

Bijlage 5 ICT infrastructuur GGD Zuid-Limburg

Huidige situatie (t/m medio 2025)

- Demarcatie service/support
 - o 1^e lijn Servicedesk ICT, netwerk- en serverbeheer zijn outsourced.
 - o Werkplekbeheer, printerbeheer, technician-to-technician support is bij team I&A belegd.
- Netwerk
 - o WAN
 - Alle locaties (hoofdlocatie en ~30 nevenlocaties) zijn verbonden met het datacenter, van waaruit een centrale internet feed beschikbaar is.
 - o LAN/WLAN
 - Alle clients authenticiseren o.b.v. 802.1x, incl. de printers/MFP's.
 - Er is sprake van netwerksegmentering o.b.v. (dynamisch toegekende) VLAN's (o.a. specifiek printer VLAN).
 - Printers hebben directe internet toegang t.b.v. ophalen firmware updates.
- Servers
 - o Betreft een hybride omgeving; deels on-prem, deels (Microsoft)cloud
 - o Eigen Microsoft 365 tenant met Entra ID (IdP), Enterprise apps, Conditional Access policies, Azure MFA, Exchange Online, OneDrive for Business e.d. ingericht
 - o On-prem Domain controllers, Active Directory (incl. AAD sync), ADFS, Fileserver, NPS server, Exchange server, Printserver (Windows Print Management + uniFLOW), Applicatieserver(s), RDS server(s)
 - o Huidige print/scan oplossing heeft relaties met:
 - uniFLOW
 - Fileserver: scan-to-folder (homefolder + afdelingsschijf)
 - Exchange Online: scan-to-mail, mail-to-print
 - Active Directory: LDAP koppeling (import gebruikers)
 - Entra ID: mail-to-print (OAuth 2.0)
 - iWMC
 - Applicatieserver (SNMP uitlezen status machines en consumables)
- Clients
 - o Laptops en desktops worden beheerd via SCCM, voorzien van een basis inrichting o.b.v. Windows 10 Enterprise (22H2).
 - o Laptops en desktops zijn Entra ID Hybrid Joined.
 - o Laptops zijn voorzien van Microsoft Direct Access VPN (medio 2024 Always On VPN), voor routing van specifiek netwerkverkeer (incl. print verkeer, in geval extern gewerkt wordt) via het datacenter.
Overig verkeer verloopt via het op dat moment geconnecteerde (privé-/bedrijfs)netwerk.
 - o Printers worden middels GPO beschikbaar gesteld.
 - Afhankelijk van groepslidmaatschap kan een gebruiker meerdere printers toegekend krijgen (meerdere verschillende printers of meerdere kopieën van dezelfde – follow-me – printer, maar met afwijkende default settings zoals kleur/zwart-wit).
 - Gebruikers hebben geen lokale beheerrechten, al kan een (lokale) thuis printer worden toegevoegd door een eindgebruiker zolang de driver standaard beschikbaar is in Windows 10 (vanwege het ontbreken van installatierechten).
 - o Printerdrivers worden opgehaald van de Windows Print Management server in het datacenter.
 - o Enkele traditionele client-server (legacy) applicaties worden o.b.v. Microsoft RDS aangeboden en zijn via RDP en clientless RDP (vanuit Workspace 365 portal) benaderbaar vanaf de clients. Ook vanuit deze RDS omgeving kan worden geprint.
 - o Bij enkele applicaties wordt gebruik gemaakt van Word sjablonen waarin meerdere laden zijn voorgedefinieerd om (deels) te kunnen printen op voorbedrukt papier.
- Specials
 - o Apparatuur
 - Zebra GK420t label printers (~ 20 st.); aangesloten op LAN, print queue management via Windows Print Management server
 - Fargo HDP5000 pasjes printer (1 st.); aangesloten op LAN, print queue management via Windows Print Management server
 - Konica Minolta 3300P (2 st.); aangesloten via USB op werkplekken voor forensisch artsen bij cellencomplexen.
 - HP LaserJet Pro M203dw (2 st.); aangesloten via USB op werkplekken bij AZC's.
 - o Gebruikersgroepen
 - GHOR: GHOR collega's van de GGD printen vanaf hun GGD laptop, maar via het Meldkamer netwerk in het MCC Maastricht, naar MFP's van de Meldkamer. De printers van de Meldkamer zijn op de Windows Print Management server van de GGD toegevoegd (o.b.v. Canon Generic Plus PCL6 driver) en print jobs worden via IP-VPN doorgezonden naar hun print server.

