Engineer

Disaster Recovery

Dienste nach großem Verlust mit erprobtem Plan zurückbringen

Was es ist

Disaster Recovery ist der Teil der Notfallplanung für den schlimmsten Fall: Der Standort eines Systems ist verloren oder lange nicht erreichbar, und das System muss anderswo aus Kopien neu aufgebaut werden. NISTs Contingency Planning Guide for Federal Information Systems, SP 800-34 Revision 1 von 2010, definiert den Disaster-Recovery-Plan als schriftlichen Plan zur Wiederherstellung eines oder mehrerer Informationssysteme an einem Ausweichstandort nach einem schweren Hardware- oder Softwareausfall oder der Zerstörung von Einrichtungen. Sein Geltungsbereich ist eng. Der Leitfaden sieht ihn für schwere, meist physische Störungen vor, die den Zugang zum Hauptstandort längere Zeit verhindern. Er deckt nur Störungen ab, die einen Standortwechsel erfordern.

Diese enge Fassung unterscheidet ihn von benachbarten Plänen. Ein Notfallplan für ein Informationssystem stellt im Sprachgebrauch des Leitfadens ein einzelnes System an seinem jeweiligen Standort wieder her, ob nach einem Festplattenausfall oder einer beschädigten Datenbank. Der Disaster-Recovery-Plan ist standortbezogen: Er verlagert den Betrieb an den Ausweichstandort. Dort wird jedes System nach seinem eigenen Notfallplan hochgefahren. Ein Plan für eine Datenbank und ein Plan für den Verlust eines ganzen Rechenzentrums, einer Cloudregion oder eines Anbieterkontos sind verschiedene Dokumente mit verschiedenen Verantwortlichen. Wer sie verwechselt, hat am Ende leicht weder den einen noch den anderen Plan.

Drei Messgrößen machen aus einer Absicht einen überprüfbaren Plan. Die maximal tolerierbare Ausfallzeit (MTD) ist die gesamte Ausfalldauer, die der Systemverantwortliche hinzunehmen bereit ist. Das Wiederanlaufzeitziel (RTO) ist die längste Zeit, die eine Systemressource nicht verfügbar sein darf, bevor der Schaden für andere Systeme und den Geschäftsbetrieb untragbar wird. Weil danach auch die unterbrochene Arbeit nachzuholen ist, muss das RTO laut Leitfaden normalerweise kürzer als die MTD sein. Das

Wiederherstellungspunktziel (RPO) blickt zurück: Es ist der Zeitpunkt vor dem Ausfall, auf den Daten aus der jüngsten Sicherungskopie wiederhergestellt werden können. Es drückt aus, wie viel Datenverlust der Geschäftsbetrieb verträgt. Einfach gesagt: Das RTO ist die Ausfalldauer, das RPO die Menge verlorener Arbeit.

Ausweichstandorte gibt es in verschiedenen Ausbaustufen. Ein kalter Ausweichstandort (Cold Site) bietet nur Raum und Infrastruktur, ein warmer (Warm Site) ist teilweise ausgestattet, und ein heißer (Hot Site) ist vollständig ausgestattet und mit Personal besetzt. Der Leitfaden ergänzt mobile Standorte, die oft innerhalb von 24 Stunden geliefert werden können, bevor der Aufbau beginnt, sowie gespiegelte Standorte: die teuerste Variante, der er „praktisch 100 Prozent Verfügbarkeit“ zuschreibt. Kalte Ausweichstandorte verursachen die geringsten Vorhaltekosten, ihre Ausstattung kann aber beträchtliche Zeit beanspruchen. Für die meiste heutige Software übernehmen eine zweite Cloudregion oder ein zweiter Anbieter dieselbe Rolle. Die Abwägung zwischen Bereitschaft und ihren Vorhaltekosten bleibt gleich.

Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist Disaster Recovery?“ für eine konkrete Entscheidung. Wir können helfen, das Konzept mit dem System in Verbindung zu bringen, das Sie entwickeln oder einkaufen. Sicherungen, deren Funktion geprüft und nicht vorausgesetzt wird, und ein schriftlicher Plan für den Morgen, an dem ein Server nicht wieder startet.

