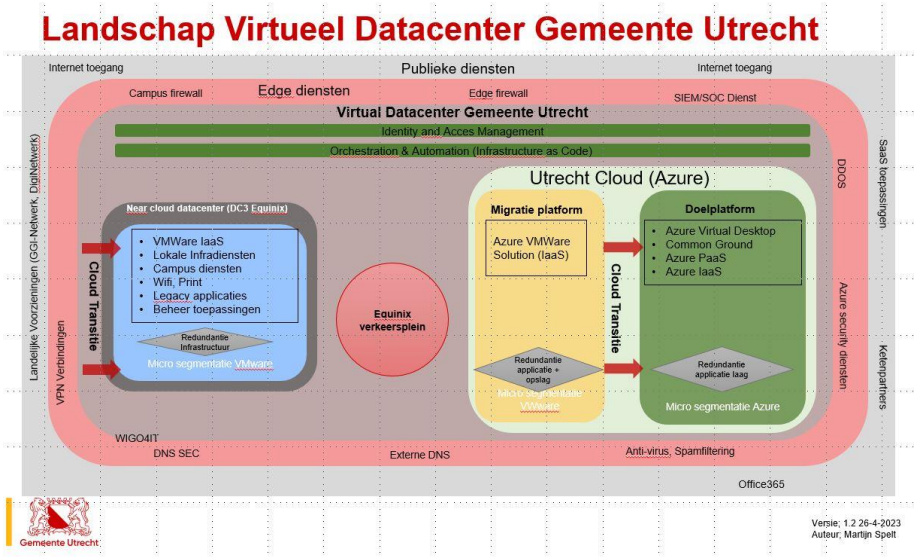
8 BIJLAGEN

8.1 VIRTUEEL DATACENTER OVERZICHT

Onderstaande architectuur geeft een hoog over beeld van het ICT-landschap van Gemeente Utrecht, en de daarbij behorende diensten en componenten. Verdere informatie wordt in de volgende paragrafen gegeven, eventuele detail vragen kunnen aan het team architectuur worden gesteld.



Figuur 1 Landschap virtueel datacenter Gemeente Utrecht

8.2 BESCHRIJVING VIRTUEEL DATACENTER GEMEENTE UTRECHT

Deze bijlage geeft een algemene beschrijving van de inrichting van het virtuele datacenter zoals boven weergeven en kan met externe partijen worden gedeeld als zijnde achtergrond informatie bij offertetrajecten en/of aanbestedingen.

De gemeente bevindt zich in een Cloud transitie programma, het eigen datacenter wordt naar een near-cloud datacenter en Azure VMWare overgezet en aansluitend vindt een applicatie transitie plaats van IaaS naar SaaS, Common Ground en/of Azure native omgeving. Dit is een langlopend programma.

8.2.1 Algemeen

De door de leverancier aan te bieden ICT Prestatie dient aan te sluiten op de binnen de Gemeente Utrecht geldende standaards ten aanzien van de ICT-infrastructuur.
In onderstaande beschrijving worden deze infrastructuur verder beschreven.

De beschreven infrastructuur en componenten zijn aan verandering onderhevig mede vanwege de Cloud transitie, onderstaande beschrijving is een momentopname en wordt twee keer per jaar geactualiseerd. De beschrijving kan op punten afwijken van de actuele situatie.

8.2.2 Gebruikers en ketenpartners

Utrecht kent ongeveer 7200 medewerkers welke beschikken over een Utrecht inlogaccount. Vaste medewerkers krijgen de beschikking over een beheerde laptop. Er is voor een groep vaste ketenpartners (zoals BGHU, RIEC) welke veelvuldig toepassingen vanuit Utrecht gebruiken een ketenpartner proces om Utrecht identiteiten uit te geven. Er wordt een hybride werken concept toegepast, werk kan zowel op kantoor als een thuis locatie plaatsvinden.

