

BIJLAGE 4: HUIDIGE ICT-INRICHTING EN DE NIEUWE CLOUDARCHITECTUUR

Behorende bij de Inschrijvingsleidraad Midoffice systeem van de gemeente Pijnacker-Nootdorp

1. Visie op Informatisering & Automatisering

Pijnacker-Nootdorp onderkent de volgende ontwikkelingen:

- ICT moet dienstbaar zijn aan de steeds digitaler werkende professional. Generieke functionaliteit organiseren we daarom steeds meer direct om de professional. Tijd-, locatie en device onafhankelijk.
- De totale overheid en daarmee ook Pijnacker-Nootdorp zal steeds meer in ketens samenwerken.
- Datagedreven sturing van zowel de bedrijfsvoering als het beleid neemt toe.
- Groei van het aantal op data en 'algoritmes' gebaseerde gemeentelijke diensten (combinatie van basis- en kernregistraties).
- Toename van (organisatie-overschrijdend) project- en programmatisch werken.
- Wens tot financiële flexibiliteit (verschuiving van statische kapitaalslasten naar operationele lasten die meebewegen met de mate waarin de organisatie gebruik maakt van de voorziening).
- Het belang van korte implementatietijden van nieuwe toepassingen groeit.
- Een groeiend belang van generieke functionaliteit binnen de digitale werkomgeving van de professional.
- Minder (technische en functionele) afhankelijkheid van de kantoorlocaties.
- Taken rond de inwinning, beheer en ontsluiting van data (kern- en basisregistraties. Administratief en geografisch) nemen toe en worden steeds meer een primair proces van de gemeente.
- Computing/automatisering verwordt steeds meer tot een commodity c.q. een dienst.

Deze ontwikkelingen hebben één gemeenschappelijk kenmerk: de informatisering en de automatisering zullen wendbaar (agile) ingericht moeten worden. Pijnacker-Nootdorp heeft dit o.a. vertaald in een cloudstrategie.

In deze paragraaf is de huidige ICT-architectuur van Pijnacker-Nootdorp beschreven. Deze infrastructuur zal als gevolg van bovenomschreven ontwikkelingen de komende jaren ingrijpend wijzigen. Pijnacker-Nootdorp gaat een hybride cloudarchitectuur realiseren. De contouren van deze strategie zijn in dit hoofdstuk beschreven.

2. Huidige architectuur

Het gemeentelijke ICT landschap bestaat bij de gemeente Pijnacker-Nootdorp uit de volgende zaken:

Client-kant

De basis configuratie wat betreft de clients zijn standaard thin clients van Dell Wise D90D (450). Deze Thin clients draaien met Windows 8 Embedded. Zij starten op via Citrix waarbij gebruik gemaakt wordt van de Citrix Receiver (op dit moment versie 4.4) om aan te loggen.

Deze clients worden door middel van de Dell Wise tool voorzien van een nieuw image waar nodig.

Er zijn 20 workstations Dell Precision T5610 in gebruik die worden gebruikt door CAD-tekenaars en GEO-specialisten mensen. Op deze workstations draait Windows 7 professional. Deze werkplekken worden handmatig geupdate via een USB-stick.

Binnen de gemeente heeft HNW zijn intrede gedaan waarbij niet alleen de thin client of workstation wordt gefaciliteerd maar afhankelijk van profiel ook andere devices ter ondersteuning worden geleverd.

De volgende devices zijn in gebruik:

