Back-up- en herstelbeleid

Sjabloon

* Inhoud

[Autoriteit en herziening 3](#_Toc157682628)

[Documentcontrole en beoordeling 3](#_Toc157682629)

[Versiebeheer 3](#_Toc157682630)

[Intro 4](#_Toc157682631)

[Verantwoordelijkheden 4](#_Toc157682632)

[Back-up- en herstelprocedure 4](#_Toc157682633)

[RPO en RTO 5](#_Toc157682634)

[Toegang tot back-up en versleuteling 5](#_Toc157682635)

[Offsite back-up 5](#_Toc157682636)

[Back-up bewaking 5](#_Toc157682637)

[Herstel test 6](#_Toc157682638)

[ANNEXES 7](#_Toc157682639)

[Intro 7](#_Toc157682640)

[ANNEX 1: GFS Backupschema 8](#_Toc157682641)

[Wat is Grandfather-Father-Son back-up? 8](#_Toc157682642)

[Het principe van GFS-back-up rotatie 8](#_Toc157682643)

[Voorbeeld van een G-F-S schema 8](#_Toc157682644)

[Schematische voorstelling G-F-S 8](#_Toc157682645)

[Soorten back-up technieken voor gegevens 9](#_Toc157682646)

[Volledige back-up van gegevens 9](#_Toc157682647)

[Incrementele gegevensback-up 9](#_Toc157682648)

[Differentiële gegevensback-up 9](#_Toc157682649)

[Gemengde back-up van gegevens 9](#_Toc157682650)

[ANNEX 2: 3-2-1 back-upstrategie 10](#_Toc157682651)

[3-2-1 back-up regel 10](#_Toc157682652)

[Het belang van de 3-2-1 regel 10](#_Toc157682653)

[3-2-1 back-upbeheer 11](#_Toc157682654)

[3-2-1 SAMENVATTING 11](#_Toc157682655)

# Autoriteit en herziening

## Documentcontrole en beoordeling

|  |  |
| --- | --- |
| **Documentcontrole** |  |
| Auteur |  |
| Eigenaar |  |
| Datum aangemaakt |  |
| Laatst herzien door |  |
| Laatste herzieningsdatum |  |

.

## Versiebeheer

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum van goedkeuring** | **Goedgekeurd door** | **Beschrijving van verandering** |
| 1.0 |  |  |  |

# Intro

Kritieke informatie en informatiesystemen moeten worden beschermd tegen gegevensverlies en gegevensbeschadiging. Back-up- en herstelprocedures stellen ons in staat om informatie te herstellen in het geval van rampscenario's zoals systeemuitval, brand, onbedoelde verwijdering of malware uitbraak.

Back-up is niet nodig wanneer verlies van gegevens acceptabel is of wanneer andere controlemaatregelen worden gebruikt om rampsituaties te overwinnen. Een veelvoorkomend voorbeeld is een PLC-systeem dat een statische configuratie bevat die eenvoudig opnieuw kan worden ingezet of vervangen in geval van een ramp.

Dit beleidsdocument maakt deel uit van een set van beleidsdocumenten die **[Organisatie]** ondersteunen bij het opstellen van een gedegen strategie rond cyberbeveiliging.

# Verantwoordelijkheden

De eigenaar is verantwoordelijk voor een efficiënt back-up- en herstelproces dat voldoet aan de bedrijfsbehoeften. Operationele taken kunnen worden gedelegeerd aan systeembeheerders of leveranciers.

# Back-up- en herstelprocedure

Er moet een back-up- en herstelprocedure zijn voor alle kritieke systemen. In de back-upprocedure moeten de volgende onderwerpen zijn vastgelegd:

• Welke informatie back-uppen (systemen EN data)?

• Een back-up maken

• Back-up bewaken

• Wanneer en hoe vaak een back-up maken?

