Engineer

Disaster recovery

at genskabe driften efter et nedbrud med en afprøvet plan

Hvad det er

Disaster recovery er den del af beredskabsplanlægningen, der tager sig af det værste tilfælde: stedet, hvor et system kører, er tabt eller uden for rækkevidde i lang tid, og systemet skal genopbygges et andet sted ud fra kopier. NIST's vejledning i beredskabsplanlægning for amerikanske føderale it-systemer, SP 800-34 Revision 1 fra 2010, definerer en disaster recovery-plan som en skriftlig plan for at genoprette et eller flere informationssystemer på en alternativ facilitet efter en alvorlig hardware- eller softwarefejl eller efter, at faciliteterne er ødelagt. Anvendelsesområdet er snævert. Vejledningen forbeholder planen store, som regel fysiske afbrydelser, der afskærer adgangen til den primære facilitet i længere tid, og den dækker kun de afbrydelser, der kræver, at driften flyttes.

Den afgrænsning skiller den ud fra naboerne. En beredskabsplan for et enkelt informationssystem, i vejledningens sprog en information system contingency plan, genopretter ét system, uanset hvor det står, for eksempel efter en død disk eller en ødelagt database. Disaster recovery-planen er knyttet til et sted: den flytter driften til det alternative sted, og derfra bringes hvert system op efter sin egen beredskabsplan. En plan for én database og en plan for at miste et helt datacenter, en cloud-region eller en konto hos udbyderen er to forskellige dokumenter med forskellige ejere, og blander man dem sammen, ender man let uden nogen af dem.

Tre mål gør planen til noget, der kan efterprøves. Maksimal acceptabel nedetid (maximum tolerable downtime, MTD) er den samlede varighed af et nedbrud, som systemets ejer er villig til at acceptere. Målet for genopretningstid (recovery time objective, RTO) er det længste, en systemressource kan være ude af drift, før skaden på andre systemer og på forretningen bliver uacceptabel, og fordi afbrudt arbejde også skal behandles igen bagefter, skriver vejledningen, at RTO normalt skal være kortere end MTD. Målet for genopretningspunkt (recovery

point objective, RPO) ser bagud: det er det tidspunkt før nedbruddet, som data kan genskabes til ud fra den seneste sikkerhedskopi, og det udtrykker, hvor meget tabt data forretningen kan leve med. Kort sagt er RTO, hvor længe man er nede, og RPO, hvor meget arbejde man mister.

Det alternative sted findes i flere grader. Et cold site rummer kun lokaler og infrastruktur, et warm site er delvist udstyret, og et hot site er fuldt udstyret og bemandet. Vejledningen nævner også mobile anlæg, der i mange tilfælde kan leveres inden for 24 timer, før opsætningen går i gang, og spejlede anlæg, den dyreste løsning, som til gengæld ifølge vejledningen sikrer praktisk talt 100 % tilgængelighed. Et cold site er det billigste at holde i drift, men det kan tage lang tid at udstyre. I dag spiller en anden cloud-region eller en anden udbyder samme rolle for det meste software, og afvejningen mellem det, der står klar, og det, det koster at holde det klar, er den samme.

Brug begrebet i en beslutning

Brug »Hvad er disaster recovery?« i en konkret beslutning. Vi kan knytte begrebet til det system, I bygger eller køber. Sikkerhedskopier, der er testet og ikke bare antaget at virke, og en nedskrevet plan for den morgen, en server ikke starter igen.

Se vores ydelser Kontakt os →

Undersøg antagelserne bag ordet

Brug forklaringen og det tilknyttede arbejde til at formulere spørgsmål til jeres projekt. Vi kan undersøge antagelserne sammen, før et værktøj vælges. Har automatiseret 100 kritiske databackups — 100 kritiske backups af databaserne automatiseret

Har automatiseret 100 kritiske databackups Kontakt os →

Hvorfor det betyder noget

En backup er en kopi, og en kopi kører ingenting af sig selv. For at komme fra kopien til et fungerende system skal man også have softwaren, der læser den, nøglerne, der dekrypterer den, servere og netværk at køre den på, konfigurationen, der binder det hele sammen, og en person, der kender rækkefølgen. Alt det, der kun fandtes på det tabte sted, gik tabt sammen med det. Disaster recovery handler om at sikre, at det hele overlever den samme hændelse, og at forløbet fra kopi til tjeneste er afprøvet, før nogen får brug for det.

