PROVINCIE UTRECHT

Globale Architectuur Schets (GAS) Cloud platform dienstverlening

26-6-2025

Finaal

Inhoudsopgave

Inhoudsopgave 2
1 Inleiding 3
2 Principes en randvoorwaarden 4
3 Samenvatting doelarchitectuur ICT-fundament 7
4 Cloud services 9
5 Datacenter services 13
6 Netwerk services 15
7 Werkplek services 18
8 Samenwerking services (O365) 23
9 Identiteit- en toegangsbeheer services 26
10 Informatiebeveiliging services 29
11 Applicatie services 32
Bijlage 1: IaaS-applicaties 35

1 Inleiding

1.1 Doel

Deze Globale Architectuur Schets (GAS) beschrijft de ICT-services en -bouwstenen voor de Cloud platform dienstverlening op hoofdlijnen vanuit het perspectief van de Aanbestedende dienst. Zodat deze door Inschrijver kunnen worden vertaald naar een Plan van Aanpak met de te realiseren werkpakketten met afhankelijkheden, prioritering en planning.

1.2 Scope

In deze GAS is het globaal ontwerp uitgewerkt van Laag 5 ICT-Infrastructuurlaag volgens de Provinciale Enterprise Referentie Architectuur (PETRA):

- Laag 1: Grondslagenlaag
- Laag 2: Organisatorische laag
- Laag 3: Informatielaag
- Laag 4: Applicatielaag
- Laag 5: ICT-Infrastructuurlaag

De architectuur van de ICT-infrastructuurlaag bestaat uit een aantal IT-services welke worden geleverd door ICT bouwstenen (BS). Een ICT-bouwsteen is gedefinieerd in NORA als: "*Voorziening die deel uitmaakt van de infrastructuur van de e-overheid.*"

#	ICT-services
8	Applicaties
7	Informatiebeveiliging
6	Identiteit & Toegangsmanagement
5	Samenwerking
4	Werkplek
3	Netwerk
2	Datacenter
1	Cloud

De ICT-infrastructuur voor gegevensopslag (registraties, databases e.d.) of voor gegevensverwerking (Applicaties, software, data services e.d.) valt niet onder de ICT-infrastructuur, maar onder de Applicatieslaag. Alhoewel in deze GAS de focus ligt op de technische infrastructuur is er een afhankelijkheid met de applicatiearchitectuur. Vandaar dat de impact op Applicaties ook is meegenomen in dit document als ICT-services laag 8.

2 Principes en randvoorwaarden

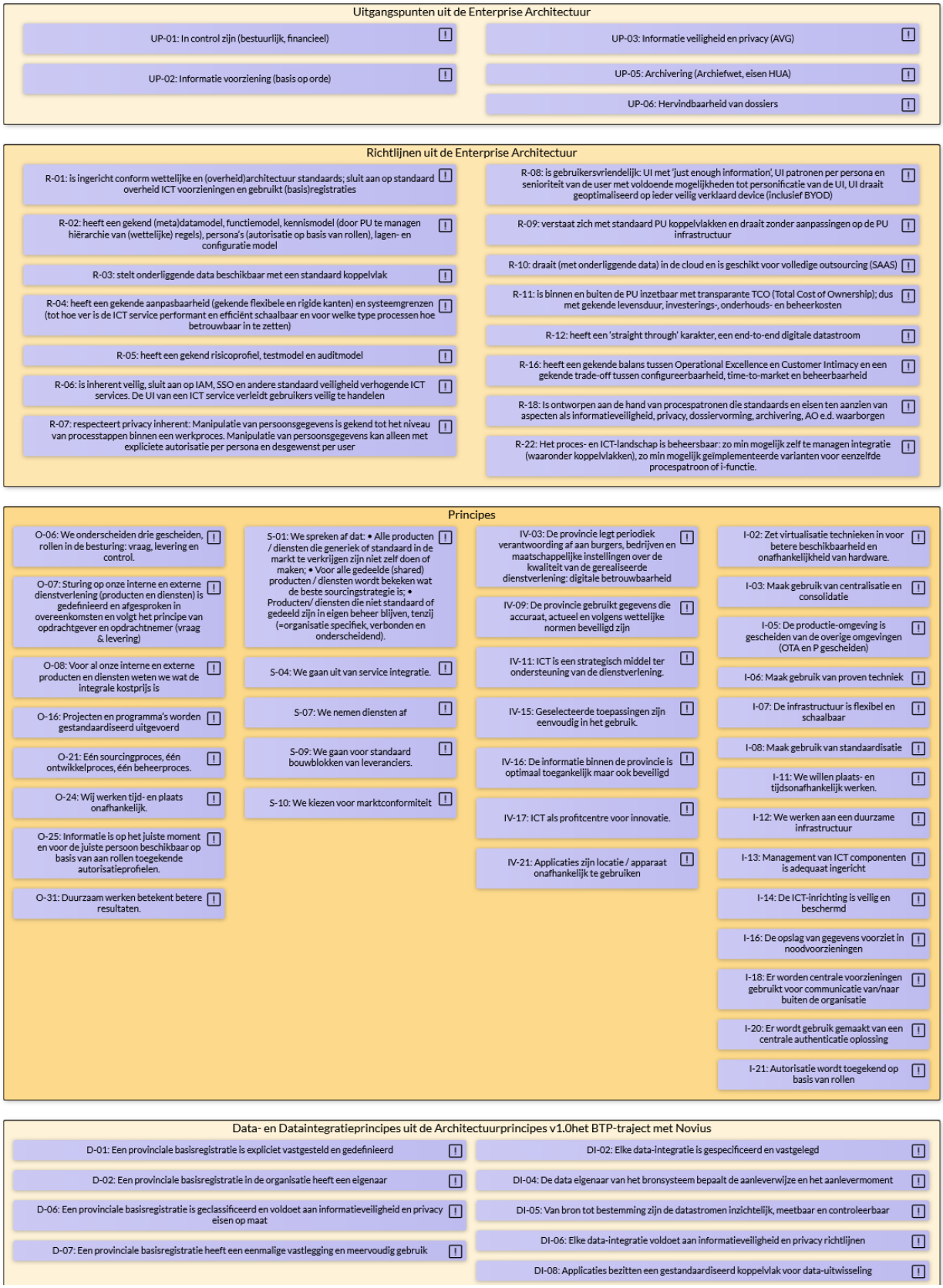
2.1 Uitgangspunten en architectuurkaders

De belangrijkste uitgangspunten die van toepassing zijn op het eindresultaat van deze GAS:

- Uitgangspunt 1: Cloud first;
- Uitgangspunt 2: Azure tenzij;
- Uitgangspunt 3: Zero-trust; never trust, always verify;
- Uitgangspunt 4: SaaS voor PaaS voor IaaS oplossingen.

De belangrijkste architectuurkaders uit de enterprise architectuur welke van toepassing zijn:

- Kader R-06: is inherent veilig, sluit aan op IAM, SSO en andere standaard veiligheid verhogende IT-services. De UI van een IT-service verleidt gebruikers veilig te handelen;
- Kader R-08: is gebruikersvriendelijk: UI met 'just enough information', UI patronen per persona en senioriteit van de user met voldoende mogelijkheden tot personificatie van de UI, UI draait geoptimaliseerd op ieder veilig verklaard device (inclusief BYOD);
- Kader R-09: verstaat zich met standaard Aanbestedende dienst koppelvlakken en draait zonder aanpassingen op de Aanbestedende dienst infrastructuur;
- Kader R-10: draait (met onderliggende data) in de Cloud en is geschikt voor volledige outsourcing (SaaS);
- Kader R-11: is binnen en buiten de Aanbestedende dienst inzetbaar met transparante TCO (Total Cost of Ownership); dus met gekende levensduur, investerings-, onderhouds- en beheerkosten;
- Kader R-22: Het proces- en ICT-landschap is beheersbaar en beheerbaar: zo min mogelijk zelf te managen integratie (waaronder koppelvlakken), zo min mogelijk geïmplementeerde varianten voor eenzelfde procespatroon of i-functie;
- Kader S-04: We gaan uit van service integratie;
- Kader S-07: We nemen diensten af;
- Kader S-09: We gaan voor standaard bouwblokken van leveranciers;
- Kader S-11: We kiezen voor marktconformiteit;
- Kader O-24: We gaan plaats en tijd onafhankelijk werken;
- Kader O-25: Informatie is op het juiste moment en voor de juiste persoon beschikbaar op basis van aan rollen toegekende autorisatieprofielen.



Figuur 1 - Architectuurkaders Toekomstig ICT-fundament 2025

2.2 Randvoorwaarden

Vanuit de Cloud first en Azure tenzij uitgangspunten, richt de Aanbestedende dienst zich op het afnemen van IT-services die bij voorkeur geleverd worden vanuit één geïntegreerd ecosysteem. In een dergelijk ecosysteem zijn IT-services naadloos integreerbaar, wordt het beheer vereenvoudigd, is de gebruikerservaring consistenter, en kan informatieveiligheid beter worden ingericht. Momenteel kunnen dergelijke ecosystemen, als gevolg van de forse jarenlange investeringen in infrastructuur en clouddienstverlening, enkel door Amerikaanse providers (hyperscalers) worden geleverd[1].

De Aanbestedende dienst is zich op het moment van schrijven bewust van de geopolitieke spanningen de verhoogde aandacht voor het gebruik van Amerikaanse cloud leveranciers binnen de Europese en Nederlandse overheid. Binnen Europa wordt gewerkt aan de ontwikkeling van volwaardige alternatieven. Het inhalen van deze achterstand vereist vele jaren van grote investeringen en vraagt om 'een lange adem en diepe zakken' [2].

Totdat Europese of Nederlandse cloud leveranciers een gelijkwaardig niveau van dienstverlening kunnen bieden, blijft de Aanbestedende dienst genoodzaakt gebruik te maken van Amerikaanse cloud leveranciers om de ambities voor de informatievoorziening te realiseren. In de tussentijd zal de Aanbestedende dienst de informatievoorziening zodanig ontwerpen en inrichten dat deze ontkoppelbaar is van een publieke cloud leverancier.

Dit betekent dat de Aanbestedende dienst de volgende randvoorwaarden hanteert:

1. Bij de inkoop van diensten en producten een 'exit-plan' in het contract opneemt. Het exit-plan is onderdeel van de exit-strategie en omvat o.a. complete, actuele en gestructureerde overzichten van alle bij opdrachtnemer beschikbare informatie (hardware, netwerkcomponenten, software, licenties, databases en gegevens, documentatie en facilitaire zaken, contracten en documenten van leveranciers van opdrachtnemer en personeel), zodat een gecontroleerde overdracht mogelijk is bij beëindiging van de samenwerking;
2. Zo zuiver mogelijk gebruik (blijft) maken van gecontracteerde diensten en/of producten, en daarbij maatwerk niet toestaat of tot een absoluut noodzakelijk minimum beperkt;
3. Borgt dat opslag en verwerking van data binnen de dienstverlening altijd binnen de Europese Economische Ruimte (EER) plaatsvindt;
4. Open standaarden toepast en gebruikt, volgens het forum standaardisatie;
5. Waar mogelijk kiest voor 'open source' oplossingen wanneer er binnen de dienstverlening van de leverancier gebruik wordt gemaakt van oplossingen van derden.

Daarnaast volgt de Aanbestedende dienst actief de ontwikkeling van Europese en Nederlandse alternatieven voor clouddiensten. Zodra er een volwaardig alternatief beschikbaar komt, wordt de strategische keuze voor Amerikaanse cloud leveranciers heroverwogen. Hiervoor wordt de architectuur nu al ingericht op maximale interoperabiliteit en portabiliteit.

[1] Eindrapport In het kader van het quickscan-onderzoek naar technische, organisatorische en juridische gaps tussen Europese/Nederlandse cloudproviders en Amerikaanse hyperscalers voor het ministerie van Economische Zaken, KPMG, 16 augustus 2024, A2400031906

[2] Marktstudie Clouddiensten, Autoriteit Consument en Markt Openbaar. 05-09-2022, ACM/INT/440323

3 Samenvatting doelarchitectuur ICT-fundament

Dit hoofdstuk geeft een korte samenvatting van de belangrijkste componenten die worden voorzien in de ICT-services van de Cloud platform dienstverlening voor Aanbestedende dienst. Gezamenlijk gaan deze componenten ervoor zorgdragen dat de gebruikers op een veilige manier productief kunnen zijn. Hiervoor begint dit hoofdstuk met een globale architectuur schets om de belangrijkste raakvlakken van deze componenten weer te geven. Vervolgens wordt er per ICT -service een korte toelichting gegeven. De verdere uitleg van de ICT-bouwstenen staan beschreven in de corresponderende hoofdstukken.

3.1 Benadering Globale architectuur schets (GAS)

De GAS is benaderd vanuit twee verschillende perspectieven:
1. vanuit het perspectief van de werkplek (de gebruiker en diens digitale omgeving), en
2. vanuit het perspectief van de publieke Cloud (de onderliggende infrastructuur en applicatielandschap).

3.1.1 Globale architectuur schets vanuit het perspectief van de werkplek

De globale architectuurschets vanuit het perspectief van de werkplek richt zich op het leveren van een veilige digitale werkplek, waarmee de gebruiker productief kan zijn. Gebruikers kunnen eenvoudig en veilig aanmelden op de digitale werkplek via Windows Hello.

De digitale werkplek architectuur steunt op de volgende uitgangspunten:
- **Zero Trust Access**: toegang is contextueel en voorwaardelijk, met continue validatie van identiteit, apparaatstatus en locatie.
- **Moderne provisioning**: werkplekken worden geautomatiseerd en veilig uitgerold via Windows Autopilot en Intune.
- **Geïntegreerde security**: bescherming van eindpunten, gebruikers en data via Microsoft Defender-integraties.
- **Cloud-native beheer**: beheer en monitoring vinden zoveel mogelijk plaats vanuit de cloud, tenzij zwaarwegende redenen anders vereisen.

3.1.2 Global architectuur schets vanuit het perspectief van de publieke Cloud

De GAS vanuit het perspectief van de publieke Cloud richt zich op de fundamenten van de ICT-infrastructuur en het applicatielandschap. Microsoft Azure wordt als voorkeursplatform gehanteerd voor het hosten van workloads, applicaties en data. Hierbij worden zowel Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) als Software-as-a-Service (SaaS)-diensten toegepast.

De publieke Cloud architectuur steunt op de volgende uitgangspunten:
- **Zero trust**: toegang is voorwaardelijk, met continue validatie van identiteit, apparaatstatus en locatie.
- **Cloud-native first**: bij voorkeur worden SaaS-oplossingen ingezet, boven PaaS-oplossingen, boven de IaaS-oplossingen, om beheerlast te minimaliseren en adoptie van moderne bouwblokken te stimuleren.
- **Security by design**: alle cloudresources worden beveiligd volgens Zero trust en Microsoft-beveiligings-richtlijnen, gebruikmakende van de Microsoft security baseline en Microsoft Sentinel als SIEM-oplossing.
- **Data compliance**: alle cloudcomponenten worden zodanig ingericht dat wordt voldaan aan wet- en regelgeving rondom gegevensbescherming (AVG), inclusief datalokalisatie binnen EU-regio's waar nodig.
- **Hybride integratie**: legacy-applicaties die (nog) niet geschikt zijn voor migratie, worden via Azure Arc geïntegreerd in de cloudarchitectuur en bewaakt binnen het centrale monitoring en securitymodel.