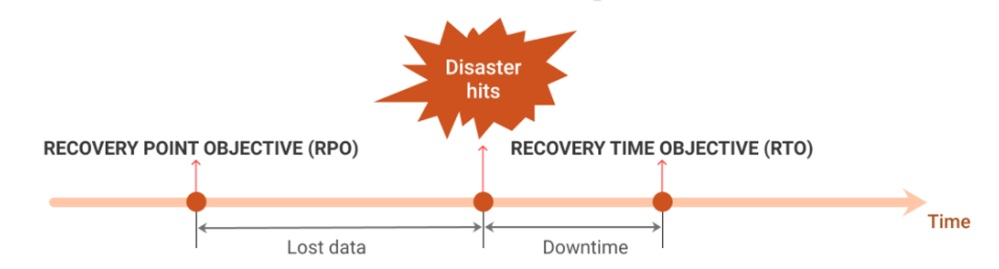
• Hoe lang de back-up bewaren?

• Hoe en waar de back-up opslaan?

• Hoe back-upgegevens worden overgedragen?

## RPO en RTO

De back-upprocedure moet voldoen aan de bedrijfsbehoeften voor RPO (recovery point objective) en RTO (recovery time objective), bijvoorbeeld op basis van risicobeoordeling en informatieclassificatie.



De RPO definieert de maximale periode waarin gegevens verloren kunnen gaan door een belangrijk incident. Als er bijvoorbeeld elke nacht om 2 uur een statische kopie wordt gemaakt, is het maximale gegevensverlies 24 uur.

RTO (recovery time objective) is de tijdsduur die nodig is om de gegevens te herstellen.

Maak hiervoor bijvoorbeeld gebruik van het GFS-schema. (**Zie ANNEX 1: GFS Backupschema.)**

## Toegang tot back-up en versleuteling

Toegang tot back-ups moet minstens hetzelfde beschermingsniveau hebben als de originele gegevens. Wanneer vertrouwelijke back-upgegevens fysiek of logisch worden opgeslagen of getransporteerd op een manier waarop de gegevens beschikbaar zouden kunnen zijn voor onbevoegden, moeten de gegevens worden versleuteld.

Voorbeelden zijn:

* Netwerkverkeer voor back-up.
* Backupmedia die zijn opgeslagen of overgedragen door personen die geen toegang mogen hebben tot de originele gegevens.
* Back-upbestanden op media die zijn opgeslagen op een locatie die toegankelijk kan zijn voor personen die geen toegang mogen hebben tot de originele gegevens.
* De back-up encryptiesleutel die nodig is om de off-site media te ontsleutelen moet niet alleen op locatie worden opgeslagen.

## Offsite back-up

Om verlies van zowel de informatie als de back-up te voorkomen, moeten back-upgegevens waar mogelijk op een andere fysieke locatie worden opgeslagen dan de gegevens zelf. Er moet een overzicht van off-site media beschikbaar zijn. Maak hiervoor bijvoorbeeld gebruik van de 3-2-1 back-upstrategie. (**Zie ANNEX 2: 3-2-1 back-upstrategie**)

## Back-up bewaking

Het back-upproces moet gemonitord worden om een goede werking te garanderen en om fouten aan te pakken. De goede werking moet kunnen worden aangetoond door logboeken, rapporten of een geautomatiseerd systeem.

## Herstel test

Voor alle back-upmethoden die voor kritieke systemen worden gebruikt, moeten minstens één keer per jaar hersteltests worden uitgevoerd. Een operationele restore (ongepland) buiten een geplande periodieke test restore kan worden gerekend als een recovery test.

# ANNEXES

## Intro

Beide schema’s in volgende annexen kunnen afzonderlijk ingezet worden.

Het **Grandfather-Father-Son** (GFS) back-upschema wordt gebruikt in omgevingen met relatief veel data of systemen, wanneer men niet voldoende tijd heeft om tussen een bepaalde tijd de back-ups uit te voeren en/of wanneer het belangrijk is om ver en in detail te kunnen terug gaan in de tijd. in dit schema wordt er geen rekening gehouden met het back-up media of locatie van de back-ups.

Het **3-2-1** schema wordt vaak genomen als basis. Dit betekent dat je minimaal drie volledige kopieën hebt op twee verschillende media. Belangrijk hierbij is dat één van de verschillende media zich op een andere locatie begeeft. In de 3-2-1 regel wordt echter niet gesproken over de RPO-RPO van de back-up.