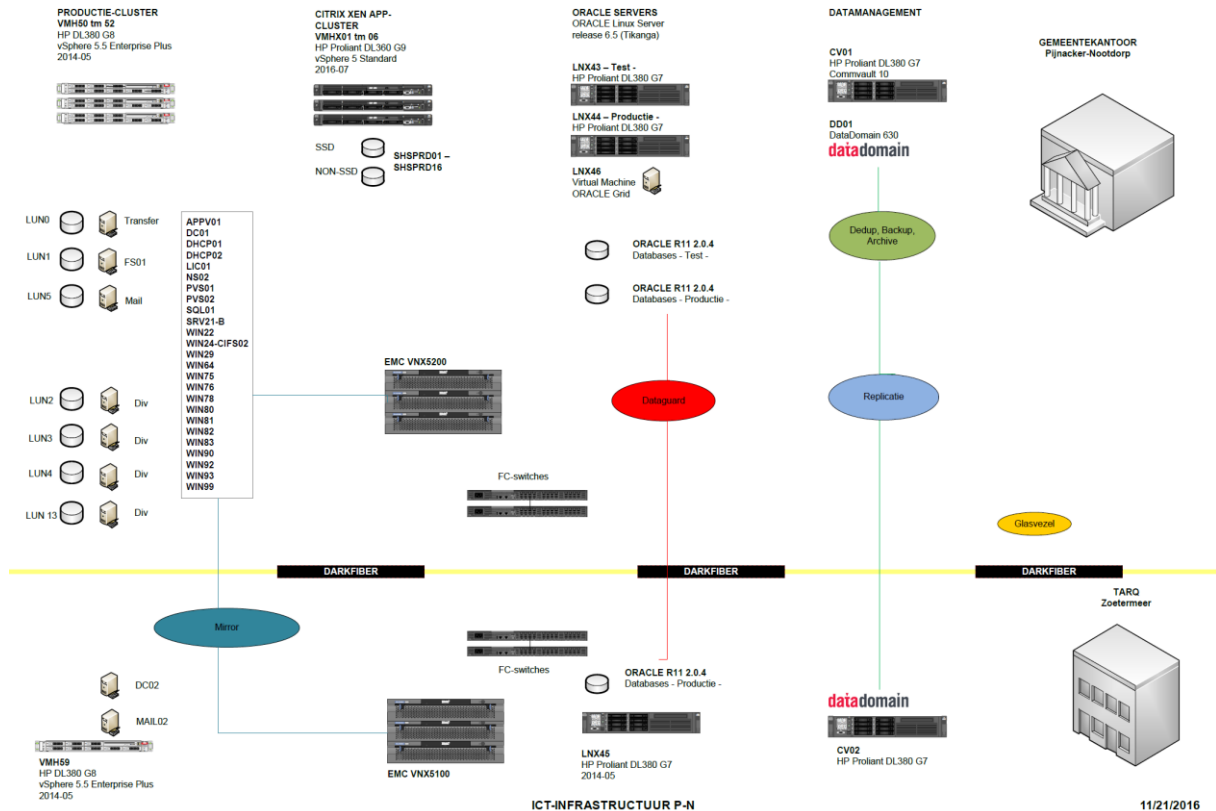
- Laptops
 - o 95 Laptops: Dell 6430U-E5450-E6420-E7440 met Windows
 - o 76 Laptops: Dell E5470 met Windows 10
 - o Beleid: Alle nieuwe laptops via Dell worden aangeschaft met Windows10 besturingssysteem.
- Tablets
 - o 170 i-Pads type 3, 4, air en air2
 - o 5 Microsoft Surface met Windows 10
- Smartphones
 - o 271 medewerkers hebben een smartphone type Samsung, HTC of Apple
 - o Na 2-3 jaar worden de smartphones vervangen.
 - o Beleid: De gemeente is voornemens om dit jaar/volgend jaar iedere medewerker te voorzien van een zakelijke smartphone.

Server-kant

De clients maken connectie met Windows Server 2012 waarop Office 2010 draait. Op mailgebied wordt gebruik gemaakt van Exchange 2010.

Telefonie wordt ingevuld door een Mitel Centrale (MXE-III) draaiende op versie 'release level 7.2'. Beleid: gemeente is voornemens om de telefooncentrale te vervangen door het Unified Communications concept.

Voor verdere specificaties wordt verwezen naar onderstaande architectuurplaat.



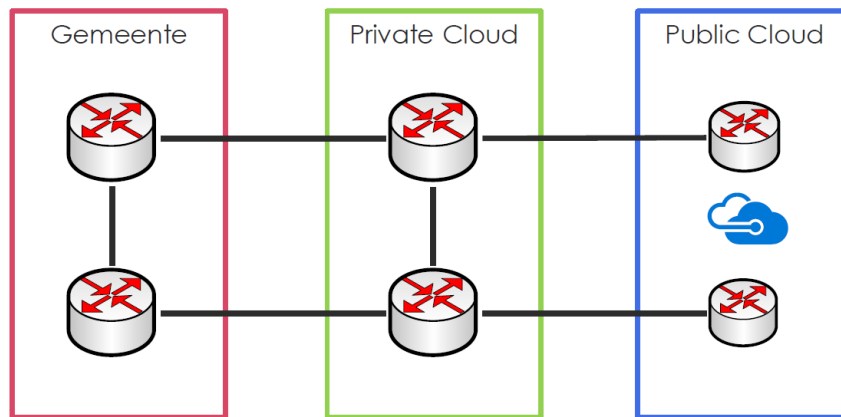
3. Cloudstrategie Pijnacker-Nootdorp

De komende 4 jaar transformeert Pijnacker-Nootdorp haar huidige ICT-infrastructuur en applicatielandschap richting een hybride cloud-architectuur. In hoofdlijnen komt deze strategie er op neer dat Pijnacker-Nootdorp haar 'eindige' on-premise infrastructuur uitbreidt naar een private cloud (IaaS oplossing van een nog te selecteren derde partij) en een public cloud (IaaS en PaaS services van het Azure platform van Microsoft). Hiertoe heeft zij momenteel de volgende Microsoft licenties aangeschaft:

