ChatGPT

Ubuntu Tabanlı Açık Kaynak Kurumsal Mimari: Bulut Bağımlılığına Karşı Veri Egemenliği Yaklaşımı

Giriş

Günümüzde kurumlar dijital dönüşümle birlikte artan veri hacimlerini yönetmek için sıklıkla bulut bilişim hizmetlerine yönelmektedir. Ancak kritik verilerin Amazon, Microsoft, Google gibi küresel bulut sağlayıcılarında barındırılması, **veri egemenliği** konusunda endişeler doğurmaktadır. Buluta yüksek bağımlılık, kurumların verileri üzerindeki tam kontrolü kaybetme, yabancı yasal düzenlemelere ve erişim taleplerine maruz kalma ve tek bir tedarikçiye mahkûm olma (vendor lock-in) risklerini beraberinde getirir [1]. Bu nedenle son yıllarda veri egemenliği kavramı öne çıkmış; kurumlar kritik verilerini kendi altyapılarında tutarak ve **açık kaynaklı** çözümlere yönelerek bulut bağımlılığını azaltmayı hedeflemektedir [2]. Açık kaynak ekosistemi, ücretsiz lisanslama ve şeffaflık avantajlarıyla hem maliyetleri düşürmekte hem de güvenlik ve uyumluluk üzerinde daha fazla kontrol sağlamaktadır [3].

Bu proje işte bu yaklaşımla, bulut sağlayıcılara bağımlılığı azaltmak ve verinin tam kontrolünü kuruma geri kazandırmak amacıyla, tamamen açık kaynak teknolojilere dayalı bir **kurumsal bilişim mimarisi** tasarlamayı önermektedir [4]. Önerilen mimari, bulut hizmetlerinin esneklik ve işlevselliğini kurum içi bir çözüme taşırken, verinin nerede saklandığı ve kimlerin erişebildiği üzerinde tam egemenlik kurulmasına olanak tanıyacaktır.

Projenin Amacı

Projenin temel amacı, **Ubuntu** işletim sistemi ve ilgili açık kaynak yazılımlar üzerine inşa edilmiş entegre bir kurumsal BT altyapısı geliştirmektir. Böylece kurumlar verilerini kendi kontrolü altında tutabilecek, Microsoft Azure gibi kapalı bulut platformlarına bağımlılığı azaltabilecek ve veri egemenliğini artırabileceklerdir [5]. Önerilen çözüm; kimlik ve erişim yönetiminden e-posta ve işbirliği araçlarına, izleme ve güvenlik bileşenlerinden otomasyon ve altyapı koduna (Infrastructure as Code) kadar geniş bir yelpazedeki hizmeti açık kaynak alternatifleriyle karşılamayı hedeflemektedir [6]. Bu sayede kurum içi bir "bulut-benzeri" mimari oluşturularak teknik gereksinimler karşılansa dahi verinin konumu ve erişimi konularında tam kontrol sağlanacaktır [7]. Projenin amacı sadece teknik bir sistem kurmak değil; aynı zamanda bu yaklaşımın toplam sahip olma maliyeti (TCO), güvenlik seviyesi, kullanılabilirlik ve kullanıcı deneyimi açılarından geleneksel bulut/kapalı kaynak çözümlere kıyasla sağladığı avantaj ve dezavantajları ortaya koymaktır [8]. Bu kapsamda, önerilecek mimari ile kurumların **lisans maliyetlerini düşürmesi**, **veri güvenliğini artırması** ve **esneklik kazanması** beklenmektedir.

Kapsam ve Hedefler

Proje Kapsamı: Bu proje, orta ölçekli bir kurumsal BT altyapısının tüm temel servislerinin açık kaynak yazılımlar kullanılarak karşılanmasını öngörmektedir [9]. Sistem mimarisi, istemci cihazlardan sunucu hizmetlerine kadar uçtan uca Ubuntu tabanlı olarak tasarlanacaktır. Örneğin, istemci bilgisayarlarda kullanıcı tercihlerine bağlı olarak Ubuntu türevi **Linux Mint** veya **Zorin OS** gibi kullanıcı dostu masaüstü sistemler kullanılacak; sunucu tarafında ise Ubuntu Server üzerine konteyner tabanlı mimaride kimlik

doğrulama, dizin hizmeti, e-posta sunucusu, güvenlik izleme, dosya paylaşımı gibi servisler konumlandırılacaktır [10]. Donanım boyutlandırması kurumun ihtiyacına göre belirleneceğinden, üç fiziksel sunucu ile oluşturulacak Kubernetes kümesinin işlemci, bellek, disk gibi özellikleri bu raporda sabit olarak tanımlanmamıştır. Ancak genel olarak, yüksek erişilebilirlik için en az üç düğümlü (node) bir Kubernetes kümesi öngörülmekte ve konteyner altyapısını verimli çalıştıracak güncel sunucu donanımları varsayılmaktadır.

Somut Hedefler: Proje kapsamında hayata geçirilmesi planlanan başlıca bileşen ve entegrasyonlar şunlardır:

- **Kimlik yönetimi ve erişim denetimi (IAM):** Kurumsal ağ ortamında merkezi bir kimlik ve erişim yönetimi sistemi olarak **Authentik** kurulacaktır. Authentik, açık kaynak kodlu bir **Identity Provider (IdP)** olup kullanıcı kimlik doğrulaması, tek oturum açma (SSO) ve erişim kontrollerinin kurum içinde barındırılmasını sağlar [11]. Authentik, SAML2, OAuth2, OpenID Connect ve LDAP gibi endüstri standardı protokolleri desteklediği için mevcut dizin ve uygulamalarla kolayca entegre edilebilir [12]. Bu projede Authentik, kullanıcı veritabanı olarak **Samba 4 Active Directory** ile entegre çalışacak şekilde konumlandırılacaktır. Samba 4, Active Directory ile uyumlu açık kaynak bir dizin hizmeti sunar ve merkezi "gerçeklik kaynağı (source of truth)" olarak tüm kullanıcı hesaplarını ve kimlik bilgilerinin depolanmasını sağlar. Samba, bir Active Directory etki alan denetleyicisi olarak kurularak, hem Windows istemcilerinin domaine katılımı ve dosya/paylaşım erişimini yönetebilecek, hem de LDAP/Kerberos altyapısı sayesinde diğer uygulamalar için tek bir kimlik kaynağı görevi görecektir [13]. Authentik ise Samba AD üzerinde bulunan kullanıcı hesaplarını **LDAP senkronizasyonu** ile kaynaktan içe aktaracak ve bu hesaplar üzerinden SSO oturumları yönetilecektir [14] [15]. Bu sayede Authentik, uygulamalar için modern SSO ve çok faktörlü kimlik doğrulama (MFA) imkânı sunarken, kullanıcı hesaplarının tek merkezden (Samba AD) yönetilmesi sağlanacaktır. Sonuç olarak tüm kullanıcılar kurumdaki uygulamalara **tek bir hesaptan** (kurumsal AD hesabı) giriş yapabilecek; web tabanlı servislerde Authentik üzerinden SSO ile oturum açarken, ek güvenlik için çok faktörlü doğrulama adımları uygulanacaktır [16]. (Örneğin, kullanıcı Zimbra web istemcisine erişirken Authentik entegrasyonu sayesinde önce Authentik üzerinden AD kimlik bilgileri ve MFA ile doğrulanacak, ardından Zimbra'ya tek oturum açma ile yönlendirilecektir.)

- **Dizin hizmetleri ve entegrasyon:** Kimlik yönetiminin temelini oluşturan dizin servisi olarak **Samba 4 Active Directory Domain Controller** kurulacaktır. Samba 4, Microsoft Active Directory ile işlevsel eşdeğerlik sunan açık kaynak bir çözümdür. Bu sayede kullanıcı ve grup bilgileri, bilgisayar nesneleri ve kimlik doğrulama verileri Active Directory şemasında tutulacak, kurum içi uygulamalar bu merkezi dizin üzerinden doğrulama yapacaktır. Samba AD, LDAP ve Kerberos desteğiyle hem Linux hem Windows istemcilerinin merkezi doğrulamasına imkan tanır. Özellikle Zimbra e-posta sunucusu ve Authentik gibi servisler, Samba AD'yi harici LDAP/AD kaynağı olarak kullanarak kullanıcı kimlik doğrulamasını gerçekleştirecektir. Samba AD'nin **Kerberos** altyapısı, tek oturum açma mekanizmalarının da temelini oluşturarak farklı servisler arasında güvenli bir kimlik biletlemesi sağlar. Böylece kurum içerisindeki tüm servisler için **tek bir kullanıcı dizini** ve oturum açma altyapısı tesis edilecektir. (Samba AD, birincil dizin olduğundan, gerektiğinde Windows sistemler de bu domaine üye yapılarak ortak kimlik doğrulama sağlanabilir. İstemci tarafında her ne kadar Linux dağıtımları kullanılsa da Samba AD, gelecekte Windows istemci entegrasyonunu veya dosya/paylaşım hizmetlerini yönetmek açısından esneklik sunacaktır.)

- **E-posta ve işbirliği altyapısı:** Kurum içi e-posta hizmeti olarak **Zimbra Collaboration Suite (Open Source Edition)** kurulacaktır. Zimbra, Linux tabanlı açık kaynak bir grup çalışma sunucusudur ve birleşik e-posta, takvim, rehber ve dosya paylaşımı hizmetleri sunar [17]. Bu yönüyle Microsoft Exchange/Office 365 gibi ticari çözümlere maliyetsiz bir alternatif

sağlamaktadır [18]. Zimbra'nın web tabanlı arayüzü ve AJAX destekli istemcisi sayesinde kullanıcılara zengin bir e-posta deneyimi sunulacaktır. Kurulum sonrasında Zimbra, kullanıcı kimlik doğrulaması için Samba AD ile entegre edilecektir. Zimbra sunucusu, **harici Active Directory kimlik doğrulaması** modunda yapılandırılarak, kullanıcıların Zimbra hesapları için Samba AD üzerindeki kimlik bilgileriyle oturum açması sağlanacaktır [19]. Bu entegrasyon sayesinde e-posta kullanıcı hesapları ve parolaları tek merkezden (AD) yönetilecek, Zimbra üzerinde ayrı bir kullanıcı yönetimine gerek kalmayacaktır. Gerekli dizin bağlantısı kurulduktan sonra, Zimbra'ya yeni kullanıcı tanımlamaları da AD'deki hesaplarla senkronize yapılabilir. Özetle, kullanıcılara kurumsal e-posta, takvim ve kişi listesi hizmetleri Zimbra üzerinden sunulurken, güvenli kimlik doğrulama altyapısı AD/Authentik ile desteklenecektir. Bu çözüm ile kurum içinde **Exchange seviyesinde** bir e-posta ve işbirliği deneyimi, tamamen açık kaynak bileşenlerle elde edilmiş olacaktır [20].

- **İstemci işletim sistemi dönüşümü:** Son kullanıcı bilgisayarlarında mevcutta Windows kullanılıyorsa, bunların **Ubuntu tabanlı Linux dağıtımlarına** geçişi değerlendirilecektir. Özellikle **Linux Mint** veya **Zorin OS** gibi Ubuntu LTS tabanlı ve kullanıcı dostu arayüzlere sahip dağıtımlar tercih edilecektir [21] [22]. Linux Mint, kullanım kolaylığı ve zengin yazılım desteğiyle bilinen popüler bir masaüstü Linux dağıtımıdır; özellikle Windows veya Mac arayüzlerine aşina kullanıcılar için tanıdık bir deneyim sunacak şekilde tasarlanmıştır [23]. Zorin OS ise görsel olarak Windows arayüzüne benzerliği ve modern, temiz tasarımıyla öne çıkan bir başka Ubuntu-tabanlı dağıtımdır; Windows'tan Linux'a geçiş yapan kullanıcılar için mümkün olduğunca düşük öğrenme eğrisi sağlamayı amaçlamaktadır [24] [25]. Proje kapsamında pilot kullanıcı gruplarıyla bu geçişin **uygulanabilirliği test edilecek**, ortaya çıkabilecek uyumluluk sorunları, son kullanıcı eğitim ihtiyaçları ve günlük iş akışına etkileri analiz edilecektir [22]. Amaç, masaüstü tarafında da lisans maliyetini ortadan kaldırmak ve kurum geneline açık kaynak kullanımını yaygınlaştırmaktır. İstemci sistemler, ofis uygulamaları, tarayıcı, e-posta istemcisi vb. günlük ihtiyaçlar için gerekli tüm yazılımlarla hazır hale getirilecek; mümkün olduğunca Windows üzerindeki kullanıcı deneyimine yakın bir ortam sağlanacaktır (örneğin, Zorin OS varsayılan arayüzü Windows 11 benzeri bir menü ve görev çubuğu sunarak geçiş yapan kullanıcıların **kendini yabancı hissetmemesini** hedefler [26]).