3.2 Samenvatting gewenste situatie

Onderstaande tabel beschrijft op hoofdlijnen de gewenste situatie.

#	It-service	Toelichting
8	**Applicaties**	Applicaties worden zoveel mogelijk gemigreerd naar SaaS of Azure waaronder het GIS-platform via AVD. Microsoft Fabric wordt het centrale dataplatform en integratie verloopt via een hybride model met Easy Bus en Azure API Management.
7	**Informatie-beveiliging**	Informatiebeveiliging is gebaseerd op zero trust en Microsoft Cybersecurity referentie architectuur, met inzet van de volledige Microsoft Defender XDR-suite, Sentinel als SIEM, en ondersteuning door een extern 24/7 SOC.
6	**Toegangs-management**	Entra ID wordt de primaire identity provider, met automatisering van identiteiten vanuit HR naar zowel Active Directory als Entra ID en inzet van Conditional Access, PIM en lifecyclebeheer voor schaalbare, veilige en toekomstbestendige toegang.
5	**Samenwerking**	Samenwerking via Microsoft 365 wordt versterkt met Microsoft Purview voor dataclassificatie (handmatig), datalekbeveiliging (DLP), retentiebeleid, compliancebeheer en eDiscovery. Er wordt toegewerkt naar E5-licenties vanaf 2027 voor meer informatiebescherming en geavanceerde compliancefuncties.
4	**Werkplek**	De digitale werkplek wordt centraal beheerd via Intune, met automatische uitrol via AutoPilot, streng toegangsbeheer, Global Secure Access VPN en cloud gebaseerd print- en scan. AVD wordt ingezet voor externe en specialistische werkplekken.
3	**Netwerk**	Het netwerk wordt getransformeerd naar een decentraal, cloudgericht ontwerp met lokale internet break-outs, vWAN-integratie in Azure, en centrale netwerkdiensten gemigreerd naar de cloud.
2	**Datacenter**	De fysieke datacenters worden uitgefaseerd; een optionele private cloud blijft mogelijk voor specifieke toepassingen. Deze wordt geïntegreerd met Azure via ExpressRoute en Azure Arc voor uniform beheer en compliance.
1	**Cloud**	De bestaande cloudomgeving wordt ingericht volgens het Microsoft Cloud Adoption Framework met Azure als primair platform. Beveiliging, netwerk en beheer worden centraal geregeld via enterprise landing zones en vWAN, ondersteund met SD-WAN en hybride connectiviteit.

De verdere details over de huidige situatie, gewenste situatie en eventuele ontwerpbesluiten zijn beschreven in de volgende hoofdstukken.

4 Cloud services

Dit hoofdstuk beschrijft in meer detail de huidige situatie, verbeterpunten, toekomstige situatie en de verbeterpunten van de *Cloud services*.

4.1 Bouwstenen

De te realiseren ICT-bouwstenen (BS) als onderdeel van de Cloud services zijn:

- BS1.1 Publieke cloud

4.2 Huidige situatie

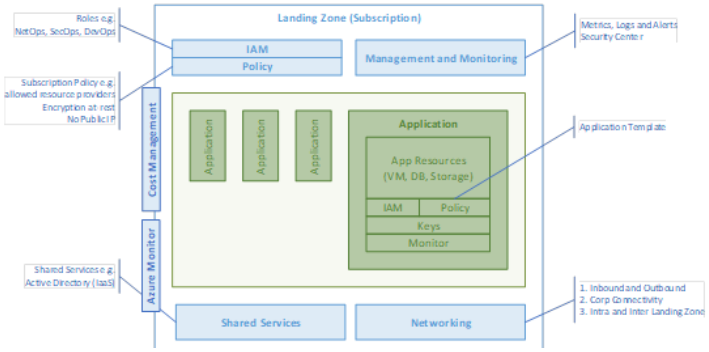
4.2.1 Publieke cloud

De Aanbestedende dienst maakt momenteel gebruik van een pay-as-you-go facturatiemodel voor Azure, met twee aparte tenants: één voor sandbox/playground en één voor productie. Deze scheiding is aangebracht om de ontwikkel- en testomgevingen strikt te isoleren van de productieomgeving, met het oog op verbeterde beveiliging en beheerbaarheid. De Azure-omgeving is primair ingezet voor Entra ID (zie Hoofdstuk 10. Identiteit- en toegangsbeheer) en voor het dataplatform.

In mei 2024 bracht Devoteam advies uit om een nieuw standaard dataplatform te bouwen, gevolgd door een Europese aanbesteding in februari 2025. Devoteam heeft tevens een evaluatie van de bestaande Azure-omgeving uitgevoerd met aanbevelingen voor verbeteringen. In april 2025 heeft InSpark ter voorbereiding op het aansluiten van het nieuwe dataplatform op de Azure-omgeving, een aantal verbeterpunten (deels) opgelost door het inrichten van een initiële 'Platform Foundation' in Azure, met focus op governance via management groups en Azure Policies. Dit zonder directe impact op bestaande workloads. Governance vormt namelijk de basis voor veilige, beheersbare en toekomstbestendige inzet van Azure binnen de Aanbestedende dienst. Binnen deze structuur zijn er drie platform subscripties ingericht met gedeelde resources, welke generiek binnen de Azure omgeving gebruikt worden:

- **Identity Subscription**: voor identiteiten gerelateerde sources, zoals domain controllers en Entra connect synchronisatie;
- **Management Subscription**: voor alle management gerelateerde componenten, zoals update management, Azure Security Center, Azure monitor en logging;
- **Connectivity Subscription**: voor alle centrale netwerk gerelateerde componenten, zoals Azure Firewall en Express Route.

Nieuwe workloads landen in zogeheten landingzones (subscription) voor productie en non-productie (Dev/Test). Deze zones worden bij onboarding automatisch geconfigureerd met standaardcomponenten (blauw) in figuur 2 en specifieke applicatie-instellingen (groen), volledig in lijn met het gewenste beleid. Ze vallen automatisch onder de juiste beleidsregels, zoals RBAC, tagging, locatiebeperkingen of kostenbeheersing.



Figuur 2 Foundation en Application landingzone

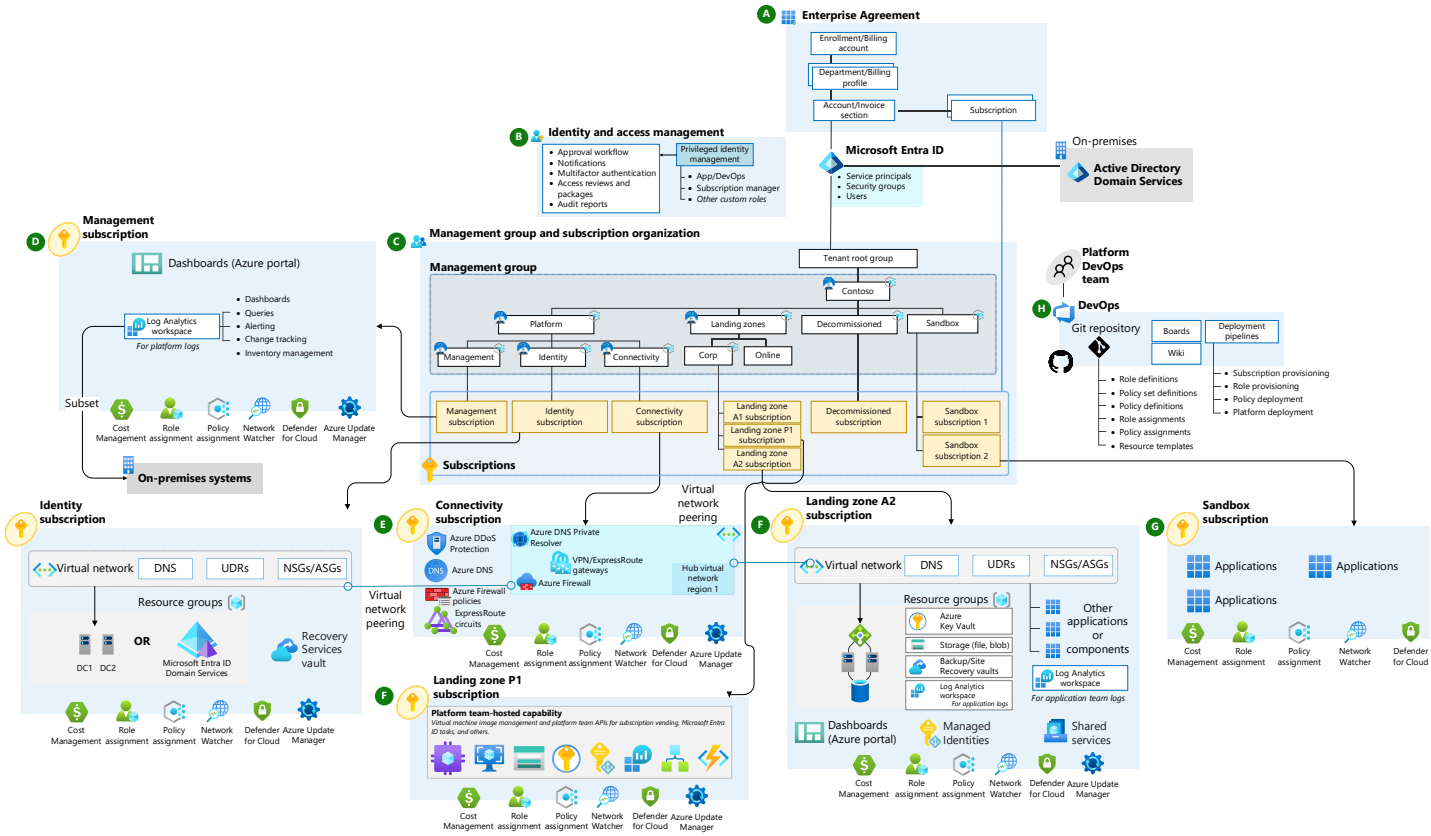
Er zal een afweging gemaakt moeten worden wanneer er een nieuwe landingzone aangemaakt wordt of wanneer een workload bijgeplaatst wordt op een bestaande landingzone. Voor bestaande subscriptions geldt dat ze wel onder de scope van het beleid vallen, maar dat de policies in eerste instantie niet afdwingend zijn ingesteld.

4.3 Gewenste situatie

4.3.1 BS1.1 Publieke cloud

Microsoft Azure met IaaS en PaaS-oplossingen is het primaire cloud platform voor alle IaaS en PaaS-workloads. Als er geen SaaS-toepassing voorhanden is en er goede redenen zijn om de publieke cloud niet te gebruiken, zoals bijvoorbeeld vanwege wetgeving of technische beperkingen, worden workloads in de private cloud omgeving binnen het datacenter geplaatst (zie Hoofdstuk 5. Datacenter services).

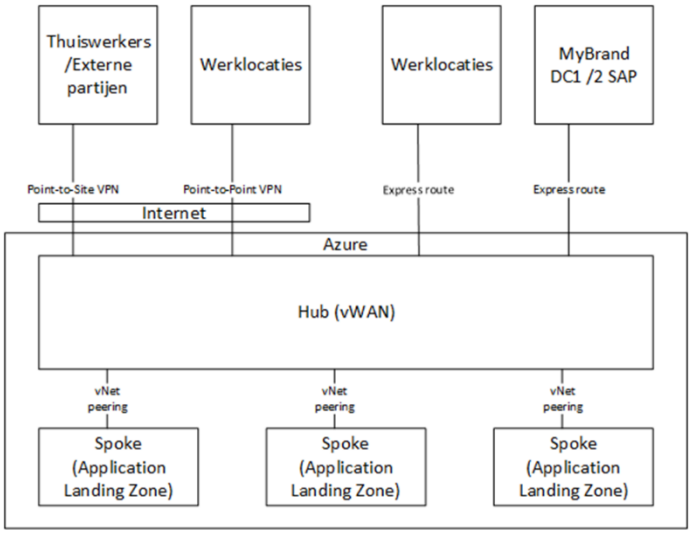
Het doel is om in Azure een gestandaardiseerde, veilige en schaalbare basis te creëren waarop workloads kunnen worden geïmplementeerd. De inrichting van Azure volgt het Microsoft Azure Cloud Adoption Framework (CAF), aangevuld met Enterprise-scale best practices. Zie de conceptuele architectuur voor Azure landing zones in Figuur 3, met de relaties tussen de acht ontwerpgebieden: Overeenkomst, facturering en Entra-tenant (A), identiteits- en toegangsbeheer (B), organisatie van beheergroepen en abonnementen (C), beveiliging, beheer, governance (D), netwerktopologie en connectiviteit (E), platform en applicaties landing zones (F), sandbox (G) en platformautomatisering en DevOps (H).



Figuur 3 - Conceptuele architectuur Azure

De resultaten van de Azure Assessment door Inspark met actuele verbeterpunten is opgenomen in Bijlage 17 Azure assessment.

Omdat Azure de transit van het complete WAN-netwerk beheert (Zie Hoofdstuk 6. Netwerkservices), is het uitgangspunt inzet van Azure Virtual WAN (vWAN). Het vWAN wordt uitgebreid met SD-WAN device orchestration, waarbij als Network Virtual Appliance (NVA) de Cisco Meraki vMX oplossing wordt toegevoegd aan vWAN. Figuur 4 toont de vereenvoudigde weergave van de gewenste situatie van het netwerk van Aanbestedende dienst binnen Azure, met weergave van het hub-spoke model en Azure als transit van het netwerk.



Figuur 4 - Azure virtueel netwerk

De vWAN Hub bevindt zich in de Azure connectivity subscription en zorgt voor de centrale connectiviteit. Elke spoke kan één of meerdere Azure Virtual Networks hebben (vNet). Een vNet kan door middel van vNet-peering aan een ander vNet gekoppeld worden, waardoor de mogelijkheid onstaat om vanuit een spoke, via de hub het internet, andere spokes, datacentra en/of on-premise locaties te bereiken. De Azure connectiviteit staat beschreven in Hoofdstuk 6 Netwerk services.

4.4 Ontwerpbesluiten

Entiteit	Toelichting/Omschrijving	Aard van de verandering
Overeenkomst	via BIJ12 en software broker	Kostenoptimalisatie
Tenantstructuur	Gebruik van 1 Entra-tenant als Productie-omgeving en 1 Entra-tenant als OTA-omgeving t.b.v. de synchronisatie met HR-systeem.	Sandbox/playground tenant wordt verwijderden in non-poduction subscription (DevTest) opgenomen
Tenantnaam	Actieve tenant naam: @provincieutrecht.onmicrosoft.com	Centraal management en governance.
Azure-regio	• Primaire: West-Europa • Fail-over: Noord-Europa	Verbeterde beschikbaarheid.
Management subscriptions	3 Platform subscriptions voor generieke resources: identity, management en connectivity	Consistentie in RBAC-toewijzingen, beleidsregels en connectiviteit met aparte facturatie voor generieke resources, geïsoleerd van de overige workloads
Productie subscriptons	Per workload een subscription als uitgangspunt (GIS, SAP etc.) maar afwegen of dit altijd zinvol is, b.v. bij homogene applicatiecategorie	Segmentatie van de workloads met afgebakende verantwoordelijk-heden, duidelijk kostenoverzicht maar tevens beperken beheerslast.

