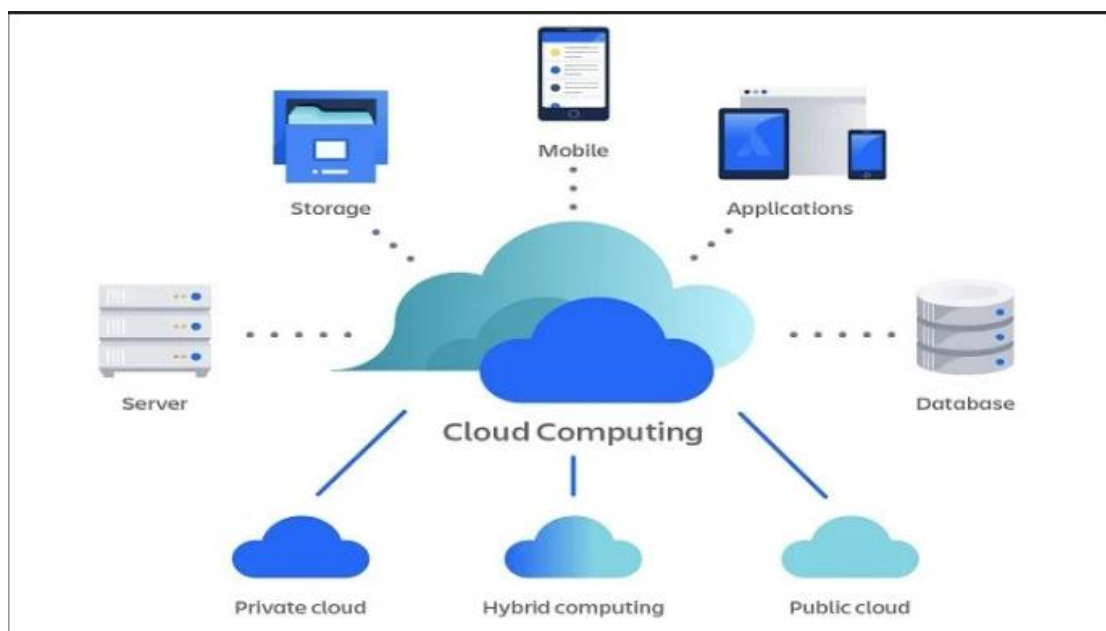


Toekomstvisie centrale ict-voorzieningen



Inhoudsopgave

1.	Inleiding.....	3
2.	Server en storageomgeving.....	4
2.1	Huidige situatie.....	4
2.2	Wie doet beheer nu?.....	4
2.3	Risico' s.....	5
2.4	Hoe nu verder?	5
3.	Applicatie servers.....	6
3.1	Huidige situatie.....	6
3.2	Wie doe het beheer nu?.....	6
3.3	Risico' s.....	6
3.4	hoe nu verder?	6
4.	Virtuele desktop	7
4.1	Huidige situatie.....	7
4.2	Wie doet beheer nu?.....	7
4.3	Risico' s.....	7
4.4	Hoe nu verder?	7
5.	Netwerk en firewall.....	8
5.1	Huidige situatie.....	8
5.2	Wie doet beheer nu?.....	9
5.3	Risico' s.....	9
5.4	Hoe nu verder?	9

1. Inleiding

In 2019 is de huidige centrale Server infrastructuur in datacenters op locatie Stationsstraat 25 (gemeentekantoor) en Mevr. Kuipers-Rietbergplein 1 (raadhuis) aangepast. Hierop zijn de nodige service-, onderhouds- en voor een deel beheerscontracten afgesloten. In 2024 zijn de contracten hiervoor met 2 jaar tot 31 juli 2026 verlengd.

Destijds is de centrale netwerkinfrastructuur zoals switches en routers die het mogelijk maakt laptops, printers, pinautomaten, wifi accesspoints en overige devices aan te sluiten op het netwerk niet vervangen. De huidige netwerk apparatuur wordt niet langer ondersteund en er komen ook geen security update meer voor. Het support op de huidige firewall stop per 29 december 2025.

Door de invoering van Microsoft 365 zijn er technisch zaken veranderd en dat zorgt er ook voor dat er op dit moment extra taken bij de systeembeheerders van de gemeente Winterswijk zijn belegd. Voor het beheer van de Citrixomgeving is daarom nu tijdelijk een externe partij ingeschakeld.

