Pink Elephant Disaster Recovery Werkboek NL

Pink maakt IT persoonlijk

Contactinformatie

Titel	Disaster Recovery Werkboek
Datum	11-7-2024
Versie	1.0
Contactpersoon Pink Elephant	Pink Elephant Data Management
Algemene gegevens	Pink Elephant B.V. Bezoekadres Gooimeer 18 1411 DE NAARDEN Postadres Postbus 134 5201 AC DEN BOSCH T 088 – 235 66 55 I www.pinkelephant.nl
Kamer van Koophandel	32055081
Btw-nummer	NL0092.63.342.B.01
IBAN Nummer	NL73RABO 0145 2846 62
Swift	RABO NL2U

Inhoudsopgave

1 Introductie

1.1 Bedrijfsvereisten

De basis van een goed DR-plan zijn de bedrijfsvereisten. Bij een ramp of calamiteit beschrijven bedrijfsvereisten wat nodig is om het bedrijf snel weer operationeel te maken. Enkele voorbeelden van bedrijfsvereisten zijn:

- Wat zijn de belangrijkste bedrijfsprocessen?
- Welke applicaties hebben we nodig om het proces uit te voeren?
- Welke data zijn nodig om de applicatie te laten draaien?
- Hoe snel moeten de data en applicaties hersteld zijn?
- Welke data en applicaties moeten we terugkrijgen en in welke volgorde?
- Wie heeft welke rol in de organisatie?
- Welke van mijn leveranciers kunnen mij helpen?

Zodra de bedrijfsvereisten zijn gedefinieerd, kan deze informatie gebruikt worden als basis voor het schrijven van het DR-plan.

1.2 Disaster Recovery Plan

Een DR-Plan is een gedetailleerd document die de herstelprocedure beschrijft na een ramp zoals:

- Natuurrampen;
- Ransomware;
- Cyberaanvallen;
- Hacking;
- Locatie problemen;
- Gebouw toegankelijkheid;
- Stroomstoringen;
- Menselijke fouten;
- Hardware en/of software fouten.

Ongeacht of u het DR-plan intern beheert of gebruik maakt van de Pink Elephant DMaaS dienstverlening, moet het document gedetailleerde, nauwkeurige en actuele informatie over de IT-activiteiten van de organisatie bevatten. Het is ook van belang dat het gemakkelijk te begrijpen is en informatie bevat die tijdens een ramp kan worden uitgevoerd. Daarnaast adviseren wij ook om het document up-to-date te houden en regelmatig tests uit te voeren om de nauwkeurigheid en volledigheid te bevestigen. De werknemers van de klant en/of Pink Elephant moeten de informatie gemakkelijk kunnen vinden zodat er snel gereageerd kan worden.

Het opstellen van een compleet Disaster Recovery Plan bestaat uit meerdere, belangrijke fases. Deze omvatten:

1. Creëren van een DR-plan;
2. Omgevingsbeoordeling;
3. Bepalen van de DR-locatie;
4. Definiëren van de juiste DR-oplossing voor elke applicatie of bedrijfsproces;
5. Creëren van een DR-omgeving;
6. Schrijven van een DR-procedure;
7. Uitvoeren van de eerste DR-test;
8. Evalueren van de DR-test en de resultaten vergelijken met de bedrijfsvereisten met betrekking tot RTO- en RPO-waarden;
9. Herschrijven, wijzigen of aanvullen van de DR-procedure indien nodig;
10. Plannen van een volgende DR-test.

1.2.1 Fase 1: Creëren van een Disaster Recovery-plan

Het Disaster Recovery plan beschrijft in een gestructureerde aanpak de standaarden en procedures die gevolgd moeten worden om belangrijke bedrijfsprocessen en applicaties zo snel mogelijk weer beschikbaar te maken na een ramp of calamiteit.