	(kantoorautomatisering) met dezelfde configuratie, kostenallocatie en applicatie-beheerders.	
Application Landing Zone design	Afwegingen maken per applicatie op basis van security, compliance en kosten.	Optimalisatie van applicatiebeheer.
Netwerkknoopunt (transit)	Verplaatsen van fysiek netwerkknoopunt in racks in datacenters PQR naar een virtueel netwerkknooppunt in Azure.	Inzet van Azure vWAN.
IP-Plan	Reserveren van IP-blok voor Azure en het automatiseren van het IP-plan door een IPAM-oplossing te implementeren	Optimalisatie netwerk.
Firewall	De Azure firewall standard is high available en schaalt automatisch en wordt ingezet voor uitgaand internetverkeer vanaf Azure, het netwerkverkeer tussen Landing Zones, van Landing Zones naar on-premise en vice versa.	Verbetering van netwerkbeveiliging.
Netwerksegmentatie	Opdelen van een vNet in subnets en filteren van verkeer met NSG's om het aanvalsoppervlak te verkleinen.	Verbetering van netwerkbeveiliging.
Azure PaaS resources	PaaS resources waar mogelijk benaderen via Private Endpoints voor maximale beveiliging	Verbetering van netwerkbeveiliging.
Beschikbaarheid	Standaard Azure SLA 99,9% exclusief onbeschikbaarheid door gepland onderhoud.	Voldoen aan BIO continuïteit oor applicaties: 99,5%
Update Management	Virtuele machines worden gepatched middels Azure Update Management	Verbetering van operationeel beheer (wordt reeds gebruikt).
Backup	Gebruik van Azure Backup en PaaS- back-up functionaliteit.	Verbetering van databescherming.
Disaster Recovery	Gebruik van Azure Site Recovery voor virtuele machines en PaaS diensten: • RTO: 4 uren • RPO: 24 uren	Verbetering van continuïteit.

5 Datacenter services

Dit hoofdstuk beschrijft in meer detail de huidige situatie, toekomstige situatie en de verbeterpunten van de *Datacenter services*.

5.1 Bouwstenen

De te realiseren ICT-bouwstenen (BS) als onderdeel van de Datacenter services zijn:
- BS2.1 Housing (optie)
- BS2.2 Private Cloud (optie)

5.2 Huidige situatie

5.2.1 Datacenters

De Aanbestedende dienst maakt momenteel gebruik van 5 datacenters:
- PQR redundant datacenter: Nutanix IaaS;
- Provinciehuis dataroom: VMware IaaS met name t.b.v. GIS;
- MyBrand redundant datacenter: levering en beheer van SAP als SaaS-dienst.

Aanbestedende dienst heeft een overeenkomst met PQR voor housing, IaaS-omgeving, technisch beheer en andere diensten die 15 november 2026 afloopt. Housing bestaat uit 2 datacenter locaties met 2 racks t.b.v. netwerkdiensten van de Aanbestedende dienst. Tevens wordt er nog een oude backup-server en appliance van de Aanbestedende dienst gehost voor het behouden van de 7 jaar retentie van de Exchange-archivering. Alle netwerkverbindingen tussen de datacenters (10Gbps t.b.v. uitwijk), het internet en de locaties van de Aanbestedende dienst worden door de Aanbestedende dienst geleverd en beheerd via Eurofiber.

Het grootste deel van de IaaS-omgeving bestaat uit een Nutanix platform met in de beide PQR datacenters 3 Nutanix virtualisatiehosts, voor zowel Windows als Linux VM's. PQR levert en beheert ook een VMWare platform in de dataroom van het provinciehuis. Hierop draait de GIS-omgeving bestaande uit meerdere applicaties en databases (ca. 15 productie-servers), vanwege performance-redenen (minimale latency) apart van Nutanix, en nog beperkt aantal andere applicaties (zie hoofdstuk 12. Applicatie services).

PQR levert in redundante datacenter en dataroom alles, met beheer met of zonder het besturingssysteem (OS):
- Hardware (servers, switches, storage, backup);
- Virtualisatiesoftware, dus Nutanix en Vmware (inclusief replicatie-tooling);
- Linux OS-licenties voor alle VM's (ook voor de 3 fysieke Oracle servers);
- Windows OS-licenties voor alle VM's;
- Antivirus voor de Windows VM's.

Virtuele servers met een Windows of Linux OS met beheer in twee varianten:
- IaaS: het OS wordt gemanaged door Aanbestedende dienst (meestal applicances);
- IaaS+: het OS wordt gemanaged door PQR.

Backup wordt door PQR op basis van Rubrik als dienst geleverd, deze is niet dedicated voor de Aanbestedende dienst.

In onderstaande tabel staat ter indicatie een overzicht met de huidige aantal virtuele en fysieke servers per OS en de hoeveelheid terrabytes dataopslag en backup:

Virtuele servers	*Windows OS*	*Linux OS*	*Tb*
VM klein test en acceptatie	21	10	
VM klein	6	5	

VM middel	31	10	
VM groot	13	4	
Fysieke servers			
Oracle Server		3	
Dataopslag			
Tier 1 High Performance			
Tier 2 Medium Performance			53
Tier 3 Low Performance			
GIS Tier 1 High Performance			13
Back-up			
Back-up			78
Totaal	**71**	**32**	**66**

5.3 Gewenste situatie

5.3.1 Housing BS2.1 Housing (optie)

Op dit moment is de verwachting dat er geen housing voor fysieke apparatuur benodigd is, bijvoorbeeld t.b.v. netwerk, Backup of uitwijk. Omdat de behoefte aan housing nog niet volledig duidelijk is, wordt housing als optie meegenomen in de aanbesteding van de Cloud platform dienstverlening. De private cloud met on-premise server-, storage- en hostinginfrastructuur wordt fysiek ondergebracht in een datacenter (housing). Het datacenter maakt op basis van Azure express route verbinding met Azure (zie Hoofdstuk 6. Netwerk services).

5.3.2 BS2.2 Private Cloud (optie)

Conform de cloud-first visie verhuist de ICT-infrastructuur van de Aanbestedende dienst naar de publieke cloud. PaaS of IaaS workloads die vanuit technische beperkingen of BIV-classificatie niet in de publieke cloud kunnen worden opgenomen, worden optioneel in een private cloud geplaatst. De combinatie van de publieke cloud en de private cloud noemen we het Cloud platform van de Aanbestedende dienst. De verwachting is dat applicaties of kunnen worden ver-SaaS-ed of in de publieke cloud kunnen draaien, daarmee vervalt de noodzaak van een private cloud in een datacenter vanuit applicatieve toepassingen. Dit is op dit moment nog niet 100% duidelijk. De keuze van de inrichting van de private cloud is afhankelijk van eisen, zoals: uniformiteit in beheer, kosten en risicospreiding (security). Op dit moment zijn deze eisen nog onvoldoende duidelijk. Gezien de visie om cloud-native te gaan werken, is het uitgangspunt om Azure Arc te implementeren voor on-premises servers. Hiermee ontstaat een centrale en uniforme manier van beheer en monitoring.

5.4 Ontwerpbesluiten

Entiteit	Toelichting/Omschrijving	Aard van de verandering
Housing	Bestaande dataroom in het provinciehuis gebruiken (uitgangspunt) en als optie alternatief uitvragen in aanbesteding.	Hardware installeren of hergebruiken en inrichten.
Private cloud	On-premises omgeving uitbreiden met Azure Arc.	Inrichting private cloud met agent op resources.
Uitwijk	Domain controller met cold-standby hardware voor email en andere 'kroonjuwelen'	Inrichting private cloud voor uitwijk.
Backup	Geen offsite backup maar online backup bij andere service provider dan Microsoft.	Uitbreiding van bestaande backup bij AvePoint.

6 Netwerk services

Dit hoofdstuk beschrijft in meer detail de huidige situatie, verbeterpunten, toekomstige situatie en de verbeterpunten van de *Netwerk services*.

6.1 Bouwstenen

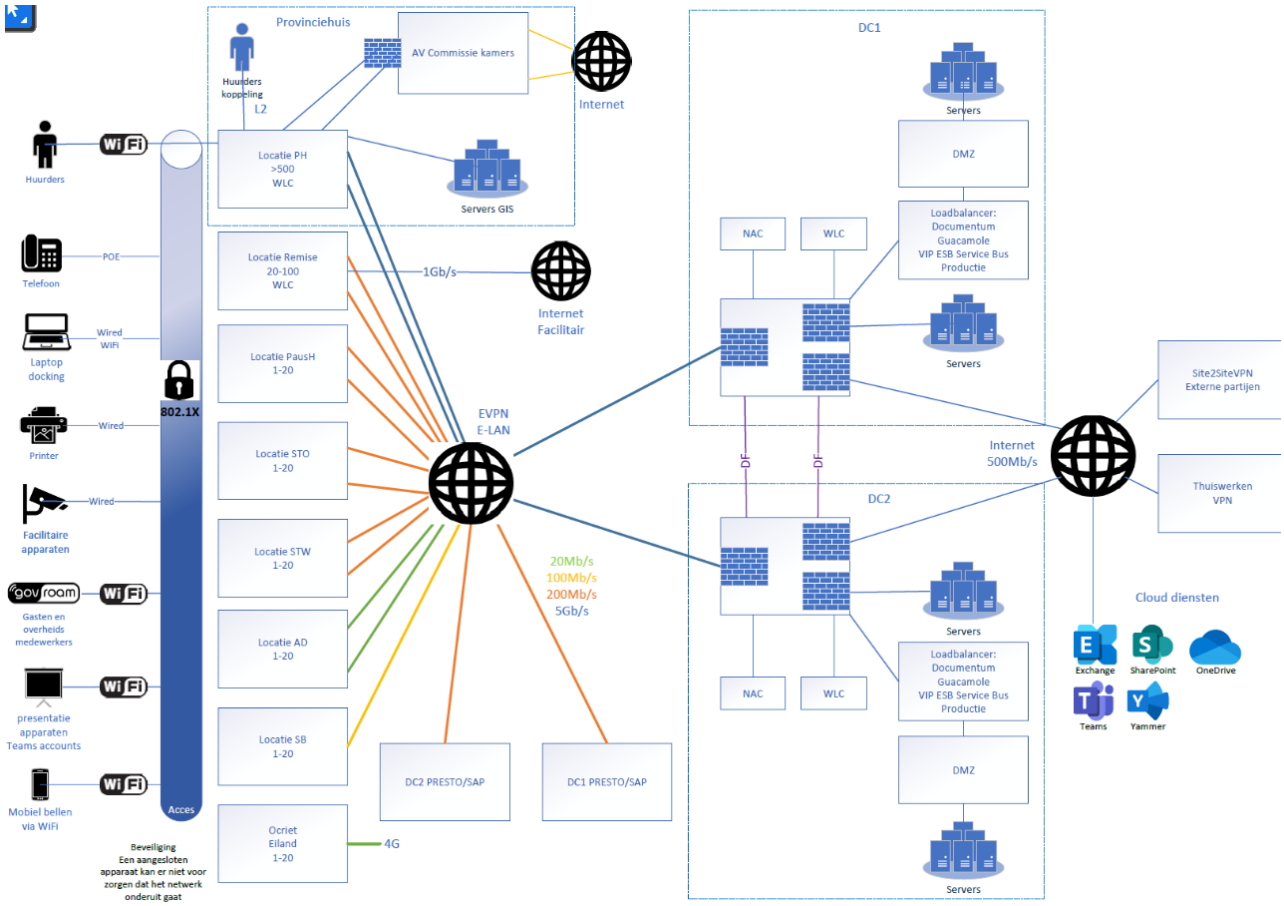
De te realiseren ICT-bouwstenen (BS) als onderdeel van de Netwerk services zijn:

- BS3.1 Publieke cloud Connectiviteit
- BS3.4 Netwerkservices (DNS/DHCP/NTP/Radius)

6.2 Huidige situatie

6.2.1 Netwerktopologie

Het Aanbestedende dienst netwerk bestaat uit lokale netwerken (w)LAN op de 7 locaties en 5 datacenters (PQR DC1/DC2, Mybrand DC1/DC2 SAP, provinciehuis dataroom GIS) en het WAN voor connectiviteit tussen deze werklocaties, datacenters én het internet. Het (w)LAN is recent vervangen door Network Infrastructure as a Service uitgevoerd door AVIT Groep. Het WAN met internetverbindingen dient eind 2025 opnieuw te worden aanbesteed. Figuur 5 toont de huidige situatie van het PU-netwerk.



Figuur 5 - Huidige situatie PU-netwerk

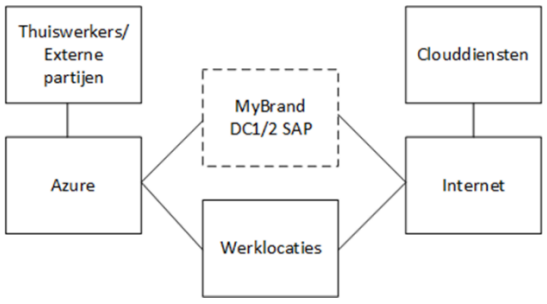
6.2.2 LAN
De LAN-switches op deze werklocaties zorgen voor het ontsluiten van apparatuur op het netwerk. Afhankelijk van de omvang van een kantoorlocatie bestaat deze uit: (on)bekabelde werkplekken, telefoons, printers, (govroam) WiFi, vergaderruimte(s), facilitaire en mobiele apparaten. Iedere locatie is voorzien van een firewall voor de veilige koppeling van het kantoornetwerk met het WAN. De Aanbestedende dienst is voor samenwerking tussen overheidsorganisaties op 'Govroam' gekoppeld. Voor gasten van de Aanbestedende dienst wordt draadloze internet connectiviteit ook middels een afgenomen dienst van 'Govroam' geleverd.

6.2.3 WAN
Het huidige WAN bestaat uit een Eurofiber EVPN-oplossing met redundante verbindingen in diverse bandbreedtes naar de werklocaties en datacenters en internet connectiviteit vanuit de PQR DC1/DC2 datacenters. In de PQR DC1/DC2 datacenters (Schiphol-Rijk en Haarlem) is als knooppunt binnen het netwerk (transit) één rack geplaatst met netwerkapparatuur voor de leveranciers van de WAN (Eurofiber) en (w)LAN-diensten (AVIT). Hierin draait de centrale netwerkapparatuur t.b.v. netwerkmanagement, RADIUS-servers, ISE (802.1x) en centrale firewalls. Netwerkservices zoals DHCP en DNS draaien nu centraal op VM's op Nutanix host. Het internet wordt ontsloten via deze centrale firewalls. Vanuit alle locaties en datacentra gaat het verkeer bestemd voor het internet (egress) via de EVPN-oplossing naar de centrale firewalls bij PQR om vervolgens naar het internet te gaan. Uitzondering hierop zijn de audiovisuele conferentiekamers, de Commissiekamers en Statenzaal in het provinciehuis. Deze gaan via de eigen firewall en internetverbinding rechtstreeks naar het internet.

6.2.4 VPN
Zowel thuiswerkers als externe partijen (nu circa 200-300 gebruikers) kunnen een ontsluiting krijgen via een VPN-verbinding met het netwerk van de Aanbestedende dienst.

