گزارش حمله به
زیرساخت رایانش ابری آروان

در دیتاسنتر IR-THR-AT1

در روزهای پایانی اسفند ۱۳۹۹ زیرساخت رایانش ابری آروان در دیتاسنتر IR-THR-AT1 با حملات سایبری مواجه شد که هدف از آن‌ها تخریب و حذف اطلاعات مشتریان بود.

در این حملات، فعالیت سایر محصولات ابر آروان شامل DNS، CDN، ویدیو پلتفرم، فضای ذخیره‌سازی ابری، هم‌چنین رایانش ابری در سایر دیتاسنترهای آروان بدون مشکل بود اما در حدود ۱۶درصد از مشتریان غیررایگان آروان که از دیتاسنتر IR-THR-AT1 استفاده می‌کردند، از این حملات متاثر شدند.

نشانه‌هایی از این حملات در روزهای یک‌شنبه و دوشنبه ۲۴ و ۲۵ اسفند دیده و منجر به بروز اختلالات محدودی شد اما با آغاز حملات گسترده و متفاوت در شامگاه سه‌شنبه و آسیب‌رسانی به دیتای مشتریان در این دیتاسنتر، تمام دسترسی‌ها را به‌منظور جلوگیری از پیش‌روی آسیب‌رسانی قطع کردیم.

در این حمله، آن گروهی از مشتریان دچار مشکل اساسی شدند که از داده‌های خود نسخه پشتیبان نداشتند، یا معماری آن‌ها به شکل ابرزی[1] نبود و به شکل Multi Availability Zone طراحی نشده بودند.

با توجه به نوع ذخیره‌سازی اطلاعات در رایانش ابری آروان، در این حمله هکر هیچ‌گونه دسترسی به دیتای مشتریان ابر آروان پیدا نکرد و تنها موفق به آسیب زدن به اطلاعات و پاک کردن بخشی از آن شد.

در این‌جا باید از نظرات و راهنمایی‌های دوستان متخصص‌مان در کشور که حتا برخی از آنان در شرکت‌های رقیب ابر آروان فعالیت دارند، هم‌چنین تیم‌های خارجی از کشورهای آلمان و ترکیه و نمایندگان‌شان تشکر کنیم؛ که با تجربه‌ها و توصیه‌هایشان در مسیر حل مساله با ما همراه بودند.

۱.Cloud Native

خط زمانی واقعه
و اقدامات

یک‌شنبه ۲۴ اسفند

آغاز رویداد[۲]

ساعت ۱۱:۳۳ یک‌شنبه شب، یک رویداد غیرعادی روی دو سوییچ در یک VPC در دیتاسنتر IR-THR-AT1 ابر آروان مشاهده شد. برآورد اولیه تیم فنی اشکال سخت‌افزاری بود که با بازیابی سوییچ‌ها این اشکال رفع شد.

دوشنبه ۲۵ اسفند

شناسایی امکان حمله‌ی سایبری

در ساعت ۴ صبح دوشنبه، دوباره اختلال روی سوییچ‌های IR-THR-AT1 اتفاق افتاد. به‌دلیل تکرار الگو، احتمال حمله‌ی سایبری داده شد.

از این زمان تا ساعت ۷ صبح روز بعد، تیم‌های ابر آروان روی موضوع کار کردند و در چند ساعت اول موفق شدند سیستم را به حالت طبیعی برگردانند.

سپس برای جلوگیری از حمله‌ی احتمالی، تغییراتی در شبکه‌ی مدیریتی دیتاسنترهای IR-THR-AT1 و IR-THR-MN1 و NL-AMS-SR1 داده شد، اما کارشناسانی که به دیتاسنتر IR-THR-AT1 اعزام شده بودند به‌دلیل خستگی، در اعمال تغییرات در شبکه‌ی این دیتاسنتر دچار اشتباه شدند و فقط بخشی از تغییرات را اعمال کردند.

۲.Incident

سه‌شنبه ۲۶ اسفند

حمله‌ی گسترده و آسیب‌رسانی به دیتای مشتریان

در حالی‌که تیم‌های امنیتی به هر دو دیتاسنتر برای بررسی دقیق اعزام شده بودند در ساعت ۵:۳۰ عصر به‌شکل ناگهانی از طریق همان بخشی از شبکه‌ی مدیریتی که هم‌چنان فعال بود، دیتاسنتر IR-THR-AT1 مورد حمله قرار گرفت.

این حملات ساعت ۸ شب با حجم بسیار بالایی ادامه پیدا کرد و تعدادی از سرورهای ذخیره‌سازی و پردازشی با هدف حذف اطلاعات و از کار انداختن سرویس مورد حمله قرار گرفتند.

با آغاز آسیب‌رسانی به دیتای مشتریان، تمام دسترسی‌ها به این دیتاسنتر قطع شد تا از توسعه‌ی آسیب‌رسانی جلوگیری شود؛ بلافاصله اینترنت و شبکه‌ی مدیریتی، هر دو به‌شکل کامل قطع و علاوه‌بر کارشناسان امنیتی، کارشناسان و اعضای تیم فنی به محل دیتاسنتر اعزام شدند تا بدون نیاز به دسترسی از راه دور –که ریسک گسترش یا تکرار حمله را افزایش می‌داد– به بررسی موضوع بپردازند.

ابر آروان برای حفظ پایداری، از هر داده (آبجکت) سه نسخه‌ی مختلف در سه دیسک متفاوت در داخل سه سرور مختلف نگهداری می‌کند، تا اگر یک یا چند دیسک یا حتا یک یا چند سرور از دسترس خارج شوند، به داده‌ها آسیبی وارد نشود. اما در حمله‌ی اتفاق افتاده، به‌شکل هم‌زمان تعداد بالایی سرور مورد آسیب قرار گرفتند، این موضوع سبب شد، علاوه‌بر حذف حدود ۱۰۰ ترابایت از یک پتابایت اطلاعات این دیتاسنتر، برخی اطلاعات، هر ۳ نسخه‌ی خود را از دست بدهند.

در تحلیل اولیه مشخص شد که از مجموع بیش از ۹۷درصد اطلاعات، حداقل یک نسخه از اطلاعات وجود دارد. اما به‌دلیل توزیع‌شدگی سه‌درصد اطلاعات حذف شده در تمام کلاستر، زیرساخت ذخیره‌سازی در ریسک از دست رفتن کل اطلاعات قرار گرفت.

ادامه‌ی سه‌شنبه شب

تشکیل کمیته‌ی بحران

بلافاصله با تشکیل تیم بحران درصدد حل مشکل و هم‌زمان اطلاع‌رسانی به کاربران برآمدیم.
در کنار تیم‌های پشتیبانی، مشتریان و اطلاع‌رسانی، در این مرحله، چهار تیم فنی شکل گرفت:

- **تیم یک**: مسوول مراقبت از دیتاسنتر IR-THR-MN1 برای پیش‌گیری از رویداد مشابه
- **تیم دو**: کار متمرکز روی زیرساخت ذخیره‌سازی دیتاسنتر IR-THR-AT1 برای برگرداندن ۱۰۰ ترابایت اطلاعات و پایدارسازی کلاستر ذخیره‌سازی
- **تیم سه**: کار متمرکز روی کل زیرساخت رایانش ابری در IR-THR-AT1 تا به‌محض رفع اشکال فضای ذخیره‌سازی، سرویس دوباره به مدار برگردد.
- **تیم چهار**: مسوول کالبدشکافی[۳] و ایمن‌سازی[۴]

با پیش‌بینی آسیب به دیتای کاربران و زمان‌بر بودن بازگشت سرویس، از کاربران خواسته شد برنامه‌ریزی Disaster Recovery خود را فعال کنند تا با استفاده از نسخه‌ی پشتیبان خود در سایر دیتاسنترهای آروان یا دیگر فراهم‌کنندگان زیرساخت، سرویس خود را مجدد راه‌اندازی و از وارد شدن خسارت به سرویس خود جلوگیری کنند.

به‌رغم تاکید به «پشتیبان‌گیری اطلاعات حیاتی از سوی مشتری» در متن «شروط فنی استفاده از خدمات زیرساخت رایانش ابری آروان[۵]»، بسیاری از کاربران با آروان تماس گرفته و اعلام کردند که نسخه‌ی پشتیبانی در دست ندارند.

۳.Forensics
۴.Hardening
۵.https://۲۱c.io/iaastc

چهارشنبه ۲۷ اسفند

بازگشت اطلاعات

پس از حدود ۳۰ ساعت کار پیوسته، با فیکس‌کردن و یکپارچه‌سازی داده در سطح کلاستر، امکان دسترسی به اطلاعات در ساعت ۱۰:۳۰ صبح چهارشنبه فراهم شد. در این زمان حدود ۹۷.۳ درصد از اطلاعات برگردانده شده بود. از این نقطه، پیچیدگی جدیدی به بحران اضافه شد چون آسیب و اختلال آن سه‌درصد اطلاعات می‌توانست سبب از بین رفتن کل کلاستر و بازیابی ناموفق شود.
از این زمان، تیم بر اصلاح یکپارچگی داده متمرکز شد تا کلاستر بالا بیاید.

- **مشکل نخست**: باید دقت شود که این سه‌درصد دیتای از دست رفته، مربوط به سه‌درصد از مشتریان نبود بلکه سه‌درصد از تمام اطلاعات تمام مشتریان این دیتاسنتر است؛ پس احتمالن اکثریت مشتریان بخش ناچیزی از اطلاعات‌شان آسیب‌دیده بود. از طرفی گاهی این بخش ناچیز ممکن است با اثرگذاری بر پارتیشن بوت مانع بالا آمدن ابرک شده یا با ایجاد مشکل در پارتیشن سیستم، کار سیستم‌عامل را با اخلال مواجه کند یا با قرار گرفتن در پایگاه داده کاربر، آن را از کارکرد عادی بازدارد.

- **مشکل دوم**: به‌طور کلی قطع ناگهانی سیستم‌عامل‌ها از زیرساخت ذخیره‌سازی سبب از دست رفتن اطلاعات در حال ذخیره‌سازی روی دیسک و افزایش احتمال آسیب‌دیدگی می‌شود.

