KÖK SEBEP ANALİZİ DETAY FORMU

Kayıt Numarası:	#368056
Proje Adı:	GlassHouse Cloud KKB Veri Merkezi
Tarih:	26.09.2024 18:09 - 21:40
İlgili İş Birimi:	GlassHouse Network & Security Team
İlgili Veri Merkezi:	GlassHouse Cloud KKB Veri Merkezi

Kök Sebebi Araştırılan Olay Özeti

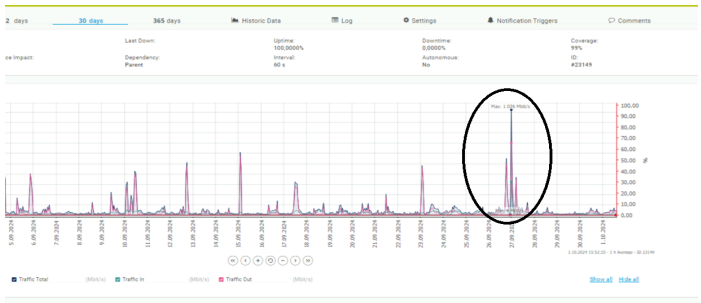
GlassHouse KKB Veri Merkezinde 26.09.2024 tarihinde 18:19 - 21:40 saat aralığında erişim sorunu yaşanması.

Tespit Edilen Kök Sebep Açıklaması

GlassHouse olarak, altyapımızda hizmet alan müşterilerimize etkisi olacak tüm çalışmaları planlı bir şekilde ilerleterek, ilgili veri merkezinde hizmet alan müşterilerimize duyurular ile bildirimlerde bulunmaktayız. Herhangi bir beklenmedik durum yaşanma ihtimaline karşılık da çalışmalarımızı müşterilerimize en az etki edecek saat aralığı olan 03:00 - 07:00 aralığında gerçekleştirmekteyiz.

GlassHouse değişiklik prosedürüne göre, kesinti riski olmayacak şekilde değerlendirilmiş network iyileştirme çalışmamız, gece saat 03:00'den sonra yapılması gerekirken, yaşanılan bir operasyonel aksaklıktan dolayı saat 18:09 saatinde gerçekleştirilmiştir.

Normal şartlar altında saat 03:00'den sonra yapılması planlanan, GlassHouse Cloud Turksat veri merkezindeki ana omurga switch'lerine yeni network switch çifti bağlanması çalışması, ilgili değişiklik yönetim prosedürümüzün işletilmesindeki operasyonel bir aksaklıktan dolayı 26.09.2024 18:09:30 saatinde gerçekleştirilmiştir. Bu bağlantı sırasında switchler arasında yapılması gereken LACP konfigürasyonu henüz tamamlanmadığı için, bağlantının yapıldığı core switch'ler üzerinde MAC adresi çakışmasına ve bunun sonucu olarak da network'ümüz içerisinde "broadcast storm" yaşanmasına sebep olmuştur. Yaşanılan "broadcast storm"un yarattığı beklenmeyen trafiğin görseli aşağı paylaşılmıştır.



Ana omurgamızın sonlandırıldığı core switchler Master ve Slave yapıda çalışmaktadır. Bu switch çifti aralarındaki yedekliliği CLAG protokolü ile sağlamaktadır. Yaşanılan kısa aralıklı kesintilerin incelemesi sonrasında, yaşanılan söz konusu broadcast storm'un sonucu olarak 26.09.2024 saat 18:09'dan itibaren CLAG protokolünde ve bağlantı portlarında tutarsızlık yaşandığı tespit edilmiştir. Bu tutarsızlık sırasında ise switch'ler üzerinde çalışmakta olan portlarda kesinti meydana gelmiştir.

Aşağıdaki görselde belirtilen örnek logdan da görülebileceği üzere, Master ve Slave switch arasındaki bond bağlantılarının up-down olduğu görülmektedir.

```
2024-09-26T18:18:26.342135+03:00 clagd[9884]: UpdateProtoDownFlags Interface bond1 add flags 0x2 del flags 0x0 final flags 0x2
```

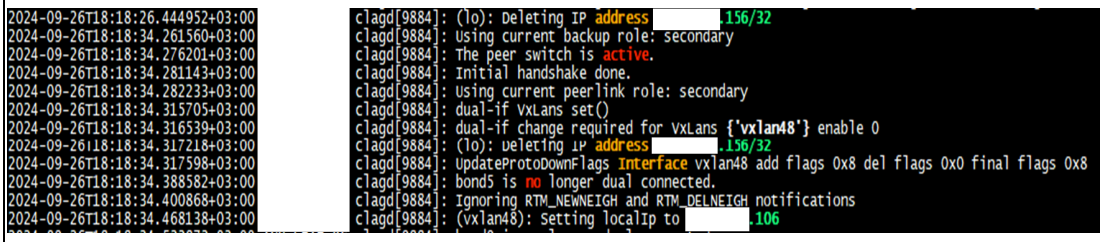
```
2024-09-26T18:09:07.705950+03:00 clagd[9884]: bond8 is no longer dual connected.

2024-09-26T18:09:09.471464+03:00 clagd[9884]: bond8 is now dual connected.
```