De data, der kan gendannes, er ikke nyere end den seneste kopi, der faktisk kan gendannes, uanset hvilket RPO backupplanen sigter mod. Har et natligt job fejlet i stilhed i en uge, risikerer man at miste en uges data, uanset hvad politikken siger. NIST’s vejledning siger det samme om bånd: sikkerhedskopier bør testes

jævnligt for at bekræfte, at data er gemt korrekt, og at filerne kan hentes uden fejl eller tab. En grøn statuslampe på et backupjob beviser, at noget blev skrevet. Kun en gendannelse beviser, at det kan læses igen.

Planen forfalder også. Folk stopper, servere bliver skiftet ud, udbydere laver deres konsoller om, og adgangskoderne i drejebogen udløber. Af de syv trin, NIST opstiller for beredskabsplanlægning, er de to sidste test, træning og øvelser samt vedligeholdelse af planen; vejledningen vil have planen til at være et levende dokument, der gennemgås mindst én gang om året, og hver gang systemet eller de ressourcer, genopretningen bruger, ændres væsentligt. En plan, der aldrig er øvet, falder typisk på detaljer, ingen tænkte på at skrive ned: rækkefølgen, tjenesterne skal startes i, en DNS-post med et døgns TTL, den ene adgangsnøgle, der lå på maskinen, som er væk.

For softwarehold er katastrofen ofte en konto snarere end en bygning. Et slettet cloud-projekt, et kompromitteret administratorlogin, en suspenderet konto hos udbyderen eller en destruktiv kommando kørt mod produktion fjerner adgangen til systemet lige så grundigt som en oversvømmelse. Standby-servere beskytter ikke mod den sidste af dem, for en standby udfører en fejlagtig `DROP TABLE` i løbet af øjeblikke, præcis som den udfører alle andre ændringer.

Sådan ser det ud i praksis

For en PostgreSQL-database kommer et RPO, der er langt kortere end intervallet mellem to backups, fra løbende arkivering af transaktionsloggen (write-ahead log, WAL) oven på en basebackup. Serveren kopierer hvert færdigt WAL-segment et sikkert sted hen, og en gendannelse afspiller segmenterne oven på basebackuppen frem til et valgfrit tidspunkt, efter at den blev taget:

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

Ved en gendannelse pakkes en basebackup ud i en ny datamappe, der lægges en tom fil ved navn `recovery.signal` i den, og genopretningsindstillingerne fortæller, hvor arkivet ligger, og hvor gendannelsen skal stoppe:

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

PostgreSQL-dokumentationen fortæller den historie, indstillingerne findes for: nogen sletter en vigtig tabel kl. 17.15 en tirsdag aften, opdager det onsdag ved middagstid og gendanner til kl. 17.14. Pause er standardhandlingen, når målet er nået, så man med forespørgsler kan bekræfte, at det er det rigtige tidspunkt, før serveren forfremmes og begynder at tage imod forbindelser; er det ikke, lukkes serveren ned, får et senere mål og startes igen. Stoppunktet skal ligge efter afslutningen af basebackuppen, og dokumentationen anbefaler at sætte arkiveringen op og teste den, før den første basebackup tages. Når gendannelsen er færdig, fjerner serveren `recovery.signal`, så den ikke ved et uheld går i gendannelsestilstand igen.

Engineer ApS tilbyder backup og disaster recovery som ydelse, beskrevet som afprøvede frem for formodede sikkerhedskopier og en skriftlig plan for den morgen, hvor en server ikke kommer op igen. To portfolio-sider viser, hvad det betyder i praksis. I backup og disaster recovery som kode fra 2025 blev opbevaringen af backups sat op i Bicep ved siden af databasen, så gendannelse til et vilkårligt tidspunkt er en del af templaten og ikke en indstilling, nogen engang klikkede på i en portal, og miljøet omkring databasen blev også defineret som kode, for en database, der gendannes i et miljø, man har genopbygget efter hukommelsen, er knap nok genoprettet. Derefter blev beredskabet gennemgået og skrevet ned med hullerne navngivet: geo-redundans var slået fra, og målet for genopretningstid var foreslået og ikke målt, fordi der ikke var gennemført nogen øvelse.