In het DR-plan zullen een aantal zaken worden vastgelegd. Op hoofdlijnen zijn dit:

- Vaststellen stakeholders, verantwoordelijkheden en bevoegdheden DR.
- Wie is verantwoordelijk voor welk component?
- Wat is de samenstelling van het DR-team?
- DR Communicatieplan.
- Communicatie afspraken en procedures bij DR.
- Overzicht taken en verantwoordlijkheden bij DR.
- Bepalen Service Level Agreements (SLA's), o.a. RTO en RPO eisen, bewaartermijnen.
- SLA's toewijzen, welke VM krijgt welke SLA.
- Review sessie.

1.2.2 Fase 2: Omgevingsbeoordeling

Een omgevingsbeoordeling wordt gebruikt om meer inzicht te krijgen in de omgeving van de organisatie. Tijdens de beoordeling wordt het belang van applicaties en gegevens gedefinieerd. Ook moeten de RTO (Recovery Time Objective) en RPO (Recovery Point Objective) van de applicaties en gegevens duidelijk zijn voor de organisatie.

1.2.3 Fase 3: Bepalen van de DR-locatie

Beslis over een DR-locatie. Denk aan bijvoorbeeld: een ander gebouw, in een datacenter of in de Cloud. Houd bij het bepalen van de DR-locatie ook rekening met het volgende:

- De afstand tussen de productielocatie en de DR-locatie;
- Het gebied dat moet worden afgezet bij een bomaanslag of terroristische aanval op de productielocatie en of de DR-locatie buiten dit gebied moet blijven;
- Of fysieke toegang tot deze DR-locatie verplicht of optioneel is;
- Of de DR-locatie alleen nodig is voor computing of ook voor kantoorgebruikers;
- Wat de overheidsvoorschriften met betrekking tot geografische gegevens zijn en of de gegevens in het land moeten blijven;
- Controleer de omgeving van de DR-locatie op andere belangrijke aspecten die bekend moeten zijn, zoals:
    - Het bewustzijn van het zeeniveau van de DR-locatie;
    - Of er chemische bedrijven in de buurt van de DR-locatie zijn en of een ramp in deze bedrijven de toegang tot uw DR-locatie zal beïnvloeden.

1.2.4 Fase 4: Definiëren van de juiste DR-oplossing voor elke applicatie of bedrijfsproces

Afhankelijk van de RTO en RPO moet het bedrijf beslissen welke software, opslag of gecombineerde oplossing ze gaan gebruiken voor DR, bijvoorbeeld:

- Data herstellen met een back-up;
- Data replicatie;
- Opslag replicatie.

Deze keuze is ook gerelateerd aan de DR-locatie, omdat niet alle oplossingen op alle DR-locaties kunnen worden gebruikt. Bijvoorbeeld, als de voorkeur uitgaat naar het gebruik van opslag replicatie van een specifiek merk, is het waarschijnlijk niet mogelijk, bijvoorbeeld in Microsoft Azure Cloud.

1.2.5 Fase 5: Het creëren van een DR-omgeving

Op basis van de beslissingen die zijn genomen in de vorige stappen, zal de DR site/-omgeving worden geconfigureerd en voorbereid om de back-up- en/of replicatiegegevens te ontvangen.

1.2.6 Fase 6: Het schrijven van een DR-procedure

Het Pink Elephant Disaster Recovery werkboek is een technische werkinstructie waarin alle benodigde handelingen op technisch niveau worden beschreven om een gehele, of een gedeeltelijke disaster recovery uit te voeren.

Het samenstellen van een compleet Disaster Recovery werkboek bestaat uit meerdere fasen die als volgt zijn opgebouwd:

- Het beoordelen van de omgeving die binnen de scope valt (uitgaande van het DR-plan);
- Het beschrijven dan de DR-procedure(s).

