



Gemeente Haarlem

Vernieuwing back-up/ disaster & recovery

Beschrijving gewenste situatie

22-04-2025

Versie: 1.0

Kenmerk: 2025/0426831

Inhoudsopgave

INHOUDSOPGAVE.....	2
1. INLEIDING.....	3
2. INITIËLE INRICHTING	4
2.1 GEWENSTE SITUATIE IN 2025.....	4
2.2 GEWENSTE SITUATIE IN 3 TOT 5 JAAR	6
2.3 STORAGE LOCATIES	6
2.4 BACK-UP STRATEGIE.....	7
2.5 RESTORE	7
2.6 HYPERVISOR (VIRTUALIZATION)	8
2.7 ARCHETYPES	8
2.8 RETENTIE	8
2.9 MANAGEMENT SERVER.....	9
2.10 HARDWARE	9
2.11 CLOUD	9
3. SECURITY	10
3.1 VALIDATIE TE HERSTELLEN DATA UIT DE BACK-UP	10
3.2 RANSOMWARE PROTECTION.....	10
3.3 COMPLIANCY	10

1. Inleiding

In 2025 verlopen de contracten van de hard- en softwarecomponenten van de back-up/disaster & recovery oplossing in de datacenters van de gemeente Haarlem en Zandvoort (Opdrachtgever).

Opdrachtgever wil middels een Europese aanbesteding het ontwerp, de configuratie, de implementatie en de support van een nieuwe back-up/ disaster & recovery oplossing aanbesteden.

Onderhavig document beschrijft de gewenste situatie van de nieuwe back-up/disaster & recovery oplossing, welke in Bijlage 4 'Programma van Eisen' verder is gespecificeerd.

2. Initiële inrichting

Opdrachtgever onderscheidt de volgende kaders en uitgangspunten voor de nieuwe back-up/disaster & recovery oplossing.

- Uitgangspunten bedrijfscontinuïteit:
 - Hoeveel gegevens mag je – uitgedrukt in uren verwerking – verliezen? Dit staat bekend als RPO of Recovery Point Objective.
 - Na hoeveel tijd moeten systemen weer beschikbaar zijn? Dit staat bekend als RTO of Recovery Time Objective.

Iedere organisatie kiest daarin een eigen positie. Opdrachtgever stelt als generieke eis dat maximaal de laatste 24 uren verwerking verloren mag gaan. Daarmee blijft het mogelijk om met een dagelijkse back-up te werken. Als wettelijke eisen op onderdelen strenger zijn, dan wordt daarin per geval een modus gekozen.

Bij technisch herstel na een calamiteit kan niet alles tegelijk. De belangrijkste systemen komen eerst en moeten binnen 5 dagen hersteld zijn. Overige systemen komen daarna, en moeten binnen 10 dagen hersteld zijn.

De nieuwe back-up/disaster & recovery oplossing dient bovenstaande te faciliteren.

Waarbij Opdrachtgever bewust is dat dit mede afhangt van de hardware en de verbindingen. Daarom wordt Inschrijver ook verzocht om in het concept Ontwerp te beschrijven wat de specs/requirements voor de hardware en de verbindingen zijn, om zorg te dragen dat de systemen van de gemeente bij een disaster met behulp van de nieuwe oplossing binnen 10 dagen hersteld zijn (zie ook 7.1.2 in de Aanbestedingsleidraad).

Dus met behulp van de nieuwe back-/disaster & recovery oplossing en de door de Inschrijver voorgestelde hardware en verbindingen dienen de systemen van de gemeente bij een disaster binnen 10 dagen hersteld te zijn.

- Uitgangspunten opslag locatie:

Vanwege die specifieke Cloud-risico's oordeelt Opdrachtgever wat wel en niet in een Cloud mag draaien. Als de applicatie te gevoelig is voor de Cloud, dan kan de back-up van de applicatie ook te gevoelig zijn voor de Cloud.

Vanuit dit gezichtspunt maakt Opdrachtgever op abstract niveau een onderscheid tussen de volgende soorten applicaties:

 - Categorie A; applicatie mag niet naar de Cloud / is te gevoelig om naar de Cloud te mogen.
 - Categorie B; applicatie mag wel naar de Cloud/ zit in de Cloud.

Back-up data van Categorie A kan dus niet in de Cloud opgeslagen worden, back-up data van Categorie B wel.