- **Siber güvenlik, log yönetimi ve izleme:** Kurum ağı ve sistemleri için güvenlik izleme ve kayıt yönetimi açık kaynak araçlarla entegre şekilde kurulacaktır. Sunucu ve istemci sistemlere **Wazuh ajanları** yüklenecek ve merkezi bir Wazuh sunucusu üzerinden tüm log kayıtları toplanıp korele edilecektir. **Wazuh**, birleşik bir açık kaynak XDR/SIEM platformudur ve uç nokta izleme, güvenlik açığı tespiti, log analizi ve gerçek zamanlı alarm üretimi gibi yetenekler sunar [27]. Wazuh ajanları, her sunucu/istemci üzerinde sistem olaylarını, kimlik doğrulama kayıtlarını, dosya bütünlüğü değişimlerini vb. izleyerek Wazuh sunucusuna iletir; Wazuh sunucusu da bu verileri analiz ederek olası güvenlik ihlallerine karşı uyarılar oluşturur. Bu sayede kurumun altyapısı için **merkezi bir log yönetimi ve saldırı tespit sistemi (SIEM)** devreye alınmış olacaktır. Bunun yanında, periyodik zafiyet taramaları için **OpenVAS** kullanılması planlanmıştır. OpenVAS (Greenbone Vulnerability Manager), ağ ve sistem zafiyetlerini tarayan açık kaynak bir güvenlik aracıdır; düzenli aralıklarla çalıştırılarak sunucuların ve ağ cihazlarının bilinen zaafiyetlere karşı taranması sağlanacak, elde edilen raporlar doğrultusunda güvenlik yamaları uygulanacaktır [28]. Ayrıca sistem performansı ve çalışma sürekliliğinin izlenmesi için Kubernetes ortamına entegre **Prometheus** ve **Grafana** gibi araçlar kullanılacaktır. Prometheus, konteynerlerin ve sunucuların CPU, bellek, disk kullanımı, servis yanıt süreleri gibi metriklerini toplayıp zaman serisi veritabanında saklayacak; Grafana ile bu metrikler görselleştirilerek **dashboard**'lar oluşturulacaktır. Kritik hizmetler için eşik değer aşımları belirlenecek ve **alarm mekanizmaları** (e-posta ya da SMS bildirimleri) yapılandırılacaktır [29]. Böylece altyapının sadece güvenliği değil, performansı ve sağlığı da proaktif olarak izlenip yönetilebilecektir.

Yukarıda özetlenen hedeflere ek olarak, altyapının **yedeklilik** ve **felaket kurtarma** kabiliyetleri de planlama dahilindedir. Bu bağlamda, sunucu tarafındaki kritik verilerin (örneğin Zimbra e-posta veritabanı, Samba AD dizin verisi, Kubernetes vb.) düzenli yedeklenmesi sağlanacaktır. Yedekleme için kurum içinde konumlandırılacak yüksek kapasiteli bir **NAS cihazı** (örneğin QNAP) kullanılabilir. QNAP gibi çözümler anlık görüntü (snapshot) alma, versiyonlu yedek saklama ve hızlı geri yükleme imkânlarıyla veri kayıplarına karşı kurumsal koruma sağlar [30]. Yedekleme stratejisi olarak 3-2-1 kuralı (3 kopya, 2 farklı ortam, 1 off-site) göz önünde bulundurularak, NAS üzerindeki yedeklerin kritik durumlar için ikinci bir harici diske veya buluta replikasyonu değerlendirilecektir. Sonuçta, olası bir donanım arızası, veri silinmesi veya fidye yazılımı saldırısı durumunda, sistemlerin hızlıca eski haline döndürülebilmesi için bir **felaket kurtarma planı** oluşturulacaktır.

Ağ güvenliği katmanında ise kurum ağı ile dış dünya arasına konumlandırılacak bir **güvenlik duvarı** (firewall) cihazı, ilk savunma hattını oluşturacaktır. Fiziksel olarak ayrı bir güvenlik duvarı cihazı (mevcut bir kurumsal firewall appliance veya açık kaynak bir pfSense/OPNsense çözümü donanım üzerinde kurulabilir) tüm kuzey-güney trafiği denetleyecektir. Güvenlik duvarı, kritik servis portlarını (örneğin Zimbra için SMTP/IMAP/HTTPS, Authentik için HTTPS, VPN varsa ilgili portlar) dış erişime kontrollü bir şekilde açarken, izinsiz erişim teşebbüslerini ve saldırı girişimlerini engelleyecektir. Güvenlik duvarı aynı zamanda iç ağ segmentasyonu yaparak sunucu kümesiyle istemci ağı arasındaki trafiği de filtreleyebilir. Bu sayede kurum ağı, dış tehditlere karşı çevre korumasına sahip olacak ve zararlı/istenmeyen trafiğin içerideki sistemlere ulaşması büyük ölçüde önlenecektir. Unutulmamalıdır ki **perimetre güvenlik duvarları**, dış tehditlere karşı iç ağı koruyan ilk savunma katmanıdır ve yetkisiz erişimleri engelleyerek veri ihlali riskini en aza indirir [31]. İlaveten, her sunucuda temel güvenlik duvarı kuralları (Ubuntu'nun UFW veya iptables ile) uygulanarak yalnızca gerekli servislerin ilgili konteyner portlarına erişimine izin verilecektir. Böylece savunma derinlemesine (defense-in-depth) prensibiyle hem konteyner seviyesinde, hem sunucu seviyesinde, hem de ağ sınırında çok katmanlı bir güvenlik sağlanacaktır.

Teknolojik Bileşenler ve Özellikleri

Bu bölümde projede kullanılan başlıca açık kaynak araçlar ve teknolojiler kısaca tanıtılmakta, seçilme nedenleri teknik özellikleriyle açıklanmaktadır:

Kubernetes ve Rancher ile Konteyner Mimari

Sunucu tarafı altyapımız **Kubernetes** üzerinde çalışan konteyner tabanlı servisler olarak planlanmıştır. Kubernetes, konteynerleşmiş uygulamaları birden çok sunucu üzerinde otomatik olarak dağıtan ve yöneten, endüstri standardı bir **orkestrasyon platformudur** [32]. Kubernetes'in temel özellikleri arasında uygulamaların kolay ölçeklenebilmesi, yük dengeleme, konteynerler arası servis keşfi, otomatik yeniden başlatma ve kendi kendini iyileştirme mekanizmaları bulunmaktadır [33]. Örneğin Kubernetes, bir uygulamaya ait konteyner sayısını tanımlı duruma getirmek için otomatik ölçeklendirme yapabilir, düğümler arası konteyner dağılımını optimize ederek donanım kaynaklarının verimli kullanılmasını sağlar [34]. Herhangi bir konteyner (pod) arızalandığında Kubernetes bunu tespit edip yeniden başlatarak sistemin kesintisiz çalışmasını temin eder; bu **self-healing** özelliği sayesinde insan müdahalesine gerek kalmadan servis sürekliliği sağlanır [35]. Tüm bu özellikler, kurumsal uygulamalar için yüksek erişilebilirlik ve dayanıklılık sunarak altyapının güvenilirliğini artırır.

Kubernetes tek başına güçlü bir platform olmakla birlikte, yönetimi karmaşık olabilmektedir. Bu projede Kubernetes cluster yönetimini kolaylaştırmak ve bir merkezi arabirim sağlamak amacıyla **Rancher** kullanılacaktır. Rancher, açık kaynak bir konteyner yönetim paneli olup bir veya birden fazla Kubernetes kümesini tek bir arayüzden yönetmeye olanak tanır. Rancher sayesinde kümenin kurulumu, node ekleme/çıkarma, Kubernetes sürüm yükseltmeleri, rol tabanlı erişim kontrolü (RBAC) ve izleme gibi

işlemler oldukça sadeleşir. Örneğin Rancher, yeni bir Kubernetes kümesi oluşturmayı veya var olan bir kümeyi içe aktarmayı grafik arayüz üzerinden mümkün kılar; birden fazla kümeyi tek ekrandan izleme ve yönetme imkânı tanır [36]. Ayrıca katalog üzerinden **helm chart** veya uygulama şablonlarıyla Prometheus, Grafana, Logging gibi sık kullanılan bileşenleri kolayca dağıtmayı destekler. Kısacası, Rancher **Kubernetes'i daha kullanıcı dostu hale getiren** ve kurumsal ortamlarda işletimini kolaylaştıran bir orkestrasyon üst katmanıdır. Kubernetes ve Rancher birlikteliği, konteyner tabanlı mimarimizin omurgasını oluşturacaktır. Tüm sunucu uygulamalar (Authentik, Samba AD, Zimbra, Wazuh sunucusu vb.) Kubernetes üzerinde ayrı konteynerler/pod'lar olarak çalışacak; Rancher ile bunların durumu, ölçeklendirmesi ve güncellemeleri rahatça yönetilecektir. Konteyner mimari sayesinde uygulamaların kurulumu ve konfigürasyonu otomatikleştirilecek, birbirinden izole çalışma ortamları yaratılacaktır. Örneğin, Samba AD ve Zimbra gibi geleneksel olarak fiziksel sunucu/VM üzerinde çalışan servisler bile konteynerleştirilerek Kubernetes üzerinde çalıştırılacaktır. Bu sayede uygulamalar arası bağımlılıklar azaltılacak, tek bir fiziksel sunucuda birden çok servis verimli biçimde koşturulabilecektir. Konteyner tabanlı yaklaşım ayrıca **taşınabilirlik** sağlar: İleride farklı bir altyapıya geçiş gerekirse (başka bir veri merkezi, bulut vb.), Kubernetes konteynerleri kolaylıkla taşınabilir veya yeniden kurulabilir. Sonuç olarak, Kubernetes + Rancher altyapısı sayesinde kurulumunu planladığımız tüm açık kaynak servisler için ölçeklenebilir, esnek, kolay yönetilebilir ve dayanıklı bir ortam tesis edilmiş olacaktır [37] [36].

Authentik (Kimlik ve Erişim Yönetimi)

Authentik, modern kurumsal ortamlarda kimlik ve erişim yönetimi ihtiyaçlarını karşılamak üzere geliştirilen açık kaynaklı bir Identity Provider (IdP) çözümüdür. Authentik'in en önemli özelliği **self-hosted** olması, yani kurumun kendi sunucularında çalışarak hassas kullanıcı verilerinin tamamen kontrol altında tutulmasına imkân vermesidir [38]. Temel işlevleri arasında kullanıcı kimlik doğrulaması, tek oturum açma (Single Sign-On) ve çok faktörlü kimlik doğrulama (MFA) yer alır. Authentik, bir IdP olarak SAML 2.0, OAuth2, OpenID Connect gibi yaygın SSO protokollerini destekler; bu sayede farklı üçüncü parti uygulamalarla entegrasyon sağlayabilir [12]. Örneğin, SAML desteği sayesinde Zimbra webmail'i Authentik ile entegre edip kullanıcıların Zimbra'ya SSO ile giriş yapması mümkün olmaktadır. Yine OAuth2/OpenID Connect desteği sayesinde uyumlu herhangi bir web uygulamasını (Wiki, issue tracker, intranet portal vb.) Authentik üzerinden çalışacak SSO'ya dahil edebiliriz. Authentik ayrıca LDAP protokolünü de destekleyerek geleneksel uygulamalara bir LDAP arayüzü sunabilmekte, RADIUS ile ağ cihazları veya VPN gibi servislere kimlik doğrulama sağlayabilmektedir [39]. Bu geniş protokol desteği, mevcut kurum altyapısındaki hemen her uygulamayı Authentik çatısı altında birleştirme esnekliği sunar.

Authentik'in mimarisinde **"flow" (akış)** adı verilen esnek iş akışları bulunmaktadır. Bu akışlar sayesinde yöneticiler kullanıcı giriş, kayıt veya parola sıfırlama gibi süreçleri adım adım özelleştirebilir; MFA adımlarını zorunlu kılabilir, Captcha veya e-posta doğrulaması ekleyebilir. Örneğin, bir kullanıcı giriş akışı tasarlanarak önce kullanıcı adı/parola doğrulaması, ardından başarılıysa OTP (tek seferlik şifre) veya WebAuthn gibi ikinci faktör doğrulaması istenebilir [40]. Bu sayede güvenlik politikaları kolaylıkla uygulanırken kullanıcı deneyimi de kontrol edilebilir. Authentik üzerinde politikalar tanımlanarak belirli IP adres aralıklarından gelen girişlere farklı kurallar uygulamak, belirli grupların belirli uygulamalara erişimini kısıtlamak gibi **rol tabanlı erişim kontrolleri** de mümkündür [41]. Yönetim arayüzü web tabanlı ve kullanımı oldukça rahattır; kullanıcılar ve gruplar oluşturmak, dizin bağlantılarını ayarlamak, uygulama entegrasyonlarını eklemek birkaç tıklama ile gerçekleştirilebilir.

Bu projede Authentik, yukarıda kapsam bölümünde detaylandırıldığı üzere Samba 4 Active Directory ile entegre çalışacaktır. Teknik olarak bu entegrasyon, Authentik içinde bir **LDAP "Source"** tanımlanarak gerçekleştirilir. Samba AD, standart bir Active Directory LDAP arayüzü sunduğundan, Authentik üzerinde bir LDAP kaynağı oluşturup Samba AD'nin IP/port ve bind bilgileri girilir [14] [15]. Böylece Authentik, AD içindeki kullanıcıları ve grupları okuyup kendi bünyesine import edebilecek, isteğe bağlı olarak şifre

doğrulamalarını da doğrudan AD'ye delege edebilecektir. Authentik'i bu şekilde yapılandırdığımızda, kullanıcıların kimlik doğrulaması arka planda Samba AD ile gerçekleşirken, Authentik ön yüzde SSO ve MFA akışlarını yönetecektir. Bu çözüm, halihazırda AD'ye entegre olan servislerle uyumlu olmayı sürdürürken (örneğin Zimbra AD'den doğrulama yapmaya devam edecek), yeni SSO entegrasyonları için de Authentik'i araya koymamıza olanak tanır. Authentik'in Keycloak gibi alternatiflerine göre daha hafif yapıda oluşu ve küçük-orta ölçekli kurumlar için daha kolay kurulup yönetilebilir oluşu da önemli bir tercih sebebidir [42]. Sonuç olarak Authentik, kurum içi tüm uygulamalara **tek merkezden güvenli erişim** sağlayacak, kullanıcıların parolalarını tek bir yerde (AD'de) tutup MFA gibi ek güvenlik adımlarıyla destekleyerek kimlik yönetimini modernize edecektir.

