

GLASSHOUSE AĞ ALTYAPISI

DENETİM, İYİLEŞTİRME VE KAPANIŞ RAPORU (Q3 2026)

Hazırlayan: IT Expert Bilişim Teknolojileri
Sunulan: GlassHouse Yönetimi ve BT Operasyon Ekipleri
Tarih: 22 Eylül 2026

1. YÖNETİCİ ÖZETİ VE GİRİŞ

Bu rapor, GlassHouse veri merkezi ağı (network) altyapısında geçmiş dönemde yaşanan majör servis kesintisinin (outage) kök neden (root-cause) analizleri doğrultusunda başlatılan altyapı transformasyon ve denetim sürecinin başarıyla tamamlandığını belgelemek amacıyla ITExpert Bilişim Teknolojileri tarafından hazırlanmıştır.

Denetimlerimiz ve uygulanan iyileştirme adımları sonucunda, ağ mimarisindeki tek nokta hataları (Single Point of Failure - SPOF) tamamen giderilmiş, topoloji modern veri merkezi standartlarına yükseltilmiştir. Alınan proaktif aksiyonlar ve uygulanan sıkılaştırma (hardening) politikaları sayesinde, son 3 aylık periyotta altyapı genelinde %100 kesintisiz (Zero-Downtime) çalışma performansı ölçümlenmiştir. Bu durum, GlassHouse altyapısının müşteri iş yüklerini en zorlu senaryolarda dahi güvenle taşıyabileceğinin en net göstergesidir.

2. DENETİM KAPSAMI VE ODAK ALANLARI

Gerçekleştirilen denetim ve iyileştirme çalışmaları, altyapının direncini kalıcı olarak artırmak amacıyla aşağıdaki stratejik hedefler etrafında şekillendirilmiştir:



Hizmet Sürekliliği (Service Continuity): Ağ mimarisi, olası donanım veya bağlantı kayıplarında mikrosaniyeler seviyesinde (sub-second) alternatif yollara geçiş yapabilecek şekilde (Fast Reroute) güncellenmiş ve L2

döngülerini önleyen aktif-aktif topoloji devreye alınmıştır. Mimari iyileştirmeler kapsamında Production (canlı) sistemleri ile Backend ağ anahtarlama mimarileri birbirinden ayrıştırılarak performans izolasyonu ve güvenlik maksimize edilmiştir. Ek olarak, yüksek erişilebilirlik planlaması dahilinde sunucu küme (cluster) node dağılımları yeniden projelendirilmiş; bir cluster'ın tamamının tek bir EVPN Multi-Homing (EVPN-MH) anahtar çifti üzerinde bulunması riski (single point of failure) ortadan kaldırılarak, iş yükleri farklı donanım çiftlerine dağıtılmış ve sistemin kayıp/yedeklilik toleransı en üst seviyeye çıkarılmıştır.

Altyapı Güçlendirme (Hardening): Ağın veri (data) ve yönetim (management) trafiğini birbirinden tamamen ayırmak amacıyla sıfırdan, fiziksel ve mantıksal olarak bağımsız bir Yönetim Ağı (Out-of-Band Management - OOB) mimarisi kurulmuştur. Tüm cihaz yönetim düzlemleri bu yeni ve tamamen izole ağa taşınarak, Control Plane Policing (CoPP) politikaları ile cihazların işlemci (CPU) kaynakları anomali trafiklerine karşı koruma altına alınmıştır.



Bununla birlikte, erişim (access) katmanında uç nokta sıkılaştırmaları (Edge Hardening)

devreye alınmıştır. Olası Layer 2 döngülerini (loop) ve trafik sıçramalarını kaynağında engellemek adına tüm ağ portlarında Storm Control, BPDU Guard, Root Guard ve STP Admin-Edge / Auto-Edge mekanizmaları standart hale getirilmiş; sunucu bağlantı sürekliliği için LACP Fallback yapılandırmaları deaktif edilerek zafiyet yaratabilecek tüm eski (legacy) protokoller kalıcı olarak kapatılmıştır.

Standardizasyon ve Otomasyon (IaC): Standardizasyon süreçlerinin en büyük adımı olarak, ağ altyapısının tamamı Ansible üzerinden otomatikleştirilmiş ve konfigüre edilmeye başlanmıştır. Komut satırı (CLI) üzerinden yapılan manuel insan müdahalesi tamamen ortadan kaldırılarak, insan kaynaklı konfigürasyon hatalarının (human-error) kesin olarak önüne geçilmiştir. Tüm ağ değişiklikleri artık versiyon kontrollü, denetlenebilir ve saniyeler içinde geri alınabilir (rollback) bir sistem (Infrastructure as Code) üzerinden yönetilmektedir. Bu sayede hem güvenlik hem de operasyonel hız maksimize edilmiştir.

Gelişmiş Telemetri ve İzlenebilirlik (Observability): Ağ altyapısının sağlığını ve performansını anlık olarak takip edebilmek amacıyla, geleneksel ve reaktif (SNMP tabanlı) izleme yöntemlerinden modern bir 'Gözlemlenebilirlik (Observability)' mimarisine geçiş yapılmıştır. Ağ mimarisindeki her bir donanıma entegre edilen akıllı telemetri ajanları (telemetry agents) sayesinde, cihazlardan saniye altı (sub-second) aralıklarla gerçek zamanlı trafik, yapılandırma durumu ve routing (yönlendirme) verileri toplanmaya başlanmıştır. Bu derinlemesine veri toplama altyapısı; olası mikro-kesintileri (micro-bursts), paket kayıplarını ve anomali trendlerini henüz kullanıcı servislerine yansımadan tespit edebilen, proaktif ve veriye dayalı (data-driven) bir operasyon modeli sunmaktadır.

Yazılım Yaşam Döngüsü ve Sürüm Yönetimi (Software Lifecycle Management):

Ağ donanımlarının işletim sistemi ve yazılım sürümlerinin yönetimi için yapısal bir yaşam döngüsü politikası oluşturulmuştur. Altyapı genelinde 'Golden Image' (Standart/Onaylı Sürüm) yaklaşımı benimsenerek, cihazlar arasındaki sürüm farklılıklarından doğabilecek uyumsuzluk veya yazılım hatası (bug) riskleri tamamen ortadan kaldırılmıştır.

3. PERFORMANS ANALİZİ VE SONUÇ

Geçmişte yaşanan kesintinin ardından devreye alınan bu kapsamlı teknik aksiyonlar (MAC Flap önleme mekanizmaları, yedeklilik testleri, Ansible tabanlı IaC otomasyonu ve Hardening) sistemin stabilitesini maksimum seviyeye çıkarmıştır.

Son 3 ay içerisinde yapılan aktif izleme ve stres testleri göstermektedir ki; altyapı üzerinde herhangi bir paket kaybı veya donanım kaynaklı bir izolasyon yaşanmamıştır. IT Expert olarak beyan ederiz ki; GlassHouse veri merkezi ağ altyapısı, mevcut durumuyla küresel servis sağlayıcı standartlarına tam uyumlu, güvenilir ve olası kriz senaryolarına karşı son derece dirençli bir yapıya kavuşmuştur.

Şeffaflık ve hızlı aksiyon kabiliyetleri için GlassHouse yönetimine ve teknik ekiplerine teşekkür ederiz.

Saygılarımızla,

IT Expert Bilişim Teknolojileri

Ağ Güvenliği ve Altyapı Denetim Ekibi