In de afgelopen jaren is het beleid erop afgestemd dat we applicaties in de cloud onderbrengen. Dit proces is nog niet afgerond.

De diverse managers hebben de afgelopen jaren aangegeven ict-beheertaken extern te willen beleggen zodat medewerkers de handen vrij krijgen voor nieuwe taken zoals beheer Microsoft 365 en portfoliomanagement.

We zijn nu op een punt aangekomen om te bepalen wat we als gemeente willen.

Door nu die stip op de horizon te plaatsen kunnen we tijdig starten met voorbereiden en uitvoeren van aanbestedingen en bijbehorende implementatie trajecten. In dit document beschrijf ik de huidige situatie en een mogelijk toekomst plaatje met de gevolgen daarvan.

2. Server en storageomgeving

2.1 Huidige situatie

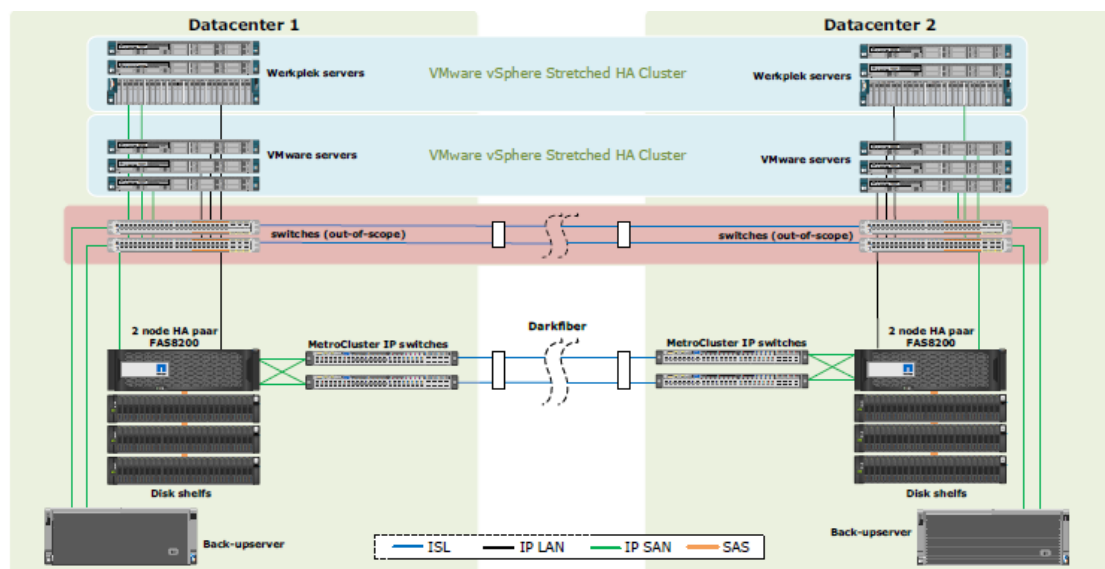
De huidige servers en storage zijn ondergebracht in 2 datacenters (gemeentekantoor en raadhuis). Deze datacenters zijn voorzien van airco t.b.v. voldoende koeling en UPS-en (Uninterruptable power supply). Deze zorgt voor constante spanning en kan tijdens eventuele stroom uitval een korte tijd de serveromgeving draaiende houden zodat deze netjes kan worden stopgezet.

De UPS is niet beschikbaar voor de werkplekken. Daarnaast zijn we niet in het bezit van een aggregaat die een deel of het gehele gebouw kan voorzien van elektriciteit. Deze moet bij calamiteiten worden gehuurd.

De datacenters draaien in een active/active modus wat inhoudt dat beide datacenters de helft van de taken voor rekening nemen. Bij uitval van de 1 van de datacenters kan het andere datacenter die taken overnemen.

Alle fysieke servers zijn voorzien van VMware vsphere ESX en gekoppeld aan de Netapp storage omgeving.

Alle applicatieservers (back- en frontend) draaien als virtuele server binnen de VM-ware omgeving. Behalve de backupservers hiervoor zijn aparte fysieke servers met eigen storage ingericht.



