

Algemeen overzicht van de huidige situatie kavel C cloud platform

Inleiding

Het huidige ICT-landschap van de provincie Noord-Brabant is sterk onderhevig aan veranderingen. Veranderingen die ook voortgaan tijdens de uitvoering van deze aanbesteding. Waarmee we willen aangeven dat de beschrijving van de huidige situatie een momentopname is. We schetsen zo veel als mogelijk het beeld op het moment van gunning. Het is niet uit te sluiten dat er wijzigingen plaatsvinden tussen het moment van aanbesteden en het sluiten van de overeenkomst met de gegunde partij. Het is aan de gegunde partij om een due diligence op de gegevens uit te voeren voordat de opdracht wordt gestart.

Het verandertraject waarin de provincie zich bevindt komt niet alleen voort uit het uitbesteden van diensten, maar ook uit het uitvoeren van onder andere de PNB Cloud Strategie met een impact op applicaties, de digitale werkplekken, dataopslag en daarmee natuurlijk op de digitale infrastructuur.

Het team (dat zich bezighoudt met Azure platform en netwerk)

PNB voert regie over haar cloudomgeving, waarbij de uitvoering van technische handelingen momenteel bij OGD ligt. Binnen PNB zijn de volgende teams/afdelingen betrokken:

1. Competence Center (CC)
 - Domain architect – Werkplek
 - Domain architect – Backup/Restore
 - Domain architect – Cloud en Infrastructure
 - Domain architect – Netwerk
 - Cloud Cost Analyst
2. OGD
 - Klantenteam PNB
 - Team Netwerk
 - Team Cloud Infra

ICT-(gebruikers)omgeving

Assets	Geschat aantal
Actieve (gebruikers-) accounts	2100
Beheerde laptops	1470
Actieve virtuele desktops (AVD)	300
Fysieke PC's op locatie (FAT client)	5
Beheerde smartphones o.b.v. MAM	1350

Buiten de beheerde werkplekken/laptops, maakt een grote populatie gebruik van voor de provincie niet vertrouwde apparatuur waarmee wordt ingelogd op bijvoorbeeld Microsoft 365. Dit moet in de nabije toekomst worden ondervangen door de inzet van onder andere Azure Virtual Desktop.

Behalve de huidige FAT-clients en servers op locatie Den Bosch bevinden laptops en andere apparaten van gebruikers zich niet op het LAN.

Provincie Noord-Brabant werkt met Microsoft 365 waarbij alle gebruikersaccounts over een E5-licentie beschikken.

Azure Platform

De Azure platform dienst en application landing zones zijn ingericht via de huidige ICT dienstverlener, OGD. In totaal zijn er 32 subscriptions verdeeld als volgt:

3. Azure Platform: 5
4. Persoonlijk: 3
5. Stuurinformatie en administratie (SIA): 4
6. Geo & Data: 6
7. Datalab: 1
8. Mobiliteit: 3
9. Dienstverlening ICT (DVI): 10

De omvang en type resources in de verschillende subscriptions zijn erg uiteenlopend. Van IaaS componenten (vm's, disks, enz) tot data pipelines en AI. Hierbij een overzicht van de meest voorkomende resources:

Type	Hoeveelheid
Network Interface	365
Disk	354
Virtual machine	179
Private endpoint	171
Storage account	122
Private DNS zone	110
Network security group	70
IP Group	63
Function App	59
Data collection rule	50
Log Analytics workspace	45
Managed Identity	40
Availability set	33
Machine - Azure Arc	29
Virtual network	29
SQL database	28
SQL Server database - Azure Arc	28
Key vault	27
Maintenance Configuration	19
Shared dashboard	18
SQL server	18
Azure Workbook	14
Disk Encryption Set	14
Recovery Services vault	14

Azure netwerk

PNB kent een uitgebreid Azure netwerk als onderdeel van haar communicatie van en naar de verschillende workloads

De diensten in de PNB Azure Cloud zijn gebaseerd op een hub-spoke architectuur. Het netwerk bestaat uit één VWAN met één secure hub. Hieraan zijn 29 VNets verbonden, waarvan 1 van een vertrouwde partner.

Er zijn 2 ExpressRoute circuits verbonden aan de VWAN voor verbinding naar on-premises locaties. Verder zijn er 2 Site-to-Site VPN's naar partners waarvan 1 actief is. Op dit moment zijn er geen Client-to-Site VPN's actief. Dit kan in de toekomst veranderen.

Alle communicatie naar Internet (egress) en onderling tussen on-premises en Azure verlopen via één Azure Firewall. Voor communicatie vanuit Internet naar PNB voor portaalfunctionaliteit of andere interfaces (ingress) wordt gebruik gemaakt van een Azure Application Gateway v2.

