KÖK SEBEP ANALİZ FORMU

Proje Adı:	GlassHouse Public Cloud
Tarih:	4.12.2025
İlgili İş Birimi:	Cloud Team
İlgili Veri Merkezi:	Ankara 1 Veri Merkezi

Kök Sebebi Araştırılan Olay Özeti

04.12.2025 Perşembe günü saat 19:03 itibarıyla, Ankara 1 Veri Merkezi'nde sanallaştırma platformunu besleyen erişim anahtarları (leaf switches) ve omurga anahtarları (spine switches) üzerinde CPU ve RAM (memory) kullanım değerlerinin anlık olarak pik seviyelere ulaştığı, ilgili ağ cihazlarının "Not Responding / Not Healthy" durumuna geçtiği ve buna bağlı olarak sanallaştırma platformuna ait fiziksel sunucular ile üzerlerinde çalışan sanal sunucuların (sanal makineler – Virtual Machine/VM) yaygın ölçekte erişilemez hale geldiği tespit edilmiştir.

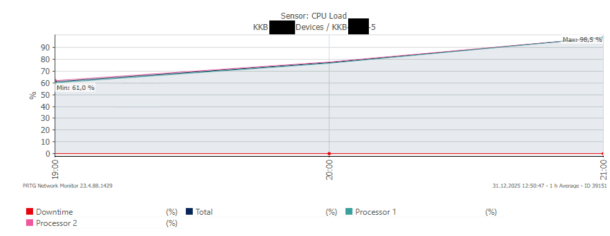
Yapılan incelemelerde, CH-6145 değişiklik kaydı kapsamında; değişiklik öncesi plan dahilinde bakım moduna (maintenance mode) alınan bir kümedeki (cluster) fiziksel sunucular üzerinde gerçekleştirilen donanım yazılımı güncellemesi (firmware upgrade) sonrasında beklenmedik şekilde, ilgili sunucuların bağlı olduğu anahtardan başlayarak yoğun tekil yönlendirme trafiği (unicast traffic) oluştuğu ve bununla birlikte MAC dalgalanması (MAC flapping / MAC flap) hareketleri gözlemlendiği anlaşılmıştır. Bu durum, leaf anahtarlar üzerinde port up/down davranışlarını tetiklemiş ve erişim katmanında kararsızlığa yol açmıştır.

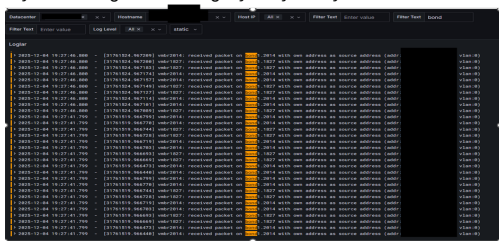
Söz konusu ağ anomalisi, sanallaştırma platformunun bağlı olduğu erişim katmanını doğrudan etkileyerek küme (cluster) üzerindeki tüm sanallaştırma sunucularında yaygın erişim problemlerine neden olmuştur. Olayın etki analizi kapsamında; veri depolama üniteleri (storage), güvenlik cihazları ve yedekleme sistemlerinde servis kesintisi gözlemlenmemiş; kesinti sanal sunucuların ağ erişimi ile sınırlı kalmıştır. Olayın herhangi bir siber güvenlik ihlali kaynaklı olmadığı değerlendirilmiş olup, ilgili süreçte bir siber güvenlik zafiyeti oluştuğuna dair bulguya rastlanmamıştır.

Kök Sebebi Araştırılan Olay Akışı ve Geçici Çözüm Uygulanması

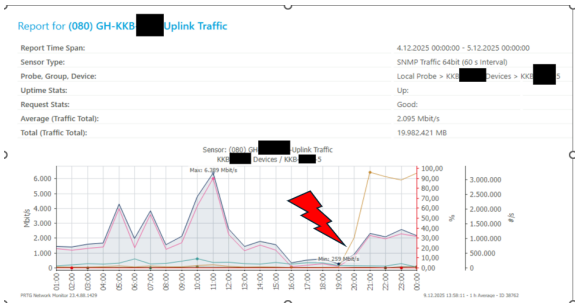
04.12.2025 günü saat 19:03'te, Ankara 1 Veri Merkezi'nde kurulu sanallaştırma platformunda yer alan sunucularda erişim problemi tespit edilmiştir. Olayın ilk dakikalarından itibaren GlassHouse teknik ekipleri ile ağ altyapı danışmanlık hizmeti alınan firmanın mühendisleri birlikte çalışmaya başlamış; etki alanı ve kök sebep analizi için eş zamanlı inceleme yürütülmüştür.

