

gemeente Eindhoven

***Doel Architectuur
Infrastructure as a Service
IaaS***



Inhoudsopgave

1 Aanleiding	3
Probleem	3
Doel.....	3
2 Doel Architectuur	4
Omgevingen.....	4
(A): Omgeving: Datacenter High Tech Campus (HTC) Colocation	4
(B): Omgeving: Datacenter Stadhuis on-premise Edge	5
(C): Omgeving: Public Cloud Microsoft Azure Tenant Eindhoven	5
(D): Omgeving: Openbare ruimte gemeente Eindhoven	5
(E): Omgeving: Elke mogelijke leverancier waarbij een applicatie of dienst wordt afgenomen	5
(F): Omgeving: Future Community Cloud.....	5
Koppeling omgevingen	5
(1): Koppeling: Private cloud Eindhoven HTC en Azure Tenant Eindhoven	5
(2): Koppeling: Private cloud Eindhoven HTC en Cloud dienstverlener	6
(3): Koppeling: Private cloud Eindhoven HTC en Eindhoven Edge omgeving	6
(4): Koppeling: Eindhoven Edge omgeving en Openbare ruimte	6
(5): Koppeling: Eindhoven Openbare ruimte en Azure Tenant Eindhoven	7
(6): Koppeling: Eindhoven Openbare ruimte met Cloud dienstverlener	7
(7): Koppeling: Private cloud Eindhoven HTC en future Community Cloud (CBI)	7

1 Aanleiding

Voor de IT-afdeling wordt het steeds moeilijker om aan de snel veranderende organisatiewensen te kunnen voldoen. Om de organisatie beter te kunnen ondersteunen bij het bereiken van de doelstellingen neemt de vraag naar een flexibele en wendbare IT-Infrastructuur en Informatievoorziening(IV) in hoog tempo toe. De inmiddels verouderde server IT-Infrastructuur wordt vanaf oktober 2023 niet meer ondersteunt en sluit niet aan op de huidige klantvraag en organisatiebehoefte. Dit document beschrijft globaal de omgeving van de te vervangen server IT-Infrastructuur.

Probleem

Door de verouderde en niet meer ondersteunde server IT-Infrastructuur loopt de organisatie risico's zoals:

