**Topic 2**

*Active directory* është një koleksion i shërbimeve (Server roles) që mundëson menagjimin e centralizuar të *identiteti* dhe *aksesit* në resurset e një rrjete.

*Shërbimet ose rolet* që përfshihen në *Active Directory* janë : *Domain Services, Federation Services, Certificate Services, Rights Managment Services, Light weight Directory Services*. Diagram

Description automatically generated

*Domain Services* : Është shërbim me të cilin menagjojmë objektet që gjinden mbrenda një korporate duke përfshirë kompjuterët, useart, printerat, policies etj, pra këtu përfshihet authentikimi dhe authorizimi i accoutant-ave internal. Ky sherbim mbane informata mbi te gjitha resurset e rrjetit.

*Certification Services* : Përdoret për implementimin e infrastrukturës PKI, gjithqka që kërkon qasje të sigurtë realizohet me anë të CS.

*Federation Services* : Përdoret kur kemi nevoj të bëjm ndërlidhje të resurseve në mes dy organizatave të ndryshme (krijimi i një Federation Trust në mes dy domains). Ky shërbim na ofron : lidhje të sigurt në mes dy organizatave, mundësi të qasjes në aplikacione nga njëra organizat në tjetrën, SSO(Single Sign-on) në mes dy directories(të organizatave) në web-aplikacione.



Web Server



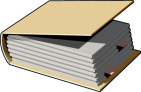
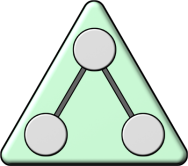
Resource   
Federation Server

Account Partner Organization

Resource Partner Organization



Account   
Federation Server



AD DS



Federation Trust

*Rights Managment Services* : Mundëson që komunikimi dhe ndarja e të dhënave të jetë i monituruar duke mundësuar administratorit që të kontrolloj se kush qfar mund të bëj me dokumentet e caktuara pa vartësisht se ku ato gjinden, mund të vendos se kush mund ti printoj ato, forward, kopjoj etj. prsh nëse një user A pranon një email nga një person B, me anë të *RMS* ne mund ta ndalojmë personit A që atë email ta bëj forward.

*Light Weight Directory Services* : Është një *DS* i zbrazët. Popullimi i të cilit mund të bëhet nga platforma tjera (domain tjera), përshembull nëse duam që me anë të gmail ti lejojmë qasje userave në domain tonë. Pra si sherbim kryesore ka SSO.

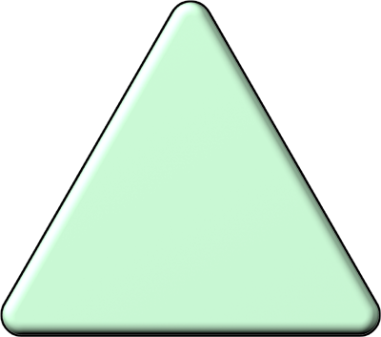
*Arsyeja pse na duhet AD DS është centralizimi i menagjimit të userave, kompjuterave dhe resurseve tjera në rrejtë.*

*Features që AD DS na i ofron* : Centralized directory, SSO access, Integrimi i sigurisë, Scalability, Common managment interface.

*Centralized Network Management* është një lokacion i vetëm ku menagjohet gjdo komponent brenda një rrjeti.

Për të instaluar *AD* *DS* duhet plotësuar disa kërkesa ato janë: *Konfigurimi i TCP/IP dhe DNS server adresave (për arsye komunikimi), Kredencialet e një useri i cili ka akses si administrator lokal i serverit (që është pjesë e Domain Admin grupit), duhet që DNS serveri të jetë i instaluar*.

*Domain* është një perimeter që përdoret për të grupuar, menagjuar, sigurar komunikimin dhe qasjen në objektet brenda një organizate.



Contoso.com

Për të krijuar një *sub-domain* duhet të trashëgohet emri primar i domain it. *Sub-domain* mund të kenë sub-domains tjetër. Në momentin kur krijohet një sub-domain krijohet një two-way transitive trust me domain tjerë. Krijimi i sub-domains rezulton në krijimin e një peme të domainave.

A picture containing text

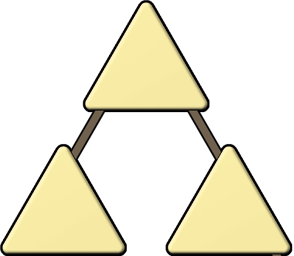
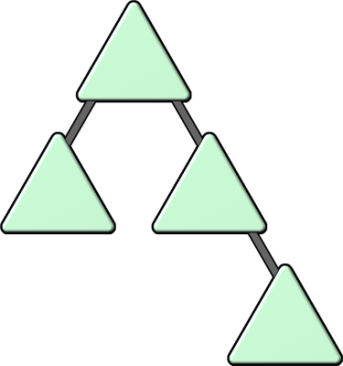
Description automatically generated

contoso.com

emea.contoso.com

emea.contoso.com

*Forest* është koleksion i një ose më shumë pemëve të domaina-ve. Secili domain në forest ka skemën e njëjtë, partitional konfigurimet e njëjta si dhe kanë trusted connection mes domainave.