CH-6145 değişiklik kaydı kapsamında 04.12.2025 tarihinde saat 13:30 - 17:30 aralığında, kümede (cluster) yer alan sanal sunucular aktif taşıma (online migration) yöntemiyle diğer fiziksel sunuculara aktarılmış; akabinde bakım moduna (maintenance mode) alınan 3 adet fiziksel host üzerinde, üretici tarafından yayımlanan firmware/yazılım güncellemesi öncesinde yapılacak kaynak doğrulama kontrollerine geçilmeden önce sistem sağlığının görülmesi amacıyla yeniden başlatma (reboot) işlemi uygulanmıştır. Yeniden başlatma sonrasında gerçekleştirilen kontroller sırasında bir fiziksel ağ kartı portunun "down" duruma geçtiği tespit edilmiş; portun ağ tanımları hem fiziksel host hem de bağlı olduğu ağ anahtarı (switch) üzerinde doğrulanmıştır. İnceleme sürecinde, portun tekrar "up" duruma getirilmesi hedefiyle host üzerindeki ağ mimarisinde (bond/bridge) konfigürasyon değişikliği yapılmış; mevcut ağ konfigürasyonuna ait bond tanımında düzenlenme yapılarak trafik aynı köprü (bridge) üzerinden yönlendirilmiştir. Bu işlem, firmware upgrade öncesi kontroller kapsamında portun erişilebilirliğini sağlamak amacıyla uygulanmış olup, olası kapsam/etki sonuçları bu aşamada öngörülmeden gerçekleştirilmiştir.



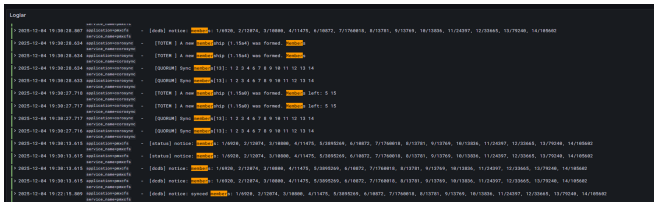


19:00 itibarıyla izleme (monitoring) sistemlerinde oluşan alarmlar ile olay ilk kez tespit edilmiş; sanallaştırma sistemlerinin bağlı bulunduğu ağ cihazlarında fiziksel kaynak kullanımının (CPU/RAM) kısa süre içinde tavan seviyelere ulaştığı gözlemlenmiştir. Eş zamanlı olarak ağ cihazları üzerinde olağandışı yoğunlukta port up/down trafiğinin tetiklendiği, MAC adres tablolarında hızlı ve tekrarlayan değişimler meydana geldiği ve ağ üzerinde MAC flapping davranışının başladığı anlaşılmıştır. İlk analizlerde, cloud ortamına hizmet veren küme (cluster) içerisinde ilgili ağ tanımının/etkisinin yaygınlaştığı; başlangıçta sınırlı sayıda fiziksel sunucudan gelen benzer log ve alarmların kısa süre içinde kümedeki diğer fiziksel sunuculardan da sırasıyla raporlandığı ve anomalinin cluster geneline yayıldığı gözlemlenmiştir. İlk müdahale kapsamında, anomalinin kaynağı olabileceği değerlendirilen bağlantılar ve sistemler üzerinde izolasyon çalışmaları başlatılarak ilgili kaynak sistemler tek tek tespit edilip ağdan ayrıştırılmış ve kapatılmıştır.