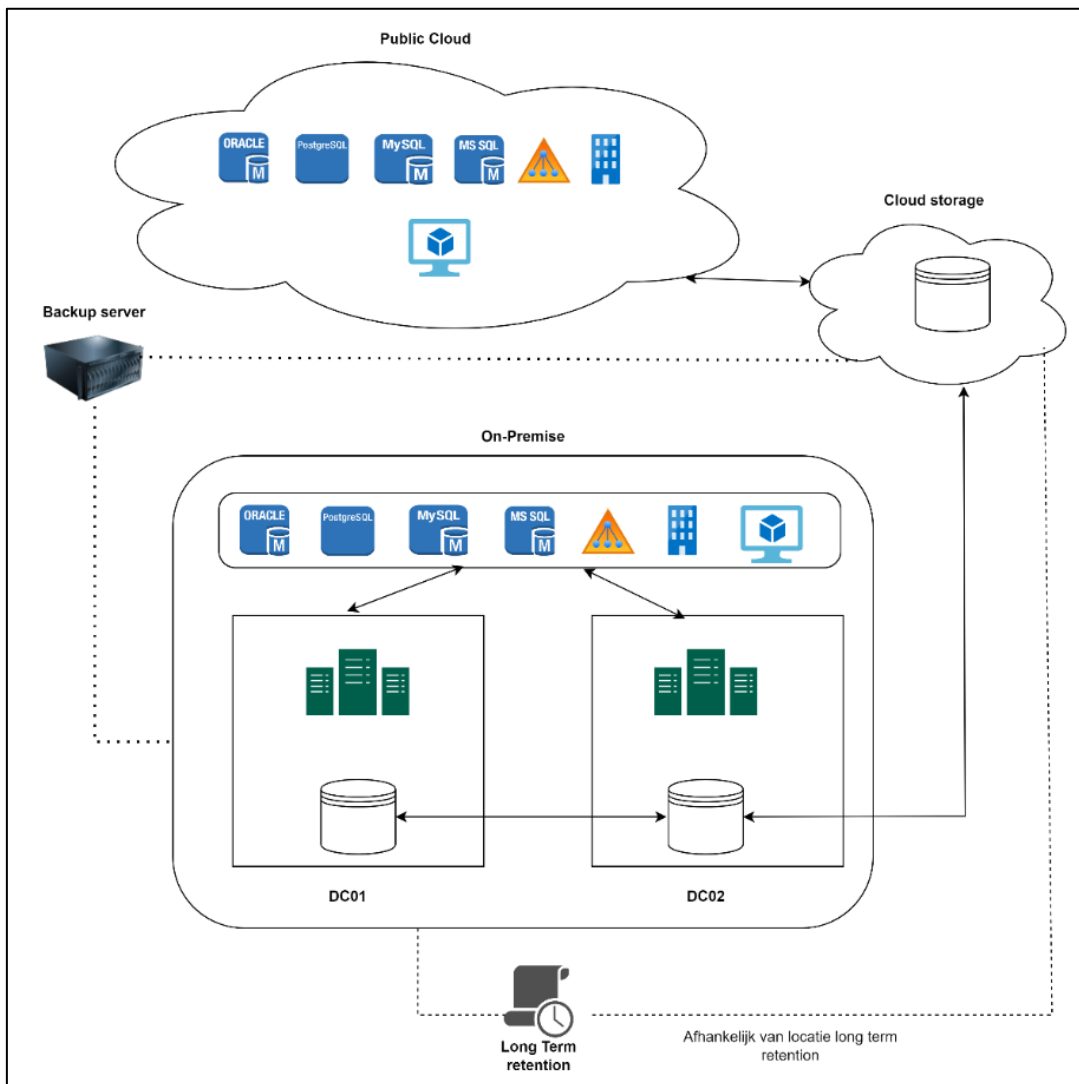
- Uitgangspunten gewenste situatie:
 - Het ontwerp en de implementatie van de nieuwe oplossing moet voldoen aan de kenmerken toekomstgericht, toekomst vast, flexibiliteit, continuïteit,

simpel (vermijden van onnodige complexiteit), geautomatiseerd en sterke beveiliging.

- Verder geldt dat de nieuwe oplossing moet voldoen aan de gedefinieerde functionele en non-functionele eisen in het Programma van Eisen, zie Bijlage 4.

