

Gpmc.msc → Computer Configuration → Windows Setting → Security Setting → Local Policies → Audit Policies → Audit Object Access → (✓ Success / ✓ Failure)

- برای اینکه بخواهیم مفصل و دقیقتر حسابرسی را فعال کنیم از این پالیسی استفاده میشود ولی در حالت عادی نیازی نیست

Gpmc.msc → Computer Configuration → Windows Setting → Security Setting → Advance Audit Policy Configuration → Object Access

- این تنظیمات پالیسی را بر روی فایل سرورها اعمال میکنیم و بر روی همه سرورها نیازی نیست انجام شود مگر اینکه بحث Hardening مد نظر باشد

2- بعد از تنظیمات GPOبه آن فایل یا فولد خاص مراجعه نموده و از طریق Properties/Security/Advanced/Auditing و Select a Principal آن Permission خاصی که مد نظر است را بطور مثال Delete را تیک میزنیم حال از طریق Event viewer میتوانیم لاگ مرتبط را چستجو کنیم ، در یک رخداد مشخص میگردد به چه فایل یا فولدری چه شخصی مراجعه کرده و در رخداد بعدی عملی که انجام داده مشخص میشود Event 4660-4663

- روش اول که در بالا توضیح داده شد کمتر استفاده میشود و عموما از یک نرم افزار 3rd Party بعنوان مثال Manage Engine File Audit Plus استفاده میشود تا بجای بررسی Event گزارش تولید شود

I

Limit User For Copy Specific File Type

- شاید بخواهیم برای کپی کردن فایل های خاصی در فولدرهای به اشتراک گذاشته شده فایل سرور مثلا ویدئو یا صوتی یا فایل های اجرائی محدودیت قائل شویم بدین معنی که فایل با چه پسوندهایی امکان کپی شدن دارند
- ابتدا رول **File server resource manager** را در سرور مد نظر نصب میکنیم تا بمعنای حقیقی امکانات فایل سرور به سرور مد نظر اضافه شود ، نکته اینکه وقتی اولیت فولدر را به اشتراک میگذاریم رول **File Server** بصورت اتوماتیک نصب خواهد شد بنابراین فقط نیاز هست که ماجول **FSRM** نصب شود

FSRM.msc —Run→ **File server resource manager**

Fsrm.msc — **File Screening Management** →
- **File Group** → انواع پسوندها بصورت پیش فرض مشخص است و میتوان به آن اضافه نمود
- **File Screen Template** → انواع Template بصورت پیش فرض وجود دارد و میتوان به آن اضافه نمود
- **File Screen** → ابتدا فولدر مورد نظر را انتخاب کرده و از Template ها مشخص میکنیم که چه نوع فایل هایی امکان کپی شدن در فولدر به اشتراک گذاشته شده را ندارند

- برای File Screen نیز همانند Quota امکان **Soft Screen** و **Hard Screen** در حالت Custom Properties وجود دارد
- در صورتیکه بخواهیم کاربران بتوانند فایل اجرایی کپی کنند ولی اجازه اجرا کردن فایل را از کاربران بگیریم از پالیسی زیر استفاده میکنیم
- فولدر مورد نظر را انتخاب نموده و

Gpmc.msc — **Computer Configuration** → **Windows Setting** → **Security Setting** → **Software Restriction Policies** → **Additional Rules(Properties)** —**New Path Rule..**→ **Security level=Disallowed**

II

Folder Quota

- فرض کنیم یک فولدر وجود دارد و فارغ از اینکه چه کسی در آن دیتا ذخیره میکند نمیخواهیم حجم آن بیشتر از یک مقدار مشخص شود بطور مثال قبلا از طریق Disk Quota مشخص کرده ایم که هر کسی داخل دیسک D: حداکثر 2GB میتواند اطلاعات ذخیره کند ولی نمیخواهیم داخل Home Folder که داخل دیسک D: قرار دارد ظرفیتش برای هر کاربر بیش از 500MB شود
- برای استفاده از Folder Quota باید روی فایل سرور FSRM نصب باشد

Fsrm.msc — **File Screening Management** → **Quota Management** →
- **Quotas** → **Quota path(Properties)** →
  - **Create Quota on path** → یعنی فولدر اشاره شده بیش از 500MB نشود
  - ✓**Auto apply Template on existing and new subfolders** → یعنی فولدرهایی که در ریشه این فولدر قرار دارند میتوانند هرکدام حداکثر 500MB شوند
- **Quota Management**

- با استفاده از گزینه دوم بعدا نیز برای یک کاربر جدید در Home Folder فولدری با حداکثر 500MB ایجاد خواهد

III

Shadow Copy

- از این قابلیت جهت احیاء نمودن فایلهایی که پاک شده اند استفاده میشود
- بهتر است در ماشین های مجازی یک دیسک به فایل سرور اضافه نمود و Shadow Copies را به آن دیسک انتقال داد

Fsmg.msc — **R-Click Shared Folder** → **All tasks/Configure Shadow Copies** → **Settings** →
- **Volume: C:**
- **Storage Area for this volume: C:**
- **Max Size: X MB**
- **Schedule: everyday 7:00 And 14:00**

Or

C: — **R-Click Shared Folder** → **Shadow Copies**

\\File SRV Folder share —**Properties**→ **Previous Verision\Open**

- جهت احیاء فایل بدین شکل عمل میکنیم
- درصورت داشتن دسترسی خود کاربر نیز میتواند فایل پاک شده را برگرداند

I

Dynamic Access Control(DAC)

- این قابلیت از Win2012 به بعد به ویندوز اضافه گردید در مطالب قبل برای کنترل دسترسی از اشتراک Shared Permission+NTFS Permission استفاده گردید که از آن به نام Effective Permission نیز یاد میشود در اینحالت اصولا Shared Permission را دست بالا مجوزدهی میکنیم و با استفاده از NTFS Permission به کنترل دقیق سطح دسترسی می پردازیم
- ابزار سومی برای کنترل سطح دسترسی DAC نام دارد که با دو روش قبلی ترکیب Merge میشود و براساس یک سری قاعده Rule کار میکند
- وقتی میگوئیم کاربر مالی هست منظور اینست که در اکتیو دایرکتوری Properties\organization\Department مالی تعریف شده است

If user belong to → Mali
If File belong to → Mali
Then → Access is Modify

- بصورت پیش فرض فایل Attribute ندارد ولی میتوانیم برای فایل صفت های مختلفی تعریف نمائیم
- بنابرای DAC بر اساس مقادیرAttribute های User,Computer,File و پیرو شرط های تعریف شده سطح دسترسی تعیین میشود و وقتی مقادیر عوض شود سطح دسترسی بصورت داینامیکی عوض خواهد شد
- از DAC به ندرت استفاده میشود و عمدتا روش کار جهت سطح دسترسی به شکل زیر میباشد

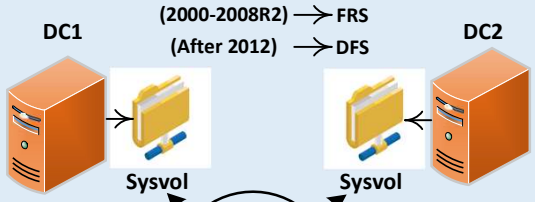
User → (گروه بندی) Group → Ex. Mali
File → (دسته بندی) Folder → Ex. Mali
Then → به گروه مالی نسبت به فولدر مالی سطح دسترسی Shared Permission+NTFS Permission تعریف میشود

- DAC از طریق Dsac (AD Administrative Center) اعمال میگردد
- اگر کاربری به فایلی دسترسی فقط خواندن داشته باشد میتواند آن فایل را پرینت نماید یا داخل فلش مموری کپی کند یا آن را ایمیل نماید به این اتفاق نشت داده Data Leakage میگویند
- Data Leakage از طریق Shared Permission+NTFS Permission+DAC قابل کنترل نیست و نیازمند DLP (Data Leakage Prevention) هستیم
- وقتی DLP بصورت دیجیتالی برقرار میگردد به آن Digital Right Management (DRM) میگویند و روش کار بطور مثال به این شکل است که وقتی کاربری که به محتویات آن دسترسی دارد آن فایل را که انتقال میدهد حال بصورت ایمیل یا کپی در محل دیگر ، امکان دسترسی به آن فایل را از دست میدهد یا اینکه خودش لایسنس استفاده از فایل را به هر طریقی دارد ولی اگر برای شخص دیگری که لایسنس ندارد ارسال نماید امکان دسترسی به محتویات فایل نخواهد بود ضمن اینکه عملکرد آن کاربر نیز مانیتور شده است البته راه کار مکمل Physically Right Management وجود دارد مانند بستن پورت های یو اس بی و غیره
- مایکروسافت راه کاری بدین منظور دارد به نام AD RMS که راه کاری دیجیتالی عدم نشت اطلاعات مایکروسافت میباشد که جزو راه کارهای متوسط در این حوزه میباشد

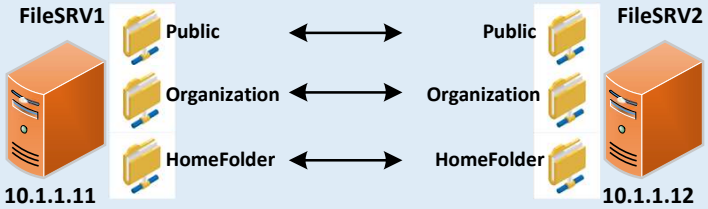
II

Distributed File System (DFS)

- نکته ای که در مورد یک سرویس باید مد نظر داشت اینستکه یک سرویس از دو بخش پیکره بندی Config که حالت Stateless و بخش دیتا بیس Database که حالت Stateful دارد تشکیل میشود
- مهم ترین وظیفه DFS اینست که محتویات دو یا چند فولدر به اشتراک گذاشته مختلف هم نام یا غیر همنام را در سیستمهای متفاوت با هم Syncنماید این موضوع شامل ...,NTFS Permission,Attribute نیز میشود
- در ویندوز(2000-2008R2) بصورت پیش فرض از FRS استفاده میشود ولی این امکان وجود دارد که آن را به DFS تبدیل کنیم
- در ویندوزهای بالاتر از 2012 سرویس File Replication وجود دارد ولی Disable است و بجای آن از دو سرویس 1-DFS Namespaces 2-DFS Replication استفاده میشود
- ساده ترین کاری که DFS میتواند انجام دهد اینست که بر روی یک فولدر به اشتراک گذاشته شده در یک فایل سرور لینک ایجاد کند به فولدرهای به اشتراک گذاشته شده فایل سرورهای دیگر اینکار باعث میشود که تعداد Network Drive هایی که برای یک کاربر ساخته میشود کاهش پیدا کند
- جهت برقراری HA در فایل سرور از DFS استفاده میشود ،