Unsere Leistungen entdecken Kontakt aufnehmen →

Die Annahmen hinter dem Begriff prüfen

Nutzen Sie die Erklärung und die verlinkten Arbeiten, um Fragen für Ihr Projekt zu formulieren. Wir können die Annahmen gemeinsam mit Ihnen prüfen, bevor ein Werkzeug ausgewählt wird. 100 wichtige Sicherungen mit Barman automatisiert — 100 automatisierte geschäftskritische Datenbanksicherungen

100 wichtige Sicherungen mit Barman automatisiert Kontakt aufnehmen →

Warum es wichtig ist

Eine Sicherung ist eine Kopie, und eine Kopie allein betreibt nichts. Von der Kopie zum funktionierenden System braucht es auch die lesende Software, die Entschlüsselungsschlüssel, Server und Netzwerk für den Betrieb, die verbindende Konfiguration und jemanden, der die richtige Reihenfolge kennt. Alles davon, was nur am verlorenen Standort existierte, ging mit ihm verloren. Disaster Recovery sorgt dafür, dass alle diese Bestandteile dasselbe Ereignis überstehen und dass der Weg von der Kopie zum Dienst schon einmal beschritten wurde, bevor ihn jemand braucht.

Die wiederherstellbaren Daten reichen nur bis zur letzten wiederherstellbaren Kopie, unabhängig davon, welches RPO der Sicherungsplan erfüllen soll. Ein nächtlicher Job, der seit einer Woche unbemerkt fehlschlägt, gefährdet die Daten einer ganzen Woche, unabhängig vom Richtliniendokument. NISTs Leitfaden macht denselben Punkt für Bandmedien: Sicherungen sollen regelmäßig geprüft werden, um die korrekte Speicherung und das Abrufen der Dateien ohne Fehler oder Verlust zu bestätigen. Eine grüne Statusanzeige eines Sicherungsjobs belegt, dass etwas geschrieben wurde. Erst eine Wiederherstellung belegt, dass es sich zurücklesen lässt.

Auch der Plan veraltet. Menschen gehen, Server werden ersetzt, Anbieter gestalten ihre Konsolen um, und Passwörter im Betriebshandbuch laufen ab. Von NISTs sieben Schritten der Notfallplanung sind die letzten beiden Tests, Schulung und Übungen sowie die Pflege des Plans. Der Leitfaden verlangt ein lebendes Dokument, das mindestens jährlich und bei wesentlichen Änderungen am System oder den Wiederherstellungsressourcen überprüft wird. Ein nie geprobter Plan scheitert oft an Details, die niemand aufgeschrieben hat: der Startreihenfolge der Dienste, einem DNS-Eintrag mit einem Tag Gültigkeitsdauer, den einzigen Zugangsdaten auf dem verschwundenen Rechner.

Für Softwareteams betrifft die Katastrophe häufig ein Konto statt eines Gebäudes. Ein gelöschtes Cloudprojekt, ein kompromittierter Administratorzugang, ein gesperrtes Anbieterkonto oder ein destruktiver Befehl in Produktion entzieht den Systemzugang genauso vollständig wie eine Überschwemmung. Standby-Server schützen vor dem letzten Fall nicht. Ein Standby übernimmt ein irrtümliches `DROP TABLE` innerhalb von Augenblicken, genau wie jede andere Änderung.

Wie es in der Praxis aussieht

Bei einer PostgreSQL-Datenbank lässt sich das mögliche Datenverlustfenster durch kontinuierliche Archivierung des Write-Ahead-Logs (WAL) zusätzlich zu einer Basissicherung weit unter den Abstand zwischen zwei Sicherungen verkürzen. Der Server kopiert jedes abgeschlossene WAL-Segment an einen sicheren Ort. Bei einer Wiederherstellung werden diese Segmente auf der Basissicherung bis zu einem beliebigen gewählten Zeitpunkt seit ihrer Erstellung nachgespielt:

