

ICT–infrastructuur gemeente Utrecht v1.6¹

Bijlage 1: De ICT-infrastructuur van de Gemeente Utrecht

Toepassing

Dit document geeft een algemene beschrijving van de technische inrichting van de ICT binnen de Gemeente Utrecht en kan met externe partijen worden gedeeld als zijnde achtergrond informatie bij offertetrajecten en/of aanbestedingen.

Algemeen

De door de leverancier aan te bieden applicatie dient aan te sluiten op de binnen de Gemeente Utrecht geldende standaards ten aanzien van de ICT-infrastructuur. In onderstaand overzicht is de vigerende ICT-infrastructuur weergegeven en daar waar van toepassing en nu reeds bekend welke de toekomstige zijn.

Kantoor locaties

De gemeente Utrecht kent diverse locaties, het Stads kantoor Utrecht (SKU) is de hoofdlocatie. De overige locaties zijn verspreid over het verzorgingsgebied van de gemeente Utrecht.

Datacenters

De Gemeente Utrecht kent twee datacenters, ieder datacenter kan de volledige uitwijk faciliteren voor het andere datacenter.

Netwerk

Het netwerk binnen de Gemeente Utrecht is opgebouwd met Cisco netwerk componenten. Netwerk virtualisatie wordt gerealiseerd met behulp van VMWare NSX.

Er wordt gebruik gemaakt van 'next gen' firewall technologie. De verschillende locaties van de Gemeente Utrecht zijn met elkaar verbonden middels een stervormig netwerk op beide datacenters.. De core netwerk infrastructuur is redundant uitgevoerd en netwerk load balancing wordt toegepast om de belasting evenredig te verdelen. Er is een draadloze infrastructuur op basis van de 802.11n standaard. Er wordt gebruik gemaakt van 802.1X authenticatie.

Storage

Er zijn twee storage platformen op basis van NetApp. Het primaire platform op basis van Metrocluster waarbij replicatie van de data vanuit het storageplatform is ingericht.

Het tweede platform voorziet in storage per datacenter, deze wordt niet vanuit het storage platform gerepliceerd. Hierop wordt op applicatie of services niveau hoog beschikbare diensten geplaatst waarbij de replicatie door de applicatie is ingeregeld.

Hosting platform

Het platform voor server en desktop hosting is gebaseerd op het FlexPod voor VMWare concept van Cisco en NetApp.

Op dit platform wordt applicatie hosting aangeboden op basis van:

- Windows Server 2019 (standard);
- RedHat 7.X Enterprise Linux;

¹ Controleer altijd of de laatste versie wordt gebruikt, deze is op het [intranet](#) te vinden.

- Oracle Linux voor hosting van Oracle databases; Het platform is gebaseerd op de keuze virtualisatie tenzij.

DMZ

Er is een apart segment beschikbaar voor de ontsluiting van extern gerichte diensten en web services. Deze omgeving wordt middels next-gen firewalls gescheiden van de overige omgevingen. In de virtuele netwerk laag (VMWare NSX) kan gebruik worden gemaakt van DMZ Anywhere.

OTAS Omgevingen

De Gemeente Utrecht maakt gebruik van het OTAS principe voor het acceptatie proces. Er wordt gebruik gemaakt van twee middels fysieke netwerk scheiding OTAS omgevingen waarbij netwerk virtualisatie wordt toegepast voor verdere scheiding binnen deze omgevingen. Er is een OTAS omgeving voor klant toepassingen en één voor ICT-beheer toepassingen. De OTAS omgevingen zijn zoveel mogelijk functioneel representatief t.o.v. productie ingericht.

Microsoft Cloud en Azure

De gemeente Utrecht heeft de beschikking over twee Microsoft Azure tenants, een productietenant welke gekoppeld is aan de productie omgeving en een test-tenant is gekoppeld aan de OTAS omgeving voor klant toepassingen. Er is een directe synchronisatie tussen de Utrecht directory en Azure AD voor beide omgevingen. Office 365 componenten en Intune voor MDM worden gebruikt.

Databases

Binnen de Gemeente Utrecht wordt gebruik gemaakt van Oracle 12 en Microsoft SQL Server 2019 databases, SQL 2017 is na goedkeuring beschikbaar. Als alternatief kan MariaDB op basis van de Linux distributie ingezet worden.

Werkplek

De werkplek wordt op basis van Windows 10 aangeboden middels VMWare Horizon. Taak applicaties worden op basis van applicatievirtualisatie aangeboden. Er wordt gebruik gemaakt van een lokale Microsoft Office 365 Proplus C2R installatie. De gemeente Utrecht maakt gebruik van een gecontroleerde standaardwerkplek. Het beheer van de werkplek vindt plaats m.b.v. Ivanti Workspace control.

