

Disaster Recovery Plan – FileCap SaaS op Scaleway (ISO 27001)

Veld	Waarde
Documentversie	2.0 (Scaleway)
Datum	25 augustus 2026
Norm	ISO/IEC 27001, Annex A.17 (bedrijfscontinuïteit)
Platform	Scaleway – regio nl-ams (Amsterdam), zone nl-ams-1
Off-site back-uplocatie	Contec datacenter

1. Doel en Scope

Dit Disaster Recovery Plan (DRP) beschrijft de procedures voor herstel van kritieke infrastructuur en data van het FileCap SaaS-product, draaiend op Scaleway, bij een incident. Dit plan is opgesteld conform de eisen van ISO/IEC 27001, Annex A.17 (informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer).

Scope van infrastructuurcomponenten (per omgeving: DEVELOPMENT, TESTING, ACCEPTANCE, PRODUCTION — elk een eigen Scaleway-project):

- Scaleway Load Balancer (productie: LB-GP-L) met Traefik als ingress controller (proxy protocol v2, sticky sessions, TLS $\geq$ 1.2)
- Scaleway Managed Database for MySQL 8 (RDB; productie: db-pop2-2c-8g, HA-cluster, uitsluitend private network) met cross-zone DR-read-replica
- Scaleway Kapsule (managed Kubernetes, Cilium CNI, private nodes, API-toegang via ACL beperkt tot het Contec-kantoor en Scaleway-ranges)
- Scaleway Object Storage buckets: config en storage (private ACL, per omgeving geprefixt, bijv. production-filecap-config)
- Scaleway Managed Database for Redis (2 nodes, TLS, uitsluitend private network) — sessie-/cachedata
- Scaleway Secret Manager (databasecredentials, Redis-credentials, S3-keys, JWT-keypair, Office 365-secrets)
- VPC met private network en public gateway (NAT, bastion, SMTP); certificaten via cert-manager met ACME (Let's Encrypt en Actalis met EAB), HTTP-01-challenge via Traefik
- Uitrol via OpenTofu (Infrastructure as Code), beheerd en uitgevoerd via GitLab CI/CD; state in de GitLab HTTP-backend (state per omgeving/branch)

Scope van data-back-up:

- Object Storage buckets: config en storage
- RDB-database (MySQL 8)
- Back-upretentietijd: 7 dagen

Buiten scope: Redis (vluchtige sessie-/cachedata, wordt bij herstel leeg opnieuw aangemaakt) en monitoringdata in Scaleway Cockpit.

2. Beleidsverklaring

Het waarborgen van de beschikbaarheid en integriteit van de cloudomgeving is essentieel voor de bedrijfscontinuïteit. Herstelprocedures zijn ontworpen om bij een storing binnen 4 uur te kunnen reageren en binnen 24 uur de dienst te herstellen.

3. Recovery Objectives

Type	Waarde
RTO (Recovery Time Objective)	24 uur
RPO (Recovery Point Objective)	24 uur (back-ups < 24 uur oud)
Back-upretentie	7 dagen
RTO/RPO bij zone-uitval database (promotie DR-replica)	RTO: minuten; RPO: replicatievertraging (nagenoeg nul, asynchrone replicatie)

Toelichting: voor uitval van een enkele database-node zorgt het HA-cluster voor automatische failover. Voor zone-uitval is er een expliciete cross-zone read-replica die handmatig gepromoveerd wordt (zie 5.2). Voor alle overige scenario's (waaronder verlies van de regio of het Scaleway-platform) geldt herstel vanuit de back-up in het Contec datacenter, binnen de algemene RTO/RPO van 24 uur.

4. Back-up Strategie

Back-ups worden niet naar een andere cloudregio gerepliceerd, maar dagelijks naar het Contec datacenter gekopieerd (off-site, buiten het Scaleway-platform). Hiermee is de back-up ook beschermd tegen platformbreed falen of verlies van toegang tot het Scaleway-account.

- Voor de Object Storage buckets (config en storage) wordt dagelijks een back-up gemaakt naar het Contec datacenter.
- De RDB-database (MySQL) wordt dagelijks geback-up: de door Scaleway beheerde automatische back-ups, plus een dagelijkse kopie (dump) naar het Contec datacenter.
- Daarnaast draait voor de productiedatabase continu een asynchrone cross-zone read-replica binnen Scaleway (nl-ams), als snelle herstellijn bij zone-uitval.
- Back-upretentie: 7 dagen voor alle componenten.
- Alle back-uptransporten zijn versleuteld en worden gemonitord op fouten; falende back-upjobs genereren een alert.
- Secrets staan in Scaleway Secret Manager en worden grotendeels door OpenTofu (her)aangemaakt; handmatig ingevoerde secrets (Office 365 OAuth-credentials, Actalis EAB-key) zijn separaat veilig vastgelegd bij Contec.