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

Zur Wiederherstellung wird eine Basissicherung in ein neues Datenverzeichnis entpackt und dort eine leere Datei namens `recovery.signal` angelegt. Die Wiederherstellungseinstellungen nennen den Archivort und den Haltepunkt:

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

Die PostgreSQL-Dokumentation erzählt den Anlass für diese Einstellungen: Jemand löscht am Dienstagabend um 5:15 eine kritische Tabelle, bemerkt es am Mittwochmittag und stellt den Stand von 5:14 wieder her. Beim Erreichen des Ziels wird standardmäßig pausiert. Abfragen können so den richtigen Zeitpunkt bestätigen, bevor der Server für die Annahme von Verbindungen hochgestuft wird. Ist es der falsche Zeitpunkt, wird der Server heruntergefahren, mit einem späteren Ziel versehen und neu gestartet. Der gewählte Wiederherstellungszeitpunkt muss nach dem Abschluss der Basissicherung liegen. Die Dokumentation empfiehlt, die Archivierung vor der ersten Basissicherung einzurichten und zu testen. Nach abgeschlossener Wiederherstellung entfernt der Server `recovery.signal`, damit er nicht versehentlich erneut in den Wiederherstellungsmodus geht.

Engineer ApS bietet Sicherung und Disaster Recovery als Leistung an: Sicherungen werden geprüft statt vorausgesetzt, und es gibt einen schriftlichen Plan für den Morgen, an dem ein Server nicht zurückkommt. Zwei Portfolioseiten zeigen, was das bedeutet. Bei Sicherungen und Disaster Recovery als Code aus der seit 2025 laufenden Tätigkeit wurde die Sicherungsaufbewahrung in Bicep neben der Datenbank festgelegt. Die zeitpunktbezogene Wiederherstellung ist so Teil der Vorlage statt einer irgendwann im Portal angeklickten Einstellung. Auch die Umgebung um die Datenbank wurde als Code definiert. Denn eine Datenbank ist kaum als wiederhergestellt anzusehen, wenn ihre Umgebung aus dem Gedächtnis neu aufgebaut wurde. Der Wiederherstellungsstand wurde anschließend geprüft und mit benannten Lücken dokumentiert: Georedundanz war abgeschaltet, und das Wiederanlaufzeitziel war vorgeschlagen statt gemessen, weil keine Übung stattgefunden hatte.

Die Automatisierung von Sicherungen und Wiederherstellungstests des Unternehmens wurde dafür entworfen, Wiederherstellung über einen Anbietersnapshot hinaus zu ermöglichen. Eine Ansible-Rolle installiert restic-Skripte und systemd-Units für einen Datenbankdump, sofern dieser konfiguriert ist, verschlüsselte, deduplizierte Snapshots per SFTP auf den Speicher eines anderen Anbieters, das Ausdünnen nach Aufbewahrungsregeln und Integritätsprüfungen. Ein getrennter monatlicher Ablauf stellt eine bekannte Datei an einem temporären Arbeitsort wieder her und vergleicht ihre Bytes. Sicherung und Wiederherstellung haben getrennte Erfolgssignale, die Passphrase kommt aus einer geschützten Datei, und die Timer hängen von einem konfigurierten Repository ab. Diese Kontrollen sind implementiert; eine tatsächlich durchgeführte Wiederherstellung ist ein gesondertes Arbeitsergebnis. Der Implementierungsnachweis vom 2026-10-27 sagt, dass die Timer ohne Repository deaktiviert waren, und verzeichnet keine tatsächlich abgeschlossene Wiederherstellung. Er belegt daher die Automatisierungsarbeit, kein zugesagtes Wiederanlaufzeitziel und keine Behauptung, das Unternehmen könne den Host bereits gefahrlos verlieren.

Wo es schiefgeht

Die Sicherung wurde nie wiederhergestellt. Ein Job, der jede Nacht Erfolg meldet, sagt nichts darüber aus, ob sich seine Ausgabe lesen, entschlüsseln und laden lässt. Die erste echte Wiederherstellung ist ein schlechter Zeitpunkt, das herauszufinden. Planen Sie Wiederherstellungen wie Sicherungen: eine automatisierte Prüfung, die bekannte Daten abruft und vergleicht, sowie eine vollständige Wiederherstellung in eine saubere Umgebung, die oft genug geübt wird, dass ihre Dauer als Messwert vorliegt.

