ram infotechnology

# Disaster Recovery Guide

## DR in gevirtualiseerde omgevingen

Powered by Zerto

# Disaster Recovery Guide
## DR in gevirtualiseerde omgevingen

INHOUD


VOORWOORD Disaster Recovery in een gevirtualiseerde wereld ..... 3

HOOFDSTUK 1 Disaster Recovery: behoeften en technologieën ..... 4

- De oorzaken en kosten van dataverlies ..... 4
- Disaster Recovery: het concept ..... 5
- Disaster Recovery als organisatiestrategie ..... 7
- DR-technologieën in gevirtualiseerde omgevingen ..... 8
- Disaster Recovery en de Cloud ..... 12
- Checklist: Disaster Recovery vereisten ..... 13

HOOFDSTUK 2 De Zerto-revolutie ..... 14

HOOFDSTUK 3 Zerto Virtual Replication ..... 16

- Architectuur ..... 16
- Volledige automatisering en orkestratie ..... 18

HOOFDSTUK 4 Zerto Virtual Replication: toepassingsvoorbeelden ..... 22

SAMENVATTING ..... 23

Over RAM-IT ..... 24

Over Zerto ..... 24

VOORWOORD

# Disaster Recovery in een gevirtualiseerde wereld

In moderne, informatiegedreven organisaties is de bedrijfscontinuïteit volledig afhankelijk van IT-infrastructuren, die 24/7 in de lucht moeten zijn. De kosten van downtime zijn astronomisch en dataverlies kan een bedrijf ruïneren. Dit dataverlies kan worden veroorzaakt door natuurrampen, stroomuitval, hardware-storingen en gebruikersfouten, maar ook – en steeds vaker – door software- en cybersecurity-issues. Doordat datacenters, private, hybrid en public clouds vaker software-defined zijn, worden ze kwetsbaarder voor deze typen bedreigingen. Om downtime en dataverlies te minimaliseren worden beveiligings- en continuïteitsstrategieën dan ook steeds belangrijker voor de moderne bedrijfsvoering.

In een software-defined, gevirtualiseerde omgeving draaien applicaties op virtuele machines, onafhankelijk van de hardware. Hoewel dit veel efficiency-voordelen biedt voor de business, gelden deze niet voor disaster recovery (DR) en business continuity (BC). Veel BC/DR-oplossingen zijn gebaseerd op fysieke entiteiten, arrays en apparaten, die moeite hebben mee te groeien met de hoeveelheid data die wordt geproduceerd in moderne organisaties. De voordelen van virtualisatie gaan verloren door de management-overhead en de complexiteit van het combineren van een virtualisatie-strategie met disaster recovery-oplossingen die ontworpen zijn voor fysieke omgevingen. Om dit probleem op te lossen zijn virtualisatie-bewuste BC/DR-oplossingen nodig.

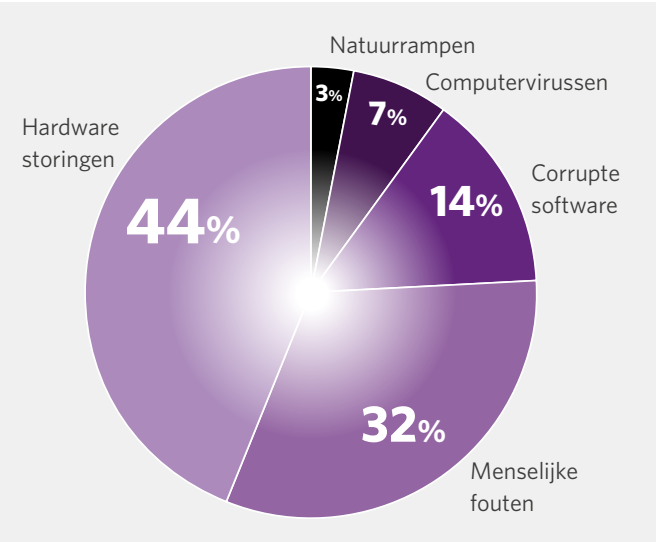
Deze brochure geeft u inzicht in de uitdagingen, behoeften, strategieën en de beschikbare oplossingen voor business continuity en disaster recovery (BC/DR), speciaal voor moderne, gevirtualiseerde omgevingen en de public cloud. Daarnaast wordt uitgelegd welke voordelen Zerto Virtual Replication biedt en hoe deze oplossing zich verhoudt tot andere BC/DR-technologieën. Dit overzicht biedt organisaties de juiste informatie om te komen tot de best mogelijke BC/DR-oplossing voor hun situatie. Heeft u naar aanleiding van deze brochure nog vragen, kijk dan op **www.ram-it.nl/DraaS**.

HOOFDSTUK 1

# Disaster Recovery: behoeften en technologieën

## De oorzaken en kosten van dataverlies

Moderne bedrijven kunnen zich niet veroorloven data te verliezen. Wat de oorzaak ook is – een natuurramp, een menselijke fout of een cyberaanval – dataverlies is kostbaar en risicovol. Onderzoek door uiteenlopende instituten toont aan dat dataverlies én de kosten ervan elk jaar toenemen. Een continuïteitsstrategie die uptime garandeert, data-verlies minimaliseert en productiviteit maximaliseert bij elke compromitterende situatie, vormt een broodnodige digitale verzekering voor ieder bedrijf. Want het is niet langer de vraag *of* u een ramp overkomt, maar *wanneer*.




TOP 5 OORZAKEN VAN DATAVERLIES EN DOWNTIME

*(bron: World Backup Day 2015)*

**...in een gevirtualiseerde wereld**

Veel organisaties hebben meetbare besparingen en efficiëntie behaald door hun productie-omgeving te virtualiseren. Echter, veel van deze voordelen gaan verloren op BC/DR-gebied, omdat BC/DR-technologieën vaak zijn gebaseerd op oudere techniek die niet virtualisatie-bewust is, zoals array-based en agent-based replicatie. Doordat er meerdere technologieën worden gecombineerd binnen een disaster recovery plan, is het lastig dit consistent en herhaalbaar te houden.

**400% GROEI**

Totaal volume aan dataverlies in twee jaar

*(Security Week)*

**$2.1 BILJOEN**

Totale kosten van dataproblemen in 2019

*(IT Web)*

**64% VAN BEDRIJVEN**

Heeft een grote storing gehad de afgelopen 12 maanden

*(EMC)*

**71% VAN IT BESLISSERS**

Zijn niet zeker over hun recovery-vermogen

*(CIO Insight)*

**15 miljoen APPLICATIES**

Draaien op gevirtualiseerde infrastructuren

*(CIO Insight)*

**86% VAN SERVER WORKLOADS**

Zijn gevirtualiseerd in 2016

*(Gartner Group)*

## Disaster Recovery: het concept

Wat is Disaster Recovery (DR) eigenlijk? Letterlijk betekent het: herstel na een ramp, ofwel de tijd en het werk die nodig zijn om systemen weer draaiend te krijgen na dataverlies of downtime. DR draait niet alleen om de tijd dat systemen en medewerkers niet kunnen werken, het gaat ook om de hoeveelheid data die verloren is gegaan als een bedrijf moet terugvallen op een vorige versie van haar data. Organisaties zouden zichzelf moeten afvragen hoeveel een uur downtime kost. En vooral: is het mogelijk om het werk dat medewerkers en systemen de afgelopen uren hebben gedaan te reproduceren? 95% van alle bedrijven kunnen deze vraag niet beantwoorden...

**Back-up is geen echte disaster recovery-oplossing**

Disaster recovery draait om verschillende termen die verwarrend kunnen werken: disaster recovery, business continuity, back-up, RTO en RPO. Het meest bekend is **back-up**, ofwel het consistent, volgens een regelmatige tijdsinterval (bijv. 24 uur), repliceren van data of van VM's naar een ander systeem of andere locatie, met het oog op herstel of voor archivering. Echter, bij incidenten is back-up een leeg concept zonder een oplossing voor **disaster recovery (DR)**, voor het herstellen van bestanden, software en functionaliteit. Dit heeft meestal meer om het lijf dan alleen het terugkopiëren van data naar het oorspronkelijke systeem. Als een server down gaat, moet deze opnieuw worden geïnstalleerd, geconfigureerd en misschien zelfs vervangen. Dat maakt een back-up geen echte DR-oplossing. Met alleen een back-up moeten VM's compleet opnieuw opgebouwd worden, omdat er geen automatisch herstel is ingebouwd in het back-upproces.

## HET ANTWOORD OP RANSOMWARE

De laatste jaren is een trend zichtbaar van hackers die proberen geld af te persen van zowel privé-personen als bedrijven, via ransomware zoals CryptoLocker. Deze kwaadaardige software versleutelt data, bestanden of zelfs complete serversystemen, met behulp van een private-public sleutelpaar. De data kan alleen ontsloten worden met behulp van de private key, waarvoor losgeld moet worden betaald aan de aanvallende partij.