پنج‌شنبه ۲۸ اسفند

حل مشکلات در بازیابی و بازکردن دسترسی مشتریان / سطح آسیب به سرورهای ابری

تا ساعت ۴ صبح روز پنج‌شنبه دو مشکل گفته شده تقریبن حل شدند؛ کلاستر بالا آمد و تیم‌های دیگر هم کارشان تمام شده بود. از این ساعت، به‌مرور دسترسی مشتریان به سرورهای ابری باز شد.
متاسفانه با بازشدن دسترسی به پاپ‌سایت و بررسی دقیق‌تر وضعیت ابرک‌ها مشخص شد حذف کم‌تر از سه درصد از اطلاعات کل دیتاسنتر، سبب تاثیرگذاری روی بخش گسترده‌ای از سرورهای ابری شده است.
میزان سکتورهای آسیب‌دیده در Block Storage متصل به ابرک، هم‌چنین نوع فایل‌سیستم، سیستم‌عامل و پایگاه داده‌ها سبب می‌شد که سطح آسیب‌پذیری برای مشتریان مختلف طیف گسترده‌ای داشته باشد.
در چنین موقعیتی، هر کدام از سیستم‌عامل‌ها رفتار متفاوتی دارند، از بین سیستم‌عامل‌های ویندوز و نسخ مختلف لینوکس و فایل‌سیستم‌های‌شان، برخی ساده‌تر و برخی با سختی بیش‌تر بازیابی می‌شوند. هم‌زمان با به‌کارگیری روش‌های بازیابی سیستم‌عامل‌ها، مقاله‌ی آموزشی آن‌ها نیز منتشر و به مرور تکمیل شد.
در میان فایل‌سیستم‌های مشتریان ابر آروان، EXT4 سازگارتر و XFS و NTFS آسیب‌پذیرتر بودند.
در این زمان، بخشی از ابرک‌ها بدون هیچ اقدامی بدون مشکل قابل استفاده بودند، بخش دیگری با Reboot و درنهایت ترمیم boot loader به مرحله‌ی استفاده می‌رسیدند و برخی نیاز به ترمیم فایل‌سیستم یا بازیابی‌های پیشرفته‌تر داشتند.

ادامه‌ی پنج‌شنبه

افزایش ۴ برابری ظرفیت تیم پشتیبانی به ۸۰ نفر

از ظهر روز چهارشنبه، تمام خطوط تلفنی ابر آروان و تمام ظرفیت تیم پشتیبانی برای پاسخ‌گویی به مشتریان به‌کار گرفته شده بودند. با بازگشایی دسترسی کاربران در صبح روز پنج‌شنبه، ظرفیت تیم پشتیبانی با حمایت تیم‌های فنی و تیم‌های کوچ ابری، چهار برابر شد.

مشتریان فعال ابر آروان در دیتاسنتر IR-THR-AT1 در حدود ۷۰۰۰ سرور ابری داشتند که تا روز پنج‌شنبه تعداد ۱۱۰۰ سرور ابری از سوی مشتریان برای بررسی به تیم‌های فنی ابر آروان ارجاع شدند.

به‌رغم افزایش ظرفیت و پاسخ‌گویی ۲۴ ساعته، حجم بالای مشتریان نیازمند کمک سبب شد فرآیند پاسخ‌گویی و حل مساله‌ی آنان با کندی همراه باشد. در ادامه مشکلات پیش‌آمده در کلاستر در مقاطعی، فرآیند بازیابی را متوقف کرد.

ادامه‌ی پنج‌شنبه

پرداخت جبران خدمات تعهد شده[۶] به تمام مشتریان زیان‌دیده با فرض حل مشکلات/ فراهم آوردن زیرساخت رایگان فضای ذخیره‌سازی ابری برای تسهیل فرآیند پشتیبان‌گیری کاربران

با تصور پایداری کلاستر ذخیره‌سازی در روز پنج‌شنبه، مدت زمان دردسترس نبودن سرویس به نسبت هزینه‌ی ماهانه‌ی هر یک از مشتریان محاسبه و مبلغی بالاتر از سقف جبران خدمات تعهد شده، به کیف پول کاربران واریز شد.

به‌علاوه مبلغی که در روزهای قطعی از کیف پول کاربران کم شده بود نیز به حساب آنان برگردانده شد.

هم‌چنین فضای ذخیره‌سازی ابری (تا سقف ۱۰ ترابایت) تا پایان فروردین ۱۴۰۰ به‌شکل رایگان در اختیار تمام مشتریان دیتاسنتر IR-THR-AT1 ابر آروان قرار گرفت تا در فرآیند پشتیبان‌گیری با مشکل فضای ذخیره‌سازی مواجه نباشند.

قرارداد جبران خدمات تعهد شده[۷] برای جبران دردسترس نبودن زیرساخت است که سطح و میزان پوشش آن در شرایط استفاده و قراردادهای ابر آروان آمده است.

متاسفانه روند روزهای آتی مشخص کرد که کلاستر ذخیره‌سازی با مشکلاتی همراه بوده و هنوز برای استفاده مشتریان آماده نیست.

۶. Service Level Agreement (SLA)
۷. https://www.arvancloud.com/fa/sla

جمعه ۲۹ اسفند

حجم درخواست بسیار بالای کاربران هم‌زمان برای بازیابی اطلاعات و بروز مشکلات زیرساختی

روز جمعه، هم‌زمان حجم بالایی از کاربران برای درست کردن فایل‌سیستم یا پشتیبان‌گیری دیتا مشغول به کار شدند. به‌دلیل مشکلات پیش‌آمده و ریکاور کردن کلاستر ذخیره‌سازی در یک فشار زمانی کوتاه، کلاستر موفق به تهیه‌ی سه نسخه از تمام داده‌ها نشده بود، هم‌چنین برای ساخت ابرک‌های جدید برای انتقال اطلاعات روی آن‌ها نیاز به فضای بیش‌تری بود و در نتیجه باید ظرفیت کلاستری که به‌سختی آسیب‌دیده بود افزایش پیدا می‌کرد. برای رفع این مشکل، به میزان ۴۰۰ ترابایت دیسک به کلاستر اضافه شد.
تزریق منابع جدید، یعنی وزن‌دهی دوباره‌ی دیسک‌ها[۸] که سبب درگیری شدید زیرساخت و قفل شدن کلاستر شد. به همین دلیل، در روز ۲۹ اسفند، وضعیت بحرانی‌تر شد.
در این مقطع چند متخصص باتجربه‌ی ایرانی برای انتقال تجربه، در کنار تیم ابر آروان قرار گرفتند، اما هم‌چنان بهبودی در وضعیت کلاستر ایجاد نشد.

شنبه ۳۰ اسفند و یک‌شنبه ۱ فروردین

کمک تیم‌های آلمانی و ترک و تداوم وضعیت کلاستر

در روزهای شنبه و یک‌شنبه، تلاش برای بهبود زیرساخت به‌منظور انجام سریع‌تر بازیابی در حال انجام بود، با توجه به این‌که پارامترهای مختلفی از جمله زیرساخت شبکه، پارامترهای سیستم‌عامل و پیکربندی زیرساخت ذخیره‌سازی به‌طور مشترک نیازمند تغییر و بهبودسازی بودند، فرآیند بازیابی سرورهای ابری متوقف و تمام تمرکز روی بهبود زیرساخت گذاشته شد.
در این مرحله با توجه به حجم بسیار بالای بازیابی و فشار روی کلاستر و عدم تاثیرگذاری پیکربندی‌های انجام شده از تیم‌های متخصص آلمانی و ترک برای کمک استفاده شد که اقدامات آنان نیز تاثیر چشم‌گیری در بهبود وضعیت نداشت.

دوشنبه ۲ فروردین

تلاش برای رفع مشکل کلاستر از طریق رفع اشکال نرم‌افزاری و اقدامات اولیه برای راه‌اندازی کلاستر جدید

به‌طور خلاصه مشکل اصلی کلاستر ذخیره‌سازی تاثیر تسلسل دو مشکل ReMirroring-Storm و یک Memory Leak در لایه‌ی نرم‌افزاری Ceph در شرایط خاص بود که هم‌افزایی آن‌ها سبب به اغما رفتن کلاستر می‌شد.
پس از تلاش‌های ناموفق تیم ذخیره‌سازی آروان، هم‌چنین بی‌نتیجه ماندن نظرات مشاوران داخلی و خارجی، تیم System Development آروان تلاش کرد با Patch کردن نرم‌افزاری و هم‌زمان افزایش منابع، مشکل را حل کنند.

چهارشنبه ۴ فروردین

تداوم احیای کلاستر

با انجام مجموعه پیکربندی‌های جدید، وضعیت کلاستر ذخیره‌سازی به آرامی رو به بهبود رفت. فرآیند Patch نرم‌افزاری نتیجه درخور توجهی در بر نداشت و از دستور کار خارج شد.

۸. Rebalance

جمعه ۶ فروردین

احیای کلاستر

از صبح جمعه وضعیت کلاستر ذخیره‌سازی پایدار شد و در نتیجه بالا آوردن کلاستر جدید نیز از دستور کار خارج شد.
با پایدارسازی کلاستر، بازیابی سرورهای ابری مشتریان با افزایش تعداد نفرات تیم‌های پشتیبانی و فنی به ۱۰۵ نفر از سر گرفته شد.

یک‌شنبه ۸ فروردین

سه ماه استفاده‌ی رایگان رایانش ابری و فضای ذخیره‌سازی برای تمام مشتریان آسیب‌دیده

ابر آروان با انتشار خبر [۹] و ارسال ایمیل به آگاهی مشتریان رساند که تا پایان بهار ۱۴۰۰ استفاده از محصول رایانش ابری و فضای ذخیره‌سازی ابری خود را برای تمام مشتریانی که در جریان حملات پایان سال به زیرساخت پردازش ابری در دیتاسنتر IR-THR-AT1 آسیب دیده‌اند، رایگان کرده است.
با توجه به تفاوت میزان مصرف هر مشتری، هزینه‌ی سه ماه بهار براساس مصرف اسفند ۹۹ این مشتریان محاسبه شد و به‌مرور و به‌شکل خودکار، به حساب کاربری آنان اضافه شد.
هم‌چنین به‌منظور تسهیل فرآیند پشتیبان‌گیری برای تمام مشتریان آسیب‌دیده، محصول فضای ذخیره‌سازی ابری تا پایان بهار امسال تا سقف ۱۰ ترابایت برای هر مشتری و بدون محدودیت ترافیک، رایگان شد.
برخی از مشتریان ابر آروان در مراحل مختلفی که امکان دسترسی به سرورهای‌شان فراهم شده بود، اقدام به جابه‌جایی سرورها به سایر دیتاسنترهای ابر آروان یا سایر فراهم‌کنندگان زیرساخت کرده بودند که این دو امکان شامل این دسته از مشتریان هم شده است.