6.3 Gewenste situatie

6.3.1 BS3.1 Publieke cloud Connectiviteit
Met de applicatiemigratie (IaaS) van PQR DC1/DC2 datacenters naar Azure veranderen de verkeersstromen binnen het netwerk. Door de introductie van een zero-trust architectuur met geïntegreerde security, verandert ook de noodzaak om alle netwerkverkeer van werklocaties via een centrale firewall naar het internet te routeren. De moderne werkplek van de gebruiker heeft alleen een directe internetverbinding nodig voor toegang tot SaaS-applicaties, Office365 of Azure. Het netwerkknooppunt (transit), wat nu in de PQR DC1/DC2 datacenters staat, wordt als virtueel netwerkknooppunt in Azure geplaatst.



Figuur *6* - Vereenvoudigde weergave toekomstige situatie PU-netwerk

Figuur 6 toont een vereenvoudigde weergave van deze toekomstige situatie van het PU-netwerk:
- De IaaS-omgeving in de PQR datacenters is gemigreerd naar Azure.
- De IaaS-omgeving in de dataroom van Aanbestedende dienst is gemigreerd naar Azure. Maar optioneel is er een private cloud;
- SAP staat voorlopig nog in de datacenters van MyBrand;
- Azure beheert de transit van het complete netwerk.

Er is gekozen dat de cloud platform leverancier het netwerk in Azure beheert en de WAN-leverancier de netwerkverbindingen inclusief Express Route. Daarbij geldt dat er gezamenlijk verantwoordelijkheden gelden tussen beide leveranciers en dat hier goede afspraken over gemaakt moeten worden.

Het on-premises datacenter cq. private cloud zal voorzien worden van een ExpressRoute verbinding. Per werkocatie dient gekeken te worden of een privéverbinding (Point-to-Site VPN) vereist is en welke eisen gesteld worden aan de locatie (denk hierbij aan betrouwbaarheid, snelheid garanties en/of lage latency). Deze keuze is mede afhankelijk voor de keuze van de WAN-verbindingen.

Op basis van het advies van Eurofiber en Avit is de keuze voor 1 EVPN verbinding en 1 lokale Internetverbinding voor het Provinciehuis en Datacenter en alleen lokale netwerkverbindingen met internettoegang (LIB) per overige werklocatie. Door de realisatie van de LIB kunnen ook de bandbreedtes van EVPN worden verlaagd.

De moderne werkplek is volledig gebaseerd op clouddiensten die vanaf de werk- of thuislocaties via de Internetverbinding worden benaderd. Hiervoor wordt iedere werklocatie voorzien van een Internetverbinding met voldoende bandbreedte, een zogenaamde lokale internet break-out (LIB). Een richtlijn voor de bandbreedte is 3 Mbps per gebruiker. De LIB wordt voor drie doeleinden gebruikt:

1. Internet toegang voor digitale werkplekken van PU-medewerkers.
2. WAN-koppeling van de werkocaties
3. Internet toegang voor gastgebruikers. (en facilitaire apparaten)

Hiervoor moet de configuratie van de Cisco Meraki Firewall op de werklocaties worden aangepast zodat DHCP en DNS services lokaal aangezet worden, waarbij soms een nieuwe vLAN en IP-reeks nodig is.

6.3.2 BS3.4 Netwerkservices (DNS/DHCP/NTP/Radius)

- DHCP wordt lokaal verzorgd door lokale Firewall op de werklocatie;
- DNS wordt verzorgd door lokale Firewall met Forward naar de private DNS servers in Azure voor gewenste DNS zone(s);
- NTP (Tijdsynchronisatie) wordt verzorgd door NTP servers in Azure voor domein apparaten;
- Authenticatie services wordt verzorgd door de Domain Controllers in Azure voor domein apparaten;
- Netwerkauthenticatie wordt verzorgd door de centrale Radius servers Cisco ISE die indien nodig Radius requests kunnen forwarden naar andere Radius servers. Dit kunnen interne en externe Radius servers zijn zoals Govroam of van huurders

6.4 Ontwerpbesluiten

Entiteit	Toelichting/Omschrijving	Aard van de verandering
Verantwoordelijkheden netwerk	Demarcatie verantwoordelijkheden: cloud platform dienstverlener beheert het netwerk op Azure en WAN-leverancier netwerkverbindingen inclusief Express Route.	Demarcatie netwerk vastleggen in RACI.
Netwerkconnectiviteit Azure - on-premise datacenter	On-premise datacenter (private cloud) zal voorzien worden van een ExpressRoute verbinding.	Inzet van Azure ExpressRoute.
Netwerkconnectiviteit werkocaties	Per werklocatie zal afhankelijk van de eisen gekeken worden of een privé-verbinding vereist is.	Inzet van Azure Site-to-Site VPN of EVPN.
Netwerkservices	Afhankelijkheid centrale netwerkservices verminderen.	DHCP en DNS door Firewall op werkocatie.

7 Werkplek services

Dit hoofdstuk beschrijft in meer detail de huidige situatie, toekomstige situatie en de verbeterpunten van de *Werkplek services*.

7.1 Bouwstenen

De te realiseren ICT- bouwstenen als onderdeel van de Werkplek services zijn:

- BS4.1 Centraal apparaat beheer en uitrol
- BS4.2 Mobiel apparaat beheer (MDM/MAM)
- BS4.3 Applicatie distributie
- BS4.4 Virtuele desktop (optie)
- BS4.5 Lokale beheerrechten
- BS4.6 VPN
- BS4.7 Printen en scannen

7.2 Huidige situatie

7.2.1 Apparaten

Binnen de 'mobile first'-strategie worden laptops en tablets in een beperkt aantal varianten gebruikt, samen met flexibele werkplekken op kantoorlocaties (inclusief monitoren, toetsenborden en muizen). Medewerkers hebben de keuze uit een laptop en een smartphone. Voor thuiswerkplekken ontvangen vaste medewerkers een monitor met dockingstation in bruikleen van de organisatie. Commissie- en statenleden gebruiken een tablet (iPad). Daarnaast zijn enkele vaste pc's in gebruik. Voor medewerkers die met CAD/GIS werken, zijn gespecialiseerde CAD/GIS-laptops beschikbaar. Laptops draaien op Windows 11 en worden geleverd met een generieke applicatie set, zie bijlage 1. Smartphones ondersteunen Apple iOS en Android en tablets ondersteunen iPadOS. Inhuur, externen en stagiaires werken zoveel mogelijk met eigen apparatuur, Bring Your Own Device (laptop, tablet, smartphone). Op het BYOD-apparaat mag in principe geen data worden bewaard van Provincie Utrecht, dit kan nu niet technisch worden afgedwongen wat risico's op datalekken met zich meebrengt. Externe medewerkers ontvangen alleen een laptop van Provincie Utrecht wanneer zij toegang nodig hebben tot applicaties die niet via internet toegankelijk zijn.

Apparaat	Aanbestedende dienst medewerkers	CvdK/Commissie- en statenleden	Externen	Totaal
Laptops	1.197	1	136	**1.234**
Tablets		84		**84**
BYOD			Ca. 430	**Ca. 430**
Smartphones				**Ca. 1.170**

7.2.2 Deployment en configuratie

Laptops worden uitgerold met behulp van OpenText ZENworks, een platform dat oplossingen biedt voor apparaat beheer, applicatie installatie en software updates via een centraal beheersysteem. Het wissen van apparaten op afstand, bijvoorbeeld bij calamiteit of diefstal, is nu mogelijk voor laptops en smartphones via Exchange ActiveSync. Configuraties worden toegepast door middel van Group Policies en op minimale schaal ook vanuit ZENworks. Apparaten worden zo veel mogelijk open ingericht, enerzijds zodat gebruikers hun werkomgeving naar eigen voorkeuren kunnen inrichten voor een optimale werkervaring binnen het werkveld van de individuele medewerker en anderzijds om de beheerlast te minimaliseren. Dit is een bewuste kostenbesparende beleidskeuze uit het verleden. Beperkt privégebruik van de apparaten is volgens de gebruiksovereenkomst toegestaan. Ten behoeve van 'deployment en configuratie' wordt gebruik gemaakt van

de on-premises infrastructuur, waarbij laptops automatisch worden gekoppeld aan een Active Directory binnen deze infrastructuur bij het imaging proces en in EntraID worden opgenomen. Tijdens het af-installeren met de gebruiker wordt de koppeling met Office365 gemaakt.

7.2.3 Applicaties

In het basis image van de laptop is alleen Windows 11 en de standaard applicaties zoals Office, Anti-virus e.d. opgenomen. Alle standaard software die voor iedere medewerker beschikbaar wordt gesteld zijn in ZENworks gepackaged en worden als losse installaties verzorgd. Zie bijlage 1 met overzicht standaard software. Dit betreft zowel lokale software als SaaS-applicaties (url). De SaaS-apps worden beschikbaar gesteld via Innerweb. Software wordt in principe niet 'gepushed' naar clients, maar gebruikers kunnen hun software ophalen vanuit de ZENworks client. Daarnaast is het mogelijk om aanvullende software aan te vragen via Assyst. Zie bijlage 2 met overzicht aanvullende software. Opmerking: een aantal van deze applicaties zijn in de tussentijd ver-Saast en worden niet langer meer als lokale software aangeboden of zijn uitgefaseerd. Deze Standaard en Aanvullende applicaties worden door Aanbestedende dienst gepackaged in ZENworks Configuration Management Console in .msi, .exe, powershell en .bat formaat. Tenslotte kan iedere medewerker voor een optimale werkervaring en hun werkomgeving naar eigen voorkeur in te richten ook zelf ook lokaal benodigde software installeren. Voor externen met BYOD is Innerweb de ingang voor SaaS-applicaties van Provincie Utrecht zoals Office365, Intranet, Assyst en Planon.

7.2.4 Toegang

Laptops die eigendom zijn van Aanbestedende dienst worden vertrouwd op het interne wLAN-netwerk. Laptops moeten aan de Active Directory zijn toegevoegd om toegang te krijgen tot interne wLAN via 802.1X inlog op basis van computeraccount. Er is een voorkeur ingesteld voor WiFi verbinding met het interne wLAN, als deze niet beschikbaar is zal geprobeerd worden met WiFi Govroam te verbinden. Smartphones, tablets en BYOD maken gebruik van het Govroam netwerk. Alle medewerkers met een account voor Aanbestedende dienst hebben Govroam voor een veilige en eenvoudig online netwerktoegang bij andere deelnemende overheidsorganisaties of eventueel binnen de provincie.

7.2.5 Printen en scannen

Voor printing/scanning worden Canon multi-functionals met follow-me printing functionaliteit gebruikt. Er staan 20 Canon MFP's in het provinciehuis en 8 op de overige kantoorlocaties. Er is een printserver ingericht voor Canon Uniflow. Printopdrachten kunnen met een toegangspas worden opgehaald bij de printer. Thuisprinters worden met printer drivers ondersteund die gebruikers nu zelf kunnen installeren. Externen en gasten kunnen printopdrachten als bijlage mailen naar print@provincie-utrecht.nl.

7.2.6 IP-telefonie

Voor IP-telefonie wordt gebruik gemaakt van Teams Phone Systems via leverancier Communicativ.

7.2.7 VPN

Er is een LAN-based VPN-oplossing beschikbaar. Dit systeem maakt gebruik van een client-applicatie om gebruikers te verbinden met de on-premises omgeving. Alleen laptops die lid zijn van de Active Directory kunnen toegang krijgen met VPN.

7.3 Gewenste situatie

7.3.1 BS4.1 Centraal apparaat beheer en uitrol

Microsoft Intune wordt ingezet om apparaten te voorzien van de juiste configuratie en beveiligingsinstellingen. Dankzij de brede ondersteuning van verschillende platformen (Windows, iOS/iPadOS, MacOS, en Android) kunnen apparaten centraal beheerd worden via één enkel portaal. Alle beheerde apparaten worden opgenomen in Intune, wat betekent dat laptops en mobiele apparaten die door de organisatie beschikbaar worden gesteld, binnen Intune worden geregistreerd en beheerd. Deze aanpak zorgt voor een uniforme en veilige werkomgeving voor alle gebruikers.

Windows Autopilot wordt ingezet om apparaten voor te bereiden en vooraf te configureren, zodat ze in een "bedrijfsklare" staat worden geleverd. Tijdens het Autopilot-proces worden de basisapplicaties (Microsoft Office, Company Portal enz.) automatisch geïnstalleerd, waardoor het apparaat direct volledig functioneel is en gebruiksklaar wordt geleverd. Met behulp van Autopilot is het mogelijk om verschillende typen werkplekken te definiëren en te beheren, zoals standaard-, staten- en commissieleden- en CAD/GIS werkplek. Door gebruik te maken van Autopilot Grouptags en Intune-filters kunnen deze werkplekken effectief worden ingericht met specifieke applicaties en configuraties, afgestemd op de behoeften van de gebruikers en het type werkplek. Daarnaast biedt deze aanpak de optie om apparaten door de leverancier vooraf te laten voorzien van een Windows-installatie. Hierdoor kunnen de apparaten direct worden geconfigureerd en uitgerold naar gebruikers, wat de implementatie aanzienlijk vereenvoudigt en versnelt.

De configuratie van de apparaten wordt uitgevoerd via Intune. Met Intune worden verschillende soorten configuraties beschikbaar gesteld:

- **Compliance policies**: regels die bepalen of apparaten voldoen aan configuratievereisten, essentieel voor veilige toegang tot bedrijfsresources.
- **Configuration policies**: bepalen apparaat instellingen, zoals beveiligingsconfiguraties, netwerkopties en appbeheer, om een consistente werkomgeving te garanderen.
- **Endpoint Security policies**: beschermen apparaten door beveiligingsinstellingen te beheren, zoals antivirus, versleuteling en firewall, tegen bedreigingen.
- **Update policies**: beheren het proces van systeem- en software-updates op apparaten, om consistentie, veiligheid en functionaliteit te waarborgen.

Hiermee wordt veilige en gecontroleerde toegang tot bedrijfsresources gewaarborgd.

7.3.2 BS4.2 Mobiel apparaat beheer (MDM/MAM)

Apparaten die door de organisatie worden verstrekt worden geregistreerd in Intune voor Mobile Device Management (MDM). Deze apparaten worden vervolgens geïntegreerd in Android Enterprise of Apple Business Manager, afhankelijk van het besturingssysteem, en geconfigureerd via Intune om optimale beveiliging en functionaliteit te bieden. Persoonlijke apparaten van medewerkers worden geregistreerd in Intune voor Mobile Application Management (MAM). Dit systeem creëert een aparte beveiligde omgeving binnen het apparaat waarin bedrijfsapplicaties en -gegevens veilig toegankelijk zijn. De gegevens blijven binnen deze beveiligde omgeving en kunnen niet worden gedeeld of gebruikt voor persoonlijke doeleinden. Het apparaat wordt niet beheerd via MAM, waardoor de verantwoordelijkheid voor onderhoud en beheer van het persoonlijke apparaat volledig bij de gebruiker blijft.

7.3.3 BS4.3 Applicatie distributie

Applicaties worden beschikbaar gesteld door middel van Intune. Dat betekent dat Standaard en Aanvullende applicaties welke door gebruikers aangevraagd of gebruikt moeten worden, te allen tijde beschikbaar worden gesteld via Intune en dus onder beheer worden genomen. Als ervoor gekozen wordt om het installeren van applicaties door gebruikers volledig te blokkeren kan gebruik worden gemaakt van Application Control in Intune. Hiermee worden alleen nog door Intune beschikbaar gesteld applicaties toegestaan.

