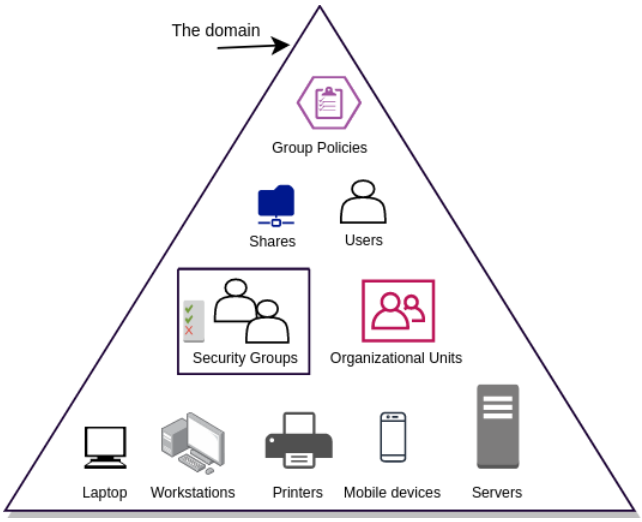
CYBER STRUGGLE
TASK- Active Directory Fundamentals

Hazırlayan:
DCS001 Hakan ŞEN
Aralık 2023
Ankara

1. What are the fundamental components and objects within Active Directory? Provide a detailed explanation.



Active directory temel bileşenleri ve objectleri aşağıda çıkarılmıştır.

Etki Alanı Denetleyicileri:

Active Directory'nin kalbinde etki alanı denetleyicileri bulunmaktadır. Onları ağın koruyucuları olarak düşünebilirsiniz; kullanıcıları doğrulama, izinleri yönetme ve Active Directory veritabanının bir replikasını koruma gibi görevlere sahiptirler. Bu sunucular, ağ içindeki tüm değişikliklerin senkronize edildiğinden emin olarak tutarlılık ve güvenilirlik sağlar.

Etki Alanları:

Etki alanları, dijital peyzajın belirli bölgelerini temsil eder. Her etki alanı belirli bir yönetimsel sınırlamayı temsil eder ve kullanıcılar, bilgisayarlar ve gruplar gibi nesnelerin bir koleksiyonunu içerir. Etki alanları, bir orman oluşturmak için bir araya getirilebilir, ağ yönetimi için hiyerarşik ve ölçeklenebilir bir yapı sağlar.

Organizasyon Birimleri (OU):

OU'ları, bir etki alanı içindeki organizasyonel bölümler olarak düşünebilirsiniz. Nesneleri daha ayrıntılı bir şekilde düzenlemek ve yönetmek için bu konteynerlar olarak hizmet verirler. Örneğin, bir şirket içinde farklı departmanlar için OU'larınız olabilir, bu da politika ve izinler üzerinde daha hassas kontrol sağlar.

Kullanıcılar:

Kullanıcılar, ağ ile etkileşimde bulunan bireyleri temsil eder. Active Directory'deki her kullanıcı nesnesi, kullanıcı adları, şifreler ve grup üyelikleri gibi bilgileri içerir. Bu bilgiler, kimlik doğrulama ve yetkilendirme süreçleri için kritiktir, kullanıcılara ağ kaynaklarına uygun erişimi sağlar.

Gruplar:

Gruplar, kullanıcı hesaplarını yönetmeyi kolaylaştıran sanal koleksiyonlardır. İzinleri bireysel kullanıcılara atamak yerine kullanıcıları gruplara ekleyebilir ve grup, izinleri devralır. Bu, erişim haklarını vermek veya geri almak için yönetimi daha verimli hale getirir.

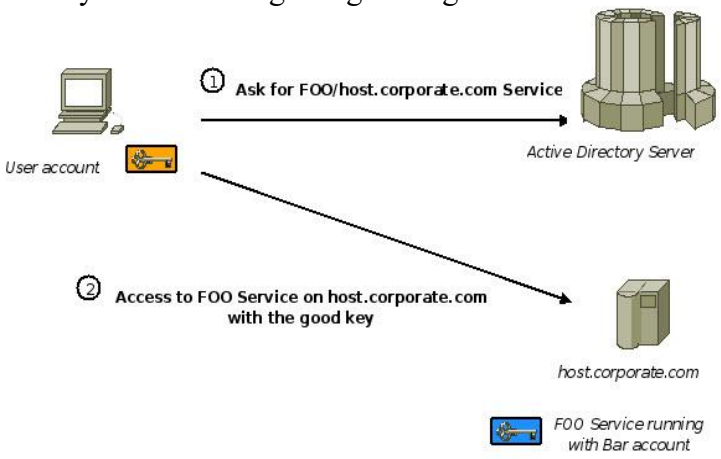
Bilgisayarlar:

Bilgisayarlar, Active Directory'deki nesneler olarak, ağa bağlı makineleri temsil eder. Bu nesneler, politikaları uygulamak, yazılım dağıtmak ve tüm etki alanındaki bilgisayarlar üzerinde tutarlı bir şekilde güvenlik yapılandırmalarını sağlamak için merkezi yönetimi kolaylaştırır.