8.2.3 Kantoor locaties (Campus)

De gemeente Utrecht kent diverse locaties, het Stads Kantoor Utrecht (SKU) is de hoofdlocatie, de overige locaties zijn verspreid over het verzorgingsgebied van de gemeente Utrecht. De locaties zijn voorzien van enkele werkplekken (bijv. zwembaden, begraafplaatsen) of honderden zoals het SKU en Stadhuis.
Het campus netwerk op de locaties is voorzien van WIFI voor mobiele apparaten, het WIFI netwerk kent een gesloten deel op basis van GOVROAM en een openbaar toegankelijk wifi netwerk, het openbare deel is alleen beschikbaar op de publieksverdiepingen. Vaste apparaten (zoals vaste werkplekken, printers enz.) maken gebruik van een bekabeld netwerk, toelating op het bekabelde netwerk vindt plaats middels authenticatie (802.1x). Het beleid m.b.t. het aansluiten van apparaten is Wifi tenzij.

8.2.4 Server hosting (datacenters)

De Gemeente Utrecht kent een Near Cloud datacenter (extern gehost) op basis van VMWare virtualisatie en een public Cloud omgeving op basis van Microsoft Azure, hierbinnen is voor IaaS zowel Azure VMWare (op basis van NSX-T) als Azure native hosting beschikbaar. De Azure en Near Cloud omgevingen vormen samen het Utrecht virtuele datacenter en zijn middels een verkeersplein oplossing met elkaar verbonden.

8.2.5 Verkeersplein (connectiviteit)

Utrecht maakt gebruik van een centrale verkeersplein oplossing, hier worden alle externe verbindingen gekoppeld zoals GGI-netwerk, internet en de verbindingen (Express route) met Azure en het campus. Deze omgeving bevat tevens Edge security functionaliteit zoals een Next Generation firewall.

8.2.6 Microsoft Azure

De gemeente Utrecht heeft de beschikking over één Microsoft Azure omgeving , ingericht conform de Microsoft Enterprise Scale Hub-Spoke architectuur. Er is een directe synchronisatie tussen de Utrecht directory en Azure AD. Er wordt gebruik gemaakt van Azure policies voor beveiliging beleid o.a. BIO, ISO27001 en beheerders policies. Subscriptions in de tenant zijn onder te verdelen in 3 hoofdgroepen;

1. Platform
    a. Centrale connectiviteit, identiteit en management diensten

2. Landing zone
    a. Locatie van de Azure diensten voor de organisatie
3. Sandboxes
    a. Geïsoleerde omgevingen voor ontwikkel en test trajecten
        i. Deze sandboxes zijn afgeschermd van de overige Azure omgeving.

Als onderdeel van de landing zone is een omgeving ingericht voor IaaS op basis van Azure VMWare Solutions, dit is netwerk technisch een extensie van het Near Cloud datacenter. Azure VMWare is voorzien van vSAN opslag en NetApp Cloud Volumes ONTAP voor de opslag van data en informatie.

8.2.7 Azure Automation

Binnen de Azure omgeving wordt zoveel mogelijk geautomatiseerd gewerkt, hiervoor wordt gebruikt van pipelines en Azure Devops CI/CD.

8.2.8 Near Cloud datacenter

Het netwerk binnen het Near Cloud datacenter is opgebouwd conform het SDDC concept, netwerk virtualisatie wordt gerealiseerd met behulp van VMWare NSX-T. Dit netwerk is uitgebreid naar de Azure VMWare omgeving. Microsegmentatie en zero trust worden als concept toegepast, er wordt gebruik gemaakt van 802.1X authenticatie. VMWare wordt als hypervisor gebruikt, het Near Cloud datacenter is voorzien van een Pure storage opslag platform.

