

دیپلوی و مدیریت حادثه

سه‌ه‌ن‌د‌ن‌و‌ع‌ی – س‌پ‌ه‌ر‌ن‌و‌ع‌ی – ا‌م‌ی‌ر‌ح‌س‌ی‌ن‌ص‌ل‌ا‌ح‌ی

ا‌م‌ت‌ی‌ا‌ز‌ی‌ا‌و‌ل

راه‌اندازی میکروسرویس‌ها با استفاده از پلتفرمی مانند Kubernetes فرآیندی ساختارمند است که به مدیریت و ارتباط بین برنامه‌های کانتینری (مانند Docker) می‌پردازد. در زیر، فرآیند راه‌اندازی روی Kubernetes، مزایا و امتیازات این روش توضیح داده شده است:

فرآیند راه‌اندازی روی Kubernetes

۱. کانتینرسازی:

– ابتدا هر میکروسرویس با استفاده از Docker یا یک ابزار کانتینری دیگر کانتینرسازی می‌شود. کانتینرسازی به معنای اجرای هر سرویس در یک محیط جداگانه با وابستگی‌های خود است که این امر باعث می‌شود فرآیند راه‌اندازی در محیط‌های مختلف یکنواخت باشد.

۲. تنظیم Kubernetes:

– Kubernetes یک پلتفرم ارکستریشن کانتینر است که به‌طور خودکار فرآیندهای مانیتورینگ، مقیاس‌پذیری و مدیریت برنامه‌های کانتینری را انجام می‌دهد. راه‌اندازی Kubernetes شامل:

– پیکربندی یک کلاستر Kubernetes که شامل نودها (ماشین‌هایی که کانتینرها در آن‌ها اجرا می‌شوند) و یک پلن کنترل (که کلاستر را مدیریت می‌کند) می‌شود.

– نصب کامپوننت‌های لازم مانند kubectl (ابزار خط فرمان Kubernetes)، عاملی که بر روی هر نود اجرا می‌شود) و یک موتور کانتینری (مانند Docker)

۳. راه‌اندازی میکروسرویس‌ها:

- رجیستر کردن کانتینرها: تصاویر کانتینرهای میکروسرویس‌ها در یک رجیستری کانتینر (مانند Docker Hub، AWS ECR، Google Container Registry) آپلود می‌شوند.

- استفاده از اشیاء راه‌اندازی Kubernetes: برای هر میکروسرویس، یک شیء راه‌اندازی Kubernetes با استفاده از فرمت‌های YAML یا JSON تعریف می‌شود. این اشیاء راه‌اندازی مشخص می‌کنند که چند نمونه از یک میکروسرویس باید اجرا شود و چگونه بروز رسانی شوند.

- کشف خدمات و توازن بار: خدمات Kubernetes از جزئیات پادها (نمونه‌های اجرایی میکروسرویس) پنهان می‌کنند و یک آدرس IP و نام DNS پایدار برای دسترسی به آن‌ها فراهم می‌کنند. همچنین خدمات توازن بار را برای توزیع ترافیک بین پادها فراهم می‌آورند.

۴. روند پیوسته‌سازی (CI/CD)

- پیاده‌سازی شیوه‌های پیوسته‌سازی (CI/CD) باعث می‌شود تغییرات در میکروسرویس‌ها به‌صورت خودکار تست شوند، تصاویر کانتینرسازی شوند و به کلاسترهای Kubernetes راه‌اندازی شوند. این کار با استفاده از ابزارهای CI/CD مانند Jenkins، GitLab CI/CD یا Tekton انجام می‌شود.

۵. نظارت و ثبت رویدادها:

- Kubernetes پشتیبانی طبیعی از نظارت و ثبت رویدادها را از طریق ابزارهایی مانند Prometheus (برای نظارت) و Elasticsearch (برای ثبت رویدادها) فراهم می‌کند. این ابزارها به تحلیل و نظارت بر عملکرد و سلامت میکروسرویس‌ها کمک می‌کنند.

