Engineer

Katastrofegjenoppretting

å gjenopprette driften etter store tap med en testet plan

Hva det er

Katastrofegjenoppretting (disaster recovery) er den delen av beredskapsplanleggingen som tar for seg det verste tilfellet: stedet et system kjører på, er tapt eller utenfor rekkevidde i lang tid, og systemet må bygges opp igjen et annet sted fra kopier. NISTs veiledning i beredskapsplanlegging for amerikanske føderale informasjonssystemer, SP 800-34 Revision 1 fra 2010, definerer en katastrofegjenopprettingsplan som en skriftlig plan for å gjenopprette ett eller flere informasjonssystemer på et alternativt anlegg etter en alvorlig maskinvare- eller programvarefeil eller etter at anleggene er ødelagt. Virkeområdet er smalt. Veiledningen forbeholder planen store, som regel fysiske avbrudd som stenger tilgangen til hovedanlegget i lengre tid, og den dekker bare de avbruddene som krever at driften flyttes.

Den avgrensningen skiller den fra naboene. En beredskapsplan for ett enkelt informasjonssystem, i veiledningens språk en information system contingency plan, gjenoppretter ett system der det står, for eksempel etter en død disk eller en ødelagt database. Katastrofegjenopprettingsplanen er knyttet til et sted: den flytter driften til det alternative stedet, og derfra settes hvert system i drift igjen etter sin egen beredskapsplan. En plan for én database og en plan for å miste et helt datasenter, en skyregion eller en konto hos leverandøren er to forskjellige dokumenter med forskjellige eiere, og blander man dem sammen, ender man lett opp uten noen av dem.

Tre mål gjør planen til noe som kan etterprøves. Maksimal akseptabel nedetid (maximum tolerable downtime, MTD) er den samlede varigheten av et avbrudd som systemets eier er villig til å godta. Målet for gjenopprettingstid (recovery time objective, RTO) er det lengste en systemressurs kan være ute av drift før skaden på andre systemer og på virksomheten blir uakseptabel, og fordi avbrutt arbeid også må behandles på nytt etterpå, skriver veiledningen at RTO normalt må være kortere enn MTD. Målet for gjenopprettingspunkt (recovery point

objective, RPO) ser bakover: det er tidspunktet før avbruddet som data kan gjenopprettes til fra den siste sikkerhetskopien, og det uttrykker hvor mye tapte data virksomheten kan leve med. Kort sagt er RTO hvor lenge man er nede, og RPO hvor mye arbeid man mister.

Det alternative stedet finnes i flere grader. Et cold site har bare lokaler og infrastruktur, et warm site er delvis utstyrt, og et hot site er fullt utstyrt og bemannet. Veiledningen nevner også mobile anlegg, som i mange tilfeller kan leveres innen 24 timer før oppsettet begynner, og speilede anlegg, det dyreste alternativet, som veiledningen til gjengjeld tilskriver praktisk talt 100 % tilgjengelighet. Et cold site er det billigste å holde ved like, men det kan ta lang tid å utstyre. I dag spiller en annen skyregion eller en annen leverandør samme rolle for det meste av programvare, og avveiningen mellom det som står klart, og hva det koster å holde det klart, er den samme.

Bruk begrepet i en beslutning

Bruk «Hva er katastrofegjenoppretting?» i en konkret beslutning. Vi kan knytte begrepet til systemet dere bygger eller kjøper. Sikkerhetskopier som er testet i stedet for tatt for gitt, og en skriftlig plan for morgenen da en server ikke kommer opp igjen.

Se tjenestene våre Ta kontakt →

Undersøk antakelsene bak ordet

Bruk forklaringen og det tilknyttede arbeidet til å formulere spørsmål for prosjektet. Vi kan undersøke antakelsene sammen før et verktøy velges. Automatiserte 100 kritiske sikkerhetskopier — 100 kritiske sikkerhetskopier automatisert på tvers av databasene

Automatiserte 100 kritiske sikkerhetskopier Ta kontakt →

Hvorfor det er viktig

En sikkerhetskopi er en kopi, og en kopi kjører ingenting av seg selv. For å komme fra kopien til et fungerende system trenger man også programvaren som leser den, nøklene som dekrypterer den, servere og nettverk å kjøre den på, konfigurasjonen som binder det hele sammen, og en person som kjenner rekkefølgen. Alt som bare fantes på det tapte stedet, gikk tapt sammen med det. Katastrofegjenoppretting handler om å sørge for at alt dette overlever den samme hendelsen, og at forløpet fra kopi til tjeneste er prøvd ut før noen trenger det.