Zoals eerder werd uitgelegd kunnen beide schema’s afzonderlijk van elkaar worden ingezet. Het is echter een meerwaarde om beide met mekaar te combineren. Het GFS schema legt de focus op de RPO-RTO van de data, waar de 3-2-1 strategie zich toelegt op het opslaan van de gemaakte back-ups.

Volgend voorbeeld geeft verduidelijking bij het gebruik van beide principes:

Alle data staan op een NAS (Network Attached Storage) met de disks in RAID 10\*. Via een back-upserver wordt er elke nacht een back-up van deze NAS op een aparte NAS. Deze NAS is via een afzonderlijke netwerk aan de back-upserver gekoppeld. Een Volledige back-up van de data duurt momenteel langer dan 12 uur. Om toch de veranderlijke data te kunnen back-uppen wordt er voor het GFS schema gekozen. De week en maand back-ups worden extra door gekopieerd naar een beveiligde cloud-omgeving. Op deze manier hebben we de 3-2-1 strategie gecombineerd met het GFS back-upschema. [\*https://en.wikipedia.org/wiki/Nested\_RAID\_levels](*https:/en.wikipedia.org/wiki/Nested_RAID_levels)

Volgende afbeelding geeft een schematische weergave van bovenstaande



## ANNEX 1: GFS Backupschema

### Wat is Grandfather-Father-Son back-up?

De GFS-back-uprotatietechniek is een populaire methode voor **gegevens**back-up, waarmee volledige en gedeeltelijke kopieën naar verschillende media kunnen worden gecombineerd om zowel de back-uptijd te verkorten als de opslagbeveiliging te verbeteren. Er zijn veel artikelen te vinden over wat de grootvader-vader-zoon back-upstrategie inhoudt.

### Het principe van GFS-back-up rotatie

In de grootvader-vader-zoon back-uptechniek maken de drie geplande stappen back-ups:

* De **"grootvader (G)"** - volledige back-up naar een bepaalde plaats, één off site of meerdere sites ;
* De **"vader (F)"** - nog een volledige back-up, regelmatiger, naar een snellere opslag;
* De **"zoon (S)"** - incrementele back-up (of differentiële back-up) naar dezelfde opslag als "vader"

### Voorbeeld van een G-F-S schema

Het GFS-schema begint met de **dagelijkse back-ups**. Meestal zijn er vier back-upmedia gelabeld voor de dag van de week waarop ze back-ups maken, bijvoorbeeld maandag tot en met donderdag. Elke tape wordt opgeroepen voor gebruik op de gelabelde dag. Als er slechts een versiegeschiedenis van bestanden van één week wordt bijgehouden, dan wordt elke tape elke week overschreven. Om een versiegeschiedenis van bestanden van 3 weken bij te houden (aanbevolen), zijn meer tapes nodig. De maandag tape van deze week wordt bijvoorbeeld pas over 3 weken overschreven.

**Wekelijkse back-ups** volgen een vergelijkbaar scenario. Een set van maximaal vijf wekelijkse back-upmedia wordt gelabeld met "Week1", "Week 2", enzovoort. Volledige back-ups worden wekelijks opgenomen op de dag dat een "Son"-medium niet wordt gebruikt. Volgens het bovenstaande voorbeeld zouden dit "Vrijdag"-tapes zijn. Dit "Vader"-medium wordt maandelijks hergebruikt. Er zijn vijf wekelijkse tapes nodig om een bestandsgeschiedenis van één maand bij te houden, aangezien sommige maanden 5 weken hebben

De laatste set van drie media wordt gelabeld met "**Maand1**", "Maand2", enzovoort, afhankelijk van welke maand van het kwartaal ze zullen worden gebruikt. Dit "Grandfather"-medium registreert volledige back-ups op de laatste werkdag van elke maand. Als je back-upplan een fiscale bedrijfskalender volgt, dan neemt je maandelijkse tape de plaats in van de week 4 of week 5 wekelijkse/Father tape, afhankelijk van de maand. Als je back-upschema kalendermaanden volgt, dan zal je maandelijkse back-up gedurende het jaar variëren en een dagelijkse of wekelijkse tape vervangen. Gewoonlijk worden maandelijkse tapes elk kwartaal of elk jaar (aanbevolen) overschreven, afhankelijk van de vereisten voor versiegeschiedenis.