7.3.4 BS4.4 Virtuele desktop (optie)

Voor externen moet het ook mogelijk zijn om gebruik te maken van de IT-faciliteiten van PU, zonder dat ze vast werkzaam zijn bij Aanbestedende dienst. Gezien het aantal externe gebruikers (400 externen, waarvan 130 met laptop van PU), is Azure Virtual Desktop (AVD) een geschikte oplossing. Hierin moet ook meegenomen worden dat AVD mogelijk ook een geschikte oplossing is voor specifieke werkplekken, zoals de GIS-werkplek en als opstap werkplek voor beheerders, waardoor dit aantal waarschijnlijk nog hoger uitvalt. Omdat de werkplekvisie nog niet is vastgesteld en de inzet van een virtuele desktop ten behoeve van het GIS-platform nog niet 100% duidelijk is, wordt de virtuele desktop als optie meegenomen in de aanbesteding.

7.3.5 BS4.5 Lokale beheerrechten

Voor een aantal typen gebruikers wordt voorzien dat het mogelijk moet zijn om tijdelijk lokale beheerrechten aan te vragen. Hiervoor kan gebruik worden gemaakt van Endpoint Privilege Management (EPM). EPM is beschikbaar als toevoeging op de standaard Intune functionaliteit en kan worden gebruikt om specifieke acties uit te voeren met verhoogde rechten. Hierbij kan het gaan om zowel de installatie van applicaties, het bijwerken van drivers, alsook het verzamelen van specifieke diagnostische data. Het gebruik van EPM vereist additionele licenties die niet standaard in de Microsoft 365 E3 of Microsoft 365 E5 licentie zitten.

7.3.6 BS4.6 VPN

Momenteel wordt een op de LAN gebaseerde VPN-oplossing gebruikt als tijdelijke voorziening. Het doel is om over te stappen naar Microsoft Global Secure Access. Deze aanpak biedt naadloze integratie met Cloud services en ondersteunt moderne beveiligingsprincipes zoals Zero Trust, Microsoft Entra en Multi-Factor Authenticatie (MFA), wat bijdraagt aan een veilige en efficiënte digitale werkomgeving. Het gebruik van Global Secure Access vereist additionele licenties die niet standaard in de Microsoft 365 E3 of Microsoft 365 E5 licentie zitten. Deze licenties kunnen per product worden afgenomen of als onderdeel van de Microsoft Entra Suite.

7.3.7 BS4.7 Printen en scannen

De overeenkomst met Canon loopt eind 2025 af en wordt opnieuw aanbesteed. Het belangrijkste bij een printoplossing voor de digitale werkplek is de toegankelijkheid en beschikbaarheid. Aangezien de werkplek vooral Internet verbonden zal zijn, zal ook de beste ervaring komen via een Cloud print oplossing. Mocht dat niet mogelijk zijn, dan kan er ook te allen tijde worden teruggevallen op Microsoft Universal Print. Universal Print biedt de mogelijkheid om Cloud printing te faciliteren, ook wanneer de printers en printservers nog in het on-premises datacenter draaien. Thuisprinters worden met standaard Windows 11 printer drivers ondersteund.

7.4 Ontwerpbesluiten

Entiteit	Toelichting/Omschrijving	Aard van de verandering
Beheer van apparaten	Volledig apparaatbeheer via Intune voor het efficiënter en gestroomlijnder distribueren van zowel apparaten als applicaties.	Verbeterd centraal beheer van apparaten en compliance.
Uitrol van apparaten	Windows Autopilot deployment profielen configureren en apparaten integreren in Intune	Nieuwe apparaten snel en efficiënt gebruiksklaar maken.
Mobiele organisatie apparaten	Inzet Intune voor mobiel device management (MDM) op mobiele organisatie apparaten, met integratie in Android Enterprise of Apple Business Manager.	Centraal beheer van mobiele organisatie apparaten.
Mobiele persoonlijke apparaten	Inzet Intune voor mobiel applicatie management (MAM) op persoonlijke mobiele via App Protection- en App Configuration-beleidsregels met Conditional Access-beleid om de toepassing van MAM effectief te handhaven.	Veilige toegang tot bedrijfs-resources op mobiele persoonlijke apparaten, binnen een gescheiden omgeving, zonder dat het apparaat zelf wordt beheerd.
Configuratie apparaten	Intune configuratieprofielen instellen, waaronder OneDrive-integratie, Microsoft 365-toepassingen, aanvullende beveiligingsmaatregelen en algemene Windows-configuraties, waardoor een moderne en flexibele aanpak mogelijk wordt.	Vervanging bestaande Group Policies, die afhankelijk zijn van de traditionele on-premises infrastructuur.
Beveiliging apparaten	Intune security baseline op alle Windows-apparaten als fundament voor het beveiligingsbeleid met aanvullende beleidsregels, waaronder Windows Updates, Defender Antivirus, Attack Surface Reduction-regels en BitLocker-encryptie.	Apparaten beter beschermen tegen mogelijke bedreigingen.

Compliance apparaten	Nalevingsbeleid om ervoor te zorgen dat Windows-apparaten voldoen aan vastgestelde configuratiestandaarden, om gecontroleerde en veilige toegang tot zakelijke bronnen te garanderen.	Apparaten voldoen aan configuratie- en beveiligingsvereisten.
Lokale beheerdersrechten	Door Autopilot deployment profiel worden gebruikers standaard voorzien van beperkte rechten op het apparaat, zoals het zelf kunnen installeren van software, om de veiligheid en betrouwbaarheid van apparaten te vergroten. Gebruikers kunnen tijdelijk lokale beheerrechten aanvragen via Endpoint Privilege Management.	Gebruikers voorzien van standaard rechten op een beheersbaar en gecontroleerd niveau.
Extern gebruik	Azure Virtual Desktop (AVD) voor toegang van externe gebruikers voor toegang tot benodigde bedrijfs-applicaties en -gegevens, ongeacht de fysieke locatie van de gebruiker. Deze AVD-omgeving kan ook gebruikt worden om specifieke applicaties aan te bieden zoals GIS.	Externe gebruikers krijgen optioneel een virtuele desktop op hun BYOD Externe gebruikers met laptop van Aanbestedende dienst (ca. 130) leveren deze in en zorgen zelf voor BYOD.
VPN	Inzet van Global Secure Access als VPN-oplossing met gebruikers- en apparaat beleid voor veilige toegang tot bedrijfsbronnen via Identity and Access Management (IAM). (Zie Hoofdstuk 11. Identiteits- en toegangbeheer services)	Vervanging van LAN-VPN door Global Secure Access.

8 Samenwerking services (O365)

Dit hoofdstuk beschrijft in meer detail de huidige situatie, verbeterpunten, toekomstige situatie en de verbeterpunten van de *Samenwerking services*.

8.1 Bouwstenen

De te realiseren ICT- bouwstenen als onderdeel van de Samenwerking services zijn:
- BS5.4 Dataclassificatie en Datalekbeveiliging
- BS5.5 Compliance management (optie)

8.2 Huidige situatie

8.2.1 Samenwerking
Er wordt gebruik gemaakt van de Microsoft 365 suite voor samenwerking en dataopslag. Persoonlijke data is opgeslagen in OneDrive, bedrijfsdata in SharePoint Online/Teams. Email bevindt zich reeds in Exchange Online. Teams wordt gebruikt voor samenwerking met chat, online vergader- en samenwerkingsplatform en IP-telefonie. SharePoint Online wordt ook ingezet voor Intranet functionaliteit en het ondersteunen van processen.

8.2.2 Beveiliging en compliance
Binnen Aanbestedende dienst omvat 'Compliance' meerdere aandachtsgebieden: van het voldoen aan bepaalde wet- en regelgeving (AVG, BIO2, Archiefwet) en interne beleidskaders Privacybeleid, Informatiebeveiligingsbeleid, handboek Informatiebeheer, Bewaartermijn persoonsgegevens en Backup beleid), tot de technische status van een apparaat. Er is reeds functionaliteit ingericht voor het monitoren van gebruik en compliance-gerelateerde kenmerken van Teams- en SharePoint-omgevingen. Zo worden via geautomatiseerde processen (o.a. Azure Automation) gegevens verzameld over het gebruik van Teams/SharePoint Sites, zoals het aantal documenten, eigenaarschap, opslagverbruik, inactiviteit en kanaalstructuur (privé/gedeeld). Deze informatie wordt centraal opgeslagen in een SharePoint-lijst, ten behoeve van o.a. DIV en Functioneel Beheer. Tevens worden per Team of SharePoint-site de aanwezige dossiers geïnventariseerd, waarbij metadata wordt benut om dossiers te verrijken en correct te archiveren in Corsa. Hoewel datagerichte compliance dus niet nieuw is, is er behoefte om de compliance status integraal bij te houden en te monitoren, zodat hier beter op gestuurd en gecorrigeerd worden.

Er wordt gebruik gemaakt van classificatie op basis van Sites en groepen. Hiervoor zijn op dit moment 4 labels:
- Open Community
- Niet Vertrouwelijk
- Vertrouwelijk
- Geheim

Deze classificatie wordt bepaald tijdens de intake met DIV waar de classificatie wordt vastgesteld met de aanvrager van Microsoft Teams omgeving. De bescherming achter deze labels is met name gericht op toegang en samenwerken (met externen) en bevat instellingen rondom delen, standaard linktype en de mogelijkheid tot het indienen van toegangsverzoeken.

Er zijn vertrouwelijkheidslabels voor documenten en e-mails ingericht en eerder getest in een pilot, maar deze zijn nooit breed geïmplementeerd vanwege archiveringsproblemen met versleutelde bestanden (E-depot verwerkt geen versleutelde bestanden) en zorgen over het gebruiksgemak en de impact en adoptie voor eindgebruikers.

8.2.3 Back-up
AvePoint wordt gebruikt voor back-up van Office365 en identiteiten in Entra ID. Er is een back-up and restore-beleid vastgesteld.

8.2.4 Archivering

Voor data-archivering wordt Corsa recordmanagement (RMA) gebruikt. In Corsa RMA worden afgesloten dossiers gearchiveerd en voorzien van allerlei metadata, zoals bewaartermijnen. In Corsa zitten te bewaren en op termijn te vernietigen projecten en dossiers. Voor functionele invulling archiefwaardige bestanden wordt E-depot gebruikt, een statisch archief alleen raadpleegbaar door ambtelijke organisaties, burgers of onderzoekers. Er zijn bewaartermijnen vastgesteld en middels een selectielijst wordt vastgesteld welke dossiers kunnen worden vernietigd en welke op termijn naar E-depot moeten. Voor gebruikers zijn SharePoint en Corsa zijn als doorzoekbare bronnen ontsloten via Enterprise Search, andere applicatiebronnen zijn hierin nog niet ontsloten vanwege issues t.a.v. informatiebeveiliging en indexering.

8.3 Gewenste situatie

De Aanbestedende dienst heeft stappen te zetten om het volwassenheidsniveau te verhogen. Om het data security & compliance volwassenheidsniveau te verhogen is dit per onderdeel verder uitgewerkt.

8.3.1 BS5.4 Dataclassificatie en datalekbeveiliging

Een heldere en consequente aanpak biedt meer controle, versterkt de beveiliging en helpt bij het voldoen aan wet- en regelgeving. Met het doorgroeien op de huidige inrichting en het bestaande beleid is het mogelijk om door te groeien naar een hoger volwassenheidsniveau. Een solide aanpak voor het bewaren en opruimen van informatie is essentieel om grip te houden op data binnen de organisatie. Met Purview Data Retention kan bewaarbeleid op een gecontroleerde en consistente manier geïmplementeerd worden.

8.3.2 BS5.5 Compliance management (optie)

Het effectief beheren van compliance-verplichtingen vraagt om inzicht, structuur en een proactieve aanpak. Purview Compliance Manager ondersteunt bij het systematisch beoordelen en verbeteren van de nalevingsstatus. Door duidelijke richtlijnen, automatisering en continue monitoring helpt het platform organisaties om risico's te minimaliseren en aan regelgeving te voldoen.

In het kader van juridische procedures, interne onderzoeken of compliance-eisen is het essentieel dat organisaties snel en nauwkeurig toegang kunnen krijgen tot relevante informatie. Purview eDiscovery en Content Searches bieden krachtige tools om gegevens op een gecontroleerde manier op te sporen, te analyseren en te exporteren. Purview eDiscovery en Content Searches bieden krachtige tools om gegevens op een gecontroleerde manier op te sporen, te analyseren en te exporteren.

Het adequaat beheren van interne dreigingen is van essentieel belang voor het beschermen van organisaties tegen misbruik en gegevensdiefstal. Purview Insider Risk Management (met de E5 Compliance Add-on) biedt een geïntegreerd platform dat gericht is op het detecteren en onderzoeken van onregelmatigheden in gebruikersgedrag, zodat risico's vroegtijdig kunnen worden gesignaleerd en aangepakt.

8.3.3 Transformatie

Gezien het data security & compliance volwassenheidsniveau van de Aanbestedende dienst wordt in 2026 eerst de compliance mogelijkheden binnen Microsoft 365 E3 ingezet om vanaf 2027 de mogelijkheden van E5-compliance Add-on licentie te benutten. Dat betekent dat de geavanceerdere functionaliteiten, die zijn beschreven, onderdeel zijn van het groeipad van Aanbestedende dienst naar een hoger volwassenheidsniveau. Hierbij gaat het om geavanceerde gevoeligheidslabeling functionaliteiten (zoals automatisch labelen), geavanceerde eDiscovery, geavanceerde DLP functionaliteiten (zoals Endpoint DLP), geavanceerde rententielabeling functionaliteiten (zoals automatisch labelen) en Insider Risk Management.

8.4 Ontwerpbesluiten

Entiteit	Toelichting/Omschrijving	Aard van de verandering
Compliance	Inzet van Purview Compliance Manager om te toetsen aan Wet en regelgeving en interne beleidskaders.	Inzicht krijgen in compliance.
Informatie Classificatie	Inzet van informatie classificatie in M365 via handmatig classificeren. In later stadium inzet Purview Information Protection voor automatische classificatie labels.	Voldoen aan de BIO/CBW.
Datalekbeveiliging	Inzet Purview DLP met beleidsregels voor meer controle op de toegang tot informatie.	Vermindert het risico op datalekken.
Informatieretentie	Inzet van Purview Data Retention retentie om meer controle uit te oefenen op de informatie levenscyclus van informatie.	Voldoen aan wetgeving zoals de AVG wanneer het gaat om privacy gevoelige informatie.
Inzage en Inzicht	Inzet van Purview eDiscovery en Content Searches om het kader van juridische procedures, interne onderzoeken of compliance-eisen snel en nauwkeurig toegang te krijgen tot relevante informatie.	Ondersteuning juridische verplichtingen en beperking risico's bij incidenten.
Risk management	Inzet van Purview Insider Risk Management (IRM) versterkt de informatiebeveiliging en er wordt een proces gehandhaafd welke interne risico's vroegtijdig meldt en mitigeert.	Beschermen tegen misbruik en gegevensdiefstal.

9 Identiteit- en toegangsbeheer services

Dit hoofdstuk beschrijft in meer detail de huidige situatie, verbeterpunten, toekomstige situatie en de verbeterpunten van de *Identiteit- en toegangsbeheer services*.