Dataene som kan gjenopprettes, er ikke nyere enn den siste kopien som faktisk lar seg gjenopprette, uansett hvilket RPO planen for sikkerhetskopiering skal oppfylle. Har en nattlig jobb feilet i det stille i en uke, risikerer man å miste en ukes data, uansett hva retningslinjene sier. NISTs veiledning sier det samme om bånd: sikkerhetskopier bør testes jevnlig for å bekrefte at dataene er lagret

riktig, og at filene kan hentes uten feil eller tap. En grønn statuslampe på en sikkerhetskopijobb beviser at noe ble skrevet. Bare en gjenoppretting beviser at det kan leses tilbake.

Planen forfaller også. Folk slutter, servere byttes ut, leverandører bygger om konsollene sine, og passordene i driftshåndboken går ut. Av de sju trinnene NIST setter opp for beredskapsplanlegging, er de to siste testing, opplæring og øvelser, og vedlikehold av planen; veiledningen vil at planen skal være et levende dokument som gjennomgås minst én gang i året, og hver gang systemet eller ressursene gjenopprettingen bruker, endres vesentlig. En plan som aldri er øvd på, faller gjerne på detaljer ingen tenkte på å skrive ned: rekkefølgen tjenestene må startes i, en DNS-post med et døgns TTL, den ene tilgangsnøkkelen som lå på maskinen som er borte.

For programvareteam er katastrofen ofte en konto snarere enn en bygning. Et slettet skyprosjekt, en kompromittert administratorinnlogging, en suspendert konto hos leverandøren eller en destruktiv kommando kjørt mot produksjon fjerner tilgangen til systemet like grundig som en flom. Standby-servere beskytter ikke mot den siste av dem, for en standby utfører en feilaktig `DROP TABLE` i løpet av et øyeblikk, akkurat som den utfører alle andre endringer.

Slik ser det ut i praksis

For en PostgreSQL-database kommer et RPO som er langt kortere enn intervallet mellom to sikkerhetskopier, fra løpende arkivering av transaksjonsloggen (write-ahead log, WAL) oppå en basebackup. Serveren kopierer hvert ferdige WAL-segment til et trygt sted, og en gjenoppretting spiller segmentene av oppå basebackupen fram til et valgfritt tidspunkt etter at den ble tatt:

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

Ved en gjenoppretting pakkes en basebackup ut i en ny datakatalog, det legges en tom fil kalt `recovery.signal` i den, og gjenopprettingsinnstillingene forteller hvor arkivet ligger, og hvor gjenopprettingen skal stoppe:

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

PostgreSQL-dokumentasjonen forteller historien innstillingene finnes for: noen sletter en viktig tabell kl. 17.15 en tirsdag kveld, oppdager det onsdag midt på dagen og gjenoppretter til kl. 17.14. Pause er standardhandlingen når målet er nådd, slik at man med spørringer kan bekrefte at det er riktig tidspunkt før serveren forfremmes og begynner å ta imot tilkoblinger; er det ikke det, stenges serveren ned, får et senere mål og startes igjen. Stoppunktet må ligge etter slutten av basebackupen, og dokumentasjonen anbefaler å sette opp og teste arkiveringen før den første basebackupen tas. Når gjenopprettingen er ferdig, fjerner serveren `recovery.signal`, slik at den ikke går inn i gjenopprettingsmodus igjen ved et uhell.

Engineer ApS tilbyr sikkerhetskopiering og gjenoppretting som tjeneste, beskrevet som sikkerhetskopier som er prøvd og ikke bare antatt å virke, og en nedskrevet plan for den morgenen en server ikke vil starte. To porteføljesider viser hva det betyr i praksis. I sikkerhetskopi og katastrofeberedskap i kode fra 2025 ble oppbevaringstiden for sikkerhetskopier satt opp i Bicep ved siden av databasen, slik at gjenoppretting til et vilkårlig tidspunkt er en del av malen og ikke en innstilling noen en gang klikket fram i en portal, og miljøet rundt databasen ble også definert som kode, for en database som gjenopprettes inn i et miljø man har bygd opp igjen etter hukommelsen, er knapt gjenopprettet. Deretter ble beredskapen gjennomgått og skrevet ned med hullene navngitt: georedundans var slått av, og målet for gjenopprettingstid var foreslått og ikke målt, fordi det ikke var gjennomført noen øvelse.