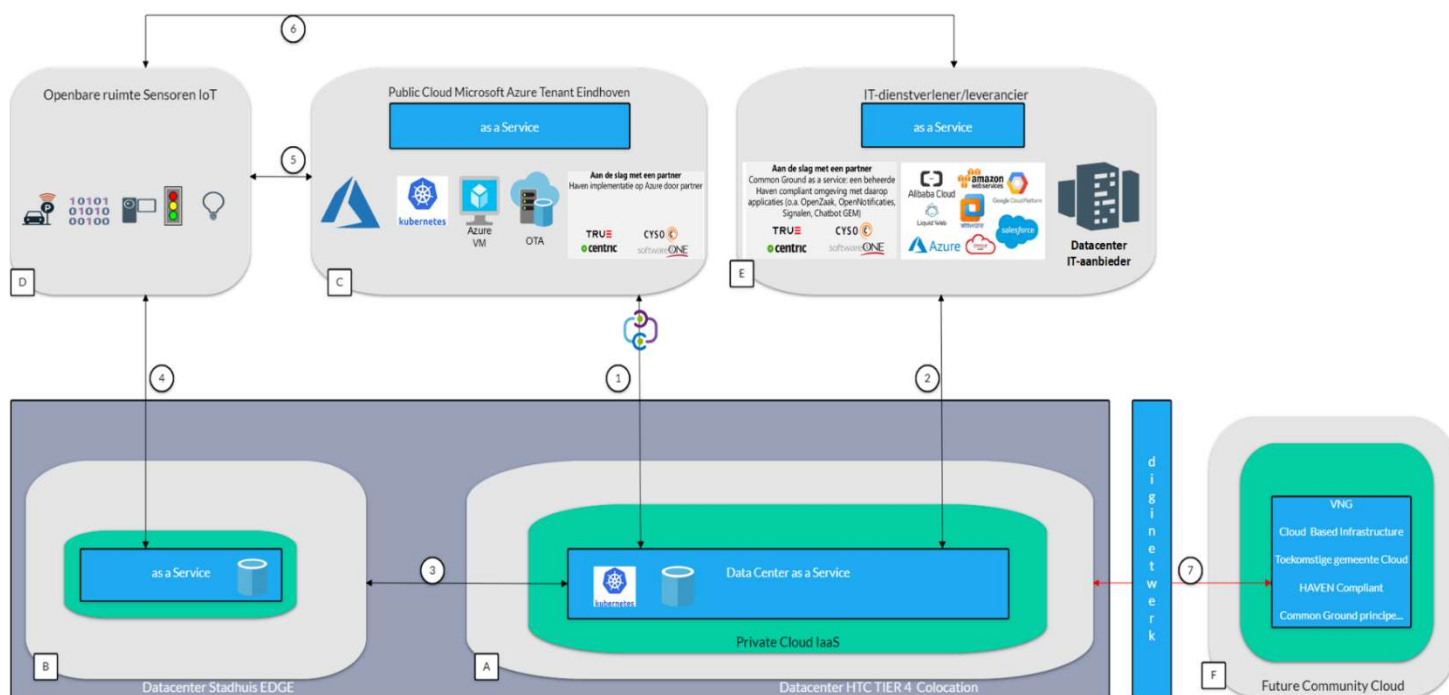
- Geen ondersteuning op de hardware waarbij in het geval van calamiteiten de bedrijfsvoering van de gemeente Eindhoven in gevaar kan komen
- Door verouderde hardware een toename van storingen van de apparatuur en daaruit voortvloeiende instabiliteit
- Geen updatemogelijkheden meer waardoor security, stabiliteit en performance issues kunnen ontstaan die niet opgelost kunnen worden
- Geen uitbreidingsmogelijkheden omdat de verouderde apparatuur niet uitgebreid kan worden
- De server IT-Infrastructuur valt onder de basisvoorzieningen die waar mogelijk van het op de organisatiebehoefte afgestemde niveau dient te zijn zodat de organisatie optimaal ondersteund wordt bij de bedrijfsvoering.

Doel

Opleveren van: 'Een server IT- infrastructuur die aan de NIST cloud kenmerken voldoet, gefaciliteerd door een IT-organisatie die over de benodigde skills, competenties en middelen beschikt waardoor op een gestructureerde en veilige manier de gemeente Eindhoven ondersteunt wordt bij het bereiken van de organisatiedoelstellingen'

2 Doel Architectuur

De onderstaande afbeelding is een weergave van de doelarchitectuur en geeft het beoogde IT-landschap weer na vervanging van de IST IT-Infrastructuur. Bij elke omgeving staat een letter en de lijnen en cijfers geven de relatie weer tussen de omgevingen. De omgevingen en relaties worden globaal beschreven in dit document. Het doel is om aanbieders een beeld te schetsen waar de gemeente Eindhoven de komende jaren naar toe gaat.



IT-Infrastructuur op basis van cloudstrategie principe: **'Cloud first met een veilig hybride service aanbod'**

Cloud First (as a Service waar mogelijk): Elk nieuw systeem of applicatie is bij voorkeur zo ontworpen dat van de voordelen van cloud leveringsmodellen geprofiteerd wordt. Deze voldoet daarbij aan de kenmerken van cloud computing zoals beschreven door het 'National Institute of Standards and Technology' (NIST) (Publication 800-145, 2011)¹ en de Cloud Computing Reference Architecture (RA)(Special Publication 500-292)²

Veilig (in control waar nodig): Als een workload en/of dataset na een impact analyse niet geschikt wordt bevonden voor een Public Cloud wordt deze in de Private Cloud geplaatst. Deze bevindt zich in datacenter HTC waarbij Security by Design het uitgangspunt is.