9.1 Bouwstenen

De te realiseren ICT- bouwstenen als onderdeel van de Identiteit- en toegangsbeheer zijn:

- BS6.1 Identity and Access Management (IAM)
- BS6.2 Priviledge Identity Management (PIM)
- BS6.3 Identity Governance Administration (IGA) (optie)

9.2 Huidige situatie

9.2.1 Identity and Access Management

De Identity and Access Management oplossing van Provincie Utrecht staat in Figuur 14 weergegeven en is gebaseerd op de OpenText Identity Manager (NetIQ). Naast OpenText worden ook Entra ID en Active Directory gebruikt voor de authenticatie richting Microsoft 365. De belangrijkste aspecten van de huidige situatie worden hieronder kort toegelicht.

De Primaire Identity Provider (IDP) is OpenText Identity en Access management[3]. Hoewel Entra ID al wordt gebruikt, fungeert deze momenteel niet als primaire Identity Provider. Authenticatie verloopt grotendeels via OpenText, ook voor de federatieve koppelingen. Er zijn meerdere applicaties geïntegreerd via Entra ID, waaronder Office365, SocialIntranet, Docgenerator en Corsa. Daarnaast wordt Active Directory gebruikt, voor de werkstations, terwijl de huidige Aanbestedende dienst laptops reeds in Entra ID staan. Federatieve toegang tot SaaS-oplossingen wordt gerealiseerd via SAML 2.0 (eis in aanbestedingen), waarbij OpenText fungeert als federatieve IDP. Op het vlak van toegangsbeheer is conditional access deels geïmplementeerd. Multi-Factor Authenticatie (MFA) wordt ondersteund en is beschikbaar via verschillende authenticatie methoden zoals SMS en email. Authenticatie via smartphone authenticator-app is technisch mogelijk. Self-Service Password Reset (SSPR) is geïmplementeerd om medewerkers meer zelfstandigheid te geven bij wachtwoordbeheer.

9.2.2 Identity Governance Administration

Het HR-systeem wordt tweemaal per dag uitgelezen door OpenText , dat vervolgens provisioning verzorgt naar Entra ID. Bij indiensttreding, ongeacht of het gaat om medewerkers, externen, inhuur en stagiaires, wordt automatisch een account aangemaakt. De leidinggevende ontvangt een notificatie per email. Medewerkers krijgen toegang tot standaardapplicaties en kunnen via functioneel beheer aanvullende applicaties en rechten aanvragen. Er is onderscheid in doelgroepen, zoals: medewerkers, statenleden, commissieleden, trambedrijf, huurders en schoonmaak/housekeeping (alleen toegangspas). Bij uitdiensttreding wordt het account na 7 dagen verwijderd uit een groep, waarmee de licenties vervallen. Vervolgens wordt het hele account na 30 dagen verwijderd.

9.3 Gewenste situatie

9.3.1 BS6.1 Identity and Access Management (IAM)

Entra ID wordt de primaire identity provider en de Active Directory on-premises zal alleen voor legacy doeleinden als identity provider gebruikt worden. Vanuit Active Directory worden alle objecten gesynchroniseerd naar Entra ID zolang Active Directory nodig blijft voor on-premises appicaties die niet tegen Entra ID aan kunnen communiceren. Dit is een zogenaamde Hybrid Identity oplossing. Dit betekent dat de identiteit zowel on-premises gebruikt kan worden als in de Microsoft Cloud.

[3] Zie: https://www.opentext.com/products

De identiteit wordt aangemaakt in het HR-systeem). Een medewerker zal na het opvoeren in het HR-systeem via een automatisch proces aangemaakt worden in de Active Directory. Doordat we gebruik maken van een on-premises Active directory hebben we te allen tijde zelf eigenaarschap en controle over de identiteiten. Met Entra Cloud Sync zal de on-premises Active Directory gesynchroniseerd worden naar Entra ID, zodat hier dezelfde user-objecten beschikbaar zijn. Een aantal groepen worden nu reeds gesynchroniseerd en zullen in de implementatie meegenomen moeten worden.

Conditional Access binnen Microsoft Entra brengt signalen samen en neemt beslissingen en dwingt organisatiebeleid af. Conditional Access policies kunnen toegang geven in combinatie met bepaalde vereisten of juist toegang blokkeren.

9.3.2 BS6.2 Priviledge Identity Management (PIM)

Het beheren van administrator accounts is een belangrijk onderdeel van het moderne identiteitsbeheer. Entra Privileged Identity Management is onderdeel van Entra ID Governance. Entra Privileged Identity Management biedt aanvullende beveiliging voor beheerder accounts die toegang hebben tot resources, Entra, Azure en andere Microsoft-diensten. Door administratieve rollen beschikbaar te stellen die gebaseerd zijn op tijd en goedkeuring wordt voorkomen dat er onnodig, verkeerd of onveilig gebruik kan worden gemaakt van een deze administratieve permissies.

9.3.3 BS6.3 Identity Governance Administration (IGA) (optie)

Microsoft Entra ID Governance[4] is een identiteitsbeheeroplossing waarmee de productiviteit en beveiliging naar een hoger niveau worden gebracht en overzichtelijk kan worden voldaan aan regelgevingsvereisten. Met Entra ID Governance wordt de identiteitslevenscyclus geautomatiseerd, zodat deze vanuit HR automatisch worden onderhouden in zowel Active Directory als Entra ID. Gezien de 'Azure tenzij' strategie is Microsoft Entra ID Governance een logische keuze als vervolgstap. Hier zal tijdens de implementatie nog meer in detail naar moeten worden gekeken in hoeverre deze de huidige OpenText NetIQ IAM functionaliteiten kan invullen.

Door Access Packages in te zetten, in plaats van het automatisch toewijzen van rechten op resources, kan een goedkeuringsflow worden gebruikt en kan er tijdelijk toegang tot een bepaalde resource worden gegeven, zonder dat deze permanent aan de gebruiker is toegewezen. Access Reviews is een onderdeel van Entra ID Governance. Access reviews zorgen ervoor dat groepslidmaatschappen, toegang tot applicaties, access packages of administratieve rol toewijzingen periodiek kunnen worden gecontroleerd om ervoor te zorgen dat alleen de juiste personen toegang hebben.

9.4 Ontwerpbesluiten

Entiteit	Toelichting/Omschrijving	Aard van de verandering
HR-provisioning	Identiteiten vanuit HR-systeem in Active Directory aanmaken en daarna naar Entra ID synchroniseren d.m.v. Entra Connect Cloud sync agents. Zodra er geen applicaties meer met Active Directory afhankelijkheid, de identiteit provisioning direct naar Entra ID realiseren. Ook externen en gast-accounts worden in dit proces meegenomen.	OpenText niet meer gebruikt als primaire platform waar identiteiten vanuit HR-systeem worden aangemaakt.
Primaire identity provider	Inzet van Active Directory en Entra ID als de primaire identity provider met de best practices voor o.a. Entra beveiligingsinstellingen, gast toegang, retentie, Conditional Access framework, Identity Protection en cloud sync. De federatieve koppelingen met SaaS-applicaties dienen te worden omgezet vanuit OpenText.	OpenText wordt niet meer gebruikt als primaire identity provider. Gebruikers zullen dit merken aan de manier waarop ze zich aanmelden, welke authenticatie methodes er

[4] Microsoft Entra ID Governance, Kuppinger cole analists, 16-09-2024

		worden gebruikt en instellen en reset van hun wachtwoord.
Governance	Inzet van Entra ID Governance met provisioning account, access packages voor aanvraag toegang door gebruiker, access reviews om toegang periodiek te controleren, just in time access.	OpenText wordt niet meer gebruikt als Governance oplossing.
RBAC	Inzet van Entra ID Governance om vanuit HR-informatie (type medewerkers, functie, afdeling, domein) het gebruikersaccounts geautomatiseerd te voorzien van basis-toegangsrechten op basis van een rolgebaseerd model (RBAC) zodat beveiligingsrisico's door menselijke autorisatiefouten worden geminimaliseerd.	Correcte HR-registratie medewerker.
Privileged Identity Management	Inzet van Entra Privileged Identity Management inrichten waarbij administrator rollen 'least privilege' aan de juiste beheerders worden gekoppeld en activititeiten worden vastgelegd voor auditing. Tevens worden er access reviews op de groepen geplaatst, zodat er periodieke controle plaatsvindt op de leden van de groepen.	Privileged Identity Management inrichten.
Entitle management aanvraag-procedure	Resources aanbieden in de vorm van een access package met beperkte toegang tot de momenten dat de gebruikers de toegang nodig hebben. Daarnaast kan er een approval flow aan dit proces worden toegevoegd.	Access Packages inrichten en approval flow toevoegen.
Entitle management beoordelings-procedure	Toegang van gebruikers en gasten tot verschillende resources periodiek controleren. Groepseigenaren, managers en/of gasten ontvangen berichten om de toegang te beoordelen. De response op deze berichten in combinatie met de beoordeling, bepaalt wat er met de toegang van het account gebeurt.	Access Reviews inrichten.

10 Informatiebeveiliging services

Dit hoofdstuk beschrijft in meer detail de huidige situatie, verbeterpunten, toekomstige situatie en de verbeterpunten van de *Informatiebeveiliging services*.

10.1 Bouwstenen

De te realiseren ICT- bouwstenen als onderdeel van Informatiebeveiliging services zijn:

- BS7.3 Security baseline (XDR)
- BS7.4 Security Information and Event Management (SIEM)
- BS7.5 Security Operations Center (SOC) (optie)

10.2 Huidige situatie

Het uitgangspunt van de Aanbestedende dienst voor informatiebeveiliging is het Informatiebeveiligingsbeleid, wat gebaseerd is op de NEN/ISO 27001 norm en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO)[5]. De actuele BIO geldt als het minimum basisniveau voor informatiebeveiligingsmaatregelen. De verwachting is dat vanaf Q4 2025 de overheid zich aan de BIO2/CBW moet conformeren. De Aanbestedende dienst beveiligt alle informatie standaard op basisniveau (zie onderstaande tabel afkomstig uit het Informatieveiligheidsbeleid).

Betrouwbaarheidseisen	**Laag** Voor beveiliging mogen geringe kosten worden gemaakt	**Basis** Beveiliging is een criterium naast kosten, effectiviteit etc.	**Hoog** Beveiliging is primair criterium, kosten spelen ondergeschikte rol
Beschikbaarheid	**Wenselijk** Een enkele uitval is aanvaardbaar • 98% per jaar • Max. 1 keer per week • 2 dagen oplostijd	**Noodzakelijk** Nauwelijks uitval • 99% per jaar • Max. 1 keer per maand • 4 uur oplostijd	**Onmisbaar** Slechts in uitzonderlijke gevallen niet operationeel • 99,5 % per jaar • Max. 4 keer per jaar • 4 uur oplostijd
Integriteit	**Actief** Bedrijfsproces tolereert enkele fouten (max. 1 dag verlies van informatie)	**Detecteerbaar** Systemen werken gecontroleerd en fouten worden gesignaleerd (max. 1 dag verlies van informatie)	**Onontbeerlijk** Bedrijfsproces eist foutloze informatie (max. verlies van informatie kleiner dan 1 dag, waarde is afhankelijk van risicoanalyse)
Vertrouwelijkheid	**Openbaar toegankelijk** Informatie hoeft niet afgeschermd te worden	**Intern relevant** Informatie mag alleen ingezien worden door provinciale organisatie	**Gevoelig** Informatie alleen toegankelijk voor direct betrokkenen en/of bedrijfsbelangen worden ernstig geschaad als niet geautoriseer-den toegang krijgen

De huidige informatiebeveiligings-maatregelen zijn gericht op meerdere individuele oplossingen voor netwerk-, werkplek- en office-beveiliging.

[5] Baseline Informatiebeveiliging Overheid (BIO): https://www.bio-overheid.nl/category/producten/bio

10.2.1 SIEM-SOC

Momenteel is er geen integrale Security Information and Event Management (SIEM) oplossing voor de logging van data. Er is ook geen Security Operations Center wat overkoepelend alle meldingen uit de SIEM-oplossing verzamelt, analyseert en oplost. Wel is er in interprovinciaal BIJ12 verband een Computer Security Incident Response Team (CSIRT). Dit voor het geval meldingen van een dusdanig complexe of dreigende aard zijn, bijvoorbeeld bij een ransomware aanval of een e-mail fraudezaak.

10.3 Gewenste situatie

Het uitgangspunt is aan te sluiten op de architectuur en ontwerpprincipes van de Microsoft Cybersecurity Referentie Architectuur (MCRA) en de oplossingen vanuit het Windows 10/11 security platform. De MCRA beschrijft end-to-end de cyberbeveiligingsmogelijkheden van Microsoft. De informatiebeveiliging in deze GAS richt zich primair op informatietechnologie (IT), maar dient uitbreidbaar te zijn naar Operationele Technologie (OT) t.b.v. procesautomatisering van verkeersregelinstallaties, bediening van bruggen en sluizen en gebruik van tunnels.

10.3.1 BS7.3 Security baseline (XDR)

Met de migratie naar de publieke Cloud met Azure en de moderne werkplek Microsoft 365 is de beveiliging op basis van perimeters niet langer voldoende. De Defender XDR-suite van Microsoft dient als security baseline te worden geïmplementeerd voor meerlaagse beveiliging met de oplossingen:

- Defender for Identity
- Defender for Identity Protection
- Defender for Endpoint (werkplekken en servers)
- Defender for Office 365
- Defender for Cloud-apps
- Defender for Cloud

MS E3/E5 Threat Protection	Identity		Applications	Data	Infrastructure
Protect (Security baseline)	**AD / Entra ID**	**Modern Workplace**	**Office 365**		**Azure IaaS/PaaS**
	MFA / Conditional Access	Endpoint Manager MDM/MAM			Defender for Cloud Server
Detect & Respond	Defender for Identity protection Defender for Identity On-prem	Defender for Endpoint	Defender for Microsoft 365	Cloud App Security	Defender for Cloud
	Microsoft Defender XDR Microsoft Sentinel				

Deze producten vormen samen een uniforme security-oplossing, waarbij de componenten (identiteiten, apparaten, applicaties, data, infrastructuur en netwerken) elkaar versterken en signalen correleren. Door correlatie en gebruik van de Defender XDR oplossingen zullen de detecties aanzienlijk verbeterd worden en zijn de inzichten meer gericht vanuit een eXtended Detection and Response (XDR) gedachten.

10.3.2 BS7.4 Security Information and Event Management (SIEM)

Opzetten van een SIEM, waarbij er een centrale SIEM ontstaat voor de logging en borging van events als ook het voldoen van de retentiebehoefte vanuit de regelgeving. Hierbij is Microsoft Sentinel de oplossing, mede door de volgende redenen: dicht bij het Microsoft ecosysteem, integratie met native Microsoft-producten en onderdeel van Defender XDR (uniforme zichtbaarheid voor zowel XDR als SIEM vanuit een centrale portal). Andere niet-Microsoft oplossingen geven vergelijkbare functionaliteiten, maar de samenwerking tussen SIEM en XDR ontbreekt. Met de aanvallen welke steeds geavanceerder worden als ook om efficiënt om te gaan met de kosten en dataoplag, is Microsoft Sentinel de beste keuze gericht op de Zero-trust strategie.