Grup İlkesi:
Grup İlkeleri, yöneticilerin merkezi olarak tanımlayabileceği bir dizi yapılandırmadır. Bu politikalar, kullanıcıların ve bilgisayarların davranışını yönetir. Güvenlik seçeneklerinden masaüstü görünümüne kadar geniş bir yelpazede ayarı içerir, organizasyonel standartları uygulamak için güçlü bir araç sağlar.
Güven İlişkileri:
Active Directory'nin bağlantılı dünyasında güven önemlidir. Güven ilişkileri, orman içindeki etki alanlarının birbirine güvenini tanımlar. Bu, farklı etki alanları arasında kaynaklara sorunsuz erişim sağlarken güvenlik ve erişim kontrolünü sürdürür.
Şema:
Şema, Active Directory'de depolanabilecek nesne türleri için yapının ve kuralların tanımını yapar. Bu, bilginin nasıl depolandığı ve erişildiği konusunda tutarlılık ve bütünlüğü sağlamak için bir çırpıda görev yapar.
Temelde, Active Directory, bu bileşenlerin bir arada çalışarak ağ yönetimi için sağlam ve ölçeklenebilir bir altyapı sağladığı dinamik bir ekosistemdir. Her bileşen, kullanıcıların ve kaynakların sorunsuz etkileşim sağladığı tutarlı ve güvenli bir ortam yaratmada benzersiz bir rol oynar.

2. How does Active Directory use Service Principal Names (SPNs) for service identification and authentication?

Active Directory, ağ içinde hizmetleri benzersiz bir şekilde tanımlamak ve kimlik doğrulamasını sağlamak için Service Principal Names - SPN kullanır. SPN'ler, belirli oturum açma hesapları ile ilişkilendirilerek istemciler ve hizmetler arasında sorunsuz ve güvenli iletişim süreçleri için bir mekanizma sunar. Bu mekanizma, Kerberos kimlik doğrulama protokolünde önemli bir rol oynayarak Active Directory ortamlarının genel güvenliğini artırır.



3. Explain the significance of Security Identifiers (SID), Fully Qualified Domain Names (FQDN), and the NTDS.DIT database in Active Directory.

SID
Windows ortamlarında kullanıcılara, gruplara ve bilgisayarlara atanmış benzersiz tanımlayıcılardır.
Erişim kontrolü, kimlik doğrulama ve yetkilendirme için Active Directory (AD) altyapısında kullanılır.

