

Recovery Bewezen

Case study: een volledige uitwijktest in 49 minuten

Inhoud

De vraag: bewijs het	3
De opzet: drie onafhankelijke lagen	3
De infrastructuur: drie Nederlandse datacenters	4
Test 1: Database-restore in 90 seconden	5
Test 2: Point-in-time recovery op de seconde	5
Test 3: De volledige uitwijktest	5
Het resultaat: cijfers in plaats van schattingen	7
Waarom dit standaard zou moeten zijn	8

De vraag: bewijs het

Een van onze klanten in een gereguleerde sector kreeg een externe audit op de beheersmaatregelen rond hun platform. De auditors stelden niet de vraag “zijn er backups?” Die stellen ze nooit. De vraag was: **laat zien dat ze werken**. Een uitgevoerde backup met log, een geteste recovery-procedure met rapportage, en hersteldoelstellingen die ergens op gebaseerd zijn.

Dat is het verschil tussen backups hebben en backups kunnen bewijzen. Wij besloten het verschil meetbaar te maken: niet één test, maar drie, op dezelfde dag, vastgelegd in de eigen rapportageformats van de auditor.

De opzet: drie onafhankelijke lagen

Het platform draait als Kubernetes-cluster op onze eigen infrastructuur. De bescherming tegen dataverlies bestaat uit drie lagen die onafhankelijk van elkaar mogen falen:

Laag	Wat	Bijzonderheden
VM-backups	Het complete platform, twee keer per dag	AES-256 versleuteld, opgeslagen in een ánder datacenter, dagelijkse checksumverificatie, getrapte retentie tot ruim 6 maanden terug
Database-backups	Applicatie-consistente PostgreSQL-backups + continue WAL-archivering	Point-in-time recovery: herstel naar een willekeurig moment, opslag buiten het cluster
Configuratie als code	Alle platformconfiguratie in git	Elke wijziging herleidbaar; het platform is reproduceerbaar

Maar een groen dashboard zegt weinig. De enige manier om te weten dat deze lagen werken, is herstellen en verifiëren.

De infrastructuur: drie Nederlandse data-centers

Het platform draait op onze eigen hardware, verdeeld over drie ISO 27001-gecertificeerde Nederlandse datacenters. De geografische spreiding maakt het uitwijkscenario echt: de backups staan in een ander datacenter dan de workload die ze beschermen.

Datacenter	Rol in deze test
Naaldwijk (DC1)	Productieworkload (bron), gedurende de hele test ongemoeid
Amsterdam (DC2)	Versleutelde backups en het uitwijk-hersteldoel, 62 km van DC1
Zoetermeer (DC3)	Offsite tape-archief

Naaldwijk (DC1) — 62 km — Amsterdam (DC2) Zoetermeer (DC3)
Productie Versleutelde backups Offsite tape-
(gesimuleerd down) + uitwijk-hersteldoel archief
x |
v
7 VM's hersteld op een geïsoleerd netwerk.
etcd-quorum, 9 databaseclusters en object-
opslag kwamen terug zonder ingrijpen.

Test 1: Database-restore in 90 seconden

De database van het platform is vanaf de objectstore hersteld naar een apart, nieuw databasecluster, zonder de draaiende omgeving aan te raken. Negentig seconden na het aanmaken van het herstelmanifest stond er een gezonde database. Verificatie op rijnniveau: identiek aan de bron, tot op het laatste record.

Test 2: Point-in-time recovery op de seconde

De sterkste vorm van databaseherstel is niet “terug naar vannacht”, maar “terug naar 13:59, vlak vóór de foutieve wijziging van 14:00”. Dat hebben we aangetoond met een markertest:

1. Marker A weggeschreven en tijdstip T vastgelegd; zes seconden later marker B om de fout te simuleren.
2. Database hersteld naar exact tijdstip T.
3. Resultaat: marker A aanwezig, marker B afwezig. Herstel op de seconde nauwkeurig, in opnieuw circa 90 seconden.

Test 3: De volledige uitwijktest

De hoofdtest simuleerde het zwaarste scenario: *het primaire datacenter is volledig onbeschikbaar*. Alle zeven virtuele machines van het platform, zes Kubernetes-nodes plus de gateway, zijn vanaf de versleutelde backups hersteld in het uitwijkdatacenter, op een volledig geïsoleerd netwerksegment. De live omgeving is op geen enkel moment geraakt.

Mijlpaal	Tijd
Restore van alle 7 VM's (parallel)	26m23s
Alle VM's gestart	+3 min
Kubernetes-cluster: quorum hersteld, alle nodes Ready	+18 min
Dataverificatie afgerond (9 databaseclusters healthy, applicatiedata gecontroleerd op rijnniveau)	+2 min

Er kwam geen handmatig ingrijpen aan te pas: het etcd-quorum vormde zich zelfstandig uit snapshots die minuten uit elkaar gemaakt waren, alle databaseclusters kwamen gezond op en de objectopslag was direct bevroegbaar. Geen datamanipulatie, geen herconfiguratie.

Waarom je test

De test leverde ook twee kleine vondsten op: gedrag dat alleen in volledige isolatie optreedt. Beide zijn direct in het herstelrunbook verwerkt. Dat is geen smetje op de test; het is wáárom je test. Een runbook dat nooit tegen de werkelijkheid is gehouden, is een hoop aannames met een nietje erdoor.

Het resultaat: cijfers in plaats van schattingen

RTO en RPO

RTO (Recovery Time Objective): hoe lang herstel mag duren voordat het platform weer draait. **RPO** (Recovery Point Objective): hoeveel data je mag verliezen, oftewel hoe ver terug de meest recente bruikbare kopie ligt.

Doelstelling	Waarde	Onderbouwing
RTO (doel)	4 uur	Inclusief detectie, besluitvorming en opkomsttijd
RTO (gemeten)	49 minuten	Volledige uitwijktest
RPO (VM-laag)	max 12 uur	Twee backups per dag
RPO (databases)	≤ 5 minuten	Continue WAL-archivering

De klant ging het auditgesprek in met gemeten cijfers in plaats van schattingen, en met testverslagen waarin elke claim te herleiden is tot letterlijke commando-uitvoer.

Wat de auditor ontving

Drie deliverables, dezelfde dag: een herstelrunbook, twee ondertekenbare testrapporten in het format van de auditor zelf, en de letterlijke commando-uitvoer achter elk cijfer (restore-tijden, etcd- en node-status, datacontroles op rijniveau, bucket-listings).

Waarom dit standaard zou moeten zijn

Een backup bestaat pas als de restore bewezen is. Daarom horen restore-tests bij ons niet alleen bij een audit, maar bij het draaien van een managed platform. Het verificatie-regime spreken we per platform af. Een typisch regime:

Wat	Frequentie
Geautomatiseerde backupverificatie	Dagelijks
Database-restoretest	Per kwartaal
Volledige uitwijktest	Jaarlijks

De audit maakt het zichtbaar; het werk gebeurt het hele jaar.

Waar dit standaard is

Dit herstelregime hoort bij onze [Managed Clusters](#) (dedicated Kubernetes, vanaf €2.500 per maand) en onze [CaffeineStacks](#) managed servers (vanaf €300 per maand). Dezelfde backuplagen, dezelfde geteste restores, op infrastructuur die we zelf bezitten.

Draait jouw platform op infrastructuur waarvan je dit kunt aantonen? Wij laten het graag zien, met een stopwatch erbij.