Voor een optimaal functionerende SIEM is het belangrijk zoveel mogelijk loggegevens en netwerkverkeer centraal te verzamelen, vanuit Defender XDR, firewalls en applicaties. Sentinel biedt een breed scala aan playbooks en connectoren voor een makkelijke integratie. Hoe meer informatie, hoe effectiever de SIEM kan reageren op dreigingen, met behulp van frameworks zoals MITRE ATT&CK[6]. Security Orchastration and Automated Response (SOAR) automatiseert de response op dreigingen en ontlast zo security-analisten. Microsoft Sentinel combineert SIEM en SOAR, biedt uitgebreide integratiemogelijkheden en kan voor geautomatiseerde incidentafhandeling binnen de ITSM-tooling zorgen.

10.3.3 BS7.5 Security Operations Center (SOC)

Voor het monitoren van informatiebeveiliging tegen interne en externe dreigingen wordt een extern Security Operations Center (SOC) ingericht. Het SOC voert 24/7 monitoring, detectie en response uit, waaronder het signaleren van hackpogingen, virus- en malware-uitbraken en denial-of-service-aanvallen.Het SOC verricht een initiële impactanalyse, waarbij onderscheid wordt gemaakt tussen 'false positives' en relevante meldingen. Deze meldingen worden zoveel mogelijk geautomatiseerd afgehandeld via playbooks in Microsoft Sentinel. Hiervoor dienen duidelijke afspraken te worden gemaakt over classificatie, prioritering en mandaat (zoals het Stekermandaat), waaronder de bevoegdheid van het SOC om in specifieke situaties zelfstandig maatregelen te nemen. Bij meldingen van een complexe of ernstige aard, zoals ransomware-aanvallen, kan de Aanbestedende dienst een beroep doen op een Computer Security Incident Response Team (CSIRT). In interprovinciaal verband (IPO/BIJ12) is een principebesluit genomen om aan te sluiten bij het CSIRT van het Nationaal Cyber Security Centrum (NCSC). Tevens wordt binnen IPO/BIJ12 onderzocht of SOC-diensten gezamenlijk kunnen worden ingekocht voor de provincies.

10.4 Ontwerpbesluiten

Entiteit	Toelichting/Omschrijving	Aard van de verandering
Beveiliging on-premises IaaS	Inzet Azure Arc voor de onboarding van Defender for Endpoint en later met de uitbreiding voor Windows Updates en meer.	Voorbereiding on-premises IaaS om te voldoen aan de regelgeving qua auditing en logging.
Beveiliging apparaten	Inzet Defender for Endpoint is de tool voor zowel AV als EDR. Hierbij zal Defender for Endpoint de dekking geven voor AV/ EDR/ Network Protection en aanvullende hardening als ASR en Firewall.	Migratie naar Defender for Endpoint, met daarbij ook de benodigde hardening als ASR en Firewall.
Beveiliging Office365	Inzet Defender for Office voor de beveiliging van e-mail, anti-phishing/anti-spam oplossing en link en bijlage beveiliging.	Toevoeging van Office 365 aan de zichtbaarheid.
Beveiliging Identiteiten	Inzet Defender for Identity voor invulling on-prem identity beveiliging en monitoring domain controllers.	Toevoeging van identiteit aan de zichtbaarheid.
Beveiliging Cloud apps	Inzet Defender for Cloud Apps voor inzicht en control shadow-IT en cloud applicatie (SaaS) monitoring.	Toevoeging van Cloud apps aan de zichtbaarheid.
Security Information &Event Management (SIEM)	Inzet Azure Sentinel voor detectie- en analysesysteem op security incidenten.	Verhogen zichtbaarheid.
Security Operations Center (SOC)	Inzet extern SOC voor proactieve bescherming en mitigatie dreigingen binnen Aanbestedende dienst.	Verhogen veiligheid.

[6] Zie: https://attack.mitre.org/

11 Applicatie services

Dit hoofdstuk beschrijft in meer detail de huidige situatie, verbeterpunten, toekomstige situatie en de verbeterpunten van de *Applicatie services*.

11.1 Bouwstenen

De te realiseren ICT- bouwstenen als onderdeel van Applicatie services zijn:
- BS8.1 Onboarden workload: Dataplatform (*project Dataplatform*)
- BS8.2 Onboarden workload: IaaS-applicaties
- BS8.3 Onboarden workload: GIS-platform
- BS8.4 Enterprise Service Bus (ESB)

11.2 Huidige situatie

11.2.1 Dataplatform
Het huidige dataplatform is opgezet in Azure met: Azure Data Factory, Azure Data Lake Storage Gen2, Azure SQL Server en Azure DevOps.

11.2.2 IaaS-applicaties
Het overzicht met de huidige IaaS-server Applicaties is opgenomen in Bijlage 1.

11.2.3 GIS-platform
Het GIS-platform ArcGis is momenteel gevirtualiseerd op VMware in het datacenter in het provinciehuis vanwege latency en performance problemen. Hierop draait het databaseplatform (Postgres-SQL), ArcGIS Enterprise, GeoWeb, Apollo Raster server, BGT-beheersysteem en dataopslag. Daarnaast worden een aantal SaaS-oplossingen gebruikt, zoals: GeoBRK, GeoHR, ArcGIS Online en Tygron. Aanbestedende dienst maakt reeds gebruikt van de ArcGis service georiënteerde architectuur, waarbij data wordt ontsloten via webservices. Laptops voorzien van de grafische desktop software zijn zwaarder uitgevoerd en software draait dus lokaal.

11.2.4 Enterprise Service Bus (ESB)
Momenteel wordt gebruik gemaakt van een ESB-integratieplatform van Itrajectum genaamd Easy bus. De ESB (Enterprise Service Bus) is een gecentraliseerd platform wat datastromen uit verschillende systemen ontvangt, transformeert en aflevert. Het biedt daarmee uniforme koppelingen van verschillende en zowel interne als externe systemen. Dit initiatief is opgestart vanuit BIJ12. Momenteel zijn hier koppelingen op actief, waaronder de Digikoppeling, IBAN-check, BRP-zoekopdracht, E-formulieren en documentregistratie in zaaksysteem. Digikoppeling is een set van standaarden en protocollen om koppelingen te realiseren tussen overheidssystemen. Deze standaarden zijn vastgesteld door Logius.

11.3 Gewenste situatie

11.3.1 BS8.1 Onboarden workload: Dataplatform
Voor de toekomstige inrichting van het dataplatform wordt Microsoft Fabric ingezet als SaaS-dienst. De oplossing gebruikt een eigen tenantstructuur die rechtstreeks is gekoppeld aan de Entra-tenant van de Aanbestedende dienst. Fabric maakt gebruik van Microsoft Entra voor authenticatie, voorwaardelijke toegang, encryptie (in rust en tijdens transport) en voldoet aan relevante compliance vereisten, waaronder de AVG.

11.3.2 BS8.2 Onboarden workload: IaaS-applicaties
Applicaties worden, op basis van de Cloud Readiness Scan (6R-model), waar mogelijk ver-SaaS-ed of gemigreerd naar Azure, afhankelijk van het applicatie-migratiescenario (bijvoorbeeld lift & shift of rebuild). Uit de Azure Migrate Assessment blijkt dat alle IaaS-applicaties technisch kunnen worden gemigreerd naar Azure.

De verwachting is dat er geen applicaties zijn met het beveiligingsniveau BBN-3, wat betekent dat migratie naar Azure in principe voor alle Applicaties is toegestaan. Het aantal virtuele machines (VM's) dat naar Azure dient te worden gemigreerd, ligt lager dan het huidige aantal VM's door:

- **Uitfasering**: zoals Documentum en vervanging 3 fysieke Oracle-servers door SQL-servers;
- **Vervanging**: bepaalde functies zoals identity & access management (IAM), monitoring, beveiliging en back-up worden als Cloud diensten afgenomen en vereisen daardoor geen aparte infrastructuur meer.
- **Ver-SaaS-ing**: zoals IaaS-applicaties vervangen door SaaS-applicaties.

Zie de toekomstige IaaS-serverapplicaties is in Bijlage 1.

11.3.3 BS8.3 Onboarden workload: GIS-platform

ArcGIS kan, conform de documentatie van zowel Esri als Microsoft[7], technisch worden gehost binnen Microsoft Azure. De SaaS-variant, is volgens Esri functioneel onvoldoende toereikend voor toepassingen waarbij veel verschillende databronnen worden geïntegreerd. Bovendien adviseert Esri expliciet het gebruik van ArcGIS in combinatie met een Virtual Desktop Infrastructure (VDI). Binnen Azure betreft dit Azure Virtual Desktop (AVD).

De architectuur in Figuur 8 toont op hoofdlijnen hoe een volledig ArcGIS-platform in Azure kan worden ingericht. Dit omvat zowel front-end (AVD) als back-end componenten, zoals ArcGIS Enterprise, waarmee een compleet GIS-platform in de cloud gerealiseerd wordt. De Figuur toont niet alle componenten van het GIS-platform van de Aanbestedende dienst (ca. 15 productieservers). Azure-diensten zoals automatische start/stop en auto-scaling zijn compatibel met deze configuratie.

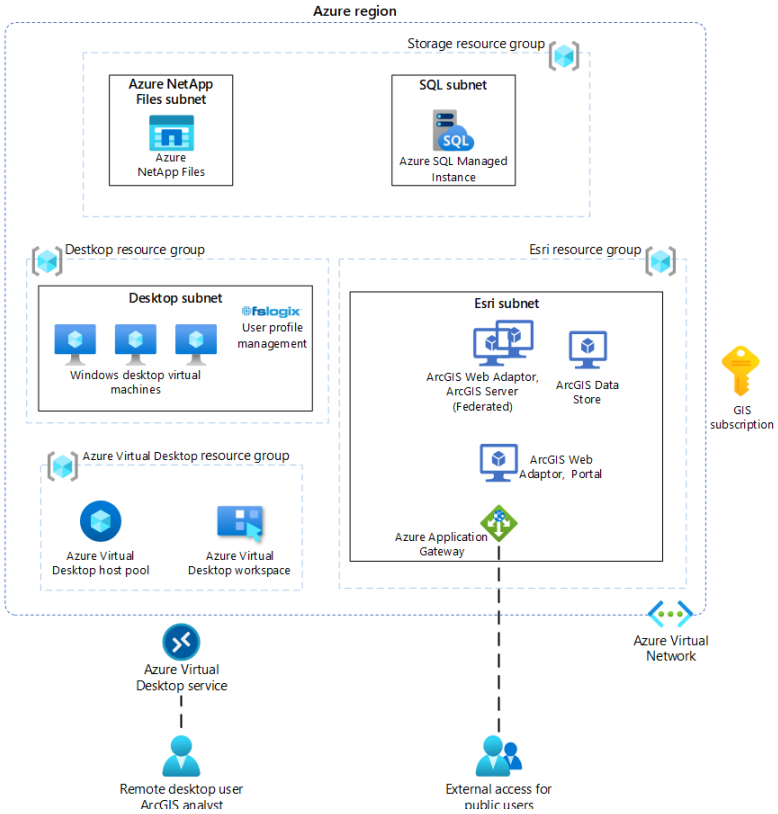
Voor rekenkracht en grafische prestaties adviseert Esri gebruik te maken van de volgende VM-series:

- NV32-series: geschikt voor zware 3D-rendering en grote datasets met complexe analyses;
- NVadsA10_v5-series: met NVIDIA GPU's, gericht op deep learning-toepassingen.

Een belangrijk aandachtspunt is het gebruik van de lokale schijf van de virtuele machines (C:), aangezien synchronisatie met OneDrive niet wordt ondersteund in deze context.

Er zijn vergelijkbare implementaties gerealiseerd bij andere overheden, waaronder Provincie Gelderland (Azure) en Noord-Holland (in AWS), waarmee de technische haalbaarheid en toepasbaarheid zijn aangetoond. Tijdens de Implementatie zal proefondervindelijk moeten worden vastgesteld (PoC, Pilot) of dit ook voor Aanbestedende dienst mogelijk is en met welk Migratie scenario en de volgordelijkheid daarvan; lift-and-shift- of rebuild. Bij rebuild wordt gebruik gemaakt van cloud-native oplossingen zoals SQL PaaS en Azure Storage. Hierbij dient ook de applicatieconfiguratie te worden aangepast, bijvoorbeeld wat betreft pad structuren.

[7] ArcGIS: https://enterprise.arcgis.com/en/server/latest/cloud/azure/overview-arcgis-server-on-microsoft-azure.htm
Microsoft: https://learn.microsoft.com/nl-nl/azure/architecture/example-scenario/data/esri-arcgis-azure-virtual-desktop



Figuur 7 – ArcGis in Azure met Azure Virtual Desktop

11.3.4 BS8.4 Enterprise Service Bus (ESB)

In de toekomstige architectuur wordt gekozen voor een hybride integratieoplossing, waarbij de bestaande Easy Bus behouden blijft. Dit is niet alleen vanwege de aanwezige koppelingen, maar expliciet als onderdeel van een exit-strategie vanuit Azure. Nieuwe SaaS-koppelingen worden gerealiseerd via Azure APIM, terwijl Easy Bus verantwoordelijk blijft voor de verwerking van bestaande en minder veranderlijke koppelingen, zoals Digikoppelingen. Met Azure API Management kunnen API's (Application Programming Interfaces) op een veilige manier worden gepubliceerd, beheerd, beveiligd en gemonitord — zowel intern als extern. API's kunnen draaien in Azure, on-premises of andere clouds en worden beheerd via één centraal platform. Azure API Management fungeert hierbij als een gateway tussen backend-services en de gebruikers van API's, zoals applicaties, ketenpartners of andere systemen. Deze opzet biedt maximale flexibiliteit en keuzevrijheid, dankzij de duidelijke scheiding tussen cloud- en niet-cloudintegraties.

11.4 Ontwerpbesluiten

Entiteit	Toelichting/Omschrijving	Aard van de verandering
Fabriq SaaS	Aansluiten Fabric SaaS op Entra Tenant.	Aansluiten Fabric SaaS.
IaaS-applicaties in Azure	Applicaties worden, op basis van 6R-model ver-SaaS-ed of gemigreerd naar Azure.	Migratie applicaties.
GIS-platform	ArcGis Pro in Azure met Azure Virtual Desktop.	Migratie GIS-platform.
Azure APIM	Hybride integratieoplossing, met bestaande Easy Bus vanuit exit-strategie voor de verwerking van bestaande en minder veranderlijke koppelingen, zoals Digikoppelingen en Azure APIM voor nieuwe SaaS-koppelingen.	Enterprise Service Bus met exit-strategie.