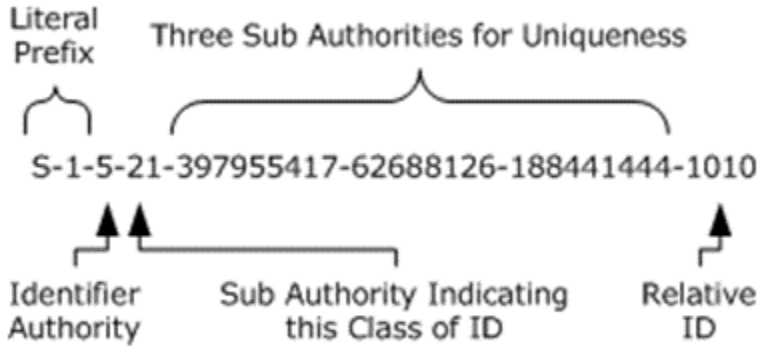
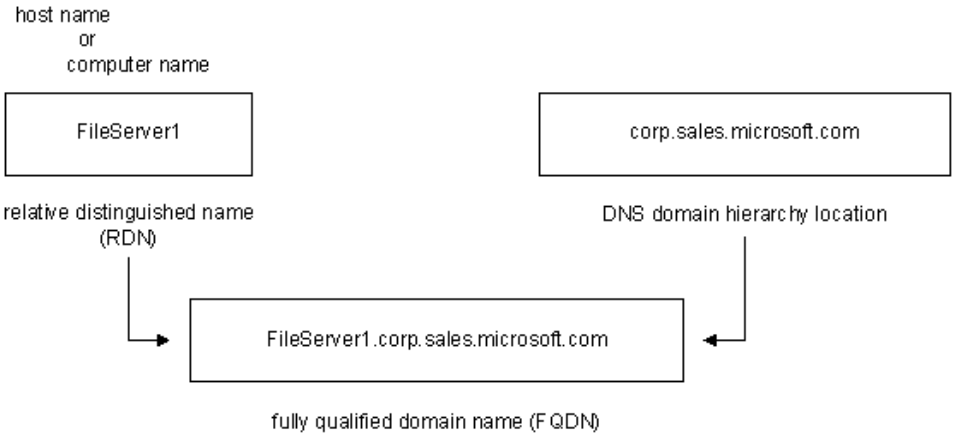
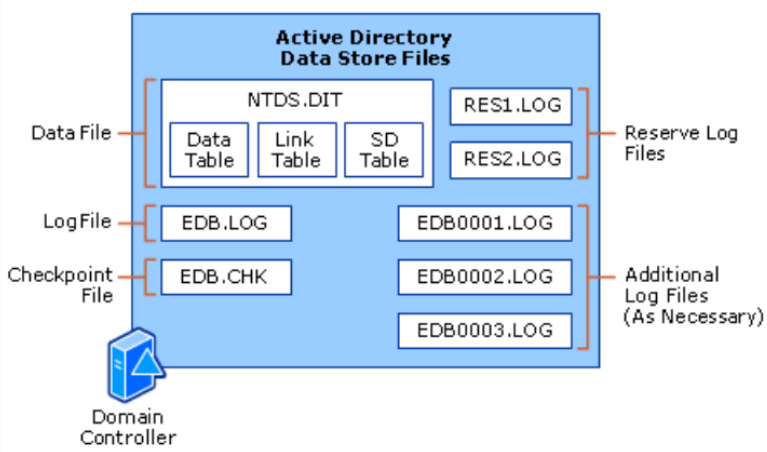


Figure 3: SID with account association

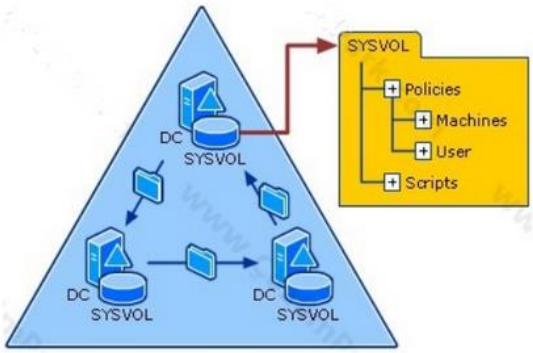
FQDN
Bir bilgisayarın veya kaynağın tam alan adını belirten, DNS hiyerarşisindeki tam konumunu gösterir.
Ağdaki kaynakların kesin tanımlanması ve konumu için temel, alan adlarını IP adreslerine çözümleme konusunda yardımcı olur.



NTDS.DIT
Active Directory'nin ana veritabanıdır ve nesneleri, öznitelikleri ve ilişkileri içerir.
AD'nin işleyişi için merkezi bir rol oynar, dizin yapısını, kullanıcı hesaplarını, güvenlik politikalarını saklar ve veri tutarlılığı için etki alanı denetleyicisi replikasyonunu kolaylaştırır.



4. Describe the role and importance of SYSVOL in Active Directory, especially in terms of replication.



SYSVOL, veya System Volume, Active Directory (AD) içinde temel bir bileşen olup, alanın işleyişi ve bütünlüğünde kritik bir rol oynar.

SYSVOL, temelde, Grup Politika Nesneleri (GPO'lar), oturum açma betikleri ve etki alanı denetleyicilerinin sorunsuz çalışması için gerekli diğer kaynaklar dahil olmak üzere temel dosyaları depolayan bir paylaşılan dizin olarak görev yapar. Alan genelinde yapılandırmalara merkezi bir depo sağlayarak AD ortamındaki ayarlar konusunda birliği destekler.

Çoğaltma açısından, SYSVOL'ün önemi daha da belirgin hale gelir. SYSVOL ile ilişkilendirilmiş çoğaltma mekanizmaları, içeriğin tüm etki alanı denetleyicileri arasında tutarlılığını sağlar. Bu birliktelik, politikaların güvenilir bir şekilde uygulanması ve oturum açma betiklerinin yürütülmesi için belirli bir etki alanı denetleyicisiyle etkileşime geçen kullanıcılara ve bilgisayarlara standart bir deneyim sunar.

