

Karakterisering ICT-infrastructuur Gemeenten Vlissingen en Middelburg.

Versie V21, 4 maart 2022

Algemeen.

De gemeenten Middelburg en Vlissingen hebben de ICT-infrastructuur gezamenlijk vormgegeven. Kernbegrippen daarbij zijn: gezamenlijk gebruik van ICT-componenten, virtual servers, serverbased computing, interne hosting, non-dedicated servers, een vergaand beveiligd, gesegmenteerd netwerk en een gecentraliseerd technisch beheer. De gezamenlijke ICT-infrastructuur wordt beheerd door de I&A Samenwerking. Nieuwe applicaties dienen clientless en bij voorkeur webbased (HTML5, zonder benodigde plug-ins) te zijn. De applicaties mogen zowel on-premise als in de cloud worden gehost. Zowel infrastructuur als beheerorganisatie zijn daar op ingericht.

Goede inpasbaarheid in de infrastructuur vinden we erg belangrijk. Om eventuele knelpunten in een zo vroeg mogelijk stadium te onderkennen geeft dit document een aantal karakteristieken weer. Aan de hand hiervan kan een leverancier van software een eerste inschatting maken van de geschiktheid van zijn software voor deze omgeving. Daarbij is het belangrijk om te realiseren dat bij incompatibiliteit de infrastructuur niet zal worden aangepast aan de software.

De eerste indruk zal niet altijd voldoende zijn om met zekerheid te kunnen vaststellen of software wel of niet in de ICT-infrastructuur volledig zal kunnen functioneren. Vaak zal gedegen overleg op technisch niveau, of zelfs een testinstallatie (pilot), nodig zijn om deze zekerheid te verkrijgen. Indien een situatie daar om vraagt, zal dit nadere onderzoek deel uitmaken van een marktverkenning of selectieprocedure en voor de verantwoordelijkheid van de leverancier komen.

De ICT-infrastructuur is continu aan veranderingen onderhevig. Gebruikte technieken zullen regelmatig veranderen gezien de ontwikkelingen in de markt. Volgens de GIBIT wordt van leveranciers verwacht dat zij zich, voordat er aanbiedingen worden gedaan, voldoende op de hoogte hebben gesteld van de ICT-omgeving (inclusief applicatielandschap) van de gemeente om te zorgen dat de aanbieder (zonder meerkosten) geschikt is om in die omgeving naar behoren te functioneren. Dit document is bedoeld om leveranciers een eerste indruk te geven van de karakterisering en is per definitie niet voldoende volledig en actueel om een beroep op te doen vanuit deze z.g. analyse-plicht zoals in de GIBIT opgenomen.

Servers.

Een farm van ca. 60 (virtuele) terminalservers voorzien van Citrix XenApp 7 1909 worden geboot vanaf dezelfde virtuele bootdisk, de z.g. Golden Image, met behulp van Citrix PVS. Alle terminalservers zijn dus identiek wat betreft instellingen en software. Het gebruikte operating system is Windows Server 2016 en de applicaties worden gestart vanaf de golden disk en geladen in het RAM geheugen van een terminalserver. Ca. 1200 werkplekken, uitgerust met thin clients, en een flink aantal remote/mobile werkplekken worden via loadbalancing verbonden met een willekeurige terminalserver in de farm waarop met behulp van een token en wachtwoord kan worden ingelogd.

Komende jaren vindt een migratie plaats van Citrix XenApp en thin clients naar managed Windows 11 laptops. Aangeboden producten dienen in beide omgevingen inpasbaar te zijn.

Voor webapplicaties en de daarbij horende databases worden applicatie- en databaseservers ingezet. Deze zijn non-dedicated, dus meerdere webapplicaties (of databases) delen een server. Webapplicatie- en databaseservers hebben Windows 2016 of 2019 x64 als operating system. De servers worden elke maand voorzien van Windows Updates. Na installatie mogen er geen handmatige acties nodig zijn om de software goed te laten functioneren.

Alle back-end servers zijn gevirtualiseerd via VMWare vSphere 6.7. De Citrix Xenapp servers zijn gevirtualiseerd via XenServer.

Software en daarbij horende services mogen nooit draaien met administrator rechten.

Databases.

Ondersteunde databases zijn een cluster SQL Enterprise 2017 en Oracle 19 Enterprise Edition (op basis van Melodies).

Op de database servers worden databases gehost van verschillende applicaties/leveranciers. Het is dus niet mogelijk om resources exclusief te reserveren voor een bepaalde database.

Clients.

Het merendeel van de gebruikers logt middels thin clients in op de terminalservers. Deze worden medio 2022 vervangen door managed Windows laptops.

Slechts bij onvermijdelijke uitzondering kan na overleg software op de laptop worden geïnstalleerd. Deze applicaties worden niet rechtstreeks geïnstalleerd, maar na installatie op een centrale package omgeving gedistribueerd naar de laptops.