Dfsmgmt.msc → Run → Distributed File System



- در ابتدا فایل سرور دوم را براساس همان تنظیماتی که در فایل سرور اول انجام داده بودیم برقرار می نمائیم بطوریکه شرایط کاملا یکسانی داشته باشد...Quota,Shares,

I

- هدف ما از برقراری DFS بین دو فایل سرور اینست که تغییراتی که در فولدرهای یک فایل سرور ایجاد میشود به دیگر فایل سرور منتقل شود و بالعکس

- حال فرض کنیم در فایل سرور اول پوشه ای به نام Public داریم که کاربران فایلهای خود را در آن کپی کرده اند و در فایل سرور دوم نیز همان فولدر را ایجاد کرده ایم و میخواهیم که محتویات این فولدر نیز با فولدر متناظر خود در فایل سرور اول همواره Sync باشد ذکر این نکته مهم است که لزومی ندارد اسامی فولدر ها یکسان باشند ، هرچند جهت نظم بیشتر ما یکسان در نظر میگیریم در واقع DFS صرفا مجموع فولدرهای داده شده را Sync میکند

- ابتدا یک فایل سرور ایجاد میکنیم به نام Namespace SRV و بر روی آن ماجول های 2-DFS Replication 1-DFS Namespaces را نصب میکنیم

NS-SRV

Dfsmgmt.msc → R-Click Namespace → Namespace srv: NS-SRV, Namespace : NS-Public → \\NS-SRV\NS-Public → C:\DFSRoots\NS-Public
Link → Name:public, Folder target 1: \\srv1\public & Folder target 2: \\srv2\public

تارگت ها را داخل یک Replication Group میگذاریم

- میتوان یک Namespace برای سینک کردن همه فولدر ها استفاده نمود یا به ازای هر کدام جداگانه تعریف کرد

Dfsmgmt.msc → R-Click Namespace → Namespace srv: NS-SRV, Namespace : NS-Organization → \\NS-SRV\NS-Organization → C:\DFSRoots\NS-Organization
Link → Name:Organization, Folder target 1: \\srv1\Organization & Folder target 2: \\srv2\Organization

تارگت ها را داخل یک Replication Group میگذاریم

Dfsmgmt.msc → R-Click Namespace → Namespace srv: NS-SRV, Namespace : NS-HomeFlders → \\NS-SRV\NS-HomeFolders → C:\DFSRoots\NS-HomeFolders
Link → Name:HomeFolders, Folder target 1: \\srv1\HomeFolders & Folder target 2: \\srv2\HomeFolders

تارگت ها را داخل یک Replication Group میگذاریم

- حال برای کلاینتها Network Drive ایجاد میکنیم

T:\\Domain Name\NS-Public\Public
Active 1: \\srv1\Public
Stand by 2: \\srv2\Public

O:\\Domain Name\NS-Organization\Organization
Active 1: \\srv1\Organization
Stand by 2: \\srv2\Organization

H\\:Domain Name\NS-HomeFolders\HomeFolders
Active 1: \\srv1\HomeFolders
Stand by 2: \\srv2\HomeFolders

- اگر UNC Path اول طی یک بازه زمانی جواب ندهد دومی جایگزین میشود

- پالیسی های Network Drive که در فایل سرور اول تعریف شده بود باید جداگانه تصحیح گردد

Gpmc.msc → User Configuration → Preferences → Drive Maps → Action:Update or Create
✓ Reconnect
✓ Location: Domain name\NS-Public\Public ← بر اساس Namespace
✓ Label as: Temperory
✓ Use: T

- تعریف DFS میتواند از یک سمت که سرور اصلی حاوی فایل میباشد انجام میشود و بعد از برقراری آن هر اتفاقی که داخل فولدر ها بیافتد با هم سینک میشوند حتی اعطای مجوز و غیره

- در حال حاضر Namespace SRV حالت SPOF دارد که میتوان Namespace SRV2 را به آن اضافه نمود بدین صورت دو رپلیکیشن یکی بین فولدرها و دیگری بین Namespace ها خواهیم داشت

- برای اینکه بین Namespace ها رپلیکیشن برقرار باشد باید Domain Namespace داشته باشیم و در حالت Standalone Namespace این رپلیکیشن برقرار نمیباشد

- طی سناریو بالا برای راه اندازی کامل DFS به چهار سرور نیازمندیم که به وضوح اشتباه است و میتوان DFS را بین همان دو فایل سرور همراه با Namespace برقرار نمود بدین معنی که فایل سرور یک میتواند Namespace اول و فایل سرور دوم Namespace دوم باشد

I — ایرادات(DFS)

- جهت ریپلیکیشن بین Sysvol در DC ها از DFS استفاده میشود که انتقال دیتا در هر چند مگابایت میباشد ولی این عدد در بین فایل سرورها اصولا بالاست که اگر چند فایل سرور بصورت همزمان بخواهند وجود داشته باشند به ضریبی از این عدد بزرگ فضای ذخیره سازی نیازمندیم که عامل مهمی میباشد نکته دوم اینکه برای ایجاد تغییرات پیکره بندی اعم از ایجاد فولدر اشتراکی جدید یا Quata,File Screen,... باید بصورت یکسان بر روی همه سرورها انجام شود نکته سوم اینکه ممکن است فاصله زمانی انتقال از تارگت اول به دوم در سازمان به چشم بیاید و نکته آخر اینکه در شرایطی فایل های باز در یک فایل سرور ممکن است یا اصلا Sync نشود و یا به زمان خیلی زیادی نیاز پیدا کند این موضوع در سازمانهای بزرگ منجر به مشکل جدی میشود
- میتوان به جای DFS از FailOver Cluster استفاده نمود یا اینکه فایل سروری که ماشین مجازی است با استفاده از نرم افزار Veeam Backup & Replication به محل دیگری نیز Replicate کنیم تا در صورت خرابی فایل سرور اول فایل سرور Replicate شده را بالا بیاوریم یا از FT در Vsphere Vcenter استفاده میکنیم

II — Internet Information Services (IIS)

- از IIS برای راه اندازی **Web SRV** و **FTP SRV** به شکل معمولی یا **Secure** استفاده میگردد HTTP,HTTPS & FTP,FTPS
- FTPS نباید با SFTP=SSH Port 22 اشتباه شود و از طریق IIS نمیتوان SFTP راه اندازی نمود و جهت راه اندازی SFTP باید از 3rd party مانند Serv-U استفاده نمود البته از ویندوز ۲۰۱۹ به بعد SFTP,SSH جایگزین Telnet SRV شده است
- SMTP SRV از ویندوز 2008 به بعد مستقل از سرویس IIS شده است ولی همچنان برای مدیریت **SMTP** از IIS 6.0 استفاده میشود که در مجموعه IIS با هر نسخه ای که در حال حاضر وجود دارد قرار دارد
- SMTP بعنوان سکوی ارسال گروهی ایمیل استفاده میشود بدین معنی که مجموعه ایمیل ها به آن فرستاده شده و برای مقصد ارسال میگردد
- جهت دسترسی کاربران به فایل از دوسرویس فایل سرور و FTP SRV استفاده میشود FTP SRV ⟶ FTP Site File SRV ⟶ Shared Folder
- تقریبا درصد کمی برای راه اندازی وب سایت یک شرکت از طریق وب سرور بعنوان میزبان استفاده میشود و در بیشتر مواقع برای راه اندازی سرویس وب بیس به کلاینتها یا مدیریت سرویس یا هر دو برای یک اپلیکیشن استفاده میشود
- اینکه IIS در موقع نصب به چه ماجولهایی نیاز دارد بستگی به اپلیکیشنی دارد که میخواهد از آن استفاده کند و عموما هنگام نصب اپلیکیشن بصورت اتوماتیک IIS و ماجولهای مرتبط نصب میگردند

III — Common Features

- دو موضوع باید برای IIS مشخص باشد ۱- Physical Path سایت کجا قرار دارد ۲- Default Page یا همان Default Document کدام فایل HTML میباشد اگر موقع نصب IIS ماجول **Default Document** نصب نشده باشد اصطلاحا وارد مد **Directory Browsing** میشود بدین شکل که به کاربر صفحه پیش فرض نشان داده نمیشود بلکه لیست کل فایلها نمایش داده میشود البته در صورت فعال بودن ماجول Directory Browsing
- اگر هر دو ماجول **Directory Browsing,Default Document** غیر فعال باشد IIS از طریق ماجول **HTTP Errors** به کاربر Error برمیگرداند
- از ماجول **Static Content** برای نشان دادن محتویات استاتیک و از ماجول **Http Redirection** برای Redirect کردن به یک یک صفحه یا سایت دیگر استفاده میشود
- از ماجول **WebDAV Publishing(Web Distributed Authoring and Versioning)** جهت اینترنت شیرینگ یا همان وب شیرینگ استفاده میشود بدین معنی که فولدر به اشتراک گذاشته شود و دسترسی به آن از طریق HTTP یا HTTPS انجام شود چیزی شبیه FTP بدون محدودیت های آن
  از این پرتکل جهت تصحیح یک وب سایت از طریق HTTP,HTTPS نیز استفاده میشود
  Network Drive X: **Double Click** ⟶ SMB ⟶ \\ **UNC** ..... Network Drive X: **Double Click** ⟶ HTTP / HTTPS ⟶ \\ **URL** .....
- تیک خوردن ماجولها به معنی مهیا شدن امکان استفاده از آن ماجول در صوت نیاز میباشد