De beste manier om bedrijven te beschermen tegen deze bedreiging is door up-to-date anti-virussoftware te gebruiken en door een solide recovery-strategie, maar ook door gebruikers te informeren over de bedreigingen van phishing mails, waar dit type virussen meestal vandaan komt. Mocht een bedrijf toch het slachtoffer worden van een ransomware-aanval, dat kan Zerto helpen het dataverlies te minimaliseren:

- Draai de systemen terug naar het laatste tijdstip voor infectie, tot binnen enkele seconden.
- Herstel alle kritische systemen binnen enkele minuten met een paar clicks.
- Niet alleen complete applicaties en databases worden consistent hersteld, dit kan ook met individuele bestanden.
- Doe op elk moment een non-disruptive failover test, om er zeker van te zijn dat de business snel weer online kan worden gebracht mocht dat nodig zijn.
- Creëer off-site kopieën van data om te bewaren voor de lange termijn naast de 14-daagse Continuous Data Protection.

## Business Continuity

Veel bedrijven hebben een **disaster recovery-site** (DR-site) waar data continue naartoe wordt gerepliceerd en die klaar staat om in gebruik genomen te worden in geval van uitval. Indien deze DR-site zich op een andere locatie bevindt dan de productie-site, kan deze ook een oplossing bieden voor **business continuity**: het vermogen van een organisatie om operationeel te blijven na een grote ramp, zoals een brand, stroomuitval of een natuurramp. Op het moment dat de oorspronkelijke site down gaat, worden de services van de productie-site overgenomen door de DR-site. Dit schakelproces wordt **failover** genoemd. Zodra de oorspronkelijke productie-site weer online is, moet het werk dat is gedaan op de DR-site weer worden teruggekopieerd om ervoor te zorgen dat er geen werk verloren gaat. Dit **failback**-vermogen is een belangrijk onderdeel van iedere solide DR-oplossing. DR-sites waren voorheen een complete kopie van de productie-omgeving op een andere locatie, maar tegenwoordig bevinden deze zich vaker in het datacenter van een cloud service provider of in de public cloud.

### RTO EN RPO UITGELEGD


Ieder **beursgenoteerd bedrijf** heeft zich te houden aan regels op het gebied van datasecurity; dataverlies resulteert in omzet- en reputatieverlies én in lagere beurskoersen.

Een **online business** die 4 uur data kwijtraakt, kan last krijgen met boze klanten die zich afvragen waar hun bestelde en reeds betaalde spullen blijven.

Als de systemen van een **transportbedrijf** een paar uur stil liggen, wordt het onmogelijk leveringen efficiënt in te plannen, met enorme gevolgen voor de toch al onder druk staande omzet.

Complexe **gerobotiseerde productieprocessen** die stil liggen na een hardware- of softwarecrash, veroorzaken productiviteits- en omzetverlies.

## RTO en RPO

Als bedrijfswensen moeten worden vertaald in Service Level Agreements (SLA's), wordt recovery meestal uitgedrukt in twee typen doelstellingen: RTO en RPO. De **Recovery Time Objective (RTO)** is de maximale tijd dat een bedrijf de service die moet worden hersteld kan missen, zonder significant verlies of risico. De **Recovery Point Objective (RPO)** is het dichtstbijzijnde tijdstip waarvan data kan worden hersteld. Traditionele back-up- en snapshottechnologieën leveren RPO's tussen 15 minuten tot wel 24 uur. In moderne, gedigitaliseerde bedrijfsomgevingen moeten zowel RTO als RPO zo laag mogelijk zijn, niet langer uitgedrukt in uren maar liever in minuten of seconden. Hoewel veel bedrijven zich focussen op RTO teneinde de business zo snel mogelijk weer up-and-running te krijgen, is het vooral het onvermogen om de verloren data te reproduceren waar bedrijven lang na elke crash last van houden.

## Hoge beschikbaarheid

Een concept dat vaak wordt verward met disaster recovery en business continuity is **high availability** (hoge beschikbaarheid). Dit betreft functionaliteit die helpt downtime door hardware-problemen te vermijden, via technologieën als RAID en redundante onderdelen, zoals bekabeling en stroomvoorziening, ook in gevirtualiseerde omgevingen. Hoge beschikbaarheid is noodzakelijk om systemen draaiende te houden, maar helpt niet bij herstel na een ramp. Hoge beschikbaarheid wordt uitgedrukt in een percentage, ergens rond de 99%. Maar zelfs 99,9% uptime betekent nog altijd 8 uur ongeplande downtime per jaar.

### HOGE BESCHIKBAARHEID IN % EN IN TIJD *(bron: Wikipedia)*

| Beschikbaarheid % | Downtime per jaar | Per week |
|---|---|---|
| 90% ("one nine") | 36,5 dagen | 16,8 uren |
| 99% ("two nines") | 3,65 dagen | 1,68 uren |
| 99,9% ("three nines") | 8,76 uren | 10,1 minuten |
| 99,99% ("four nines") | 52,56 minuten | 1,01 minuten |
| 99,999% ("five nines") | 5,26 minuten | 6,05 seconden |

## Disaster Recovery als organisatiestrategie

Dataverlies en downtime hebben directe gevolgen voor de business. Daarom is disaster recovery een zaak waarover beslist zou moeten worden op basis van strategische bedrijfscriteria en -doelstellingen. Hoeveel downtime een organisatie kan overleven en hoeveel dataverlies acceptabel is – de basis van RTO en RPO – is onmogelijk alleen vanuit een technisch niveau te beantwoorden. De antwoorden zijn afhankelijk van omzetstromen uit IT-systemen, de waarde van bedrijfsdata, logistiek en andere bedrijfsprocessen die afhangen van IT. Hoewel het om technologie gaat, wordt een DR-plan vooral gebaseerd op bedrijfsdoelstellingen.

### Wat is écht belangrijk

Bij het ontwikkelen van een DR-strategie is het belangrijk te constateren dat niet alle systemen, applicaties en data even bedrijfskritisch zijn. Voor de meest bedrijfskritische applicaties is een werkende DR-strategie essentieel, met een DR-site op een andere locatie, een lage RTO en RPO (weinig dataverlies en een snel herstel) en een getest recovery-plan. Voor andere applicaties en typen data kunnen goedkopere oplossingen en hogere RPO's en RTO's acceptabel zijn.

Prioriteiten stellen is belangrijk bij DR-planning. Onderzoek samen met de bedrijfsverantwoordelijken hoeveel downtime acceptabel is voor elke applicatie, zodat duidelijk wordt welke applicaties beschikbaar moeten blijven met zo min mogelijk dataverlies en welke een bedrijf best een aantal uren zou kunnen missen. Wat belangrijk is, is overeenstemming met de eindverantwoordelijken over het serviceniveau, zodat er geen verrassingen zijn bij calamiteiten.

### BC/DR is een financiële beslissing

Een DR-oplossing kan worden gebaseerd op uiteenlopende structuren en oplossingen, met uiteenlopende prijskaartjes. De goedkoopste oplossing is een traditionele back-up, maar die biedt onvoldoende zekerheid in moderne omgevingen. Implementeren van een DR-site kan op basis van een stand-by kopie van de productie-omgeving op een andere locatie, maar ook op basis van een cloud-service (DRaaS). Dit is tevens een keuze tussen Capex en Opex, tussen de uitgaven en kosten van het bezitten van een oplossing of de operationele kosten van een online service.

Daarnaast is het aantal tools en technologieën een belangrijke overweging. Een DR-plan dat is gebaseerd op veel verschillende, complexe technologieën zal leiden tot een gecompliceerd recovery-proces, dat onder de druk van een calamiteit kan leiden tot fouten, juist als deze het meeste kwaad kunnen doen.

### DR is governance

Grotere organisaties moeten bij DR ook denken aan compliance en governance. Voldoen aan steeds strengere wet- en regelgeving rond data moet een onderdeel vormen van iedere DR-strategie. Om dit te kunnen realiseren dienen procedures te worden vastgelegd en oplossingen te worden getest op betrouwbaarheid. Bij de keuze voor een cloud-oplossing komt daarbij nog vraag wie controle heeft over die cloud en waar de data in de cloud wordt opgeslagen.

## DR-technologieën in gevirtualiseerde omgevingen

Virtualisatie heeft grote veranderingen teweeggebracht in het datacenter, door meer flexibiliteit en controle te bieden over productie-workloads en door de implementatie en operationele ondersteuning te stroomlijnen. Om de voordelen van deze software-defined omgeving – de private of hybrid cloud – volledig te realiseren, moeten organisaties alle IT-processen rond de virtuele omgeving optimaliseren: security, compliance én business continuity/disaster recovery (BC/DR). Veel organisaties zien BC/DR vooral als een kostbare verzekeringspolis, vooral omdat de beschikbare oplossingen vaak kostbaar zijn en inadequaat voor een gevirtualiseerde omgeving.

### Hardware en software

Veel DR-oplossingen richten zich op het minimaliseren van downtime gebaseerd op hardware-problemen, stroomuitval of natuurrampen. Echter, de meeste calamiteiten betreffen niet een complete uitval van het datacenter. Over het algemeen gaat het vaker om het herstellen van per ongeluk verwijderde bestanden of van een enkele VM. Calamiteiten worden niet altijd veroorzaakt door hardware-problemen en dus ook niet opgelost door een puur op hardware gebaseerde oplossing.

