2025

Technisch ontwerp

FONTEYN VAKANTIEPARKEN

PROFTAAK

Inhoud

1. Inleiding

1.1 Doel van het document

Het bedrijf Fonteyn vakantiepark heeft ons ingehuurd als IT-bedrijf om hen oude omgeving volledig om te bouwen en te migreren naar de Cloud,

Hierin willen hen zoveel mogelijk geautomatiseerd hebben, En willen ze zoveel mogelijk naar de Cloud zodat hen gebruik kunnen maken van de oude server ruimte als een kantoor

1.2 Scope

1.2.1 Reikwijdte van het Ontwerp

De reikwijdte van het ontwerp voor de ICT-omgeving van Fonteyn Vakantieparken omvat de integratie, consolidatie en modernisatie van hun bestaande IT-infrastructuur en applicaties. Het ontwerp richt zich specifiek op de volgende elementen:

1. **Centralisatie van ICT-Omgevingen:**
    - Migratie van bestaande client/server architecturen naar cloud-gebaseerde SaaS-oplossingen voor HRM, boekhouding en het online reserveringssysteem.
    - Implementatie van een centraal documentbeheersysteem om bestandshantering, samenwerking en versiebeheer te stroomlijnen.
2. **Identiteits- en Toegangsbeheer:**
    - Implementatie van een Single Sign-On (SSO) systeem voor gebruikers om toegang te krijgen tot alle benodigde applicaties met één set inloggegevens.
    - Koppeling van het identiteitsbeheer met het HR-systeem om automatische toewijzing van toegangsrechten op basis van functie en afdeling te waarborgen.
3. **Data Bescherming en Back-up:**
    - Ontwikkeling van een externe back-upoplossing die veilig en effectief de data van alle systemen verzamelt en opslaat, met regelmatige restore-tests.

4. **IoT Integratie en Innovatie:**
    - Integratie van relevante IoT-systemen en sensoren die helpen bij het verzamelen van data voor optimalisatie en duurzaamheid, inclusief de ontwikkeling van een bezoekersapp voor het beheren van boekingen en het bijhouden van de carbon footprint.
5. **Automatisering van IT-processen:**
    - Implementatie van tools en processen voor het automatiseren van IT-beheer om de efficiëntie te verhogen en de werkdruk op IT-personeel te verlichten.

1.2.2 Beperkingen

1. **Budgettaire Limieten:**
    - Het ontwerp moet binnen het beschikbare budget blijven, wat kan resulteren in een beperking van de keuze aan technologieën en voorzieningen.
2. **Huidige Infrastructuur:**
    - De transformatie moet rekening houden met de bestaande infrastructuur, waarbij sommige legacy-systemen mogelijk moeilijk te migreren zijn.
3. **Regelgeving en Compliance:**
    - Het ontwerp moet voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en andere lokale wet- en regelgeving in de landen waar Fonteyn actief is. Dit kan beperkingen opleggen aan hoe data verzameld, opgeslagen en beheerd kunnen worden.

4. **Tijdslijnen:**
    - De implementatie moet in fasen worden uitgevoerd om de impact op de dagelijkse werkzaamheden te minimaliseren, wat kan leiden tot langere doorlooptijden voor volledige uitvoering.
5. **Technologische Vaardigheden:**
    - Medewerkers kunnen beperkte ervaring hebben met nieuwe technologieën, wat extra training en ondersteuning vereist bij de implementatie.

1.2.3 Afbakeningen

1. **Geen Hardware-Focus:**
    - Het ontwerp richt zich primair op software- en cloudoplossingen, met minimale focus op de vervanging van hardwarecomponenten, tenzij deze essentieel zijn voor de migratie of efficiëntie.
2. **Bedrijfsspecifieke Applicaties:**
    - Het ontwerp bevat geen maatwerksoftware die buiten de standaard SaaS-oplossingen valt, tenzij dit onmisbaar wordt geacht voor de bedrijfsvoering.
3. **Fysieke Locaties:**
    - Het ontwerp houdt alleen rekening met de centrale ICT-infrastructuur en het hoofdkantoor van Fonteyn de afzonderlijke parken blijven voorlopig onafhankelijk tot volledige centralisatie mogelijk is.

4. **Beperkte Integratie met Externe Partners:**
    - De initiële implementatie van de gedeelde document en informatiesystemen richt zich op interne medewerkers, met externe partners als een latere uitbreidingsfase.