۹. https://rnc.io/at۳m

پنج‌شنبه ۱۲ فروردین

پایان بررسی تمام ابرک‌ها

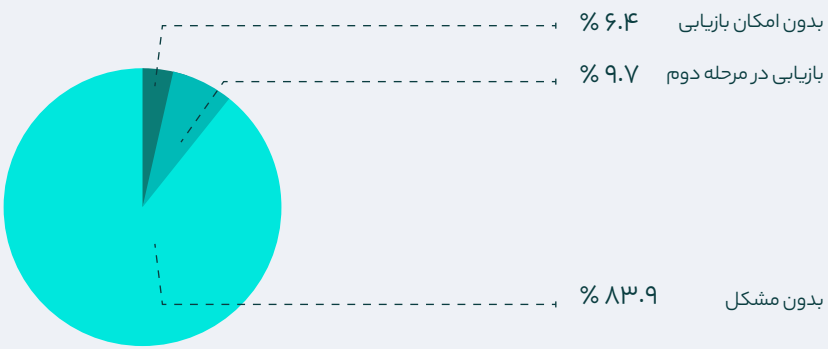
با تداوم پشتیبانی و بازیابی سرویس مشتریان، تا روز پنج‌شنبه، تمامی ابرک‌های موجود در دیتاسنتر IR-THR-AT1 که قابلیت بررسی سیستمی را داشتند، مورد بررسی اولیه قرار گرفتند. از این میان سیستم‌عامل ۸۳.۹ درصد بدون مشکل بود یا مشکل آن به‌کمک تیم‌های فنی برطرف شد. هم‌چنین ۹.۷ درصد ابرک‌های بررسی شده در دستور کار برای مرحله دوم بازرسی و بازیابی قرار گرفتند. متاسفانه امکان بازیابی ۶.۴ درصد از ابرک‌ها وجود نداشت که تلاش شد دیتای این ابرک‌ها به ابرک جدید منتقل شود.

نگاه کلی به آمار پشتیبانی
در این بازه‌ی زمانی

تیم پشتیبانی اولیه	افزایش ۴ برابری تیم پشتیبانی	افزایش دوباره‌ی تیم پشتیبانی
۲۰ نفر	۸۰ نفر	۱۰۵ نفر

تماس تلفنی	پاسخ‌گویی به تیکت
۸۳۰۰	۳۶۰۰

۷۰۰۰ ابرک بررسی شده



گزارش فنی
از پایدارسازی کلاستر ذخیره‌سازی
و رفع مشکلات ثانویه

چند روز پس از بازیابی اولیه‌ی کلاستر ذخیره‌سازی، مشکلات ثانویه این کلاستر سبب شد روند بازیابی ابرک‌ها با وقفه و اختلال چند روزه‌ای مواجه شود. در این بخش به توضیح این مشکل و راه‌حل‌های تیم فنی آروان می‌پردازیم.

حجم درخواست بسیار بالای کاربران هم‌زمان برای بازیابی اطلاعات و بروز مشکلات زیرساختی

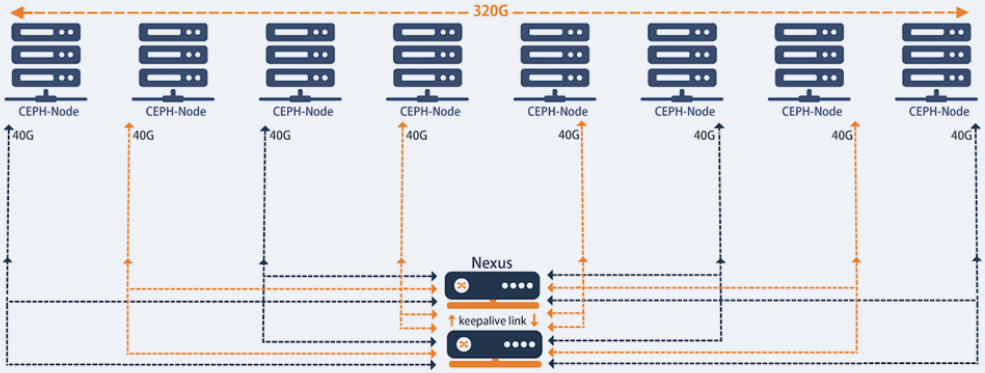
روز جمعه ۲۹ اسفند۱۳۹۹، هم‌زمان حجم بالایی از کاربران برای درست کردن فایل‌سیستم یا پشتیبان‌گیری دیتا مشغول به کار شدند. به‌دلیل مشکلات پیش‌آمده و ریکاور کردن کلاستر ذخیره‌سازی در یک فشار زمانی کوتاه، کلاستر موفق به تهیه‌ی سه نسخه از تمام داده‌ها نشده بود، هم‌چنین برای ساخت ابرک‌های جدید برای انتقال اطلاعات روی آن نیاز به فضای بیش‌تری بود و در نتیجه باید ظرفیت کلاستری که به‌سختی آسیب‌دیده بود نیز افزایش پیدا می‌کرد. برای رفع این مشکل، به میزان ۴۰۰ ترابایت دیسک به کلاستر اضافه شد.
تزریق منابع جدید، یعنی وزن‌دهی دوباره‌ی دیسک‌ها (Rebalance) که سبب درگیری شدید زیرساخت و قفل شدن کلاستر می‌شود. به همین دلیل، در این روز، وضعیت بحرانی‌تر شد.
به‌طور خلاصه مشکل اصلی کلاستر ذخیره‌سازی تاثیر تسلسل دو مشکل ReMirroring-Storm و یک Memory Leak در لایه‌ی نرم‌افزاری Ceph در شرایط خاص بود که هم‌افزایی آن‌ها سبب به اغما رفتن کلاستر می‌شد. تعداد بالایی از Placement groupهای کلاستر ذخیره‌سازی در حالت خطا قرار گرفتند و میزان سرعت نوشتن و خواندن اطلاعات از سوی کاربران (ابرک‌ها) کاهش و به عدد صفر نزدیک شد.
کلاستر در چنین موقعیتی و در هنگامی‌که در حالت ریکاور برای اصلاح وضعیت PGها قرار می‌گرفت، به دلایلی که گفته شد با flapشدن OSDها (سرویس‌های نگهدارنده‌ی اطلاعات) دوباره سبب به اغما رفتن کلاستر و شروع دوباره‌ی یک چرخه معیوب می‌شدند.
برای حل مشکل در طول چهار شبانه‌روز، مجموعه اقدامات بسیاری انجام و درنهایت منجر به احیای کلاستر شد. در ادامه برخی از اقدامات فنی ابر آروان برای حل این مشکل را شرح داده‌ایم.

ابعاد کلاستر

کلاستر ذخیره‌سازی ابر آروان در دیتاسنتر IR-THR-AT1 در شهریور ۱۳۹۶ ایجاد شده است. این کلاستر در طول این‌سال‌ها بهبود و به‌روز رسانی شده و درنهایت با عملکرد مقبولی در حال سرویس‌دهی به کاربران بوده است.
زیرساخت‌های شبکه، تنظیمات سیستم‌عامل و تنظیمات کلاستر در وضعیت مناسبی بوده است، اما زمانی‌که کلاستری با این ابعاد –با ظرفیت ۱.۵ پتابایت و از دسترس خارج شدن حدود ۱۰۰ ترابایت اطلاعات به‌شکل ناگهانی– با مشکل مواجه می شود، زمان بسیاری برای رفع مشکل و پایداری مجدد کلاستر نیاز است. مشکلی اصلی تیم ابر آروان، فشردگی بسیار بالای زمانی و تلاش برای حل مشکلات در کوتاه‌ترین زمان ممکن بوده است.

ارتقای زیرساخت شبکه و ارتقای منابع

در نخستین اقدام RAM تمام سرورهای کلاستر ذخیره‌سازی شامل MON, MGR, OSD از 128GB به 384GB ارتقا پیدا کرد. موضوعی که می‌توان گفت تاثیری اندک روی وضعیت عمومی کلاستر گذاشت. در واقع OSDها به حافظه‌ی بیش‌تر نیاز نداشتند، آن‌ها فقط به هنگام اختلال (Memory Leak) شروع به مصرف بیش‌تر می‌کردند و در کم‌تر از چند ثانیه تمام Memory موجود را هم اشغال می‌کردند.
گام بعدی بهینه‌سازی و بهبود زیرساخت‌های شبکه بود، تا تمام نودها بتوانند در بهترین وضعیت ممکن با یک‌دیگر ارتباط برقرار کنند. ارتباط OSDها برای ریکاور کردن، سه حالت مختلف را پوشش می‌دهد؛ ارتباط بین OSDهای داخل یک سرور، ارتباط بین OSDها بین دو سرور مختلف متصل به یک سوییچ و درنهایت ارتباط بین OSDها بین سوییچ‌های مختلف که از طریق VPC به یک‌دیگر متصل شده‌اند.
در این بخش ارتباط بین سرورها از 10gbps به 20gbps ارتقا یافت هم‌چنین ارتباط سوییچ‌های VPC از 60gbps به 80gbps افزایش پیدا کرد. (ارتباط بین سرورها در طراحی کلاسترهای جدید ابر آروان به‌شکل پیش‌فرض 40gbps و ارتباطات آپلینک بین سوییچ‌ها 200gbps است)



یکی از نکات بسیار مهم در این وضعیت، شناسایی، تمرکز و کاهش TCP Retransmission در شبکه‌ی سرورهای کلاستر ذخیره‌سازی است.