Samba 4 Active Directory (Açık Kaynak Dizin Hizmeti)

Samba 4 yazılımı, Linux/Unix sistemler üzerinde **Active Directory Domain Controller (Etki Alan Denetleyicisi)** işlevi sunabilen açık kaynaklı bir çözümdür. Microsoft Active Directory'nin temel özelliklerini (LDAP dizin, Kerberos bileti, DNS entegrasyonu, grup politikaları, vs.) özgür bir implementasyon olarak gerçekleştirmiştir. Samba 4 AD DC kurulduğunda, Windows Server'ın Active Directory'sine denk bir dizin altyapısı elde edilir: Kullanıcılar, gruplar, bilgisayar nesneleri merkezi olarak LDAP veritabanında tutulur; Kerberos protokolü ile tek oturum açma ve biletleme mekanizması sağlanır; istemci makineler (Windows veya Linux) domaine katılabilir ve etki alanı politikaları uygulanabilir.

Bu projedeki rolü itibarıyla Samba AD, kurumun **kimlik deposu** olacaktır. Tüm çalışanların kullanıcı hesapları, parola özetleri, grup atamaları Samba AD üstünde yer alacaktır. Windows sistemlerde olduğu gibi, kullanıcılara ait kimlik bilgilerinin merkezi bir dizinde olması, farklı uygulamalar arasında tutarlılığı sağlayacaktır. Örneğin bir çalışan işe başladığında Samba AD üzerinde hesabı açılacak; böylece e-posta sisteminden VPN erişimine kadar her alanda aynı kullanıcı hesabı geçerli olacaktır. Kimlik siloları oluşmayacak, personel ayrıldığında tek bir noktadan (AD) hesabı kapatılarak tüm yetkileri sonlandırılabilecektir. Samba AD ayrıca **NTLM ve Kerberos** desteği sayesinde hem eski hem yeni uygulamalarla uyumlu kimlik doğrulama sunar. Linux istemci makineleri, **SSSD** veya benzeri mekanizmalarla Samba AD'den kullanıcı kimlik bilgilerini doğrulayabilir, hatta otomatik ev dizini oluşturma, merkezi kimlik doğrulama (Single Sign-On) gibi özelliklerden yararlanabilir. Windows istemciler ise Samba AD'yi tıpkı bir Windows AD DC gibi görüp domain join olabilir, grup politikaları alabilir.

Samba AD'nin bir diğer avantajı, entegre DNS sunucusu sayesinde etki alanına ait DNS kayıtlarını da yönetebilmesidir. Örneğin "**kurum.local**" gibi iç etki alanı tanımlanıp Samba AD kurulurken bu DNS bölgesi oluşturulacak; AD'ye eklenen her makine için DNS kaydı otomatik eklenecektir. Bu durum, özellikle Active Directory ortamının tutarlılığı ve Kerberos'un düzgün çalışması için kritik önemdedir.

Açık kaynak ve lisans maliyeti olmaksızın, Samba 4 ile bir AD altyapısı kurmak kurum için büyük bir esneklik sağlar. Windows Server lisansına ihtiyaç duymadan, aynı hizmetleri görebilecek bir dizin denetleyicisine sahip olunur. Topluluk tarafından geliştirilen Samba, yıllar içinde oldukça olgunlaşmış olup, 100.000'den fazla kullanıcıyı kaldırabilecek ölçeğe erişmiştir [43]. Elbette Samba AD kullanırken dikkat edilmesi gereken noktalar vardır: Windows AD'ye göre yönetim araçları ve entegrasyonlar sınırlı olabilir, belirli şema güncellemelerinde uyumluluk testleri yapmak gerekir. Ancak projede öngörülen kullanım (temel kullanıcı/grup yönetimi ve kimlik doğrulama) için Samba fazlasıyla yeterli olacaktır.

Özetle, Samba 4 AD DC kurum içinde **Active Directory eşdeğeri** bir dizin ve kimlik doğrulama hizmeti sunarak, kullanıcı yönetimini merkezileştirecek ve diğer bileşenlerin (Authentik, Zimbra, vs.) etrafında entegre olacağı bir temel sağlayacaktır. Bu temel üzerinde, Authentik gibi IdP araçları Samba'yı "kaynak" alarak SSO kuracak, Zimbra gibi uygulamalar Samba'yı "harici LDAP" olarak kullanarak kullanıcı

doğrulayacaktır. Böylece her şeyin kalbinde Samba AD yer alacak ve **"her servis için tek kullanıcı hesabı"** ilkesi gerçekleştirilmiş olacaktır.

Zimbra Collaboration Suite (Open Source Edition)

Zimbra açık kaynak e-posta ve işbirliği platformu, kullanıcıların e-posta, takvim, rehber ve belge yönetimi ihtiyaçlarını karşılayan bütünleşik bir çözüm sunar. Zimbra'nın açık kaynak sürümü (OSE), kurumsal düzeyde bir e-posta sunucusunun temel tüm fonksiyonlarına sahiptir ve Microsoft Exchange Server gibi pahalı ürünlere güçlü bir alternatif olarak görülmektedir [17] . Web tabanlı Zimbra arayüzü, zengin özelliklere sahip bir AJAX istemcisidir: Kullanıcılar tarayıcı üzerinden e-postalarını okuyup gönderebilir, takvim girdilerini yönetebilir, başkalarıyla toplantı davetleri paylaşabilir ve kişi listelerini düzenleyebilir. Zimbra aynı zamanda IMAP/POP3, CalDAV, CardDAV gibi standart protokolleri desteklediği için masaüstü e-posta istemcileri (Thunderbird, Outlook – eğer açık kaynak eklentilerle desteklenirse vs.) veya mobil cihazlarla da uyumlu çalışabilir.

Zimbra'yı bu proje kapsamında seçmemizin nedeni, **toplam sahip olma maliyetini** düşürürken kuruma özelleştirilebilir ve verisi üzerinde tam kontrol sahibi olacağı bir e-posta sistemi kazandırmaktır. Açık kaynak olması sayesinde Zimbra'nın kodları incelenebilir, topluluk tarafından güvenlik açıkları hızla yamalanır ve gerekirse özelleştirmeler yapılabilir. Ayrıca eklenti mimarisi ile Zimlet adı verilen eklentiler yüklenerek ek fonksiyonlar kazanabilir (örneğin WhatsApp entegrasyonu, CRM entegrasyonu gibi).

Zimbra kurulumu Ubuntu Server üzerinde konteyner içindeki bir hizmet olarak gerçekleştirilecektir. Kurulum sonrasında web yönetim konsolu üzerinden alan adı ve e-posta uçbirimleri tanımlanacak, DNS kayıtları (MX, A, SPF, DKIM vs.) ayarlanarak e-posta akışı sağlıklı şekilde çalışır hale getirilecektir. Kullanıcı hesaplarının oluşturulması ve yetkilendirilmesi konusunda Samba AD ile entegrasyon devreye girecektir. **External LDAP/AD Authentication** özelliği kullanılarak, Zimbra'nın her oturum açma isteğinde Samba AD'ye gidip kullanıcı adı/parola kontrolü yapması sağlanacaktır [19] [44] . Böylece Zimbra üzerinde bir kullanıcı hesabı açılırken, aynı bilgiler Samba AD'de olduğu sürece kullanıcı doğrudan AD parolasını kullanarak e-postasına erişebilecektir. İdari kolaylık açısından, Zimbra'da **Auto Provisioning (otomatik hesap oluşturma)** mekanizması da değerlendirilebilir. Bu mekanizma ile AD'de var olan kullanıcılar için Zimbra üzerinde otomatik mailbox oluşturulması mümkün olur (örneğin belirli bir AD grubu üyeleri için Zimbra'da hesap aç gibi) [45] .

Zimbra'nın bir diğer avantajı, **mobil cihaz senkronizasyonu** ve **Outlook entegrasyonu** gibi konularda da çözümler sunmasıdır. Açık kaynak sürüm ActiveSync desteğini doğrudan içermezken, gerek duyulursa Z-Push gibi açık kaynak bir ActiveSync sunucusu eklenerek mobil push mail kabiliyeti eklenebilir. Outlook veya diğer EWS istemcileri için de açık kaynak eklentiler veya IMAP/CalDAV kullanımı ile entegrasyon sağlanabilir. Kullanıcıların büyük kısmının web arayüzünü kullanacağı varsayımıyla, Zimbra tümleşik bir çözüm sunacaktır.

Performans ve ölçeklenebilirlik açısından, Zimbra tek sunucu modunda yüzlerce kullanıcıya hizmet verebilecek kapasitededir (sunucu donanımına bağlı olarak). İleride kullanıcı sayısı çok artarsa, Zimbra'nın çok sunuculu dağıtık kurulumu (ayrı MTA, ayrı mailbox sunucuları vb.) da değerlendirilebilir. Ancak mevcut proje kapsamında tek bir konteyner içinde tüm Zimbra bileşenlerinin (MTA, Mailbox, LDAP, Proxy vb.) çalışacağı bir **hepsi bir arada (all-in-one)** kurulum yeterli olacaktır.

Sonuç olarak Zimbra, kullanıcı deneyimi olarak alışılmış kurumsal e-posta fonksiyonlarını sağlayan, açık standartlarla uyumlu, güvenilir bir platformdur. Bu projede Zimbra ile kurum içi e-posta sistemi kurularak Exchange Online/Office 365 gibi bulut hizmetlerine bağımlılık ortadan kaldırılacak; tüm e-posta verisi kurum sunucularında güvenle saklanacaktır. Kullanıcılar herhangi bir web tarayıcıdan ya da istemci programdan şirket e-postalarına erişebilecek, takvim randevularını paylaşabilecek ve dosya

alışverişi yapabilecektir. Tüm bu iletişim verisinin yedeği de düzenli olarak alınarak (örneğin Zimbra'nın built-in tool'ları veya harici yedekleme ile QNAP NAS'a kopyalayarak) olası veri kayıplarına karşı koruma sağlanacaktır.

Wazuh (Log Yönetimi ve Güvenlik İzleme)

Wazuh, kurumların uç nokta ve sunucu güvenliğini izlemelerine yardımcı olan, açık kaynak kodlu bütünleşik bir **XDR (Extended Detection and Response)** ve **SIEM (Security Information and Event Management)** platformudur. Wazuh'un temel bileşenleri; ajan (agent), merkezi sunucu (server veya manager) ve alarm konsolu (Kibana veya Wazuh Dashboard) şeklindedir. Bu projede Wazuh ajanları tüm önemli sistemlere kurulacaktır: Kubernetes node'ları (Ubuntu sunucular), kritik konteynerler (mümkün olanlarda), ve hatta istemci Linux sistemler. Wazuh ajanı, sistemde gerçekleşen güvenlik ile ilgili her olayı yakalar ve Wazuh sunucusuna iletir [46]. Toplanan veriler arasında syslog kayıtları, kimlik doğrulama girişimleri, dosya bütünlüğü değişimleri, rootkit tespitleri, ağ bağlantı kayıtları gibi birçok bilgi bulunur. Wazuh sunucusu ise tanımlı kural setlerine göre bu logları analiz eder, belirli bir saldırı modeline uyan kalıplar tespit ettiğinde alarm üretir (örneğin, kısa sürede çok sayıda başarısız giriş denemesi -> brute force alarmı, kritik bir dosyada değişiklik -> dosya bütünlüğü alarmı gibi). Wazuh sayesinde, sistem yöneticileri tek bir arayüz üzerinden tüm altyapının güvenlik durumunu gözlemleyebilir, **gerçek zamanlı bildirimler** alabilir.

Wazuh platformu, **OSSEC** tabanlı bir ajan kullandığı için oldukça hafiftir ve sistem performansına minimal etki eder. Topladığı loglar Wazuh sunucusunda Elasticsearch tabanlı bir veritabanında tutulabilir, böylece geçmişe dönük aramalar ve raporlamalar yapmak mümkün olur. Wazuh'un arayüzü (Kibana plugin veya yeni Wazuh Dashboard) ile belirli zaman aralıklarında kaç tane güvenlik olayı olduğu, bunların kategorileri (ör. malware, policy violation, anomaly vs.) gibi bilgiler görselleştirilebilir. Ayrıca Wazuh, **MITRE ATT&CK** çerçevesine göre tespit ettiği olayları sınıflandırarak, olası bir saldırının kill chain üzerindeki aşamasını anlamaya yardımcı olur.

Bu projede Wazuh kullanımı, özellikle **log yönetimi** ve **izinsiz giriş tespiti (IDS)** konularında merkezi bir çözüm sunacaktır. Örneğin, Authentik üzerinde başarısız giriş denemeleri veya Zimbra üzerinde çok sayıda gönderim yapmaya çalışan bir hesap, Wazuh tarafından tespit edilip anında güvenlik ekibine alarm geçilecektir. Yine sistem kaynaklarının anormal kullanımı, beklenmedik servis durmaları gibi operasyonel olaylar da Wazuh tarafından görülebilir (her ne kadar Prometheus bu konuda asıl araç olsa da, Wazuh da temel metric izleme yapabilir).