Hybride (samenwerken waar gewenst): Combinatie van een Private Cloud (HTC) & Public Cloud (Microsoft Azure) en in een later stadium een Community Cloud. De future Community Cloud wordt in de toekomst door samenwerking met andere gemeenten, de VNG en geselecteerde marktpartijen vormgegeven, zoals een gemeentelijke Cloud Based Infrastructure (CBI) en HAVEN en 'aan de slag met Common Ground' initiatieven.

Service aanbod (afgestemd op organisatie en taakstelling Bedrijfsvoering): Moderniserend, Faciliterend, Kaderstellend, Adviserend & Monitorent.

Omgevingen

(A): Omgeving: Datacenter High Tech Campus (HTC) Colocation

Colocation datacenter van NorthC gebouwd volgens de Tier 4 norm voor optimale veiligheid en beschikbaarheid. Het datacenter is strategisch gelegen op de High Tech Campus (HTC) en verbonden met alle andere datacenters van NorthC. Het datacenter biedt toegang tot een groot aantal nationale en internationale clouddiensten en -providers en beschikt over 24/7/365 on-site beveiliging.

¹ Bron: <https://www.nist.gov/publications/nist-definition-cloud-computing>

² Bron: <https://www.nist.gov/publications/nist-cloud-computing-reference-architecture>

(B): Omgeving: Datacenter Stadhuis on-premise Edge

Het eigen on-premise datacenter onder het stadhuis van de gemeente Eindhoven. Het datacenter vormt een transparant netwerk via een dubbele glasverbinding naar het HTC-datacenter. Naast de datacenter ruimte onder het stadhuis beschikt de gemeente Eindhoven over meerdere panden (NRE, Mercado) waarin zich een MER/SER-ruimte bevindt die kunnen fungeren als Edge locatie in de toekomst.

(C): Omgeving: Public Cloud Microsoft Azure Tenant Eindhoven

De Eindhoven tenant is een omgeving die gecreëerd is bij Microsoft voor de gemeente Eindhoven. Hierin worden alle onlineservices van Microsoft opgeslagen. De gemeente Eindhoven maakt al gebruik van Office 365 welke draait in het datacenter van Microsoft op de Windows Azure omgeving. Er kunnen extra diensten afgenomen worden binnen de Azure omgeving zoals een Kubernetes cluster en er kunnen Virtuele Machines (VM), databases en volledige workloads worden geplaatst.

(D): Omgeving: Openbare ruimte gemeente Eindhoven

De openbare ruimte in de Stad Eindhoven. Hierin bevinden zich o.a. IoT devices, sensoren, camera's en dus steeds meer 'slimme' apparaten welke veel data genereren.

(E): Omgeving: Elke mogelijke leverancier waarbij een applicatie of dienst wordt afgenomen

De gemeente Eindhoven heeft geen DevOps teams mede daardoor wordt 80% van de applicaties aangekocht of steeds vaker als SaaS-oplossing afgenomen bij een IT-dienstverlener. Deze IT-dienstverlener kan zijn SaaS-dienst beschikbaar stellen vanuit een willekeurige Publieke Cloud (Azure, AWS, Google), vanuit een eigen datacenter of hosting omgeving door eigen servers te plaatsen in een door een andere partij geleverde datacenter services. Hierbij dient altijd getoetst te worden of aan wet- en regelgeving zoals de AVG en normenkaders als de BIO voldaan wordt. De gemeente Eindhoven blijft ook in het geval van een SaaS applicatie verantwoordelijk voor de inhoud van de gehoste data op het gebied van Identity Access Management (IAM), Governance en endpoint security.

(F): Omgeving: Future Community Cloud

De gemeente Eindhoven heeft met een aantal andere gemeenten en de VNG deelgenomen aan een onderzoek dat is uitgevoerd door Solventa architecten. De onderzoeksvraag was of het opzetten van een Cloud Based Infrastructure (CBI) van en voor gemeenten van toegevoegde waarde kon zijn. Het antwoord was positief maar concreet is er nog geen uitvoerende fase en wordt deze CBI (nog) niet gebouwd. Vandaar dat het als future cloud placeholder is opgenomen welke in de toekomst een gemeentelijke community cloud kan gaan vormen. Het CBI gaat dan de gemeenten ontzorgen door een Infrastructuur aan te bieden die BIO compliant is en waarbij een gemeente vooraf weet als een workload geplaatst wordt op de CBI dat aan wet- en regelgeving voldaan kan worden.

