Engineer

Katastrofåterställning

att återställa driften efter ett haveri med en testad plan

Vad det är

Katastrofåterställning (disaster recovery) är den del av beredskapsplaneringen som tar hand om det värsta fallet: platsen där ett system körs har gått förlorad eller är utom räckhåll under lång tid, och systemet måste byggas upp på nytt någon annanstans utifrån kopior. NIST:s vägledning för beredskapsplanering för amerikanska federala informationssystem, SP 800-34 Revision 1 från 2010, definierar en katastrofåterställningsplan som en skriftlig plan för att återställa ett eller flera informationssystem vid en alternativ anläggning efter ett allvarligt maskinvaru- eller programvarufel eller efter att anläggningarna har förstörts. Tillämpningsområdet är snävt. Vägledningen reserverar planen för stora, oftast fysiska, störningar som förhindrar åtkomst till den primära anläggningen under en längre tid, och den omfattar bara de störningar som kräver att verksamheten flyttas.

Den avgränsningen skiljer den från grannarna. En beredskapsplan för ett enskilt informationssystem, i vägledningens språk en information system contingency plan, återställer ett system där det står, till exempel efter en trasig disk eller en korrupt databas. Katastrofåterställningsplanen är knuten till en plats: den flyttar driften till den alternativa platsen, och därifrån tas varje system i drift igen enligt sin egen beredskapsplan. En plan för en databas och en plan för att förlora ett helt datacenter, en molnregion eller ett konto hos leverantören är två olika dokument med olika ägare, och den som blandar ihop dem står lätt utan någon av dem.

Tre mått gör planen till något som går att pröva. Längsta acceptabla driftstopp (maximum tolerable downtime, MTD) är den sammanlagda längd på ett avbrott som systemets ägare är beredd att godta. Målet för återställningstid (recovery time objective, RTO) är den längsta tid en systemresurs kan vara ur drift innan skadan på andra system och på verksamheten blir oacceptabel, och eftersom avbrutet arbete också måste bearbetas på nytt efteråt skriver vägledningen att

RTO normalt måste vara kortare än MTD. Målet för återställningspunkt (recovery point objective, RPO) blickar bakåt: det är den tidpunkt före avbrottet som data kan återställas till från den senaste säkerhetskopian, och det uttrycker hur mycket förlorade data verksamheten kan leva med. Kort sagt är RTO hur länge man ligger nere och RPO hur mycket arbete man förlorar.

Den alternativa platsen finns i flera grader. Ett cold site erbjuder bara lokaler och infrastruktur, ett warm site är delvis utrustat och ett hot site är fullt utrustat och bemannat. Vägledningen nämner också mobila anläggningar, som i många fall kan levereras inom 24 timmar innan uppsättningen börjar, och speglade anläggningar, det dyraste alternativet, som vägledningen i gengäld tillskriver praktiskt taget 100 % tillgänglighet. Ett cold site är billigast att underhålla, men det kan ta lång tid att utrusta. I dag fyller en andra molnregion eller en andra leverantör samma roll för det mesta av all programvara, och avvägningen mellan det som står redo och vad det kostar att hålla det redo är densamma.

Använd begreppet i ett beslut

Använd ”Vad är katastrofåterställning?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. Säkerhetskopior som testas i stället för att tas för givna, och en skriftlig plan för den morgon då en server inte startar igen.

Se våra tjänster Hör av er →

Granska antagandena bakom ordet

Använd förklaringen och det länkade arbetet för att formulera frågor till projektet. Vi kan undersöka antagandena tillsammans innan ett verktyg väljs. Automatiserade 100 kritiska säkerhetskopior — 100 automatiserade kritiska säkerhetskopior av databaserna

Automatiserade 100 kritiska säkerhetskopior Hör av er →

Varför det spelar roll

En säkerhetskopia är en kopia, och en kopia kör ingenting på egen hand. För att komma från kopian till ett fungerande system behövs också programvaran som läser den, nycklarna som dekrypterar den, servrar och nätverk att köra den på, konfigurationen som binder ihop alltihop och någon som kan ordningen. Allt som bara fanns på den förlorade platsen försvann tillsammans med den. Katastrofåterställning handlar om att se till att allt detta överlever samma händelse, och att återställningen från kopia till tjänst har prövats innan någon behöver den.