Wazuh ajanlarının yanı sıra, Wazuh sunucusuna harici cihazlardan (firewall, switch, vs.) Syslog gönderimi de yapılandırılabilir. Böylece ağ cihazlarının logları da aynı SIEM havuzunda toplanmış olur. Wazuh, **PCI-DSS, GDPR** gibi standartlar için uyumluluk kontrol modülleri de içerir; sistemlerde güvenlik yapılandırması taraması yaparak zayıf konfigürasyonları raporlayabilir.

Genel olarak Wazuh'un bu altyapıdaki rolü, **her şeyin kayıt altına alınması ve izlenmesi** prensibini hayata geçirmektir. Log yönetimi doğru yapıldığında, bir olay olduktan sonra kök neden analizi yapılabilir veya proaktif olarak şüpheli aktiviteler fark edilip engellenebilir. Örneğin, Wazuh alarm ürettiğinde tetiklenen bir kuralla ilgili hesabı otomatik kilitlemek veya ilgili IP'yi firewall'da engellemek mümkündür (Wazuh'in aktif yanıt – active response özelliği). Bu tür ileri entegrasyonlar projede zaman kalırsa değerlendirilebilir.

Ubuntu LTS ve Masaüstü Linux Dağıtımları

Altyapının hem sunucu hem istemci kanadında **Ubuntu** tabanlı işletim sistemleri kullanılacaktır. Ubuntu Server LTS (Long Term Support) sürümleri, kararlılık ve uzun vadeli güvenlik güncellemeleri sunması

nedeniyle tercih edilmektedir. Canonical firması, her LTS sürümüne en az 5 yıl boyunca ücretsiz güvenlik yamaları ve bakım güncellemeleri sağlamaktadır ki bu üretim ortamları için kritik bir avantajdır [47]. Uzun destek süresi sayesinde sık sık dist-upgrade yapma gereksinimi olmadan sistemler stabil kalabilir, yalnızca gerekli güvenlik yamaları alınarak işletim devam eder. LTS sürümler ara sürümlere göre daha **denenmiş ve test edilmiş** paketler içerdiğinden beklenmedik uyumsuzluklar veya konfigürasyon değişiklikleriyle karşılaşma riski düşüktür [48] [49]. Dolayısıyla sunucularımızda Ubuntu 22.04 LTS (Jammy Jellyfish) veya çıkmışsa 24.04 LTS sürümü kullanılacaktır. Bu sayede Kubernetes, Zimbra, Samba gibi bileşenlerin paket uyumluluğu ve desteği de en iyi şekilde sağlanmış olacaktır.

İstemci tarafında kullanılacak **Linux Mint, Zorin OS** gibi dağıtımlar da Ubuntu LTS tabanını kullandığından, altyapı ile bütünlük içinde olacaktır. Bu dağıtımların seçimi, son kullanıcı deneyimini iyileştirmeye yöneliktir. Linux Mint, özellikle Cinnamon masaüstü ortamıyla Windows'a alışkın kullanıcılar için oldukça tanıdık bir arayüz sunar; başlat menüsü, görev çubuğu ve sistem tepsisi gibi öğeler klasik masaüstü metaforuna dayalıdır. Mint, kullanıcı dostu olması amacıyla birçok codec, eklenti ve sürücüyü önceden yüklü getirir, böylece günlük kullanımda ekstra kurulum gerektirmez [50] [23]. Zorin OS ise görsel açıdan çekici ve modern bir tema ile gelir; Windows, macOS veya Linux geleneksel arayüzlerine benzer düzen seçenekleri mevcuttur. Özellikle Zorin'in arayüzü Windows 10/11'e benzer şekilde düzenlenebilir ve bu sayede Windows'tan geçen kullanıcılar minimum uyum süreci ile çalışmaya devam edebilir [26]. Her iki dağıtım da **son kullanıcı odaklı** tasarlandığından, ofis uygulamaları (LibreOffice), web tarayıcı (Firefox/Chrome), multimedya oynatıcılar gibi sık kullanılan yazılımlar kutudan çıktığı gibi hazır gelir [50]. Kullanıcılar yazıcı, tarayıcı gibi çevrebirimlerini Ubuntu depolarındaki sürücüler sayesinde tanımakta genellikle zorluk yaşamazlar.

İstemci Linux dağıtımlarına geçişte, kullanıcılara gerekli eğitim ve alışma süresi tanınacaktır. BT birimi, Mint/Zorin üzerinde temel işlemler (dosya yönetimi, ağ sürücülerine erişim, yazıcı ekleme, vb.) konusunda kısa eğitimler ve dokümantasyon sağlayacaktır. Ayrıca, bazı özel kurumsal uygulamalar sadece Windows üzerinde çalışıyorsa, bu durumda geçiş aşamalı planlanacak veya bu uygulamalar için alternatif çözümler (ör. Wine ile çalıştırma, sanal makine kullanma ya da web tabanlı muadillere geçiş) değerlendirilecektir. Genel beklenti, birçok kullanıcının iş ihtiyaçlarının zaten web tabanlı uygulamalar, ofis yazılımları ve e-posta ile sınırlı olması nedeniyle Linux ortamına geçişte büyük bir sorunla karşılaşmayacağı yönündedir. Bu sayede, masaüstü tarafında da lisans maliyetlerinden tasarruf edilebilecek, güvenlik açıkları hızlı kapanan ve kullanıcı verilerinin izinsiz telemetri ile toplanmadığı (Windows 10+'un sık eleştirilen telemetri özellikleri malum) bir çalışma ortamı tesis edilecektir. Sonuç olarak Ubuntu tabanlı istemci ve sunucu işletim sistemlerinin kurumdaki kullanımı, açık kaynak mimarimizin temelini oluşturan bir diğer önemli adımdır [21].

Önerilen Sistem Mimarisi ve Entegrasyonlar

Projede hayata geçirilecek sistem mimarisi, yukarıda bahsedilen tüm bileşenleri bütüncül bir yapıda bir araya getirecektir. **Şekil 1**, tasarlanan mimarinin genel görünümünü sunmaktadır (*/ Not: Şekil 1 varsayımsaldır, metin açıklaması aşağıdadır /*). Bu mimaride, üç adet fiziksel sunucu üzerine kurulan bir **Kubernetes kümesi** çekirdek altyapıyı oluşturur. Kubernetes kümesinin yönetimi Rancher aracılığıyla basitleştirilmiş olup, tüm konteyner tabanlı servislerin yaşam döngüsü bu ortamda idare edilir.

Sunucuların her biri Ubuntu Server LTS çalıştırmakta ve Kubernetes düğümü (node) olarak konfigüre edilmektedir. Yük dengeleme ve yüksek erişilebilirlik amacıyla Kubernetes kontrol düzlemi (control plane) bileşenleri birden fazla sunucuya dağıtılabilir; ancak burada Rancher yönetimli bir RKE2 kümesi kullanıldığı için bu detaylar Rancher tarafından soyutlanmaktadır.

Konteyner Dağılımı: Kubernetes kümesi içerisinde farklı namespace'lerde çeşitli uygulama servisleri çalışacaktır. Örneğin, *infrastructure* adlı bir namespace altında Authentik, Samba AD ve Zimbra servisleri konuşlandırılırken, *monitoring* namespace'i altında Wazuh server, Prometheus, Grafana gibi izleme/güvenlik servisleri çalıştırılabilir. Her bir uygulama, ilgili Docker container imajları kullanılarak **Deployment** nesneleri şeklinde tanımlanacaktır.

- **Authentik:** Resmi Authentik Docker imajı kullanılarak (goauthentik) bir deployment oluşturulur. Authentik'in PostgreSQL veritabanı ihtiyacı için aynı pod içinde (sidecar) veya cluster genelinde ayrı bir PostgreSQL servisi de konuşlandırılır. Authentik servisinin dış erişimi için Kubernetes **Ingress** kaynakları tanımlanarak, örneğin `auth.kurum.local` şeklindeki bir DNS adı üzerinden 443 portundan erişim sağlanacaktır. Authentik konteyneri Samba AD ile entegre çalıştığından, Samba'nın LDAP ve Kerberos portlarına (389, 636, 88 vs.) erişim yetkisi olacaktır.

- **Samba Active Directory:** Samba AD için kararlı bir Docker imajı (örneğin `dc` adıyla bir container) kullanılıp StatefulSet veya Deployment olarak çalıştırılır. AD'nin veri bütünlüğü kritik olduğundan, bu container'a ait bir **persistent volume** tanımlanarak, Samba'nın `sysvol` ve `NTDS` veritabanı dosyaları bu kalıcı disk alanına yazılacaktır. Bu sayede container yeniden başlasa da dizin verisi kaybolmayacaktır. Samba AD konteyneri, yüksek erişilebilirlik için istenirse çoğaltılabilir (birden fazla DC kubernetes üzerinde farklı nodelarda çalıştırılıp AD replikasyonu yapılabilir), fakat ilk aşamada tek bir DC yeterli görülmektedir. DNS hizmeti de Samba tarafından sağlanacağı için, kubernetes içi CoreDNS ayarları Samba'yı forward edecektir ya da Samba konteyneri hostNetwork modunda çalıştırılarak doğrudan kurumsal ağa entegre edilecektir. Samba AD'ye istemci makineler (Linux Mint/Zorin OS) katılmayacak olsalar bile, AD bir kullanıcı veritabanı olarak hizmet edecektir.

- **Zimbra:** Zimbra konteynerleştirmesi nispeten ağır bir servistir ve çok bileşenli yapısı nedeniyle özen ister. Proje kapsamında üçüncü parti bir Zimbra Docker imajı (örn. **Zimbra 9 OSE** için mevcut bir imaj) kullanılması ya da Zimbra'nın klasik kurulumu için konteyner içinde bir Ubuntu instance'ı oluşturulması düşünülebilir. Tercihen her Zimbra bileşenini ayrı konteyner olarak çalıştıran bir çözüm yerine, hepsi bir arada tek konteyner yaklaşımı yönetimsel olarak daha kolay olabilir. Zimbra konteyneri için de persistent volume ayrılarak, /opt/zimbra altında biriken tüm posta kutusu verisi ve konfigürasyonun kalıcı depolanması sağlanacaktır. Zimbra servisi de `mail.kurum.local` benzeri bir adresten erişilebilir olacaktır. Dış dünyadan gelen e-postalar kurumun MX kaydı üzerinden bu sunucuya ulaşacak, güvenlik açısından istenirse bir **mail gateway** (antispam/antivirüs için Proxmox Mail Gateway benzeri açık kaynak bir çözüm) konteyneri de önüne konulabilir. Fakat Zimbra kendi bünyesinde ClamAV ve SpamAssassin barındırdığı için bu ekstra bileşen opsiyoneldir.

- **Wazuh ve İzleme Bileşenleri:** Kubernetes kümesinin *monitoring* namespace'inde Wazuh sunucusu, Elasticsearch ve Kibana (ya da Wazuh dashboard) konteynerleri çalışacaktır. Wazuh ajanları ise sunuculara host bazında kurulacağından konteyner değildir, ancak node'larda daemonset olarak çalıştırılan izleme ajanları da eklenebilir. Prometheus ve Grafana ise Rancher'ın katalogundan veya helm chart ile kurulabilir. Prometheus, cluster içindeki tüm pod'lardan metrikleri toplamak üzere konfigüre edilir; node-exporter, kube-state-metrics gibi ek bileşenler devrede olacaktır. Grafana arayüzü ise `grafana.kurum.local` gibi bir adresten erişime açılarak, yöneticilerin metrik dashboardlarına kolayca ulaşması sağlanır.

- **Ağ ve Servis Yönlendirme:** Tüm bu servislerin dış erişimi için Kubernetes Ingress nesneleri ve bir **Ingress Controller** (muhtemelen NGINX Ingress) kullanılacaktır. Tek noktadan TLS terminasyonu ve sanal host yönlendirmesi ile, dışarıya yalnızca Kubernetes node'larının 80/443

(ve e-posta için 25, 587, 993 gibi) portları açılacak; Ingress, istemci isteklerini host adına göre doğru servisin doğru porta yönlendirecektir. İnternal servisler (örneğin Samba AD LDAP, Kerberos) için ise cluster içi servis tanımları yoluyla Authentik gibi uygulamalar iletişim kuracak, dış dünyaya açılmasına gerek olmayacaktır.

- **Güvenlik Duvarı Entegrasyonu:** Kubernetes cluster'ın dış IP'si veya bulunduğu alt ağ, kurumun fiziksel güvenlik duvarı arkasında olacağı için, yalnızca ihtiyaç duyulan servis portları NAT veya port yönlendirme ile internete açılır. Örneğin, dışarıdan e-posta alabilmek için 25/TCP portu Zimbra konteynerine yönlendirilir; web erişimleri (Auth, Zimbra web, Grafana vs.) 443/TCP üzerinden cluster ingress IP'sine yönlendirilir. Tüm diğer portlar kapalı tutulur. Güvenlik duvarı ayrıca tersine proxy/IDS cihazlarıyla entegre ise (mesela bir WAF), web istekleri önce WAF üzerinden de filtrelenebilir. Ancak burada WAF kurulumuna gerek duyulmayabilir, Kubernetes Ingress + ModSecurity eklentisi hafif bir WAF işlevi görebilir.