Koppeling omgevingen

Bij de koppelingen worden niet alle mogelijke opties beschreven maar enkel een paar voorbeelden ter illustratie. De doelarchitectuur geeft een globaal beeld van de toekomstige server IT-Infrastructuur. Het dient als richtinggevend hulpmiddel waarmee er een server IT-Infrastructuur opgezet kan worden die is afgestemd op het - door het MT I&B en CIO-Office bekrachtigde - cloudstrategie principe.

(1): Koppeling: Private cloud Eindhoven HTC en Azure Tenant Eindhoven

Door het afnemen van een IaaS IT-infrastructuur in de vorm van een van een Cloud Data Center as a Service en het support en onderhoud daarvan bij een leverancier te beleggen vervallen hardware werkzaamheden voor de eigen IT-medewerkers. Daarbij kan gebruik gemaakt worden van de voordelen van cloud computing maar met controls die je in een Public Cloud niet hebt en waar de eigen IT-organisatie de regie over voert.

- Private Cloud wordt gekoppeld aan de Azure Tenant Eindhoven waardoor een hybride omgeving ontstaat. Dit is nu buiten scope maar het moet mogelijk zijn om deze koppeling te leggen vanuit de oplossing van de aanbieder.
- Diensten aangeboden in de Azure omgeving worden via de hybride verbinding transparant uitgerold over de (eigen) Private Cloud. Denk aan security en andere monitoring tools die zowel in Azure draaien maar ook de Private Cloud kunnen bewaken. Dit is nu buiten scope maar het moet mogelijk zijn om deze koppeling te leggen vanuit de oplossing van de aanbieder.
- Uitwijk en Disaster Recovery wordt een combinatie van een clouddienst zoals DRaaS en private cloud uitwijk in het geval dat een data-set niet naar de public cloud verplaatst mag worden (hierbij kan de stadhuis edge omgeving een rol spelen of een ander NorthC datacenter). Het is hierbij van belang dat de data, applicatie en Virtuele Machine (VM) van elkaar gescheiden kunnen worden.
- Ontwikkel Test en Acceptatie (OTA) omgevingen kunnen in Azure aangemaakt worden en alleen opgestart worden als deze gebruikt worden. Na het opstarten van een testserver gaan de kosten pas lopen – het pay as you go principe – waardoor een server niet onnodig aanstaat zoals nu het geval is. Dit bespaart energie en is meer secure omdat servers enkel aanstaan als ze gebruikt worden. Dit is nu buiten scope maar het moet mogelijk zijn om deze koppeling te leggen vanuit de oplossing van de aanbieder.
- In de Eindhoven Tenant omgeving is het mogelijk om ‘aan de slag te gaan met Common Ground’ op basis van Kubernetes waarbij het beheer en support volledig of gedeeltelijk bij een dienstverlener ligt. Dit is nu buiten scope maar het moet mogelijk zijn om deze koppeling te leggen vanuit de oplossing van de aanbieder.

(2): Koppeling: Private cloud Eindhoven HTC en Cloud dienstverlener

Applicaties worden steeds vaker als Software as a Service (SaaS) afgenomen. De benodigde kennis verschuift dan veelal van zelf installeren en beheren naar het integreren van de data en processen uit de SaaS omgeving met on-premise of andere SaaS diensten. De gemeente Eindhoven blijft ook in het geval van een SaaS applicatie verantwoordelijk voor de inhoud van de gehoste data op het gebied van Identity Access Management (IAM), Governance en endpoint security

- Op de Private Cloud worden tools beschikbaar gesteld waarmee de IT-organisatie de benodigde beheertaken en monitoring kan uitvoeren.
- Tooling in de Private Cloud zorgt ervoor dat de Cloud Governance afgestemd kan worden op de eisen die daaraan gesteld worden.