SYSVOL replikasyonu, AD altyapısının hata toleransı ve yedekliliğine katkı sağlar. Eğer bir etki alanı denetleyicisi başarısız olursa, SYSVOL replikasyonu, alternatif denetleyicilerin paylaşılan dizinin güncel kopyalarını bulundurmalarını sağlar, böylece kesintileri en aza indirir ve hizmet sürekliliğini sürdürür.

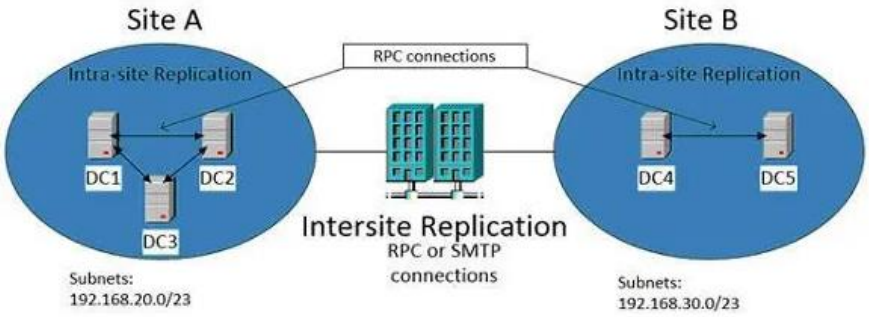
GPO'ların veya oturum açma betiklerinin üzerinde yapılan değişiklikler, SYSVOL replikasyonu aracılığıyla etkili bir şekilde yayılır, değişikliklerin hızlı bir şekilde dağıtılmasını sağlar. Bu, tüm etki alanının en son yapılandırmaları hızlı bir şekilde yansıtmasını sağlayarak, organizasyonel gereksinimlere hızlı bir şekilde uyum sağlar.

Ayrıca, SYSVOL'ün rolü, etki alanı genelinde iletişimi teşvik etmeye yöneliktir. Tüm etki alanı denetleyicilerinin aynı kritik dosyalara ve politikalara erişim sağlanmasıyla SYSVOL, AD ortamında uyumu ve entegrasyonu kolaylaştırır. Bu paylaşılan temel, etki alanı genelinde tutarlı işlemleri mümkün kılarak, bütünleşik ve birbirine bağlı bir ağın oluşturulmasına olanak tanır.

Özetle, SYSVOL, kritik dosyalar ve yapılandırmalar için bir depo olarak görev yaparak Active Directory'nin sorunsuz çalışmasına integraldir. Replikasyon içindeki rolü hayati önem taşır, içerik tutarlılığını, hata toleransını ve değişikliklerin etkili bir şekilde dağıtılmasını sağlayarak AD ortamının güvenilirliğine ve birliğine katkıda bulunur.

5. What is the process of Active Directory replication, and how does it ensure consistency among domain controllers?

The diagram below shows a typical **two-site Active Directory environment** with some of the replication components.