IV — Security Features

- اگر بخواهیم برای بازدید یک سایت یا بخش هایی از آن **Authenticate** انجام شود باید متد آن مشخص شود که شامل ماجول های **Basic Authentication** که شامل همه پلتفرم ها میگردد ولی رمز Clear تبادل میشود و همراه با HTTPS استفاده میشود یا **Digest Authentication** که بصورت امن کار میکند ولی نیاز به دامین کنترلر جهت Authenticate دارد ولی اگر بخواهیم Authenticate,Locally کنیم از ماجول **Windows Authentication** استفاده میکنیم یا ماجول **IP and Domain Restriction** که برای فیلتر کردن بر اساس نام یا آی پی انجام میگردد
- در شرایط واقعی عموما از **FormBase Authentication** استفاده میشود که باید طراحی گردد مانند نرم افزار اتوماسیون از طریق وب البته این نوع Authenticate نیز Secure نیست و امنیت آن از طریق HTTPS فراهم میشود
- بعد از نصب IIS دو فولدر ایجاد میگردد
  C:**inetpub**
  C:\windows\system32**inetsrv**
  - **Config Folder** ⟶ **Config File**
  - **Inetmgr.exe**
  - **iis.msc**
  - **Appcmd.exe**

  Inetmgr **Run** ⟶ **IIS Console**
- برای ریست کردن سرویس وب بهتر از دستور **iisreset** از طریق کامند استفاده گردد و اگر در محیط عملیاتی باشد از سوئیچ **/noforce** استفاده میشود تا سر فرصت ریستارت شود

I

- کانفیگ IIS از نسخه ۷ به بعد داخل یک فایل txt ذخیره میشود درصورتیکه در نسخه های قبل تر در رجیستری ویندوز ذخیره میشد ، بنابراین اگر بخواهیم IIS را مجدد بصورت پیش فرض راه بیندازیم بعد از حذف IIS باید فولدرهای مورد اشاره را نیز حذف نمود و مجددا IIS را راه اندازی کرد
- پس از نصب IIS فایلهای کانفیگ داخل فولدر inetsrv قرار میگیرد و و فایلهای وب سایت پیش فرض در فولدر **Inetpub\wwwroot** قرار میگیرد
- پس از برخی تغییرات در داخل فولدر Inetpub\wwwroot یک فایلی با نام **Web.config** ایجاد میشود که در صورت نیاز کانفیگ اختصاصی و انحصاری وب سایت در آن ذخیره میشود ، ممکن است در حالت معمول وجود نداشته باشد
- نکته مهم اینکه اگر همه شرایط IIS و نحوه Authentication نیز اگر درست باشد ولی NTFS Permission از Inetpub\wwwroot گرفته شود دسترسی به IIS کار نخواهد کرد این را میدانیم که برای دسترسی به فایل یا فولدر باید یا NTFS Permission داشته باشیم یا مالک Owner آن باشیم ، در تنظیمات پالیسی مشخص میگردد که چه کسانی میتوانند خود را مالک فایلها یا فولدر ها نمایند پس نهایتا ابتدا مالک فایل های داخل فولدر Inetpub\wwwroot را عوض میکنیم و سپس دسترسی به کاربران دلخواه را برای رویت سایت میدهیم

IUSR → Buit-in System for IIS

Gpmc.msc → Computer Configuration → Windows Setting → Security Setting → User Right Assignment → **Take ownership of files or other objects**

- برای اینکه وب سایت بصورت Anonymous ویزیت شود باید به اکانتی که نماینده گروه بازدید کنندگان بصورت Anonymous در داخل وب سرور میباشد **IUSR** دسترسی Read را بدهیم
- مجموعه ای از ماجولها در کنار هم باعث عملکرد IIS میشود که از طریق کنسول IIS و Feature ماجول در دسترس هستند ولی نکته مهمی که باید حتما مدنظر قرار بگیرد اینست که مجموعه ای از چند ماجول در کنار هم باعث ایجاد یک **Handler Mapping** میشود که آن نیز از طریق کنسول در دسترس است و باعث میشود درخواست هایی که به سمت IIS می آید به دست آن برسد و درصورت پاک شدن عملکرد IIS مفروش میگردد یعنی اگر **Handler** نباشد درخواست ها به سرانجامی نمیرسند
- اگر بخواهیم بخش هایی از محتوای سایت متمایز از دیگر بخش ها گردد چه از لحاظ دسترسی یا استفاده از HTTPS استفاده شود بهترین راه حل کدنویسی میباشد ولی بصورت موقت امکان استفاده از امکانات IIS نیز میسر است که باعث میشود محتوای وب براساس یک وب سایت و تعدادی **Virtual Directory** که کانفیگ آنها به مقدار زیادی متفاوت از وب سایت باشد عرضه شود

بطور مثال

Inetpub\wwwroot → (Copy) → Inetpub\OWA

Inetpub\wwwroot → (R-Click) → Add Virtual Directory

Path=
Alias=owa → **...../owa**
Physical path: c:\inetpub\owa

- با **HTTP Redirect** میتوان یک سایت را به سایتهای دیگر **Redirect** نمود

Inetpub\wwwroot → Http Redirect

http://127.0.0.1/owa
✓ **Only redirect to content in this directory**

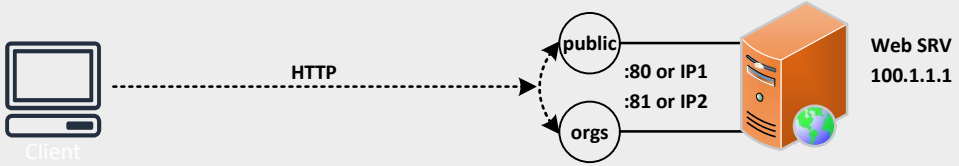
IP address and Domain Restrictions

- میتوان برای محدود شدن محتویات یک وب سایت بر اساس آی پی و نام دامنه محدودیت اعمال نمود بطور مثال آی پی خاصی یا نام دامنه خاصی اجازه رویت یا عدم رویت یک سایت را داشته باشد
- اگر بخواهیم بر اساس اسم و نام دامین محدودیت ایجاد کنیم ابتدا باید در از قسمت Edit features Setting مورد Enable Domain Restriction را فعال نمائیم و لازم بذکر است که این نوع محدودیت بعلت استفاده از DNS PTR بار زیادی روی IIS میگذارد و باید از قبل در شبکه فعال باشد

II

روش ایجاد تمایز بین وب سایتهای یک وب سرور

- فرض کنیم بر روی یک سرور دو سرویس HTTP,FTP فعال میباشد و سرور بر اساس شماره پورتی که ویزیت کننده در خواست میکند متوجه خواهد شد که کدام سرویس را باید ارائه دهد حال اگر سرور میزبان بیش از یک وب سایت باشد به روش های زیر تمایز ایجاد خواهد شد



1. - تخصیص دادن آی پی آدرس های متفاوت به وب سایتهای مختلف از طریق وب سرور ، اگر تعداد وب سایتها زیاد باشد و مجبور به تخصیص آی پی Public باشیم این روش منطقی به نظر نمی آید
2. - تخصیص دادن شماره پورت های متفاوت به وب سایتهای مختلف از طریق وب سرور ، این روش به شرطی که بتوان کاربر را از تغییر پورت مطلع نمود جواب خواهد داد ولی در مورد بازدید عموم از وب سایت جواب نخواهد داد
- دو روش ذکر شده بالا از طریق انتخاب سایت و سپس انتخاب **Binding** از پنل مرتبط با سایت امکان پذیر است

I

3 – میتوان از یک آدرس لایه اپلیکیشنی برای تمایز استفاده نمود که به آن اصطلاحا **Hostname** گفته میشود که برای وب سایت اختیاری میباشد

– نام هاست در فیلد Host Header پرتکل HTTP بصورت یک مقدار ثبت میگردد و وب سرور از طریق این فیلد متوجه میشود که دیتا را به سمت کدام سایت هدایت کند

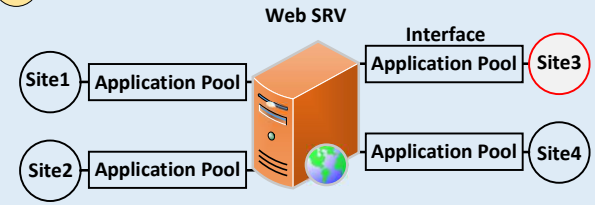
– اگر برای سایتی Hostname تعریف شود دیگر بر اساس IP کار نخواهد کرد

1 – اگر سایتی با IP ویزیت شود ولی با Hostname نشود بیشترین احتمال عدم Name Resolution میباشد

2 – اگر سایتی با IP ویزیت نشود ولی با Hostname شود بیشترین احتمال تعریف Hostname برای سایت میباشد

II

Application Pool



– فرض میکنیم چهار سایت بر روی وب سرور قرار داده شده است و Site3 از استانداردهای طراحی وب سایت برخوردار نیست بطور مثال از وب سرور منابع میگیرد ولی بعد از انجام کار آن منابع را آزاد نمیکند و برای آزاد سازی منابع مجبوریم وب سرور را ریستارت کنیم

– میتوانیم برای استفاده از منابع وب سرور برای هر سایت یک چارچوب مشخصی تعیین کنیم که به آن **Application Pool** گفته میشود و برای برطرف کردن مشکل منابع بجای ریستارت کردن کل سرور صرفا Application Pool آن سایت مورد نظر را ریستارت میکنیم که لفظ درست آن به جای ریستارت **Recycle** نامیده میشود

– این امکان وجود دارد که از طریق ...Recycling ریستارت شدن منابع را بصورت سفارشی اتوماتیک نمود

– بین وب سایت یا وب اپلیکیشن و IIS رابطی وجود دارد به نام Application Pool که درخواست منابع برای یک وب سایت از طریق آن به IIS داده میشود و بعد منابع در اختیار وب سایت قرار میگیرد

– هنگام Recycle کردن اغلالی در سرویس آن وب سایت بوجود نمی آید چون از یک Application Pool واسط جهت اینکار استفاده میشود و پردازش های جدید به آن انتقال می یابد و بعد از اتمام پردازش ها Application Pool قدیمی بسته میشود

– میشود به یک وب سایت یک Application Pool جدید نسبت نداد و آن را به یکی از Application Pool موجود لینک نمود و هرچند وب سایت را دسته بندی نمود که البته ایده آل نیست و وقتی منابع محدودی وب سرور دارد از این روش استفاده میشود

– یک وب سایت با همه Virtual Directory های آن داخل Application Pool آن سایت قرار میگیرند هرچند از میتوان از این روند پیروی ننمود و به Application Pool دلخواه نسبت داد