### Wat maakt BC/DR anders in een gevirtualiseerde omgeving?

- **Software-defined** – In een virtuele omgeving is replicatie op hardwareniveau niet adequaat. Replicatie moet plaatsvinden in de hypervisor om applicaties en data beschikbaar te houden bij calamiteiten. Eindgebruikers zijn niet op zoek naar een logische storage-unit, maar naar een applicatie, zoals Oracle of Microsoft Exchange.
- **Virtualisatie-bewust** – De keuze voor een virtualisatiestrategie betekent dat een DR-oplossing ook virtualisatie-bewust moet zijn. Dit zorgt ervoor dat veranderingen in de productie-omgeving terug te vinden zijn in de DR-processen, waardoor dataprotectie consistent blijft en de flexibiliteit en het reactievermogen van virtualisatie in stand gehouden worden.
- **Applicatie-consistent** – Veel bedrijfskritische applicaties gebruiken meerdere VM's die afhankelijk zijn van elkaar. Dat betekent dat deze gezamenlijk moeten worden gerepliceerd om consistent te blijven.
- **Schaalbaar** – Omdat data en applicaties explosief groeien, moet een DR-oplossing gebouwd zijn voor protectie van vele VM's. De DR-oplossing moet kunnen meegroeien zonder complexiteit en overhead toe te voegen.
- **Veranderlijk** – Vanwege hun dynamische aard neigen virtuele omgevingen zich uit te spreiden en zich te vermeerderen, waardoor BC-DR bemoeilijkt wordt.
- **Granulair** – Om tegemoet te komen aan de belangrijkste oorzaken van downtime, zoals datacorruptie en gebruikersfouten, moet een oplossing granulair genoeg zijn om losse bestanden of VM's te herstellen.
- **Hoogfrequent** – Nu IT-omgevingen – niet alleen de gevirtualiseerde – cruciaal zijn voor het voortbestaan van ondernemingen, moet het repliceren van VM's, data en bestanden veel vaker geschieden dan een ouderwetse, dagelijkse back-up.

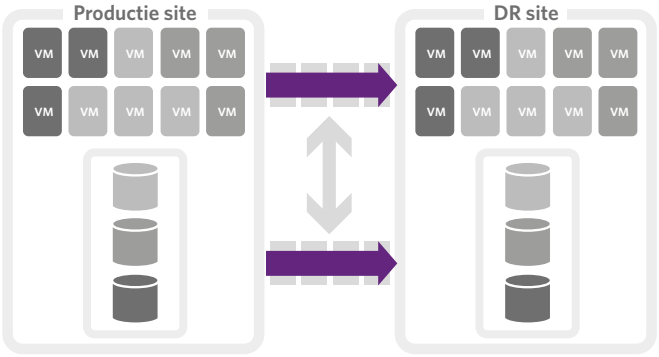
## Beschikbare DR-oplossingen

In de loop der jaren zijn diverse disk-to-disk-oplossingen voor disaster recovery op de markt gekomen, geen van alle volledig virtualisatie-bewust. Een kort overzicht van de oplossingen, hun werking en hun tekortkomingen in een gevirtualiseerde omgeving.

## Array-based replicatie

Array-based replicatie-oplossingen worden geleverd door storageleveranciers en werken als modules binnen een storage array. Het zijn oplossingen die alleen werken met de specifieke oplossing die al in gebruik is. De relatie tussen VM's en storage staat vast en de totale LUN wordt gerepliceerd, of hiervan nu 40% of 90% wordt gebruikt.

- **Hardware-gebaseerd** – Array-based replicatie is ontworpen om fysieke entiteiten te repliceren. Het 'ziet' geen VM's, laat staan configuratieveranderingen.
- **Niet onafhankelijk** – Hoewel geoptimaliseerd voor een bepaalde storage array, beperkt het een organisatie tot één leverancier.
- **Meer beheerpunten** – Naast de managementconsole voor de fysieke storage, moeten de gevirtualiseerde systemen los worden beheerd vanuit een virtualisatie managementconsole.
- **Groei en verandering** – De relatie tussen de VM en de storage staat vast, wat de flexibiliteit en het reactievermogen van virtualisatie elimineert.
- **Granulair** – Omdat de hele LUN wordt gerepliceerd, is array-based replicatie niet granulair genoeg voor virtuele omgevingen.
- **Kosten** – De totale LUN wordt gerepliceerd, of hiervan nu 40% of 90% wordt gebruikt, met meer power, cooling en storagekosten als gevolg.
- **Single point for recovery** – Veel array-based oplossingen leggen de historische performance van een LUN niet vast. Is het laatste datatijdstip corrupt, moet dit toch voor herstel worden gebruikt, wat de complete DR-oplossing nutteloos maakt.
- **Tijd** – Recovery is zeer tijdrovend en gecompliceerd omdat er geen automatische processen zijn en VM's compleet opnieuw moeten worden opgebouwd.

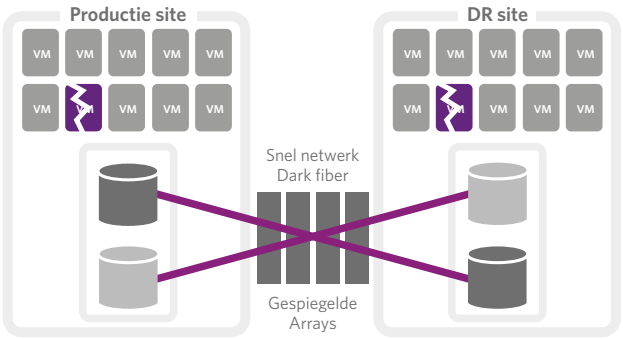



***Figuur 1.*** *Array-based en appliance-based replicatie vereisen coördinatie tussen twee replicatie-producten: voor de fysieke en voor de gevirtualiseerde omgeving. Dit verhoogt de complexiteit en ondermijnt de investeringen in virtualisatie.*

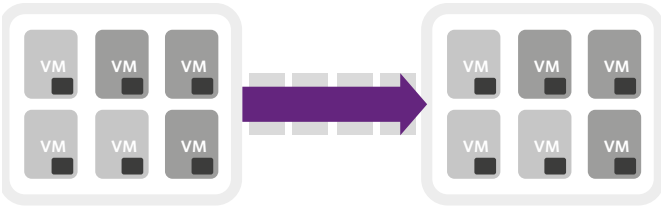
## Appliance-based replicatie

Ook appliance-based replicatie-oplossingen zijn gebaseerd op hardware en specifiek voor één bepaald platform. Het belangrijkste verschil is dat replicatie geschiedt op een extern apparaat en niet binnen de storage array zelf. Als gevolg hiervan zijn deze oplossingen flexibeler en leggen ze minder druk op array resources. Maar de nadelen zijn min of meer hetzelfde als voor array-based replicatie.

- **Hardware-gebaseerd** – Ook dit is ontworpen om fysieke entiteiten te repliceren in plaats van virtuele.
- **Niet onafhankelijk** – Hoewel het flexibeler is dan array-based replicatie, is het nog steeds beperkt tot een bepaald platform.
- **Meer beheerpunten** – Ook hier is naast een management-console voor de fysieke storage een managementconsole nodig voor virtualisatie.
- **Groei en verandering** – Het 'ziet' geen configuratieveranderingen, waardoor BC/DR niet meer synchroon loopt met de huidige productieomgeving, wat de flexibiliteit en het reactievermogen van virtualisatie elimineert.
- **Granulair** – Appliance-based replicatie richt zich meer op de logische eenheid en niet op de VM. Dit gebrek aan granulariteit conflicteert met de belofte en de eisen van virtualisatie.
- **Kosten** – Omdat de hele LUN wordt gerepliceerd, stijgen de kosten voor power, cooling, storage en networking.




***Figuur 2.*** *Door systemen te spiegelen via een snel netwerk wordt een zeer hoge beschikbaarheid mogelijk, maar corrupte softwarecomponenten worden ook gerepliceerd.*




***Figuur 3.*** *Guest/OS-gebaseerde replicatie vereist de installatie van een agent op iedere VM en dat veroorzaakt complexiteit.*

## Synchrone replicatie

Een andere optie is het installeren van een complete kopie van een infrastructuur op een andere locatie, waar elke 'write' op een schijf naartoe wordt gekopieerd of gestriped. In het geval van een calamiteit wordt een automatische failover geïnitieerd waarbij de DR-site actief wordt. Synchrone replicatie, zoals gevonden in NetApp's MetroCluster, klinkt als een perfecte, hoewel kostbare, oplossing, maar het is volledig gebaseerd op hardware en meer een oplossing voor hoge beschikbaarheid dan voor disaster recovery. Failover werkt in geval van een hardware-probleem, stroomuitval of een natuurramp, maar zodra de oorzaak een corrupte database, een virus of een ander software-probleem is, zijn deze problemen ook al gerepliceerd naar het andere systeem. Dit maakt de replicatie-oplossing nutteloos en dwingt de organisatie terug te vallen op een back-up voor herstel.