Bijlage 1: IaaS-applicaties

Platform	Test/ productie	Type	Migr-atie	vCPUs	vRAM (GB)	Provisioned Space (GB)	Used Space (GB)	Network adapters	Disk Count	Azure VM readiness	Compute monthly cost est.EUR	Storage monthly cost est. EUR	Estimated monthly savings Azure Hybrid Benefit WinOS	Security readiness	Security monthly cost est. EUR	Categorie
Nutanix	P	Beheer	Ja	1	4	540	193	7	3	Ready	393,61	36,62	0	Ready	13,08	PVM KleinLinux
Nutanix	P	GIS	Ja	2	8	120	29	1	2	Ready	75,84	8,44	30,08	Not Ready	0	PVM MiddelWindows
Nutanix	P	SAP	Ja	2	8	160	83	1	2	Ready	122,92	14,12	60,15	Ready	13,08	PVM MiddelWindows
Nutanix	P	LIAS	Ja	1	8	95	35	1	3	Ready	75,84	6,74	30,08	Not Ready	0	PVM kleinWindows
Nutanix	P	SQL	Ja	2	16	310	118	1	3	Ready	75,84	21,09	30,08	Not Ready	0	PVM MiddelWindows
Nutanix	P		Ja	2	4	100	35	1	3	Ready	66,69	7,79	30,08	Not Ready	0	PVM MiddelWindows
Nutanix	P		Ja	8	64	5100	21	1	2	Ready	122,92	367,97	60,15	Ready	13,08	PVM DocumentumWindows
Nutanix	P	GIS	Ja	2	12	80	59	1	2	Ready	122,92	8,44	60,15	Ready	13,08	PVM MiddelWindows
Nutanix	P	SQL	Ja	2	16	210	39	1	5	Ready	122,92	14,77	60,15	Ready	13,08	PVM MiddelWindows
Nutanix	P	DC	Ja	2	8	125	50	1	2	Ready	75,84	7,79	30,08	Not Ready	0	PVM MiddelWindows
Nutanix	P	DC	Ja	2	8	125	43	1	2	Ready	75,84	7,79	30,08	Not Ready	0	PVM MiddelWindows
Nutanix	P	Beheer	Ja	2	8	170	117	1	2							PVM MiddelWindows
Nutanix	T	LIAS	Ja	1	8	95	28	1	2	Ready	75,84	6,74	30,08	Not Ready	0	TVM KleinWindows
Nutanix	T	LIAS	Ja	1	4	96	24	1	2	Ready	66,69	6,81	30,08	Not Ready	0	TVM KleinWindows
Nutanix	T	SQL	Ja	2	8	180	117	1	2	Ready	122,92	14,12	60,15	Ready	13,08	TVM KleinWindows
Nutanix	T	Burg. ben.	Ja	2	8	100	31	1	2	Ready	75,84	7,79	30,08	Not Ready	0	TVM KleinWindows
Nutanix	T	Blue Dolphin	Ja	1	4	131	29	1	2	Ready	122,92	9,97	60,15	Ready	13,08	TVM KleinWindows
VMWare	P	GIS	Ja	4	26	1327	1327	1	2							PVM GrootLinux
VMWare	P	GIS	Ja	2	16	147	147	1	2	Ready	75,84	9,18	30,08	Not Ready	0	PVM MiddelWindows
VMWare	P	GIS	Ja	2	8	209	209	1	2	Ready	75,84	14,22	30,08	Not Ready	0	PVM MiddelWindows

VMWare	P	GIS	Ja	4	16	177	177	1	2	Ready	122,92	11,34	60,15	Ready	13,08	PVM GrootWindows
VMWare	P	GIS	Ja	4	16	267	267	1	2	Ready	122,92	17,81	60,15	Ready	13,08	PVM GrootWindows
VMWare	P	GIS	Ja	4	32	283	283	1	2	Ready	286,38	17,81	120,31	Ready	13,08	PVM DocumentumWindows
VMWare	P	GIS	Ja	4	12	513	513	1	2	Ready	122,92	35,79	60,15	Ready	13,08	PVM GrootWindows
VMWare	P	GIS	Ja	4	32	283	283	1	2	Ready	143,19	17,81	60,15	Ready	13,08	PVM DocumentumWindows
VMWare	P	GIS	Ja	2	16	97	97	1	2	Ready	75,84	5,58	30,08	Not Ready	0	PVM MiddelWindows
VMWare	P	GIS	Ja	2	12	3657	3657	1	2	Ready	84,34	261,91	30,08	Not Ready	0	PVM MiddelWindows
VMWare	P	GIS	Ja	1	4	105	105	1	2	Ready	75,84	7,79	30,08	Not Ready	0	PVM KleinWindows
VMWare	P	GIS	Ja	4	8	239	239	1	2	Ready	122,92	19,15	60,15	Ready	13,08	PVM GrootWindows
VMWare	P	GIS	Ja	4	16	177	177	1	2	Ready	122,92	11,34	60,15	Ready	13,08	PVM GrootWindows
VMWare	P	GIS	Ja	2	4	84	84	1	2	Ready	66,69	7,02	30,08	Not Ready	0	PVM MiddelWindows
VMWare	P	GIS	Ja	4	8	289	289	1	2	Ready	75,84	22,75	30,08	Not Ready	0	PVM GrootWindows
VMWare	P	GIS	Ja	2	8	199	199	1	2	Ready	75,84	13,5	30,08	Not Ready	0	PVM MiddelWindows
VMWare	P	GIS	Ja	4	32	273	273	1	2	Ready	122,92	17,09	60,15	Ready	13,08	PVM DocumentumWindows
VMWare	T	GIS	Ja	2	24	725	725	1	2							TVM KleinLinux
VMWare	T	GIS	Ja	2	12	113	113	1	2	Ready	75,84	7,02	30,08	Not Ready	0	TVM KleinWindows
VMWare	T	GIS	Ja	2	8	119	119	1	2	Ready	122,92	7,74	60,15	Ready	13,08	TVM KleinWindows
VMWare	T	GIS	Ja	4	18	119	119	1	2	Ready	122,92	7,02	60,15	Ready	13,08	TVM KleinWindows
VMWare	T	GIS	Ja	2	8	509	509	1	2	Ready	84,34	17,81	30,08	Not Ready	0	TVM KleinWindows
VMWare	T	GIS	Ja	4	18	179	179	1	2	Ready	122,92	11,34	60,15	Ready	13,08	TVM KleinWindows
VMWare	T	GIS	Ja	4	16	177	177	1	2	Ready	122,92	11,34	60,15	Ready	13,08	TVM KleinWindows
VMWare	T	GIS	Ja	1	4	105	105	1	2	Ready	75,84	7,02	30,08	Not Ready	0	TVM KleinWindows
VMWare	T	GIS	Ja	2	8	149	149	1	2	Ready	122,92	9,9	60,15	Ready	13,08	TVM KleinWindows
Fysiek	P	Oracle	Nee													
Fysiek	P	Oracle	Nee													
Fysiek	T	Oracle	Nee													

Nutanix	P	IAM	Nee	2	16	115	26	2	2							PVM MiddelLinux
Nutanix	P	IAM	Nee	2	16	100	18	2	1							PVM MiddelLinux
Nutanix	P	IAM	Nee	1	3	40	18	1	1	Ready	69,31	4,22	0	Not Ready	0	PVM kleinLinux
Nutanix	P	Wiki	Nee	1	2	32	28	1	1							PVM kleinLinux
Nutanix	P	Zen-works	Nee	8	16	440	263	1	2	Ready	125,54	33,61	0	Ready	13,08	PVM GrootLinux
Nutanix	P	Zen-works	Nee	2	16	1000	19	1	1							PVM MiddelLinux
Nutanix	P	Beheer	Nee	1	2	100	15	1	1							PVM kleinLinux
Nutanix	P	Zen-works	Nee	2	8	76	17	1	2	Ready	85,52	5,27	0	Not Ready	0	PVM MiddelLinux
Nutanix	P	Oracle	Nee	2	18	300	141	1	3							PVM MiddelLinux
Nutanix	P	Zen-works	Nee	8	16	440	235	1	2	Ready	125,54	33,61	0	Ready	13,08	PVM GrootLinux
Nutanix	P	IAM	Nee	2	8	80	5	1	1	Ready	69,31	8,44	0	Not Ready	0	PVM MiddelLinux
Nutanix	P	IAM	Nee	2	16	312	27	1	2	Ready With Conditions	62,77	33,75	0	Ready With Conditions	13,08	PVM MiddelLinux
Nutanix	P		Nee	2	24	380	74	1	2							PVM MiddelLinux
Nutanix	P	IAM	Nee	2	8	60	15	1	1	Ready	124,88	4,22	0	Ready	13,08	PVM MiddelLinux
Nutanix	P	IAM	Nee	2	16	60	26	1	1	Ready	105,27	4,22	0	Ready	13,08	PVM MiddelLinux
Nutanix	P	IAM	Nee	2	16	80	7	1	1	Ready	116,38	8,44	0	Ready	13,08	PVM MiddelLinux
Nutanix	P	IAM	Nee	2	16	115	25	1	2	Ready	85,52	8,44	0	Not Ready	0	PVM MiddelLinux
Nutanix	P	LIAS	Nee	2	4	96	30	2	3	Ready	122,92	6,81	60,15	Ready	13,08	PVM MiddelWindows
Nutanix	P	Docu-mentum	Nee	2	8	1363	29	2	3	Ready	122,92	100,5	60,15	Ready	13,08	PVM MiddelWindows
Nutanix	P	Docu-mentum	Nee	2	8	163	29	2	2	Ready	122,92	14,26	60,15	Ready	13,08	PVM MiddelWindows
Nutanix	P	Beheer	Nee	1	2	80	74	2	2	Ready	122,92	7,02	60,15	Ready	13,08	PVM kleinWindows

Nutanix	P	Docu-mentum	Nee	2	8	233	128	2	4	Ready	122,92	17,09	60,15	Ready	13,08	PVM MiddelWindows
Nutanix	P	Docu-mentum	Nee	2	4	121	73	2	3	Ready	75,84	9,97	30,08	Not Ready	0	PVM MiddelWindows
Nutanix	P	Beheer	Nee	8	32	100										
Nutanix	P	Assyst	Nee	2	16	140	77	1	3	Ready	143,19	9,9	60,15	Ready	13,08	PVM MiddelWindows
Nutanix	P	Beheer	Nee	2	16	180	123	1	2	Ready	75,84	14,12	30,08	Not Ready	0	PVM MiddelWindows
Nutanix	P	Beheer	Nee	2	8	100	28	1	2	Ready	75,84	7,79	30,08	Not Ready	0	PVM MiddelWindows
Nutanix	P	Beheer	Nee	2	8	531	209	1	2	Ready	66,69	40,73	30,08	Not Ready	0	PVM MiddelWindows
Nutanix	P	Docu-mentum	Nee	2	64	620	103	1	2	Ready	268,07	42,18	120,31	Ready	13,08	PVM MiddelWindows
Nutanix	P	PowerBI	Nee	4	16	1280	255	1	3	Ready	245,84	87,49	120,31	Ready	13,08	PVM GrootWindows
Nutanix	P	PowerBI	Nee	4	32	381	42	1	4	Ready	122,92	28,43	60,15	Ready	13,08	PVM DocumentumWindows
Nutanix	P	Beheer	Nee	2	8	633	98	1	4	Ready	122,92	42,18	60,15	Ready	13,08	PVM MiddelWindows
Nutanix	P	Print	Nee	8	8	180	55	1	3	Ready	122,92	14,12	60,15	Ready	13,08	PVM GrootWindows
Nutanix	P	FS	Nee	4	32	3321	2428	1	7	Ready	133,38	238,37	60,15	Ready	13,08	PVM DocumentumWindows
Nutanix	P	AV	Nee	2	8	181	35	1	2							PVM MiddelWindows
Nutanix	P	Print	Nee	4	8	180	23	1	3	Ready	122,92	14,12	60,15	Ready	13,08	PVM GrootWindows
Nutanix	P	SQL	Nee	4	16	125	34	1	3	Ready	85	8,44	60,15	Ready	13,08	PVM GrootWindows
Nutanix	p	Docume ntum	Nee	2	16	11000	8908	2	3	Ready	122,92	1527,28	60,15	Ready	13,08	pVM MiddelWindows
Nutanix	p	Docu-mentum	Nee	6	32	580	207	2	5	Ready	143,19	163,07	60,15	Ready	13,08	pVM DocumentumWindows
Nutanix	P		Nee	2	16	5080	1005	1	2	Ready	122,92	367,97	60,15	Ready	13,08	PVM MiddelWindows
Nutanix	p	Print	Nee	4	8	180	29	1	3	Ready	122,92	14,12	60,15	Ready	13,08	pVM GrootWindows
Nutanix	P	Backup	Nee	1	4	111	87	2	2	Ready	75,84	7,86	30,08	Not Ready	0	PVM KleinWindows
Nutanix	P	CA	Nee	2	8	190	28	1	2							PVM MiddelWindows
Nutanix	P	CA	Nee	2	8	190	25	1	3	Ready	75,84	13,54	30,08	Not Ready	0	PVM MiddelWindows
Nutanix	P		Nee	2	4	480	382	1	3							PVM MiddelWindows

Nutanix	P	Beheer	Nee	4	16	140	121	1	2							PVM GrootWindows
Nutanix	T	IAM	Nee	2	8	115	24	2	2							
Nutanix	T	IAM	Nee	2	8	100	9	2	1							
Nutanix	T	IAM	Nee	2	8	80	5	1	1	Ready	69,31	8,44	0	Not Ready	0	TVM KleinLinux
Nutanix	T	IAM	Nee	2	8	92	27	1	2	Ready With Conditions	56,3	8,44	0	Ready With Conditions	13,08	TVM KleinLinux
Nutanix	T	IAM	Nee	1	4	40	10	1	1	Ready	85,52	4,22	0	Not Ready	0	TVM KleinLinux
Nutanix	T	IAM	Nee	2	16	100	17	1	2							TVM KleinLinux
Nutanix	T	IAM	Nee	2	8	100	16	1	1	Ready	124,88	8,44	0	Ready	13,08	TVM KleinLinux
Nutanix	T	IAM	Nee	2	4	60	21	1	1	Ready	69,31	4,22	0	Not Ready	0	TVM KleinLinux
Nutanix	T	IAM	Nee	2	8	115	25	1	2	Ready	85,52	8,44	0	Not Ready	0	TVM KleinLinux
Nutanix	T	Beheer	Nee	2	16	230	30	1	2	Ready	75,84	19,15	30,08	Not Ready	0	TVM KleinWindows
Nutanix	T	DC	Nee	1	8	110	35	1	2							TVM KleinWindows
Nutanix	T	DC	Nee	1	8	110	31	1	2							TVM KleinWindows
Nutanix	T	Assyst	Nee	2	8	140	73	1	2	Ready	122,92	9,9	60,15	Ready	13,08	TVM KleinWindows
Nutanix	T	Docu-mentum	Nee	2	64	17242	10154	1	2	Ready	572,76	1239,81	240,61	Ready	13,08	TVM KleinWindows
Nutanix	T	Oracle	Nee	2	16	125	25	1	3	Ready	75,84	8,44	30,08	Not Ready	0	TVM KleinWindows
Nutanix	T	Beheer	Nee	2	16	120	30	1	2							TVM KleinWindows
VMWare	P	Beheer	Nee	1	8	158										
VMWare	P	Beheer	Nee	2	16	232				Ready	147,77	15,08	0	Ready	13,08	
VMWare	P	Beheer	Nee	8	16	272				Ready	73,88	17,38	0	Ready	13,08	
VmWare	P	Beheer	Nee	8	32	100										
VMWare	P	Beheer	Nee	2	16	266										
VMWare	P	Beheer	Nee	4	16	1,13 tb				Ready With	245,84	9,9	120,31	Ready With Conditions	13,08	

										Conditions						
VMWare	P	Docu-mentum	Nee	4	16	2077	2077	1	2	Ready	122,92	139,2	60,15	Ready	13,08	PVM GrootWindows
VMWare	P	Beheer	Nee	2	16	236										
VMWare	P	Beheer	Nee	2	32	383										
VMWare	P	Zen-works	Nee	2	16	346				Ready	122,92	22,56	60,15	Ready	13,08	