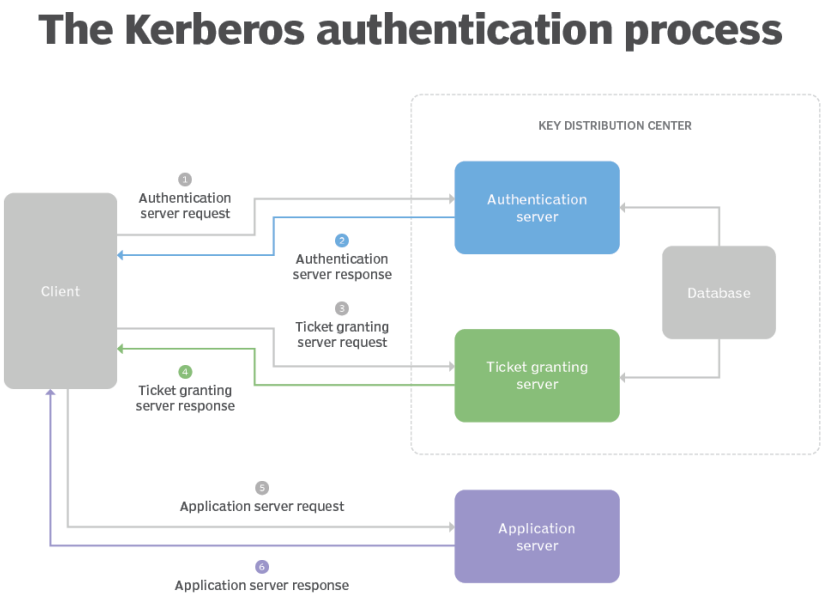
Active Directory replikasyonu, kullanıcılar, gruplar ve politikalar gibi dizin nesnelerine yapılan değişikliklerin bir ağdaki tüm etki alanı denetleyicilerine yayılma sürecidir. Bu, tüm denetleyicilerin tutarlı ve güncel bilgiye sahip olmasını sağlayarak birleştirilmiş ve güvenilir bir dizin hizmetini teşvik eder.
Replikasyon süreci, bir etki alanı denetleyicisinde bir nesnenin oluşturulması veya değiştirilmesiyle başlar. Bu, kullanıcı hesapları, grup üyelikleri veya Grup Politika Nesneleri (GPO'lar) üzerindeki değişiklikleri içerebilir. Bir değişiklik meydana geldiğinde, Bilgi Uygunluk Denetleyicisi (KCC), değişikliğin ağ üzerinde nasıl yayılacağını belirleyen bir replikasyon topolojisi oluşturur.
Replikasyon, iki temel türde gerçekleşir: etki alanı içi replikasyon ve etki alanları arası replikasyon.
Etki Alanı İçi Replikasyon: Bir site içinde, etki alanı denetleyicileri doğrudan birbirleriyle iletişim kurar. Değişiklikler genellikle her 15 saniyede bir replike edilir, bu da güncellemelerin hızlı bir şekilde yayılmasını sağlar. Bu sık iletişim, aynı site içinde tutarlılığı sürdürmeye yardımcı olur.

Etki Alanları Arası Replikasyon: Siteler arasında, replikasyon potansiyel bant genişliği sınırlamaları nedeniyle daha az sıklıkta gerçekleşir. Replikasyon programı varsayılan olarak genellikle her üç saatte bir gerçekleşir. Bu, uzak siteler arasında gereksiz trafiği önlerken değişikliklerin nihayetinde yayılmasını sağlar.
Tutarlılığı daha da sağlamak için Active Directory, çoklu ana replikasyon modelini kullanır. Bu, herhangi bir etki alanı denetleyicisinin güncellemeleri kabul edebileceği ve bu güncellemelerin daha sonra diğer denetleyicilere yayılabileceği anlamına gelir. Bu tasarım, hata toleransını artırır ve değişikliklerin herhangi bir etki alanı denetleyicisinde yapılmasına izin vererek esneklik ve ölçeklenebilirlik sağlar.
Ayrıca, Güncelleme Sıra Numarası (USN), değişiklikleri izlemek için kullanılır. Her etki alanı denetleyicisi, her nesne üzerinde bir USN tutar ve bu, hangi değişiklikleri replike etmesi gerektiğini belirlemesine yardımcı olur. Bu, yalnızca gerekli değişiklikleri verimli bir şekilde ileterek gereksiz ağ trafiğini azaltmaya yardımcı olur.
Özetle, Active Directory replikasyon süreci, dizin nesnelerine yapılan değişikliklerin etki alanı denetleyicileri arasında etkili bir şekilde yayılmasını içerir. Etki alanı içi ve etki alanları arası replikasyon aracılığıyla sistem, tüm denetleyicilerin tutarlı ve güncel bilgiye sahip olmasını sağlar, ağda güvenilir ve birleştirilmiş bir dizin hizmetini destekler.