مزایای راه‌اندازی روی Kuberne

۱. مقیاس‌پذیری و در دسترس بودن بالا:

- Kubernetes امکان مقیاس‌پذیری افقی میکروسرویس‌ها را با افزودن یا حذف نمونه‌ها بر اساس تقاضای ترافیک فراهم می‌آورد. این پلتفرم همچنین با بازیابی خودکار کانتینرهای مختلف و توزیع بار بین نمونه‌های سالم، در دسترس بودن بالایی را فراهم می‌کند.

۲. عملیات خودکار:

- Kubernetes بسیاری از وظایف عملیاتی مانند راه اندازی، مقیاس پذیری، بروزرسانی و برگرداندن به وضعیت قبلی را به طور خودکار انجام می دهد. این امر باعث کاهش مداخله دستی و خطاهای انسانی می شود که قابلیت اعتماد سیستم را بهبود می بخشد.

۳. بهره‌وری منابع:

- Kubernetes با بهینه سازی استفاده از منابع، کانتینرها را به صورت بهینه بر روی نودها پخش می کند که این امر منجر به استفاده بهینه از سخت افزار می شود و هزینه ها را کاهش می دهد.

۴. کشف خدمات و توازن بار:

- خدمات Kubernetes جزئیات پادها را پنهان می کنند و برای دسترسی به آنها یک آدرس IP و نام DNS پایدار فراهم می آورند. این خدمات همچنین توازن بار ترافیک را بین پادها فراهم می کنند که به بهره‌وری و عملکرد بهتر کمک می کند.

به طور کلی، Kubernetes به عنوان یک پلتفرم ارکستریشن کانتینری، فرآیندهای راه اندازی، مقیاس پذیری و مدیریت میکروسرویس ها را بهبود می بخشد و به توسعه سریع و ایمن برنامه های کانتینری کمک می کند.

امتیازی دوم

برای اطمینان از پایداری و در دسترس بودن میکروسرویس‌هایی که روی سیستم خودمان دیپلوی کرده‌ایم، ایجاد اعلان‌های مناسب بسیار حیاتی است. این اعلان‌ها باید برای اطلاع‌رسانی در هنگام تجاوز به حدود یا شرایط خاصی که نشانگر مشکلات یا نقص‌های محتمل هستند، طراحی شوند. در زیر، توضیحی در مورد اعلان‌ها برای سه میکروسرویس اصلی در یک پلتفرم آنلاین اجاره مسکن ارائه شده است.

اعلان‌ها و فاکتورهای اهمیت برای میکروسرویس‌ها

۱. سرویس رزرو

- اعلان‌ها:

۱. نرخ بالای شکست رزرو: هنگامی که درصد شکست درخواست‌های رزرو از یک حد مشخص (مثلاً ۵ درصد) بیشتر شود، اعلان فعال می‌شود.

۲. تاخیر بالا در پردازش رزرو: هشدار زمانی که زمان متوسط برای پردازش درخواست‌های رزرو از یک حد مشخص (مثلاً ۱ ثانیه) بیشتر شود.

۳. خطاهای دروازه پرداخت: هنگامی که ارتباط با دروازه پرداخت بیشتر از تعداد مشخصی بار خطا داشته باشد، اعلان فرستاده می‌شود.

- فاکتورهای اهمیت:

- تأثیر تجاری: نرخ بالای شکست رزرو مستقیماً به درآمد و رضایت مشتریان تأثیر می‌گذارد. نیاز به بررسی و حل مشکلات اساسی فوری دارد.

- تجربه کاربری: تاخیر در پردازش رزروها تجربه کاربری را تحت تأثیر قرار می‌دهد و ممکن است منجر به رها کردن رزروها یا نظرات منفی شود.

- تأثیر مالی: خطاهای دروازه پرداخت ممکن است باعث از دست رفتن درآمد شود اگر رزروها به درستی پردازش نشوند و پرداخت‌ها به طور صحیح ثبت نشوند.

۲. سرویس کاربر

- اعلان‌ها:

۱. نرخ بالای خطا در تأیید هویت کاربر: هشدار زمانی که نرخ تلاش‌های ناموفق برای ورود به حساب کاربری از یک حد مشخص (مثلاً ۳ تلاش ناموفق در دقیقه) بیشتر شود.

۲. افزایش ناگهانی در ثبت نام کاربر: هنگامی که تعداد ثبت‌نام‌های کاربران ناگهان افزایش یابد نسبت به الگوهای معمول، که ممکن است نشان‌دهنده مشکل امنیتی یا فعالیت رباتی باشد.