- **Lock-in** – Een exacte kopie van de hardware is noodzakelijk, van dezelfde leverancier, op een andere locatie.
- **Kostbaar** – Dit is uiteraard een zeer kostbare oplossing, die letterlijk de hardwarekosten verdubbelt en bovendien een netwerkoplossing met een zeer hoge bandbreedte vereist.
- **Incompleet** – Volledig hardware-gebaseerd; bij software-calamiteiten moet het terugvallen op snapshots.

## Guest/OS-gebaseerde replicatie

Bij een guest/OS-gebaseerde replicatie-oplossing worden softwarecomponenten geïnstalleerd op iedere fysieke en gevirtualiseerde server. Hoewel dit meer flexibiliteit biedt dan hardware-gebaseerde oplossingen, is het niet geschikt voor grote ondernemingen.

- **Groei en verandering** – Omdat er op iedere server en in iedere VM een module moet worden geïnstalleerd, is de schaalbaarheid beperkt. Dat maakt het onmogelijk te implementeren en te beheren in grootschalige omgevingen. Bovendien kan de aanwezigheid van een agent in elke VM leiden tot performance-problemen binnen applicaties.
- **Complexiteit** – Schaduw-VM's vormen vaak een onderdeel van een implementatie en maken het beheer complexer.
- **Geen applicatie-consistentie** – Iedere VM wordt individueel beschermd, wat het onmogelijk maakt om groepen VM's voor een applicatie consistent te beheren en te repliceren.
- **Management overhead** – Alle agents moeten worden beheerd en onderhouden. Dat is geen probleem als het gaat om een paar VM's, maar zodra het er meer dan 20 worden, wordt het beheer complexer. Onderhoud en updates voor de DR-strategie worden dan een weekendklus, waarbij downtime niet uitgesloten is.

## Snapshots

Veel oplossingen gebruiken snapshots om een snel herstel mogelijk te maken. Een snapshot is een manier om een live storagesysteem of VM te 'bevriezen' op een bepaald tijdstip. Veranderingen blijven doorgaan nadat het snapshot is genomen. Indien er tijdens deze veranderingen een probleem optreedt binnen de VM of binnen het storagesysteem, is het mogelijk deze veranderingen teniet te doen door het systeem terug te zetten naar het tijdstip dat het snapshot werd genomen. Snapshots zijn vooral nuttig als er veranderingen worden gemaakt aan een VM waarbij terugzetten mogelijk noodzakelijk wordt.

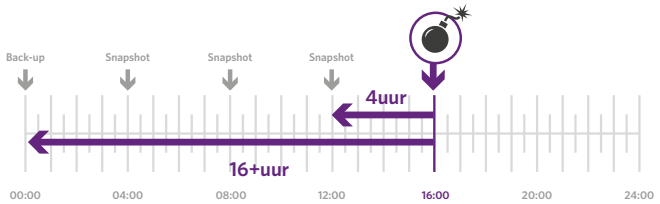
Er zijn twee typen snapshots: **storage snapshots**, gebaseerd op hardware, en **virtual machine snapshots**.

### Storage snapshots: kostbaar

Storage snapshots worden genomen van het totale storagevolume. Ze kunnen exponentieel groeien in omvang en nemen veel storageruimte in de productie-omgeving in beslag. 30% van de netto diskruimte is geen uitzondering. Dit is vooral het geval als er veel veranderingen plaatsvinden in de data nadat het snapshot voor het eerst werd genomen. De meeste storage snapshot-technologieën zijn ook afhankelijk van de originele disks.

### Virtual Machine snapshots: onvolledig

VM snapshots zijn van toepassing op specifieke, individuele VM's en maken geen kopieën van VM's. Dit snapshot zorgt er alleen voor dat een reeds bestaande VM kan worden teruggezet naar een vorige versie (dit geldt overigens ook voor storage snapshots, maar dan voor een compleet storagevolume in plaats van een enkele VM). De VM is niet beschermd in het geval van een hardwareprobleem. Indien de bestanden waarbinnen een VM zich bevindt verloren gaan, zijn ook de bijbehorende snapshots nutteloos.




***Figuur 4.*** *Hoewel snapshots de RPO verkorten worden zij normaal gesproken elke 4 tot 8 uur genomen (anders hebben ze teveel impact op performance en storage). Dit resulteert in een betere RPO dan traditionele back-up, maar nog steeds gaat 4 tot 8 uur werk verloren bij een incident.*

**De vraag luidt: vormen Snapshots een adequate DR-oplossing?**

- **Geen echte DR** – Snapshots worden gebruikt om een tijdstip tijdelijk vast te leggen, niet voor de langere termijn. Om een kopie van een VM vast te leggen is een DR-site of een back-up nodig, niet een snapshot.
- **Performance** – Virtual Machine snapshots hebben een grote impact op de performance van een VM en kunnen ook een grote impact hebben op de totale omgeving met extra overhead op hypervisors en storage.
- **Management** – Grote aantallen snapshots zijn moeilijk te beheren.
- **Frequentie** – Omdat snapshots over het algemeen om de 4 uur worden genomen (meer heeft teveel impact op performance en storage), is er nog steeds 4 uur dataverlies na herstel (zie figuur 4). De claim dat een RPO van 15 minuten haalbaar is, geldt alleen voor zeer kleine omgevingen. In moderne omgevingen is een meer continue replicatie-oplossing nodig, zonder performance-impact op de productie.
- **Snapshots en de cloud** – Hoewel sommige DR-oplossingen snapshots opslaan in de cloud (DRaaS), moeten deze wel eerst worden gemaakt binnen de productie-omgeving voordat ze worden gerepliceerd naar de cloud. De storage- en performance-impact blijft dan gelijk. Het is belangrijk te weten welk type snapshot een DRaaS-oplossing gebruikt: een storage snapshot of een VM-snapshot. Storage snapshots hebben identieke hardware nodig en dat beperkt cloud providers en hardware lifecycles tussen beide betrokken organisaties.

### Hypervisor-gebaseerde replicatie

Alle genoemde replicatie-technologieën hebben kritieke beperkingen in een virtuele context. Hierdoor ondermijnen zij de belofte van virtualisatie en beperken zij haar functionaliteit. Om volledig te kunnen profiteren van de investeringen in virtualisatie zonder compromissen als het gaat om BC/DR, is een nieuwe aanpak nodig: hypervisor-gebaseerde replicatie. Zerto heeft replicatie verplaatst uit de storagelaag, boven de resourceslaag, binnen de virtualisatie/hypervisorlaag. **Hoofdstuk 2** beschrijft hoe Zerto's innovatieve hypervisor-gebaseerde replicatie-oplossing virtuele replicatie en BC/DR-mogelijkheden levert voor grootschalige datacenters en de cloud.

### DR aangeboden door hypervisors

Hypervisor-leveranciers, zoals VMware, bieden ook eigen software-based replicatie-oplossingen, beperkt tot hun eigen hypervisor. Een oplossing als VMware vSphere Replication (VR) biedt beperkte replicatie-functionaliteit, maar niet de orkestratie-, test-, rapportage- en andere DR-functies die nodig zijn voor grootschalige IT-omgevingen. Zelfs in combinatie met VMware Site Recovery manager (SRM) komt de schaalbaarheid en hersteltijd niet tegemoet aan de eisen van moderne bedrijfsvoering. Hoewel SRM functionaliteit toevoegt op het gebied van planning, testen en de uitvoering van disaster recovery, blijft het beperkt door de mogelijkheden die vSphere Replication biedt op basis van VM snapshot-technologie.

## Disaster Recovery en de Cloud

Nu de cloud meer en meer een optie wordt, kijken meer ondernemingen naar een public, private of hybrid cloud als onderdeel van hun BC/DR-oplossing. Virtualisatie heeft de mogelijkheid geschapen, maar er kan nog steeds een hiaat in de beschikbare technologie zitten, afhankelijk van de gekozen oplossing. Bedrijfskritische applicaties kunnen effectief worden gevirtualiseerd en beheerd, maar niet effectief worden beschermd in een cloud-omgeving als daarvoor de verkeerde tools worden gekozen.

### Disaster Recovery as a Service (DRaaS)

De cloud als DR-oplossing is een verstandige keuze, omdat de cloud meer flexibiliteit en normaal gesproken minder kosten met zich meebrengt dan een eigen DR-site. Bij het kiezen van een cloud service provider en een DRaaS-service, is het belangrijk u te realiseren dat DRaaS geen technologie is. Het is een service gebaseerd op één van de technologieën die hier behandeld zijn. Het enige grote verschil is de plaats waar de DR-bestanden worden opslagen. Dit betekent dat een DRaaS-oplossing die is gebaseerd op snapshots, dezelfde beperkingen heeft, inclusief de performance- en storage-impact aan de productiezijde. En bovendien: een RPO van 15 minuten op basis van snapshots blijft onrealistisch.

Bij het zoeken naar een DRaaS-service is het belangrijk nader te onderzoeken op welke technologie de service is gebaseerd, met de zekerheid dat de RTO en RPO die worden geboden realistisch en bewijsbaar zijn zonder extra investeringen vooraf. Om u te helpen met deze keuze hebben we een DR en DRaaS checklist opgesteld die u vindt op de pagina hiernaast.