Data som går att återställa är inte nyare än den senaste kopia som faktiskt går att återställa, oavsett vilket RPO schemat för säkerhetskopiering ska uppfylla. Har ett nattligt jobb misslyckats utan att någon märkt det i en vecka riskerar man att förlora en veckas data, vad policyn än säger. NIST:s vägledning säger samma sak

om band: säkerhetskopior bör testas regelbundet för att bekräfta att data lagras korrekt och att filerna kan hämtas utan fel eller förluster. En grön statuslampa på ett säkerhetskopieringsjobb bevisar att något skrevs. Bara en återställning bevisar att det går att läsa tillbaka.

Planen åldras också. Folk slutar, servrar byts ut, leverantörer gör om sina konsoler och lösenorden i driftshandboken går ut. Av de sju steg som NIST ställer upp för beredskapsplanering är de två sista test, utbildning och övningar samt underhåll av planen; vägledningen vill att planen ska vara ett levande dokument som ses över minst en gång om året och varje gång systemet eller de resurser som återställningen använder ändras väsentligt. En plan som aldrig har övats faller ofta på detaljer som ingen tänkte på att skriva ner: ordningen som tjänsterna måste startas i, en DNS-post med ett dygns TTL, den enda åtkomstnyckeln som låg på maskinen som är borta.

För programvaruteam är katastrofen ofta ett konto snarare än en byggnad. Ett raderat molnprojekt, en kapad administratörsinloggning, ett avstängt konto hos leverantören eller ett destruktivt kommando som körts mot produktion tar bort åtkomsten till systemet lika grundligt som en översvämning. Standbyservrar skyddar inte mot det sista, eftersom en standby tillämpar en felaktig `DROP TABLE` inom några ögonblick, precis som den tillämpar alla andra ändringar.

Så ser det ut i praktiken

För en PostgreSQL-databas kommer ett RPO som är mycket kortare än intervallet mellan två säkerhetskopior från löpande arkivering av transaktionsloggen (write-ahead log, WAL) ovanpå en basbackup. Servern kopierar varje färdigt WAL-segment till en säker plats, och en återställning spelar upp segmenten ovanpå basbackupen fram till en valfri tidpunkt efter att den togs:

```
# postgresql.conf på den skyddade servern
wal_level = replica
archive_mode = on
archive_command = 'test ! -f /mnt/archive/%f && cp %p /mnt/archive/%f'
```

Vid en återställning packas en basbackup upp i en ny datakatalog, en tom fil med namnet `recovery.signal` läggs i den, och återställningsinställningarna anger var arkivet ligger och var återställningen ska stanna:

```
restore_command = 'cp /mnt/archive/%f %p'
recovery_target_time = '2026-03-10 17:14:00+01'
recovery_target_action = 'pause'
```

PostgreSQL-dokumentationen berättar historien som inställningarna finns till för: någon tar bort en viktig tabell kl. 17.15 en tisdagskväll, upptäcker det på onsdagen vid tolvtiden och återställer till kl. 17.14. Paus är standardåtgärden när målet är nått, så att man med frågor kan bekräfta att det är rätt tidpunkt innan servern befordras och börjar ta emot anslutningar; är det inte det stängs servern av, får ett senare mål och startas igen. Stoppunkten måste ligga efter slutet av basbackupen, och dokumentationen rekommenderar att arkiveringen sätts upp och testas innan den första basbackupen tas. När återställningen är klar tar servern bort `recovery.signal`, så att den inte går in i återställningsläge igen av misstag.

Engineer ApS erbjuder säkerhetskopiering och återställning som tjänst, beskriven som säkerhetskopior som är prövade och inte bara antas fungera, och en nedskriven plan för den morgon då en server inte kommer upp igen. Två portföljsidor visar vad det innebär i praktiken. I säkerhetskopior och återställning som kod från 2025 sattes lagringstiden för säkerhetskopior upp i Bicep bredvid databasen, så att återställning till valfri tidpunkt är en del av mallen och inte en inställning som någon en gång klickade fram i en portal, och miljön runt databasen definierades också som kod, eftersom en databas som återställs till en miljö som byggts upp igen ur minnet knappast är återställd. Därefter granskades beredskapen och skrevs ner med luckorna namngivna: georedundans var avslagen, och målet för återställningstid var föreslaget snarare än uppmätt, eftersom ingen övning hade genomförts.

