



KÖK SEBEP ANALİZİ DETAY FORMU

Proje Adı:	GlassHouse Public Cloud
Tarih:	20.02.2026 15:40 - 16:24
İlgili İş Birimi:	Cloud Operations - Linux Team
İlgili Veri Merkezi:	Ankara 1 Veri Merkezi
Kök Sebebi Araştırılan Olay Özeti	
<p>20.02.2026 tarihinde Ankara 1 Veri Merkezi'nde yer alan ANKARA 1 – Yeni 1. Cluster'da, yeni node devreye alma çalışması sırasında Corosync (KNET) haberleşmesi kesintiye uğramış ve cluster quorum/membership kaybı nedeniyle HA üzerinden VM'lerde failover/taşıma işlemleri tetiklenmiştir.</p> <p>Sanallaştırma katmanı üretici destek incelemesi sonucunda, Cluster'a ait Corosync ağlarında uçtan uca MTU uyumsuzluğu (MTU mismatch) tespit edilmiştir. Bu uyumsuzluk, bazı paket boyutlarının karşı uç tarafından kabul edilmemesine (PMTUD uyarıları) ve Corosync'un down olmasına yol açarak kısa süreli servis kesintisi oluşturmuştur.</p>	
Kök Sebebi Araştırılan Olay Akışı ve Uygulanan Çözümler	
<p>15:39 civarında yeni node devreye alma çalışması kapsamında küme konfigürasyonu ve üyelik yapısı güncellenirken Corosync/KNET katmanında iletişim kararsızlığı oluşmuştur. Uçtan uca MTU uyumsuzluğu nedeniyle bazı paket boyutlarının karşı uç tarafından kabul edilmediği, buna bağlı olarak Corosync günlüklerinde PMTUD uyarılarının oluştuğu ve üyelik/quorum yapısının kararsız hale geldiği anlaşılmıştır. Quorum kararsızlığının stabil hale gelmemesi üzerine, mimarinin veri tutarlılığını korumaya yönelik HA/watchdog yaklaşımı devreye girmiş ve olası split-brain riskini engellemek amacıyla hostlar kontrollü şekilde self-fencing davranışı göstermiştir. Hostların yeniden başlaması sırasında sanal makinelerde yeniden başlama ve power-off etkileri oluşmuş, bu durum uygulama ve servis erişimlerine kısa süreli kesinti olarak yansımıştır.</p> <p>15:44 itibarıyla HA mekanizması sanal sunucuların uygun hostlar üzerinde otomatik olarak yeniden çalıştırılmasını başlatmış ve ortamın kademeli olarak normale döndüğü görülmüştür. Bu süreçte bazı VM'lerin HA tarafından otomatik olarak ayağa kaldırılmadığı, bazı VM'lerin ise yeniden başlatma sonrasında işletim sistemi veya servis seviyesinde müdahale gerektirdiği tespit edilmiştir. Bu nedenle 15:44–16:24 aralığında ilgili VM'lerde manuel start/restart işlemleri uygulanmış, konsol erişim kontrolleri gerçekleştirilmiş, kritik servislerin çalışırılığı doğrulanmış ve servis bağımlılıkları dikkate alınarak kademeli sağlık kontrolleri tamamlanmıştır. 16:24 itibarıyla ortam genelinde erişim ve servis doğrulamalarıyla olay etkisinin sonlandığı teyit edilmiştir.</p> <p>Olay sonrası yürütülen detaylı üretici incelemesinde, Corosync trafiğinin geçtiği ağlarında MTU standardizasyonunun uçtan uca sağlanmadığı netleştirilmiştir. Bulgular doğrultusunda Corosync/KNET ağında MTU standardizasyonu tamamlanmış, uçtan uca doğrulamalar gerçekleştirilmiş ve cluster değişiklik/devreye alma adımlarında runbook kullanımı operasyonel standart haline getirilmiştir.</p>	

Kök Sebebe Yönelik Uygulanan Çözümler

Olay anında hizmet sürekliliğinin sağlanması amacıyla HA mekanizmasının otomatik düzeltme aksiyonları işletilmiş ve ortamın durumu uçtan uca izlenmiştir. Sonrasında sanal sunucuların yalnızca erişilebilir olmasının yeterli olmadığı dikkate alınarak, kritik servisler özelinde servis sağlık kontrolleri ve erişim doğrulamaları uygulanmıştır. Otomatik açılma sonrasında manuel müdahale gerektiren VM'lerde açılış, konsol ve servis doğrulamaları yapılarak hizmet sürekliliği yeniden sağlanmıştır.

Kalıcı iyileştirme kapsamında Corosync/KNET ağında MTU standardizasyonu tamamlanmış, ilgili ağ segmentlerinde uçtan uca jumbo frame doğrulaması gerçekleştirilmiş ve cluster değişiklik/devreye alma süreçlerinde runbook kullanımı uygulamaya alınmıştır.

Kök Sebebe Yönelik Kalıcı Çözümler

Kök Sebep; Corosync/KNET trafiğinin geçtiği ağlarda uçtan uca MTU standardı sağlanmadığı için MTU mismatch oluşmuştur. Sanallaştırma katmanı üretici destek incelemesinde Corosync ağlarında PMTUD kaynaklı "possible MTU misconfiguration" uyarıları ile MTU asimetrisi doğrulanmıştır. Bu asimetri, Corosync membership ve quorum yapısının kararsız hale gelmesine, devamında Corosync'un down olmasına ve HA/fencing mekanizmalarının tetiklenmesine neden olmuştur.

Kalıcı Çözüm kapsamında;

- Corosync/KNET ağında MTU standardizasyonu tamamlanmıştır.
- İlgili ağ segmentlerinde uçtan uca jumbo frame doğrulaması gerçekleştirilmiştir.
- Cluster değişiklik ve devreye alma süreçlerinde runbook kullanımı uygulanmıştır.
- Runbook içeriğine MTU/Jumbo doğrulama ve değişiklik sonrası kontrol adımları dahil edilmiştir.

Kök Sebebe Yönelik Alınacak Aksiyonlar

Aksiyon 1:	Corosync/KNET ağında MTU standardizasyonu ve uçtan uca doğrulama	Sorumlu:	Linux Team	Hedef Tarih:	24.02.2026	Durum:	Tamamlandı.
Aksiyon 2:	Cluster değişiklik / devreye alma için Runbook kullanımının uygulanması	Sorumlu:	Linux Team	Hedef Tarih:	25.02.2026	Durum:	Tamamlandı.

Aksiyon Sonuç Değerlendirmesi

Sanallaştırma katmanı üretici çağrısının nihai değerlendirmesine göre olayın temel nedeni, Cluster'a ait Corosync/KNET ağlarında oluşan uçtan uca MTU mismatch'tir. Üretici incelemesinde PMTUD kaynaklı MTU uyumsuzluğu bulguları doğrulanmış; bu durumun Corosync membership ve quorum yapısını bozarak Corosync'un down olmasına, devamında ise HA/fencing ve VM failover süreçlerinin tetiklenmesine yol açtığı netleştirilmiştir.

Bu RCA kapsamında tanımlanan kalıcı aksiyonlar tamamlanmıştır. Corosync/KNET ağında MTU standardizasyonu sağlanmış, uçtan uca doğrulamalar gerçekleştirilmiş ve cluster değişiklik/devreye alma süreçlerinde runbook kullanımı operasyonel standart haline getirilmiştir. Uygulanan iyileştirmelerle birlikte aynı riskin tekrar etmesini önlemeye yönelik teknik ve operasyonel kontroller devreye alınmıştır.