Die Kopie teilt das Schicksal des Originals. Ein Snapshot im selben Cloudkonto, eine Sicherungsplatte im selben Rack oder ein Archivbucket hinter demselben Administratorzugang fällt mit dem Primärsystem aus. NISTs Leitfaden verlangt, externe Lagerorte und Ausweichstandorte danach auszuwählen, wie gering die Wahrscheinlichkeit ist, dass dieselbe Katastrophe sie ebenfalls trifft. Halten Sie mindestens eine Kopie bei einem anderen Anbieter oder in einem anderen Konto mit getrennten Zugangsdaten vor. Bewahren Sie Entschlüsselungsschlüssel an einem Ort auf, der nicht von den geschützten Systemen abhängt.

Nur die Daten wurden eingeplant. Die Wiederherstellung einer Datenbank ist nur ein kleiner Teil des Wiederanlaufs eines Dienstes, wenn Server, Firewallregeln, DNS, Zertifikate und Geheimnisse aus dem Gedächtnis neu

erstellt werden müssen. Definieren Sie die Umgebung als versionsverwaltete Infrastructure as Code und machen Sie ihren Neuaufbau ebenso zum Übungsteil wie das Laden der Daten.

Die Ziele sind Schätzungen. Ein RTO ohne vorausgegangene Übung ist im Dokument ein Vorschlag. Ein RPO, das jede Sicherung für erfolgreich hält, ist optimistisch. Messen Sie beide in einer Übung. NIST unterscheidet Planspiele, die nur aus Gesprächen bestehen und keine Geräte einsetzen, von funktionalen Übungen, die den Betrieb simulieren, bis hin zu Vollübungen für jedes Element des Plans. Die Zahlen stammen aus der zweiten Art.

Ein Standby zählt als Sicherung. Ein Standby-Server oder eine georeplizierte Datenbank bietet Schutz für den Fall eines Hardwareverlusts, kopiert aber Löschungen, Beschädigungen und durch Ransomware verschlüsselte Dateien genauso treu wie korrekte Schreibvorgänge. Halten Sie zeitpunktbezogene Kopien vor, die ein Fehler auf dem Primärsystem nicht erreichen kann, und bewahren Sie sie länger auf, als das Bemerken eines Fehlers üblicherweise dauert.

Der Plan beschreibt das System vom letzten Jahr. Ein Betriebshandbuch mit ausgemusterten Servern, ausgeschiedenen Personen und ungültigen Passwörtern bremst eine Wiederherstellung, statt sie anzuleiten. Prüfen Sie den Plan nach jeder wesentlichen Änderung und jeder Übung, halten Sie Übungsfehler fest und prüfen Sie häufig geänderte Teile wie Kontaktlisten noch öfter, wie auch NIST empfiehlt.

Weiterführende Lektüre

- SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems — der vollständige Leitfaden: Definition und Umfang des DRP, die sieben Planungsschritte, MTD, RTO und RPO, Ausweichstandorte und Übungsarten samt Planvorlagen.
- Kontinuierliche Archivierung und zeitpunktbezogene Wiederherstellung (PITR) — das Kapitel von PostgreSQL 18 über WAL-Archivierung, Basissicherungen und Wiederherstellung auf einen gewählten Zeitpunkt.
- Write Ahead Log — die Konfigurationsreferenz für `archive_command`, `restore_command` und die Zielparameter der Wiederherstellung.

Glossar

Für Ihre tatsächlichen Rahmenbedingungen auswählen

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

Preise ansehen Kontakt aufnehmen →

Die Begriffe praktisch nutzbar machen

Fragen Sie, wie „Was ist Disaster Recovery?“ auf Ihre Organisation zutrifft. Ein konkretes Beispiel aus Ihrem bestehenden System reicht aus, um das Gespräch zu beginnen.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

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

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://engineer.company/de/glossary/disaster-recovery/