Bij uitzondering kan voor grafisch zware applicaties en applicaties die backend servers nodig hebben uitgeweken worden naar VDI. De VDI omgeving is op basis van XenDesktop. Het gaat hierbij om non-persistent Windows 10 virtual machines. Alle VDI werkstations worden geboot vanaf dezelfde bootdisk, de z.g. Golden Image, met behulp van Citrix PVS. Alle VDI werkstations zijn dus identiek wat betreft instellingen en software.

Bij geen enkel workstation (thin of fat) bestaat de mogelijkheid om via USB, Bluetooth, WiFi etc. verbindingen te maken met andere devices of netwerken.

De software mag nooit draaien met administrator rechten.

Gebruikers hebben geen administrator rechten op werkstations, servers etc.

Voor tablets en smartphones wordt gebruik gemaakt van apparatuur van Apple in combinatie met MDM van Mobile Iron. Medio 2022 hiervoor naar verwachting Microsoft Intune worden ingezet.

Netwerkbeveiliging.

Datacommunicatie van binnen naar buiten (buiten het gemeentelijk netwerk) loopt altijd via onze authenticated firewall.

Datacommunicatie van buiten naar binnen loopt altijd via onze reverse proxy en of firewall. Servers mogen niet naar buiten communiceren, in uiterste gevallen alleen naar een bekende en passend beveiligde destination. De te ontsluiten websites mogen geen gebruik maken van Websockets.

Terminalservers en applicatieservers (w.o. databaseservers) zitten in verschillende netwerksegmenten. Datacommunicatie tussen deze servers wordt gecontroleerd en beperkt door een firewall.

Alle gebruikers delen een 1000 mb/s up en down internetverbinding voor alle internetverkeer. Toegang tot public Cloud services zoals DropBox, iCloud, etc. vanuit het netwerk is niet toegestaan. De gemeenten maken gebruik van een eigen corporate cloud o.b.v. Nextcloud, medio 2023 zal hiervoor Onedrive worden ingezet.

Bij dataverbindingen naar externe partijen zoals landelijke voorzieningen en leveranciers wordt er altijd gebruik gemaakt van OpenTunnel als Enterprise ServiceBus. Aansluitingen op MijnOverheid worden ook via OpenTunnel gerealiseerd. Alleen de protocol TLS 1.3 wordt gebruikt. HTTP-koppelingen zijn altijd op basis van certificaten, dus HTTPS.

Voor gegevens uit de BRP, BAG en HR wordt aangesloten op de databroker key2DD van Centric.

Websites.

Vanuit de eigen infrastructuur wordt een aantal extern bereikbare (openbare) websites gehost. Hiertoe zijn in de infrastructuur voor bepaalde typen websites (vertrouwelijkheid, performance, gebruikte technieken, ...) speciale voorzieningen getroffen. Aan de ene kant betekent dit dat bepaalde websites on-premise gehost kunnen worden. Anafhankelijk van de hosting-variant moeten openbare websites toegankelijk zijn voor de archiveringssoftware van onze archiefdiensten, veelal gebaseerd op webcrawlers en andere geautomatiseerde onderzoeks- en inventarisatieprocessen. Voor het ontsluiten van websites worden zowel intern als in de cloud de richtlijnen van het NCSC gevolgd. Daarvoor benodigde informatie wordt door de leverancier aangeleverd.

Software.

Standaard software is MS Office 2013 (met outlook/Exchange), laatste of 1-na laatste versie FireFox, laatste of 1-na laatste versie Edge (met Chromium Open Source als basis). Medio 2022 zal worden overgegaan op MS Office 365.

Voor Unified Communications wordt gebruik gemaakt van Skype. Medio 2022 zal worden overgegaan op MS Teams.

Standaard schermresolutie is 1920 x 1080 of 1920 x 1200.

Single Sign On wordt ondersteund op basis van Azure AD en ADFS (legacy).

Niet-versleutelde authenticatiestings zijn - ook binnen het netwerk - niet toegestaan.

Remote support.

24*7 remote toegang tot systemen, bijvoorbeeld via een VPN is niet toegestaan.

Installaties, updates, tests, configuraties, troubleshooting etc. worden waar mogelijk on-site uitgevoerd. Alle acties tijdens deze activiteiten worden automatisch gelogd. In geval van calamiteiten kan voor troubleshooting gebruik worden gemaakt van Remote Access.

Clouddiensten.

De gemeente biedt haar medewerkers een integrale en veilige digitale werkomgeving. De gemeente wil vanuit deze werkomgeving alle benodigde applicaties en diensten kunnen aanbieden. Af te nemen Cloud diensten dienen naadloos opgenomen te kunnen worden binnen deze digitale werkomgeving. De gemeente ziet een verbinding vanuit deze werkomgeving van gemeente naar een Clouddienst door middel van bijvoorbeeld RDP of VDI niet als een naadloze integratie.

Data-uitwisseling tussen lokale ICT-infrastructuur en Clouddiensten vindt plaats door middel van een Enterprise Service Bus (ESB). Hiervoor gebruiken de gemeenten Opentunnel.