به‌کمک دستورهای netstat و sar می‌توان وضعیت TCP Retransmission در شبکه را مشاهده کرد، هم‌چنین می‌توان هم‌زمان به‌کمک IPERF3 یا راهکارهای مشابه، بار شبکه را در حالت بیشینه قرار داد و مجدد وضعیت را مورد بررسی قرار داد:

```
$ netstat –s | grep retransmitted
  184042627 segments retransmited
```

```
$ sar –n ETCP 1

12:50:44 PM  atmptf/s  estres/s retrans/s isegerr/s  orsts/s
12:50:46 PM    0.00    0.00  189.00    0.00    2.00
12:50:47 PM    0.00    0.00   61.00    0.00    2.00
12:50:48 PM    0.00    0.00   12.00    0.00    0.00
12:50:49 PM    0.00    1.00   67.00    0.00    0.00
```

```
$ iperf3 –c [destination] –P 20 –t 100

SENDER START
Connecting to host [destination], port 5201
[ 15] local LOCAL port 37535 connected to REMOTE port 5208
[  4]  7.00–8.00  sec  111 MBytes  932 Mbits/sec  0  588 KBytes
[  6]  7.00–8.00  sec  112 MBytes  937 Mbits/sec  0  506 KBytes
[  8]  7.00–8.00  sec  112 MBytes  935 Mbits/sec  0  539 KBytes
[ 10]  7.00–8.00  sec  111 MBytes  926 Mbits/sec  0  489 KBytes
[ 12]  7.00–8.00  sec  111 MBytes  930 Mbits/sec  0  471 KBytes
[ 14]  7.00–8.00  sec  110 MBytes  923 Mbits/sec  0  587 KBytes
[ 16]  7.00–8.00  sec  111 MBytes  930 Mbits/sec  0  574 KBytes
[ 18]  7.00–8.00  sec  111 MBytes  934 Mbits/sec  0  564 KBytes
[ 20]  7.00–8.00  sec  111 MBytes  934 Mbits/sec  0  419 KBytes
[ 22]  7.00–8.00  sec  111 MBytes  929 Mbits/sec  0  303 KBytes
[ 24]  7.00–8.00  sec  111 MBytes  927 Mbits/sec  0  404 KBytes
[ 26]  7.00–8.00  sec  111 MBytes  932 Mbits/sec  0  327 KBytes
```

```
[ 28] 7.00–8.00  sec  111 MBytes  929 Mbits/sec  0   380 KBytes
[ 30] 7.00–8.00  sec  111 MBytes  928 Mbits/sec  0   380 KBytes
[ 32] 7.00–8.00  sec  111 MBytes  930 Mbits/sec  0   409 KBytes
[ 34] 7.00–8.00  sec  111 MBytes  931 Mbits/sec  0   344 KBytes
[ 36] 7.00–8.00  sec  112 MBytes  935 Mbits/sec  0   448 KBytes
[ 38] 7.00–8.00  sec  110 MBytes  926 Mbits/sec  0   444 KBytes
[ 40] 7.00–8.00  sec  110 MBytes  926 Mbits/sec  0   529 KBytes
[ 42] 7.00–8.00  sec  111 MBytes  929 Mbits/sec  0   458 KBytes
[SUM] 7.00–8.00  sec 2.17 GBytes 18.6 Gbits/sec  0
```

معمولن در توصیه‌های مربوط به بهبود و کاهش TCP Retransmission پیشنهاد می‌شود، کیفیت ارتباطات فیزیکی، فیبر و SFP مورد توجه قرار بگیرد، اما در موقعیت ابر آروان، مشکل از این بخش‌ها نبود و دو اصلاح مهم کمک کرد که TCP Retransmission کاهش یابد. در مجموع باید تلاش کرد همواره این عدد کم‌تر از ۳درصد از کل پکت‌های رد و بدل شده در واحد ثانیه باشد.

این دو اصلاح، یکی به‌روزسانی firmware کارت‌های شبکه و مورد مهم‌تر خاموش کردن فرآیند checksum روی کارت شبکه در هنگام ارسال و دریافت ترافیک بود:

https://www.kernel.org/doc/html/latest/networking/checksum-offloads.html

```
$ ethtool --offload eth0 rx off tx off
Actual changes:
rx-checksumming: off
tx-checksumming: off
    tx-checksum-ipv4: off
    tx-checksum-ipv6: off
tcp-segmentation-offload: off
    tx-tcp-segmentation: off [requested on]
    tx-tcp6-segmentation: off [requested on]
```

بهبود تنظیمات کلاستر Ceph

بخش مهمی از اقدامات انجام شده تلاش برای بهینه‌سازی تنظیمات Ceph و تغییر گام‌به‌گام متغیرها در لحظات مختلف و با توجه به شرایط مختلف بود.
همان‌طور که توضیح داده شد برای پایدار شدن کلاستر Ceph و اصلاح وضعیت PGها که منجر به پایداری دسترسی به اطلاعات می‌شود، کلاستر باید در وضعیت ریکاور قرار می‌گرفت، اما مشکل اصلی زمانی رخ می‌داد که چند دقیقه پس از قرار گرفتن کلاستر در وضعیت ریکاور، OSDها شروع به down و up شدن می‌کردند و این OSD flapها مهم‌ترین عامل ناپایداری و عدم بهبود وضعیت PGها و Objectها بودند. این چرخه‌ی معیوب همواره ادامه داشت و کلاستر نمی‌توانست مقاصد مطمین و پایداری برای دسترسی به اطلاعات و ایجاد یک نقشه‌ی مطمین از وضعیت PGها و Objectها را در خود بسازد.
با توجه به این‌که این اتفاق پس از رفتن به حالت ریکاور اتفاق می‌افتاد، نخستین حدس ما در دامنه‌ی سرویس Ceph، بالا بودن مقدار op/s و اعداد پیش‌فرض ریکاور بود. ما حدس زدیم با توجه به این‌که کلاستر تغییرات کلانی در وضعیت PGها و OSDهای خود دیده است، شاید یکی از پارامترهای مربوط به مقدار backfilling یا recovery بالاست که منجر به exhaust شدن OSDها و restart شدنشان می‌شود. به‌سرعت از این موضوع اطمینان پیدا کردیم و دوباره تمامی این اعداد را در حالت کم و پایین قرار دادیم:

```
osd_max_backfills 1
osd_recovery_max_active 1
osd_recovery_max_single_start 1
osd_recovery_op_priority 10
```

پس از اطمینان از این موضوع، دقت و تمرکز را روی اعداد recovery گذاشتیم تا ببینیم op/s و recovery throughput روی مقدار کمی باشد. خروجی ceph –s همین موضوع را به ما نشان می‌داد. op/s و سرعت بازیابی بسیار پایین آماده بود اما ارتباطی با کم کردن فشار روی OSDها و Flap شدن‌شان نداشت.

```
recovery: 11MiB/s, 14keys/s, 2objects/s
```

در این موقعیت سعی کردیم با بررسی OSDهایی که در این مدت Flap شدند، تلاش کنیم ببینیم آیا می‌توانیم به یک الگوی خاص و مشخص برسیم؟ در این‌باره، موارد مختلف را بررسی کردیم؛ پراکندگی این OSDها محدود به سرورهای خاص نمی‌شد، هیچ ارتباطی بین درصد utilization این OSDها و نسبت Flap شدن‌شان وجود نداشت و...

سعی کردیم رفتار یک OSD خاص را هدف قرار دهیم و آن را به‌طور دقیق بررسی کنیم.

```
$ sudo docker stats |grep ceph_osd_219
177fb403b141  ceph_osd_219    26.95%  3.591GiB / 377.8GiB
177fb403b141  ceph_osd_219    28.12%  4.139GiB / 377.8GiB
177fb403b141  ceph_osd_219    29.30%  4.984GiB / 377.8GiB
...
177fb403b141  ceph_osd_219    55.22%  23.019GiB / 377.8GiB
177fb403b141  ceph_osd_219    57.38%  24.291GiB / 377.8GiB
177fb403b141  ceph_osd_219    59.18%  25.739GiB / 377.8GiB
177fb403b141  ceph_osd_219    52.13%  26.304GiB / 377.8GiB
...
177fb403b141  ceph_osd_219    66.72%  101.481GiB / 377.8GiB
177fb403b141  ceph_osd_219    62.60%  102.672GiB / 377.8GiB
177fb403b141  ceph_osd_219    64.20%  103.211GiB / 377.8GiB
...
177fb403b141  ceph_osd_219    127.42%  148.536GiB / 377.8GiB
177fb403b141  ceph_osd_219    127.42%  149.409GiB / 377.8GiB
177fb403b141  ceph_osd_219    127.42%  151.967GiB / 377.8GiB
```

چیزی که برای ما نمایان بود این بود که چند دقیقه پس از استارت شدن OSD، مصرف Memory آن OSD کم‌کم افزایش پیدا می‌کرد و این موضوع آن‌قدر ادامه می‌یافت که تمام RAM سرور پر شود. در این وضع، زمانی‌که تمامی RAM سرور اشغال می‌شود، OOM Kill اتفاق می‌افتد و OSD Process را terminate می‌کند.

OOM Kill چیست؟

در سیستم‌عامل وضعیتی به نام Out Of Memory و فرآیندی به نام Out of Memory Killer برای محافظت کرنل سیستم‌عامل وجود دارد. هنگامی‌که مموری به‌شکل کامل با یک یا چند Process مصرف شود، این خطر وجود خواهد داشت که سیستم‌عامل به‌طور کامل Crash کند و سیستم از دسترس خارج شود، کرنل برای محافظت از خود این فرآیند را آغاز می‌کند و فرآیندی که بیش‌ترین مصرف Memory دارد را Kill خواهد کرد. به‌طور مشخص، بروز این اتفاق سبب Killشدن ناگهانی OSD و در نتیجه Flap شدن آن‌ها و ناپایدار کردن فرآیند این بازیابی می‌شود. این موضوع کلاستر را وارد یک حلقه‌ی معیوب می‌کند و بهبود وضعیت کلاستر را متوقف می‌کند.

https://www.kernel.org/doc/gorman/html/understand/understand۰۳۰.html

در این موقعیت سعی کردیم دو موضوع را بسیار سریع امتحان کنیم.
نخستین مورد بررسی پارامتر osd_memory_target بود که مقدار رم اختصاص داده شده به OSDها را در کلاستر تعیین می‌کرد. در کلاستر این مقدار را برابر با ۴ گیگابایت برای هر OSD تعیین کرده بودیم. با توجه به این‌که بسیاری از OSDها مصارفی نزدیک به این عدد داشتند، برای تست، موقت این مقدار را on the fly با injectargs به مقدار ۸ گیگابایت رساندیم.
دومین مورد، امتحان کردن memory limit روی کانتینر OSDها بود. این موضوع را بسیار سریع با گرفتن runlike از چند OSD container برای نمونه و اعمال hard limit روی memory آن‌ها انجام دادیم. اعمال این محدودیت نیز تاثیری در مشکل Memory Leak نداشت، چون با بیشینه شدن مصرف Memory هر Container اتفاق مشابه داخل آن تکرار می‌شود و OOM_Killer رفتار مشابهی را انجام خواهد داد.
پس از مشخص شدن این خروجی‌ها، با هم‌فکری سعی کردیم تا مواردی‌که به نظرمان به‌طور مستقیم بر مصرف Memory روی OSDها تاثیر دارد را شناسایی و سپس اقدامات لازم برای کاهش مصرف Memory آن‌ها را انجام دهیم.