2.1 Gewenste situatie in 2025

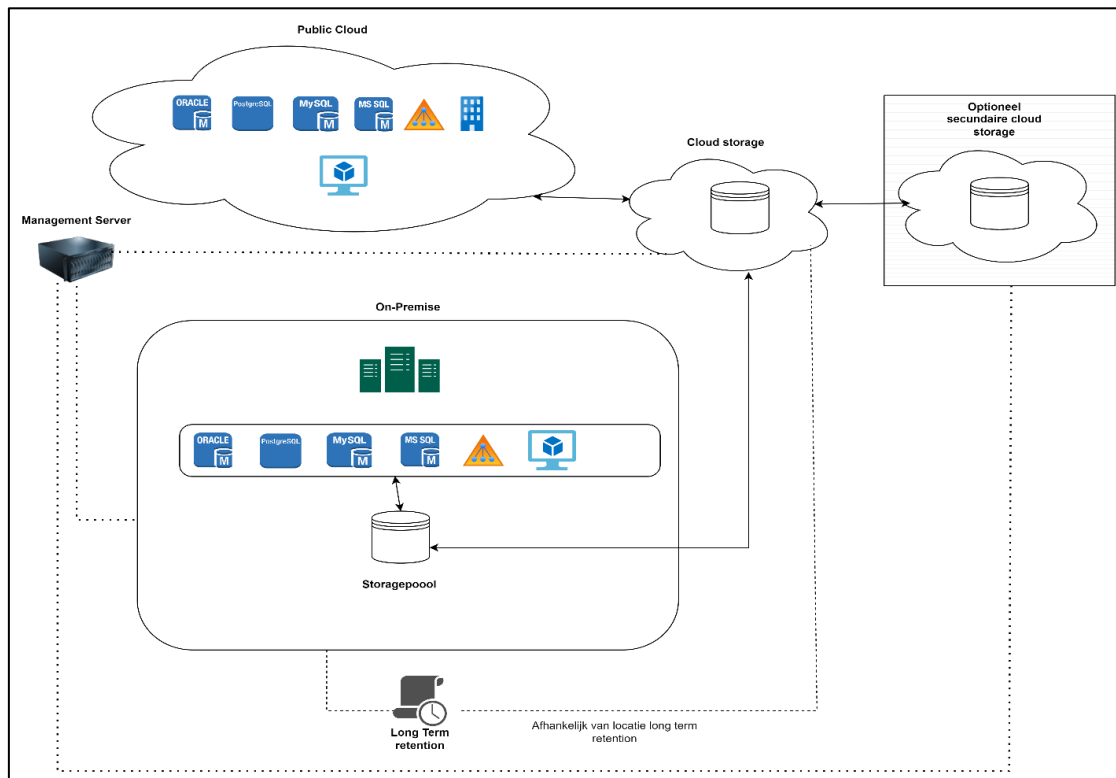
Schematisch ziet de initiële inrichting (2025) van de back-up/disaster & recovery oplossing er als volgt uit:



Schematische weergave architectuurplaat initiële inrichting back-up/ disaster & recovery oplossing.

2.2 Gewenste situatie in 3 tot 5 jaar

De Opdrachtgever staat aan de vooravond van de migratie naar de Cloud. Schematisch ziet de inrichting van de back-up/disaster & recovery oplossing over 3 tot 5 jaar er dan als volgt uit:



Schematische weergave architectuurplaat back-up/ disaster & recovery oplossing over 3 tot 5 jaar

2.3 Storage locaties

Opdrachtgever onderscheidt de volgende eisen m.b.t de storage locaties:

- Opdrachtgever wil 2 storage pools on-premise, 1 per datacenter; deze storage pools worden onderling gerepliceerd.
- Verder is het waarschijnlijk dat in de toekomst 1 datacenter zal worden geconsolideerd. In dat geval is het een optie om een 2e Cloudstorage locatie te gaan gebruiken. Al dan niet bij een andere Cloudprovider, deze storage zal een extra kopie herbergen.
- Back-ups van componenten in de Cloud worden primair weggeschreven naar de Cloud storage om vervolgens te worden gerepliceerd naar de on-premise storage als secundaire kopie.
- Back-up van componenten on-premise (Categorie B) worden primair weggeschreven naar de on-premise storage om vervolgens te worden gerepliceerd naar de Cloud storage als extra kopie.
- Back-up van componenten on-premise (Categorie A) worden primair weggeschreven naar de on-premise storage om vervolgens te worden gerepliceerd naar de andere on-premise storagepool als extra kopie.
- Alle kopieën worden immutable opgeslagen.
- Er dient een selectieve set aan data kunnen worden weggeschreven naar een storage oplossing voor lange termijn retentie (≥ 7 jaar). De bron voor deze set aan data moet zowel de primaire- als secundaire kopie kunnen zijn.