Aşağıdaki CLAG bazında loglar görülmektedir. Bu loglar, iki CLAG switch'i arasındaki iletişimin tamamen kesildiğini göstermektedir. Switch, CLAG üzerindeki tüm bağlantıları devre dışı bırakmıştır.

```
2024-09-26T18:18:25.678239+03:00 clagd[9884]: Peer communication timeout. No data has been received from the peer for 20 seconds.
2024-09-26T18:18:25.688198+03:00 clagd[9884]: Peer link is down; checking if the peer switch is alive.
2024-09-26T18:18:25.688426+03:00 clagd[9884]: HealthCheck: Rapid detection start
2024-09-26T18:18:26.339912+03:00 clagd[9884]: The peer switch is no longer active
2024-09-26T18:18:26.341270+03:00 clagd[9884]: Setting Wait on All Clag Bonds Down Event
```

Bu flap sırasında ana omurga switch'leri sistemler üzerinde tutulan MAC adreslerini tekrar sorgulamak için broadcast sorgusu göndermeye başlamıştır. Turksat Veri Merkezi ile KKB Veri Veri Merkezi arasında kullanmakta olduğumuz Layer2 network devresi üzerinden ise bu broadcast sorguları KKB Veri Merkezi'mize yayılmıştır. Turksat Veri Merkezi'mizdeki ana omurga switch'lerinde yaşanan CLAG flap sorununun aynısının KKB Veri Merkezi'mizdeki ana omurga switch'lerde de yaşanmasına sebep olmuştur. Bu sırada KKB Veri Merkezi'mizde hizmet alan müşterilerimizde sık aralıklar ile kesintiler yaşanmıştır.

Sorun anında aşağıdaki loglardan görülebileceği gibi, Master switch, peer'ı olan Slave switch'e erişemediğinde yedeklilik ortamının bozulduğunu düşünüp, tüm trafiği üzerine almak için uplink'lere anons ettiği IP'sini değiştirmektedir. Yaptığımız incelemeler ve dış kaynaklar ile olan incelemelerimiz sonucunda Master ve Slave olarak çalışmakta olan omurga switch çiftlerimizin, CLAG protokolü gereği beklenen davranışları sergilediği ve konfigurasyonal bir bug olmadığı netleştirilmiştir. Fakat aradaki sorunun saniye içinde birden çok kez gerçekleşmesi sonucunda, trafik üzerinde kesintiler meydana gelmiştir.



Kesinti yaşanan zaman diliminde ana problem tespit edildikten sonra her iki veri merkezimizdeki Slave konumundaki switch'lerin devre dışı bırakılması için ilgili konfigürasyonlar yapılmış fakat cihazın komutları kabul etmediği görülmüştür. Akabinde cihazlara "shutdown" komutu gönderilmiştir. Bu noktadan sonra ilgili switch'lerin uzaktan kapalı görünmesine rağmen, hala çalışmaya devam ettiği ve soruna sebep olduğu tespit edilmiştir. Veri Merkezlerine sorun anında gönderilen danışmanlarımız tarafından fiziksel olarak kapatılması ile yaşanan sorun 21:40'da giderilmiştir.

Kök Sebebe Yönelik Kalıcı Çözümler

1 - Bu gibi yedekli yapıda çalışan altyapılar üzerinde, çakışan MAC adresi ve sonucunda oluşacak broadcast storm sorunu yaşanması olasılıklar dahilindedir. Bu tarz sorunlardan omurgamızın etkilenmemesi için, altyapımızda kullanılan Leaf switch'lerimizde "LACP Bypass Off" koruması aktiflenecektir. Bu sayede çakışan MAC adresi sorunu yaşandığında ana omurga switch'lerinde CLAG flapping yaşanmasının önüne geçilecektir.

2- Omurgamız üzerinde kullanılan ve Layer2 seviyesinde çalışan cihazlar arasında herhangi bir "broadcast storm" yaşanması ihtimaline karşılık, tüm switch'ler üzerindeki Broadcast, Unknown Unicast Flooding ve Multicast frameleri engellemek için BUM policy'leri sıkılaştırılacaktır.

Kök Sebebe Yönelik Alınacak Aksiyonlar

Aksiyon 1:	Leaf switch'lerde LACP Bypass Off konfigurasyonunun yapılması	**Sorumlu:**	Mert Şahbandar Network & Security Manager	**Hedef Tarih:**	25.10.2024	**Durum:**	**Tamamlandı.**
Aksiyon 2:	Broadcast, Unknown Unicast flooding ve Multicast policy'lerinin sıkılaştırılması	**Sorumlu:**	Mert Şahbandar Network & Security Manager	**Hedef Tarih:**	25.10.2024	**Durum:**	**Tamamlandı.**
Aksiyon 3:	Disiplin sürecinin işletilmesi	**Sorumlu:**	Devrim Akpınar	**Hedef Tarih:**	15.10.2024	**Durum:**	**Tamamlandı.**

Aksiyon Sonuç Değerlendirmesi