نخستین گام ما برای بهینه‌تر کردن مصرف رم OSDها، تغییر در مقدار PG Log بود. هر نوع تغییر در وضعیت PGها و هر نوع transaction log در سطح کلاستر به عنوان PG Log روی OSDها ثبت می‌شود. ثبت این وقایع به Ceph کمک می‌کند تا به هنگام بازیابی با بررسی این لاگ‌ها با سرعت بسیار بالاتری بازیابی کند. اما با توجه به شرایط کلاستر که همواره OSDها در حال flap هستند و mapping مربوط به PGها همواره در حال تغییر است، ما حدس زدیم که احتمالن حجم بسیار بالایی از رم را PG Logها و ثبت این وقایع استفاده می‌کنند. این موضوع را با استفاده از گرفتن dump_mempool از چند OSD که در لاگ flapبرای آن‌ها ثبت شده بود، ارزیابی کردیم:

```
ceph daemon osd.[id] dump_mempools
```

سپس مقدار pg_log_entries را برای این بازه از مقدار ۱۰۰۰۰ به ۵۰۰ کاهش دادیم.

```
# last value 10000
osd_max_pg_log_entries 500

# last value 3000
osd_min_pg_log_entries 500
```

در گام بعدی باید مطمین می‌شدیم که این حجم از PG Logهایی که تا به آن لحظه روی OSDها ثبت شده‌اند با اعمال این تغییر، حتمن سبک‌تر می‌شوند و عملیات PG log trimming روی آن‌ها اعمال می‌شود. برای این کار مقدار threshold مربوط PG log trimming روی هر OSD را به‌طور دقیق برابر با مقدار PG log entries قرار دادیم:

```
# last value 10000
osd_pg_log_trim_max: 500
# last value 100
osd_pg_log_trim_min: 500
```

پس از اعمال این تغییرات روی تمامی OSDها، انتظار داشتیم تا فرآیند PG log trimming روی OSDها آغاز شود. پس از کمی انتظار و ارزیابی دقیق وضعیت چند OSD، برخلاف انتظار ما هیچ تغییری روی PG Logها اتفاق نیفتاد و هیچ فرآیند trimming روی هیچ OSDیی شروع نشد. کمی بیش‌تر بررسی کردیم و متوجه شدیم با توجه به وضعیت کلاستر و مقدار درخور توجه PGهای غیر active/clean، هیچ کدام از پارامترهای PG log و PG log trim در این موقعیت روی کلاستر اعمال نمی‌شوند.

در این موقعیت با توافق داخلی و بررسی جوانب مختلف تصمیم گرفتیم تا PG Log تمامی OSDهای کلاستر (بیش از صدها OSD) را به‌شکل offline و دستی trim کنیم.

برای این کار باید بسیار محتاط عمل می‌کردیم؛ سرور به سرور و OSD به OSD جلو می‌رفتیم تا کم‌ترین فشار به کلاستر، آن هم در این شرایط، وارد شود. برای اطمینان از این موضوع باید تمامی تمهیدات لازم برای جلوگیری از بازیابی، جابه‌جایی PG و هر پردازش اضافی روی کلاستر را متوقف می‌کردیم. مطمین شدیم تمامی فلگ‌های زیر در این بازه حتمن روی کلاستر اعمال شده‌اند:

```
noout,norecover,norebalance,noscrub,nodeep-scrub
```

سپس اسکریپتی نوشتیم تا به‌ترتیب با iterate روی تک‌تک سرورها و OSDها، این فرآیند را به‌طور manual روی آن‌ها و PGهای آن‌ها اعمال کند. در قلب این اسکریپت دو عمل مهم انجام می‌شد. گرفتن فهرست PGهای قرار گرفته روی OSD مقصد و انجام فرآیند PG log trim روی آن PGها.

```
# get pgs from osd
ceph-objectstore-tool --op list-pgs --data-path [osd-path]

# trim pg log of specific pgid
ceph-objectstore-tool --data-path [osd-path] --pgid [pgid] --op trim-pg-log
```

با این‌که این فرآیند تمام خودکار بود و به‌کمک اسکریپت انجام می‌شد، اما این فرآیند زمان بسیاری از ما گرفت. برخی OSDها بسیار سریع بین یک تا دو دقیقه ولی برخی OSDها تا ۳۰ دقیقه فرآیند PG log trimشان طول می‌کشید.

چون احتمال می‌دادیم این فرآیند بین ۱۲ تا ۲۴ ساعت طول بکشد، اجازه دادیم این فرآیند به‌شکل جداگانه انجام شود و ما به‌طور موازی هم‌چنان به بررسی دقیق‌تر مشکل و موارد دیگر بپردازیم.

جلوگیری از OOM Kill شدن OSDها

در این مدت متوجه شدیم سه OSD مشکل جدی پیدا کرده‌اند و استارت نمی‌شوند. با بررسی اولیه لاگ‌های آن‌ها، متوجه شدیم که rocksdb آن‌ها corrupt شده است، با خطای Compaction error: Corruption: block checksum mismatch مواجه می‌شوند و امکان initialize اولیه را ندارند. نمونه ای از این خطا به‌شکل زیر است:

```
  -8> 2021-04-01 21:21:05.177415 7fdb7ec4d700  3 rocksdb: [/build/ceph-m3XNYa/ceph-12.2.13/src/
rocksdb/db/db_impl_compaction_flush.cc:1591] Compaction error: Corruption: block checksum mismatch
  -7> 2021-04-01 21:21:05.177472 7fdb7ec4d700  4 rocksdb: (Original Log Time 2021/04/01-
21:21:05.177375) [/build/ceph-m3XNYa/ceph-12.2.13/src/rocksdb/db/compaction_job.cc:621] [default]
compacted to: base level 1 max bytes base 268435456 files[36 2 0 0 0 0 0] max score 0.00, MB/sec: 306.1 rd,
152.0 wr, level 1, files in(36, 2) out(1) MB in(44.0, 85.7) out(64.4), read-write-amplify(4.4) write-amplify(1.5)
Corruption: block checksum mismatch, records in: 485190, records dropped: 693

  -6> 2021-04-01 21:21:05.177477 7fdb7ec4d700  4 rocksdb: (Original Log Time 2021/04/01-
21:21:05.177405) EVENT_LOG_v1 {"time_micros": 1617295865177390, "job": 3, "event": "compaction_
finished", "compaction_time_micros": 444273, "output_level": 1, "num_output_files": 1, "total_output_
size": 67522337, "num_input_records": 357972, "num_output_records": 357279, "num_subcompactions":
1, "num_single_delete_mismatches": 0, "num_single_delete_fallthrough": 0, "lsm_state": [36, 2, 0, 0, 0, 0,
0]}
  -5> 2021-04-01 21:21:05.177480 7fdb7ec4d700  2 rocksdb: [/build/ceph-m3XNYa/ceph-12.2.13/src/
rocksdb/db/db_impl_compaction_flush.cc:1275] Waiting after background compaction error: Corruption:
block checksum mismatch, Accumulated background error counts: 1
```

```
  -4> 2021-04-01 21:21:05.177524 7fdb89311f80 -1 rocksdb: submit_transaction error: Corruption: block
checksum mismatch code = 2 Rocksdb transaction:
Put( Prefix = _ key = (SER_0000000000045117_USER_)0x00303030)0886363.00000000000000189910)
Value size = 173)
Put( Prefix = _ key = (SER_0000000000045117_USER_)0x005f6661)stinfo) Value size = 186)
```

عمل force termination که سیستم‌عامل برای فرآیند OSDها به‌دلیل پر شدن حافظه ایجاد می‌کرد، موجب آسیب زدن به rocksdbهای مربوط به OSDها می‌شد. برای جلوگیری از آسیب‌دیدگی OSDهای بیش‌تر، تصمیم گرفتیم با نوشتن یک اسکریپت ساده که از اجرای پیوسته‌ی آن به‌کمک Monit یا هر Daemon مشابه بشود اطمینان پیدا کرد، وضعیت Memory را به‌شکل پیوسته روی OSD Serverها را چک کنیم، و اگر از یک بیشینه‌ای افزایش پیدا کرد، Container مرتبط با OSD دچار مشکل شده را Restart کند. مهم‌ترین تفاوت این restart دستی این است که پردازش OSD به‌شکل graceful stop می‌شد که از تخریب ساختار OSD و محتوای آن جلوگیری می‌کرد.

```
#!/bin/bash

### Check available memory
free_mem=$(free -g |grep Mem |awk {(print $7)})



### Restart the top osd with memory consumption
if [[ $free_mem -lt 50 ]];then
 ### Check if any restart process is already running
 process_count=$(ps aux |grep ((docker restart)) |grep -v ((grep)) |wc -l)

 if [[ $process_count < 1 ]];then
```

```
  osd_number=$(ps aux --sort -rss |head  -n 10 |grep osd  |awk -F (ceph-) {(print $3)} |cut -d/) -f1 |head -n
1)
  sudo docker restart ceph_osd_$osd_number
 else
  exit 0
 fi
fi
```

افزایش سرعت عملیات Trim روی Snapshotها

درخواست‌های Trim برای Snapshotهای PGها در یک صف به نام snap trim queue قرار می‌گیرند، کلاستر در وضعیتی قرار داشت که صف snap trim queue بسیار شلوغ بود و نیاز داشتیم تا هر PG که در وضعیت Clean قرار می‌گیرد بسیار سریع پردازش شود و از صف خارج شود. ما سرعت این فرآیند را با افزایش اولویت و افزایش هم‌زمانی بهبود دادیم.

```
# default 5
osd_snap_trim_priority 25

# default 2
osd_max_trimming_pgs 4

# default 4
osd_pg_max_concurrent_snap_trims 8
```

متغیرهای مربوط به timeout فرآیندهای بازیابی و Suicide را افزایش دادیم:

```
osd_recovery_thread_suicide_timeout 900
osd-recovery-thread-timeout 1200
```

بررسی و رفع Bottleneckها

تمام نودهای کلاستر ذخیره‌سازی، تمام OSDها و در گام بعدی PGها مورد بررسی دقیق قرار گرفت. یکی از نودها به‌دلیل داشتن IRQ بالا به‌شکل کامل از مدار خارج شد. سپس گام‌به‌گام شروع به از مدار خارج کردن OSDهایی کردیم که Latency بالاتر نسبت به میانگین کلاستر داشتند.