### Schematische voorstelling G-F-S

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Maandag** | **Dinsdag** | **Woensdag** | **Donderdag** | **Week 1** |
| **Maandag** | **Dinsdag** | **Woensdag** | **Donderdag** | **Week 2** |
| **Maandag** | **Dinsdag** | **Woensdag** | **Donderdag** | **Week 3** |
| **Maandag** | **Dinsdag** | **Woensdag** | **Donderdag** | **Maand1** |

### Soorten back-up technieken voor gegevens

Elke back-upsoftware voor bestanden biedt ten minste één methode voor het opslaan van gegevens, de volledige back-up, voor het kopiëren van een volledige dataset naar een laatste bit. Er bestaan echter ook andere back-up types voor gegevens, vaak om tijd en ruimte te besparen voor regelmatige back-ups. Deze back-up types zijn:

* **Volledige back-up** - volledig kopiëren van gegevens zoals eerder beschreven;
* **Gedeeltelijke back-up** - alleen gegevens kopiëren die na de laatste back-up zijn gewijzigd:
  + **Incrementele back-up** - alleen gegevens kopiëren die zijn gewijzigd na de laatste incrementele back-up
  + **Differentiële back-up** - alleen gegevens kopiëren die zijn gewijzigd na de laatste volledige back-up
* **Gemengde back-up** - een opeenvolging van volledige back-ups en een aantal gedeeltelijke back-ups, die herhaaldelijk worden geroteerd:
  + Gemengde incrementele back-up - een keten van volledige en enkele incrementele back-ups;
  + Gemengde differentiële back-up - een reeks volledige en enkele differentiële back-ups.

De volledige back-up is een basis voor elke differentiële back-up of incrementele back-up, maar ook voor gemengde back-ups.

### Volledige back-up van gegevens

Bij een volledige back-up wordt ervan uitgegaan dat elke keer dat je de taak uitvoert, de volledige gegevensset wordt gekopieerd naar de gekozen plaats. Een volledige back-up neemt veel ruimte, tijd en pc-bronnen in beslag en maakt vaak veel overbodige gegevenskopieën, omdat de meeste gegevens in de dataset geen wijzigingen ondergaan tussen back-ups.

### Incrementele gegevensback-up

Incrementele back-up verwerkt alleen bestanden die zijn verschenen of gewijzigd sinds de vorige incrementele back-up. Na een eerste volledige back-up zal elke volgende back-up incrementeel zijn, waarbij alleen een verschil tussen de huidige dataset en een vorige incrementele kopie wordt opgeslagen.

### Differentiële gegevensback-up

Differentiële back-up lijkt veel op incrementele back-up, maar maakt gebruik van verschillende soorten gegevensback-upstrategieën. Na een eerste volledige back-up zal elke volgende back-up incrementeel zijn, waarbij alleen een verschil tussen de huidige dataset en een vorige incrementele kopie wordt opgeslagen.

### Gemengde back-up van gegevens

Deze aanpak is een combinatie van de twee verschillende soorten back-ups: volledige en gedeeltelijke back-ups (incrementeel of differentieel). Het lijkt ook op een back-uptechniek met versiebeheer. Bij deze methode vindt een volledige back-up plaats, gevolgd door een vaste hoeveelheid gedeeltelijke back-ups.

## ANNEX 2: 3-2-1 back-upstrategie

De **3-2-1 back-up** is een beproefde methode voor gegevensbescherming en -herstel om ervoor te zorgen dat gegevens adequaat worden beschermd en dat up-to-date reserve backups van de gegevens beschikbaar zijn wanneer ze nodig zijn. Het basisconcept van de 3-2-1 back-upstrategie is dat er drie backups worden gemaakt van de gegevens die moeten worden beschermd, dat de backups worden opgeslagen op twee verschillende soorten opslagmedia en dat één backup van de gegevens naar een andere locatie wordt gestuurd.