# CHECKLIST: DISASTER RECOVERY VEREISTEN

**voor zowel in-house- als DRaaS-oplossingen**

## Performance

1. Biedt de DR-oplossing continue replicatie? Wat is de impact op de productie-site op basis van de gebruikte technologie (zoals snapshots)?
2. Welke RTO en RPO biedt de oplossing? Wordt deze gemeten in seconden, minuten of uren? Kan dit worden bewezen en heeft u continu inzicht in beide?
3. Komen de RPO en RTO daadwerkelijk tegemoet aan uw business-eisen, en tegen welke offers en kosten?
4. **DRaaS** – Biedt de Cloud Service Provider een betrouwbare en snelle netwerkoplossing en biedt de DRaaS-oplossing efficiënt netwerkgebruik, bijvoorbeeld door compressie?

## Ondersteuning van uw systemen

5. Is de DR-oplossing storage- en hypervisor-onafhankelijk? Oftewel: kunt u vanuit ieder type omgeving repliceren naar de DR-oplossing?
6. Is de oplossing applicatie-bewust en biedt het applicatie-consistent groeperen van VM's?
7. Hoe schaalbaar is de oplossing (zowel omhoog als omlaag in een DRaaS-omgeving)?
8. Hoe ziet de installatie eruit? Moet u applicaties, LUN's en VM's opnieuw configureren?
9. Ondersteunt de oplossing verandering, indien VM's worden verplaatst naar een andere storagelocatie of indien u een migratie wilt doorvoeren?
10. **DRaaS** – Worden meerdere sites ondersteund en is de oplossing multi-tenant? Biedt de oplossing veilig geïsoleerde datastromen voor bedrijfskritische applicaties en voor compliance?

## Functionaliteit

11. Gaat het om een complete off-site protectie-oplossing met storage voor zowel DR- als archivering (back-up), zonder veel impact op de productie-site?
12. Is de oplossing geschikt voor zowel hardware- als softwareproblemen?
13. Biedt de oplossing afdoende failover en failback functionaliteit, inclusief recovery-automatisering en orkestratie, pre- en post-recovery scripts, automatische IP-aanpassing enz.
14. Wat is de impact op de productie in het geval van een failover of failback? Hoe ziet het failback-proces eruit? Is het gelijk aan het failover-proces?

## Compliance

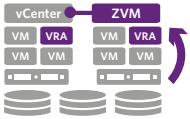
15. Kan de oplossing worden getest en zijn testrapporten beschikbaar? Welke impact heeft de test? Kan deze gedaan worden tijdens kantooruren of is het een weekend-klus? Moet de productie hiervoor stilgelegd worden? Wordt replicatie gepauzeerd of afgebroken tijdens de test?
16. **DRaaS** – Moeten er licenties worden aangeschaft of zijn er andere investeringen vooraf?
17. **DRaaS** – Waar wordt de data opgeslagen? Voldoet de service provider aan EU-regelgeving?

## Gebruik

18. Is de oplossing eenvoudig te leren en te gebruiken? Voegt het extra beheerpunten toe of integreert het naadloos?
19. Is granulaire recovery mogelijk? Kan een los bestand, een losse VM, een losse applicatie, een paar applicaties of een hele site hersteld worden?
20. **DRaaS** – Biedt de DRaaS-oplossing zowel self-service als managed services?

HOOFDSTUK 2

# De Zerto-revolutie




## DR naar een nieuw niveau

Zerto heeft replicatie verplaatst van de storagelaag naar de virtualisatie-/hypervisorlaag. Dit resulteert in een innovatieve, hypervisor-gebaseerde, virtualisatie-bewuste replicatie-oplossing die replicatie- en BC/DR-functionaliteit biedt voor grootschalige datacenters en de cloud.

## Continue replicatie

Zerto Virtual Replication (ZVR) repliceert I/O continu zodra deze wordt gecreëerd en biedt RPO's van seconden.

## Applicatie-consistent

Omdat applicaties vaak uit meer dan één VM bestaan, heeft Zerto Virtual Protection Groups (VPG's) ontwikkeld, een unieke functie die replicatie van meerdere VM's als groep mogelijk maakt. Replicatie van VPG's biedt de mogelijkheid om een complete groep consistent te herstellen vanaf een enkel tijdstip, in de juiste schrijfvolgorde.

## Technologie-onafhankelijk

Zerto is hypervisor- en hardware-onafhankelijk. Het verwijdert grenzen naar innovatie en vergroot de efficiency. Doordat het niet gebonden is aan hardware kunnen ook oudere en goedkopere arrays worden gebruikt en verschillende hypervisors. Bovendien is het eenvoudiger nieuwe technologieën toe te passen en te testen, zoals flash arrays.


## Schaalbaar en granulair

Met deze software-gebaseerde oplossing is het eenvoudig recovery-processen te schalen met de infrastructuur. Indien een nieuwe virtual host wordt toegevoegd hoeft alleen een nieuwe virtual appliance te worden geïnstalleerd. Hoewel ZVR zeer grote omgevingen ondersteunt, biedt het de mogelijkheid losse bestanden, VM's, applicaties en complete sites te herstellen voor omgevingen van ieder omvang.

## Eenvoudig beheer

Zerto Virtual Replication integreert naadloos met de bestaande infrstructuur zonder configuratie-aanpassingen in de hypervisor, applicatie of storage. De console kan overal benaderd worden en biedt een compleet overzicht van de omgeving, waarbij issues eenvoudig op te sporen zijn, wat troubleshooting en oplossingen versnelt. ZVR biedt een krachtig dashboard met een consistente look-and-feel op verschillende platforms.

## Eenvoudige recovery

In het geval van een calamiteit kan een eenvoudig failover- en recovery-proces worden gestart vanuit de console. Het is eenvoudig disaster recovery-automatisering te configureren, te testen en uit te voeren. Tests kunnen worden gedaan zonder enige impact op de productie-site of op de replicatie, inclusief testrapporten voor compliance.

## Compleet

Zerto levert een complete oplossing voor virtuele omgevingen met disaster recovery, testen, lange-termijn archivering en migratie voor private, hybrid en public clouds.

HOOFDSTUK 3

# Zerto Virtual Replication

Indien productie wordt gevirtualiseerd ontstaat er een hiaat in de dataprotectie-strategie, omdat deze over het algemeen is gebaseerd op verouderde technieken die zijn gebaseerd op de beperkingen van fysieke systemen. Zerto Virtual Replication brengt de productie-omgeving en het disaster recovery-proces weer op één lijn met een hypervisor-gebaseerde replicatie-oplossing.

In dit hoofdstuk leggen we uit hoe de Zerto-oplossing werkt en welke voordelen deze biedt.

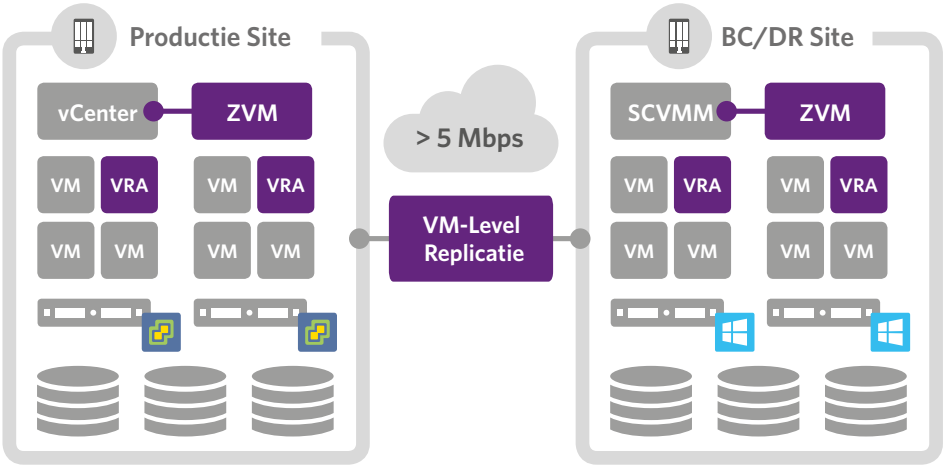
## Architectuur

Het hart van de Zerto replicatie-technologie wordt gevormd door twee componenten:

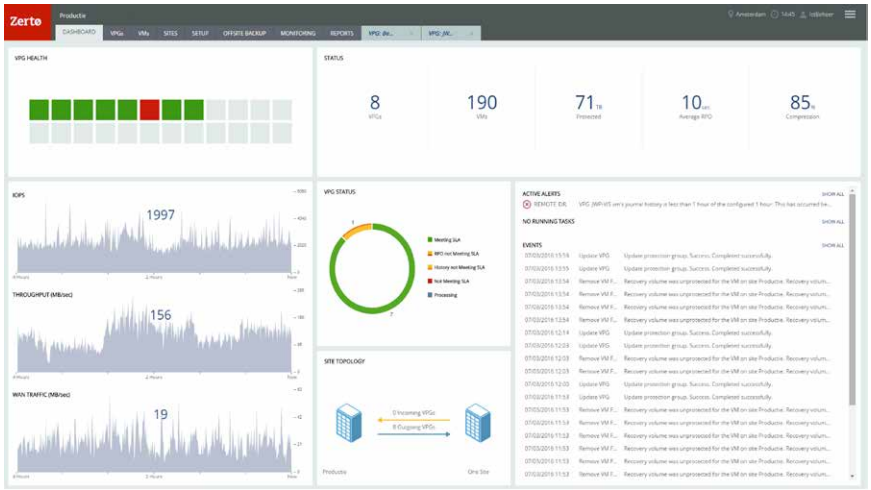
- **Zerto Virtual Manager (ZVM)** – Zerto Virtual Manager beheert de functionaliteit disaster recovery, business continuity en off-site back-up op site-niveau. Het werkt als plug-in voor VMware vCenter of Microsoft System Center Virtual Machine Manager en biedt ook een browser-versie.
- **Virtual Replication Appliance (VRA)** – Repliceert VM's en de bijbehorende virtuele schijven; één VRA wordt geïnstalleerd per ESXi/Hyper-V host.