8.2.9 Netwerkvirtualisatie en zero trust

Utrecht volgt het zero trust concept met segmentatie waar benodigd. ICT-systemen worden op basis van functie, locatie en gebruik gescheiden van elkaar. Hiervoor is op het VMWare platform NSX-T beschikbaar. Binnen Azure native wordt er gebruik gemaakt van NSG's en USG's voor netwerkscheiding.

8.2.10 Container platform (Otomi)

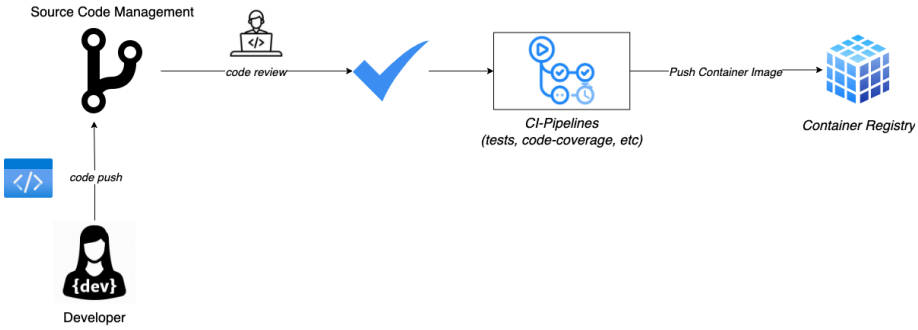
Utrecht heeft een PaaS platform voor Docker containers beschikbaar binnen de Azure tenant. Deze is gebaseerd op Azure Kubernetes met daar boven op een open source multitenancy toolset. Dit platform is onderdeel van de Azure omgeving van Gemeente Utrecht en Haven compliant ingericht, Kubernetes is een subscription binnen deze tenant. Er is een acceptatie en productie omgeving welke identiek ingericht zijn. Daarnaast is er een ontwikkel en test omgeving, deze zijn enkelvoudig ingericht.

CI/CD straat

Utrecht maakt gebruik van Git lab (Gemeente Utrecht · GitHub) hierop worden nieuwe of bestaande projecten gepubliceerd.

CI proces

De exacte stappen en processen kunnen per type applicatie verschillen, maar over het algemeen bevat een CI-pipeline in ieder geval de volgende stappen:



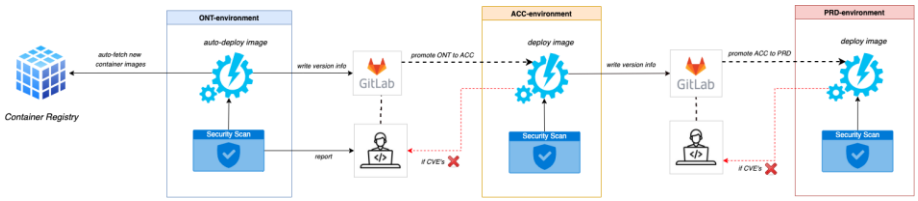
Er wordt voor de uitrol gebruik gemaakt van Helm charts, deze worden bij een leverancier door deze beschikbaar gesteld. Voor applicaties die worden opgeleverd door leveranciers, geldt dat de CI-pipelines ook beheerd worden door de betreffende leverancier (op hun eigen infrastructuur). Voor applicaties die in-house ontwikkeld worden, zullen de CI-pipelines in Git lab ingericht worden door Utrecht.

Ieder productteam krijgt de beschikking over een eigen Git lab project met daarin alle benodigde deployment configuratie. Via dit Git lab project kunnen zij hun applicaties deployen naar de acceptatie- en productieomgeving. Deployments naar de ontwikkelomgeving gebeuren geheel automatisch zodra er een container image in de container registry geüpload wordt.

CD-pipelines

Onder Continuous Delivery vallen de geautomatiseerde stappen en processen die een deploybaar artifact (het resultaat vanuit de CI-pipeline) uitrollen op de doelomgeving (bijvoorbeeld een container image welke uitgerold wordt op een Kubernetes cluster).