- Office365 E3
 - Exchange Online Plan 2
 - SharePoint Online Plan 2
 - Skype for Business Online Plan 2
 - Yammer Enterprise
 - Office Online
 - Office 365 ProPlus
 - OneDrive
 - Sway

In de volgende uitwerkingen is aangegeven met welke producten de architectuur invulling krijgt.

Voor de traditioneel gemeentelijke applicaties zal Pijnacker-Nootdorp gebruik gaan maken van SaaS oplossingen.



3.1 Ontwikkelingen functioneel

Pijnacker-Nootdorp herkent een trend rond een verschuiving van taakspecifieke toepassingen naar generieke toepassingen (waaronder Pijnacker-Nootdorp ook de Midoffice applicaties schaaft). Routinematige werkzaamheden worden toenemend geautomatiseerd. Wat resteert zijn de niet-routinematige werkzaamheden die professionals uitvoeren met behulp van generieke functionaliteit. Pijnacker-Nootdorp heeft de volgende drie concepten vertaald in een architectuur rond generieke functionaliteit.

Content & Communicatievormen gekoppeld

De techniek maakt het mogelijk om synchrone (voice, chat, video) en a-synchrone (e-mail, voicemail) vormen van communicatie te koppelen aan content (sites, zaken, documenten/ bestanden, agenda). De gebruiker staat in dergelijke concepten centraal.



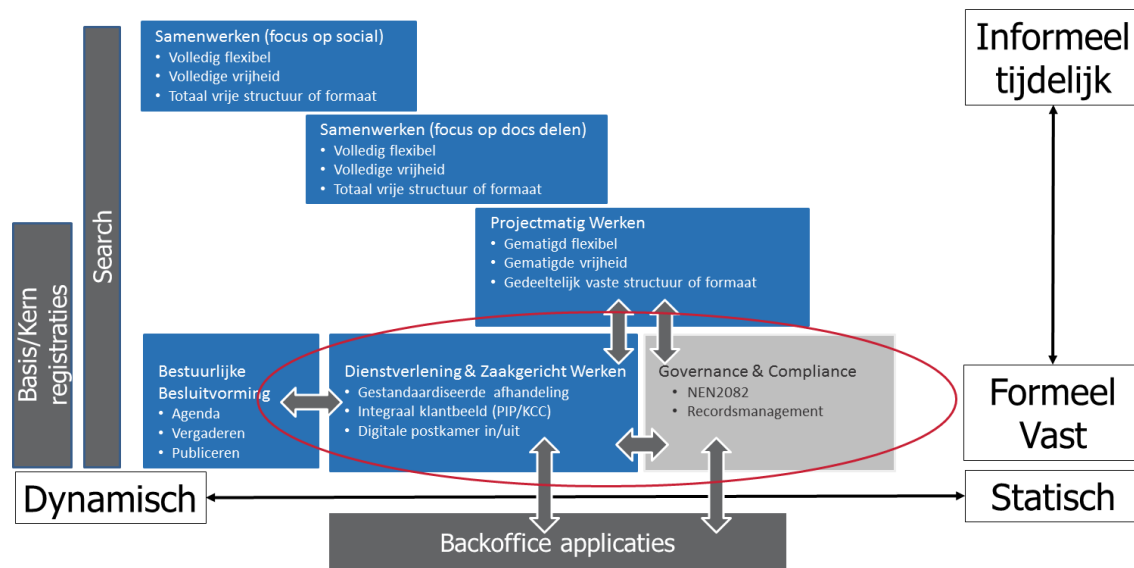
Dergelijke concepten zijn door marktpartijen uitgewerkt in Unified Communications concepten. De identiteit van de gebruiker staat in UC-concepten centraal. Door koppeling van UC-functionaliteiten aan één identity-store creëren we een single sign-on beleving voor de gebruiker. Variatie in de user-interface wensen we zoveel mogelijk te voorkomen om de leercurve voor de gebruiker zo stijl en kort mogelijk te houden.