### Hoe werkt replicatie?

De Zerto Virtual Replication Appliances (VRA) kopiëren I/O zodra het wordt gecreëerd, voordat het de hypervisor verlaat. Deze continue block-level replicatie levert een RPO van seconden en minimaliseert dataverlies in het geval van calamiteiten.




***Figuur 5.*** *De Zerto-architectuur*




***Figuur 6.*** *De interface van Zerto Virtual Manager*

## Functies en voordelen

- **Replicatie-capaciteiten** – Biedt continue, block-level replicatie zonder impact op de applicatie-performance en levert herstel vanuit het journaal dat tussen 1 uur tot en met 14 dagen aan recovery-tijdstippen vastlegt.
- **Hardware- en hypervisor-onafhankelijk** – Verwijdert de grenzen naar innovatie met een replicatie-oplossing zonder afhankelijkheid van hardware of van hypervisors.
- **Eenvoudige, naadloze installatie** – Integreert naadloos met de bestaande infrastructuur zonder downtime of configuratie-aanpassingen.
- **Beschermt productie-workloads** – Zorgt voor applicatie-consistentie met groepen VM's die worden beschermd, beheerd, gerepliceerd en hersteld als één eenheid.
- **Schaalbaar** – Als software-gebaseerde oplossing groeit ZVR mee met de infrastructuur, hoe snel de business ook uitbreidt.
- **Simpel gecentraliseerd beheer** – Gecentraliseerd beheer voor twee sites met Zerto Virtual Manager en voor meerdere sites met Zerto Cloud Manager.
- **Agressieve serviceniveaus** – Behaalt een Recovery Point Objective (RPO) van seconden en een Recovery Time Objective (RTO) van minuten.
- **Complete orkestratie** - Automatiseert failover, failback, omgekeerde protectie is uitgevoerd met een paar muisklikken.
- **Non-disruptive DR testing** – Test het volledige recovery-proces, zonder impact op de productie-site of op de voortgang van de replicatie. Dit biedt u de zekerheid dat het recovery-proces werkt in geval van een calamiteit.
- **Enterprise-class support** – Zerto levert enterprise-class support services die zijn ingebouwd in al haar producten. Deze services behelzen real-time meldingen als RPO's en RTO's niet behaald worden, meldingen bij vertragingen in het netwerk en reminders om de configuratie en de Virtual Protection Groups te checken. Zerto oplossingen worden ondersteund door wereldwijde support service centra die on-demand toegang bieden tot een deskundig team van support engineers.

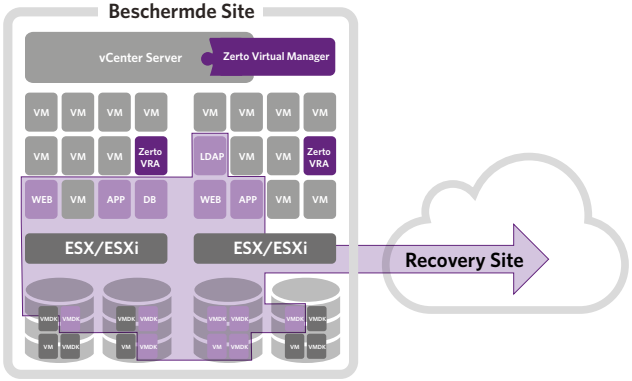
## Management

De Zerto Virtual Manager (ZVM) werkt als een plug-in voor de virtual managementconsole en geeft een grafische weergave van de VM's op de site en hun performance. Indien er een probleem optreedt, wordt dit visueel weergegeven terwijl ook meldingen worden verstuurd. In de tabs bovenaan het scherm is de functionaliteit voor orkestratie en automatisering van failback en recovery-processen, zoals boot order, re-IP, scripts, test en validatie-opties beschikbaar.

### Applicatie-protectie: Virtual Protection Groups

Veel bedrijfsapplicaties bestaan uit meer dan één virtuele server die onderling afhankelijk zijn: een webserver, een applicatieserver, een database-server enz. Indien recovery nodig is, moeten al deze servers consistent worden hersteld vanuit één en hetzelfde tijdstip. Om dit te kunnen heeft Zerto Virtual Protection Groups (VPG) ontwikkeld, die consistentie waarborgen binnen een groep VM's. Op deze manier zorgt Zerto ervoor dat bedrijfsapplicaties consistent worden gerepliceerd en hersteld, ongeacht de onderliggende infrastructuur. Zerto Virtual Replication herkent en onderhoudt de onderlinge relaties en maakt VMware-functies als DRS, vMotion en Storage vMotion mogelijk.

- **Consistent** – Repliceert en herstelt complete, multi-VM applicaties consistent.
- **Flexibel** – Organisaties kunnen een applicatie op verschillende fysieke apparaten installeren, de performance en capaciteit maximaliseren en de complexiteit van de infrastructuur verminderen.
- **Granulair** – Maakt het mogelijk om zowel een enkele VM als groepen VM's te herstellen na verschillende typen calamiteiten.
- **Prioriteiten** – Stelt prioriteiten voor de replicatie en recovery van Virtual Protection Groups.
- **Ondersteuning** – Ondersteunt virtualisatie-functies als vMotion, svMotion, HA, etc.




*Figuur 7. De verschillende VM's waaruit een applicatie bestaat worden in een Virtual Protection Group consistent gerepliceerd, zelfs als deze zijn verspreid over verschillende hosts en datastores.*

## Volledige automatisering en orkestratie

Replicatie van de data naar de DR-site is slechts de helft van het verhaal. De informatie die daar is opgeslagen moet eenvoudig te gebruiken zijn, indien er sprake is van een calamiteit. Zerto herkent dit aspect en heeft geautomatiseerde en georkestreerde processen ingebouwd die kunnen worden uitgevoerd met slechts een paar muisklikken op de precaire momenten dat IT onder hoge druk staat.

### Volledig geconfigureerd failover-proces

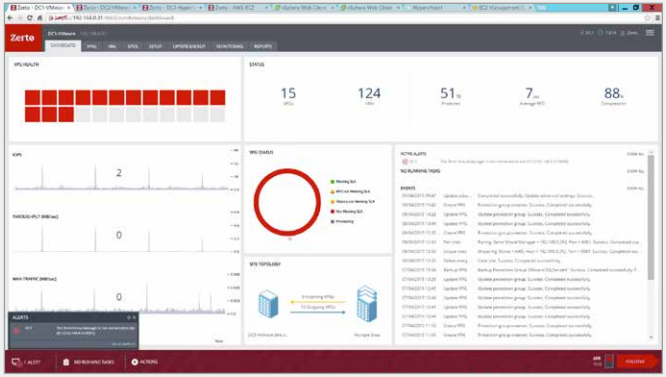
Onderdeel van de VPG-configuratie is het vastleggen van het failover-proces. Onderdeel van deze configuratie zijn boot order, re-IP bij failover, lengte van het replicatie-journaal en andere parameters. Als dit werk vooraf wordt gedaan, reduceert dit het recovery-proces tot een paar muisklikken.

### Failover als business-beslissing

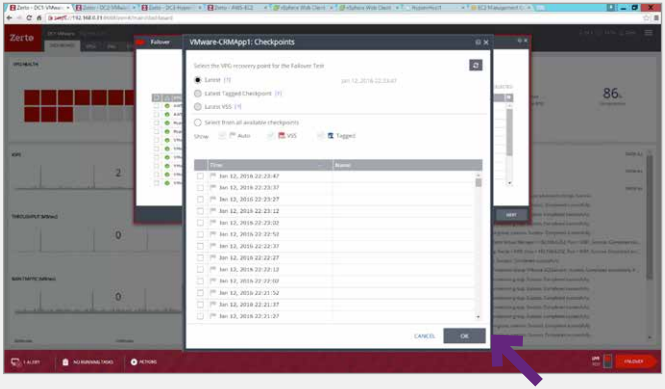
Omdat iedere calamiteit anders is, gelooft Zerto dat failover een business-beslissing zou moeten zijn en niet alleen een geautomatiseerd proces. Omdat het mogelijk is een moment in de tijd uit te kiezen, is deze beslissingsfase essentieel voor een correcte failover. Nadat op de failover-button wordt geklikt start een geautomatiseerd en georkestreerd proces om de services weer online te brengen. Op deze manier kan een failover worden gedaan met de mogelijkheid om een moment in de tijd te kiezen, bijvoorbeeld het moment waarop een database nog niet corrupt was.