Företagets automatiserade säkerhetskopiering och återställningstest utformades för att utöka återställningsberedskapen bortom en ögonblicksbild hos leverantören. En Ansible-roll installerar restic-skript och systemd-enheter för en databasdump där det är konfigurerat, krypterade, deduplicerade ögonblicksbilder via SFTP till lagring hos en annan leverantör, gallring enligt bevarandepolicyn och integritetskontroller. Ett separat månatligt arbetsflöde återställer en känd fil till ett tillfälligt arbetsutrymme och jämför dess byte. Säkerhetskopiering och återställning har separata signaler för lyckade körningar, lösenfrasen kommer från en skyddad fil, och timerenheterna är beroende av ett konfigurerat repo. De kontrollerna är implementerade; en återställning i drift är en separat leverans. Implementeringsbeskrivningen daterad 2026-10-27 anger att timerenheterna var inaktiverade utan ett repo och redovisar ingen

genomförd återställning i drift. Den ger därför belägg för automatiseringsarbetet snarare än ett åtagande om återställningstid eller ett påstående om att företaget redan kan förlora värddatorn utan att äventyra sina data.

Var det går fel

Säkerhetskopian har aldrig återställts. Ett jobb som rapporterar framgång varje natt säger ingenting om huruvida resultatet går att läsa, dekryptera och läsa in, och den första riktiga återställningen är ett dåligt tillfälle att ta reda på det. Schemalägg återställningar på samma sätt som du schemalägger säkerhetskopiering: en automatisk kontroll som hämtar ut kända data och jämför dem, och en fullständig återställning i en ren miljö så ofta att tiden den tar är ett uppmätt tal.

Kopian delar öde med originalet. En ögonblicksbild i samma molnkonto, en backupdisk i samma rack eller en arkiv-bucket bakom samma administratörsinloggning går ner tillsammans med det som slår ut det primära systemet. NIST:s vägledning ber att extern lagring och alternativa platser väljs utifrån hur osannolikt det är att samma katastrof drabbar dem. Ha minst en kopia hos en annan leverantör eller i ett annat konto med separata inloggningsuppgifter, och förvara dekrypteringsnycklarna någonstans som inte är beroende av de system de skyddar.

Bara data har planerats. Att återställa en databas är en liten del av att få en tjänst på fötter igen om servrar, brandväggsregler, DNS, certifikat och hemligheter runt den måste återskapas ur minnet. Beskriv miljön som versionshanterad infrastruktur som kod, och gör återuppbyggnaden av den till en del av övningen, inte bara inläsningen av data.

Målen är gissningar. Ett RTO som skrivits in i ett dokument utan en övning bakom sig är ett förslag, och ett RPO som förutsätter att varje säkerhetskopiering lyckades är optimistiskt. Mät båda i en övning. NIST skiljer mellan skrivbordsövningar (tabletop), som bara är diskussion och inte sätter igång någon utrustning, och funktionella övningar som simulerar driften, upp till fullskaliga övningar som täcker varje del av planen; siffrorna kommer från den senare sorten.

En standby räknas som en säkerhetskopia. En standbyserver eller en georeplikerad databas skyddar mot förlust av maskinvara, men den kopierar raderingar, korruption och filer som krypterats av utpressningsprogram lika troget som korrekta skrivningar. Ha kopior för valfria tidpunkter som ett misstag på det primära systemet inte kan nå, och behåll dem längre än det brukar ta att upptäcka ett misstag.

Planen beskriver förra årets system. En driftshandbok med avvecklade servrar, folk som har slutat och lösenord som inte längre fungerar bromsar en återställning i stället för att vägleda den. Se över planen efter varje väsentlig förändring och efter varje övning, skriv ner vad övningen avslöjade och se över de delar som ändras oftast, som kontaktlistor, med kortare mellanrum, precis som NIST rekommenderar.

Läs mer

- SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems — hela vägledningen: hur den definierar och avgränsar en DRP, de sju planeringsstegen, MTD, RTO och RPO, alternativa platser och övningstyper, med mallar för planerna.
- Continuous Archiving and Point-in-Time Recovery (PITR) — kapitlet i PostgreSQL 18 om WAL-arkivering, basbackuper och återställning till en vald tidpunkt.
- Write Ahead Log — konfigurationsreferensen för `archive_command`, `restore_command` och inställningarna för var en återställning ska stanna.

Ordlista

Välj utifrån era faktiska förutsättningar

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

Se vad det kostar Hör av er →

Gör begreppen praktiska

Fråga hur ”Vad är katastrofåterställning?” gäller i er organisation. Ett konkret exempel från ert nuvarande system räcker för att börja samtalet.

Se våra tjänster

welcome@engineer.company +45 50 10 61 84 Köpenhamn, Danmark

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/glossary/disaster-recovery/