5. Herstelprocedures

5.1 Scaleway Load Balancer en Traefik ingress

- De load balancer en Traefik worden volledig automatisch uitgerold via OpenTofu (module `traefik_ingress_controller`); Traefik koppelt zich via de `scw-loadbalancer-id`-annotatie aan de aangemaakte LB.
- Herstel: `tofu apply` uitvoeren vanuit versiebeheer (GitLab-pipeline of lokaal).
- Certificaten hoeven niet handmatig gekoppeld te worden: `cert-manager` vraagt ze automatisch opnieuw aan zodra DNS naar de nieuwe load balancer verwijst (zie 5.5 en 5.6).
- Na heruitrol: het nieuwe publieke LB-IP opvragen met `"tofu output traefik_load_balancer_ip"` en DNS bijwerken (zie 5.6).

5.2 Scaleway Managed Database MySQL (RDB)

Scenario A – zone-uitval (productie en LWI): promotie van de cross-zone DR-replica, conform de runbook docs/db-dr-promote.md in de Terraform-repository:

1. Bevestig dat de hoofdinstantie daadwerkelijk onbereikbaar is (Scaleway-statuspagina, zone-incident). Promotie is onomkeerbaar: de replica stopt met repliceren en wordt zelfstandig.
2. Zoek de replica op: "scw rdb read-replica list region=nl-ams" (IP ook via "tofu output db_dr_replica_ip").
3. Promoveer: "scw rdb read-replica promote <replica-id> region=nl-ams --wait".
4. Stel het private IP van de gepromoveerde instantie vast ("scw rdb endpoint list").
5. Werk in Secret Manager het host-veld bij van de secrets filecap-db-credentials, fcl-db-credentials en filecap-db-root-credentials (nieuwe secret-versie; gebruikersnaam en wachtwoord blijven gelijk).
6. Herstart de afnemers: "kubectl -n filecap rollout restart deployment" en "kubectl -n filecap-license rollout restart deployment".
7. Verifieer: portal bereikbaar, transfers werken, applicatielogs tonen een gezonde databaseverbinding. Reconcileer daarna de OpenTofu-state (state surgery of fail-back) volgens de runbook.

Scenario B – dataverlies of volledig verlies van de instantie: herstel uit back-up.

- Herstel uit de door Scaleway beheerde back-up (Scaleway Console of "scw rdb backup restore"), of — indien Scaleway zelf niet beschikbaar is — herstel de laatste dagelijkse dump uit het Contec datacenter op een nieuw aangemaakte RDB-instantie.
- Na herstel: het host-veld in de drie databasecredential-secrets bijwerken indien het IP gewijzigd is, deployments herstarten en verbindingen vanuit Kapsule en de applicatielaag testen.
- Overige omgevingen (development, testing, acceptance) hebben geen DR-replica; daar is herstel uit back-up altijd de herstellijn.

5.3 Scaleway Kapsule (Kubernetes)

- Cluster, nodepool, VPC, private network, public gateway, IAM en ACL's herstellen via OpenTofu ("tofu apply" met de tfvars van de betreffende omgeving).
- Na apply: kubeconfig ophalen ("scw k8s kubeconfig install <cluster-id> region=nl-ams") en de GitLab Kubernetes-agent opnieuw koppelen (FileCap/kubernetesagents).
- Kubernetes-workloads worden uitgerold via de GitLab CI/CD-deploymentrepositories, in deze volgorde: rabbitmq-deployment, filecap-app-deployment, filecap-jobs-deployment, filecap-address-book-deployment, filecap-license-deployment.
- Secrets worden hersteld vanuit Scaleway Secret Manager; de S3-access-/secret-key (tofu-output) in de filecap-app-deployment zetten.
- Handmatige nazorg: de Office 365 OAuth-secrets (office-365-client-secret, office-365-token-cache-secret) bevatten na een verse apply placeholderwaarden en moeten handmatig via de Scaleway-console worden gevuld; de OAuth-flow is niet te automatiseren.
- Basiscomponenten (cert-manager, Kyverno-polities, NFS-provisioner met storageclass nfs-rwx, external-secrets, kube-prometheus-stack, Promtail) worden door dezelfde tofu apply geïnstalleerd.

5.4 Scaleway Object Storage

- Beschadigde of verwijderde objecten in de buckets config en storage herstellen vanuit de dagelijkse back-up in het Contec datacenter (terugkopiëren naar de bucket).
- Indien de buckets zelf gewist zijn: "tofu apply" om lege buckets opnieuw aan te maken, daarna de objecten terugzetten vanuit de back-up in het Contec datacenter.
- Toegang tot de buckets loopt via de IAM-applicatie en bijbehorende API-keys die OpenTofu aanmaakt (secret s3-app-credentials); na heruitrol de nieuwe keys in de applicatiedeployment doorvoeren.