## SNEL FAILOVER-PROCES IN 4 STAPPEN

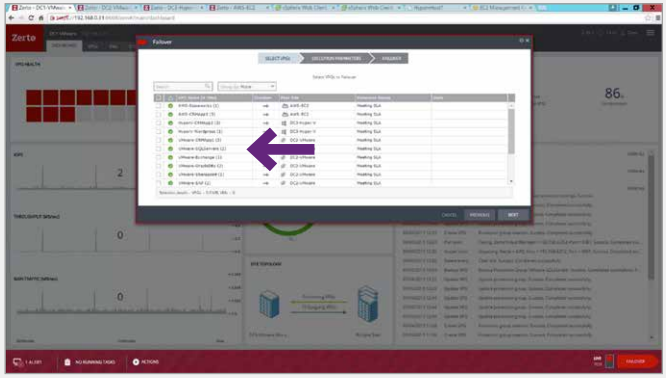
Het failover-proces bestaat uit 4 eenvoudige stappen. Nadat een incident zichtbaar wordt in de managementconsole:



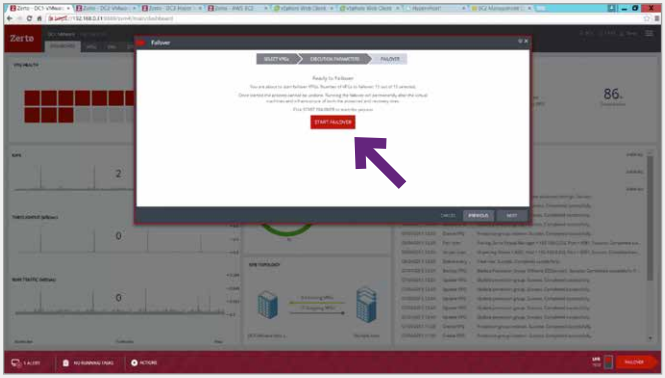
1. **Klik op failover.**



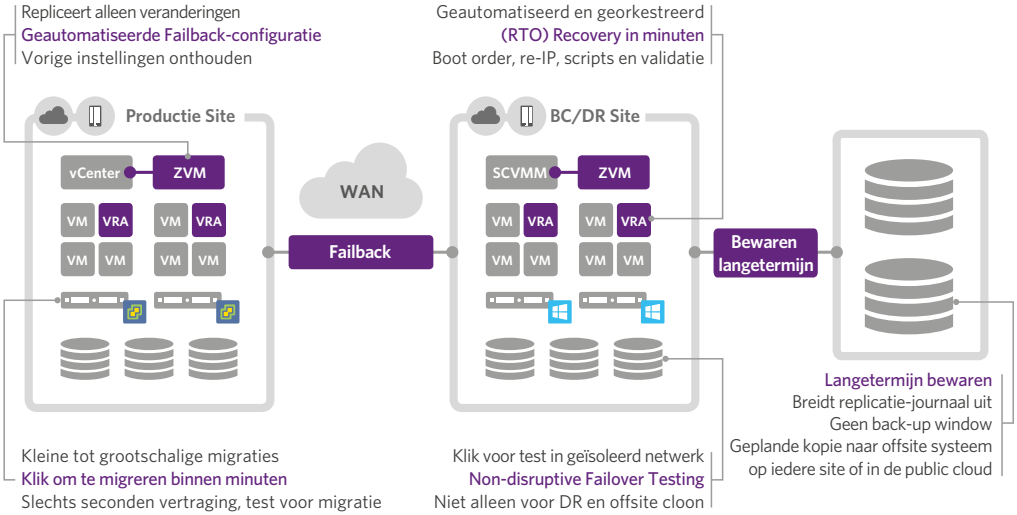
3. **Verifieer het tijdstip** waarnaar de applicaties moeten worden hersteld. Om ervoor te zorgen dat er geen corrupte applicaties worden hersteld, is het nodig terug te gaan naar het punt waarop deze nog niet beschadigd waren.



2. **Selecteer de applicaties** (Virtual Protection Groups) die hersteld moeten worden uit de lijst.



4. **Start het failover-proces.** Het failover-proces vangt aan en VM's worden opgestart en geconfigureerd zoals benodigd.




***Figuur 8.*** *Als het gaat om failback, biedt Zerto volledige automatisering en orkestratie, plus non-disruptive failover tests. Dezelfde functionaliteit kan ook worden ingezet voor sandbox testing en voor datamigratie. De dataprotectie-functionaliteit wordt compleet gemaakt door de mogelijkheid de data op de DR-site te gebruiken om datakopieën voor een langere termijn te bewaren.*

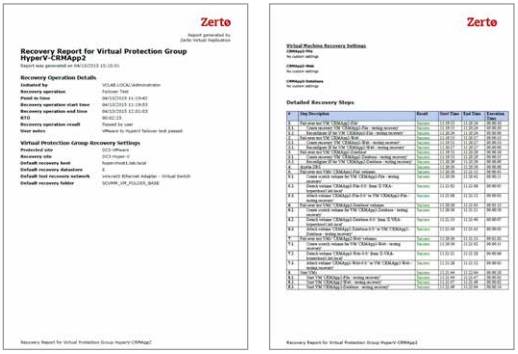
## Automatische failover en failback

Met de configuratie van de VPG's is het recovery-plan gereed. Pre- en post-recovery-scripts kunnen per VPG worden geconfigureerd. Failover en failback zijn met een paar muisklikken uit te voeren. En zelfs als het DR-proces al is geïnitieerd, is het mogelijk om de failover terug te draaien, mochten er issues zijn die niet direct met Zerto te maken hebben, zoals netwerkproblemen. Na een succesvolle failover maakt reverse protection het failback-proces eenvoudig. Reverse protection begint met het synchroniseren van het werk dat is gedaan op de DR-site zodra deze weer klaar is voor gebruik. Nadat de applicaties op de originele productie-site weer up-to-date zijn, is failback wederom in slechts een paar muisklikken geschied. Veel organisaties willen geen failover, juist omdat failback zo'n lastig proces is. Zerto Virtual Replication maakt dat een stuk gemakkelijker.



## Non-disruptive disaster recovery tests

Om te voldoen aan interne en externe compliance-eisen moet een organisatie er wel zeker van zijn dat disaster recovery werkt in het geval van een calamiteit. Zerto Virtual Replication maakt non-disruptive testing mogelijk binnen een sandbox-omgeving, waarbij een succesvolle failover volledig wordt aangetoond. Tijdens de test wordt de productie-omgeving nog steeds beschermd en gaat het replicatie-proces gewoon door. Dit betekent dat DR-tests niet meer in het weekend plaats hoeven te vinden, omdat de productie-site niet hoeft te worden stilgelegd om de test te doen.




***Figuur 9.*** *Non-disruptive disaster recovery tests resulteren in audit-rapporten die kunnen worden gebruikt voor compliance-doeleinden.*

### Sandbox testing

Met behulp van de failover testfunctionaliteit kan Zerto ook een geïsoleerde test- en ontwikkelomgeving creëren.

### Datamigratie

Migraties en consolidaties in het datacenter zijn complexe, tijdrovende projecten die zorgvuldig moeten worden voorbereid en gepland om downtime en productiviteitsverlies te minimaliseren. Met Zerto's hypervisor-gebaseerde replicatietechnologie worden migraties een bijna pijnloze activiteit. Door de kernattributen van ZVR in te zetten, kunnen gevirtualiseerde applicaties vooraf worden getest en worden gemigreerd in een paar minuten met minimale downtime.

- **Eenvoud** – Het migreren van VM's is even eenvoudig als het aanwijzen van de doellocatie voor replicatie en maakt replicatie naar de nieuwe locatie in de achtergrond mogelijk.
- **Granulair** – Migraties kunnen op elk niveau gedaan worden met de mogelijkheid om te migreren op VM-diskniveau (VMDK), waarbij verschillende storage tiers aangewezen kunnen worden.
- **Flexibel** – Ondersteuning voor heterogene omgevingen maakt migraties tussen verschillende typen hardware en tussen verschillende VMware en Hyper-V versies mogelijk, van een vCenter-omgeving naar een vCloud-omgeving, en tussen verschillende versies van ZVR.
- **Volledig geautomatiseerd** – Door de VPG-configuratie te gebruiken kunnen VM's eenvoudig met een paar muisklikken naar een nieuwe locatie worden verplaatst. Dit reduceert downtime van de applicatie tot hooguit enkele minuten met een minimale impact op de productiviteit.

### Datakopieën voor de lange termijn

Omdat de data wordt gerepliceerd naar de DR-site, wordt het eenvoudig om een off-site kopie van de data te maken om te bewaren voor langere termijn of voor compliance-doeleinden. Dit proces en de bijbehorende infrastructuur maken geen deel uit van de productie-omgeving en kunnen zonder impact of overhead worden beheerd vanuit dezelfde ZVR-interface.