III

IIS Backup

– در محیط گرافیکی در حالت معمول آیتمی برای بکاپ وجود ندارد و برای اینکار باید از کامند **appcmd** استفاده کنیم که فقط کانفیگ وب سرور بکاپ گرفته میشود و نه محتوای سایت

```
C:\Windows\System32\inetsrv>appcmd list backup
BACKUP "CFGHISTORY_0000000031"
BACKUP "CFGHISTORY_0000000032"
BACKUP "CFGHISTORY_0000000033"
BACKUP "CFGHISTORY_0000000034"
BACKUP "CFGHISTORY_0000000035"
BACKUP "CFGHISTORY_0000000036"
BACKUP "CFGHISTORY_0000000037"
BACKUP "CFGHISTORY_0000000038"
BACKUP "CFGHISTORY_0000000039"
BACKUP "CFGHISTORY_0000000040"
```

→ Automatic backup list Per Changes

C:\inetpub\history

```
C:\Windows\System32\inetsrv>appcmd add backup
BACKUP object "20220306T101727" added
```

```
C:\Windows\System32\inetsrv>appcmd restore backup "20220306T101727"
BACKUP object "20220306T101727" restored
```

Remote Management IIS

– میتوان فقط کنسول مدیریتی IIS را بر روی یک ماشین دیگر نصب نمود و از طریق inetmgr به IIS دلخواه وصل شد ولی قبل از اینکار باید بر روی سرور IIS تنظیمات مرتبط انجام شود

Servermanager → **Add roles and features** → **Management Tools** → **Management Service**

– سپس در قسمت Management Service وب سرور آن را Enable میتمائیم و در صورت نیاز تنظیمات بیشتر را برای اجازه ریموت انجام میدهیم

I

FTP Service

- برای راه اندازی این سرویس به غیر از نرم افزار Serv-U که قابلیتهای کاملتری را ارائه میکند میتوان از طریق ویندوز ماجول آن را نصب مینمائیم و وارد کنسول مدیریتی IIS میشویم (inetmgr)
- بصورت پیش فرض در مسیر C:\inetpub\ftproot فایلهای FTP ذخیره میشوند ولی میتوان بعلت نظم بیشتر هر فولدری در مسیر C:\inetpub ایجاد نمود
- از طریق Browser,file explorer,Command میتوان به FTP Server وصل شد Ftp:\\ftpservername or ip
- از طریق FTP Isolation میتوان بر اساس نام کاربران در زیر شاخه Localuser برای غیر دامین و زیر شاخه با نام دامین برای کاربران دامینی محیط ایزوله ایجاد کرد چیزی شبیه ABE در فایل سرور

II

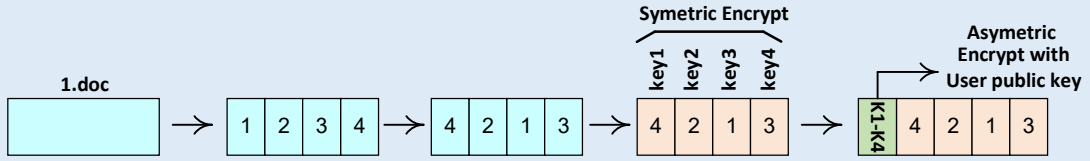
Encrypted File System (EFS)

EFS is the ability of the New Technology File System (NTFS) file system to encrypt files on disk in a manner that is transparent to the user.

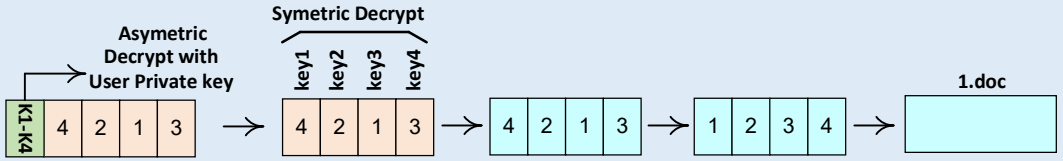
- EFS جزو ویژه گیهای فایل سیستم NTFS میباشد که بصورت Transparent اینکار را انجام میدهد یعنی برای رمز کننده بصورت رمز برداری شده نشان داده میشود

File or Folder → R-Click → Advanced → Encrypt Content to secure data

- ترکیب EFS+Compress بر روی فایل یا فولدر بصورت همزمان امکان پذیر نیست
- ایده استفاده از رمزگذاری عدم دسترسی به فایلهای محرمانه در صورت سرقت فیزیکی ذخیره داده میباشد و رمز نگاری فولدر شامل فایلهای داخل آن فولدر و فایلهایی که بعدا اضافه خواهد شد میشود
- در حالت معمول صرفا کسی که رمزگذاری نموده است امکان رمزبرداری دارد ، رمزگذاری نیاز به NTFS Permission نوشتن Write دارد تا بتواند Attribute یک فایل یا فولدر را تغییر دهد
- روش کار EFS بدین شکل است که بطور مثال وقتی بر روی یک فایل اعمال میشود ابتدا آن را به قطعات کوچک تقسیم میکند و سپس ترتیب قرار گیری آن را تغییر میدهد وبعد هر کدام از قطعات کوچک شده را با استفاده از الگوریتم AES و عموما با کلید 256bit بصورت Symetric و به شکل مجزا رمز میکند ، سپس مجموعه کلیدهای استفاده شده را بصورت یک فیلد به اول فایل اضافه میکند و بعد این فیلد را با Public Key کاربری که اقدام به رمز کردن نموده است بصورت Asymetric رمز مینماید



Data → Symetric Encrypt
Key → Asymetric Encrypt



Key → Asymetric Decrypt
Data → Symetric Decrypt

- Public & Private Key داخل Certificate قرار دارند که بصورت Self Sign مختص EFS تولید میشود
- بعد از اولین رمز گذاری یک Certificate به سیستم با نام کاربری که رمزگذاری نموده است ایجاد میشود که از طریق Certmgr.msc\personal\certificates قابل رویت است
- اگر رمز عبور کاربری که رمز گذاری کرده ریست شود و نه Change در آن صورت دسترسی به فایلهای رمز شده میسر نخواهد بود مگر اینکه به مجردا به همان رمزی که موقع رمزگذاری کاربر داشته ریست شود
- برای غیر فعال کردن EFS بر روی یک سیستم از این پالیسی استفاده میشود

Gpmc.msc → Windows Setting → Security Setting → Public key Policies → Encrypting file system → R-Click\General → File encrypting using EFS(Don't Allow)

- با داشتن Certificate طبق هر شرایطی میتوان به فایلهای رمز گذاری دسترسی پیدا کرد

Certmgr.msc\personal\certificates\EFS certificate → All task → Export → Export with private key → PFX file

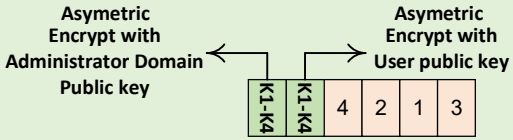
- از طریق Control panel\user account\manage your file encryption account میتوان مجموعه گواهینامه های مرتبط با EFS را مدیریت نمود ، اگر بیش از یک گواهینامه بدین منظور به سیستم اضافه کنیم جهت مشخص نمودن اینکه از چه گواهینامه ای برای EFS استفاده خواهد شد در قسمت مدیریت گواهینامه ها از Select Certificate استفاده میکنیم که باعث میشود گواهینامه مورد نظر برای EFS در وضعیت Binding قرار گیرد

I

Recovery Agent

– همانند یک پست سازمانی یا یک جایگاه در سیستم میباشدکه ممکن یک یا چندین نفر این جایگاه را داشته باشند که فایلهای رمز شده دیگران را رمز برداری کند درLSDهیچ کاربری بصورت پیش فرض چنین جایگاهی ندارد اما در اکتیو دایرکتوری Administratorدامین این جایگاه را دارد و بعلت جایگاهش یک گواهینامه برای اینکار دارد که روی اولین دامین کنترلر قرار میگیرد

Certmgr.msc\personal\certificates**Administrator** **(With File recovery intnded purposes)**



– Recovery Agent همانند این است که برای ادمین یک درب دوم برای دسترسی به فایلهای رمز شده کاربران در شبکه دامین مدل تعبیه نمائیم و نه کلید دوم چون صدور گواهینامه بصورت اختصاصی برای هر کاربر میباشد بدین صورت که یک فیلد کلیدها که قبلا گفته شد نیز بصورت مجزا برای ادمین دامین به هر فایل یا فولدری اضافه خواهد شد

– برای ساختن یک Recovery Agent در صورت عدم وجود بدین شکل عمل میکنیم

1 – ورود با ادمین دامین به دامین کنترلر و سپس مراجعه به کامند از طریق CMD

2 – ساخت یک فولدر مثلا C:\filerecovery و تایپ دستور روبرو

```
C:\Windows\system32>cipher /r:c:\filerecovery\filerecovery
Please type in the password to protect your .PFX file:
Please retype the password to confirm:
Your .CER file was created successfully.
Your .PFX file was created successfully.
```

C:\filerecovery → filerecovery.CER → **Public Key**
filerecovery.PFX → **Public+Private Key**

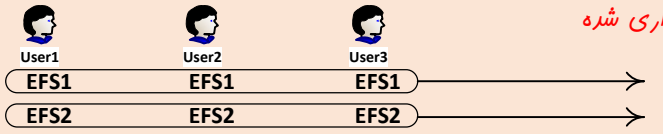
3 – باز کردن درب دوم برای و اضافه شدن فیلد کلید عمومی ادمین دامین در کنار فیلد کلید عمومی کاربران در هنگام رمزگذاری از لحظه به بعد

Gpedit.msc in workgroups ← Gpmc.msc → **Windows Setting** → **Security Setting** → **Public key Policies** → **Encrypting file system** → **R-Click\General** → **Add Data Recovery agent** → **Add filerecovery.cer**

II

4 – نصب **filerecovery.pfx** بر روی دامین کنترلر

استفاده همزمان چند نفر از فایل های رمزگذاری شده



– جهت رمز گذاری فایلهای مشترک بین سه نفر این گواهینامه ها برای هر کاربر Export شده و در اختیار ۲ کاربر دیگر قرار میگیرد

– جهت رمز گذاری فایلهای غیر مشترک که هر کاربر که گواهینامه فقط توسط همان کاربر استفاده میشود و در اختیار دیگر اعضاء قرار نمیگیرد