*Trust* në mes domains mund të jetë *Directional* (Trusted domains can access Trust domain). *Transitive* (Domains access each others).

*Objektet në një DS konsiderohen* : User, InetOrgPerson, Contacts, Groups, Computers, Printers, Shared Folders. Këto objekte *DS* i menagjon me anë të *Group Policy*.

*AD DS* është e përbërë nga *komponenta fizike*: Domain controller, Data Store, Global Catalog Server, Replications. *Komponenta logjike*: OU, Domain, Tree, Forest, Schemas, Sites.

Diagram

Description automatically generated*Domain Controller* Është serveri i domainit i cili e ka të instaluar *AD DS* dhe konfigurimet e bëra si prsh objektet e shtuara(kompjuterët, userat, OU...), Group Policies. E gjithë domain dështon nëse *Domain Controlleri* dështonë, për këtë arsye *Domain Controlleri*, duhet të bëhet back-up. Ka disa forma si bëhet back-up mirpo më e aplikueshme është replikimi i *Domain Controllerit*.

*Global Catalog Serveri* është i ngjajshëm me Controllerin vetëm se në vete nuk mban të gjitha attributet e objekteve por vetëm më të rëndësishmet.

*AD DS Data Store* përbman data base file në të cilin ruhen të dhënat rreth userave, shërbimeve dhe aplikacioneve, ruhet në follderin %SystemRoot%\NTDS dhe në të kan qasje vetëm domain controllerat.

*AD DS Replication* – Kujdeset për kopjimin e ndryshimeve në AD DS databazën në të gjith domain controllerat. Na siguron konsistenc të të dhënave në domain controllera.

*AD SD Sites* – Paraqet një network segment në të cilin të gjithë domain controllerat komunikojnë me shpejtësi dhe siguri.

*AD DS Scheme* – Definon llojin e objekteve dhe rregullat që duhet ndjekur për konfigurimin dhe krijimin e tyre.

*OrganizationUnit:* Janë kontenier që bëjnë orgaznimin hierarkik dhe logjik të objekteve për konsistencë në menagjimin e tyre si dhe aplikimin e politikave. Arsye pse përdoren *OU* është aplikimi i rregulloreve(group policy) në bazë të njësisë, prsh në bazë të departamentit. Mund të shihet se më poshtë përveq ndarjes në departamenta janë bërë ndarje edhe në llojin e paisjes, kjo për arsye se në rastin kur kemi le të themi një update në drivera të grafikave, update i ndryshëm duhet të meret për laptop e tjetër për pc.

*GPO’ (Group Policies)* – janë konfigurime dhe settings që aplikohen në users ose computers.

Graphical user interface, text, application, email

Description automatically generated

*Grupet* ndahen në dy kategori : *Security groups(usera të cilëve i jep qasje në resourse të caktuara)* dhe *Distributed groups(grup që përdoret për shpërndarje të informatave, nuk mund të përdoret për qasje)*.

*Active Directory Sites and Services* : përdoret në raste kur kemi dy domain që duan të komunikojnë dhe janë në lokacione të ndryshme gjeografikave.

*DNS* është roli i dytë më i rëndësishëm pas *DS*.

Në kuadër të *DNS* ekzistojnë disa rekorde të rëndësishme të cilat i ndajmë në : 1.*Host record (A or AAAA) – Ky rekord bën shoqërimin e IP adresës me një emër (A-IPV4, AAAA-IPV6). 2.Alias record (CNAME) – Ky rekord bën përkthimin e një emri në një emër tjetër. 3.Mail exchanger record (MX) – Përdoret për konfigurim të email-ave, mundëson komunikimin mes hostave në domainin tonë me domain ku gjendet shërbimi i email, një ip e ktij rekordi mund të përdoret vetëm për email. 4.Name server record (NS) – Tregon se cili Name Server të përdoret në një DNS zone*.

*Back Up And Restore* : është roli më i thjeshtë që mund të instalohet në serverë mirpo, është më i ndjeshmi dhe më obligativ pas *DS*.

Llojet e Back-up : *1.Full* – E dhëna ruhet kompletë. 2.*Incremental* – Pas full të parë backup tjerë vetëm shtojnë ndryshime në backup e parë. (best, lejon kthim në versione të vjetra) 3.*Differential* – Pas full i ruan vetëm dallimet mes backup të parë dhe të dytë. (kthimi problem) 4.*Schedule* – Orar specifik. 5.Automate.