افزایش فشار تدریجی روی کلاستر

از طریق افزایش گام‌به‌گام سه متغیر مهم max_backfill, max_active، هم‌چنین اولویت‌دهی به فرآیند بازیابی از طریق متغیر recovery_op_priority فشار روی کلاستر را افزایش دادیم.

- نکته: در نظر داشته باشید که این تغییرات به‌دلیل شرایط کلاستر و افزایش سرعت بازگشت به حالت استفاده است و برای کلاستر در حالت عادی توصیه نمی‌شود.

```
# last osd_max_backfill 1
osd_max_backfill 50


# last osd_recovery_max_active 1
osd_recovery_max_active 12

# last osd_recovery_op_priority 1
osd_recovery_op_priority 63
```

متغیرهای sysctl

ابر آروان برای کلاستر ذخیره‌سازی خود از نسخه‌ی Lowlatency کرنل استفاده می‌کند. با این وجود از تنظیم سراسری برخی از پارامترهای کرنل برای قرار گرفتن در حالت Lowlatency باید اطمینان پیدا کرد. برای نمونه، در فرآیند بازیابی، تعداد بالایی کانکشن TCP بین سرورها برقرار و بسته می‌شود. در این فرآیند تعداد بسیار بالایی کانکشن در وضعیت TIME_WAIT قرار می‌گیرد و سبب می‌شود سیستم در وضعیتی قرار گیرد که کانکشن جدیدی نتواند باز کند.

تنظیمات مربوط به TCP را در حالت زیر قرار دادیم:

```
net.ipv4.tcp_low_latency=1
net.ipv4.tcp_fastopen=1
net.ipv4.tcp_sack = 1
net.ipv4.tcp_max_tw_buckets = 500000
net.ipv4.tcp_tw_reuse = 1
```

هم‌چنین مهم است متغیرهای Network Buffers و Connections در حالت بهینه قرار بگیرند:

```
net.core.netdev_max_backlog
net.core.somaxconn
net.core.rmem_max
net.core.wmem_max
```

مقدار vm.min_free_kbytes را هم از قبل، برابر با یک گیگابایت قرار داده بودیم تا کرنل همیشه یک گیگابایت فضای آزاد Memory برای سیستم نگه دارد.

```
vm.min_free_kbytes = 1048576
```

اطمینان از خاموش بودن Connection Tracking

برای درگیری کم‌تر networking stack سرورها، مطمین شدیم connection tracking برای ارتباط بین سرورهای استوریج غیرفعال است.

```
$ iptables –t raw –I OUTPUT –o [interface] –j NOTRACK
$ iptables –t raw –I PREROUTING –i [interface] –j NOTRACK
```

وصله‌ی کد Ceph برای حل مشکل مدیریت مموری

کلاستر ذخیره‌سازی در دیتاسنتر IR-THR-AT1 از نسخه‌ی ceph-v12.2.13 استفاده می‌کند، با مشاهده‌ی رفتاری شبیه به مموری لیک، ایشوترکرِ ceph به‌دقت مورد بررسی قرار گرفت، بهبودهای مرتبط به Memory Leak در نسخه‌های دیگر مورد بررسی قرار گرفت. یکی از مشکلات گزارش از یک اشکال مرتبط به memory pool برنامه در مشکل شماره ۴۶۰۲۷ بود:

https://tracker.ceph.com/issues/46027

bufferlist c_str() sometimes clears assignment to mempool

Sometimes c_str() needs to rebuild underlying buffer::raw.

It that case original assignment to mempool is lost.

این تغییر روی نسخه‌ی 12.2.13 انتقال پیدا کرد، اما تاثیر مهمی روی کلاستر نداشت.

سه نشانه‌ی مهم سبب شد، روشن شود که مشکل پیش‌آمده مربوط به memory fragmentation است:

- رفتاری که در موردِ مموری دیده می‌شد، نشان می‌داد که کرنل امکان آزادسازی مموری را ندارد، در حالی‌که خود برنامه (کانتینرهای OSDها) هیچ استفاده‌ای از فضای مموری اشغال شده نداشتند.

- به هنگام رخ دادن مموری فرگمنتیشن، allocation زمان‌بر خواهد شد و برنامه کند می‌شود. کند شدن ceph و مشکلی که در ارتباط با OSDها دیده می‌شد تاییدکننده‌ی اختلال در allocation بود.

- در فرآیندِ بازیابی، تعدادِ بالایی allocation کوچک نیاز خواهد بود. در نتیجه در وضعیت ویژه‌ی کلاستر، سیستم به‌شدت مستعد memory fragmentation بود.

در نسخه‌های بعدی (ماژور آپدیت‌ها که در شرایط DR امکان مهاجرت به آن وجود نداشت، برای جلوگیری از memory fragmentation تغییرات مهمی داده شد، از جمله می‌توان به تغییر زیر اشاره کرد:

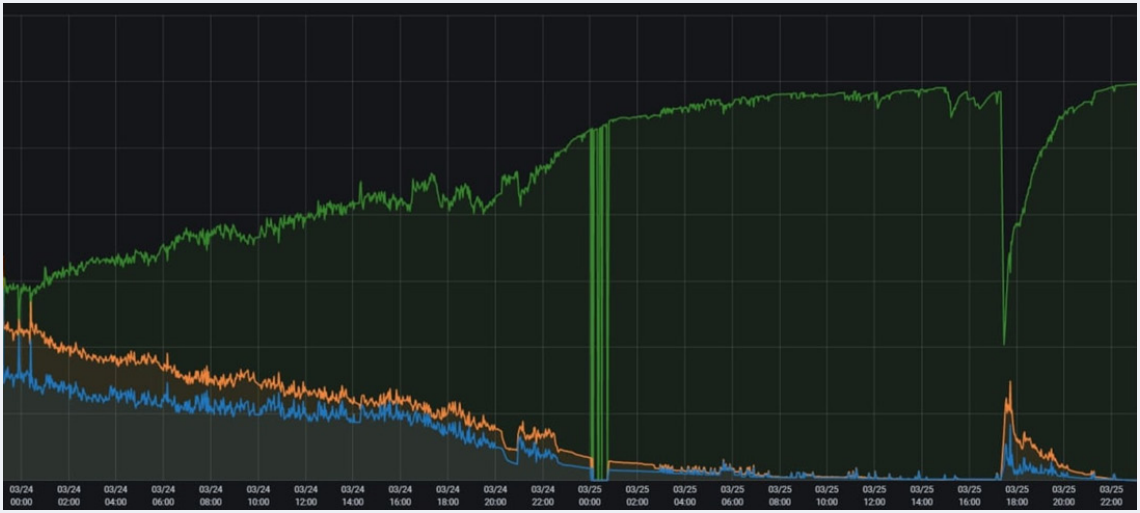
https://github.com/ceph/ceph/pull/25077
common: drop append_buffer from bufferlist. Use simple carriage instead #25077

در اقدامات بعدی تلاش شد، تمام کامیت‌های مرتبط به موضوع در نسخه‌ی ۱۶ در نسخه‌ی ۱۲ سازگار و ارایه شود.

حرکت کلاستر به‌سمت بهبود

با مجموع اقدامات انجام شده، کلاستر در وضعیت مناسب‌تری قرار گرفت، تیم فنی تصمیم گرفت با تنظیم مجدد Flagها کلاستر را در وضعیت Recover قرار دهد. از ساعت ۱۸:۰۰ روز سه‌شنبه ۳ فروردین ماه وضعیت کلاستر به‌سمت بهبود حرکت کرد.

در این نمودار رنگ سبز افزایش Placement Groupهای Clean و رنگ‌های نارنجی و آبی به ترتیب کاهش Placement Groupهای Degraded و Undersized را نشان می‌دهد و به‌معنای حرکت کلاستر به‌سمت پایداری است. حدود ۴۸ ساعت زمان برد، تا نزدیک به ۱۰۰درصد از Placement Groupها در حالت Clean قرار بگیرند:



Ceph Status (22 March | 13:39)	Ceph Status (25 march | 23:30)	Ceph Status (26 march | 04:00)
Object misplaced (7.594%) Object unfound (0.000%) Object degraded (5.870%) Snap trim queue (0.09%) Recovery: 9.91MiB/s (79 mbps)	Object misplaced (0.626%) Object unfound (0.000%) Object degraded (0.2221%) Snap trim queue (0.001%) Recovery: 3.95GiB/s (31.6 gbps) Recovery Peak ~ 30GiB/s (240 gbps)	Object misplaced (0%) Object unfound (0%) Object degraded (0%) Snap trim queue (0%) Recovery: 0

در طول این مسیر براساس وضعیت تمام سرورها و OSDها چندبار فرآیند ریکاور شدن متوقف و دوباره از سر گرفته شد. هم‌چنین برخی از OSDها از مدار خارج شدند، برخی کاهش یا افزایش وزن‌دهی شدند، خطاهای برخی از OSDها برطرف و هم‌چنین با انتقال داده‌های برخی از Placement Group ها به سایر بخش‌ها، PG دارای اشکال حذف شدند.

از بامداد روز جمعه وضعیت کلاستر به‌شکل طبیعی خود برگشت و امکان دسترسی Read/Write پرسرعت ابرک‌ها روی کلاستر ذخیره‌سازی فراهم شد.

گزارش کالبدشکافی (Forensics)
از حمله به زیرساخت رایانش ابری
دیتاسنتر IR-THR-AT1

تاریخ حمله: ۲۶ اسفند ۱۳۹۹

سطح تاثیر: ۲۵۰۰ مشترک، ۷۰۰۰ ابرک (سرور ابری)

خلاصه‌ی حمله: حمله‌ی سایبری به‌منظور تخریب و حذف اطلاعات مشتریان در دیتاسنتر IR-THR-AT1 که منجر به از دسترس خارج شدن سرویس‌های ۲۵۰۰ مشترک شد. پس از این حمله، بیش از ۹۷ درصد از اطلاعات حذف شده به‌طور کامل بازیابی شد، اما این ۳درصد اطلاعات حذف شده، باعث آسیب به حدود ۹درصد از کل ابرک‌ها شدند.