Date Time	Traffic Total (Volume)	Traffic Total (Speed)	Traffic In (Volume)	Traffic In (Speed)	Traffic Out (Volume)	Traffic Out (Speed)	Unicast In (Volume)	Unicast In (Speed)	Unicast Out (Volume)	Unicast Out (Speed)	Multicast In (Volume)	Multicast In (Speed)
4.12.2025 13:00:00 – 14:00:00	403.614 MB	1.901 Mbit/s	56.398 MB	266 Mbit/s	347.215 MB	1.636 Mbit/s	31.394.558 #	17.630 #/s	70.195.903 #	39.419 #/s	2.940 #	1,65 #/s
4.12.2025 14:00:00 – 15:00:00	671.016 MB	1.564 Mbit/s	157.601 MB	367 Mbit/s	513.415 MB	1.196 Mbit/s	67.195.333 #	18.667 #/s	108.753.125 #	30.212 #/s	6.261 #	1,74 #/s
4.12.2025 15:00:00 – 16:00:00	146.159 MB	341 Mbit/s	109.558 MB	255 Mbit/s	36.601 MB	85 Mbit/s	43.218.880 #	12.006 #/s	44.685.952 #	12.414 #/s	6.232 #	1,73 #/s
4.12.2025 16:00:00 – 17:00:00	228.212 MB	532 Mbit/s	150.173 MB	350 Mbit/s	78.040 MB	182 Mbit/s	57.166.406 #	15.881 #/s	62.852.177 #	17.460 #/s	6.287 #	1,75 #/s
4.12.2025 17:00:00 – 18:00:00	264.475 MB	616 Mbit/s	146.231 MB	341 Mbit/s	118.244 MB	276 Mbit/s	46.343.738 #	12.874 #/s	70.551.091 #	19.599 #/s	6.259 #	1,74 #/s
4.12.2025 18:00:00 – 19:00:00	110.930 MB	259 Mbit/s	69.542 MB	162 Mbit/s	41.388 MB	96 Mbit/s	24.972.748 #	6.937 #/s	79.506.969 #	22.087 #/s	6.181 #	1,72 #/s
4.12.2025 19:00:00 – 20:00:00	355.671 MB	909 Mbit/s	57.652 MB	147 Mbit/s	298.019 MB	762 Mbit/s	19.835.366 #	6.044 #/s	3.354.607.095 #	1.022.232 #/s	6.251 #	1,90 #/s
4.12.2025 20:00:00 – 21:00:00	426.464 MB	2.323 Mbit/s	25.368 MB	138 Mbit/s	401.096 MB	2.185 Mbit/s	6.650.116 #	4.318 #/s	5.000.263.356 #	3.247.030 #/s	3.766 #	2,45 #/s
4.12.2025 21:00:00 – 22:00:00	37.178 MB	2.080 Mbit/s	2.196 MB	123 Mbit/s	34.982 MB	1.957 Mbit/s	452.224 #	3.015 #/s	464.449.614 #	3.096.950 #/s	492 #	3,28 #/s
4.12.2025 22:00:00 – 23:00:00	933.464 MB	2.584 Mbit/s	104.968 MB	291 Mbit/s	828.496 MB	2.293 Mbit/s	22.995.062 #	7.587 #/s	9.035.284.019 #	2.981.224 #/s	10.301 #	3,40 #/s
4.12.2025 23:00:00 – 00:00:00	933.026 MB	2.174 Mbit/s	24.644 MB	57 Mbit/s	908.382 MB	2.117 Mbit/s	6.660.969 #	1.850 #/s	11.580.117.847 #	3.216.967 #/s	11.072 #	3,08 #/s

Ağ katmanında tespit edilen anomali ilerledikçe, sanallaştırma ortamına hizmet veren küme (cluster) içi iletişimin de olumsuz etkilendiği; düğümler arası erişim, sağlık kontrolleri ve yönetim katmanı üzerindeki sinyallerde tutarsızlıklar oluştuğu gözlemlenmiştir. Bu aşamada, olası veri bütünlüğü bozulması ve zincirleme etki riskini sınırlamak amacıyla sanallaştırma platformunda cluster yapısı kontrollü şekilde devre dışı bırakılarak ortamın stabilizasyonu hedeflenmiştir. Cluster kapanma/açılma adımları planlı biçimde yürütülürken, olayın yayılımını ve etkisini artırabilecek unsurların ayrıştırılması amacıyla ilgili network tanımları gözden geçirilmiş ve kullanım dışı olduğu belirlenen tanımlar (bridge) kontrollü şekilde devre dışı bırakılmıştır.