– نکته مهم اینکه کاربر وقتی میخواهد یک فایل مشترک را رمزگذاری کند باید از طریق کنترل پنل و انتخاب گواهینامه مرتبط با رمزگذاری مشترک فایلهای مورد نظر را رمزگذاری نماید

– یک را بسیار ساده تر بدین شکل است که وقتی میخواهیم باکس رمز گذاری را تیک کنیم دکمه Detail را میزنیم که از طریق آن میتوانیم گواهینامه عمومی کاربرانی که میخواهند به آن فایل دسترسی داشته باشند را مشخص نمائیم پر واضح است که برای کاربرانی که اضافه میشوند درب هایی بصورت فیلد به فایل های رمزگذاری شده اضافه میگردد

III

Network Load Balancing (NLB) implementation

RAID → **(Disk Groups) Or (Disk Array) + { Rule Or Policy}** → Data

Server Cluster → **(SRV Groups) Or (SRV Array) + { Rule Or Policy}** → Service

(HA+LB+Quick Access)

– به گروهی از سرورها که مطابق یک قاعده و قانون مشخص جهت ارائه یک سرویس با یکدیگر همکاری دارند سرور کلاستر گویند

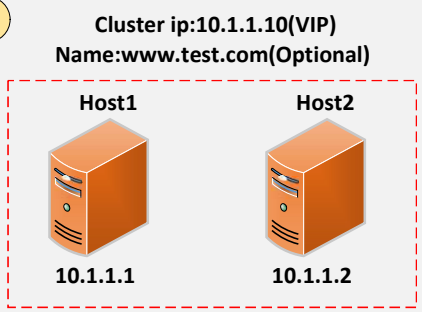
– مجموعه **(HA+LB+QA)** از طریق **DNS** نیز قابل پیاده سازی است همانند اکتیو دایرکتوری ولی ارزش افزوده سرور کلاستر بدین صورت است که مجموعه ای از سرورها با یک آی پی و نام سرور در معرض دید کاربران قرار میگیرد و کاربر درگیر تعدد سرور نمیشود

– ویندوز دو Feature وجود دارد که با آنها میتوان کلاستر ساخت **NLB & Failover Cluster**

Cluster IP Address : VIP
Cluster Computer Account (in The Active Directory) : CAP

NLB (Network Load Balancing) Cluster (L4), Stateless , IIS , Web Server ; Host Support ---> 32 ;No Application Aware;no Share Storage
Failover Cluster (L7), Stateful , Hyper-V Server , File Server , SQL Server , Exchange Server , ... ; Node Support ---> 64; Application Aware ; Shared Storage needed

I



- میخواهیم یک NLB Cluster با دو سرور Host راه اندازی کنیم
- ابتدا باید NLB Feature بر روی همه سرورهای موجود در کلاستر نصب شود ، پس از نصب در قسمت شبکه سرورها آیتم NLB اضافه خواهد شد
- از طریق **Nlbmgr** در Run ابزار گرافیکی ساخت و مدیریت NLB در اختیارمان قرار میگیرد البته ابزارهای کامندی **Nlb,Wlbs** نیز وجود دارند
- ابزار مدیریتی Nlbmgr بصورت پیش فرض در ویندوز وجود دارد و نیازی نیست از پای سرور از آن استفاده نمود و میتوان از پای کلاینت هاست ها را اضافه و مدیریت نمود
- در موقع راه اندازی از طریق ابزار مدیریتی وقتی یک هاست را اضافه میکنیم اگر بیش از یک کانکشن وجود داشته باشد باید مشخص کنیم کدام کانکشن شبکه در NLB شرکت دارد
- وقتی هاست اضافه میشود به آن به ترتیب از ۱ تا ۳۲ **Priority(unique host identifier)** تخصیص داده میشود که کاربرد دوگانه دارد یکی بحث **Priority** و دیگری شماره ای که به هاست نسبت داده شده است
- سپس به هاست اضافه شده به کلاستر آی پی یا آی پی های کلاستر را نسبت میدهیم که باید حتما استاتیک باشد

MAC Cluster: VIP+Mode → **1-Mode is unicast then mac start with 02:bf..... 1-Mode is multicast then mac start with 03:bf.....1-Mode is IGMP multicast then mac start with 01.....**

- ادامه مک آدرس بدین صورت است که آی پی کلاستر هگزادسیمال شده و به انتهای مک آدرس اضافه میشود

Cluster ip:10.1.1.10(VIP) —Multicast→ **03:bf:0a:01:01:0a**

- مک آدرس میتواند توسط کارخانه سازنده تولید شود Burn In Address:BIA که در اینصورت بیت هفتم از ۴۸ بیت صفر خواهد بود یا اینکه بصورت مجازی در سطح سیستم عامل تغییر داده شده یا تولید شود که در اینحالت بیت هفتم یک خواهد بود حال اگر بیت هشتم صفر باشد یعنی Unicast address و اگر یک باشد No Unicast address
- مک آدرس کلاستر جایگزین مک آدرسهای سرورهای موجود در کلاستر میشود و باعث میگردد تا سوئیچ دو مک آدرس یکسان را یاد بگیرد ولی از دو پورت مختلف ، به اینحالت MAC Flap میگویند بنابراین اگر مک آدرس کلاستر در حالت Unicast باشد باعث میشود هم سوئیچ و هم ارتباط بین سرورهای کلاستر دچار مشکل شود بنابراین مجبوریم سرورها را به هاب به جای سوئیچ وصل کنیم و به سرورها کارت شبکه دوم اضافه کنیم تا باهم در ارتباط باشند بنابراین برای رفع این مشکل از مک آدرس Multicast یا IGMP Multicast در صورت پشتیبانی سوئیچ استفاده میکنیم
- بین هاست های یک کلاستر ثانیه ای یکبار Heartbit تبادل میشود و بعد از ۵ ثانیه عدم تبادل Fail قلمداد میگردد
- NLB نقشی در جهت Sync شدن سرورهای داخل کلاستر ندارد

II

Rule in Server Cluster

1. **Per Ip Address** – بر اساس آی پی هایی که به کلاستر تخصیص داده شده است و سپس مراجعه کلاینت به بصورت مشخص به هر کدام از این آی پی ها نحوه تعامل بین سرورها از قانون خاصی تبعیت کند
2. **Per Port** – بر اساس پورت آی پی هایی که به کلاستر تخصیص داده شده است و سپس مراجعه کلاینت به بصورت مشخص به هر کدام از این پورت آی پی ها نحوه تعامل بین سرورها از قانون خاصی تبعیت کند
3. **Per Protocol** – نحوه همکاری سرورها در کلاستر بر اساس TCP,UDP شامل قانون های متفاوتی گردد

- بنابراین بر اساس ترکیب سه موضوع بالا میتوان Rule های مختلفی جهت همکاری هاستهای یک کلاستر تعریف نمود
- اگر کلاستر را درحالت **Single Host** قرار دهیم یعنی دیگر Load Balance وجود ندارد و سرورهای کلاستر را بصورت Active/Passive میخواهیم تعریف نمائیم و در لحظه فقط یک هاست سرویس خواهد داد و بقیه هاست ها رزرو هستند
- اگر از هاست Properties بگیریم در قسمت Port Rules ایتمی با عنوان **Handling Priority** وجود دارد که ترتیب جایگزینی در Single Host را مشخص میکند
- در حالت **Multiple Host** هر دو **FT+LB** را خواهیم داشت و در صورت انتخاب این گزینه میتوانیم نوع قرابت و وابستگی **Afinity** بین هاست ها و کلاینتها را بعد از اولین بار که ارتباط بین این دوبرقرار شد را مشخص نمائیم

1. **None** – وابستگی برقرار نخواهد شد و ممکن است کلاینت دفعه بعد به هاست دیگری وصل شود
2. **Single** – تا موقعیکه آی پی کلاینت عوض نشود و یا پارامترهای تقسیم کار بین هاست ها تغییر نکند کلاینت به همان هاست اولیه متصل شود
3. **Network** – تا موقعیکه NetID عوض نشود که شامل ۲۴ بیت اول آی پی کلاینت خواهد بود وابستگی برقرار خواهد بود و قویترین Afinity میباشد

– در این دو حالت میتوان Time out مشخص نمود و بعد تز آن بازه زمانی کار مجددا همانند بار اول سرویس گرفتن از هاست از نو تقسیم میشود

I

- در حالت Multiple Host پارامتری به نام Load Weight وجود دارد که میتوان به هاست ها با توجه به قدرت سخت افزاریشان وزن های متفاوتی داد تا سرویس بیشتری ارائه دهند
- حالت پیش فرض بدین شکل میباشد Multiple Host+Afinity(Single)
- فرض کنیم که در کلاستر دو هاست ویندوزی با دو IIS داریم بنابراین تا موقعیکه ویندوز ها پایدار باشند برای هم Heartbit میفرستند ولی اگر IIS هاست اول مشکل پیدا کند برفی از کلاینتها که به آن وصل میشوند سرویس نمیگیرند ولی کلاستر بعلت برقرار بودن Heartbit متوجه این موضوع نمیشود چون تا لایه ۴ کار میکند و از لایه ۷ که اپلیکیشن میباشد بی خبر است ، این موضوع جزو ایرادات NLB میباشد
- Afinity به این علت استفاده میشود تا اگر یک کلاینت یک Session باز برای یک اپلیکیشن یا سرویس خاصی با یک هاست داشته باشد مثلا Disconnect کرده باشد برای مراجعات بعدی بتواند ادامه کار را با همان هاست از سربگیرد

II

Active Directory Backup

- قبل از هر چیز بهتر است که AD اصلی بر روی یک ماشین فیزیکی نصب باشد تا به زیر ساخت مجازی وابسته نباشیم و نکته دیگر اینکه از بین دامین کنترلر ها حداقل یکی از آنها Core Mode باشد
- برای بکاپ گیری دامین کنترلرهای مجازی عمدتا از نرم افزار Veeam Backup and Replication استفاده میشود چون Application Aware نیز میباشد و در همین مورد دامین کنترلر را میشناسد و با لحاظ کردن این موضوع مبادرت به بکاپ گیری مینماید این موضوع در موقع برگرداندن بکاپ باعث میشود الزامات اکتیو دایرکتوری نیز مد نظر قرار بگیرد
- از ویندوز ۲۰۰۸ به بعد برنامه NTBackup حذف شده و به جای آن از Windows Server Backup استفاده میشود که با بکاپ گیری از System State دامین کنترلر عملا از اکتیو دایرکتوری نیز در کنار ویندوز بکاپ میگیرد
- این موضوع مهم است که بکاپ گرفتن از اکتیو دایرکتوری ارتباطی با مستر رولها ندارد بنابراین بکاپ گرفتن از System State یکی از دامین کنترلها برابر با بکاپ گرفتن از اکتیو دایرکتوری میباشد(DC+DNS SRV+GC SRV=SystemState)
- بنابراین فرقی نمیکند که از کدام دامین کنترلر System State را بکاپ بگیریم ⟵ Forest=Directory(ntds.dit+sysvol):DC1,DC2,....