Hieronder staan de high-level pipeline stappen beschreven;



IAM integratie (Keycloak)

Keycloak wordt ingezet als identity broker tussen Container toepassingen op Kubernetes en de Azure Active directory van gemeente Utrecht. Er wordt voor de ontwikkel, test en productie omgevingen gebruik gemaakt van separate Keycloak instances die de omgevingen afzonderlijk faciliteren op basis van de OIDC en OAUT2 protocollen.

De productie Keycloak instance is opgedeeld in 4 federatieve koppelingen met Azure AD, elke koppeling correspondeert met een BIV-classificatie niveau. Elk niveau kent een set met andere voorwaarden waaraan voldaan dient te worden voordat een applicatie benaderd mag worden. Deze voorwaarden worden afgedwongen m.b.v. Azure AD Conditionele toegang.

Applicaties (clients) worden afhankelijk van de BIV-classificatie geconfigureerd voor authenticatie door de betreffende federatieve Azure AD koppeling.

Voorwaarden / benodigdheden

- Welke BIV-classificatie heeft de applicatie?
- Heeft de applicatie een rollenmatrix?
- Ondersteunt de applicatie Keycloak client roles?
- Welke gebruikers dienen initieel lid te worden van de applicatie rollen?
- Welke redirect URI's dienen er geconfigureerd te worden?

8.2.11 Ondersteunde operating systemen

Utrecht ondersteunt de volgende systemen binnen zijn virtuele datacenters;

- Windows Server 2019 en hoger;
- Red Hat 8.X Enterprise Linux;
- Oracle Linux voor hosting van Oracle databases;
- Windows 10 64 bits en hoger (werkplek)

8.2.12 Databases

Er worden een aantal soorten databases ondersteunt;

- SQL Server 2019 en hoger (op Windows Server)
- Maria DB (op Redhat Linux)
- Oracle 12 (op Oracle Linux)
- Postgress (op Docker Otomi platform)

8.2.13 Security monitoring

Utrecht maakt voor het monitoren van beveiliging en aanvallen primair gebruik van Microsoft Sentinel, extern gehoste toepassingen zoals SaaS en Azure diensten worden indien nodig hierop aangesloten conform het aansluitmodel security monitoring **Fout! Verwijzingsbron niet gevonden.**. Systemen in het Near Cloud datacenter op basis van Windows of Linux IaaS worden vooralsnog op QRadar aangesloten totdat de migratie van QRadar naar Sentinel is afgerond.
Utrecht beschikt over een SECOPS team voor security monitoring processen en onboarding en werkt conform het Mitre AAT&CK use case model voor het bepalen van de te monitoren use cases.

8.2.14 OTAP Omgevingen

De Gemeente Utrecht maakt gebruik van het OTAP concept waar benodigd. De OTAP omgevingen zijn zoveel mogelijk functioneel representatief t.o.v. productie ingericht en zijn logisch van elkaar gescheiden door middel van netwerkvirtualisatie.

8.2.15 De werkplek

De werkplek wordt tweeledig aangeboden;

1. Een mobiele werkplek op basis van Windows 10 of hoger.
2. Een Azure Virtual Desktop op basis van Windows 10 Multiuser of hoger.
3. Voor specials zoals presentatie pc's is een aparte procedure beschikbaar.

Taak applicaties worden op basis van applicatievirtualisatie aangeboden op de werkplekken. Daarnaast wordt er gebruik gemaakt van een "bedrijfsportal" en Application proxy om legacy applicaties te presenteren op de mobiele werkplek. Er wordt gebruik gemaakt van een lokale Microsoft Office 365 installatie.

Voor het beheer van de werkplekken wordt gebruik gemaakt van zowel SCCM als Microsoft Endpoint manager (Intune) in Azure. SCCM wordt gebruikt voor het distribueren van datacenter gebonden servers en werkplekken en Endpoint manager voor het configureren op afstand van de mobiele werkplekken.