Invulling Pijnacker-Nootdorp:

- Microsoft Skype for Business in combinatie met Microsoft Office365 (E3)
- Integratie vaste en mobiele telefonie op basis van Skype for Business (PBX)
- Windows Active Directory in combinatie met Azure Active Directory.

Verscheidenheid in samenwerkingsvormen

Medewerkers werken steeds meer team-, afdelings- en organisatie-overschrijdend samen in meer en minder geformaliseerde werkprocessen. In processen met een hoog en een laag documentair karakter. Dit is in onderstaande afbeelding gevisualiseerd:



De Midoffice dekt – inclusief de diverse koppelingen – het omcirkelde deel in bovenstaande afbeelding af. Daarbovenop onderkennen we samenwerkingsfunctionaliteit die steeds meer vrijheidsgraden biedt aan de gebruikers. Vanuit de samenwerkingsomgeving voor projectmatig werken moet het mogelijk zijn om geautomatiseerd documenten over te hevelen naar het Zaaksysteem cq. het formele archief (die beiden onderdeel uitmaken van de Midoffice). Het moet mogelijk zijn om gebruikers van buiten het eigen Pijnacker-Nootdorp domein toegang te geven tot een deel van de samenwerkingsfunctionaliteit.

Invulling Pijnacker-Nootdorp:

- Samenwerken met focus op social: hiervoor zal separaat een social intranet worden geselecteerd en geïmplementeerd.
- Samenwerken met focus op het delen van documenten: deze functionaliteit wordt ondergebracht in Microsoft OneDrive (als onderdeel van Office365).
- Projectmatig werken: hiervoor wordt een SharePoint omgeving ingericht. Het is nog niet besloten of deze SharePoint op de Azure IaaS omgeving wordt geïnstalleerd of dat hiervoor SharePoint online van Office365 wordt ingezet.

Mobile first

De professional kiest het device dat het beste past bij zijn specifieke situatie (werklocatie, applicaties, digitale vaardigheden, persoonlijke voorkeur). Functionaliteit en content bieden we medewerkers locatie- en device-onafhankelijk aan. Het design van (vak)applicaties is responsive zodat hiermee gewerkt kan worden vanaf een diversiteit aan mobiele devices. Om de kracht van het device optimaal te benutten (multimedia, connectiviteit, GPS) en het gebruiksgemak te bevorderen (1 click verwijderd van functionaliteit) moeten applicaties

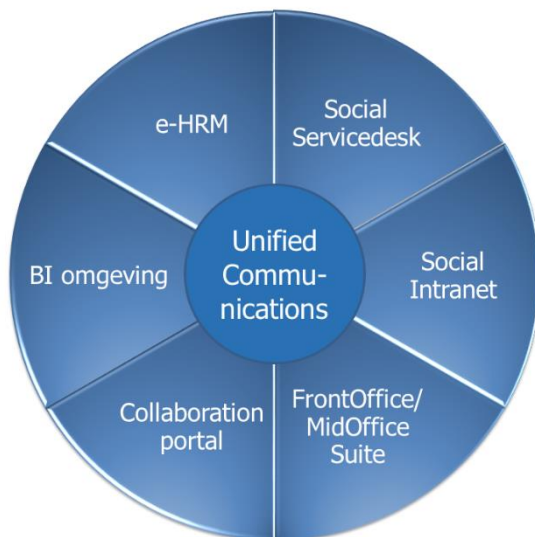
rechtstreeks richting de devices gepubliceerd worden en niet indirect via een 'virtuele' desktop.

Invulling Pijnacker-Nootdorp:

- Pijnacker-Nootdorp gaat voor de benodigde applicaties SaaS oplossingen selecteren.
- Pijnacker-Nootdorp gaat de lokale AD extender naar de Azure AD van Microsoft. Dit biedt de mogelijkheden om een groeiend aantal SaaS oplossingen op eenvoudige wijze aan onze AD te koppelen.
- Pijnacker-Nootdorp gaat gebruik maken van het public cloud Azure platform van Microsoft (IaaS) als doelplatform ter vervanging van de on-premise infrastructuur. On-premise geïnstalleerde toepassingen zullen op basis van een technisch/financiële afweging worden ondergebracht op dit Azure platform.

3.2 Generieke functionaliteit

Deze 3 concepten leiden tot een laag 'Generieke functionaliteit' in onze architectuur met de volgende functionele toepassingen die door alle medewerkers gebruikt kunnen worden:



Het Unified Communications concept vormt het hart van deze generieke laag in onze functionele architectuur.

Applicaties zijn bij voorkeur 'UC-aware' (de accountnaam van de medewerker wordt in alle applicaties gebruikt en maakt het mogelijk om van daaruit UC-functionaliteit te gebruiken zoals presence indicator, chat middels voice/tekst/video, mail en agenda).