6. In Active Directory, what purpose do trusts serve, and how are secure connections established between domains?

Active Directory'de güven ilişkileri, farklı alanlar arasında ilişkiler kurmanın amacını taşır. Bu ilişkiler, kullanıcıların bir alan içindeki kaynaklara erişmesini sağlamak üzere kimlik doğrulama ve yetkilendirme bilgilerini paylaşma olanağı tanır. Güven ilişkileri, çoklu alan veya çoklu ormanlı AD altyapılarında birleşik ve işbirliğine dayalı bir ağ ortamı oluşturmak için önemlidir.
Farklı alanlar arasında güvenli bağlantılar kurmak için Active Directory, bir güven ilişkisi kullanır. Bu ilişki, güvenen ve güvenilen alanlar arasındaki kimlik doğrulama isteklerinin akış yönünü ve güven seviyesini tanımlar. Güven ilişkileri tek yönlü veya çift yönlü olabilir ve geçişli veya geçişsiz olabilir, bu da güven ilişkisinin kapsamını ve derinliğini etkiler.
Farklı alanlar arasında güvenli bağlantılar genellikle şifreleme ve güvenli protokoller kullanılarak kurulur. Bir alanın kullanıcıları veya hizmetleri, başka bir alanın kaynaklarına erişmeye çalıştığında, kimlik doğrulama istekleri Kerberos gibi protokoller kullanılarak güvenli bir şekilde alanlar arasında iletilir. Güven ilişkisi, kimlik doğrulama sürecinin güvenilir ve güvenli bir şekilde gerçekleşmesini sağlar.
Daha karmaşık senaryolarda, birden fazla alan veya ormanın dahil olduğu durumlarda, yöneticilerin doğru erişim kontrolü ve güvenliği sağlamak için güven ilişkilerini dikkatlice planlaması ve yapılandırması gereklidir. Güven ilişkileri, farklı alanlar arasında kullanıcı erişimini düzenleme ve genel Active Directory ortamının güvenliğini koruma konusunda kritik bir rol oynar.

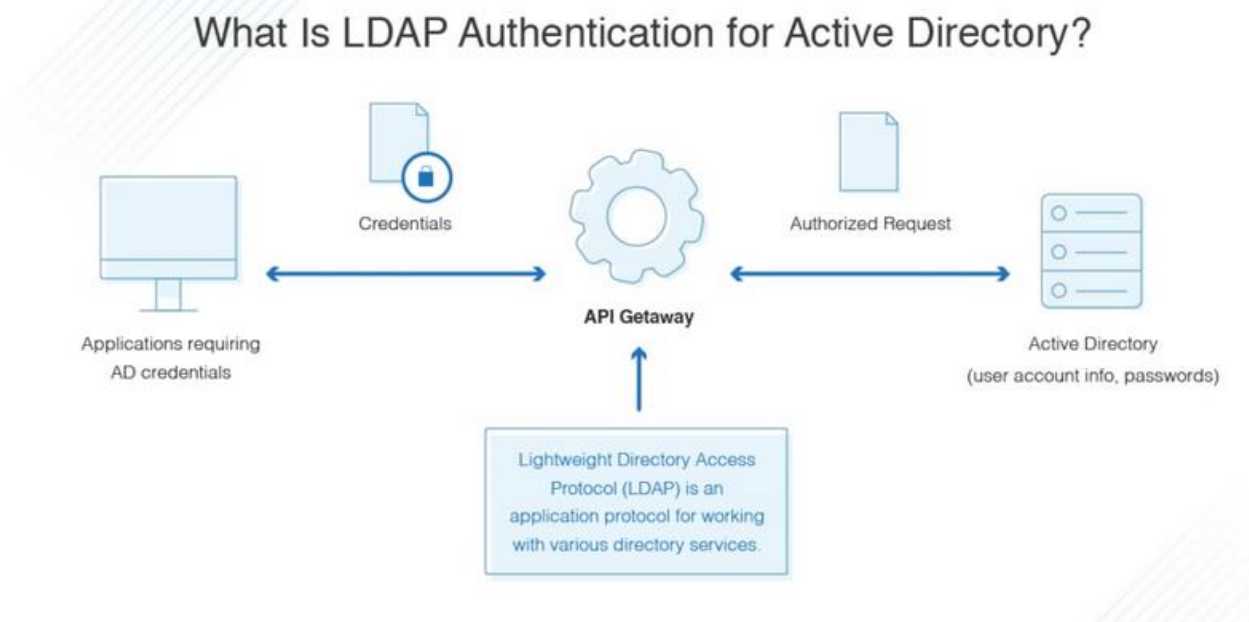
7. Provide an overview of how Kerberos authentication works in an Active Directory environment.