Selskapets automatisering av sikkerhetskopiering og gjenopprettingstester ble utformet for å utvide gjenopprettingsberedskapen utover leverandørens øyeblikksbilde. En Ansible-rolle installerer restic-skript og systemd-enheter for en databasedump der dette er konfigurert, krypterte, dedupliserte øyeblikksbilder over SFTP til lagring hos en annen leverandør, opprydding etter oppbevaringsregelen og integritetssjekker. En separat månedlig arbeidsflyt gjenoppretter en kjent fil til et midlertidig arbeidsområde og sammenligner bytene. Sikkerhetskopiering og gjenoppretting har separate signaler ved vellykket kjøring, passfrasen hentes fra en beskyttet fil, og timerne avhenger av et konfigurert sikkerhetskopirepo. Disse kontrolltiltakene er implementert; en gjenoppretting i drift er en separat leveranse. Implementeringsdokumentasjonen datert 2026-10-27 sier at timerne var

deaktivert uten et repo, og dokumenterer ingen fullført gjenoppretting i drift. Den underbygger dermed automatiseringsarbeidet, ikke en forpliktelse om gjenopprettingstid eller en påstand om at selskapet allerede trygt kan miste verten.

Hvor det går galt

Sikkerhetskopien er aldri blitt gjenopprettet. En jobb som melder suksess hver natt, sier ingenting om hvorvidt resultatet kan leses, dekrypteres og lastes inn, og den første ordentlige gjenopprettingen er et dårlig tidspunkt å finne ut av det på. Planlegg gjenopprettinger slik du planlegger sikkerhetskopier: en automatisk sjekk som henter ut kjente data og sammenligner dem, og en full gjenoppretting i et rent miljø så ofte at tiden den tar, er et målt tall.

Kopien deler skjebne med originalen. Et øyeblikksbilde i samme skykonto, en backupdisk i samme rack eller en arkiv-bucket bak samme administratorinnlogging går ned sammen med det som rammer primærsystemet. NISTs veiledning ber om at lagring utenfor stedet og alternative steder velges ut fra hvor usannsynlig det er at den samme katastrofen rammer dem. Ha minst én kopi hos en annen leverandør eller i en annen konto med egne påloggingsopplysninger, og oppbevar dekrypteringsnøklene et sted som ikke er avhengig av systemene de beskytter.

Det er bare lagt planer for dataene. Å gjenopprette en database er en liten del av å få en tjeneste opp igjen hvis servere, brannmurregler, DNS, sertifikater og hemmeligheter rundt den må gjenskapes etter hukommelsen. Beskriv miljøet som versjonskontrollert infrastruktur som kode, og gjør gjenoppbyggingen av det til en del av øvelsen, ikke bare innlastingen av data.

Målene er gjetning. Et RTO som er skrevet inn i et dokument uten en øvelse bak seg, er et forslag, og et RPO som forutsetter at hver eneste sikkerhetskopi lyktes, er optimistisk. Mål begge i en øvelse. NIST skiller mellom bordøvelser, som bare er diskusjon og ikke setter i gang utstyr, og funksjonelle øvelser som simulerer driften, opp til fullskalaøvelser som dekker alle deler av planen; tallene kommer fra den siste sorten.

En standby regnes som en sikkerhetskopi. En standby-server eller en georeplikert database beskytter mot tap av maskinvare, men den kopierer slettinger, korrupsjon og filer kryptert av løsepengevirus like trofast som gode

skrivinger. Ha kopier for vilkårlige tidspunkter som en feil på primærsystemet ikke kan nå, og behold dem lenger enn det vanligvis tar å oppdage en feil.

Planen beskriver fjorårets system. En driftshåndbok med nedlagte servere, folk som har sluttet, og passord som ikke lenger virker, sinker en gjenoppretting i stedet for å lede den. Gå gjennom planen etter hver vesentlig endring og etter hver øvelse, skriv ned hva øvelsen avslørte, og gå gjennom de delene som endres oftest, som kontaktlister, med kortere mellomrom, slik NIST også anbefaler.

Les mer

- SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems — hele veiledningen: hvordan den definerer og avgrenser en DRP, de sju planleggingstrinnene, MTD, RTO og RPO, alternative steder og øvelsestyper, med maler for planene.
- Continuous Archiving and Point-in-Time Recovery (PITR) — kapitlet i PostgreSQL 18 om WAL-arkivering, basebackuper og gjenoppretting til et valgt tidspunkt.
- Write Ahead Log — konfigurasjonsreferansen for `archive_command`, `restore_command` og innstillingene for hvor en gjenoppretting skal stoppe.

Ordliste

Velg ut fra deres faktiske rammer

Ta med utrullingsløpet, driftsrisikoene og dem som har vakt. Vi kan avgrense en endring med kontroller, en vei tilbake og tydelig ansvar.

Se hva det koster Ta kontakt →

Gjør begrepene praktiske

Spør hvordan «Hva er katastrofegjenoppretting?» gjelder i organisasjonen deres. Et konkret eksempel fra dagens system er nok til å starte samtalen.

Se tjenestene våre

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

Ta med deg denne siden

Visittkort

Laget med kjærlighet av D.

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

Opphavsrett © 2025 – nå · Engineer ApS · Alle rettigheter forbeholdt.

Skrevet ut fra https://engineer.company/nb/glossary/disaster-recovery/