8.2.16 Microsoft 365

De werkplek is voorzien van de OneDrive client, deze fungeert als opslag van persoonlijke informatie, SharePoint wordt gebruikt voor de opslag van afdelings- en bedrijf -informatie.
De werkplek is tevens voorzien van de Microsoft Teams client voor communicatie en delen van niet bedrijf kritische informatie met collega's en externe partijen.

8.2.17 Email

De mailomgeving is gebaseerd op Exchange online. Er is een lokale Exchange server aanwezig voor legacy applicaties en specials, deze is hybride verbonden met Exchange online. Indien er aansluiting benodigd is op de mailomgeving wordt er gebruik gemaakt van een centrale SMTP gateway. (zie bijlage aansluiting op de mail). Er is geen centrale bulkmail voorziening.

Voor het versturen van gevoelige informatie is er een veilige mail voorziening.

8.2.18 IAM proces identity provisioning

Utrecht conformeert zich aan de IAAA standaard (Identificatie, Authenticatie, Autorisatie en Accountability). Hiervoor is een geautomatiseerd proces ingericht; Medewerkers, externen en ketenpartners worden vanuit bronsystemen geautomatiseerd beheerd gedurende de gehele levenscyclus van het identiteit. Binnen het IAM systeem is selfservice beschikbaar en kunnen rollen worden toegekend.
Taak applicaties kunnen worden aangesloten voor identity provisioning middels SCIM. Hiervoor is Azure Identity provisioning beschikbaar en een lokale SCIM API voor specials.

8.2.19 Authenticatie en SSO

Utrecht hanteert het Single Sign On beleid voor interne en externe applicaties aangevuld met een tweede factor. Medewerkers van de Gemeente Utrecht beschikken over één identiteit en een 2e factor op basis van Microsoft MFA. Ten behoeve van SSO wordt er federatie toegepast op basis van Azure Federatie aangevuld met conditionele toegangs beleid.
Identiteiten worden automatisch beheerd, applicaties worden aangesloten voor authenticatie op de Utrecht identiteit. Hiervoor zijn aansluitvoorwaarden van toepassing (zie Authenticatie en provisioning standaarden)

8.2.20 Telefonie

Het telefonieplatform is gebaseerd op een Avaya VOIP oplossing. Daarnaast wordt er gebruik gemaakt van openbare GSM oplossingen. Op de werkplek wordt gebruik gemaakt van de Avaya One-X Communicator. In combinatie met de GSM oplossing wordt deze gebruikt voor signalering en gaat spraak over het GSM netwerk. De oplossing van Avaya wordt op verschillende locaties gebruikt.
Het telefonieplatform wordt vernieuwd en zal op basis van Microsoft Teams en Phone system worden aangeboden. Het klant contact centrum gaat gebruik maken van Storm.

Met opmerkingen [ZE1]: Het telefonie platform wordt in januari 2025 vernieuwd en ipv Avaya stappen we over naar MSTeams phonesystem. Voor het KCC gaan we gebruikmaken van Storm.

Met opmerkingen [FJ2R1]: @Zeehuisen, Eddy Volgens mij eindigt deze alinea met de aanpassingen die je voorstelt. Ik heb de laatste zin toegevoegd. Is dat akkoord?

Met opmerkingen [ZE3R1]: ja je hebt gelijk, deze opm kan dus vervallen. ik had even door moeten lezen

8.2.21 Privileged Access Management en sleutelbeheer

Voor het beheer van toegang tot interne systemen en verhoogd risico accounts wordt er gebruik gemaakt van een digitale kluis in de vorm van een password vault. Alle verhoogde accounts worden hierin opgenomen en wachtwoorden worden zo mogelijk automatisch gerouleerd. Dit geldt voor beheerders-, service-, leveranciers en andere verhoogde toegang accounts. Toegang tot de digitale kluis vindt plaats middels een tweede factor. Alle beheerwerkzaamheden dienen via de CyberArk portal plaats te vinden.