2.4 Back-up strategie

Opdrachtgever onderscheidt de volgende back-up strategie:

- Er moet minimaal aan de 3-2-1-1-0 norm voldaan worden. De 3-2-1-1-0 back-up strategie bestaat uit de volgende elementen:
 - **Ten minste 3 kopieën van gegevens:** Het hebben van ten minste 3 kopieën van gegevens, waarvan één de primaire kopie is en twee extra kopieën zijn, zorgt voor redundantie en minimaliseert de kans op gegevensverlies.
 - **Opslaan van kopieën op ten minste 2 verschillende media:** Door de gegevens op ten minste twee verschillende media op te slaan, zoals harde schijven, tapes of cloudopslag, wordt het risico van gegevensverlies als gevolg van een storing in één medium geminimaliseerd.
 - **Ten minste 1 kopie van de gegevens moet extern worden opgeslagen:** Het extern opslaan van ten minste één kopie van de gegevens, bijvoorbeeld op een offsite server of in een cloudopslag, zorgt voor extra bescherming tegen gegevensverlies door diefstal, brand of overstroming.
 - **Ten minste 1 kopie van de gegevens moet immutable worden opgeslagen:** Het opslaan van ten minste één kopie van de gegevens, die de gegevens beschermt tegen ransomware en andere kwaadaardige software die het netwerk kan infecteren.
 - **0 fouten in de back-up- en herstelprocessen:** Het uitvoeren van regelmatige testen om ervoor te zorgen dat de back-up- en herstelprocessen correct werken, is essentieel om de gegevensveiligheid te garanderen en eventuele problemen snel op te lossen.
- Waar mogelijk dient het incremental forever principe gehanteerd te worden. Denk hierbij, maar niet uitsluitend, aan:
 - Virtual Machines (VMware, KVM, Hyper-V)
 - Microsoft 365 (Exchange Online, Teams, OneDrive en SharePoint)
 - Kubernetes
- Bij een incremental forever back-up moet er op (nader te definiëren) reguliere basis een synthetic full gemaakt kunnen worden.
- Databases en (Azure) Active Directory zullen op (nader te definiëren) reguliere basis een Full back-up nodig hebben, en zijn derhalve uitgesloten van bovenstaande.
- Er dienen op reguliere basis automatisch health checks uitgevoerd te worden op de Incremental back-ups en back-up chains.

2.5 Restore

Opdrachtgever stelt de volgende eisen t.a.v. restore:

- Item level restore moet vanaf zowel primaire- als secundaire storage mogelijk zijn.
- Item level restore vanaf long term retention storage is een pré.
- Item level restore moet voor de volgende archetypes in ieder geval mogelijk zijn:
 - Exchange (on-prem en Online)
 - Fileservers
 - SharePoint Online
 - Teams
 - OneDrive
 - Database servers (MS SQL, PostgreSQL, Oracle, MariaD, enz).
- Restores moeten zowel in-place als out-of-place mogelijk zijn. Dit geldt voor zowel full restore als Item level restore.
- Item level Out-of-place restore moet zowel on-prem als in de Cloud mogelijk zijn. Ongeacht de bron van de data.

- Een full restore moet bij elke archetype mogelijk zijn.
- Bij restore van een fysieke of virtuele server kan, na een basis installatie van het OS, de system state vanuit de back-up hersteld worden (bare metal restore).
- De oplossing kan cross hypervisor herstellen zonder dat de beheerder een conversie hoeft uit te voeren.
- Er is altijd herstel mogelijk vanuit de back-up data. Ook in de toekomst als de licentie / support is verlopen. Daarbij is ook geen afhankelijkheid van connectiviteit.

2.6 Hypervisor (virtualization)

De volgende Hypervisors dienen minimaal te worden ondersteund:

- VMware vSphere;
- Microsoft Hyper-V;
- Oracle KVM;
- Azure IaaS.

2.7 Archetypes

De volgende archetypes dienen minimaal te worden ondersteund

- VMware Virtual Machine;
- Oracle KVM virtual machine;
- Microsoft Hyper-V virtual machine;
- Oracle Database;
- SQL database;
- PostgreSQL database;
- MySQL database;
- MariaDB database;
- Microsoft Exchange database (On-prem);
- Microsoft Exchange mailbox (on-prem en Exchange Online);
- Microsoft Active Directory;
- Microsoft Entra:
- Microsoft 365:
 - Sharepoint Online
 - OneDrive for Business
 - Teams
 - Exchange Online
- Paas / IaaS bij diverse cloud providers;
- Kubernetes.