فرض DC1:10.1.1.1 / DC1:10.1.1.2 → Active Directory Site and Services (NTDS Setting Replicated is Ok) Or→ Cmd → Repadmin /replsum is OK

- از طریق Server Manager اقدام به نصب Windows Server Backup Feature مینمائیم و سپس Wbadmin.msc Run→ Win SRV Backup
- از کامند نیز قابل اجراست ⟵ Wbadmin.exe
- در قسمت Local Backup در بخش Optimize Backup Performance جهت بکاپ گیری از درایو ها تنظیماتی وجود دارد که مربوط به System State نمیباشد ونقشی در بکاپ گیری صرفا اکتیو دایرکتوری ندارد

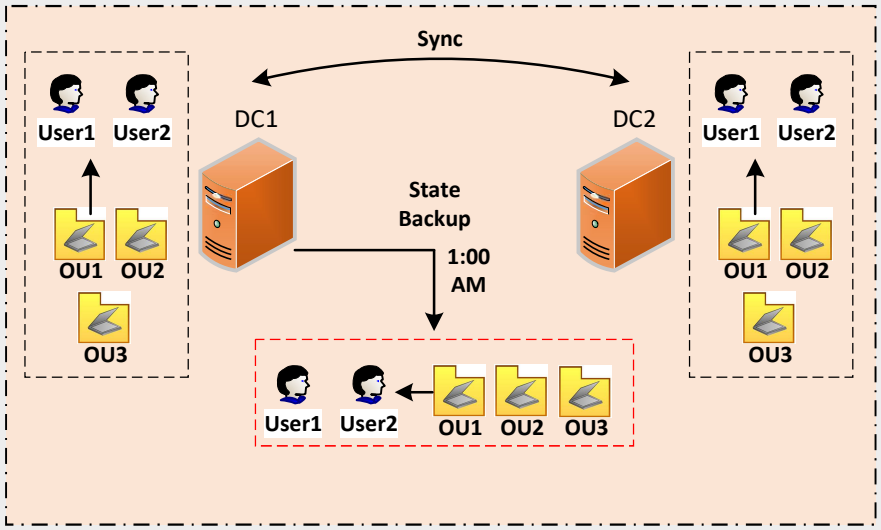
Local Backup → Backup once wizard →
- ① Schedule Backup Options — Schedule بکاپ بر اساس تنظیمات
- ② ✓Different options → ① Full Server
- ② ✓Custom —Add Items→ System State Backup → Choose Destination → Advanced Setting

Or
- ✓VSS Full Backup → پس از اتمام بکاپ گیری Transaction Log را پاک میکند
- ✓VSS Copy Backup → پس از اتمام بکاپ گیری Transaction Log را پاک نمیکند

- VSS (Volume Shadow copy Service) یک قابلیت در هنگام بکاپ گیری میباشد که این امکان را به سیستم بکاپ گیری میدهد تا بتواند از فایلهای In-Use بکاپ بگیرد
- این نکته مهم است که زمان بکاپ گیری به زمان شروع بکاپ برمیگردد و نه زمان اتمام آن
- بکاپ در داخل شافه WindowsImageBackup قرار میگیرد و بصورت یک هارد مجازی vhdx. گرفته میشود

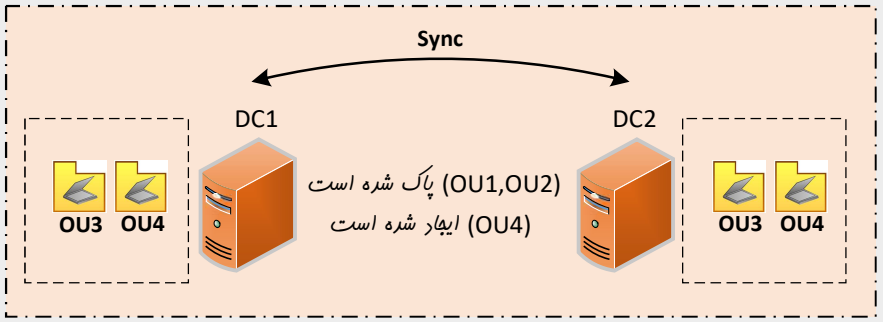
Data	Full Backup →	بکاپ از کل داده بصورت کامل
Full Backup	Differential Backup →	بکاپ از تغییرات نسبت به فول بکاپ گرفته شده
Last Backup	Increment Backup →	بکاپ از تغییرات نسبت به آخرین بکاپ گرفته شده
Daily Backup	→	بکاپ از تغییرات روزانه

Restore AD Backup



Stateful حالت AD دارد و خود به خود در حال تغییر است

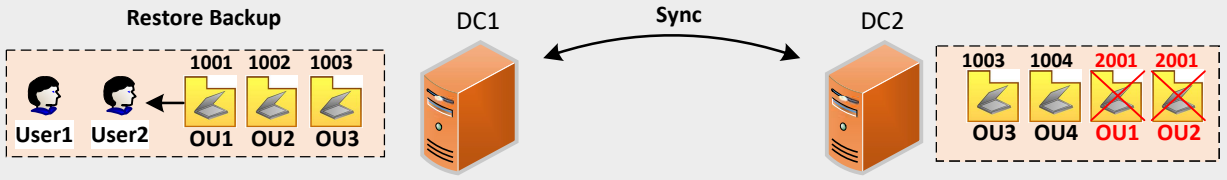
Change AD in 8:00 AM



- فرض کنیم که به شکل بالا انجام شده است ، بنابراین ابتدا دامین کنترلر اول را که توسط آن بکاپ گرفته بودیم در حالت DSRM بالا می آوریم در اینحالت هم میتوان از طریق Domain\administrator در صورت داشتن DNS DC2 و هم از طریق پسورد DSRM طبق هر شرایطی به دامین کنترلر لاگین نمود که اگر رمز آن را فراموش کرده بودیم قبل از ریستارت دامین کنترلر آن را ریست میکنیم

CMD → Ntsdutil → Set dsrm password
1. reset password on server null → New password:
2. reset password on server Servername → New password:

- جهت بالا آمدن ویندوز در حالت DSRM msconfig → Boot tab → ✓ safemode → ✓Active directory repair - نکته مهم اینکه پسورد DSRM وقتی ریست میشود یکبار مصرف است
- USN آبجکتها در هر دو اکتیو دایرکتوری یکسان هستند
- Object ها در اکتیو دایرکتوری صفتی Attribute دارند به نام Update Sequence Number که مشخص کننده Version Object میباشد فرض اینکه در موقع بکاپ USN ou1=1001 & ou2=1002 & ou3=1003 & ou4=1004
- حال وقتی Ou1,Ou2 پاک میشوند USN آنها تغییر میکند مثلا Ou1=2001,Ou2=2002 و به مدت ۱۸۰ روز Tomb Stone میشود
- حال فرض میکنیم ساعت **8:30 AM** بکاپ را بر روی **DC1** بر میگردانیم



بکاپ بر میگردد به یک بامداد

- طبق قاعده در چنین شرایطی به آخرین USN انجام میشود و دامین کنترلر ۱ همانند ۲ میشود و انگار هیچ کاری صورت نپذیرفته است

- نکته بسیار حائز اهمیت است که وقتی بکاپ را در دامین کنترلر اول در حالت DSRM برگرداندیم قبل از ریستارت کردن دامین کنترلر در حالت نرمال باید USN آبجکتهایی که نمیخواهیم در موقع سینک شدن در حالت نرمال تغییر یابند را افزایش دهیم

- بنابراین بعد از بکاپ گیری و قبل از ریستارت اگر مثلا Ou1=3001 قرار دهیم Ou1 در موقع سینک بین دو دامین حذف نخواهد شد و بدین روش Ou1 را احیاء نموده ایم که شامل زیرشاخه آن که User1,User2 میباشد نیز میشود

Local Backup → Recover → Select Backup Date (Catalog Backup (Meta data)) → System Sate → ✓Orginal location / ✗Perform an authorative restore of active directory

برگرداندن کل اکتیودایرکتوری به زمان بکاپ گیری
یعنی USN Database کل اکتیودایرکتوری افزایش پیدا کند

وقتی بخواهیم کل اکتیو دایرکتوری را برگردانیم از این گزینه استفاده میکنیم که مد نظر مانیست چون فعلا میخواهیم بخشی از آن را که شامل Ou1 میباشد برگردانیم

Primary Restore

- بعد از اتمام پروسه Restore و در مد DSRM باید USN Ou1 را افزایش دهیم و بعد در حالت نرمال ویندوز را بالا بیاوریم

I

افزایش USN برای Ou1

3 object(ou1,user1,user2)

معمولا تا سقف صد هزار تا USN را افزایش میدهد

CMD → Ntsdutil → Activate Instance ntds → Authorative restore → Restore subtree ou=ou1,dc=test,dc=com → Or → Restore subtree ou=ou1,dc=test,dc=com Version 10000

Restore subtree ← مثلا یک کانتینر یا OU

Restore object ← مثلا یک عدد یوزر یا کامپیوتر اکانت

II

Windows Deployment Service(WDS)

نصب ویندوز از طریق شبکه

RIS (Remote Installation Service) → (تغییر نام) Windows Deployment Service(WDS)

- نصب ویندوز از طریق شبکه توسط SCCM نیز امکان پذیر و مفصل میباشد
- از ویندوز ویستا و ویندوز ۲۰۰۸ به بعد نصب ویندوز به شکل برگرداندن ایمیج انجام میگردد و به همین دلیل نصب ویندوز سریعتر شده است
- برای نصب ویندوز به دو ایمیج نیازمندیم