Voor toegang tot de Azure omgeving wordt tevens gebruik gemaakt van Azure Privileged Identity Management (PIM) en Azure Keyvault voor het uitgifte en beheer van eigen sleutels. Toegang is beperkt tot landen uit het EER verdrag.
Er is een RDP beheeromgeving beschikbaar voor het uitvoeren van beheer werkzaamheden aan de IaaS omgevingen en een virtuele PAW werkplek voor Azure beheer activiteiten.

8.2.22 Beheer op afstand door leverancier

Er is geen directe toegang mogelijk tot systemen vanaf externe omgevingen. Leveranciers dienen via de werkplek (AVD) en CyberArk of Azure PIM gecontroleerd toegang aan te vragen. De sessie daaruit voortkomend kan live ingezien of opgenomen worden voor audit doeleinden.

8.2.23 Multi functionele printers

Voor afdruk, scan en mail taken wordt er gebruik gemaakt van Multi Functionele Printers. Alle printers hebben meerdere papierlades met verschillende types papier. Er is één uniforme driver in gebruik. Dit is beschikbaar voor zowel de mobiele werkplek als voor het Azure Virtual Desktop platform.

8.2.24 Intranet en internet website

Voor het intranet en internet site van de gemeente Utrecht wordt gebruik gemaakt van het Content management Systeem Typo3.

8.2.25 Integratie met clouddiensten

Voor de ontsluiting en het uitwisselen van gegevens met clouddiensten beschikt de gemeente over verschillende koppelvlakken. Uitwisseling van gegevens dient plaats te vinden op basis van encryptie op zowel de transport- als de data laag (data at rest) bij voorkeur middels een pull vanuit de gemeente.

8.3 AUTHENTICATIE EN PROVISIONING STANDAARDEN

De Gemeente maakt gebruik van moderne authenticatie op basis van Azure Federatie.
Onderstaande tabel bevat de door Utrecht ondersteunde protocollen en toepassing daarvan.
Er is een IAM loket beschikbaar welke de federatieve koppeling samen met de leverancier realiseert. (IAM@Utrecht.nl)

Authenticatie middelen (*1,2*)

Nr.	Protocol	Status	Middel	Interne applicaties	SaaS/Cloud-applicaties
1	**OpenID Connect Oauthv2**	**Voorkeur**	**Azure Federatie** (*3*)	**Ja**	**Ja**
2	SAML v2.0	Alternatief	Azure Federatie	Ja	Ja
3	Kerberos	Alleen intern	Active Directory	Ja	Nee
4	LDAPS	Niet toegestaan		n.v.t.	n.v.t.

Identity Provisioning[5]

Nr.	Protocol	Status	Middel	Interne applicaties	SaaS/ Cloudapplicaties
1	**SCIMv2**	**Voorkeur**	**Azure SCIM endpoint**	**Ja**	**Ja**
2	SCIMv2	Alternatief	Interne SCIM endpoint	Ja	Ja
3	Maatwerk REST API	Indien beschikbaar	Azure SCIM	Ja	Ja
4	Maatwerk XML SOAP	Alleen bij uitzondering		Ja	Ja
5	Eigen implementatie	Alleen bij uitzondering		Ja	Ja
6	Handmatig	Afhankelijk van BIV classificatie toegestaan		Ja	Ja
7	Microsoft LDAPS	Niet toegestaan		n.v.t.	n.v.t.
8	Bestand: XML, JSON (beveiligd)	Niet toegestaan		n.v.t.	n.v.t.

Toelichting;

1. Nummering van protocollen staat in volgorde van voorkeur
2. De mate en inrichting van identity provisioning is mede afhankelijk BIV-classificatie en het gebruik van rollen.
3. Bij Container platform met Keycloak als broker
4. Alleen bij uitzondering; na afstemming met architectuur