1.2.7 Fase 7: Uitvoeren van de eerste DR-test

Een van de belangrijkste fasen bij het creëren van een DR-oplossing is de DR test. Het testen van het DR-plan moet op terugkerende intervallen worden ingepland om ervoor te zorgen dat alle aspecten van het plan nog steeds correct zijn. Belangrijke kwesties die worden aangepakt door een uitgebreid DR-plan zijn onder andere:

- Zijn de medewerkers en/of Pink Elephant Data Management personeel in staat om het plan uit te voeren?
- Zijn de gegevens binnen de gewenste tijdschema's toegankelijk?
- Zijn er voorzieningen getroffen om middelen of medewerkers aan te passen die mogelijk niet kunnen deelnemen aan het herstelproces vanwege de ramp?
- Wordt het Recovery Time Objective (RTO) behaald?
- Wordt het Recovery Point Objective (RPO) behaald?

1.2.8 Fase 8: Evaluatie van de DR Test

Het evalueren van de DR test omvat het beoordelen van wat positief was en wat moet worden gewijzigd. Controleer ook of het mogelijk was om te voldoen aan de RTO- en RPO-eisen, evenals de bedrijfsvereisten. Als niet, wat moet er dan worden aangepast?

1.2.9 Fase 9: Herschrijven/ wijzigen of aanvullen van de DR-procedure indien nodig

Afhankelijk van de uitkomst van de evaluatie moet de procedure worden aangepast of aangevuld.

1.2.10 Fase 10: Plannen van een volgende DR

Ons advies is om kort na het aanpassen/aanvullen van de DR test als gevolg van de eerste DR een volgende DR test in te plannen, om de procedure verder te optimaliseren.

2 Beoordeling

Tijdens de beoordeling wordt een overzicht gemaakt dat kan worden gebruikt om de kritieke applicaties, gegevens en middelen te bepalen die nodig zijn voor het hosten van de applicaties of gegevens.

Deze beoordeling moet worden gemaakt voor elke applicatie of proces dat kan helpen bij het vaststellen van de bedrijfsvereisten.

2.1 Beoordeling CIA-driehoek (Triad)

Vertrouwelijkheid (Confidentiality), integriteit (Integrity) en beschikbaarheid (Availability (CIA), ook bekend als de CIA-driehoek, is een model dat is ontworpen om richtlijnen te geven voor informatiebeveiliging binnen een organisatie. Door dit model te gebruiken wordt het gemakkelijker om te beslissen welke applicaties en/of gegevens cruciaal zijn voor de bedrijfscontinuïteit en welke niet.

Hieronder is een beschrijving te zien van de drie belangrijkste concepten van de CIA-driehoek:

- Vertrouwelijkheid (**Confidentiality**) komt ruwweg overeen met ‘Vertrouwelijkheidsmaatregelen’ en is bedoeld om te voorkomen dat gevoelige informatie door onbevoegden wordt benaderd. Gegevens worden vaak gecategoriseerd op basis van de hoeveelheid en het type schade die zou kunnen ontstaan als ze in verkeerde handen zouden vallen. Op basis van deze categorieën kunnen meer of minder strikte maatregelen worden geïmplementeerd.
- Integriteit (**Integrity**) houdt in dat de consistentie, nauwkeurigheid en betrouwbaarheid van de gegevens gedurende hun hele levenscyclus worden gehandhaafd. Gegevens mogen niet worden gewijzigd tijdens verzending en er moeten stappen worden genomen om ongeoorloofde wijziging van gegevens te voorkomen (bijvoorbeeld bij een schending van de vertrouwelijkheid).
- Beschikbaarheid (**Availability**) betekent dat informatie consistent en gemakkelijk toegankelijk moet zijn voor geautoriseerde partijen. Dit omvat het goed onderhouden van hardware en technische infrastructuur en de systemen die de informatie dragen en weergeven.

Wij raden aan om deze CIA-driehoek beoordelingen te gebruiken om uw applicaties te classificeren in een bedrijfscontinuïteitsplan. De CIA-driehoek beoordeling kan worden gebaseerd op de waarden zoals weergegeven in de onderstaande tabel.