2.8 Retentie

Standaard retentie

Voor de standaard retentie gelden de volgende eisen (deze zijn ook verwoord in het PvE, zie Bijlage 4):

- De retentie moet per archetype instelbaar zijn.
- Binnen een archetype moet de retentie kunnen verschillen op basis van classificatie
- De retentie moet per kopie (primair/ secundair) instelbaar zijn.
- Als de retentie is verlopen moet de betreffende data automatisch en onherroepelijk worden verwijderd/ ontoegankelijk gemaakt.

- Het moet mogelijk zijn de retentie van een specifieke set aan data te verlengen. Denk hierbij bijvoorbeeld, maar niet uitsluitend, aan een scenario waarbij een lopend WOO-verzoek waarbij de benodigde data grenst aan de retentie periode.

Lange termijn retentie

Voor lange termijn retentie storage wordt er gedacht aan de volgende oplossingen:

- Tape;
- Archief storage in de cloud;
- Lokale storage (On-premise storage).

Idealiter zou een combinatie van Tape en Archief storage in de Cloud de mooiste oplossing zijn.

2.9 Managementserver

Met managementserver wordt de server bedoelt die de aansturing van de back-up oplossing regelt (core component).

Er worden de volgende eisen gesteld aan de managementserver:

- De managementserver draait primair alleen on-prem. Het moet echter wel mogelijk zijn om de managementserver in de cloud eenvoudig op te spinnen om het disaster & recovery proces op te starten.
- Vanaf het moment dat een virtuele server beschikbaar is moet de managementserver binnen 2 uur op te spinnen zijn.
- De managementserver dient on-prem in 2 uur hersteld te kunnen worden.
- De configuratie van de managementserver moet minimaal 1 keer per uur veilig worden gesteld.
- Dit veilig stellen dient op een dusdanige manier gedaan te worden dat er, bij uitval van de managementserver (om welke reden dan ook), gemakkelijk een nieuwe managementserver in de lucht kan worden gebracht.
- De managementserver mag zowel hardware matig, softwarematig (VM) als Cloud based zijn.
- Bij verlies van de back-up oplossing door een aanval (maar geen verlies van de immutable back-up data) kan er eenvoudig herstel plaatsvinden vanuit deze back-up data.
- Er hoeft niet eerst een complexe infrastructuur opgetuigd te worden voordat er hersteld kan worden vanuit de back-up. Denk bijvoorbeeld aan het beschikbaar zijn van de back-up metadata of de-duplicatie databases.

2.10 Hardware

Benodigde on-premise hardware wordt ingericht op basis van Referentie architectuur, appliances voor managementserver rol is niet gewenst.

2.11 Cloud

De gangbare cloud providers dienen minimaal, maar niet beperkt tot, ondersteund te worden:

- Microsoft Azure.
- AWS.
- Google cloud.
- Oracle cloud.

3. Security

3.1 Validatie te herstellen data uit de back-up

Opdrachtgever stelt de volgende eisen t.a.v. validatie van te herstellen data:

- Herstel van data uit de back-up moet pro-actief geverifieerd kunnen worden door middel van recovery in een afgeschermd omgeving. Dit pro-actieve herstel mag nooit de data in productie hinderen.
- Tijdens dit pro-actieve herstel wordt er gecontroleerd of de herstelde data nog vrij is van indicatoren van besmetting (ransomware en andere bekende virussen).

3.2 Ransomware protection

De opdrachtgever stelt het volgende t.a.v. ransomware beveiliging:

- De back-up oplossing dient een mechanisme te bezitten die verdachte activiteiten en bestanden pro-actief detecteert.
- Bij detectie van verdachte activiteiten en/ of bestanden worden notificaties verstuurd. Denk hierbij aan notificatie via E-mail naar beheerders maar ook aan registratie in een syslog server (SOC/ SIEM).

3.3 Compliancy

Aan de volgende compliancy dient voldaan te worden:

- Voor Opdrachtgever is het toepassen van normeringen momenteel aan de orde van de dag. Denk hierbij aan CIS hardening guidelines en BIO richtlijnen.
- Inmiddels is uitgesproken dat nieuwe oplossingen moeten voldoen aan BIOv2, NIS2 (Cbw), en ISO27001.