Kerberos kimlik doğrulama protokolü, bir Active Directory ortamında şu şekilde çalışır:
Kerberos, ağdaki varlıkların kimliklerini güvenli bir şekilde kanıtlamalarına olanak tanıyan bir ağ kimlik doğrulama protokolüdür. Active Directory bağlamında, Kerberos varsayılan kimlik doğrulama protokolüdür.
Bir kullanıcı bir bilgisayara giriş yapmaya veya bir ağ kaynağına erişmeye çalıştığında, Kerberos kimlik doğrulama süreci başlar. Kullanıcının bilgisayarı, istemci olarak bilinen, Key Distribution Center'ın (KDC) bir parçası olan, Active Directory tarafından bir bilet talep eder.
KDC, kullanıcının kimlik bilgilerini doğruladıktan sonra istemciye Bir Kullanım Biletini (TGT) verir. Bu TGT, kullanıcının kimliğini alan içinde (alan) ispatlayan bir belge görevi görür.
Kullanıcı belirli bir kaynağa, örneğin bir dosya sunucusuna, erişmek istediğinde, istemci TGT'yi KDC'deki Ticket Granting Service (TGS) 'ye sunar. Karşılığında, TGS, istenen kaynak için bir Servis Bileti sağlar.
İstemci, Servis Biletini kaynak sunucusuna (örneğin, dosya sunucusuna) erişim talebiyle birlikte gönderir. Kaynak sunucusu, Service Ticket'ı KDC ile paylaştığı gizli anahtarı kullanarak doğrular.
Eğer Service Ticket geçerli ise, kaynak sunucusu istenen kaynağa erişimi sağlar. Tüm kimlik doğrulama süreci, karşılıklı kimlik doğrulamaya dayanarak, istemci ve kaynak sunucunun birbirlerinin kimliğini doğrulamalarını sağlar.
Kerberos kimlik doğrulama sürecinde önemli noktalar arasında zaman damgalarının ve oturum anahtarlarının kullanımı güvenliği arttırmaktadır. Zaman damgaları, yeniden oynatma saldırılarını önlemeye yardımcı olurken, oturum anahtarları, istemci ve kaynak sunucunun kullanıcının şifresini ortaya çıkarmadan güvenli bir şekilde iletişim kurmalarını sağlar.

Özetle, Active Directory ortamında Kerberos kimlik doğrulama, Key Distribution Center tarafından biletlerin verilmesi ve doğrulanması üzerine kuruludur, bu da ağ kaynaklarına güvenli iletişimi ve erişimi kolaylaştırırken hassas kimlik bilgilerinin açığa çıkma riskini en aza indirir.

8. What is Lightweight Directory Access Protocol (LDAP)?



Lightweight Directory Access Protocol (LDAP), dizin bilgi hizmetlerine erişim ve yönetim için kullanılan standartlaştırılmış bir iletişim protokolüdür. TCP/IP stack üzerinde çalışan hafif, open source bir protokoldür.
LDAP özellikle dizin hizmetlerini sorgulama ve değiştirme amacıyla tasarlanmıştır. Bu hizmetler genellikle kullanıcılar, gruplar, cihazlar ve diğer nesneler gibi ağ kaynakları hakkında bilgi içerir. Bu dizin hizmetleri arasında Active Directory, OpenLDAP ve diğerleri bulunabilir.
LDAP, LDAP istemcileri ile sunucular arasındaki iletişim için bir dizi kural tanımlar. İstemciler, sunucuya taleplerde bulunur ve sunucu, istenen bilgiyi yanıtlar veya belirtilen işlemi gerçekleştirir. LDAP, bilgiyi benzersiz bir Distinguished Name (DN) tarafından tanımlanan girişlere hiyerarşik bir veri modeli üzerine kurar.
Yaygın LDAP işlemleri arasında belirli kriterlere dayalı olarak dizin girişlerini arama, yeni girişler ekleme, mevcut girişleri değiştirme ve girişleri silme bulunur. LDAP, basit ve etkili bir sorgu dilini kullanarak arama kriterlerini ifade etmek için kullanır, bu da istemcilerin dizinden belirli bilgileri almasını sağlar.
LDAP, istemcilerin dizin işlemleri gerçekleştirmek için LDAP sunucularına bağlandığı bir istemci-sunucu modelinde çalışır. Ağ ortamlarında merkezi kimlik doğrulama ve yetkilendirme için yaygın olarak kullanılır. Uygulamalar ve hizmetler, çeşitli platformlarda ve sistemlerde dizin bilgilerine erişim ve yönetim için LDAP'ı kullanabilir, böylece dizin hizmetlerine yönelik birleşik ve ölçeklenebilir bir yaklaşım sağlanır.

9. Explain the characteristics of group objects in Active Directory and highlight the differences between "Domain Admins" and "Enterprise Admins."

Active Directory'deki grup nesneleri, işlevselliğini ve amacını tanımlayan ortak özelliklere sahiptir. Gruplar, dizin içindeki kullanıcıları, bilgisayarları ve diğer nesneleri düzenlemek ve yönetmek için kullanılır. İlgili varlıkları bir araya getirerek erişim kontrolünü, izin atama işlemlerini ve politika uygulamayı basitleştirirler.
Active Directory'de "Domain Admins" ve "Enterprise Admins" olmak üzere iki farklı türde grup bulunmaktadır ve bunlar farklı roller ve kapsama sahiptir.