Betrouwbaarheids-aspect	Betrouwbaarheidsniveau (klasse)		
	1 (Gewenst)	2 (Aanbevolen)	3 (Vereist)
Vertrouwelijkheid	Afgeschermd Informatie is alleen beschikbaar voor geselecteerde personen. (Alleen voor intern gebruik)	Cruciaal Informatie is alleen beschikbaar voor degenen die direct betrokken zijn. (Vertrouwelijk)	Verplicht Bedrijfsbelangen worden ernstig geschaad als er ongeautoriseerde toegang wordt verkregen. (Geheim)
Integriteit	Actief Sommige fouten zijn toegestaan.	Detecteerbaar Er is een zeer klein aantal fouten toegestaan.	Onmisbaar Er zijn geen fouten toegestaan.
Beschikbaarheid	Noodzakelijk Af en toe is verstoring acceptabel.	Essentieel Tijdens kantooruren is vrijwel geen verstoring toegestaan.	Onmisbaar Verstoring kan alleen voorkomen in zeldzame omstandigheden.

Om de toepassingsclassificaties te correleren met de CIA-TRIAD-beoordeling, wordt de volgende tabel gebruikt.

Classificatie	C	I	A	
Platinum	3	3	3	Alle systemen met deze CIA-driehoek beoordeling of hoger
Goud			3	Alle systemen met deze CIA-driehoek beoordeling of hoger
Zilver			2	Alle systemen met deze CIA-driehoek beoordeling of hoger
Brons	1	1	1	Alle systemen met deze CIA-driehoek beoordeling of hoger

Het wordt aanbevolen om een RPO en RTO toe te wijzen aan elke toepassingsclassificatie. Om een wildgroei te verschillende RPO- en RTO-waarden te voorkomen, is er een classificatie in serviceniveaus vastgesteld. Deze worden getoond in de volgende tabel.

Classificatie	Omschrijving	RPO	RTO
Platinum	Missie kritiek		
Goud	Bedrijfskritisch		
Zilver	Ondersteunend voor het bedrijf		
Brons	Ondersteunend		

2.1.1 Data en back-ups

Op basis van de bovenstaande classificatie kunnen de applicaties en gegevens in de organisatie nu in een classificatie worden ingedeeld. Voeg indien nodig rijen toe of verwijder deze in de onderstaande tabel.

Klasse	Applicatie / Data	Classificatie (Platinum, Goud, Zilver en Brons)	Huidige back-up frequentie (Uurlijks, Dagelijks, Wekelijks, enz.)	Back-up Locaties (Locatie waar de gegevens worden geback-upt)
	Email	*Platinum*	*Dagelijks*	*Op locatie en een kopie naar de DMP Cloud*
1				
2				
3				
4				

2.2 Middelen

Nu we de toepassingsclassificatie hebben, is het duidelijk welke applicaties nodig zijn tijdens een ramp. De volgende stap is om de benodigde middelen op de ramp locatie te bepalen. Deze middelen kunnen in twee typen worden onderverdeeld.

- Kern infrastructuurmiddelen: dit zijn middelen die nodig zijn om een nieuwe infrastructuur op te bouwen, zoals hypervisors, Active Directory, DNS, DHCP, enz.
- Applicatiemiddelen: deze middelen zijn nodig om een applicatie te hosten en te laten draaien. Bijvoorbeeld een applicatie die is geïnstalleerd op een dedicated server en een SQL-database gebruikt die is opgeslagen op een aparte SQL-server. In dit voorbeeld gebruikt deze applicatie twee servers.

2.2.1 Kern infrastructuurmiddelen

De servers die in de onderstaande tabel worden genoemd, zijn alle servers die de kerninfrastructuur vormen en beschikbaar moeten zijn voordat de applicaties kunnen worden gestart, maar zijn niet exclusief voor bepaalde applicaties. Voeg indien nodig rijen toe of verwijderd deze in de onderstaande tabel.

		Configuratie				
Server	Rol	vCPU	Geheugen (Gb)	Schijf	Doel	Grootte (Gb)
DC01	*Active Directory*	*2*	*16*	*C*	*OS*	*100*
				D	*Applicatie*	*50*

2.2.2 Applicatiemiddelen

Op basis van onze ervaring hebben we geconstateerd dat het voor het IT-team veel moeilijker is om te bepalen welke middelen bij een applicatie horen. We zien vaak dat het IT-team alleen verantwoordelijk is voor het leveren van de infrastructuur van een applicatie, terwijl de applicatiebeheerder de gedetailleerde configuratie van een applicatie kent.