1 Boot Image

- یک WinPE (Windows Preinstallation Environment) شفارشی Customize شده و سبک است و وظیفه آن پیرو درک اولیه از سفت افزار سیستم فراهم نمودن یک محیط برای نصب ویندوز است
- از WinPE برای Live Recovery نیز استفاده میشود
- فایل با پسوند wim (Windows Image format). در برگیرنده ایمیج میباشد و فودش ایمیج نیست و همچنین Boot.wim دربرگیرنده WinPE

2 Install Image

- شامل ایمیج ویندوز میباشد و داخل فایل Install.wim قرار میگیرد
- ایمیج Install.wim اصطلاحا Sysprep یا همان Generalize شده است و در واقع ایمیج بی هویت تلقی میگردد

Boot.wim

```
PS C:\Windows\system32> dism /get-wiminfo /wimfile:g:\sources\boot.wim

Deployment Image Servicing and Management tool
Version: 10.0.19041.844

Details for image : g:\sources\boot.wim

Index : 1
Name : Microsoft Windows PE (x64)
Description : Microsoft Windows PE (x64)
Size : 1,399,799,034 bytes

Index : 2
Name : Microsoft Windows Setup (x64)
Description : Microsoft Windows Setup (x64)
Size : 1,549,873,579 bytes

The operation completed successfully.
```

Install.wim

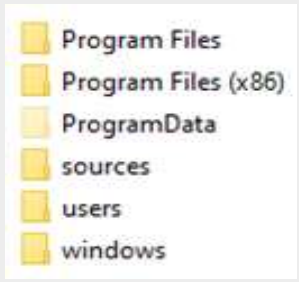
```
PS C:\Windows\system32> dism /get-wiminfo /wimfile:g:\sources\install.wim

Deployment Image Servicing and Management tool
Version: 10.0.19041.844

Details for image : g:\sources\install.wim

Index : 1
Name : Windows Server 2016 Standard
Description : This option (recommended) reduces management and servicing by installing only what is needed to run most server roles and applications. It does not include a GUI, but you can fully manage the server locally or remotely with Windows PowerShell or other tools. For more details see "Windows Server Installation Options."
Size : 9,481,916,907 bytes

Index : 2
Name : Windows Server 2016 Standard (Desktop Experience)
Description : This option is useful when a GUI is required—for example, to provide backward compatibility for an application that cannot be run on a Server Core installation. All server roles and features are supported. For more details see "Windows Server Installation Options."
Size : 15,560,241,110 bytes

The operation completed successfully.
```

Windows Deployment Service(WDS)

```
PS C:\Windows\system32> dism /mount-image /ImageFile:g:\sources\boot.wim /index:1 /mountdir:d:\temp  /readonly

Deployment Image Servicing and Management tool
Version: 10.0.19041.844

Mounting image
[==========================100.0%==========================]
The operation completed successfully.
```

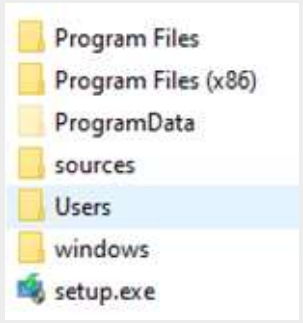
- از همین روش برای تغییر در یک ایمیج نیز میتوان استفاده نمود
- مانند اضافه نمودن ویژگی یا درایور به ایمجهای Install.wim

D:\temp →

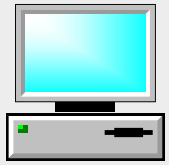



```
PS C:\Windows\system32> dism /mount-image /ImageFile:g:\sources\boot.wim /index:2 /mountdir:d:\temp  /readonly

Deployment Image Servicing and Management tool
Version: 10.0.19041.844

Mounting image
[==========================100.0%==========================]
The operation completed successfully.
```

D:\temp →



- فرض که یک کامپیوتر BareMetal داریم بدین معنی که خام است و فاقد هر گونه سیستم عامل



BareMetal → Via → NetworkCard PXE Bootrom → ① Boot from PXE → ② DHCP Discover, Take IP → ③ Connet to WDS, Boot images, Install Images

① WDS,DHCP SRV Are In one Broadcast Domain

- چون WDS و DHCP SRV هردو بر روی پورت ۶۷ گوش میدهند جهت دیسکاور شدن کفایت میکند ، حال در مرحله بوت از TFTPبدون احراز هویت و در مرحله نصب از SMBبا احراز هویت استفاده میشود

② WDS,DHCP SRV Are in different Broadcast Domain

- در اینحالت که مرسوم است DHCP SRV باید Option مرتبط با WDS را ارائه دهد

Option 66 =WDS Name or IP

Option 67 =WDS Boot File Name Location

Boot\x64\pxeboot.com

③ WDS,DHCP SRV Are on Same Server

- در اینحالت نیاز است بر روی DHCP SRV فقط Option 60 =PXE Client تنظیم شود
- بهتر است برای سازمان Win Enterprise LTSC در نظر گرفته شود
- در محیط ویندوز در حال حاضر از Capture image استفاده میگردد که از روی Boot image ساخته میشود

(win 10 LTSC+office2019+Application+Utility+Driver+agent+full update) → Sysprep → **Capture image**

Server Manager → Add Roles & Features → **Role Windows Deployment Service**

Wdsmgm.msc → Run → **Win Deployment Service**

I

Windows Server Update Services (WSUS)

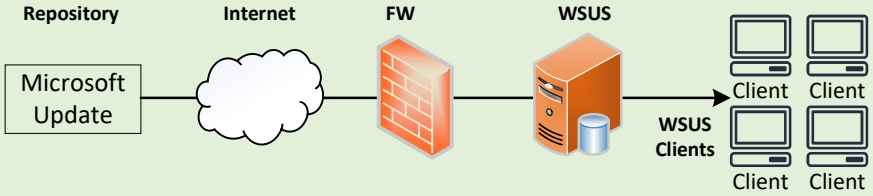
- جهت برقراری امنیت بیشتر محصولات مایکروسافت و برطرف شدن Bug های احتمالی و اضافه شدن امکانات و قابلیتها الزام به بروزرسانی خواهیم داشت
- پروسه بروز رسانی شامل چند مرحله میشود **(1-Check site for new update 2-Download 3-Test 4-Deployment)**
- در صورت اتوماتیک آپدیت دافلی کلاینتها مشخص است که مرحله سوم حذف خواهد شد و ممکن است باعث بروز مشکل در کلاینتها شود و بهتر است در تنظیم آن Notify گذاشته شود تا با اطلاع دانلود یا نصب گردد هرچند که مدیریت آن غیر متمرکز است و مطلوب نیست بنابراین از WSUS استفاده میکنیم
- کلاینتها بعد از تایید WSUS میتوانند خود مستقیم از طریق اینترنت آپدیتها را دریافت و نصب کنند و یا اینکه آپدیتها در سرور WSUS ذخیره شود و کلاینتها با مراجعه به سرور آپدیت را دریافت نمایند تا باعث کاهش مصرف اینترنت شود که کار فرعی این سرور محسوب میشود

II

WSUS Planning

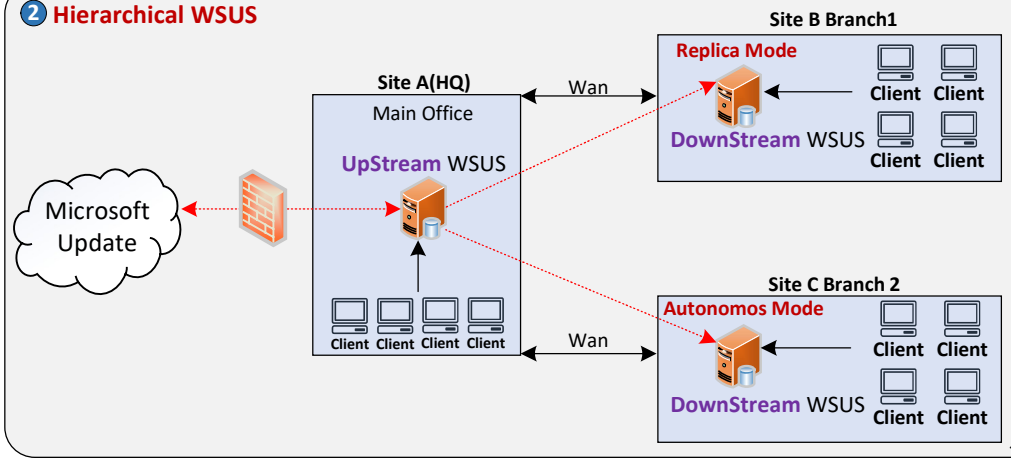
- WSUS از ویندوز 2008R2 به بعد به مجموعه رولهای ویندوز اضافه شده است

1 Simple Deployment With Computer Groups



- طراحی های مختلفی برای پیاده سازی WSUS و جود دارد ولی عموما از روش Simple Deployment+Computer Groups استفاده میگردد از ویندوز ۲۰۱۲ به بعد از پورت ۸۵۳۰ برای Http و ۸۵۳۱ برای Https استفاده میشود
- ویژگی WIB از ویندوز ۲۰۰۸ به بعد به ویندوز اضافه گردید که تقریبا SQL Express میباشد و برای مدیریت کامپوننت های ویندوز اعم از Roles & Features نیز استفاده میشود ، عموما WIB برای دیتابیس WSUS تا ۲۰۰ کلاینت کافی میباشد
- جهت ایجاد و مدیریت دیتا بیس WSUS میتوان از WIB(Windows Internal Database) یا SQL استفاده نمود

2 Hierarchical WSUS



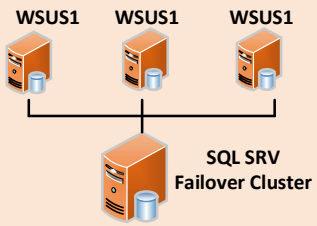
1 Centralize Management → Replica Mode (Microsoft Update+Config Replication)

- فقط یکبار کانفیگ از طریق UpStream WSUS به DownStream WSUS اعمال گردیده و مدیریت متمرکز انجام میشود
- برای مدیریت مشترک گروه های ایجاد شده یکسان در کل WSUS ها کاربرد دارد