De backup wordt van en op beide locaties gemaakt. Daarnaast is er nog een 3^e locatie in de cloud. Dit is een zogenaamde airgapped backup. De verbinding naar deze omgeving is er alleen gedurende korte tijd als de backup wordt gemaakt.

2.2 Wie doet beheer nu?

De hardware en de VM-ware vsphere esx laag en het beheer van backup en restore is in beheer bij Axians. Het contract met Axians loopt tot 31 juli 2026. Ook de bijbehorende licenties die buiten dat contract vallen hebben dezelfde vervaldatum.

De virtuele laag met alle applicatieservers is in beheer bij systeembeheer van gemeente Winterswijk.

De bedoeling was om ook dat beheer extern te beleggen om medewerkers vrij te maken voor hun nieuwe taken. Dat is tot op heden nog niet gerealiseerd.

2.3 Risico's

Op dit moment zijn de beheerders belast met oude en nieuwe taken. Om oude en nieuwe taken te doen zijn onvoldoende uren beschikbaar. De gemeente Winterswijk loopt hierdoor risico op continuïteit versturende incidenten. Daarnaast is er het risico van overbelasting van de medewerkers.

2.4 Hoe nu verder?

Uitgangspunten:

- De systeembeheerders moet capaciteit beschikbaar krijgen om door te kunnen groeien in de nieuwe rol als functioneel beheerder Microsoft 365.
- het datacenter moet worden ontmanteld om taken te laten vervallen zodat systeembeheerder het nieuwe takenpakket van portfoliomanager op zich kan nemen.

Om tijdig voor 31 juli 2026 een vervangende omgeving te hebben moeten gaan uitschrijven wat we willen. We hebben daarbij keuze uit meerdere opties met elk zijn eigen voor en nadelen.

Optie 1 : geheel in de cloud onder te brengen bij een leverancier.

Optie 2 : geheel onderbrengen onder azure vmware services inclusief beheer

3. Applicatie servers

3.1 Huidige situatie

Op dit moment is er nog zijn er nog 88 virtuele server operationeel voor applicaties en beheer.

- 2 zijn operationeel voor het beheer van het wifinetwerk
- 2 voor firewall, fortimail, fortianalyzer
- 14 zijn operationeel voor het beheer van de server en storage omgeving
- 70 zijn operationeel voor verschillende applicatie doelen.

De virtuele server zijn voorzien van Windows server 2016 of Windows server 2019 of Windows server 2022. Een enkeling draait onder Linux.

3.2 Wie doe het beheer nu?

De 14 virtuele servers voor het beheer van server en storage zijn in beheer bij Axians.

De Linux servers zijn in beheer bij de Leverancier van de applicatie of wordt op adhoc basis voor beheer extern ingehuurd.

De overige virtuele servers zijn in beheer bij systeembeheer van gemeente Winterswijk. Een 2-tal systeembeheerder voert de Microsoft updates op deze machines uit. Daarnaast worden storingsen verholpen door het team. Het uitvoeren van deze taken staat onderdruk doordat extra taken die vanuit de invoering van Microsoft 365 komen ook moeten worden uitgevoerd. Er is op dit moment geen capaciteit om de gevolgen van de nieuwe wetgeving rond Nist-2 in kaart te brengen en mogelijke maatregelen te implementeren.

3.3 Risico's

Taken worden niet of onvoldoende uitgevoerd waardoor continuïteit van de systemen in gevaar komt. Hierdoor komt het uitvoeren van wettelijke taken en dienstverlening naar de burger en bedrijfsleven in gevaar.

3.4 hoe nu verder?

Uitgangspunten:

- De systeembeheerders moeten capaciteit beschikbaar krijgen om door te kunnen groeien in de nieuwe rol als functioneel beheerder Microsoft 365 en portfoliomanager.
- het datacenter moet worden ontmanteld om taken te laten vervallen zodat de andere systeembeheerder het nieuwe takenpakket van portfoliomanager op zich kan nemen.

Om continuïteit te waarborgen moeten we bepalen wie deze taken moet uitvoeren. Een deel van het beheer zal vervallen omdat applicaties in toenemende mate in de cloud worden ondergebracht. We zullen moeten bepalen welke applicaties er naar de cloud kunnen en welke niet. Voor de achterblijvende applicaties moeten we kijken of er vervangende applicaties zijn die wel in de cloud kunnen. Is dat niet het geval dan zullen we de beschreven opties in hoofdstuk 2.4 moeten onderzoeken en uitwerken.