Yedekleme ve Kurtarma: Mimarinin bir önemli boyutu, yedeklemelerin düzenli yapılıp doğrulanmasıdır. Kubernetes ortamında vs. klasik VM ortamında yedekleme farklılıkları vardır. Örneğin Samba AD veritabanı için en iyi yedekleme yöntemi, `samba-tool` ile dizin yedeği almak ya da ilgili konteyner PV'sini anlık görüntülemektir. Zimbra için ise `zmbackup` (Network Edition'da tam, OSE'de bazı açık kaynak scriptler) veya doğrudan `/opt/zimbra` klasörünün yedeği kullanılabilir. Authentik ve Wazuh gibi uygulamaların da düzenli veritabanı dump'ları (PostgreSQL, etc.) alınıp NAS'a aktarılacaktır. QNAP NAS, çeşitli protokoller (NFS, SMB, rsync) desteklediğinden, Kubernetes persistent volume'lerinin anlık görüntülerini veya uygulama bazlı yedekleri NFS share'lar üzerinden NAS'a kopyalamak mümkündür. Yedekleme planı, **günlük** incremental ve **haftalık** tam yedekler olacak şekilde tasarlanabilir. NAS üzerindeki yedekler belirli bir saklama süresi (ör. 30 gün) tutulacak, kritik veriler için ayrıca harici bir diske veya buluta (şifreli olarak) periyodik kopyalar oluşturulacaktır. Bu sayede herhangi bir veri kaybı durumunda, **RPO (Recovery Point Objective)** değeri düşük, yani kısa süre öncesine ait veriler geri yüklenebilir halde olacaktır.

Ölçeklenebilirlik ve Gelecek Genişlemeler: Önerilen mimari, ileride ortaya çıkabilecek yeni ihtiyaçlara uyum sağlayabilecek esnekliktedir. Kubernetes üzerinde yeni bir açık kaynak servis eklemek gerekirse (örneğin kuruma **Nextcloud** dosya paylaşım sistemi eklenmek istenirse), bunu mevcut cluster ve Rancher yönetimi altında kolaylıkla devreye almak mümkün olacaktır. Yine kullanıcı sayısının artması veya yükün büyümesi halinde, Kubernetes node'larına ek sunucular eklenerek yatay ölçekleme yapılabilir. Rancher arayüzünden birkaç tıklama ile cluster'a yeni bir fiziksel sunucu katmak mümkündür, bu da altyapının büyümesini zahmetsiz kılar. Authentik/Samba AD ikilisinin kaldırabileceği kullanıcı sayısı on binlere kadar ölçeklenebilir durumdadır (Samba AD'nin arka uç veritabanı oldukça optimize edilmiştir, Authentik ise çoğu işlemde AD'ye danışacağından yatay klonlanabilir). Zimbra için gerekirse ayrı bir konteyneri ikinci sunucuya taşıyarak yük dağıtılabilir (multi-server mod). Wazuh sunucusu da benzer şekilde cluster modunda çalışabilir. Özetle, bu mimari başlangıçta orta ölçekli bir kurum için yeterli olacak şekilde planlanmış olsa da, hem kullanıcı artışına hem de servis genişlemesine karşı hazırlıklıdır.

Sonuç ve Değerlendirme

Bu raporda tasarlanan açık kaynak tabanlı BT mimarisi, kurumun temel bilişim ihtiyaçlarını karşılarken **veri egemenliği**, **maliyet etkinliği** ve **esneklik** sağlamayı hedeflemektedir. Önerilen sistem; Authentik + Samba AD ile merkezi kimlik ve erişim yönetimi, Zimbra ile e-posta ve işbirliği, Kubernetes + Rancher ile modern konteyner altyapısı, Wazuh + OpenVAS ile entegre güvenlik izleme ve Ubuntu tabanlı istemci/sunucu işletim sistemleriyle uçtan uca özgür bir ekosistem ortaya koymaktadır. Bu çözüm, bulut

hizmetlerinin sunduğu pek çok avantajı (esneklik, ölçeklenebilirlik, erişim kolaylığı) kurum içi bir yapıda yeniden üretirken, aynı zamanda verinin tam kontrolünü kuruma vermektedir.

Açık kaynak teknolojilerin kullanımı, uzun vadede lisans maliyetlerini ciddi ölçüde azaltacağı gibi, kurum içinde bir **bilgi birikimi** oluşmasını da teşvik edecektir. BT ekibi, kullanılan sistemlerin iç yapısını öğrenip gerektiğinde özelleştirmeler yapabilecek, dışa bağımlılık en aza inecektir. Güvenlik açısından bakıldığında, kapalı kaynak sistemlere kıyasla açık kaynak kodlu sistemlerde şeffaflık ve denetlenebilirlik daha yüksektir; olası zaafiyetler topluluk tarafından hızla ortaya çıkarılıp yamalanır. Ayrıca veri kurum sınırları içinde kaldığından, özellikle kişisel verilerin korunması, yasal uyumluluk (ör. KVKK/GDPR) konularında riskler azaltılmış olur.

Önerilen mimarinin başarılı bir şekilde hayata geçirilebilmesi için aşama aşama bir plan izlenmelidir: Öncelikle fiziksel altyapının (sunucular, ağ, depolama) kurulumu ve Kubernetes cluster'ın yapılandırılması, ardından sırasıyla Samba AD, Authentik, Zimbra ve diğer bileşenlerin devreye alınması planlanabilir. Her bir aşamada testler yapılarak sistemlerin beklenen şekilde çalıştığı doğrulanmalıdır. Özellikle kimlik yönetimi entegrasyonları (Authentik ↔ Samba AD ↔ Zimbra) dikkatlice test edilmeli, kullanıcıların tüm hizmetlere erişimi sorunsuz sağlandığından emin olunmalıdır. Pilot kullanıcı grubuyla istemci Linux dönüşümü denemeleri yapılarak, günlük iş akışlarının aksamadığı görülmelidir. Sonrasında kademeli bir geçişle tüm kullanıcılar yeni sistemlere alınabilir.

Elbette her projenin barındırdığı riskler ve zorluklar gibi, bu açık kaynak mimarinin de dikkat edilmesi gereken noktaları vardır. Mevcut sistemlerden geçişte veri migrasyonu (özellikle e-posta arşivlerinin Zimbra'ya aktarımı, dizin verisinin AD'ye importu vs.) titizlikle planlanmalıdır. Kullanıcılara yeni sistemlerin eğitimi verilmelidir. Açık kaynak araçların sürüm güncellemeleri yakından takip edilip düzenli uygulanmalıdır (LTS sürümler bu nedenle seçildi). Ancak tüm bu yönetilebilir zorlukların ötesinde, projenin sonunda kurum için uzun ömürlü, özgür ve kontrolün elde olduğu bir bilişim altyapısı kurulmuş olacaktır.

Sonuç itibariyle, **"Ubuntu tabanlı açık kaynak kurumsal mimari"** projesi, günümüzün bulut odaklı BT yaklaşımına alternatif, **yerelleştirilmiş bir bulut** modelini temsil etmektedir. Bu mimari sayesinde kurum, kendi veri merkezinde bulut konforunu ve ölçeklenebilirliğini yaşarken, stratejik verilerini güvence altında tutabilecek, özelleştirme özgürlüğüne sahip olacak ve yüksek lisans maliyetlerinden kurtulacaktır. Projenin başarıyla uygulanması, benzer durumda olan diğer kurumlar için de bir örnek teşkil edebilir ve açık kaynak çözümlerin kurumsal ölçekte uygulanabilirliği konusunda farkındalık yaratabilir. Bu tez önerisi, belirtilen hedeflere ulaşmak üzere kapsamlı ve planlı bir yol haritası ortaya koymuş olup, uygulama sürecinde elde edilecek bulgular ile açık-kapalı kaynak kıyaslamasına dair akademik katkılar da sunmayı amaçlamaktadır.

Kaynaklar:

- [1] [2] Avrupa pazarında bulut sağlayıcılarına bağımlılık ve veri egemenliği tartışması
- [4] Açık kaynak tabanlı mimari ile bulut bağımlılığını azaltma hedefi
- [5] Projenin amacı ve Azure bağımlılığını azaltma vurgusu
- [6] [7] Açık kaynak alternatiflerle tüm temel BT servislerini karşılama ve veri kontrolünü elde tutma
- [47] Ubuntu LTS sürümlerinin 5 yıl destekle kararlılık sunması (üretim ortamları için ideal)
- [9] Proje kapsamının orta ölçekli bir kurumsal BT altyapısındaki tüm servisleri kapsaması
- [10] İstemci tarafında Linux Mint/Zorin OS, sunucuda Ubuntu Server ve açık kaynak servislerin konumlandırılması
- [11] Authentik'in açık kaynak kimlik sağlayıcı olarak tanımı (SSO ve erişim kontrol yetenekleri)

- [12] Authentik'in SAML, OAuth2, OIDC, LDAP gibi protokolleri desteklemesi (geniş entegrasyon yeteneği)
- [13] Samba AD'nin merkezi kimlik kaynağı olarak kullanılıp IAM çözümleriyle entegre edilebilmesi (Windows ve SSO dünyasını birleştirmesi)
- [14] [15] Authentik ile Active Directory (Samba) entegrasyonu için LDAP kaynağı oluşturma adımları (AD'nin Authentik'e bağlanması)
- [16] Merkezi IAM ile tüm kullanıcıların SSO ve MFA ile güvenli erişim kazanması (Keycloak örneğinden uyarlanmıştır)
- [27] Wazuh'un açık kaynak XDR/SIEM olarak tanımı ve güvenlik olaylarını izleme yeteneği
- [31] Ağ çevre güvenlik duvarlarının dış tehditlere karşı iç ağı korumadaki rolü (ilk savunma hattı olması)
- [23] Linux Mint'in Windows/Mac kullanıcıları için tanıdık ve kullanımı kolay bir masaüstü sunacak şekilde tasarlanması
- [25] Ubuntu'nun birçok türev dağıtımı olduğu; Windows'a aşina kullanıcılar için Zorin OS'nin önerilmesi (Windows benzeri arayüzüyle)
- [33] [35] Kubernetes'in otomatik ölçeklendirme, kaynak optimizasyonu ve pod hata toleransı (self-healing) kabiliyetleri
- [37] Kubernetes'in Rancher olmadan da çalışabileceği ancak Rancher'ın özellikle güvenlik, yönetim ve ölçekleme konusunda ek kolaylıklar sağladığı
- [36] Rancher'ın merkezi çoklu Kubernetes küme yönetimi, yönetim paneli ve diğer konteyner orkestratörlerini de yönetebilme özellikleri
- [17] Zimbra'nın açık kaynak bir grupware sistemi olarak e-posta, takvim, rehber hizmetlerini bir arada sunması ve Exchange/Google Apps'e alternatif olması
- [19] Zimbra'nın kimlik doğrulama yöntemleri ve Samba4/AD'nin harici kimlik kaynağı olarak kullanılabileceğinin belirtilmesi
- [44] Zimbra ile Samba4 AD entegrasyonunun kurulması ve test edilmesi (harici AD doğrulaması için)
- [20] Zimbra kurulumu ile kurum içi Exchange alternatifinin oluşturulması, e-posta, takvim, adres defteri ihtiyaçlarının karşılanması
- [22] Son kullanıcı Linux geçişinin değerlendirilmesi, uyumluluk ve kullanıcı deneyimi analizinin hedeflenmesi
- [51] Wazuh ile merkezi log toplanması, SIEM yetenekleri kurulması; OpenVAS ile zafiyet taramaları; Prometheus ile metrik izleme ve alarm mekanizmaları
- [30] QNAP NAS'ın anlık görüntü, yedekleme ve veri kurtarma senaryoları için sağladığı çözümler (örnek bir markanın veri koruma vurgusu)

---

[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [16] [20] [21] [22] [28] [29] [51] tez konusu.pdf
file://file_000000008f9472438484fa7b0ca12770

[11] [12] [38] [40] [41] [42] What is Authentik? — WorkOS
https://workos.com/blog/what-is-authentik

[13] Samba Active Directory in a Docker Container: Installation Guide
https://helgeklein.com/blog/samba-active-directory-in-a-docker-container-installation-guide/

[14] [15] Active Directory | authentik
https://docs.goauthentik.io/users-sources/sources/directory-sync/active-directory/

[17] [18] Zimbra Collaboration Suite (Open Source Edition) review | IT Pro
https://www.itpro.com/mail-servers/25870/zimbra-collaboration-suite-open-source-edition-review

19 44 45 Zimbra Tips : Integration of Active Directory/Samba4 with Zimbra Mail Server - Ahmad Imanudin
https://imanudin.net/2014/12/07/zimbra-tips-integration-of-active-directorysamba4-with-zimbra-mail-server/

23 25 50 Best first time Linux OS, for someone who isn't computer savvy - Software Recommendations Stack Exchange
https://softwarerecs.stackexchange.com/questions/28199/best-first-time-linux-os-for-someone-who-isnt-computer-savvy

24 26 Zorin OS: A User-Friendly Linux Alternative for Windows Migrants | Windows Forum
https://windowsforum.com/threads/zorin-os-a-user-friendly-linux-alternative-for-windows-migrants.356860/

27 Wazuh - Open Source XDR. Open Source SIEM.
https://wazuh.com/

30 Back up files, VMS, and cloud data with snapshot - QNAP
https://www.qnap.com/en-us/solution/data-protection

31 What is a Perimeter Firewall? Fundamentals & Benefits
https://www.timusnetworks.com/understanding-perimeter-firewall-fundamentals/