شرح حادثه

۲۶ اسفند ۱۳۹۹ یک حمله‌ی سایبری به زیرساخت ابر آروان در یکی از سه دیتاسنتر محصول رایانش ابری یعنی دیتاسنتر IR-THR-AT1 انجام شد. دقایقی پس از اعلام حادثه، تیم امنیت آروان تحلیل و کالبدشکافی این حملات را آغاز کردند.
برخی از سیستم‌ها به‌شکل آنلاین و فقط با قطع کامل از شبکه و برخی از سیستم‌ها پس از خاموش شدن در اختیار این تیم قرار گرفتند. هم‌چنین دسترسی به تمام لاگ‌ها و گزارش‌های سیستم‌های مانیتورینگ و ثبت وقایع تمام تجهیزات و شبکه در اختیار تیم کالبدشکافی قرار گرفت.

در هیچ‌کدام از این سیستم‌ها مطلقن هیچ داده‌ای از مشتریان وجود نداشته است.

علاوه‌بر تیم ابر آروان که مدیریت این فرآیند را آغاز کردند، مشاوران و همکاران ما از شرکت‌های رها، راوین و پادویش در بخش‌های مختلف این آنالیز در کنار ما بودند تا بتوانیم با بالاترین دقت این مراحل را به اتمام برسانیم و نتایج آن را منتشر کنیم.
با جمع‌آوری شواهد و بررسی زوایای مختلف، تیم بررسی به یک سناریوی نهایی به عنوان قوی‌ترین احتمال نفوذ دست یافت.

به‌طور کلی، در بیش‌تر سناریوهای نفوذ، ترکیبی از چند عامل آسیب[10] سبب بروز مشکل نهایی می‌شود، می‌توان این آسیب‌ها رو به گروه‌های زیر تقسیم‌بندی کرد:

- اشکال در طراحی یا اجرای سیاست‌های امنیتی (تنظیم ضعیف امنیتی، پیکربندی نادرست و...)
- بهره‌کشی[11] از سرویس‌ها از طریق یک یا چند آسیب‌پذیری منتشر شده یا منتشرنشده[12]
- استفاده از ضعف‌ها (آسیب‌پذیری‌های) منطقی

با توجه به این‌که در بررسی یک حمله‌ی چندبعدی و پیچیده، تمام شواهد دردسترس تیم کالبدشکافی نیست، بخشی از سناریو براساس گمانه‌زنی‌های معقول پیش می‌رود؛ در نتیجه، ممکن است توانایی تیم هکری چندان قدرت‌مند ارزیابی نشود یا برعکس بخش‌هایی از مهارت‌های تیم هکری در طراحی و اجرای حملات بیش از آن‌چه هست، ارزیابی شود.
در روزهای آینده ممکن است تیم امنیتی آروان در بررسی‌های خود به سرنخ‌های تازه‌ای برسند یا تیم‌های هکری ادعاهای جدیدی را در فضای عمومی اینترنت مطرح کنند. در این موقعیت، ابر آروان با بررسی سرنخ‌های جدید اقدامات ثانویه‌ی خود را انجام خواهد داد و نسبت به تکمیل گزارش خود اقدام خواهد کرد.
هم‌چنین ممکن است مانند همیشه متخصصانی آسیب‌پذیری‌های دیگری، مرتبط یا نامرتبط با حادثه‌ی پیش‌آمده را کشف کنند، که از ایشان دعوت می‌کنیم به صفحه‌ی باگ‌بانتی ابر آروان [13] که پس از این حادثه، مبلغ جوایز آن نیز دو برابر شده است، مراجعه و گزارش‌های‌شان را ثبت کنند. ابر آروان بلافاصله گزارش‌های امنیتی دریافتی را بررسی و با معتبر بودن، جوایز مرتبط به سطح آسیب‌پذیری گزارش شده را پرداخت و با نام فرد گزارش‌دهنده، مشکل امنیتی را در صفحه‌ی باگ‌بانتی خود منتشر خواهد کرد.

۱۰. Vulnerability Chain
۱۱. Exploit
۱۲. Zero Day
۱۳. https://www.arvancloud.com/fa/landing/bug-bounty

بخش اول

دامنه‌ی حمله

همان‌طور که گفته شده، حمله محدود به یکی از محصولات ابر آروان (زیرساخت رایانش ابری) واقع در دیتاسنتر IR-THR-AT1 بوده است. زیرساخت رایانش ابری به‌طور کلی دارای سه نتورک مستقل شامل موارد زیر است:

- شبکه‌ی ارتباطی اصلی برای استفاده شبکه‌ی داخلی ابرک‌ها و شبکه‌ی اتصال به اینترنت
- شبکه‌ی مربوط به ذخیره‌سازی (برای اتصال ابرک‌ها به بلاک استورج)
- شبکه‌ی مدیریت (به‌شکل out of band)

در این حمله، دامنه‌ی حضور هکرها از طریق شبکه‌ی مدیریت بوده است. ابر آروان در طراحی‌های خود در دیتاسنترها و محصولات مختلف براساس اصول امنیتی، شبکه‌ی مدیریت خود را مستقل از سایر شبکه‌ها (out of band) طراحی کرده است. اما در هر حال امکان دسترسی از راه دور به این شبکه وجود داشته است.
ابر آروان پس از این واقعه، با سخت‌گیرانه‌تر کردن فرآیندهای دسترسی و افزایش لایه‌های امنیتی، سطح امنیتی دسترسی به شبکه مدیریتی را افزایش چشم‌گیری داده است.

بخش دوم

دسترسی و انجام عملیات تخریب

اتصال هکرها ابتدا به شبکه‌ی مدیریتی و درنهایت آسیب‌رساندن به زیرساخت‌ها از طریق دسترسی‌های تعریف شده در آن لایه بوده است. هکرها توانسته‌اند با نفوذ و سواستفاده از کلیدهای مجاز همکاران ابر آروان (کلیدهایی با سطح دسترسی پایین که مجوز اتصال به Virtual Private Network و از طریق آن برقراری ارتباط با شبکه‌ی مدیریتی را صادر می‌کرده است)، یا از طریق عبور از نقطه‌ی رابطی که قابلیت اتصال به شبکه‌ی مدیریت را فراهم می‌کرده است، به این شبکه دسترسی پیدا کنند و با اسکن کامل شبکه، طراحی حمله‌ی خود را انجام دهند.

تیم CDN و سامانه‌ی امنیت ابری آروان برای اتصال به شبکه و سرورها، از کلید سخت‌افزاری با قابلیت جلوگیری از Exploit یا Proxy شدن کلید استفاده می‌کنند. پس از این حملات، استفاده از این کلید برای تمام تیم‌های فنی و پشتیبانی آروان اجباری شد. علاوه‌بر آن اصلاحات مورد نیاز روی شبکه‌ی مدیریتی نیز انجام شد.

نفوذگر پس از این مرحله با اسکن کامل شبکه توانسته از حداقل یک آسیب‌پذیری بالقوه سواستفاده کند. سوییچ‌هایی که به‌شکل VPC تنظیم شده بودند دارای سیستم‌عامل NX-OS بودند، این سیستم‌عامل‌ها در برخی نسخه‌های خود دارای آسیب‌پذیری CVE-2019-1962 هستند، نفوذگر با بهره‌کشی از این آسیب‌پذیری‌ها، توانسته باعث ایجاد اختلال در فرآیند این سوییچ‌ها و در نتیجه‌ی آن از دسترس خارج شدن بخش مهمی از شبکه بشود.

ابر آروان در طراحی و اجرای دیتاسنترهای جدید خود لایه‌ی شبکه و سیستم‌عامل‌های آن لایه را به‌طور کامل ارتقا داده است و از آخرین نسل تجهیزات سیسکو استفاده می‌کند. ارتقای شبکه و تجهیزات دیتاسنتر IR-THR-AT1 نیز پس از حمله، با اولویت در دستور کار قرار گرفت و هم‌زمان با انجام سایر فرآیندهای بازیابی، تمام سوییچ‌های فعلی با آخرین نسل از سوییچ‌های Nexus جایگزین شدند.

بخش دوم حمله، آسیب رساندن به تجهیزات پردازشی و ذخیره‌سازی از طریق iLO بوده است. به‌طور کلی آسیب‌پذیری متعددی روی پورت‌های iLO وجود دارد، هم‌چنین روش‌های احراز هویت ساده‌ای برای اتصال استفاده می‌شود. به همین دلیل معمولن تلاش می‌شود دسترسی به این پورت‌ها (همانند طراحی انجام شده در شبکه‌ی آروان) همیشه از طریق شبکه‌ی OOB انجام شود. هکرها در این بخش و پس از اتصال به شبکه OOB و از طریق اتصال به iLO توانسته‌اند با تخریب تنظیمات RAID و حذف کامل Partition Tables، سبب حذف اطلاعات برخی از سرورهای ذخیره‌سازی، هم‌چنین آسیب زدن به برخی سرورهای پردازشی شوند. با این اتفاق در حدود ۱۰۰ ترابایت از اطلاعات سرورهای پردازشی حذف شد.

همان‌طور که پیش از این در گزارش اولیه نیز بیان شد، هکرها امکان دسترسی خواندن (Read) روی اطلاعات کلاستر ذخیره‌سازی را نداشتند و تخریب تنها از طریق حذف Partition Tableها انجام شده و در نتیجه هیچ‌گونه نشت اطلاعات در این بخش انجام نشده است.

بخش سوم

اقدامات موازی هکر(ها) برای ایجاد ازدحام در لایه‌ی شبکه

با اسکن Range هر سرویس‌دهنده‌ی ابری در جهان، از میان هزاران سرور ابری ایجاد شده از سوی مشتریان، حتمن با تعدادی سرور مواجه خواهید شد که یا به‌دلیل عدم اهمیت (سرورهایی که معمولن برای تست یا به‌شکل موقت ایجاد می‌شوند) یا به‌دلیل رعایت نکردن اصول امنیتی، به‌راحتی از اینترنت نفوذپذیر هستند.
این‌گونه نفوذها معمولن از طریق آسیب‌پذیری‌های پیش‌فرض، استفاده از رمزعبورهای ساده برای کاربران پیش‌فرض، یا عدم رعایت اصول امنیتی در احراز هویت پایگاه داده رخ می‌دهد.
هکرها از طریق آلوده کردن تعدادی از ابرک‌های آسیب‌پذیر برخی مشتریان میزبانی شده (زامبی کردن) در دیتاسنتر IR-THR-AT1 هم‌زمان با حمله، شروع به ارسال پکت‌های Broadcast (به نشانی 255.255.255.255) کردند. انجام حمله‌ی TCP Flood و UDP Flood هم‌زمان با حمله‌ی اصلی با هدف ایجاد کندی، افزایش تعداد لاگ‌ها و تمرکززدایی انجام شده است.