Stabilizasyon sürecinde, ağ üzerindeki dalgalanmayı azaltmak ve sorunun kaynağını daha net izole edebilmek amacıyla topoloji sadeleştirme yaklaşımı uygulanmıştır. Bu kapsamda, ağ cihazları ve fiziksel sunucular üzerinde bulunan yedekli bağlantılar (redundant links) geçici süreyle devre dışı bırakılarak iletişim yolları tekilleştirilmiş; böylece port up/down tetiklemelerinin ve MAC adres tablosu hareketlerinin azaltılması hedeflenmiştir. Eş zamanlı olarak hem ağ cihazları hem de host tarafında log/telemetri çıktıları takip edilerek, MAC flapping davranışının hangi segment ve hangi kaynaklarla korele ilerlediği analiz edilmiş; ayrıca ilgili anahtar (switch) üzerinde daha önce devreye alınmış olan ve mevcut işletimde sistemin bu şekilde stabil çalıştığı bilinen LACP BYPASS mekanizmasının aktif olduğu gözlemlenmiştir. Bu aşamada anomaliyi tetiklediği değerlendirilen bağlantı ve sistemler üzerinde kademeli izolasyon uygulanmıştır.

Yapılan izolasyon ve topoloji sadeleştirme adımlarının ardından, MAC flapping davranışına neden olan sistemler tespit edilerek devre dışı bırakılmış; ilgili hareketin ağ üzerinde durduğu ve cluster iletişimi açısından stabil sinyallerin geri geldiği doğrulanmıştır. Bu doğrulama sonrasında sanal sunucular kontrollü ve kademeli biçimde yeniden devreye alınmış; ancak ağ yedekliliğini sağlayan bileşenler/bağlantılar devreye alınmadan network katmanındaki topoloji tekil yapı üzerinden izlenmeye devam edilmiştir. Bu aşamadan sonra her adımda ağ davranışı ve sanallaştırma bileşenlerinin sağlık kontrolleri izlenerek servislerin kesinti öncesindeki sağlıklı çalışma durumuna geri döndüğü teyit edilmiştir. MAC flapping davranışına neden olduğu belirlenen ilgili fiziksel sunucu cluster dışı bırakılmış ve stabilite sürekliliği sağlanana kadar cluster içerisine yeniden dahil edilmemiştir.

Kök Sebebe Yönelik Geçici Çözümler

Geçici çözüm kapsamında, ağ üzerindeki kararsızlığı azaltmak ve etki alanını sınırlandırmak amacıyla ağ yedekliliği geçici olarak devre dışı bırakılarak topoloji tekilleştirilmiştir.

Bu süreçte, veri bütünlüğü riskini minimize etmek amacıyla sanallaştırma platformunda cluster yapısı kontrollü şekilde devre dışı bırakılarak stabilizasyon sağlanmış; olayın yayılımını artırabilecek unsurların ayrıştırılması için network tanımları gözden geçirilmiş ve kullanım dışı olduğu belirlenen tanımlar (bridge) kontrollü biçimde devre dışı bırakılmıştır.

Eş zamanlı olarak MAC flapping davranışı ile korele olduğu tespit edilen sistemler kademeli biçimde belirlenerek ağdan ayrıştırılmış ve ilgili hareketin ağ üzerinde durduğu doğrulanmıştır. Doğrulama sonrasında sanal sunucular kontrollü ve kademeli biçimde yeniden devreye alınmış; stabilite teyidi tamamlanana kadar ağ yedekliliğini sağlayan bileşenler/bağlantılar devreye alınmadan network katmanındaki topoloji tekil yapı üzerinden izlenmeye devam edilmiştir. Bu aşamadan sonra ağ üzerinde tekrar MAC flapping gözlemlenmediği ve ağ trafiğinin kararlı (stabil) hale geldiği teyit edilmiştir.