32 33 34 35 36 37 Rancher vs. Kubernetes: Key Differences & Features
https://www.groundcover.com/blog/rancher-vs-kubernetes

39 Authentik: Open-source identity provider - Help Net Security
https://www.helpnetsecurity.com/2024/08/16/authentik-open-source-identity-provider/

43 Samba 4 as an Active Directory Domian Controller : r/sysadmin
https://www.reddit.com/r/sysadmin/comments/3fi835/samba_4_as_an_active_directory_domian_controller/

46 Configuration for monitoring log files - Log data collection
https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection/monitoring-log-files.html

47 48 49 Why do many people recommend the LTS version of Ubuntu? : r/Ubuntu
https://www.reddit.com/r/Ubuntu/comments/1jp2hhz/why_do_many_people_recommend_the_lts_version_of/

ChatGPT

Ubuntu Tabanlı Açık Kaynak Kurumsal Mimari: Microsoft'un Cloud-First Yaklaşımına Karşı Veri Egemenliği Odaklı Bir Alternatif

Giriş

Dijital çağda kamu ve özel sektör kurumları hızla dijitalleşirken, ürettikleri verinin hacmi katlanarak artmaktadır. Bu durum, bulut bilişim hizmetlerine yönelimi de hızlandırmış ve birçok kuruluş kritik veri ve uygulamalarını Amazon Web Services (AWS), Microsoft Azure ve Google Cloud gibi uluslararası sağlayıcılarda barındırmaya başlamıştır. Nitekim Avrupa pazarının yaklaşık %70'inin Amazon, Microsoft ve Google gibi ABD merkezli bulut sağlayıcılarının kontrolünde olduğu belirtilmektedir [1]. Ancak bu yüksek bulut bağımlılığı bazı stratejik endişeleri beraberinde getirmektedir: Kurumlar verinin tam kontrolünü kaybetme, yabancı hukuk ve erişim taleplerine maruz kalma ve tek bir hizmet sağlayıcıya mahkûm olma (vendor lock-in) riskiyle karşı karşıyadır. Bu nedenle *veri egemenliği* kavramı, dijital çağda verinin kontrolünü elde tutmanın anahtarı olarak gündeme gelmiştir. Veri egemenliği yalnızca teknik bir güvenlik konusu olmayıp, kurumsal bağımsızlığın ve yasal uyumluluğun temel unsurlarından biri olarak görülmektedir.

Bulut bilişimin sağladığı esneklik ve maliyet avantajları yadsınamaz; ancak kritik veriler söz konusu olduğunda birçok kurum, verilerini kendi altyapılarında tutarak ve açık kaynaklı çözümlere yönelerek bulut tekellerine bağımlılığı azaltmayı hedeflemektedir. Açık kaynak ekosistemi, ücretsiz lisanslama ve şeffaflık sayesinde kurumlara hem maliyet avantajı hem de güvenlik üzerinde daha fazla kontrol sunmaktadır. Bu bağlamda, Ubuntu gibi Linux tabanlı işletim sistemleri ve beraberindeki açık kaynak araçlar kullanılarak bulut hizmetlerine alternatif oluşturabilecek kurumsal bir bilişim mimarisi tasarlamak mümkündür. Örneğin, açık kaynak *egemen bulut* platformları (OpenStack, Nextcloud, Kubernetes vb.), kurumların kendi veri merkezlerinde özel veya hibrit bulutlar kurmasına olanak tanıyarak verinin yerel kalmasını sağlamaktadır [2]. Bu proje de tam olarak bu yaklaşımla, bulut bağımlılığına karşı veri egemenliğini önceleyen Ubuntu tabanlı açık kaynak bir kurumsal mimari ortaya koymayı amaçlamaktadır.

Microsoft'un Cloud-First Stratejisi ve Azalan On-Premises Desteği

Microsoft son yıllarda "cloud-first" yaklaşımını açık biçimde benimsemiş ve yeni ürün ile hizmetlerini Azure bulutu etrafında konumlandırmıştır. Geleneksel şirket içi (on-premises) sistemlere verilen destek ve yenilikler azalırken, bulut ile entegrasyon ön plana çıkmıştır. Örneğin Windows Server 2019 sürümü klasik on-prem araçlara hala tam destek sağlarken, 2021'de piyasaya çıkan Windows Server 2022 ile birlikte Microsoft, **Azure Edition** adını verdiği özel bir sürüm tanıtmıştır. Windows Server 2022 Datacenter: Azure Edition, yalnızca Azure veya Azure Stack HCI üzerinde sanal makine olarak çalışacak şekilde tasarlanmış ve normal sürümlerde bulunmayan bazı bulut odaklı özellikleri içermektedir [3]. Hotpatch (sunucuyu yeniden başlatmadan Azure üzerinden güvenlik güncellemesi uygulama), SMB over QUIC (internet üzerinden güvenli dosya paylaşımı) ve Azure Extended Network (yerel bir ağı Azure'a genişleterek sanal makinelerin aynı IP'lerle buluta taşınabilmesi) gibi yenilikler yalnızca Azure Edition'a eklenmiştir [3] [4]. Bu özellikler, Microsoft'un sunucu işletim sistemini bile bulutla bütünleşik hale getirme stratejisini yansıtmaktadır. Benzer şekilde, Windows Server 2022'nin ardından gelen Windows

Server 2025 sürümünde de bazı geliştirmeler olmakla beraber, yeni özelliklerin önemli bir kısmı Azure Arc/Azure Stack HCI entegrasyonuna ve Microsoft Entra ID (eski adıyla Azure AD) ile hibrit çalışmaya yöneliktir. Örneğin Windows Server 2025'te Hotpatch özelliği Azure Arc bağlantılı sunucularda kullanılabilir hale gelmiş [5], sunuculara doğrudan Entra ID hesapları ekleme desteği getirilmiştir [6]. Bu da gösteriyor ki Microsoft, sunucu tarafında dahi yenilikleri bulutla bütünleştirerek sunmaktadır.

Microsoft'un bulut öncelikli stratejisinin en somut göstergelerinden biri, kendi on-premises sistem araçlarını devre dışı bırakmasıdır. Örneğin, yıllardır şirket içi yama yönetimi için kullanılan Windows Server Update Services (WSUS) rolü 2024 itibariyle *"deprecated"* ilan edilmiş, yani yeni özellik geliştirmeleri durdurulmuştur. Microsoft resmi duyurusunda WSUS'un artık aktif geliştirilmediğini, mevcut işlevlerin bir süre destekleneceğini ancak kurumların **bulut tabanlı yama araçlarına geçmesini tavsiye ettiğini** açıklamıştır [7]. Gerçekten de Microsoft, WSUS yerine Windows 10/11 istemcileri için Windows Autopatch ve Intune, sunucular için ise Azure Update Manager gibi Azure hizmetlerinin kullanılmasını önermektedir [7]. Bu durum, Microsoft'un klasik şirket içi altyapılardan ziyade güncelleme gibi kritik işlevleri bile kendi bulutuna taşımaya zorladığını göstermektedir. On-prem sistemlere yatırımlar azalırken, müşteriler bulut hizmetlerine yönlendirilmektedir. Nitekim BT topluluğunda bu değişim, *"Microsoft artık mevcut platformu desteklemek yerine yeni bir gelir stratejisi olarak herkesi Intune gibi ücretli bulut hizmetlerine yönlendiriyor"* şeklinde yorumlanmıştır [8].

Bulut baskısının bir diğer yönü, artan lisans maliyetleridir. Microsoft ürünlerinin lisans ücretleri son yıllarda düzenli olarak yükselmiş ve özellikle şirket içi sunucu yazılımlarının maliyeti küçük/orta ölçekli kurumlar için zorlayıcı hale gelmiştir. Örneğin Windows Server ve SQL Server gibi sunucu ürünlerinde 2025 Temmuz itibarıyla dünya genelinde yaklaşık **%10'luk bir zam** yapılacağı, kullanıcı erişim lisanslarında (Core/Enterprise CAL paketleri) ise **%15–20** seviyesinde artış olacağı Microsoft tarafından duyurulmuştur [9]. Bu zamlar, Microsoft'un bulut hizmetlerini tercih eden abonelik modellerine kıyasla şirket içi lisansları görece daha pahalı hale getirerek müşterileri buluta teşvik etme stratejisinin parçasıdır [10]. Nitekim Microsoft yetkilileri, bu fiyat güncellemelerinin *"müşterileri uzun vadede daha maliyet-etkin olan bulut çözümlerine yönlendirmek"* amacıyla yapıldığını ifade etmektedir [11]. Sonuçta, Windows Server, SQL, Exchange gibi sunucu yazılımlarının yanı sıra İstemci Erişim Lisansları (CAL) ve Microsoft 365 E3/E5 aboneliklerinin sürekli artan ücretleri, özellikle kısıtlı bütçeli kurumlarda sürdürülebilir değildir. Tüm bu tablo, Microsoft ekosistemine alternatif olarak açık kaynak sistemlere geçişi teknik olduğu kadar ekonomik açıdan da cazip hale getirmektedir.

Veri Mahremiyeti ve CLOUD Act Endişeleri

Microsoft, Avrupa pazarındaki müşterilerini elde tutabilmek için "Data Residency" (Veri Yerelliği) ve "Microsoft Cloud for Sovereignty" gibi inisiyatifler duyurmuş olsa da, yabancı yasa ve talepler karşısında bu çabaların sınırları bulunmaktadır. Özellikle ABD'de 2018'de yürürlüğe giren *CLOUD Act* yasası, ABD merkezli bulut şirketlerine dünya çapındaki veriler için dahi belirli şartlarda hükümet erişim taleplerine uyma zorunluluğu getirmektedir [12]. Bu yasa, veriler ABD dışında bir ülkede depolansa bile, eğer ilgili bulut sağlayıcısı ABD merkezliyse mahkeme celbi veya benzeri hukuki taleplerle söz konusu verilere erişim sağlanabilmesinin yolunu açmaktadır [13]. Dolayısıyla, örneğin bir Avrupa ülkesi sınırları içindeki veri merkezi üzerinden hizmet alsa bile, Microsoft gibi firmalar "doğru biçimde yapılmış" resmi bir talep karşısında ilgili müşteri verilerini ABD makamlarına iletmekle yükümlü kalabilir.

Nitekim 2025 yılında Fransa Senatosu'nda gerçekleştirilen bir oturumda Microsoft Fransa'nın hukuk işler direktörü Anton Carniaux bu gerçeği teyit etmiştir. Senato soruşturmasında bir senatör, *"Verilerinize yönelik düzgün biçimde hazırlanmış bir devlet talebi gelirse, iletmek zorunda kalır mısınız?"* diye sorduğunda Carniaux **"Kesinlikle, gerekli prosedüre riayet ederek."** yanıtını vermiştir [14]. Carniaux her ne kadar bugüne dek Avrupa'da böyle bir durum yaşanmadığını ve haksız talepleri hukuken geri çevirmek için

çabaladıklarını belirtse de, *"usulünce yapılmış resmi talepleri geri çeviremeyeceklerini"* açıkça ifade etmiştir [15]. Bu itiraf, veriler Avrupa'da barındırılsa dahi yabancı devletlerin yasal erişim riski bulunduğunu net biçimde ortaya koymaktadır. Benzer şekilde, Microsoft'un üst düzey yöneticileri *"müşterilere ait verileri ABD hükümetine asla iletmeyeceğimize dair bir garanti veremeyiz"* diyerek bu konuda %100 güvence sunamadıklarını dile getirmiştir [16] [15].

Öte yandan Microsoft, Avrupa Birliği'ndeki endişeleri yatıştırmak adına 2024 yılında kapsamlı bir *AB Veri Sınırı* programı açıklamıştır. Ocak 2024'te Microsoft, **Avrupa bulut müşterilerinin kişisel verilerinin tamamının Avrupa içinde tutulacağı** vaadinde bulunmuş ve hizmet logları gibi sistem tarafından üretilen verileri dahi Avrupa'da tutmak için kademeli bir plan başlatmıştır [17]. Hatta müşterilere Avrupa içinde kalacak şekilde teknik destek sunma (yerel destek ekipleri, ek ücretli destek opsiyonları vb.) gibi adımlar da bu programda yer almıştır [18]. Ancak Microsoft'un *"veriler Avrupa'da kalacak"* şeklindeki güvencesi, yukarıda bahsedilen yasal zorunluluklar nedeniyle koşulludur. Şirket, Avrupa'daki bulut altyapısını genişletmek ve verileri Avrupa hukukuna tabi kılmak için teknik ve operasyonel önlemler alsa da, **CLOUD Act** gibi yasalar karşısında bu önlemler ancak belirli bir noktaya kadar koruma sağlar. Nitekim The Register, Microsoft'un 2025'te bir yandan Avrupa'da verilerin yerelliğini vurgulayan pazarlama söylemleri geliştirirken diğer yandan *"yasal olarak zorunlu kaldığında veriyi ABD hükümetine iletmekten kaçınamayacağını"* itiraf ettiğini ve bu gölgenin halen durduğunu vurgulamıştır [19]. Kısacası, teknoloji devlerinin tek taraflı sözleri değil, bağlı oldukları ülkenin yasaları nihai belirleyici olmaktadır.