Daardoor moeten de toepassingen voor authenticatie doeleinden gekoppeld kunnen worden aan de identity store van Pijnacker-Nootdorp (AD, Azure AD).

De smartphone wordt steeds meer het primaire device (mobile first). De volgende apps worden op termijn richting de smartphone gepubliceerd:

- Chat & Presence app
- Helpdesk app
- Office apps
- Social Intranet app
- Vergader app
- Zaaksysteem app (Inbox)
- VTH apps
- Sociaal Domein apps
- HRM app (ziekmelding, verlof)
- BI app
- Etc.

Invulling Pijnacker-Nootdorp:

- Microsoft Intune als Mobile Device Management tool.
- Microsoft Skype for Business in combinatie met Microsoft Office365 (E3)

- Integratie vaste en mobiele telefonie op basis van Skype for Business (PBX)
- Windows Active Directory in combinatie met Azure Active Directory.
- Pijnacker-Nootdorp gaat in de toekomst toenemend gebruik maken van Azure PaaS functionaliteit ten aanzien van open data, big data, BI, IoT ontwikkelingen.
- (SaaS-)applicaties moeten platform onafhankelijk aangeboden kunnen worden aan de gebruikers (Windows, iOS, Android).
- De vormgeving van de applicaties moet responsive zijn. Dat wil zeggen dat de schermopbouw van de applicatie zich technisch en functioneel aanpast aan de schermresolutie van het device;
- Applicaties moeten zero-impact hebben op het besturingssysteem van het device.
- Applicaties maken gebruik van API's van het Microsoft platform (Office365, SharePoint, Skype for Business, etc.). Hierdoor worden applicaties in zekere mate 'UC-aware'.

3.3 Identity & Access Management (IAM)

Tegenover de groeiende flexibilisering (qua devices, werklocaties en tijdstippen, wisselende samenwerkingsverbanden binnen en buiten de eigen organisatie) staan ook toenemende bedreigingen op het gebied van informatie- en privacy beveiliging. Het belang van een juiste authenticatie en autorisatie groeit. Pijnacker-Nootdorp gaat hiervoor de Kernregistratie Medewerker inrichten. In deze registratie worden Medewerkers gekoppeld aan Rollen en daarmee aan Rechten in onze ICT-omgeving (IAM).

Wijzigingen in deze registratie zullen op termijn geautomatiseerd (RBAC tooling) leiden tot mutaties in de Active Directory en andere toepassingen. In feite wordt dan deze kernregistratie de leidende identity store van Pijnacker-Nootdorp. Tot die tijd is de Active Directory de leidende identity store.

IAM gaat Pijnacker-Nootdorp op termijn de volgende mogelijkheden bieden:

- Helpdesk delegatie
 - o Handmatige en op scripts gebaseerde handelingen vastleggen in scenario's en tools
- User Provisioning vanuit P&O systeem
- Workflow management en self-service
 - o Door managers/gebruikers zelf toegang tot share, functionele mailbox, distributielijst laten aanvragen (helpdesk ontlast, verantwoordelijkheid naar de lijnorganisatie)
- Role Based Access Control (RBAC)
 - o Welke resources in het netwerk voor welk (type) medewerker (voldoet aan audit en compliance)
- Authenticatie
 - o Verdedigingsgordel verschuift naar binnen (data protectie in plaats van kantoorlocatie protectie)
 - o Conditional Access (locatie en device condities)
 - o Two Factor Authentication waar nodig (op applicatie niveau toe te passen)

Invulling Pijnacker-Nootdorp:

- Voor het realiseren van bovenomschreven mogelijkheden gaat Pijnacker-Nootdorp gebruik maken van het IaaS/PaaS platform Azure van Microsoft.

3.4 Definities clouddiensten

Samenvattend betekent dit dat Pijnacker-Nootdorp voor ieder systeem/applicatie die aangeschaft, vernieuwd of gebouwd moet worden, het volgende afwegingsschema van toepassing verklaard in volgorde van voorkeur:

1. SaaS
2. PaaS
3. IaaS
4. On premise als het onontkoombaar is (wettelijk, technisch, financieel).

Pijnacker-Nootdorp definieert het verschil tussen deze clouddiensten in termen van de verdeling van verantwoordelijkheden tussen de Opdrachtnemer en Pijnacker-Nootdorp. In onderstaande figuur zijn de definities van On-Premises, IaaS, PaaS en SaaS gevisualiseerd.