۳. خطاهای به‌روزرسانی اطلاعات کاربر: هشدار زمانی که به‌روزرسانی اطلاعات پروفایل کاربری به‌طور مداوم با خطا مواجه شود و تأثیر بر امکان ارائه خدمات شخصی‌سازی شود.

- فاکتورهای اهمیت:

- امنیت: خطاهای تأیید هویت ممکن است نشانگر حملات نیروی افزایشی یا تلاش‌های نفوذ به سیستم باشند که نیاز به بررسی و بستن آسیب‌پذیری‌ها دارند.

- قابلیت مقیاس‌پذیری: افزایش ناگهانی در ثبت‌نام کاربران می‌تواند زیرساخت‌های سرویس کاربر را تحت فشار قرار دهد و تأثیر منفی بر عملکرد کل سیستم داشته باشد.

- صحت داده: خطاهای به‌روزرسانی اطلاعات کاربر ممکن است منجر به نمایش یا پردازش نادرست اطلاعات کاربری شود که اعتماد کاربران را به خدمات تحت تأثیر قرار می‌دهد.

۳. سرویس پرداخت

- اعلان‌ها:

۱. نرخ بالای خطا در پرداخت: هشدار زمانی که درصد خطاهای ارتباط با دروازه پرداخت از یک حد مشخص (مثلاً ۲ درصد) بیشتر شود.

۲. تاخیر بالا در تأیید پرداخت: اعلان هنگامی که زمان متوسط برای تأیید پرداخت از یک حد مشخص (مثلاً ۵۰۰ میلی ثانیه) بیشتر شود.

۳. تراکنش‌های ناقص: هشدار زمانی که تعداد تراکنش‌های ناقص یا پرداخت‌های غیرقابل بررسی افزایش یابد.

- فاکتورهای اهمیت:

- اطمینان مالی: خطاهای دروازه پرداخت می‌توانند منجر به از دست رفتن درآمد شوند اگر پرداخت‌ها به درستی پردازش نشوند یا تأیید نشوند.

- کارایی: تأخیر در تأیید پرداخت می‌تواند به تجربه کاربری تأثیر منفی بیانجامد و باعث نارضایتی کاربران شود.

- دقت و صحت: تراکنش‌های ناقص ممکن است به نمایش اطلاعات نادرست یا پردازش نادرست تراکنش‌ها منجر شوند که اعتماد و رضایت کاربران را کاهش می‌دهد.

با استفاده از اعلان‌های مناسب برای هر یک از میکروسرویس‌های این پلتفرم، می‌توان به موقعیت سیستم اطمینان داشت و به مشکلات زودتر پاسخ داد تا برای کاربران و کسب‌وکار آسیب کمتری وارد شود.

امتیازی سوم

با توجه به نیاز به افراد آنکال برای نظارت و پاسخگویی به alert های سرویس ها، الزم است یک شیت آنکالی ماهانه برای هر سرویس تهیه و ارائه شود. این شیت باید جزئیات زمانی و اطلاعات تماس فرد آنکال را برای هر میکروسرویس و در هر بازه زمانی مشخص کند تا در صورت بروز هرگونه مشکل، فرد مسئول به سرعت واکنش نشان دهد و سیستم را به حالت عادی بازگرداند.

شیت آنکالی ماهانه برای سرویس ها

۱. سرویس رزرو

- تاریخ های آنکال:

- ۱ تا ۷ فروردین: سهپدر نوعی

- ۸ تا ۱۴ فروردین: سپهر نوعی

- و...

- توضیحات

- هر آنکال باید آمادگی کامل برای پاسخگویی به alert های مرتبط با سرویس رزرو را داشته باشد.

- زمان حضور آنکال باید برای هر بازه زمانی تعیین شود تا در صورت لزوم بلافاصله واکنش نشان دهد.

- نکات فنی مربوط به سیستم و alert های مرتبط باید به طور کامل به آنکال ارائه شود تا بتواند بهترین تصمیمات را برای بازگردانی سیستم بگیرد.