Bu durum, Avrupa genelinde de dijital egemenlik tartışmalarını alevlendirmiştir. Avrupa Birliği, GAIA-X gibi girişimlerle kıtada **dijital egemenlik** sağlamayı, yani verinin Avrupa kontrolünde kalacağı bulut altyapıları oluşturmayı hedeflemektedir [1]. GAIA-X projesi, ABD merkezli bulut devlerine karşı Avrupa değerlerine dayalı, birlikte çalışabilir bir bulut ekosistemi kurma çabası olarak ortaya çıkmıştır [1]. Bunun arkasında yatan temel motivasyon, yabancı sağlayıcılara bağımlılığı azaltmak ve veriyi yerel hukuk çerçevesinde güvende tutmaktır. Benzer şekilde, birçok ülke kritik verilerinin yurtdışına çıkmasını engellemek amacıyla *veri yerelleştirme* yasaları getirmekte, kamu kurumlarında yabancı bulut kullanımını kısıtlayıcı politikalar benimsemektedir. Avrupa'da Schrems II kararı sonrası bulut sağlayıcıları arasında artan belirsizlikler ve ABD ile AB arasındaki veri transferi sorunları da kurumları alternatif arayışlarına itmiştir [20] [21].

Sonuç itibarıyla, %100 veri mahremiyeti ve egemenliği sağlamak isteyen kurumlar için en güvenilir yöntem, verinin tamamen kurum içerisinde tutulduğu ve yabancı bir bulut firmasına emanet edilmediği senaryodur. Bu da pratikte, **kendi kendine yeterli yerel altyapılar** kurmakla mümkün olabilir. Açık kaynak teknolojiler tam da bu noktada kritik bir rol oynamaktadır: Kod şeffaflığı ve özelleştirilebilirlik sayesinde, kurumlar açık kaynak yazılımlarla kendi bulut benzeri platformlarını inşa edip verilerini kendi egemenlik alanlarında tutabilirler [22]. Örneğin, bir ülke veya kurum açık kaynak bulut platformları (OpenStack gibi), depolama sistemleri ve uygulamalar kullanarak hizmetlerini kendi veri merkezinde sunarsa, hem yabancı yasaların etki alanı dışında kalır hem de güvenlik denetimini bizzat yapabilir. Bu tez çalışmasının önerdiği Ubuntu tabanlı mimari de tam olarak böyle bir ihtiyacı adreslemekte; veriyi ülke sınırları içinde tutarken modern bulut hizmetlerinin avantajlarını da sunabilecek bir açık kaynak çözüm ortaya koymayı hedeflemektedir.

Projenin Amacı

Bu projenin temel amacı, Ubuntu işletim sistemi ve ilgili açık kaynak yazılımlar üzerine inşa edilmiş bütünleşik bir kurumsal bilişim mimarisi geliştirerek kurumların **verilerini kendi kontrolü altında tutmasını** sağlamaktır. Başka bir deyişle, bulut tabanlı kapalı platformlara (özellikle Microsoft Azure ekosistemine) bağımlılığı azaltan ve veri egemenliğini artıran entegre bir çözüm önerilmektedir. Proje kapsamında kurulacak sistem, kimlik yönetiminden e-posta ve ofis işbirliği araçlarına, izleme ve güvenlik

bileşenlerinden otomasyon ve altyapı yönetimine (Infrastructure as Code) kadar bir orta ölçekli kurumun ihtiyaç duyacağı tüm temel BT hizmetlerini açık kaynak alternatiflerle karşılamayı hedeflemektedir. Böylece kurum içi bir *özel bulut* (on-premises cloud) mimarisi oluşturularak, teknik gereksinimler karşılansa dahi verinin nerede saklandığı ve kimlerin erişebileceği hususlarında tam kontrol sağlanacaktır.

Önerilen mimari, Kubernetes tabanlı bir kurum içi bulut altyapısı olarak tasarlanmıştır. Tüm sunucu servisleri bir Kubernetes kümesi üzerinde konteyner olarak çalışacak ve merkezi bir orkestrasyon aracı ile yönetilecektir. Bu amaçla Rancher gibi bir yönetim platformu kullanılarak Kubernetes kümesi kolay yönetilir hale getirilecektir. Sistemin bileşenleri, Microsoft'un kapalı kaynak hizmetlerine karşılık gelecek şekilde seçilmiştir: Örneğin **Keycloak**, Azure Active Directory'ye alternatif açık kaynak kimlik ve erişim yönetimi sunucusu olarak konumlandırılırken; **Zimbra**, Microsoft Exchange/Office 365 yerine kurum içi e-posta ve işbirliği platformu olarak hizmet verecektir. Benzer şekilde istemci tarafında **Ubuntu/Linux Mint** dağıtımları Windows işletim sistemine alternatif olarak değerlendirilecek; **Wazuh SIEM** agent'ları, Microsoft Defender/Sentinel yerine uç nokta güvenliği ve log takibi yapacaktır. Bu bileşenlerin tümü birbiriyle entegre çalışacak şekilde kurulacak ve merkezi kimlik doğrulama (SSO), izleme panoları, yedekleme ve benzeri kurum geneli servisler açık kaynak araçlarla sağlanacaktır. Özetle proje, **Azure-merkezli kapalı mimariye karşı, tümüyle kurum içinde çalışacak açık kaynak bir "küçük ölçekli bulut" modeli** ortaya koymaktadır.

Burada hedeflenen sadece teknik bir sistem kurmak değil, aynı zamanda bu yaklaşımın toplam sahip olma maliyeti (TCO), güvenlik seviyesi, yönetim kolaylığı, kullanılabilirlik ve son kullanıcı deneyimi gibi açılardan geleneksel Microsoft çözümleriyle karşılaştırıldığında sağladığı avantaj ve dezavantajları da ortaya koymaktır. Böylece kurumlar için uzun vadede açık kaynak bir istifin sağlayabileceği kazanımlar somut verilerle değerlendirilmiş olacaktır.

Yöntemoloji: Değerlendirme Ölçütleri ve Test Yaklaşımları

Önerilen açık kaynak mimarinin etkinliği ve geçerliliği, çeşitli boyutlarda yapılacak test ve analizlerle değerlendirilecektir. Bu kapsamda aşağıdaki yöntem ve ölçütler planlanmıştır:

- **Toplam Sahip Olma Maliyeti (TCO) Analizi:** Açık kaynak çözümlerin lisans ücreti barındırmaması önemli bir avantaj olmakla birlikte, gerçekçi bir maliyet karşılaştırması için tüm gider kalemleri hesaba katılacaktır. Proje kapsamında kurulan altyapının donanım maliyetleri, elektrik/soğutma giderleri, sistem yönetimi için gereken iş gücü ve olası bakım/arıza maliyetleri kalem kalem hesaplanacaktır. Elde edilen 5 yıllık TCO değeri, benzer ölçekli bir Microsoft Windows Server tabanlı altyapının veya aynı hizmetleri Azure üzerinden almanın maliyetiyle karşılaştırılacaktır. Böylece açık kaynak mimarinin uzun vadeli ekonomik performansı ortaya konacak, lisans maliyetinden tasarrufun toplam masraflar içindeki payı analiz edilecektir. Beklenti, lisans ücretlerinin çıkarılmasıyla önemli bir maliyet avantajı sağlanacağı yönündedir. Nitekim bazı araştırmalar, açık kaynak yazılımların toplam sahip olma maliyetinde kapalı muadillerine yakın performans sergilediğini, özellikle lisans ücretlerinin olmamasının ölçek büyüdükçe ciddi tasarruf getirdiğini belirtmektedir [23] [24]. Bu analiz, bu tez kapsamında söz konusu tasarrufun pratikte ne ölçüde gerçekleşebileceğini gösterecektir.

- **Güvenlik Değerlendirmesi:** Geliştirilen sistem, siber güvenlik açısından derinlemesine testlere tabi tutulacaktır. Bu kapsamda tüm sunucu ve istemciler üzerinde **OpenVAS** aracı ile ayrıntılı zafiyet taramaları yapılıp bulunan güvenlik açıkları listelenecek; kritik açıklar tespit edilirse kapatılması için iyileştirmeler uygulanacaktır. Ayrıca **Wazuh** SIEM platformu üzerinden deneme amaçlı güvenlik olayları üretilecektir (örneğin bir fidye yazılımı saldırısı simülasyonu veya yetkisiz

erişim denemesi) ve sistemin bunları algılama, uyarı verme kabiliyeti ölçülecektir. Toplanan log kayıtları incelenerek sızma girişimleri veya şüpheli hareketler karşısında alarm üretip üretmediği, üretiyorsa ne hızla tepki verilebildiği gözlemlenecektir. Elde edilen bulgular, aynı senaryoların geleneksel bir Windows tabanlı sistemde (örneğin Windows Defender, Azure Sentinel gibi araçlarla) nasıl olabileceğiyle niteliksel olarak karşılaştırılacaktır. Sonuç olarak, açık kaynak mimarinin güvenlik seviyesi ile kapalı kaynak alternatiflerin güvenlik seviyesi mukayese edilip güçlü ve zayıf yönler ortaya konacaktır. Özellikle açık kaynak araçların sağladığı şeffaflık ve özelleştirilebilirlik sayesinde, güvenlik denetimlerinin daha iç rahatlığıyla yapılabildiği vurgulanabilir [25] [26]. Örneğin açık kaynak kodlu bir güvenlik aracında arka kapı olmadığından emin olunabilir ve ihtiyaç halinde kurumun kendi güvenlik gereksinimlerine göre kodda değişiklik yapmasına imkân vardır.

- **Kullanılabilirlik Analizi (Yönetim ve Son Kullanıcı Perspektifi):** Sistemin kurulumu, yönetimi ve günlük kullanımının pratikliği değerlendirilecektir. BT yöneticileri açısından açık kaynak ortamın yönetim kolaylığı **Ansible** ve benzeri otomasyon araçları ile incelenecektir. Örneğin yeni bir kullanıcı hesabı ekleme veya bir sunucuya güncelleme geçme işleminin Keycloak + LDAP + Ansible kombinasyonuyla ne kadar sürede ve kaç adımda yapılabildiği belirlenecek; aynı işlemin Active Directory + Windows Server ortamında (örn. ADUC ile kullanıcı ekleme, WSUS/ConfigMgr ile yama geçme) gerektirdiği adımlar ile karşılaştırılacaktır. Beklenen, otomasyon sayesinde açık kaynak tarafta iş gücü gereksiniminin azalması ve tekrar eden işlerin daha hızlı yapılabilmesidir. Son kullanıcılar açısından ise Linux tabanlı istemci ortamının (örneğin Ubuntu veya Linux Mint masaüstü) ofis çalışanlarınca benimsenme durumu değerlendirilecektir. Küçük ölçekli bir pilot kullanıcı grubu belirlenerek bu kişilerden bir hafta boyunca günlük işlerini (e-posta okuma, ofis dokümanı hazırlama, kurumsal sohbet uygulaması kullanma vb.) Linux yüklü dizüstü bilgisayarlarda yürütmeleri istenecektir. Bu süreçte karşılaştıkları zorluklar (alışkanlık değişimi, yazılım uyumluluğu, dil desteği gibi) kaydedilecektir. Hafta sonunda kullanıcılarla yarı yapılandırılmış görüşmeler yapılarak deneyimleri hakkında niteliksel veriler toplanacaktır. Özellikle memnuniyet düzeyi, öğrenme eğrisi, işbirliği verimliliği gibi boyutlarda geri bildirim alınacaktır. Kullanılabilirlik analizi sonucunda, açık kaynak sistemin hem yönetici hem kullanıcı deneyimi bakımından artıları ve eksileri ortaya çıkarılacak; gerekli görülen noktalarda eğitim veya ek dokümantasyon gibi çözümler önerilecektir.

- **Yeniden Üretilebilirlik ve Taşınabilirlik Testi:** Altyapının tekrar kurulabilirliği (reproducibility) ve farklı ortamlara taşınabilirliği, projenin kritik başarı ölçütlerinden biridir. Bu amacı test etmek için hazırlanan Ansible playbook'ları ve Infrastructure-as-Code betikleri kullanılarak sistemin sıfırdan başka bir ortama kurulması denenecektir. Örneğin mevcut ortamı taklit eden farklı bir fiziksel sunucu grubuna veya bir özel bulut altyapısına (farklı ağ adresleri veya donanım ile) aynı betikler çalıştırılarak kurulum yapılacaktır. Tüm servislerin (Keycloak, Zimbra, Wazuh, Prometheus vb.) tanımlı betikler ile hatasız şekilde ayağa kalkıp kalkmadığı gözlemlenecektir. Eğer imkan bulunursa, aynı betikler minimal değişikliklerle bir genel bulut ortamında (örneğin Azure veya AWS üzerinde) çalıştırılarak açık kaynak istifin bulut sağlayıcıdan bağımsızlığı da test edilecektir [27] [28]. Bu deneyler sayesinde, kurulan sistemin *vendor lock-in*'den ne derece bağımsız olduğu, gerektiğinde farklı platformlara taşınmak istendiğinde ne kadar çaba gerektireceği ölçülmüş olacaktır. Başarılı bir yeniden üretilebilirlik ve taşınabilirlik, açık kaynak mimarinin esnekliği ve uzun vadeli sürdürülebilirliği adına önemli bir gösterge sayılacaktır.