Het zal dus meer tijd kosten om de middelen te bepalen die voor een applicatie nodig zijn. De volgende paragrafen beschrijven een procedure voor het uitvoeren van een beoordeling van deze applicaties.

2.2.2.1 Beoordeling Applicatiemiddelen

Deze sectie moet worden uitgevoerd voor elke applicatie in de bedrijfsomgeving die nodig is tijdens een Disaster Recovery.

2.2.2.1.1 Samenvatting (voorbeeld)

"KLANTAPPLICATIE" is een applicatie die aan gebruikers worden aangeboden en die toegankelijk is vanaf kantoorlocaties of vanaf externe locaties via een Citrix Netscaler verbinding.

Het gebruik van de "KLANTAPPLICATIE" kan in eerste instantie alleen basisfunctionaliteiten bieden om het mogelijk te maken om kernbedrijfsprocessen zo snel mogelijk op te starten in geval van een ramp. Om het bedrijfsproces weer te herstellen, is het noodzakelijk om de systemen die verbonden zijn met de "KLANTAPPLICATIE" zo snel mogelijk weer online te brengen nadat de basisfunctionaliteiten beschikbaar zijn gesteld.

De middelen die nodig zijn om de basisfunctionaliteiten van de "KLANTAPPLICATIE" online te brengen zijn:

	Aantal
Totaal Servers/ VM's	
Totaal (v) CPU-gebruik	
Totaal geheugengebruik in GB	
Totaal schijfgebruik in GB	

De middelen die nodig zijn om de volledige functionaliteiten van de "KLANTAPPLICATIE" online te brengen zijn:

	Aantal
Totaal Servers / VMs	
Totaal (v) CPU-gebruik	
Totaal geheugengebruik in GB	
Totaal schijfgebruik in GB	

2.2.2.2 Kenmerken van de “KLANTAPPLICATIE”

2.2.2.2.1 Applicatie-eigenaren

Om de applicatie “KLANTAPPLICATIE” online te brengen, zijn Applicatie-eigenaren aangesteld. Deze Applicatie-eigenaren zijn verantwoordelijk voor de applicatie (server) evenals voor de overige generieke en verbonden servers/diensten. Deze eigenaren zijn opgenomen in de volgende tabel.

Eigenaar	Rol	Telefoonnummer
John Doe	*Exchange administrator*	*+31 645 123 123*

2.2.2.2.2 Applicatie servers

De servers die in de onderstaande tabel worden getoond, zijn alle servers of diensten die essentieel zijn om de basisfunctionaliteiten van de “KLANTAPPLICATIE” beschikbaar te maken.

		Configuratie				
Server	Rol	CPU	Geheugen (Gb)	Schijf	Doel	Grootte (Gb)
SQL01	*Active Directory*	*2*	*16*	*C*	*OS*	*100*
				D	*Application*	*50*

2.3 Verbonden servers

De servers die in de onderstaande tabel worden getoond, zijn alle servers die deel uitmaken van de “KLANTAPPLICATIE” of verantwoordelijk zijn voor de invoer of uitvoer van informatie vanuit de “KLANTAPPLICATIE”, maar die niet nodig zijn voor de basisfunctionaliteit.

		Configuratie				
Server	Rol	vCPU	Geheugen (Gb)	Schijf	Doel	Grootte (GB)
Print01	*Print Server*	*2*	*16*	*C*	*OS*	*100*
				D	*Application*	*50*

2.4 Connectiviteit

Het gebruik van de “KLANTAPPLICATIE” wordt mogelijk gemaakt door verschillende methoden, afhankelijk van het gebruik. In de onderstaande tabel worden de vereiste connectiviteitsopties voor elke variatie getoond.

