

ICT Infrastructuur gemeente Eemsdelta

Datum: december 2023
Auteur(s): Marko Overzet
Versie: 19.0



Inhoud

Inleiding.....	3
Netwerk.....	3
Servers.....	3
Operating systemen	3
Databases.....	3
Datagedreven werken	4
Werkstation omgeving	4
Remote support.....	4
Definitie SAAS.....	5
Algemeen.....	5
Authenticatie.....	5
Continuïteit	5
E-Mail.....	5
Integraties.....	6

Inleiding

De ICT infrastructuur van de gemeente Eemsdelta is gehuisvest in twee datacenters. Beide datacenters bevinden zich in Groningen. Eén van de datacenters is gevestigd op het bedrijventerrein Westpoort en de andere aan de Zernikelaan.

Netwerk

De gemeentehuizen in Appingedam, Delfzijl en Loppersum en de overige gemeentelijke locaties zijn voorzien van een internetverbinding. Werkplekken, laptops en thin clients, maken via internet verbinding met de Citrix farm in het datacenter. Alleen apparatuur dat rechtstreeks met back-end voorzieningen in het datacenter communiceert, maakt via een VPN-tunnel verbinding met de datacenters.

Beide datacenters zijn middels een redundante 10Gb verbinding met elkaar verbonden.

Servers

Het virtualisatieplatform, gebaseerd op technologie van VMware, is ondergebracht in het datacenter en is verdeeld in twee VMware clusters:

- Frontend voor de hosting van de virtuele Citrix Farm.
- Backend voor de hosting van de applicatieservers.

Alle storage wordt via VMware gekoppeld aan de vm's. Er wordt geen directe koppeling vanuit vm's aan storage shares toegestaan. Dit onder meer vanwege de back-up tool die gebruikt wordt voor het veiligstellen van de omgeving. Alle applicatieservers moeten middels VMware worden gevirtualiseerd op de bestaande infrastructuur. Het plaatsen van fysieke servers is niet toegestaan.

Operating systemen

De standaard operating system voor de kantooromgeving is Microsoft Windows. Op de applicatieservers en de Citrix servers is de standaard Windows 2016.

De autorisaties zijn geregeld via Active Directory. Er is één forest en één domein voor alle gebruikers. Voor mail, agenda en dergelijke wordt gebruik gemaakt van Exchange Online. Alle gebruikers vallen onder één Exchange omgeving.

Databases

De Aanbestedende Dienst heeft een nadrukkelijk SAAS tenzij beleid, maar biedt in haar datacenter ruimte en capaciteit voor on-premise oplossingen. On-premise applicaties kunnen op het bestaande virtualisatieplatform worden geïnstalleerd. Over de sizing van applicatieservers dient vooraf afstemming plaats te vinden. Voor eventuele databases hebben we alleen de beschikking over een Microsoft SQL en een PostgreSQL server. De Aanbestedende Dienst heeft de ambitie om een variëteit aan databasesystemen sterk te beperken. Niet Microsoft SQL en PostgreSQL databases dient de inschrijver op een door haarzelf, of door een derde, geleverde en beheerde omgeving te installeren. Deze kosten zoals bijvoorbeeld hardware, beheer, verbindingen en licentiekosten, dienen in de aangeboden prijs verdisconteerd te zijn.

Datagedreven werken

Om beter onderbouwde beslissingen te nemen en als organisatie beter aan te sluiten op de maatschappelijke opgaven, zet de gemeente Eemsdelta in op datagedreven werken. Voor het presenteren van analyses wordt gebruik gemaakt van Power BI dashboards. Applicaties, SAAS en on premise, die gebruik maken van een database, bieden minimaal de mogelijkheid om op gezette tijden (dagelijks, wekelijks) een extract van de database te maken naar een csv-bestand die vervolgens kan worden ingelezen in Azure Data Factory. Het maken van het database extract en het plaatsen van het csv-bestand op een on premise locatie wordt middels een geautomatiseerd proces uitgevoerd. De voorkeur geniet een API-koppeling tussen de database en Azure Data Factory.

Werkstation omgeving

Er wordt gebruik gemaakt van Citrix XenApp en Ivanti Workspace Control, toegankelijk vanaf thin clients die op de gemeentelijke locaties zijn geplaatst. Daarnaast vindt er een transitie plaats naar een moderne werkplek waarbij de medewerkers de beschikking hebben over een met Microsoft Intune beheerde laptop. Hiermee kan men verbinding maken met de Citrix Netscaler indien men gebruik wil maken van de Citrix desktop en de daarop aangeboden on prem toepassingen. Daarnaast heeft men met de laptop toegang tot de M365 tenant van de gemeente Eemsdelta en de verschillende cloud applicaties waar de gemeente gebruik van maakt.

De Windows Server versie op de XenApp servers is Windows 2016. Voor de applicatievirtualisatie wordt gebruik gemaakt van Microsoft AppV.

Het momenteel gebruikte office pakket op de Citrix farm is de 32-bits versie van Microsoft 365 Office. Voor mail wordt gebruik gemaakt van de Microsoft 365 Outlook client. Op de beheerde laptops wordt de 64-bits versie van Microsoft 365 Office aangeboden.

