Ubuntu Tabanlı Açık Kaynak Kurumsal Mimari:

Microsoft’un Cloud-First Yaklaşımına Karşı Veri Egemenliği Perspektifiyle Bir Alternatif Model

Tez Önerisi (Yüksek Lisans)
Sunucu: Kubernetes (Rancher), IAM/MFA: Authentik, Dizin/E-posta: Samba AD + Zimbra CE, İstemci: Ubuntu LTS ve Türevleri

Kısa Türkçe Açıklama

Bu tez önerisi, kurumların bulut bağımlılığını azaltmak ve veri egemenliğini güçlendirmek amacıyla, Ubuntu LTS temelli ve tamamen açık kaynak bileşenlerden oluşan kurum-içi (on-prem) bir mimari önermektedir. Sunucu tarafında Kubernetes (Rancher yönetimli) üzerinde konteyner tabanlı servisler çalıştırılır; kimlik yönetimi ve MFA, Authentik üzerinden sağlanır; dizin ve e-posta servisleri Samba 4 AD ve Zimbra Community Edition ile karşılanır. Güvenlik ve gözlemlenebilirlik katmanında Wazuh (SIEM), OpenVAS (zafiyet taraması), Prometheus + Grafana (metrik/uyarı) bulunur. Ağ çevresi fiziksel güvenlik duvarıyla korunur; yedekleme QNAP NAS gibi fiziksel bir çözümle yürütülür. Çalışma; TCO, güvenlik, kullanılabilirlik ve taşınabilirlik boyutlarında Microsoft ekosistemi ile karşılaştırmalı kanıt üretmeyi hedefler.

Abstract (EN)

This proposal presents a fully on-prem, Ubuntu LTS-based open-source enterprise architecture designed to reduce cloud dependence and strengthen data sovereignty. Server-side services run as containers on Kubernetes managed by Rancher; identity and MFA are provided by Authentik; directory and mail are implemented with Samba 4 Active Directory and Zimbra CE. Security and observability rely on Wazuh (SIEM), OpenVAS (vulnerability scanning), Prometheus + Grafana (metrics and alerting). A physical firewall protects the perimeter; backups are handled by a physical appliance such as QNAP NAS. The study aims to produce comparative evidence—against Microsoft’s cloud-first ecosystem—across TCO, security, usability, and portability, with a legal focus on data residency and sovereignty.

1. Giriş

Kamu ve özel sektörde hızlanan dijitalleşme, bulut bilişim platformlarını cazip kılarken; veri egemenliği (data sovereignty), mahremiyet ve toplam sahip olma maliyeti (TCO) gibi kritik konuları ön plana taşımıştır. ABD CLOUD Act gibi düzenlemeler, verilerin yabancı hukuk taleplerine maruz kalma riskini artırmaktadır. Microsoft ekosistemi özelinde; Windows Server 2019–2025 sürümlerindeki yeniliklerin Azure merkezli hâle gelmesi ve WSUS'un "deprecated" edilmesi gibi adımlar, kurumları hibrit/bulut çözümlerine yönlendirmektedir. Bu tez, söz konusu risklere karşı açık kaynak ve kurum-içi bir mimariyi, teknik ve yönetsel ölçütlerle değerlendirir.

2. Arka Plan – Microsoft'un Cloud-First Stratejisi ve On-Prem Eğilimler

• Windows Server 2019: Klasik on-prem yüklerin sürdürülebilirliği. • Windows Server 2022: Azure Edition, Hotpatch, SMB over QUIC, Azure Extended Networking – hibrit/bulut entegrasyonları. • Windows Server 2025: AD DS/LAPS iyileştirmeleri olmakla birlikte Azure Local/Arc/Entra ID entegrasyonlarının belirginleşmesi. • WSUS: 2024'te "deprecated"; yeni özellik yatırımları durdurulmuş, müşteriler Azure Update Manager/Intune/Autopatch'e yönlendirilmektedir. • Lisans Dinamikleri: Çekirdek bazlı lisanslama ve abonelik modelleri, uzun vadeli bütçe baskısı oluşturur. Bu yönelim, egemenlik ve maliyet odağında kurum-içi, açık kaynak alternatifleri stratejik hâle getirir.

3. Amaç ve Araştırma Soruları

Amaç: Bulut sağlayıcılarına bağımlılığı azaltan, veri egemenliğini güçlendiren, yönetilebilir ve yeniden üretilebilir Ubuntu tabanlı açık kaynak kurumsal mimariyi tasarlamak ve Microsoft ekosistemiyle çok boyutlu kıyaslamaktır. Araştırma soruları: (1) TCO avantajı nedir? (2) Güvenlik/uyumluluk (SSO/MFA/SIEM/zafiyet) seviyesi nasıldır? (3) Kullanılabilirlik ve yönetilebilirlik Rancher/Kubernetes ile nasıl iyileşir? (4) Veri egemenliği ve yasal riskler nasıl azalır?