1.3 Achtergrondinformatie

Toekomstige ICT-omgeving

- De directie van Fonteyn Vakantieparken heeft echter het inzicht ontwikkeld dat de huidige ICT-omgeving niet meer voldoet aan hun groeiambities en de veranderende behoeften van de markt. Ze streven naar:
- **Consolidatie en Centralisatie:** De integratie van alle ICT-systemen tot een standaard corporate omgeving die efficiëntie en samenwerking bevordert.
- **Cloud-gebaseerde oplossingen:** Overstappen naar Software as a Service (SaaS) om flexibiliteit, schaalbaarheid en een vermindering van upfront investeringen te realiseren.
- **Innovatie en Duurzaamheid:** Het ontwikkelen van nieuwe applicaties en systemen, waaronder mobiele apps, die de beleving van de gasten verbeteren en helpen bij het monitoren van duurzaamheid.
- **Geautomatiseerde en veilige processen:** Het implementeren van een robuust beveiligingssysteem en het professionaliseren van back-up- en herstelprocedures om de databeveiliging te waarborgen.

2. Architectuuroverzicht

2.1 Gewenste situatie

De vernieuwd infrastructuur moet er als volgt uit zien.

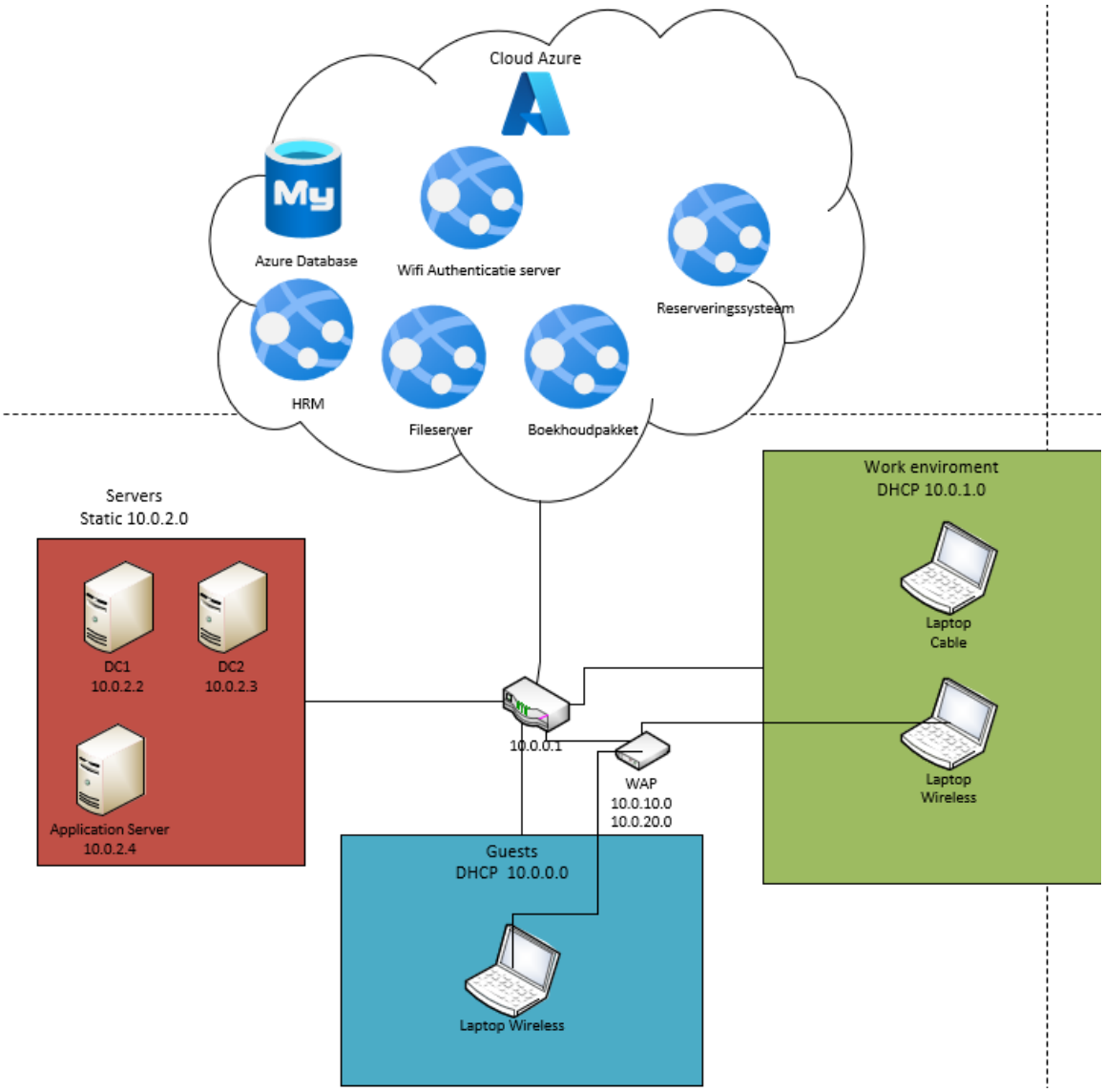
- Alle ICT-omgevingen centraliseren tot 1 omgeving.
- Gebruik maken van Cloud. – Mail server staat al in cloud.
- Website en boekingswebsite moeten aanpasbaar zijn aan de tijd
- Aantal applicaties moet als SaaS-dienst afnemen (Software as a Service)
- Microsoft Entra ID – Cloud AD
- Scripts om druk van ICT-werkzaamheden af te nemen - zoveel mogelijk automatiseren.
- Rekening houden met de verschillende talen voor waar de parken zijn gevestigd
- Privacy, wet- en regelgeving.
- Uptime is key.
- Script voor gebruikers uit dienst – Policy bespreken,
- HR-systeem die werkt met Microsoft AD – Cloud.
- Back-up mag niet intern gehost worden - Extern en moet elke maand getest worden.