### Herstel van bestanden en mappen

Het meest voorkomende incident waar beheerders mee te maken krijgen is niet een natuurramp of een stroomuitval, maar bestanden en mappen die kwijt zijn of per ongeluk verwijderd. ZVR biedt een oplossing voor dit probleem door de mogelijkheid om losse bestanden of mappen te herstellen, tot 14 dagen terug in de tijd. De continue block-level replicatie biedt hersteltijdstippen die slechts seconden van elkaar verwijderd zijn, waardoor het mogelijk wordt terug te gaan tot het punt net voordat een bestand is verwijderd of verdwenen. Dit kan met een paar klikken gedaan worden, waardoor verloren werk tot een minimum wordt beperkt.

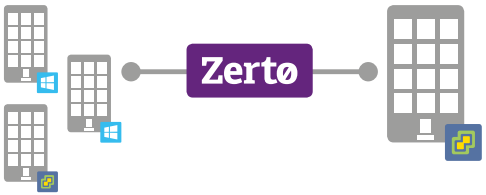
- **Risico** – Minimaliseert verlies van bestanden, mappen, VM's, applicaties en sites door de mogelijkheid om te herstellen op elk niveau en elk moment in de tijd.
- **Eenvoud** – Reduceert de tijd die nodig is voor herstel met de mogelijkheid voor een geautomatiseerde workflow om bestanden, applicaties en data te herstellen.
- **Bescherming van productiviteit** – Als een bestand of map per ongeluk wordt verwijderd, hoeven gebruikers niet langer hun werk opnieuw te doen en dat is goed voor de productiviteit en de motivatie.

HOOFDSTUK 4

# Zerto Virtual Replication: toepassingsvoorbeelden

Zerto Virtual Replication biedt voordelen in uiteenlopende omgevingen. De technologie is storage-onafhankelijk en ondersteunt een mix van hypervisors, wat inhoudt dat iedere site kan worden gerepliceerd naar iedere site, of het nu gaat om een private cloud, een public cloud, een service provider of een lokale vestiging.


**Private Cloud naar Private Cloud**
Het meest traditionele voorbeeld is het opzetten van een DR-site als een versie van het interne datacenter op een andere locatie. Minder traditioneel is de mogelijkheid om elk type storage te gebruiken van elke leverancier met een mix van hypervisors. Zerto ondersteunt het allemaal zonder limiet als het gaat om afstand.



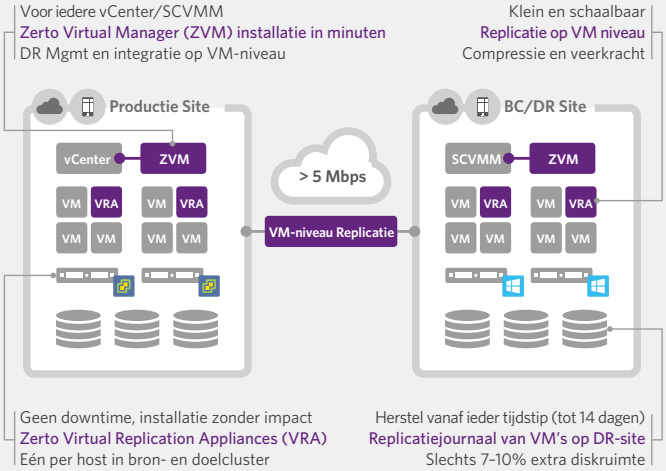

**Dataprotectie en migratie voor vestigingen**
Zerto kan ook worden ingezet voor dataprotectie of migratie van applicaties tussen verschillende vestigingen, wederom met gebruik van elk type storage van iedere leverancier en een mix van hypervisors.


**Hybrid cloud, Disaster Recovery as a Service (DRaaS)**
Diverse cloud service providers bieden de mogelijkheid de cloud in te zetten als DR-site. Indien deze Disaster Recovery as a Service is gebaseerd op Zerto, biedt deze ook alle voordelen van Zerto. Binnen deze services is het mogelijk om DR zelf te configureren via een self-service portal of het te laten beheren door de service provider (Managed Disaster Recovery as a Service). Het is zelfs mogelijk een private cloud in te zetten als DR-site voor een productie-site die zich in de cloud bevindt.


**Self-Service Disaster Recovery as a Service**
Verder is het mogelijk een public cloud service, zoals Amazon Web Services, als DR-site in te zetten. Organisaties moeten dan zelf de service configureren op dezelfde manier als het opzetten van een DR-site op een andere locatie.

# Zerto Samenvatting

## ZERTO ARCHITECTUUR




## ZERTO FUNCTIES

**Hypervisor-based replication** – Hypervisor-gebaseerde replicatie – Continue block-level replicatie tussen VMware en/of Microsoft Hypervisors en tussen meerdere sites.

**Granulaire dataprotectie op VM-niveau** – Bescherm precies wat nodig is: VM's en VMDK's/VHD's.

**Volledige orkestratie** – Automatiseer failover, failback, reverse protection en disaster recovery tests.

**Continue dataprotectie** – Herstel na elk incident vanuit om de paar seconden bewaarde momenten in de tijd, die tot 14 dagen terug kunnen gaan.

**Complete dataprotectie** – Één complete, storage- en hypervisor-onafhankelijke oplossing voor BC/DR, inclusief lange-termijn retentie.

**Eenvoudig management** – Gecentraliseerd management voor twee sites met Zerto Virtual Manager of voor meerdere sites met Zerto Cloud Manager.

**Agressieve serviceniveaus** – Realiseer RPO's van seconden en RTO's van minuten.

**Eenvoudige installatie** – Compleet in een uur zonder applicatie- of storage-configuraties aan te passen.

**Bescherm productie-workloads** – Verzeker u van applicatie-consistentie met groepen VM's die worden beschermd, beheerd en gerepliceerd als een eenheid.

**Off-site retentie** – Breid het nut van gerepliceerde data uit met bewaarmogelijkheden voor de lange termijn vanuit de DR-site.

**Storage-onafhankelijke replicatie** – Geen grenzen tussen systemen door storage-onafhankelijke replicatie.

**Ondersteuning voor de public cloud** – Repliceer, bescherm en migreer workloads naar public cloud services als Amazon Web Services.

## GRATIS DEMO

**Wij laten u graag zien hoe simpel RAM DRaaS werkt. Maak een afspraak via onze website: www.ram-it.nl/DraaS**

ram infotechnology

Zerto

**RAM Infotechnology. Betrokken en Betrouwbaar**

Bij ICT draait het uiteindelijk altijd om het goede gevoel dat alles werkt en blijft werken zoals het hoort. Het vertrouwde gevoel dat alle data, applicaties en software veilig zijn opgeslagen. RAM Disaster Recovery as a Service is daarom de perfecte aanvulling op elke back-up.

Geen organisatie kan het zich permitteren uren, soms zelfs maar minuten, uit de lucht te zijn. En wat denkt u van criminelen die met Locky Ransomware data gijzelen voor losgeld? Juist zorgorganisaties staan op hun targetlist.

Dat maakt DRaaS onmisbaar voor iedere IT-infrastructuur, ook als u werkt met gevirtualiseerde datacenters en cloud-omgevingen. Want met DRaaS is de hersteltijd minimaal. Onze oplossing is een digitale verzekering voor gegarandeerde uptime en minimaal dataverlies.

Wij zijn specialist voor ICT in de zorg. Wij nemen uw ICT net zo serieus als u dat zelf doet. We zitten er bovenop en u kunt altijd op ons rekenen. Ook voor DRaaS.

Zerto levert disaster recovery en business continuity software speciaal voor grootschalige gevirtualiseerde datacenters en cloud-omgevingen.

Zerto's prijswinnende oplossing biedt ondernemingen continue datareplicatie en recovery, specifiek ontworpen voor gevirtualiseerde infrastructuren en de cloud. Zerto Virtual Replication is de eerst hypervisor-gebaseerde replicatie-oplossing voor bedrijfskritische applicaties op de markt en vervangt traditionele array-based BC/DR-oplossingen die niet zijn ontworpen voor de eisen van virtualisatie.

Tegenwoordig nemen ondernemingen van iedere omvang applicaties in gebruik die draaien op gevirtualiseerde infrastructuren en in de cloud. Om de investeringen in deze technologieën optimaal te kunnen inzetten is het noodzakelijk voor organisaties om hun totale IT-strategie op één lijn te brengen. Dat betekent dat de impact van een virtualisatie-strategie in de productie-omgeving alleen ten volle tot haar recht komt als virtualisatie ook in alle andere IT-processen en –procedures wordt betrokken, dus ook in disaster recovery en business continuity.

**RAM Infotechnology**
Ptolemaeuslaan 69
3528 BR Utrecht
Tel: 030 - 2 390 390
**E** marketing@ram-it.nl
**W** www.ram-it.nl

## GRATIS DEMO

**Wij laten u graag zien hoe simpel RAM DRaaS werkt. Maak een afspraak via onze website: www.ram-it.nl/DraaS**