Domain Admins:

- "Domain Admins", etki alanı düzeyinde yönetici yetkilerine sahip bir gruptur.
- "Domain Admins" grubunun üyeleri, belirli bir etki alanındaki kaynaklar üzerinde geniş kontrol sahibidir.
- Etki alanı içinde kullanıcıları, bilgisayarları ve grupları ekleyebilir veya kaldırabilir, aynı zamanda etki alanı genelinde ayarları değiştirebilirler.
- "Domain Admins", Grup Politika Nesnelerini (GPO'lar) yönetme yetkisine sahiptir ve etki alanını etkileyen değişiklikler yapabilir.
- Bu grup, temel olarak bir etki alanındaki yönetim üzerine odaklanır ve yetkilerini orman içindeki diğer etki alanlarına genişletmez.

Enterprise Admins:

- "Enterprise Admins", orman düzeyinde yönetici yetkilerine sahip bir gruptur.
- "Enterprise Admins" grubunun üyeleri, Active Directory ormanındaki tüm etki alanlarında yükseltilmiş haklara sahiptir.
- Domainler arasındaki güven ilişkilerini yönetebilir, orman genelinde değişiklikler yapabilir ve ormandan etki alanı ekleyip çıkarabilirler.
- "Enterprise Admins", en yüksek düzeyde yönetici yetkisine sahiptir ve tüm Active Directory ormanını denetleme sorumluluğuna sahiptir.
- "Enterprise Admins" grubunun üyeleri tarafından yapılan değişiklikler, tüm ormanı etkiler ve bu nedenle çoklu etki alanlı ortamlarda kritik bir role sahiptir.

Özetle, "Domain Admins" ve "Enterprise Admins" grupları, her ikisi de yönetici rollerine sahip olmalarına rağmen "Domain Admins" bir tek etki alanına odaklanırken, "Enterprise Admins" orman düzeyinde çalışır ve birden fazla etki alanını kapsar.

10. What is the function of Access Control Lists (ACLs) in Active Directory, and how are permissions controlled for resources?

Active Directory'deki Erişim Kontrol Listeleri (ACL'ler), dizin içindeki kaynaklar için izinleri düzenleme ve yönetme görevini üstlenir. Bu listeler, belirli nesnelere kimin erişebileceğini, hangi işlemleri gerçekleştirebileceğini ve hangi koşullar altında bu erişimi sağlayabileceğini tanımlar.

ACL'ler, kullanıcılar, gruplar, organizasyon birimleri ve bilgisayar hesapları gibi çeşitli dizin nesnelerine uygulanır. Bu listeler, dosyalar, klasörler, yazıcılar ve diğer dizinle ilgili öğeler gibi kaynaklara sahip olan her varlığın ne kadar erişime sahip olacağını belirler.

ACL'ler içindeki izinler, belirli hakların varlıklara atanmasıyla kontrol edilir. Bu haklar arasında okuma, yazma, değiştirme, silme ve daha fazlası bulunur ve bir kullanıcının veya grubun belirli bir kaynak üzerinde gerçekleştirebileceği işlemleri belirler. Örneğin, bir kullanıcının bir dosyayı okuma hakkı olabilir, ancak değiştirme veya silme hakkına sahip olmayabilir.

Active Directory'de, izinler varsayılan olarak miras alınır, yani bir hiyerarşideki nesneler, ebeveyn nesnelerine atanan izinleri miras alırlar. Bununla birlikte, yöneticiler, izinleri özelleştirmek için hiyerarşinin farklı seviyelerinde açıkça tanımlayabilirler.

Ayrıca, güvenlik grupları, izinleri kontrol etmede önemli bir rol oynar. Kullanıcılar genellikle güvenlik gruplarına eklenir ve bu gruplara belirli izinler atanır. Bu, izinleri bireysel kullanıcılar yerine gruplarla ilişkilendirerek izin yönetimini basitleştirir.

ACL'ler aracılığıyla, yöneticiler, kullanıcıların ve grupların gerekli görevleri gerçekleştirmek için gerekli izinlere sahip olduğundan emin olacak şekilde ayrıntılı ve hassas bir erişim yönetimi uygulayabilirler; aynı zamanda Active Directory ortamında güvenliği ve uyumluluğu sürdürebilirler.