- Covid: De covid-medewerkers maken gebruik van compacte machines – zowel MFP als kleur laserprinters – die tijdens de pandemie binnen het bestaande contract zijn bijgeplaatst. Deze machines wijken qua specificaties af van de standaard binnen het contract geleverde A4 en A3 machines, maar zijn wel op de bestaande uniFLOW omgeving aangesloten en printen werkt eveneens op basis van secure print (aanmelding middels pasje).
De “special” in deze betreft het feit dat ad hoc is uitgebreid met een afwijkend type machine, wat qua configuratie enige uitdaging gaf vanwege afwijkende machine client. Qua werking en werkwijze is aangesloten op/bij de bestaande situatie, om extra beheerlast te voorkomen.
- MEES catering: medewerkers van de cateraar werken – enkel op de GGD hoofdlocatie – vanuit hun eigen VDI omgeving en printen naar een lokaal op hun laptop aangemaakte printer, die de jobs middels LPR forward doorstuurt naar de print server van de GGD. Op basis van generiek in uniFLOW aangemaakt account worden opdrachten opgehaald op de MFP.
- Ease Travel Clinic: medewerkers van de Ease Travel Clinic werken – op twee GGD locaties – deels lokaal op hun laptop(s), deels vanuit een VDI omgeving van MUMC. Lokaal op de laptop(s) is een printer aangemaakt die jobs middels LPR forward doorstuurt naar de print server van de GGD. Op basis van een tweetal generieke uniFLOW accounts worden opdrachten opgehaald op de MFP.
De VDI omgeving van MUMC ondersteunt geen local printer mapping. Derhalve is een S2S VPN connectie opgebouwd tussen de print server van MUMC en de print server van GGDZL, om printverkeer door te kunnen sturen.

Toekomstige situatie (vanaf medio 2025)

Op moment van schrijven (Q1 – 2024) vindt een heroriëntatie plaats t.a.v. de ICT infrastructuur i.v.m. een Europese aanbesteding voor ICT outsourcing medio 2024. Derhalve is er nog geen compleet beeld van de uiteindelijke ICT infrastructuur voor medio 2025 en daarna.

Enkele uitgangspunten en verwachtingen t.a.v. afwijkingen t.o.v. de huidige infrastructuur zijn wel reeds te benoemen (N.B. wat niet beschreven is, wijzigt niet ten opzichte van de huidige situatie):

- Demarcatie service/support
 - o N.v.t.
- Netwerk
 - o SD-WAN oplossing i.p.v. huidige IP-VPN/MPLS setup, i.v.m. meer flexibiliteit bij op- en afschaling van locaties (in crisissituaties). Uiteindelijke keuze afhankelijk van voorstel ICT dienstverlener.
- Servers
 - o Uitgangspunt wordt SaaS-/Cloud-tenzij, Microsoft 365 tenzij, dus minder on-prem servers, minder hybride configuraties (minder complexiteit).
 - o Fileserver: de verwachting is dat persoonlijke- en afdelingsdata gemigreerd worden naar respectievelijk OneDrive for Business en SharePoint Online, waarbij laatstgenoemde mogelijk pas in een tweede fase plaatsvindt i.v.m. complexiteit van inrichting.
 - o RDS server(s): zolang de traditionele client-server (legacy) applicaties niet zijn uitgefaseerd danwel gemigreerd naar de cloud, verwachten wij een virtual desktop omgeving (voorkeur Azure Virtual Desktop, maar RDS, Citrix, VMware VDI kunnen op dit moment niet uitgesloten worden) nodig te hebben voor het ontsluiten van deze applicaties, van waaruit geprint moet kunnen worden.
- Clients
 - o Laptops en desktops zullen voorzien worden van Windows 11 Enterprise.
 - o Uitrol van clients zal plaatsvinden o.b.v. Windows AutoPilot en beheer op basis van Intune (i.p.v. SCCM).
- Specials
 - o GHOR: De GHOR splitst per 1-1-2025 af van de GGD. Deze special vervalt derhalve.
 - o Covid: De covid-organisatie is intussen ingebed in de reguliere GGD organisatie, maar fors afgeschaald in omvang. In verband met pandemische paraatheid kan dit organisatie onderdeel indien nodig snel opgeschaald worden (verspreid over diverse – al dan niet tijdelijke en niet van directe datacenter connectie voorziene – locaties), waarbij de werkprocessen naar verwachting print functionaliteit zullen vereisen.
Datzelfde geldt voor periodieke vaccinatiecampagnes.