۲. سرویس کاربر

- تاریخ های آنکال:

- ۱ تا ۷ فروردین: سپهر نوعی

- ۸ تا ۱۴ فروردین: امیرحسین صلاحی

- و...

- توضیحات

- هر آنکال باید با دانش کافی از مشکلات محتمل سرویس کاربر آشنا باشد و به سرعت تصمیمات لازم را بگیرد.
- باید آمادگی برای حل مشکلات امنیتی، مقیاس‌پذیری و دیگر نیازهای سرویس کاربر را داشته باشد.

۳. سرویس پرداخت

- تاریخ‌های آنکال:

- ۱ تا ۷ فروردین: سه‌هفته‌ای

- ۸ تا ۱۴ فروردین: سه‌هفته‌ای

- و...

- توضیحات

- آنکال باید قادر به ارزیابی وضعیت پرداخت‌ها، امنیت تراکنش‌ها و دیگر نیازهای سرویس پرداخت باشد.
- باید در زمان‌های تعیین شده حضور داشته باشد تا به مشکلات مالی و ارتباطی سریعاً واکنش نشان دهد.

نکات مهم

- آموزش: آنکال‌ها باید قبل از شروع به کار به دوره‌های آموزشی دسترسی داشته باشند تا با ابزارها و فنون مورد نیاز برای مدیریت حوادث آشنا شوند.
- روند آنکالی: انجام آنکالی می‌تواند خسته‌کننده باشد، بنابراین نیاز به چرخه تنظیم و آموزش مستمر دارد تا افراد آماده و با انرژی برای واکنش به حوادث باشند.
- این اطلاعات به تیم آنکال کمک می‌کند تا سیستم را در مواقع ضروری با حداقل تأخیر و با کمترین زیان ممکن برای کاربران و کسب‌وکار بازیابی کنند.

امتیازی چهارم

وقتی که در سیستم یک حادثه رخ می دهد، مانند اینکه ی ک alert فعال می شود که نشانگر وقوع یک مشکل یا خطا است، فرد oncall باید به سرعت وارد عمل شود تا مشکل را شناسایی کند و به آن واکنش مناسبی نشان دهد. پس از بروز حادثه، معمولاً یک گزارش به نام "گزارش" postmortem نوشته می شود که شامل تحلیل علل حادثه، اقدامات انجام شده و پیشنهادات برای جلوگیری از تکرار آن حادثه در آینده است. این گزارش باید به صورت شفاف و دقیقی توضیح دهد که چه چیزهایی به حادثه منجر شدند و چگونه می توان از آن ها پاسخگویی بهتری داشت.

پروسه گزارش Postmortem

در مواقع بروز حوادث در سیستم، مانند فعال شدن یک alert که نشانگر وقوع یک مشکل یا خطا است، فرد oncall باید به سرعت وارد عمل شود تا مشکل را شناسایی کرده و به آن واکنش مناسب نشان دهد. پس از بروز حادثه، یک گزارش به نام "گزارش" postmortem نوشته می شود که شامل تحلیل علل حادثه، اقدامات انجام شده و پیشنهادات برای جلوگیری از تکرار آن حادثه در آینده است. این گزارش باید به صورت شفاف و دقیق توضیح دهد که چه چیزهایی به حادثه منجر شدند و چگونه می توان از آنها پاسخی بهتری داشت.

مراحل گزارش Postmortem:

۱. تعریف حادثه:

- توضیح نوع و شدت حادثه که باعث فعال شدن alert شده است.

- تعیین زمان بروز حادثه و نحوه کشف آن.

۲. تحلیل علل:

- بررسی دقیق عوامل و عللی که منجر به حادثه شده اند، از جمله مشکلات سیستمی، خطاهای کد، یا عملکرد نامناسب سرویس ها.

- شناسایی عوامل محرک (root cause) که باعث وقوع حادثه شده اند.

۳. اقدامات انجام شده:

- توضیح اقدامات فوری و اضطراری که برای مهار حادثه انجام شده است.
- توضیح اقدامات بهبودی که برای بازسازی سیستم و رفع مشکلات بلافاصله انجام شده‌اند.

۴. پیشنهادات برای اقدامات آینده:

- ارائه پیشنهاداتی برای جلوگیری از تکرار حادثه، از جمله بهبود فرآیندها، بهبود مانیتورینگ، و افزایش اعتمادپذیری سیستم.
- تعیین اقدامات پیشگیرانه و نقاط ضعفی که باید بهبود یابند.