5.5 Certificaten (cert-manager / ACME)

- Certificaten worden niet handmatig beheerd: cert-manager in het cluster geeft ze uit via ACME met HTTP-01-challenges via Traefik.
- Issuers: Let's Encrypt (productie en staging) en Actalis (met External Account Binding). De Actalis EAB-HMAC-key wordt als OpenTofu-variabele aangeleverd en als Kubernetes-secret (actalis-eab) geplaatst.
- Herstel: zodra het cluster draait en DNS naar de nieuwe load balancer verwijst, worden certificaten automatisch opnieuw aangevraagd. Controle: "kubectl get clusterissuer -A" en de status van de Certificate-resources.

5.6 DNS-herstel – TransIP (filecap.tech)

Bij een DR waarbij een nieuwe Scaleway-omgeving wordt uitgerold, krijgt de load balancer een nieuw publiek IP-adres. De DNS-records bij TransIP moeten dan handmatig worden bijgewerkt: de A-records verwijzen naar het publieke IP van de load balancer, voor zowel de app- als de license-hostnamen.

1. Vraag het nieuwe LB-IP op: "tofu output traefik_load_balancer_ip".
2. Log in op het TransIP-controlepaneel.
3. Ga naar Domeinbeheer > filecap.tech.
4. Werk de A-records voor de applicatie- en license-hostnamen bij naar het nieuwe LB-IP.
5. Sla de wijzigingen op.
6. Controleer DNS-propagatie met dig, nslookup of online tooling; controleer daarna dat cert-manager de certificaten opnieuw uitgeeft (zie 5.5).

6. OpenTofu (IaC) Herstelstrategie

- De infrastructuur wordt beheerd met OpenTofu (CI: via de GitLab OpenTofu-component); de code staat in GitLab (FileCap/filecap-terraform-scaleway).
- De state staat in de GitLab HTTP-backend (Terraform state per omgeving), niet in pipeline-artifacts: branchnaam = omgevingsnaam = statenaam = tfvars-bestand (bijv. branch production met vars/production.tfvars).
- Herstel van infrastructuur: de pipeline van de betreffende branch draaien (validate en plan automatisch, apply handmatig), of lokaal "tofu init / plan / apply" met de juiste tfvars en Scaleway-credentials.
- De GitLab-server (inclusief repository en state) valt onder de eigen back-up van de Contec GitLab-omgeving; bij verlies van de state kan de omgeving met "tofu import" worden gereconcilieerd of opnieuw worden uitgerold.

- Cockpit-push-URL's en -tokens en overige gevoelige variabelen staan niet in de repository, maar in GitLab CI/CD-variabelen (en lokaal in .envrc-bestanden); deze moeten bij DR beschikbaar zijn vanuit de wachtwoordkluis.

7. Testfrequentie & Validatie

- Disaster-recoverytests worden minimaal één keer per jaar uitgevoerd.
- Tests omvatten: volledig herstel van de RDB-database en de Object Storage buckets vanuit de Contec-back-up, heruitrol van de infrastructuur met OpenTofu en deployment van de Kubernetes-workloads.
- De promote-flow van de DR-databasereplica wordt vooraf getest op de LWI-omgeving (conform docs/db-dr-promote.md) voordat er in productie op wordt vertrouwd; bevindingen (IP-gedrag, duur, reconcile-commando's) worden in de runbook vastgelegd.
- Elke test wordt geëvalueerd op duur, volledigheid en verbeterpunten; resultaten worden vastgelegd voor de ISO 27001-audit.

8. Rollen & Verantwoordelijkheden

Rol	Verantwoordelijkheid
DR-coördinator	Initiëren en coördineren van DR-procedures
Infra Engineer	OpenTofu-herstel uitvoeren (Scaleway-infrastructuur), databasepromotie/-restore
DevOps	Kubernetes-workloads herstellen via GitLab CI/CD
Security Officer	Controleren op naleving ISO 27001, auditlogs

9. Communicatieprotocol

- Een incident wordt binnen 30 minuten geëscaleerd naar het SIRT-team.
- Klantcommunicatie volgt binnen 2 uur via de statuspagina of e-mail.
- Regelmatige updates totdat volledig herstel bevestigd is.

10. Log & Audit

- Alle herstelacties worden gelogd en bewaard.
- Metrics en logs van de omgeving gaan naar Scaleway Cockpit (kube-prometheus-stack via remote_write naar Cockpit/Mimir; Promtail verzendt logs van de namespaces filecap, filecap-trial en filecap-license naar Cockpit/Loki).
- Wijzigingen aan de infrastructuur zijn herleidbaar via GitLab (merge requests, pipeline-logs, state-versies).
- Secretwijzigingen zijn herleidbaar via versies in Scaleway Secret Manager.
- Herstelprocessen worden geëvalueerd op effectiviteit en waar nodig verbeterd.