(3): Koppeling: Private cloud Eindhoven HTC en Eindhoven Edge omgeving

Het datacenter stadhuis wordt maximaal ontdaan van de IT-systemen die daar nu draaien (met name OTA en uitwijk). Maar deze locatie kan een HUB, Edge of een Disaster Recovery taak krijgen indien bepaalde data niet naar de Public Cloud verplaatst mag worden. Ook in dat geval dient er zoveel als mogelijk hardware als IaaS afgenomen te worden waarover de beheerorganisatie enkel de regie voert. Het nadeel van het datacenter stadhuis is dat deze in eigen beheer is (anders dan de HTC).

(4): Koppeling: Eindhoven Edge omgeving en Openbare ruimte

De gemeente Eindhoven maakt steeds meer gebruik van Internet of Things (IoT) devices zoals sensoren en camera's die in korte tijd veel data genereren. De grote hoeveelheid data die de IoT devices produceren worden in het geval van een public cloud backend oplossing direct over het netwerk verstuurd (koppeling 5&6). De centrale cloud omgeving verwerkt de data en geeft indien noodzakelijk een response terug naar het IoT device (koppeling 5&6). Dit kan leiden tot vertraging en overbelasting van de netwerkverbinding als ook het opslaan van een overvloed aan niet noodzakelijke of gevoelige data op de cloud backend. Een oplossing is de data lokaal (edge) te verzamelen en enkel een subset naar de public cloud te verplaatsen voor centrale analyse. Een IoT-device met voldoende resources kan dat zelf uitvoeren of er wordt gebruik gemaakt van een Edge omgeving dichtbij in een private omgeving.

Met de groei van IoT in de openbare ruimte kan - afhankelijk van de gevoeligheid en de hoeveelheid te verwerken data - het opzetten van verschillende lokale Edge backend omgevingen in de gemeentelijke gebouwen een oplossing bieden. Denk hierbij aan de camerabeelden die vanwege bandbreedte en privacy gevoeligheid niet naar de public cloud verplaatst mogen of kunnen worden.

Beschrijving eisen en wensen dienen afgestemd te worden met de datastrategie. De koppelingen zijn hier opgenomen omdat deze van invloed zijn op de inrichting van de SOLL IT-Infrastructuur

Mogelijke Opties:

- IoT device heeft voldoende rekenkracht en opslagcapaciteit en verwerkt de data zelf waarbij deze niet van het IoT device verplaatst wordt(of enkel een subset van de data) naar een andere omgeving
- IoT devices verplaatsen de data naar een Edge backend omgeving van de gemeente Eindhoven
- IoT devices verplaatsen de data naar de Azure Tenant Eindhoven
- IoTdevices verplaatsen de data naar de omgeving van een Cloud dienstverlener (Public Cloud)

Dit is nu buiten scope maar het moet mogelijk zijn om deze koppeling te leggen vanuit de oplossing van de aanbieder.

(5): Koppeling: Eindhoven Openbare ruimte en Azure Tenant Eindhoven

Beschrijving eisen en wensen dienen afgestemd te worden met de datastrategie. De koppelingen zijn hier opgenomen omdat deze van invloed kunnen zijn op de aan de inrichting van de SOLL IT-Infrastructuur

(6): Koppeling: Eindhoven Openbare ruimte met Cloud dienstverlener

Beschrijving eisen en wensen dienen afgestemd te worden met de datastrategie. De koppelingen zijn hier opgenomen omdat deze van invloed kunnen zijn op de aan de inrichting van de SOLL IT-Infrastructuur

(7): Koppeling: Private cloud Eindhoven HTC en future Community Cloud (CBI)

Een IaaS omgeving die via Diginet beschikbaar gesteld wordt voor en door gemeentes met behulp van geselecteerde marktpartijen. De gemeente Eindhoven hoeft zich geen zorgen te maken over compliance en weet dat als er een workload op de CBI geplaatst wordt dat deze BIO compliant is en aan alle wetgevingen voldoet.