Locatie	Onderdeel	Connectiviteit
Offices	Thin Client	Port gebruik
Offices	Desktop	Port gebruik
Remote	Laptop	Internet connective middels Gateway

3 Pink Elephant Data Management diensten

3.1 Pink Elephant Data Management Dienstverlening

Pink Elephant biedt verschillende soorten cloudopslag- en back-up oplossingen aan die gebruikt kunnen worden met de producten in ons portfolio.

- DMaaS Hybrid Cloud (DHC)
- DMaaS Disaster Recovery

Al deze diensten worden aangeboden op basis van een Cloud model met een pay-per-use systeem.

3.1.1 Pink Elephant DMaaS Hybrid Cloud

DMaaS Hybrid Cloud is ondergebracht op de infrastructuur van Pink Elephant welke gesitueerd is in datacenters in Nederland en Duitsland. Binnen de infrastructuur wordt gebruik gemaakt van NVMe technologie van NetApp en Intel-CPU gebaseerde server systemen. Het virtualisatie platform is op basis van VMware.

In DMaaS Hybrid Cloud krijgt de klant een tenant met alle beheers mogelijkheden die nodig zijn om virtuele machines aan te maken, te verwijderen of van samenstelling te veranderen.

Daarnaast zijn er binnen de tenant mogelijkheden om netwerken aan te maken en verschillende connecties te leggen.

Voor overige details verwijzen wij u graag naar de Product Catalogus van Pink Elephant.

3.1.2 DMaaS Disaster Recovery

DMaaS DR is een “Assisted DR”, een service waarbij Pink Elephant de klant helpt bij het plannen, implementeren en beheren van DR-processen en -procedures. De klant heeft hierbij nog steeds een actieve rol in het DR-proces, maar kan vertrouwen op de expertise en ondersteuning van de derde partij om ervoor te zorgen dat de DR-strategie effectief is en voldoet aan de vereisten. DMaaS DR kan de klant helpen om te besparen op de kosten en middelen die nodig zijn voor het beheer van DR, terwijl toch een hoog niveau van bescherming tegen uitval en storingen wordt geboden.

Als een belangrijk onderdeel van de DR-dienstverlening zullen Pink Elephant en de klant gezamenlijk een DR-plan uitwerken. Geen enkele organisatie is gelijk. Daarom wordt er organisatie specifiek en in samenwerking met de relevante stakeholders een Disaster Recovery Plan (DRP) opgesteld. In dit plan wordt onder andere vastgesteld wie er verantwoordelijk is voor welke stappen binnen het herstelproces, de technische afhankelijkheid tussen de verschillende workloads en welke applicaties essentieel zijn voor de bedrijfsvoering.

Om tot dit plan te komen vindt er een workshop plaats. Deelnemers hier in zijn in ieder geval beheerders van het back-up platform als ook de beheerder(s) van de applicatie(s).

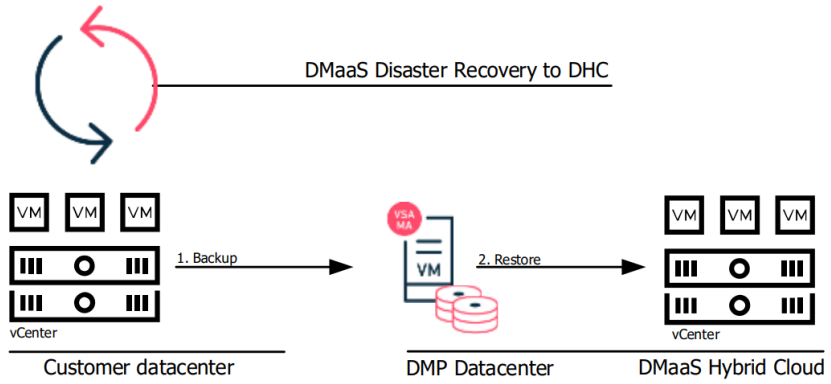
Het DR-werkboek is een werkdocument, uniek voor elke organisatie, waarin de noodzakelijke stappen worden beschreven om te herstellen van een ramp of serviceonderbreking. Het omvat primaire en escalatiecontacten, samen met infrastructuur- en procesinstructies die teamleden moeten volgen. Een DR-werkboek richt zich voornamelijk op de technische details van het herstelproces. Het opstellen van het DR-werkboek maakt geen onderdeel uit van DMaaS DR. Op basis van professional services kan Pink Elephant ondersteunen bij het opstellen van het DR-werkboek.