4. Virtuele desktop

4.1 Huidige situatie

De virtuele desktop omgeving is geplaatst op een 6-tal VMware Esx-hosts verdeeld over 2 locaties. Op de Esx-servers draaien 40 virtuele Windows servers 2019 waarop de medewerkers landen voor de standaard digitale werkplek. Daarnaast zijn er nog 14 virtuele servers t.b.v. autocad i.v.m. gebruik GPU-kaart.

Voor het operationeel houden van de Citrix omgeving is er een 10-tal virtuele servers nodig voor uitrol, controle en testen van deze omgeving.

Daarnaast zijn er een 2-tal geclusterde Netscalers operationeel voor toegang en loadbalancing van die Citrix omgeving.

Voor het beschikbaar stellen van applicatie-snelkoppelingen en uitrollen van policies wordt gebruik gemaakt van VMware-DEM.

4.2 Wie doet beheer nu?

Het beheer op deze omgeving werd tot op heden uitgevoerd door een systeembeheerder van de gemeente Winterswijk. Per 19 november is er tijdelijk een externe beheerder ingehuurd om het dagelijks beheer te doen en ook een upgrade uit te voeren naar een volgende versie van de Citrix software. Tevens gaat hij zich ook bezighouden met de migratie van de Windows 10 naar Windows 11 look and feel Windows server 2022.

4.3 Risico's

Voor de korte termijn is beheer nu geborgd. Voor de lange termijn moet er naar een oplossing worden gezocht. De vraag is echter blijven we bij Citrix of gaan we naar een Microsoft variant. En doen we dat dan in eigen beheer of gaan we dat belegen bij een externe partij?

4.4 Hoe nu verder?

Uitgangspunten:

- De systeembeheerders moet capaciteit beschikbaar krijgen om door te kunnen groeien in de nieuwe rol als functioneel beheerder Microsoft 365. Er moet dus een structurele oplossing komen om het beheer van de nieuwe virtuele desktop omgeving te borgen.
- het datacenter moet worden ontmanteld om taken te laten vervallen zodat de andere systeembeheerder het nieuwe takenpakket van portfoliomanager op zich kan nemen.

We moeten gaan bepalen of we al dan niet verder gaan met Citrix. We hebben een aantal opties:

Optie 1 : Verder met Citrix onderbrengen bij een externe partij inclusief beheer.

Optie 2 : Verder gaan met Citrix onderbrengen bij Microsoft Azure services met beheer door externe partij

Optie 3 : Stoppen met Citrix en overgaan op andere variant van virtuele desktop inclusief beheer

Optie 4 : Stoppen met Citrix , zoveel mogelijk applicaties verslaan, en offloaden naar laptop

5. Netwerk en firewall

5.1 Huidige situatie

Het huidige netwerk is een stretched netwerk over meerdere locaties.

De locaties zijn:

Gemeentekantoor, Stationsstraat 25 te Winterswijk

Raadhuis, Mevr. Kuipers-Rietbergplein 1 te Winterswijk

De post, Balinkesstraat 4 te Winterswijk

Sporthal de Spoorzone, Parallelweg 9 te Winterswijk

Locatie Gemeentekantoor

MER

Deze locatie heeft een 500Mbit internetverbinding en een 100Mbit Gemnet/KPNVPN. Deze zijn aangesloten op een KPNrouter en doorgezet naar een 24poorts switch. Deze is dan weer doorgezet naar de firewall.

Deze MER is door middel van een redundant darkfiber gekoppeld aan de SER op locatie Gemeentekantoor.

Hier zijn 3 switches met verschillende modules geplaatst t.b.v. netwerkaansluiting werkplekken en overige devices en 2 switches t.b.v. Wifi accespoints. Voor het wifinetwerk zijn er 2 virtuele servers ingericht voor het beheer en configureren van de Wifi Accespoints. Voor de genoemde switches loopt geen supportcontract meer.

Over alle switches lopen verschillende vlan's t.b.v. werkplek, facilitaire diensten.