In het klassieke 3-2-1 back-upscenario wordt back-upsoftware gebruikt om een backup te maken van de bedrijfskritische gegevens, waarbij de backup van de gegevens wordt opgeslagen op een ander apparaat voor gegevensopslag op locatie. Tijdens dat proces, of onmiddellijk daarna, worden nog twee backups van de gegevens opgeslagen op twee andere apparaten; traditioneel was ten minste één van die apparaten een tapelibrary. Tape was een standaardonderdeel van het proces omdat het eenvoudig was om een draagbare backup van de gegevens te maken in de vorm van een tapecartridge die eenvoudig van de locatie kon worden verzonden. In veel omgevingen is tape echter vervangen door een opslagsysteem met harde schijf.

Hoewel de 3-2-1 back-upaanpak al tientallen jaren een hoeksteen is van gegevensbescherming in grote en kleine datacenters, is het een concept dat nog steeds wordt omarmd door de meeste leveranciers van back-upsoftware en -hardware als “best practice” voor het effectieve gebruik van hun producten. De leveranciers erkennen dat het algemene concept nog steeds geldig is, ongeacht hoe of waar een bedrijf zijn gegevens opslaat -- zelfs nu nieuwe vereisten en omvangrijke gegevens de 3-2-1 vergelijking iets ingewikkelder hebben gemaakt.

### 3-2-1 back-up regel

De 3-2-1 back-upstrategie bestaat uit drie regels:

* **Drie gegevenskopieën**. Van alle kritieke gegevens moeten regelmatig drie kopieën van backups worden gemaakt -- dagelijks of vaker -- inclusief de originele gegevens en ten minste twee back-ups.
* **Twee soorten opslag.** Er moeten twee verschillende opslagtypes worden gebruikt om de gegevens op te slaan. Beide kopieën van de back-upgegevens moeten op twee verschillende opslagtypes worden bewaard om de kans op storingen te minimaliseren. Soorten opslagapparaten kunnen zijn: een interne harde schijf, externe harde schijf, verwijderbare opslagschijf, een tapelibrary, een secundaire opslagarray of een cloudback-upomgeving.
* **Eén off-site locatie**. Eén kopie van de backupgegevens moet worden verzonden naar een off-site opslagfaciliteit. Ten minste één gegevenskopie moet worden opgeslagen op een externe locatie om ervoor te zorgen dat natuurrampen of geografische rampen niet alle gegevenskopieën kunnen treffen. Deze kopie kan fysiek worden afgeleverd op de off-site locatie, zoals bij back-ups op tape, of kan worden gerepliceerd naar de secundaire locatie via telecommunicatiefaciliteiten.

### Het belang van de 3-2-1 regel

De 3-2-1 back-upstrategie wordt erkend als een “best practice” voor professionals op het gebied van informatiebeveiliging en gegevensbescherming. Hoewel het proces niet garandeert dat alle gegevens nooit op een of andere manier gecompromitteerd zullen worden, elimineert de strategie een aantal risico's die gepaard gaan met back-upprocedures. De 3-2-1 methodologie is belangrijk om ervoor te zorgen dat er geen single point of failure is voor gegevens. Een organisatie is niet alleen gedekt als een kopie beschadigd raakt of als een technologie faalt, maar ook als er een natuurramp of diefstal plaatsvindt waardoor de fysieke opslagtypes worden vernietigd.

Het gegevensherstelproces volgens de 3-2-1 methode zou er als volgt uitzien:

* Originele (actieve) gegevens zijn corrupt, beschadigd of verloren gegaan. Als de productiekopie van gegevens niet beschikbaar is, is het eerste alternatief om de benodigde gegevens te herstellen van de reservekopie die intern is opgeslagen op een ander medium of secundair opslagsysteem.
* Tweede gegevenskopie is niet beschikbaar of onbruikbaar. Als het systeem - tape of schijf - dat wordt gebruikt om de tweede gegevenskopie op te slaan niet beschikbaar is of als de gegevenskopie beschadigd, verouderd of op een andere manier onbruikbaar is, moet de off-site kopie worden teruggehaald naar de interne servers.
* Start het 3-2-1 proces zo snel mogelijk opnieuw. Zodra een geschikte gegevenskopie is aangekoppeld en de werking is hersteld, moet het back-upproces zo snel mogelijk opnieuw beginnen om ervoor te zorgen dat de gegevens voldoende beschermd blijven.