نمونه‌های گزارش Postmortem برای سه حادثه احتمالی:

حادثه: انقطاع خدمات به دلیل حمله DDoS

- تعریف حادثه: در تاریخ ۱۵ مرداد، سیستم ما مورد حمله DDoS قرار گرفت که منجر به انقطاع خدمات به مدت ۲۴ ساعت شد.

- تحلیل علل: پس از بررسی، مشخص شد که حمله DDoS با تعداد زیادی درخواست بدون اعتبار به سرورهای اصلی ما صورت گرفته بود. این درخواست‌ها بسیار بالا بودند و باعث بار زیادی بر روی بخش شبکه و سرورهای ما شدند که منجر به انقطاع خدمات شد.

- اقدامات انجام شده:

۱. شناسایی الگوی حمله: تیم امنیتی ما الگوی حمله را شناسایی کرد و نقاط ضعف احتمالی در شبکه و سرورهای ما را تحلیل کرد.

۲. افزایش مانیتورینگ: مانیتورینگ شبکه و سرورها تقویت شد تا بتوانیم حملات مشابه را در زمان واقعی تشخیص دهیم و به طور سریع واکنش مناسبی نشان دهیم.

۳. تقویت امنیتی: بهبود سیاست‌ها و تنظیمات امنیتی بر روی شبکه و سرویس‌های ما صورت گرفت تا از حملات DDoS و دیگر حملات امنیتی پیشگیری شود.

- پیشنهادات برای اقدامات آینده:

۱. استفاده از (CDN (Content Delivery Network: این کار به کاهش تأثیر حملات DDoS کمک می‌کند و بار سرورها را توزیع می‌کند.
۲. استفاده از فایروال قدرتمند: فایروال‌های محافظتی با قابلیت شناسایی و مسدودسازی حملات DDoS باید پیکربندی شوند.
۳. تست و اجرای سناریوهای حملات: برنامه‌ریزی و اجرای سناریوهای مختلف حملات بر روی سیستم برای آمادگی بهتر در مواجهه با حملات واقعی.

حادثه: خرابی سرور اصلی

- تعریف حادثه: در تاریخ ۲۵ خرداد، سرور اصلی سیستم با مشکلات سخت‌افزاری روبرو شد که منجر به قطع خدمات گردید.
- تحلیل علل: خرابی هارد دیسک اصلی سرور به عنوان عامل اصلی شناسایی شد که منجر به از دست رفتن داده‌ها و عدم وجود سرویس‌ها گردید.
- اقدامات انجام شده: توسط تیم فنی، بسته‌بندی سرور فرعی و بازسازی داده‌ها انجام شد و خدمات برنامه به طور معمولی بازگشت.
- پیشنهادات برای اقدامات آینده: برای جلوگیری از این موضوع، ما از پشتیبان‌گیری مکرر و استفاده از سرورهای دوم به عنوان بک‌آپ سرور اصلی استفاده می‌کنیم.

حادثه: خرابی پرداخت برنامه

- تعریف حادثه: در ۱۲ اردیبهشت، خطا در پرداخت برنامه باعث شد که تراکنش‌های مشتری تحت تأثیر قرار گیرند و برخی از تراکنش‌ها ناقص شوند.
- تحلیل علل: بررسی نشان داد که یک ارتباط نامناسب با سرویس بانکی خارجی باعث این خطا شد.
- اقدامات انجام شده: پس از شناسایی مشکل، ارتباط با سرویس بانکی بازسازی شد و تراکنش‌ها با دقت مجدداً پردازش شدند.

- پیشنهادات برای اقدامات آینده: به منظور پیشگیری از این مشکلات، یک سیستم پشتیبانی موازی از سرویس‌های بانکی مورد نظر برای حداقل دسترسی تا تمام اطلاعات مورد نیاز است.

این پروسه به تیم آنکال کمک می‌کند تا با تحلیل دقیق علل حوادث و اتخاذ اقدامات مناسب، از تکرار مشکلات جلوگیری کرده و سیستم را در مواقع ضروری به سرعت بازیابی کنند.