3.2 Pink Elephant DMaaS DR Priority levels

Als onderdeel van de DR-diensten biedt DMaaS Back-up verschillende Disaster Recovery diensten aan met verschillende Service Level Agreements (SLA's):

- DMaaS DR Zilver
  - De VM's gaan mee in de back-up. Bij calamiteit wordt een restore van de VM gestart.
- DMaaS DR Goud
  - De VM's gaan mee in de back-up, zodra de back-up klaar is, wordt deze ge-restored op de uitwijk locatie. De VM consumeert minimaal CPU en geheugen tijdens de validatie.
- DMaaS DR Platinum
  - De VM's worden gerepliceerd tussen productie en de uitwijk omgeving door het DMaaS platform Periodic Replication proces. De VM consumeert minimaal CPU en geheugen tijdens de validatie.

Voor zilver, goud en platinum wordt gebruik gemaakt van DMaaS CloudDrive Standaard als primaire bron van restore.



Op basis van een TAG op de VM wordt door de klant bepaald welke SLA van toepassing is op de desbetreffende VM. Voor elke VM met DR-tag zal een availability fee worden berekend, wat garandeert dat erbij uitwijk voldoende resources beschikbaar zijn.

3.2.1 DMaaS DR Zilver

Uitgangspunt is dat 20% van alle VM's bij de klant gebruik maken van de Zilver SLA:

- De RPO is in deze situatie maximaal 24 uur. Dit is gebaseerd op één back-up per dag. Deze RPO kan worden geoptimaliseerd door meerdere keren per dag incrementele back-ups uit te voeren.

Concreet zal dit betekenen dat de klant voor een herstel van productiedata een RPO heeft van maximaal 24 uur en een RTO van ca 300-500 GB/h per VM. In totaal is de restore snelheid 1TB/uur.

Groot voordeel van deze methode is dat er afgezien van de gerepliceerde back-up data er geen compute, memory en productie storage consumptie is. Dit zal pas plaats vinden op het moment dat de restore gestart wordt.

3.2.2 DMaaS DR Goud

Uitgangspunt is dat 70% van alle VM's bij de klant gebruik maken van de Goud SLA:

- De RPO is in deze situatie maximaal 24 uur. Dit is gebaseerd op basis van één back-up per dag. Deze RPO kan worden geoptimaliseerd door meerdere keren per dag een incrementele back-up uit te voeren.
- De RTO van Goud is veel korter dan bij de Zilver. Dit komt doordat er na de back-up direct replicatie (restore) plaatsvindt, waardoor VM's hersteld klaar staan.
- Er vindt na replicatie een validatie van de VM plaats, door de VM kort aan en uit te schakelen.

Concreet zal dit betekenen dat de klant een RPO heeft van maximaal 24 uur en een RTO van bijna nul en eventuele incrementele restore tijd krijgt. Hierdoor zijn systemen bij een DR vrijwel direct weer beschikbaar.

SLA goud maakt gebruik van productie storage op DMaaS Hybrid Cloud.

3.2.3 DMaaS DR Platinum

Uitgangspunt is dat 10% van alle VM's bij de klant gebruik maken van de Platinum SLA:

- De RPO is in deze situatie minimaal 15 minuten.
- Er vindt na replicatie een validatie van de VM plaats, door de VM kort aan en uit te schakelen.

Concreet zal dit betekenen dat de klant een RPO van minimaal 15 minuten krijgt. En een RTO van bijna nul. Mocht er behoefte zijn aan een nog kortere RPO dan adviseren we applicatie redundantie of hardware/storage replicatie.

SLA Platinum maakt gebruik van productie storage op DMaaS Hybrid Cloud.