Tegenwoordig zijn back-ups niet alleen maar verzekeringspolissen die worden weggestopt tot er iets misgaat. Bedrijven halen meer waarde uit hun back-up datastores door die gegevens te gebruiken voor zaken als het ontwikkelen en testen van nieuwe applicaties. Hedendaagse benaderingen van programmeren, zoals DevOps, vereisen eenvoudige toegang tot gegevens die zo dicht mogelijk bij live applicatiegegevens liggen om ervoor te zorgen dat applicaties op de juiste manier worden ontwikkeld in een echte omgeving. Back-upgegevens voldoen hier prima aan, omdat ze waarschijnlijk regelmatig en frequent vers worden gegenereerd.

Analytische toepassingen kunnen ook toegang nodig hebben tot grote hoeveelheden actuele gegevens. Door verse back-upgegevens te gebruiken, zijn de resultaten van het analytische proces waarschijnlijk betrouwbaarder en nauwkeuriger. Strengere controles en beheer van gegevensbedrijven zijn nodig om ervoor te zorgen dat deze toepassingen de best mogelijke gegevens krijgen, terwijl de primaire concepten van 3-2-1 back-up behouden blijven. Merk op dat als een van de back-upkopieën wordt gebruikt voor applicatieontwikkeling of voor analyse, deze kan worden gewijzigd of niet beschikbaar is, waardoor een van de vereiste drie kopieën onbruikbaar wordt als herstel nodig is.

Gegevensintegriteit is altijd al een belangrijk aandachtspunt geweest bij gegevensbeschermingsactiviteiten. Het is niet genoeg om alleen maar een back-up te maken van gegevens en de kopieën weg te sluizen; het is noodzakelijk om ervoor te zorgen dat back-ups compleet, onbeschadigd en herstelbaar zijn. Hersteltesten helpen hierbij, net als het gebruik van enkele van de meer geavanceerde functies die back-up apps bieden om ransomware en andere bedreigingen te detecteren. Nogmaals, deze zorgen hoeven een 3-2-1 back-upaanpak niet noodzakelijkerwijs in de weg te staan, maar ze kunnen wel een aantal stappen aan het proces toevoegen, zoals regelmatig geplande hersteltests.

### 3-2-1 back-upbeheer

Er zijn een aantal basisprincipes voor een succesvolle 3-2-1 back-up implementatie:

* Alle gegevenskopieën zijn identiek en up-to-date.
* De media waarop de kopieën zijn opgeslagen, zijn leesbare media.
* Alle exemplaren en apparatuur worden getest en er wordt bevestigd dat ze werken.
* Kopieën op afstand worden veilig opgeslagen.
* Herstel van enkele/meerdere bestanden of een volledige back-up wordt regelmatig getest.
* Interne gegevenskopieën staan op verschillende opslagsystemen en netwerken en zijn niet toegankelijk van buiten het bedrijf.

De back-upsoftware die wordt gebruikt in het 3-2-1 proces kan erg nuttig zijn omdat het automatisch de dispositie van back-ups kan sturen terwijl het alle back-upactiviteiten catalogiseert. De meeste back-up-apps hebben ook functies toegevoegd om te controleren op bedreigingen, zoals malware, ransomware en virussen in back-up kopieën.

### 3-2-1 SAMENVATTING

**Sla 1 van deze offsite op   
(**beveiligdeopslag, cloud,...)

2 verschillende media

Bewaar gegevens op minstens **2 soorten opslag**.  
 (lokale schijf, NAS, Tape,..)

Maak **3 kopieën** van back-up gegevens.   
(1 primaire en 2 back-ups

1 kopie off-site

3 kopieën van gegevens