پخش چهارم

اقدامات ابر آروان در مواجه به حمله

با آغاز حمله، شبکه‌ی مدیریتی به‌طور کامل قطع شد تا از نفوذ و تخریب بیش‌تر جلوگیری شود. هم‌چنین اینترنت دیتاسنتر نیز به‌طور کامل قطع شد تا اطمینان پیدا کنیم که هیچ‌گونه اتصال ریموت یا یک اتصال معکوس (Connect Back) به دیتاسنتر برقرار نیست و تنها اعضای تیم که به‌شکل حضوری در محل حضور دارند امکان دسترسی پیدا می‌کنند.
در لحظه‌ی بروز حادثه، دو نفر از همکاران ابر آروان در دیتاسنتر حضور داشتند، بلافاصله دو تیم دیگر از همکاران به محل دیتاسنتر اعزام شدند و یک سکوی آنلاین برای مدیریت حادثه ایجاد شد. سکویی که در تا ۵ روز پس از حمله، بی‌وقفه و به‌شکل شبانه‌روزی ادامه داشت. در مجموع تا پایان بحران، ۷۶۸ نفر-ساعت بدون وقفه مشغول کار در دیتاسنتر بوده‌اند.

همان‌طور که پیش‌تر هم گفته شد، در نخستین اقدام چهار تیم مختلف تشکیل شد تا به موازات یک‌دیگر موضوعات را پی‌گیری کنند:

- **تیم یک**: مسوول مراقبت از دیتاسنتر IR-THR-MN1 برای پیش‌گیری از اتفاق مشابه
- **تیم دو**: کار متمرکز روی استورج دیتاسنتر IR-THR-AT1 برای برگرداندن ۱۰۰ ترابایت اطلاعات و پایدارسازی کلاستر ذخیره‌سازی
- **تیم سه**: کار متمرکز روی کل زیرساخت رایانش ابری در IR-THR-AT1 تا به‌محض رفع اشکال فضای ذخیره‌سازی، سرویس دوباره به مدار برگردد.
- **تیم چهار**: مسوول کالبدشکافی (Forensics) و ایمن‌سازی (Hardening)

برخی از مهم‌ترین اقدامات امنیتی برای ارتقای ایمن‌سازی

- بازنگری و ارتقای امنیتی شبکه‌ی مدیریتی (OOB)
- سرعت بخشیدن به فرآیند ارتقای تجهیزات شبکه و ارتقای نسل تجهیزات
- بازنگری و سخت‌گیرانه‌تر کردن تنظیمات دیواره آتش (Firewall)
- ارتقای visibility و سیستم‌های اخطاردهی امنیتی
- تغییر تمام رمزهای عبور در تمام لایه‌ها، باطل کردن تمام کلیدها و ایجاد پروتکل‌های سخت‌گیرانه‌تر برای استفاده از کلیدهای سخت‌افزاری
- افزایش سخت‌گیری بیش‌تر در لایه‌بندی سطح دسترسی
- بازنگری و مرور تنظیمات ایمن‌سازی (Hardening) روی تمام سرورها و تجهیزات شبکه
- استقرار تیم تست نفوذ (Red Team) بیرونی به موازات تیم تست نفوذ ابر آروان برای کشف آسیب‌پذیری‌های احتمالی
- افزایش جوایز مسابقه‌ی باگ‌بانتی به دوبرابر و استقرار هم‌زمان آن روی سکوی باگ بانتی راورو

چه آموختیم؟

ابر آروان یک زیرساخت یکپارچه‌ی ابری است، یکی از محصولات ما، «امنیت ابری» برای جلوگیری از حملات DDoS و حملات مرسوم وب است، محصولی که اگرچه حوزه فعالیت آن با حمله‌ی انجام شده کاملن متفاوت است، همواره از بسیاری از حملات سایبری به بزرگ‌ترین کسب‌وکارهای کشور جلوگیری کرده است. با وجود این نکات، ما نیز با حادثه‌ای امنیتی مواجه شدیم تا نشان دهد اگرچه هیچ‌وقت امنیت ۱۰۰درصدی وجود ندارد، اما باید به‌شکل پیوسته امنیت را چون همیشه در صدر اولویت‌های سازمان نگاه داریم و تدابیری را اتخاذ کنیم تا سطح امنیت در تمامی بخش‌ها بیش از پیش تقویت شود.

ابر آروان با داشتن پروتکل‌های سخت‌گیرانه‌ی امنیتی، تیم امنیت داخلی، استفاده از مشاوران و شرکت‌های بیرونی، برگزاری جوایز باگ‌بانتی و انجام دوره‌های تست نفوذ باز هم برای ارتقای امنیت خود به اقدامات مهمی نیاز دارد و در این مسیر گام‌های بلندی طی خواهد کرد.

هم‌چنین تمرین و تمرکز روی پروتکل‌های واکنش به وقایع (Incident Response) می‌تواند کمک کند به هنگام بروز حوادث مشابه از شدت آن کاسته و واکنش‌های دقیق‌تر و چابک‌تری به آن نشان داده شود. از آن گذشته ابر آروان خود را موظف می‌داند با ترویج و فرهنگ‌سازی استفاده از معماری‌های ابرزی را به کاربران خود توصیه کند، تا طراحی زیرساخت‌های خود را به‌سمت معماری‌های توزیع شده و پایدارتر سوق دهند.

قطعن برطرف کردن و رفع مشکلات امنیتی کاری سخت و پیچیده است، اما برطرف کردن نگرانی‌های امنیتی کاربران‌مان کاری بسیار سخت‌تر و پیچیده‌تر خواهد بود. ما خودمان را موظف می‌دانیم علاوه‌بر انجام اقدامات گسترده، با گزارش دقیق و شفاف آن، مشترکان و شرکای تجاری خود را از این اقدامات آگاه کنیم.

اقدامات پیش‌گیرانه
و رو به آینده‌ی ابر آروان

ابر آروان با تجربه‌ی اتفاق پیش آمده و سطح آسیب‌پذیری مشتریان، مجموعه اقداماتی را در حوزه‌های «محصول»، «اقدمات و فرآیندهای امنیتی» و «جبران خدمت»، طراحی و اجرا خواهد کرد. در ادامه به توضیح هر یک از حوزه‌ها می‌پردازیم.

محصول

ابر آروان با ایجاد یک Region بزرگ و پایدار به اسم «تهران بزرگ»، چهار Availability Zone این منطقه را به یک‌دیگر متصل خواهد کرد. ما در منطقه غرب تهران، در منطقه شرق تهران، هم‌چنین دو Availability Zone تهران مرکزی را به یک‌دیگر متصل خواهیم کرد. هم‌چنین دیتاسنترهایی در تبریز و اصفهان افتتاح خواهیم کرد.
به‌علاوه، امکاناتی فراهم خواهیم کرد تا مهاجرت در داخل یک Region و ایجاد کلاسترهای پایدار به‌شکل Multi Availibilty Zone به آسان‌ترین شکل ممکن انجام شود. هم‌چنین پس از این اقدامات محصول فضای ذخیره‌سازی ابری آروان پایداری در سطح Region خواهد داشت و در منطقه‌ی اصلی (تهران بزرگ) اطلاعات را در بیش‌تر از یک AZ ذخیره خواهد شد.
توسعه‌ی امکان پشتیبان‌گیری خودکار ابرک‌ها، تمرکز روی پایداری و SLA محصولات، هم‌چنین فیچرهایی مرتبط با مهاجرت، حفظ و یکپارچگی اطلاعات اولویت خواهند داشت.
هم‌چنین ابر آروان با ایجاد و ارتقای Tier رایگان روی تمام محصولات به‌ویژه فضای ذخیره‌سازی ابری برای پشتیبان‌گیری، و رایگان کردن کامل ترافیکCDN، ارتقای تایر رایگان سامانه‌ی امنیتی ابری تلاش خواهد کرد، به فرهنگ‌سازی در شکل‌گیری معماری‌های ابرزی کمک کند.

اقدامات و فرآیندهای امنیتی

ابر آروان سازوکارهای مربوط به تست نفوذ را ارتقا خواهد داد. فاصله بین تست‌های نفوذ داخلی را کاهش و شرکای بیرونی خود در این زمینه را افزایش می‌دهد.
جوایز باگ بانتی آروان به ۲ برابر افزایش یافته و این موضوع در یک سکوی بیرونی نیز قرار گرفته است؛ این مسیر را با جدیت ادامه خواهیم داد.
ابر آروان ارتقا و افزایش سخت‌گیری در سازوکارهای ایمن‌سازی (Hardening)، مدیریت کلیدها، مدیریت سطح دسترسی و... را در دستور کار قرار داده است و ارتقا و افزایش سخت‌گیری‌ها در اجرای سازوکارهای مدیریت بحران، مدیریت ریسک و مدیریت تغییرات را سرعت خواهد بخشید.

جبران خدمت

ابر آروان با تغییر سطوح پشتیبانی، «پشتیبانی پایه» و «تماس تلفنی» را برای بخش بزرگی از مشترکان غیررایگان خود بدون پرداخت هزینه فعال خواهد کرد، در همین رابطه، در تلاش هستیم تا خدمات خود در بخش مشاوره و طراحی راهکارهای ابرزی را توسعه دهیم.
هم‌چنین در تلاش‌ایم با مذاکره با شرکت‌های معتبر بیمه، نوعی از بیمه‌ی مسوولیت در مواجهه با حملات سایبری و آسیب‌های زیرساخت را در ایران، ایجاد کنیم که هم شرکت‌های ارایه‌دهنده‌ی زیرساخت ابری از آن بهره ببرند و هم مشتریان محصولات ابری با پوشش‌های متنوع بتوانند از جبران خسارت در قالب حمایت‌های بیمه‌ای بهره‌مند شوند.