4. Kapsam ve Sistem Mimarisi

Sunucu tarafı: 3 fiziksel sunucu üzerinde 1 kontrol (master) + 2 işçi (worker) düğümden oluşan Kubernetes kümesi. Rancher ile yaşam döngüsü yönetimi, RBAC, katalog dağıtımı ve gözlemlenebilirlik. Tüm servisler konteyner tabanlıdır; Helm/manifester ile sürümlenir; CI/CD entegre edilebilir. İstemci tarafı: Ubuntu LTS türevleri (Linux Mint, Zorin OS vb.) kullanıcı deneyimine göre seçilir ve kademeli pilotlarla yaygınlaştırılır. Ağ güvenliği: Fiziksel firewall; ağ segmentasyonu/VPN; IDS/IPS entegrasyon opsiyonu. Yedekleme: QNAP NAS üzerinde snapshot/versiyonlama; 3-2-1 kuralı ve periyodik geri dönüş tatbikatları.

4.1 Kullanılacak Açık Kaynak Bileşenler

Servis Alanı	Bileşen	Öne Çıkan Özellikler
İşletim Sistemi	Ubuntu LTS (server) + Mint/Zorin (client)	LTS ömür, yaygın paket ekosistemi; kullanıcı dostu masaüstü
Küme Yönetimi	Kubernetes + Rancher	Çoklu küme GUI, RBAC, katalog, sürüm/ölçek/yedek süreçlerinin
Dizin	Samba 4 Active Directory	AD uyumlu LDAP/Kerberos; Windows/Linux istemciler ve servis e
IAM / SSO / MFA	Authentik	SAML/OIDC/LDAP/RADIUS; MFA (TOTP/WebAuthn); politika/akış ta
E-posta & İşbirliği	Zimbra CE	AD ile harici doğrulama; web istemci; takvim/rehber; kurum-içi b
SIEM/XDR	Wazuh (ajanlar)	Merkezi log, korelasyon, kural seti, uyumluluk raporları
Zafiyet Yönetimi	OpenVAS	CVSS tabanlı tarama, risk önceliklendirme, kapanış takibi
Gözlemlenebilirlik	Prometheus + Grafana	Metrik toplama, dashboard, uyarı mekanizması
IaC/Otomasyon	OpenTofu (+ Ansible opsiyonel)	Kod'la altyapı, tekrar edilebilir ve taşınabilir kurulumlar

Yedekleme	QNAP NAS	Snapshot/versiyonlama; 3-2-1 stratejisi; hızlı geri dönüş
Ağ Güvenliği	Fiziksel firewall (veya pfSense/OPNsense)	Segmentasyon, VPN, erişim kontrolü, gerekirse IDS/IPS

5. Entegrasyon Tasarımı (IAM/SSO/MFA ve Servis Akışı)

• Kaynak Dizin: Samba 4 AD, kullanıcı/grup ve politika için “source of truth”. • IAM/IdP: Authentik, Samba AD ile senkron; SAML/OIDC ile Zimbra ve diğer uygulamalara SSO; MFA (TOTP/WebAuthn) zorunlu politikalar. • E-posta: Zimbra CE, dış AD kimlik doğrulamasıyla çalışır; Authentik üzerinden SSO akışı uygulanabilir. • Güvenlik ve İzleme: Wazuh ajanları tüm uçlardan log toplar; OpenVAS periyodik tarar; Prometheus metrikleri izler, Grafana gösterir. • Ağ/Yedekleme: Fiziksel firewall üstünden segmentasyon; QNAP NAS ile periyodik snapshot ve geri dönüş tatbikatları.

6. Yöntem (Metodoloji)

(1) TCO Analizi: 5 yıllık projeksiyonda lisans (OSS: 0), donanım/enerji/işgücü/bakım kalemleri; Microsoft on-prem + Azure senaryolarıyla karşılaştırma. (2) Güvenlik Değerlendirmesi: OpenVAS bulgu kapanış döngüsü; Wazuh’da örnek olaylar (yetkisiz erişim, brute-force, FIM); Authentik MFA/SSO politikaları. (3) Kullanılabilirlik/Yönetilebilirlik: Rancher ile sürüm/ölçek/rollback işlem adımı ve süre kıyası; istemci pilotları ve kısa anketler (Linux Mint/Zorin). (4) Yeniden Üretilebilirlik/Taşınabilirlik: OpenTofu ile sıfırdan kurulum tekrarı; farklı donanım/ortama taşınma deneyi. (5) Veri Egemenliği Değerlendirmesi: Kurum-içi modelin yasal/operasyonel risk azaltımı; CLOUD Act kaynaklı riskler ile nitel karşılaştırma.