Via de switches is ook de netwerkverbinding naar de serverstorage netwerkomgeving gerealiseerd.

Via de MER is ook de straalverbinding naar locatie sporthal de Spoorzone geregeld. De straalzender hangt op een van de balkons op de 2^e etage.

Er is op deze locatie een firewall aanwezig die in een cluster is geconfigureerd met de firewall die op locatie Raadhuis is geplaatst.

SER

Deze SER is door middel van een redundant darkfiber gekoppeld aan de MER op locatie Gemeentekantoor. Hier zijn 2 switches geplaatst t.b.v. netwerkaansluiting werkplekken en overige devices en 2 switches t.b.v. Wifi accespoints. Voor de genoemde switches loopt geen supportcontract meer.

Over alle switches lopen verschillende vlan's t.b.v. werkplek, Wifi en facilitaire diensten

Locatie Raadhuis

Deze locatie heeft een 500Mbit internetverbinding en een 100Mbit Gemnet/KPNVPN. Deze zijn aangesloten op een KPNrouter en doorgezet naar een 24poorts switch. Deze is dan weer doorgezet naar de firewall.

Deze locatie is door middel van een darkfiber gekoppeld aan locatie Gemeentekantoor. Op deze locatie is 1 HP-Switch die is uitgerust met 3 modules met 24 poorten. Voor de genoemde switch loopt geen supportcontract meer.

Over de switches lopen verschillende vlan's t.b.v. werkplek, Wifi en facilitaire diensten

Op deze switch is ook de netwerkverbinding naar de serverstorage netwerkomgeving gerealiseerd.

Er is op deze locatie een firewall aanwezig die in een cluster is geconfigureerd met de firewall die op locatie Gemeentekantoor is geplaatst.

Locatie De Post

Deze locatie is door middel van een darkfiber gekoppeld aan locatie Gemeentekantoor. Op deze locatie zijn 2 24 poorts switches geplaatst. Voor de genoemde switches loopt geen supportcontract meer.

Deze switches zijn onderling gekoppeld via **XXXXXXXXXXXX**. 1e router is voor receptie en kantoren, 2^e router is voor Spot jongerenwerk. Over beide switches lopen verschillende vlan's t.b.v. werkplek, Wifi en facilitaire diensten

Locatie de Spoorzone

Deze locatie is door middel van een straalverbinding gekoppeld aan locatie Gemeentekantoor. Op deze locatie is een 24 poort router geplaatst. Voor de genoemde switch loopt geen supportcontract meer. Over de switch lopen verschillende vlan's t.b.v. werkplek, Wifi en facilitaire diensten. In de beheerdersruimte is een Wifi accesspoint geplaatst. De straalzender bevindt zich op het dak.

5.2 Wie doet beheer nu?

De medewerker die belast was met netwerkbeheer vertrokken. Deze taken zijn tijdelijk deels overgenomen door medewerkers en deels wordt op adhoc basis ingehuurd. Maar niet alle taken zijn nu belegd. De bedoeling was om netwerkbeheer extern te beleggen. Dat is tot op heden nog niet gerealiseerd.

5.3 Risico's

Naast dat het netwerkbeheer nog niet volledig is belegd, maar ook omdat de netwerkinfrastructuur inmiddels is verouderd loopt de gemeente Winterswijk ernstige informatiebeveiligingsrisico's. Vervanging is dan ook noodzakelijk.

5.4 Hoe nu verder?

Taken zijn nu onvoldoende belegd en geborgd. Dit is i.v.m. 24 uursdienstverlening 24x7, vakantie en ziekte verzuim niet door 1 persoon te doen. Advies is daarom deze taken bij een externe partij onder te brengen.

Hiervoor zijn 2 opties;

- Optie 1 : Bestaande situatie continueren en aanbesteding starten voor het aanschaffen hardware en beheer inclusief SIEM/SOC beleggen bij een externe partij.
- Optie 2 : Bestaande situatie continueren en aanbesteding starten voor het afnemen van Netwerk as a Service inclusief SIEM/SOC bij een externe partij.
- Optie 3 : Aanbesteding starten om de huidige situatie in beheer geven bij externe partij en om te zetten naar Netwerk as a Service inclusief SIEM/SOC.