DNS wordt door meerdere componenten waaronder Private DNS Zones, een DNS caching service en interne DNS verzorgd door Active Directory Domain Controllers.

Datacenter Den Bosch

De datacenter in Den Bosch wordt ingezet voor vooral applicatie hosting en traditionele infrastructuur componenten. Het bestaat uit het volgende:

Hardware:

- 4 x Dell PowerEdge servers (applicatie hosting/infra diensten)
- 2 x Dell PowerEdge servers (DMZ)
- 1 x Hitachi SAN

Hypervisor:

- VMware ESXi v7

Virtuele guests:

- 171 x Windows Server
- 21 x Linux Server (meerdere distro's)

Rakende/aanpalende kavels

Security Operations Center (SOC):

De SOC-dienst maakt primair gebruik van Sentinel als SIEM. Hierdoor hebben ze toegang tot de omgeving via Azure Lighthouse.

Werkplek:

De werkplek dienst maakt gebruik van Azure Virtual Desktop. Deze wordt gezien binnen PNB Azure Cloud als een specifieke cloud workload.

Netwerk:

De aansluiting naar on-premises locaties verloopt momenteel via de genoemde ExpressRoute verbindingen. Er is echter een afhankelijkheid met fysieke *point-of-presence* (POP) in Equinix Amsterdam.

Identity Access

Authenticatie en autorisatie binnen PNB Azure Cloud verloopt via Entra ID. Hiervoor worden per subscription groepen en rollen gedefinieerd in Entra Privileged Identity Management (PIM). Eigenaarschap en toekenning van de rollen, alsook periodieke controle, wordt afgehandeld door de business eigenaar of een gedelegeerde.

Beheer en onderhoud

Met OGD is een beheer- en onderhoudsovereenkomst overeengekomen voor de scope van kavel C die loopt tot uiterlijk 30 november 2025.

Microsoft Unified Support

Ten tijde van opstellen van dit document wordt door PNB gebruik gemaakt van Unified Support bij Microsoft (looptijd tot eind april 2025). PNB heeft vooralsnog de focus op een degelijke invulling van support door Microsoft. Het totaal aantal ingeleide tickets bij Microsoft bedraagt ca. 50 stuks per jaar.

Ons Loket (onsite support en servicedesk ICT en facilitair)

Ons Loket is opgericht vanuit de behoefte aan een centraal aanspreekpunt waar gebruikers terecht kunnen met al hun vragen. Om dit mogelijk te maken zijn de disciplines ICT, Facilitair en het Brabant Loket (klantcontactcentrum) samengebracht in één geïntegreerd loket. Daarnaast fungeert Ons Loket ook als het frontoffice voor de financiële administratie en subsidieaanvragen. Binnen Ons Loket wordt gewerkt als één team, waarin iedere discipline vanuit zijn eigen expertise bijdraagt aan een gastvriendelijke en klantgerichte dienstverlening.

Ons Loket werkt volgens het Click, Call, Face-principe. Dit houdt in dat gebruikers ons kunnen bereiken via:

1. Click: Een Selfservice Management Tool (SMT).
2. Call: Telefonisch contact.
3. Face: Een fysiek bezoek aan de balie.

Via deze kanalen worden meldingen geregistreerd, worden waar mogelijk direct problemen opgelost en worden meldingen overgedragen die verdere specialistische aandacht vereisen van de juiste vakgroep die in diverse programma's werken.

De resultaten van Ons Loket laten zien dat de eerste lijn een grote rol speelt in het oplossen van gebruikersvragen of verstoringen:

- Aantal meldingen afgemeld door de eerste lijn in 2023: 11.118
- Aantal meldingen afgemeld door de eerste lijn in 2024: 10.399
 - 55% zijn service requests
 - 45% zijn incidenten

Naast eerstelijns servicedesk ondersteuning biedt Ons Loket ook aanvullende diensten waaronder userbeheer, telecombeheer, eenvoudige fysiek werkplekbeheer, voorbereiden en uitleveren van hardware.

Ons Loket bestaat uit 18 medewerkers:

- 1 opdrachtnemer
- 2 procescoördinatoren (1 gericht op Facilitair en 1 op ICT)
- 8 ICT-medewerkers
- 7 Facilitair medewerkers

Momenteel wordt gebruik gemaakt van Facilitator als SMT-tool. Er loopt een aanbestedingstraject voor aanschaf, implementatie en onderhoud van een vervangende SMT-tool. Verwacht wordt dat die in de 1^e helft van 2025 wordt geïmplementeerd.

Daarnaast wordt gewerkt met callcentersoftware Cloudoe. Voor de ICT-omgeving maakt Ons Loket gebruik van Intune, Azure, en Active Directory.