Voor het printen wordt op de Citrix desktop een Ricoh Follow Me print-service ter beschikking gesteld waarbij het mogelijk is om prints in een wachtrij te plaatsen en vervolgens op één van de beschikbare Follow Me printers na authenticatie op te roepen en af te drukken. De printers kunnen allemaal A4 en A3 in kleur en grijs tinten, enkel- of dubbelzijdig printen.

Als antivirus programma wordt op alle servers Sophos Intercept X Endpoint toegepast.

Gebruikers kunnen vanuit de Citrix desktop het internet alleen benaderen via een centrale firewall.

Gebruikers kunnen vanaf mobiele werkstations (laptops, tablets, smartphones) mail uitwisselen met de Exchange Online oplossing en verbinding maken met de Citrix Netscaler om vervolgens hun desktop omgeving te benaderen. Dit laatste werkt via two-factor authenticatie. Mobile werkstations maken via een Wifi-netwerk verbinding met het internet en hebben geen rechtstreekse verbinding met het on prem netwerk.

Remote support

Het is mogelijk om middels Teamviewer vanaf de leverancier een sessie naar een zogenaamde inbelmachine te krijgen. Vanaf deze inbelmachine wordt toegang naar de applicatieserver verzorgd. Inbellen gaat altijd in overleg met de applicatiebeheerder en, indien de applicatiebeheerder akkoord is, via de ICT servicedesk van de gemeente Eemsdelta.

Definitie SAAS

De gemeente Eemsdelta heeft gekozen voor een nadrukkelijk SAAS, tenzij beleid bij de aanschaf van nieuwe applicaties. De definitie, afgezien van specifieke functionele eisen, die de gemeente Eemsdelta voor SAAS hanteert is als volgt:

Algemeen

- Voor het gebruik van de oplossing volstaat de webbrowser Edge Chromium. De browser is qua versie/updates maximaal 1 jaar oud en ondersteund door de ontwikkelaar van de browser.
- Gebruik van een plug-in (o.a. Java/Flash/Silverlight) is in verband met informatieveiligheid, beheer en onderhoud niet toegestaan.
- Er is geen installatie van software(componenten) nodig om de oplossing te kunnen gebruiken. Een uitzondering hierop is de eventuele installatie van software die zorgdraagt voor beveiligde gegevensuitwisseling tussen de on premise omgeving en de SAAS oplossing. Deze software voldoet aan de onderstaande eisen:
 - o Indien de applicatie op de werkplek (XenApp server) wordt aangeboden, is de applicatie multi-user aware, compatible met Citrix XenApp en Ivanti Workspace Control en draait deze niet als een Windows service.
 - o De gegevensuitwisseling is versleutelt.
- Onder een eindgebruiker worden alle gebruikers verstaan die gebruik maken van de SAAS oplossing.
- De oplossing draait volledig in het datacenter van de opdrachtnemer.
- De leverancier zorgt er voor dat de opdrachtgever geen last heeft van onwenselijk gedrag van andere klanten. (Bijv. spamming vanuit eenzelfde ip-adres)
- De leverancier zorgt er voor dat het netwerkverkeer tussen de verschillende omgevingen niet kan worden onderschept door andere klanten die actief zijn binnen de systeemomgevingen van de leverancier.

Authenticatie

Authenticatie voor SAAS toepassingen verloopt middels OAuth 2.0 in combinatie met Azure Active Directory. Kosten hiervan zijn volledig inbegrepen in de aanbieding.

Binnen de Citrix sessie hebben de gebruikers na authenticatie via de on premise Active Directory door middel van Single Sign On (SSO) direct toegang tot alle onderdelen van de SAAS oplossing. Uiteraard voor zover ze daartoe zijn geautoriseerd. Met SSO hoeft de gebruiker niet apart in de login in de oplossing nadat de gebruiker is aangemeld op het netwerk (via Active Directory). Alleen om specifieke functioneel beheer-rechten te krijgen is het toegestaan dat er een handmatige login nodig is.

Continuïteit

Onderliggende softwarecomponenten, zoals besturingssystemen, databasesoftware, browser versie, programmeer framework, enz., waarop de software is gebouwd en draait dienen altijd een door de oorspronkelijke leverancier van de betreffende software of framework ondersteund te zijn.

E-Mail

Het versturen van e-mail dient te verlopen via de gemeentelijke Exchange Online omgeving. Indien nodig wordt er gebruik gemaakt van de FileCap plug-in om beveiligd te kunnen mailen.

Integraties

- Indien de opdrachtgever er voor kiest om tussen de oplossing en andere systemen basisgegevens uit te wisselen, gebeurt dit conform het sectormodel StUF BG v3.10¹. Indien binnen de looptijd van het contract een nieuwe StUF formaat wordt uitgebracht, dient de opdrachtnemer deze binnen 1 jaar na vaststelling van het nieuwe StUF formaat te ondersteunen.
- De opdrachtnemer waarborgt dat de oplossing niet meer dan één major versie achterloopt ("backwards compatible") op de open standaarden van het Forum Standaardisatie. Daarnaast wordt de oude versie nog minimaal 12 maanden ondersteund.

¹ https://www.gemmaonline.nl/index.php/Sectormodel_Basisgegevens:_StUF-BG#Documenten