- **Kullanıcı Deneyimi (UX) Testleri:** Son kullanıcıların açık kaynak uygulamalarla etkileşimde ne derece verimli olabildiğini değerlendirmek için kullanıcı deneyimi testleri yapılacaktır. Örneğin, kurumdaki birkaç gönüllü çalışan bir hafta boyunca e-postalarını Zimbra Web istemcisi üzerinden kullanacak, dosyalarını alıştıkları gibi ağ sürücüsü yerine (varsa) Nextcloud benzeri açık kaynak bir dosya paylaşım sistemine yükleyecek ve Windows yerine Linux yüklü bilgisayarlarında günlük

işlerini sürdürecektir. Bu sürecin sonunda kullanıcılarla görüşmeler yapılarak deneyimleri hakkında niteliksel veriler toplanacaktır. Özellikle açık kaynak arayüzlerin kullanım kolaylığı, performans memnuniyeti, beklenmedik sorunlar (örneğin ofis belgelerinin uyumluluğu veya yazıcı, kamera gibi çevre birimlerinin çalışması) gibi konular tartışılacaktır. Elde edilen içgörüler, açık kaynak çözümlerin son kullanıcı tarafından kabul edilebilirliği ve olası eğitim/destek ihtiyaçları konusunda önemli geri bildirim sağlayacaktır. Bu testlerden çıkarılacak dersler, projenin sonuç bölümünde değerlendirilerek önerilen mimarinin gerçek dünyada hangi alanlarda iyileştirmeye ihtiyaç duyabileceği tartışılacaktır.

Yukarıdaki yöntemler sayesinde proje çıktıları nicel (sayısal) ve nitel (kalitatif) verilerle desteklenmiş olacaktır. Örneğin TCO analizi için ayrıntılı maliyet tabloları, güvenlik değerlendirmesi için zafiyet tarama raporları, kullanılabilirlik için anket/görüşme sonuçları gibi somut veriler elde edilecektir. Bu çok boyutlu değerlendirme yaklaşımı, çalışmanın bulgularını sağlam temellere dayandırarak tez önerisinin güvenirliğini artıracaktır.

Akademik Özgünlük ve Katkı

Bu projenin akademik özgünlüğü, güncel bir endüstri problemi olan **veri egemenliği** ve **bulut bağımlılığı** konusunu bütüncül bir açık kaynak çözüm mimarisiyle ele almasından kaynaklanmaktadır. Literatürde bulut bilişimin faydaları veya açık kaynak vs. kapalı kaynak maliyet karşılaştırmaları üzerine çeşitli çalışmalar bulunmakla birlikte, verinin yasal egemenliği perspektifinden hareketle açık kaynak odaklı entegre bir kurumsal mimari tasarımına nadiren rastlanmaktadır. Mevcut akademik çalışmalar genellikle ya teknik performans/maliyet boyutuna odaklanmakta ya da bulut hizmetlerinin yasal/regülatif yönlerine değinmektedir. Bu tez ise her iki boyutu bir araya getirmekte; birbirinden bağımsız görünen çeşitli açık kaynak bileşenleri (Linux dağıtımları, kimlik yönetimi, e-posta sunucusu, güvenlik araçları, otomasyon yazılımları vb.) tek bir çatı altında entegre ederek bütünleşik bir *alternatif model* ortaya koymaktadır. Üstelik bu modeli, gerçek dünyadaki karşılıklarıyla (Azure, Windows Server gibi endüstri standartlarıyla) çok yönlü bir kıyaslamaya tabi tutarak hem mühendislik hem de yönetim bilimleri açısından yeni veriler üretmeyi hedeflemektedir. Dolayısıyla çalışma, mevcut bilgi birikimine hem teknik uygulama hem de stratejik değerlendirme anlamında özgün bir katkı sunacaktır.

Projenin bir diğer özgün yönü, **veri egemenliği kavramını somut bir prototip üzerinden incelemesidir**. Günümüzde dijital egemenlik tartışmaları daha çok politika ve regülasyon ekseninde sürmektedir (örneğin AB'nin GAIA-X inisiyatifi, ulusal bulut stratejileri vb.). Bu tez ise kavramı akademik düzeyde teknik bir uygulamayla birleştirerek, veri egemenliğinin sağlanmasında açık kaynak teknolojilerin rolünü ortaya koyacaktır. Avrupa'da GAIA-X ve benzeri dijital egemenlik girişimleri, ABD'li bulut tekellerine karşı alternatif ekosistemler oluşturmayı amaçlamaktadır [1] [29]. Bu proje de benzer bir vizyonu ulusal ölçekte ele almakta; Türkiye özelinde kurumların yabancı bulut sağlayıcılarına bağımlılığını azaltması ve yerli/açık kaynak teknolojilere yönelmesi stratejisine somut bir model sunmaktadır. Son yıllarda ülkemizde kamuda ve kritik sektörlerde verinin ülke sınırları içinde tutulması ve açık kaynak çözümlerin desteklenmesi yönünde irade beyanları mevcuttur. Bu tez, söz konusu stratejinin uygulanabilirliğini ve etkinliğini gerçek bir prototip ve bilimsel analizlerle ortaya koyarak literatürde bu alandaki boşluğu dolduracaktır.

Ayrıca çalışma, çeşitli boyutlardaki değerlendirmeleriyle akademik literatüre yöntemsel bir katkı da yapacaktır. Örneğin açık kaynak bir sistemin TCO analizinin detaylandırılması, güvenlik açısından açık kaynak vs. kapalı kaynak karşılaştırmasının vaka çalışması şeklinde sunulması, son kullanıcı deneyiminin nitel verilerle ölçülmesi gibi yaklaşımlar ileride benzer araştırmalar için referans oluşturabilir. Özellikle veri egemenliği gibi disiplinlerarası bir konuda, hem teknik performans metrikleri hem de yasal/stratejik

implikasyonlar birlikte ele alınarak kapsamlı bir değerlendirme yapılması bu tezin özgün değerini artırmaktadır.

Projenin elde edeceği bulguların, uygun görülürse akademik yayınlara dönüştürülmesi de planlanmaktadır. Özellikle uluslararası konferanslarda sunulabilecek nitelikte bir çalışma ortaya çıkması hedeflenmektedir. Böylece tez çalışmasının sonuçları bilim dünyasıyla da paylaşılacak, benzer alandaki diğer araştırmacılar için yeni bir referans noktası oluşacaktır. Sonuç olarak, bu tez çalışmasının özgünlüğü ve katkısı; **açık kaynak teknolojilerini stratejik bir vizyonla harmanlayarak**, hem kuramsal hem de pratik boyutta dijital egemenlik sorununa yenilikçi bir çözüm önermesinden ileri gelmektedir.

Beklenen Çıktılar

Projenin başarıyla tamamlanması sonucunda elde edilmesi beklenen somut çıktılar aşağıdaki gibi sıralanabilir:

- **Çalışır Durumda Açık Kaynak Mimari Prototipi:** Ubuntu tabanlı sunucu ve istemciler üzerinde, tüm hedeflenen servislerin kurulu ve entegre şekilde çalıştığı bir *demo* ortamı oluşturulacaktır. Bu ortamda kimlik doğrulamadan e-posta alışverişine, izleme panellerinden güvenlik uyarılarına kadar projenin kapsamındaki tüm fonksiyonlar sergilenecektir. Ortaya çıkan prototip sistem, gerektiğinde jüri sunumlarında veya ilgili paydaşlara yapılacak gösterimlerde kullanılmak üzere hazır tutulacaktır. Bu sayede önerilen modelin **çalışabilirliği pratikte ispatlanmış** olacaktır.

- **Teknik Dokümantasyon ve Kılavuzlar:** Projede gerçekleştirilen kurulum ve konfigürasyon adımlarının ayrıntılı dokümantasyonu hazırlanacaktır. Örneğin *"Ubuntu Server üzerine Zimbra kurulumu ve yapılandırması"*, *"Keycloak ile LDAP entegrasyonu ve SSO ayarları"*, *"Wazuh ajanlarının istemcilere dağıtılması ve kural yazımı"* gibi alt konularda adım adım yönergeler içeren kılavuz dokümanlar üretilecektir. Bu dokümantasyon, tezin ekinde veya ayrı bir teknik rapor olarak sunulacak; böylece benzer bir altyapıyı kurmak isteyen mühendisler için referans niteliğinde olacaktır. Hazırlanacak kılavuzlar, açık kaynak teknolojilerin kurumsal ortamlara uyarlanmasında karşılaşılan pratik sorunlara ışık tutacak şekilde gerçek deneyimleri yansıtacaktır.

- **Karşılaştırmalı Analiz Raporları:** Proje kapsamında gerçekleştirilen TCO hesaplamaları, güvenlik test sonuçları, kullanılabilirlik anketleri gibi veriler derlenerek karşılaştırmalı tablolar ve grafikler oluşturulacaktır. Örneğin açık kaynak mimarinin yıllık maliyeti ile eşdeğer hizmetleri Azure üzerinden almanın maliyetinin karşılaştırılması, veya OpenVAS taramalarında bulunan zafiyet sayılarının benzer bir Windows ortamındaki sonuçlarla kıyaslanması gibi somut çıktıların yer aldığı raporlar sunulacaktır. Bu raporlar tez belgesinin ilgili bölümlerine entegre edilecek ve gerektiğinde bağımsız infografikler olarak sunumlarda kullanılacaktır. Böylece önerilen modelin *niceliksel* olarak avantaj ve dezavantajları net şekilde ortaya konmuş olacaktır.

- **Tez Dokümanı ve Akademik Yayınlar:** Çalışmanın tüm birikimi, akademik usullere uygun bir tez dokümanı olarak derlenecektir. Tez belgesi giriş-gelişme-sonuç bölümleri ve referanslar ile birlikte kapsamlı bir şekilde hazırlanacaktır. Ayrıca yukarıda belirtildiği gibi, elde edilen önemli bulgular ve yöntem, uygun görüldüğü takdirde akademik makale haline getirilip bir konferans bildirisi veya dergi makalesi olarak yayımlanacaktır. Bu sayede projenin sonuçları akademik camia ile de paylaşılmış olacak, literatüre katkı sağlanacaktır.

- **Sunum ve Savunma Materyalleri:** Tez önerisinin jüriye sunumu ve nihai tez savunması için gerekli sunum dosyaları hazırlanacaktır. Bu sunumlarda proje boyunca elde edilen önemli

noktalar görsel olarak vurgulanacak, grafik ve şekillerle desteklenecektir. Ayrıca mümkün olduğu takdirde canlı demo veya video gösterimleriyle prototip sistemin kabiliyetleri jüriye aktarılacaktır. Tüm bu materyaller, projenin anlaşılır ve etkili bir şekilde iletişimini sağlamak üzere çıktı setine dahil edilmiştir.

Yukarıdaki çıktılar, projenin hem akademik başarı kriterlerini karşılamasını hem de gerçek dünyada uygulanabilirliğini ortaya koymasını hedeflemektedir. Özellikle teknik prototip ve dokümantasyon, çalışmanın **pratik değerini** öne çıkaracak; analiz raporları ve tez yazımı ise **araştırma niteliğini** ortaya koyacaktır. Bu dengeli çıktı seti sayesinde projenin sonuçları çok yönlü olarak değerlendirilebilecek ve ilgilenen herkes için faydalı bir kaynak oluşturacaktır.

---

1 29 GAIA-X: Europe’s values-based counter to U.S. cloud dominance - Leiden Law Blog
https://www.leidenlawblog.nl/articles/gaia-x-europes-values-based-counter-to-u-s-cloud-dominance

2 22 24 25 26 The enduring value of open source in a data-driven world | ICT Pulse – The leading technology blog in the Caribbean
https://ict-pulse.com/2025/04/the-enduring-value-of-open-source-in-a-data-driven-world/

3 4 Windows Server 2022 Datacenter Azure Edition: Key Upgrades – TrustedTech
https://www.trustedtechteam.com/blogs/windows-server/microsoft-windows-server-2022-datacenter-azure-edition-all-you-need-to-know?srsltid=AfmBOoqUiIa8PYKM_NwHdDBs0Mr6GoKUhGxTILRA-gsAwIDLdbvnLq0g

5 6 What's new in Windows Server 2025 | Microsoft Learn
https://learn.microsoft.com/en-us/windows-server/get-started/whats-new-windows-server-2025

7 8 Windows Server Update Services (WSUS) deprecation - Windows IT Pro Blog
https://techcommunity.microsoft.com/blog/windows-itpro-blog/windows-server-update-services-wsus-deprecation/4250436

9 10 11 Microsoft price increase for on-premises servers July 2025
https://ultima.com/blog/microsoft-price-increase-for-on-premises-servers-july-2025/

12 13 14 Microsoft exec admits it 'cannot guarantee' data sovereignty • The Register
https://www.theregister.com/2025/07/25/microsoft_admits_it_cannot_guarantee/

15 16 Not sovereign: Microsoft cannot guarantee the security of EU data | heise online
https://www.heise.de/en/news/Not-sovereign-Microsoft-cannot-guarantee-the-security-of-EU-data-10494789.html

17 18 Microsoft offers to store all personal data of cloud customers in EU | Reuters
https://www.reuters.com/technology/microsoft-offers-store-all-personal-data-cloud-customers-eu-2024-01-11/

19 Microsoft's data sovereignty: Now with extra sovereignty! • The Register
https://www.theregister.com/2025/11/07/microsoft_announces_strengthening_of_sovereignty/

20 21 27 28 The Data Sovereignty Revolution in Enterprise IT
https://www.exasol.com/blog/data-sovereignty-revolution/

23 Open Source vs Proprietary Enterprise AI Platforms and LMS
https://botscrew.com/blog/open-source-proprietary-enterprise-ai-comparison/