Email

De primaire mailserver bestaat uit een Exchange 2016 omgeving met database replicatie. Er is een hybride koppeling met de Office 365 omgeving. Inkomende en uitgaande email wordt via Microsoft Endpoint Protection verzonden. De migratie van mailboxen naar Exchange online wordt in 2021 gestart.

Telefonie

Het telefonieplatform is gebaseerd op een Avaya VOIP oplossing. Daarnaast wordt er gebruik gemaakt van openbare en Private GSM oplossingen. Op de werkplek wordt gebruik gemaakt van de Avaya One-X Communicator. In combinatie met de GSM oplossingen wordt deze gebruikt voor signalering en gaat spraak over het GSM netwerk. Voor kleinere locaties wordt gebruik gemaakt van de SIP oplossing van Avaya en ook de IP-Dect oplossing van Avaya wordt op verschillende locaties gebruikt. Het telefonieplatform is redundant uitgevoerd.

Privileged Access Management

Voor het beheer van toegang tot systemen en verhoogd risico identiteiten wordt er gebruik gemaakt van een digitale kluis in de vorm van CyberArk. Alle verhoogde accounts worden hierin opgenomen en wachtwoorden worden zo mogelijk automatisch gerouleerd. Dit geldt voor beheerders-, service-,

leveranciers en andere verhoogde toegang accounts. Toegang tot de digitale kluis vindt plaats middels een tweede factor.
Alle beheerwerkzaamheden dienen via de CyberArk portal plaats te vinden.

Beheer op afstand door leverancier

Er is geen directe toegang mogelijk tot systemen vanaf externe netwerken. Leveranciers dienen via de werkplek (VDI) en CyberArk gecontroleerd toegang aan te vragen. De sessie daaruit voort komend kan live ingezien of opgenomen worden voor audit doeleinden.

Multi functionele printers

Voor afdruk, scan en mail taken wordt er gebruik gemaakt van Multi functionele printers. Alle printers hebben meerdere papierlades met verschillende types papier. Er is één uniforme driver in gebruik.

Intranet en internet website

Voor het intranet en internet site van de gemeente Utrecht wordt gebruik gemaakt van het Content management Systeem Typo3.

Samenwerkingsomgeving

Voor het samenwerken maakt Gemeente Utrecht gebruik van Alfresco. Deze is middels een web interface intern toegankelijk. Er wordt tevens gebruik gemaakt van Microsoft Teams voor video vergaderen en team sites.

IAM proces

Medewerkers, externen en ketenpartners worden vanuit bronsystemen geautomatiseerd beheerd gedurende de gehele levenscyclus van het identiteit. Binnen het IAM systeem is selfservice beschikbaar en kunnen rollen worden toegekend. Taak applicaties kunnen worden aangesloten op het IAM systeem zowel voor identiteiten provisioning als voor rollen en RBAC. De gemeente Utrecht is actief met het verder ontwikkelen van het IAM systeem en het toekennen van rollen en rechten.

Identity management en federatie

Medewerkers van de Gemeente Utrecht beschikken over één identiteit en een 2^e factor op basis van Microsoft MFA. Ten behoeve van SSO voor SaaS applicaties en cloud diensten is er federatie mogelijk. Er wordt gewerkt met een RBAC model volgens least-privilege en SSO integratie. Er is een intern IAM systeem waarop taak applicaties voor rollen en identiteitsmanagement worden aangesloten. Hiervoor zijn aansluitvoorwaarden van toepassing (zie bijlages)

Integratie met clouddiensten

Voor de ontsluiting en het uitwisselen van gegevens met clouddiensten beschikt de gemeente over verschillende koppelvlakken. Uitwisseling van gegevens dient plaats te vinden op basis van encryptie op zowel de transport- als de data laag bij voorkeur middels een pull vanuit de gemeente. Externe verbindingen worden altijd in het DMZ ontsloten. De omgeving is afgeschermd middels een Nextgen firewall. Een Enterprise Service Bus oplossing is beschikbaar.

Tabel 1 Revisietabel

Versie	Naam	Datum	Wijziging
1.3	Martijn Spelt	ntb	Eerdere versies
1.4	Martijn Spelt	14-12-2020	Algehele update UDW/cloud + revisietabel
1.5	Martijn Spelt	21-12-2020	Actualisatie nieuwe infracomponenten
1.6	Martijn Spelt	12-05-2021	Windows Server 2019 als standaard