7. Değerlendirme Ölçütleri (Metrikler)

- TCO: 3–5 yıllık toplam maliyet; CapEx/OpEx dağılımı
- Güvenlik: Zafiyet sayısı, kritik bulgu kapanış süresi, olay tespit/yanıt süresi (MTTD/MTTR), MFA kapsam oranı
- Kullanılabilirlik: Görev tamamlama süresi, yönetim işlem adımı sayısı, kullanıcı memnuniyeti anketleri
- Performans/Kapasite: Servis yanıt süreleri, kaynak kullanımı (CPU/RAM/IO), ölçeklenebilirlik
- Taşınabilirlik/Yeniden Üretilebilirlik: OpenTofu ile temiz kurulum süresi, yeniden kurulum başarım oranı

8. Akademik Özgünlük ve Katkı

Literatürde bulut avantajları ya da tekil OSS bileşen karşılaştırmaları bulunsa da; veri egemenliği odağında, Ubuntu LTS + Kubernetes (Rancher) + Samba AD + Authentik + Zimbra + Wazuh/OpenVAS/Prometheus/Grafana + QNAP/Firewall birleşimini kurum-içi, yeniden üretilebilir bir mimari olarak bütünleşik ve karşılaştırmalı ele alan çalışma sınırlıdır. Tez; (i) bütünleşik OSS kurumsal model, (ii) TCO/güvenlik/kullanılabilirlik kanıtları ve (iii) egemenlik/uyumluluk analizleriyle literatüre katkı hedefler.

9. İş Kırılımı ve Zaman Planı

Aşama	İçerik	Süre
1	Gereksinimler, ağ/topoloji, güvenlik ilkeleri, yedekleme stratejisi; OpenTofu temel modülleri	Ay 1–2
2	K8s kümesi (Rancher), çekirdek servisler: Samba AD, Authentik, Zimbra; Wazuh/Prometheus/Grafana	Ay 3–4
3	OpenVAS/zafiyet yönetimi, MFA/SSO politikaları, firewall/segmentasyon ince ayarı	Ay 5
4	TCO ölçümü, kullanılabilirlik testleri, taşınabilirlik deneyi; raporlama ve nihai yazım	Ay 6

10. Riskler ve Azaltımlar

- Kullanıcı Değişim Direnci → Eğitim, kademeli pilot, destek masası
- Uyumsuz Eski Uygulamalar → VM/uyumluluk katmanı, kısmi geçiş
- Operasyonel Karmaşıklık → Rancher, IaC ve runbook'larla standardizasyon
- Yasal/Politik Riskler → Kurum-içi veri, dışa veri akışını asgariye indirme, sözleşmesel kontroller
- Felaket Yedekleme → QNAP snapshot, offline kopya, düzenli geri dönüş tatbikatı

11. Etik, KVKK/GDPR ve Uygunluk

Proje; kişisel verilerin yalnızca kurum-içi sistemlerde işlenmesini, erişimlerin rol-tabanlı ve izlenebilir olmasını, retansiyon/anonimleştirme politikalarının uygulanmasını ve test verilerinin kişisel veri içermemesini gözetir. MFA, denetim logları ve en az ayrıcalık ilkesi esas alınır.

12. Beklenen Çıktılar ve Teslimatlar

- Çalışır prototip (K8s/Rancher üzerinde tüm servisler)
- Kurulum ve yapılandırma dokümantasyonu (runbook, diyagramlar, IaC betikleri)
- Karşılaştırmalı TCO/Güvenlik/Kullanılabilirlik raporları
- Tez belgesi ve sunum materyalleri (TR/EN özet)

13. Kısa Sözlük/Terminoloji

• Data Sovereignty: Verinin üzerinde yargı ve kontrolün yerel hukuk ve kurumda kalması. • IAM/SSO/MFA: Kimlik ve erişim yönetimi / Tek oturum açma / Çok faktörlü doğrulama. • SIEM: Güvenlik olayları ve loglarının merkezi izlenmesi/korelasyonu. • IaC: Altyapının kod ile tanımlanması ve sürümlenmesi.

Not: Donanım boyutlandırması ve marka/model seçimleri kurum gereksinimlerine göre belirlenecektir.