Virksomhedens automatiserede sikkerhedskopiering og gendannelsestest blev udformet til at udvide gendannelsesberedskabet ud over et udbydersnapshot. En Ansible-rolle installerer restic-scripts og systemd-enheder til et databasedump, hvor det er konfigureret, krypterede, deduplikerede snapshots over SFTP til lager hos en anden udbyder, udtynding efter opbevaringspolitikken og integritetstjek. Et separat månedligt workflow gendanner en kendt fil til et midlertidigt arbejdsområde og sammenligner dens bytes. Sikkerhedskopiering og gendannelse har hver sit successignal, adgangssætningen kommer fra en beskyttet fil, og timerne afhænger af et konfigureret backuplager. De kontroller er implementeret; en gendannelse i drift er en særskilt leverance. Implementeringsbeskrivelsen dateret 2026-10-27 angiver, at timerne var deaktiveret uden et backuplager, og dokumenterer ingen gennemført

gendannelse i drift. Den underbygger derfor automatiseringsarbejdet frem for et tilsagn om gendannelsestid eller en påstand om, at virksomheden allerede kan miste værten uden at bringe sine data i fare.

Hvor det går galt

Backuppen er aldrig blevet gendannet. Et job, der melder succes hver nat, siger intet om, hvorvidt resultatet kan læses, dekrypteres og indlæses, og den første rigtige gendannelse er et dårligt tidspunkt at finde ud af det på. Planlæg gendannelser, ligesom man planlægger backups: et automatisk tjek, der henter kendte data ud og sammenligner dem, og en fuld gendannelse i et rent miljø så tit, at den tid, den tager, er et målt tal.

Kopien deler skæbne med originalen. Et snapshot på samme cloud-konto, en backupdisk i samme rack eller en arkiv-bucket bag samme administratorlogin går ned med det, der rammer det primære system. NIST's vejledning beder om, at eksternt lager og alternative steder vælges ud fra, hvor usandsynligt det er, at den samme katastrofe rammer dem. Hav mindst én kopi hos en anden udbyder eller på en anden konto med separate adgangsoplysninger, og opbevar dekrypteringsnøglerne et sted, der ikke afhænger af de systemer, de beskytter.

Der er kun lagt planer for data. At gendanne en database er en lille del af at få en tjeneste op igen, hvis servere, firewallregler, DNS, certifikater og hemmeligheder omkring den skal genskabes efter hukommelsen. Beskriv miljøet som versionsstyret infrastruktur som kode, og gør genopbygningen af det til en del af øvelsen, ikke kun indlæsningen af data.

Målene er gætværk. Et RTO, der er skrevet ind i et dokument uden en øvelse bag sig, er et forslag, og et RPO, der forudsætter, at hver eneste backup lykkedes, er optimistisk. Mål begge i en øvelse. NIST skelner mellem bordøvelser, som kun er diskussion og ikke sætter udstyr i gang, og funktionelle øvelser, der simulerer driften, op til fuldskalaøvelser, der dækker alle dele af planen; tallene kommer fra den sidste slags.

En standby regnes for en backup. En standby-server eller en georeplikeret database beskytter mod tab af hardware, men den kopierer sletninger, korruption og filer krypteret af ransomware lige så trofast som gode skrivninger. Hav kopier til et vilkårligt tidspunkt, som en fejl på det primære system ikke kan nå, og behold dem længere, end det normalt tager at opdage en fejl.

Planen beskriver sidste års system. En drejebog med nedlagte servere, folk, der er stoppet, og adgangskoder, der ikke længere virker, sinker en genopretning i stedet for at guide den. Gennemgå planen efter hver væsentlig ændring og efter hver øvelse, skriv ned, hvad øvelsen afslørede, og gennemgå de dele, der skifter oftest, som kontaktlister, med kortere mellemrum, sådan som NIST også anbefaler.

Læs mere

- SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems — hele vejledningen: hvordan den definerer og afgrænser en DRP, de syv planlægningstrin, MTD, RTO og RPO, alternative steder og øvelsestyper, med skabeloner til planerne.
- Continuous Archiving and Point-in-Time Recovery (PITR) — kapitlet i PostgreSQL 18 om WAL-arkivering, basebackups og gendannelse til et valgt tidspunkt.
- Write Ahead Log — konfigurationsreferencen for `archive_command`, `restore_command` og indstillingerne for, hvor en gendannelse skal stoppe.

Ordliste

Vælg ud fra jeres faktiske vilkår

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Gør begreberne praktiske

Spørg, hvordan »Hvad er disaster recovery?« gælder i jeres organisation. Et konkret eksempel fra jeres nuværende system er nok til at begynde samtalen.

Se vores ydelser

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

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

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

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://engineer.company/da/glossary/disaster-recovery/