



Gemeente Haarlem

Vernieuwing back-up/ disaster & recovery

Beschrijving Proof of Concept

18-04-2025

Versie: 1.0

Kenmerk: 2025/0426831

Inhoudsopgave

INHOUDSOPGAVE.....2

1. INLEIDING3

2. PROOF OF CONCEPT4

1. Inleiding

In 2025 verlopen de contracten van de hard- en software van de huidige back-up en disaster en recovery oplossing 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.

Het doel van de Proof of Concept (PoC) is om tijdens de verificatiefase te controleren of de oplossing voldoet aan de in onderhavig document beschreven functionaliteit/eisen (een subset van de eisen uit Bijlage 4 Programma van Eisen).

Om zo enerzijds de Opdrachtnemer in de gelegenheid te stellen om aan te tonen dat wat in dit document beschreven is werkt conform de eisen, en anderzijds de Opdrachtgever de gelegenheid te geven om deze eisen in een test omgeving zelf te verifiëren.

Indien uit de PoC blijkt dat aan een of meerdere eisen niet wordt voldaan, dan zal de Inschrijving terzijde worden gelegd en zal de PoC plaatsvinden met de eerstvolgende Inschrijver in rangorde.

Over dit document

Dit document beschrijft in het kort de PoC en welke eisen minimaal in deze PoC aan de orde moeten komen.

2. Proof of Concept

Aanpak Proof of Concept

Opdrachtgever laat het aan de Opdrachtnemer over hoe zij de PoC wil inrichten. Vanuit Opdrachtgever zijn er wel 2 eisen:

1. Opdrachtnemer toont in een of meerdere sessies de werking van onderstaande functionele en non-functionele eisen in een omgeving aan.
2. Opdrachtgever krijgt vervolgens een 2-tal weken de tijd om zelf deze functionele en non-functionele eisen in deze omgeving te testen.

Aan te tonen functionaliteit/eisen

Deze tabel beschrijft een subset van functionele en non-functionele eisen uit het Programma van Eisen (Bijlage 4), die Opdrachtgever in de PoC in ieder geval wil verifiëren.

Eis	Omschrijving	Onderdeel PoC
Retentie		
1	De retentie moet per archetype instelbaar zijn	X
2	Binnen een archetype moet de retentie kunnen verschillen op basis van classificatie	X
3	Als de retentie is verlopen moet de betreffende data automatisch en onherroepelijk worden verwijderd/ ontoegankelijk gemaakt	X
4	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 waar de benodigde data grenst aan de retentie periode	X
5	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	X
Back-up strategie		
6	Waar mogelijk het incremental forever principe hanteren. Denk hierbij, maar niet uitsluitend, aan: • Virtual Machines (VMware, KVM, Hyper-V) • Microsoft 365 (Exchange Online, Teams, OneDrive en SharePoint) • Kubernetes	X
7	Databases, Active Directory en EntraID zullen op regelmatige basis een Full back-up nodig hebben en zijn derhalve uitgesloten van bovenstaande	X
8	Bij een incremental forever back-up moet er op reguliere basis een synthetic full gemaakt kunnen worden	X
9	Er dienen op reguliere basis automatisch health checks uitgevoerd te worden op de Incremental back-ups en back-up chains	X

Eis	Omschrijving	Onderdeel PoC
Restore		
10	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, MariaDB enz.	X
11	Restores moeten zowel in-place als out-of-place mogelijk zijn. Dit geldt voor zowel full restore als item level restore.	X
12	De oplossing kan cross platform restoren zonder dat de beheerder een conversie hoeft uit te voeren	X
13	Een Full restore moet bij elke archteype mogelijk zijn	X
Archetypes		
14	De volgende archetypes dienen minimaal te worden ondersteund • VMware Virtual Machine; • Software Defined configuraties, inclusief koppelingen met objecten. • 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; • Entra ID; • Microsoft 365: ○ Sharepoint Online ○ OneDrive for Business ○ Teams ○ Exchange Online • Paas / IaaS bij diverse cloud providers; • Kubernetes.	In PoC: • Software Defined configuratie • EntraID • Kubernetes
Herstel validatie data in back-up		
15	Herstel van data uit de back-up moet proactief geverifieerd kunnen worden door middel van recovery in een afgeschermd omgeving. Deze proactieve herstel mag nooit de data in productie hinderen	X

Eis	Omschrijving	Onderdeel PoC
16	Tijdens dit proactieve herstel wordt er gecontroleerd of de herstelde data nog vrij is van indicatoren van besmetting. (Ransomware en andere bekende virussen).	X
Ransomware protection		
17	De back-up oplossing dient een mechanisme te bezitten die (near real-time) verdachte activiteiten en bestanden kan detecteren (thread detection).	X
18	Bij detectie van verdachte activiteiten en / of bestanden worden er notificaties verstuurd. Denk hierbij aan notificatie via E-mail naar beheerders maar ook aan registratie in een syslog server (SOC/ SIEM).	X
Management server		
Met managementserver wordt de server bedoelt die de aansturing van de back-up oplossing regelt (core component)		
19	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	X
Beveiligingseisen		
20	De oplossing moet volgens het 4 ogen principe werken bij het verwijderen of aanpassen van configuratie gegevens.	X
21	Het systeem heeft mogelijkheden extra MFA af te dwingen.	X
22	De autorisaties dienen rol gebaseerde autorisaties te zijn. De autorisaties kunnen per gebruikersrol, per groep, per team en per medewerker ingericht worden. Er dient verschil te worden gemaakt tussen creëren, raadplegen, wijzigen en verwijderen.	X
23	Verificatie dat de verbindingen en versleuteling (encryptie) voldoen aan de gevraagde standaarden.	X