Kök Sebebe Yönelik Kalıcı Çözümler

Kalıcı çözüm kapsamında, Ankara 1 Veri Merkezi başta olmak üzere sanallaştırma platformu altyapısında fiziksel sunucuların daha hızlı ölçeklenebilmesi ve olası bir sorunda etki alanının azaltılabilmesi amacıyla fiziksel olarak birbirinden ayrıştırılmış birden fazla küme (cluster) mimarisi kurulacaktır. Bu kapsamda yeni kümenin kurulum çalışmalarına başlanmış olup yeni kümeler birbirinden bağımsız anahtarlama altyapısı (switching) üzerinde çalışacak şekilde tasarlanmıştır. Yeni küme (cluster) yapısı test edilmekte olup, mevcut problem yaşanan küme (cluster) aktarımı planlanmıştır.

Sanallaştırma platformunda fiziksel sunucuların küme içi iletişimini sağlayan Corosync/KNET haberleşmesinde oluşabilecek gecikme (latency) ve benzeri iletişim problemlerinin küme mimarisini etkilememesi amacıyla, Corosync/KNET trafiği için ayrı bir fiziksel ağ altyapısı kapalı bir ağ yapısında devreye alınacaktır. I/O ağı ise GH Public Cloud ağından bağımsız olacak şekilde; yalnızca fiziksel sunucu ve depolama (storage) sistemleri arasında çalışan kapalı (izole) ayrı bir fiziksel ağa taşınacaktır. İlgili ağın kurulumunun tamamlanmasını takiben sunucu ve storage bağlantılarının bu ağ üzerine taşınmasına yönelik geçiş çalışmaları planlanmıştır.

Ayrıca GlassHouse veri merkezlerinde yer alan anahtarlama altyapısında katman 2 (Layer 2) seviyesinde yaşanabilecek ağ problemlerinin tespiti ve etkisinin azaltılması amacıyla danışman firma ile görüşülerek önerilen konfigürasyon iyileştirmeleri ivedilikle uygulanacaktır. Olay sonrası üretici firma yönlendirmeleri doğrultusunda sanallaştırma platformunda sürüm yükseltmesi (version upgrade) planlanmış olup yeni küme (cluster) mimarisinde devreye alınacaktır.

Bunlara ek olarak, host ağ konfigürasyonlarında (bond/bridge/VLAN) yapılacak değişikliklerin standardizasyonu amacıyla kontrol listesi ve ikinci göz (peer review) yaklaşımı işletilecek; port up/down yoğunluğu, MAC flapping ve ağ cihazı CPU/RAM artışlarını korele edecek izleme ve alarm eşikleri gözden geçirilerek güncellenecektir. Switch tarafındaki işletimsel konfigürasyonların (ör. LACP BYPASS gibi) güncel envanteri çıkarılarak periyodik gözden geçirme sürecine dahil edilecektir.

Kök Sebebe Yönelik Alınacak Aksiyonlar

Aksiyon 1:	Sanallaştırma platformunun farklı kümelere (clusters) bölünmesi	**Sorumlu:**	Linux Ekibi	**Hedef Tarih:**	30.03.2026	**Durum:**	Devam Ediyor
Aksiyon 2:	Küme iletişim/kalp atışı ağının (cluster heartbeat – Corosync/KNET) ayrı fiziksel ağ üzerinde yapılandırılması	**Sorumlu:**	Infra Ekibi	**Hedef Tarih:**	30.03.2026	**Durum:**	Devam Ediyor
Aksiyon 3:	I/O ağının ayrı fiziksel ağ üzerinden yapılandırılması	**Sorumlu:**	Infra Ekibi	**Hedef Tarih:**	30.03.2026	**Durum:**	Devam Ediyor
Aksiyon 4:	Network anahtarlarında konfigürasyon sıkılaştırması	**Sorumlu:**	Network Ekibi	**Hedef Tarih:**	30.03.2026	**Durum:**	Devam Ediyor
Aksiyon 5:	Sanallaştırma platformu sürüm yükseltmesi (version upgrade)	**Sorumlu:**	Linux Ekibi	**Hedef Tarih:**	30.03.2026	**Durum:**	Devam Ediyor

Aksiyon Sonuç Değerlendirmesi