2 Distributed Management → Autonomos Mode (Microsoft Update)

- اگر بخواهیم مدیریت DownStream WSUSها بصورت مستقل انجام شود مورد استفاده قرار میگیرد
- در حالتی که گروهای مختلفی با پالیسی های متفاوت در سایت های متفاوت مورد نیاز باشد مورد استفاده قرار میگیرد
- اجازه دسترسی Full Control به سرور های پایین دستی همراه با WSUS Administrator مستقل مورد استفاده قرار میگیرد

3 Network Load Balancing



- اگر تعداد کامپیوترهایی که به WSUS برای آپدیت وصل میشوند بسیار بالا باشد از Load Balance استفاده میگردد
- جهت برقراری Load Balance باید الزاما از SQL استفاده نمود
- همانطور که تعداد SQL ها میتواند بیش از یک سرور با یک ماهیت باشد در مورد WSUS ها نیز میتوان NLB برقرار نمود

I 4 Disconected WSUS SRV

- ممکن است در سازمانی یک شبکه مستقل از شبکه اصلی داشته باشد مانند شبکه حراست که یک شبکه ایزوله بدون اینترنت دارد
- یک WSUS در شبکه حراست راه اندازی میشود سپس میتوان مجموعه فعالیتهای یک WSUS ی که خارج از شبکه حراست به اینترنت وصل می باشد را Export نموده و بر روی WSUS شبکه حراست Import می نمائیم
- از Import-Export بعنوان بخشی از بکاپ گیری WSUS نیز استفاده میشود

II WSUS installation

1-Hardware
2-Software
2-1 windows Component
2-2 Report Viewer Redistributed (optional)
3-System (NTFS volume)
4-Install (Pre & Post)
5-Config wsus

- در مواقعی که فقط یک سایت داریم عموما از Simple Deployment With Computer Groups استفاده میشود
- جهت عملکرد بهینه WSUS باید حتما بر اساس مستندات مایکروسافت Customize شود بطور مثال تنظیمات IIS
- WSUS تا موقعیکه آپدیت نشود عملا کاربردی نیست چون باید لسیت انواع آپدیتها (Products) را بروز نماید
- در هنگام نصب WSUS اگر محلی را برای ذخیره سازی آپدیتها مشخص نکنیم بدین معنی تلقی میشود که فقط میخواهیم از طریق WSUS آپدیتها را مدیریت نمائیم تا پس از تایید ، توسط کلاینتها از اینترنت بصورت مستقیم دانلود شوند و نمیخواهیم کلاینتها آپدیت ها را پس از تایید از WSUS دریافت نمایند
- در حالتیکه محلی برای ذخیره آپدیتها برای WSUS مشخص کنیم صرفا متا دیتا یا فهرست آپدیتها دانلود میشود و پس از تایید WSUS مبادرت به دانلود و ذخیره آپدیتها در محل ذخیره سازی می کند
- پس از نصب WSUS برای اولین اجرا Wizard نشان داده میشود که میتوان کنسل نمود و بصورت دستی کانفیگ را انجام داد
- برای اجرای کنسول WSUS از طریق Run باید مسیر این فایل را به پیش فرض ویندوز اضافه کرد یا از میان بر استفاده نمود

Wsus.msc Run WSUS Console

Windows Administrative Tools → Windows server update services → Wsus.msc

- اگر در شبکه از Web Proxy Server استفاده شود باید اپلیکیشن WSUS رابعنوان Web Proxy Client کانفیگ نمائیم

III WSUS Console Options

1 Update Source and Proxy Servers

- جهت تعریف UpStream & DownStream WSUS, Autonomos Mode , Replica Mode, Web Proxy Client استفاده میشود

2 Product & Classification

- جهت مشخص نمودن انواع آپدیتها (Products) در شبکه مورد استفاده قرار میگیرد کانفیگ نمودن این بخش نیازمند آپدیت اولیه WSUS میباشد
- مجموعه محصولات ویندوز یا آفیس هایی یا غیره که در شبکه مورد استفاده قرار میگیرند را انتخاب می نمائیم

Classification

- بعد از مشخص نمودن Products باید Category آن را نیز مشخص نمود (Critical Updates,Definition Updates,Feature Packs,Security Update,Service Packs,Tools,Update Rollups,Updates,Upgrade)

3 Update File and Languages

- بصورت پیش فرض به همه زبانها آپدیت را میگیرد که باید فقط برای زبان انگلیسی آن را از بخش Update Languages فعال نمود
- جهت مشخص نمودن وضعیت سرور برای ذخیره سازی آپدیتها بر روی خود سرور یا سپردن این وظیفه به کلاینتها از بخش Update Files استفاده میشود
- این امکان وجود دارد که DownStream WSUS به شکلی تنظیم گردد که توسط UpStream WSUS مدیریت بشود ولی برای گرفتن آپدیتها بعد از تایید ، آنها را بصورت مستقل از اینترنت دریافت نماید
- Express Update روشی است که دانلود آنها نسبت به حالت نرمال زمان بیشتری در برخواهد داشت چون از نظر حجم بزرگتر از Normal Update هستند ولی نصب آنها بر روی کلاینتها سریعتر از حالت نرمال میباشد

I

4 Synchronization Schedule

- مشخص میشود آپدیت فهرست از بالادستی Upstream WSUS or Internet بصورت دستی انجام شود و یا طبق زمانبندی خاصی بصورت اتوماتیک با آفست ۳۰ دقیقه میباشد

5 Automatic Approvals

- آیا آپدیت های خود WSUS اتوماتیک تایید شوند؟
- اگر یک آپدیت توسط ادمین مورد تایید قرار گرفت آیا Verision جدید آن آپدیت بصورت اتوماتیک تایید گردد یا خیر؟ البته در صورتیکه وریژن قبلی قبلا مورد تایید قرار گرفته باشد
- اگر Verision جدید یک آپدیت مورد تایید قرار گرفت آیا نسخه قبلی Decline شود؟
- در این قسمت میتوان Rule نوشت مثلا Security Update برای گروه تست اتوماتیک تایید شود

II

تنظیم کامپیوترها برای آپدیت گرفتن از WSUS در شبکه دامین مدل

Gpmc.msc → Computer Configuration → Administrative Templates → Administrative Templates → Windows Components → Windows Update → ✓Configure Automatic Updates / ✓Specify Interanet Microsoft Update Service Location

Configure Automatic Updates → **4-Auto Download and Schedule the install**

- نکته اول اینکه زمانبندی مر بوط به نصب آپدیتها میباشد و نه دریافت آن و دوم اینکه اگر فرضا زمانبندی نصب فرضا ۳ بامداد باشد کلاینتهایی که در آن زمان خاموش بوده اند بعد از روشن شدن با کمی تاخیر مبادرت به نصب مینمایند

Specify Interanet Microsoft Update Service Location → **1-Set the intranet statistics server 2-Set the alternate download server**

- بعد از اینکه طبق گزینه اول مشخص کردیم ویندوز آپدیت فعال است حال از طریق این گزینه مشخص میکنیم که WSUS بر روی چه سروری قرار دارد و رفتار آن باید به چه شکل باشد
- کلاینت جهت اعلام وضعیت خود و دانلود آپدیت های تایید شده به WSUS مراجعه میکند ، این امکان وجود دارد که سروری که اعلام وضعیت را دریافت میکند از سروری که آپدیت را ارائه میدهد جدا باشد
- بعد از اعمال پالیسی بر روی کامپیوترها آنها به WSUS مراجعه نموده و بعنوان کلاینت آن بصورت Unassigned رجیستر میشوند
- میتوان از طریق کنسول WSUS و کلیک سمت راست بر روی Computers گروه های مختلفی را ایجاد کرد و کامپیوترهای Unassigned را به این گروه ها نسبت داد
- اگر یک آپدیتی توسط آپدیت دیگر Supersed شده باشد یعنی آن آپدیت با حضور آپدیت جدیدتری از دور خارج شده است و در چنین شرایطی باید آپدیت قدیمی منسوخ شده را Declined نمائیم
- به این مفهوم که هر کامپیوتری در WSUS عضو چه گروهی باشد Targeting گفته میشود که شامل Client Side که کلاینت به WSUS میگوید عضو چه گروهی است و یا Server Side که از طریق کنسول مشخص میکنیم هر کلاینتی عضو چه گروهی است ، برای بحث Client Side نیاز به یک پالیسی داریم

Gpmc.msc → Computer Configuration → Administrative Templates → Administrative Templates → Windows Components → Windows Update → ✓Enable Client Side Targeting → **(Insert Name of Group)**

5 Computers

- میتوان چگونگی Assign شدن کامپیوترها به گروه ها را میتوان مشخص نمود که Client Side , Wsus عمل نماید یا Server Side
- در صورت Crash کردن WSUS باید از طریق IIS/application pools عمل recycle و یا Stop/Start را انجام داد

WSUS Import/Export

- برای این کار باید از کامند **Wsusutil.exe** استفاده کنیم و جهت استفاده از طریق Run باید مسیر این فایل اجرائی به مسیرهای ویندوز اضافه گردد

Wsusutil Run→ WSUS Utilities

- Export کردن صرفا شامل متا دیتا یا همان کاتالوگ میگردد و حاوی خود آپدیتها نمیباشد و برای خود آپدیتها باید از فولدر مربوطه بکاپ جداگانه گرفته شود فقط باید دقت نمود که اگر بصورت معمولی Copy/Paste شود NTFS Permission تغییر میکند جهت رعایت این موضوع میتوان از دستور Robocopy استفاده نمود یعنی از روندی همچون Backup/Restore استفاده نمود Wsusutil Import , Wsus Export

- جهت تغییر محل ذخیره سازی آپدیتهای WSUS باید از کامند Wsusutil movecontent استفاده نمود

BITS (Backgroung Intelligent Transfer Service)

- قابلیتی است که در بحث ترنسفر فایل مطرح میشود و دو امکان به میدهد

1. طرفینی که در تبادل داده شرکت میکنند از پهنای باند آزاد موجود و قابل استفاده یکدیگر مطلع میشوند و از همان پهنای باند موجود استفاده میکنند و تلاشی برای آزاد کردن پهنای باند بیشتر نمیشود
2. درصد ترنسفر دیتا و میزان باقیمانده دیتا مشخص میگردد

- WSUSمیتواندراز حالت BITS استفاده کند که بدین منظور باید از طریق Featuresهای ویندوز نصب و راه اندازی شود