3. Netwerktopologie

3.1 Logisch ontwerp

10.0.0.0 - 255.255.255.0 - VLAN A - Guests
10.0.1.0 - 255.255.255.0 - VLAN B - Work enviroment
10.0.2.0 - 255.255.255.0 - VLAN C - Servers

3.2 Ontwerp



4. Netwerk & Cloud integratie

4.1 Cloud Platform en Architectuur

Het cloud platform waarop we onze migratie gaan uitvoeren, wordt ‘Microsoft Azure’.

We gaan gebruik maken van de volgende cloud diensten:

- Software as a Service (SaaS) – HRM, Boekhoudpakket
- Platform as a Service (PaaS) – Database
- Infrastructure as a Service (IaaS) – Online reserveringssysteem, fileserver

1. Software as a Service (SaaS)

- SaaS-oplossingen worden volledig door de serviceprovider (Azure), en dus hebben wij hierover een beperkt beheer. Alles voor ons HRM-systeem en boekhoudpakket wordt dus door de serviceprovider uitgevoerd.
-

4.3 On-premise Architectuur

De on-premise omgeving bestaat uit verschillende fysieke en virtuele componenten die gezamenlijk de lokale IT-infrastructuur vormen. Hieronder volgt een overzicht van de belangrijkste onderdelen, ingedeeld in netwerk, servers, en clientomgevingen.

Netwerkcomponenten

- **PfSense Router**
  De centrale firewall en router binnen het netwerk. Deze regelt netwerkverkeer tussen interne netwerken en de buitenwereld (internet), en verzorgt tevens DHCP, DNS-forwarding en VPN-functionaliteiten.

Serveromgeving

De serveromgeving bestaat uit meerdere virtuele of fysieke servers die verschillende rollen vervullen:

- **DC1(Domain Controllers)**
  1 domain controller binnen een Active Directory-omgeving. Ze verzorgen authenticatie, groepsbeleid (GPO's), DNS en gebruikersbeheer.
- **Applicatieserver**
  Server waarop interne bedrijfsapplicaties draaien. Denk hierbij aan maatwerksoftware of tools die niet in de cloud staan.

Werkplekomgeving (Work Environment)

- **WAP Work Environment (Wireless Access Point)**
  WiFi-toegangspunt voor werknemers. Verzorgt veilige draadloze verbindingen binnen het interne netwerk.
- **Windows Clients (Werkplekken)**
  De reguliere werkstations van gebruikers. Deze zijn onderdeel van het domein en ontvangen groepsbeleid via de domain controllers. Ze zijn verbonden via Ethernet of WAP.

Gastennetwerk (Guests)

- **WAP Guests**
  Een afgescheiden draadloos netwerk speciaal voor bezoekers. Heeft geen toegang tot het interne bedrijfsnetwerk.
- **Windows Clients (Gastgebruikers)**
  Tijdelijke of niet-beheerde apparaten die via het gastnetwerk internettoegang krijgen. Deze zijn volledig gescheiden van de productieomgeving.

Opmerkingen en Veiligheid

- **Netwerkscheiding:**
  Er is een duidelijke segmentatie tussen productie- en gastnetwerk, o.a. via VLAN's of firewallregels in PfSense.
- **Redundantie & Beschikbaarheid:**
  Door twee Domain Controllers te gebruiken, is de authenticatie-infrastructuur veerkrachtig tegen storingen.

- **Voorbereiding op Cloud:**
  Deze on-prem omgeving is deels gekoppeld aan cloudservices via synchronisatie met Azure Active Directory.

5. Beveiliging

Voor de nieuwe IT omgeving van fonteyn, moeten verschillende beveiligings maatregelen getroffen worden. Dit omdat zij veel omgaan met onderandere klant gegevens.

Er zijn een aantal belangrijke onderdelen die je kunt beveiligen, zoals:

- Bestanden
- Netwerk
- Inloggen
- Monitoring
- Onderhoud

Bestanden

Aangezien een vakantiepark met veel bestanden bezig is, is het van groot belang dat deze op een veilige manier worden opgeslagen en dat hier veilig mee om wordt gegaan. Dit omdat er veel belangrijke gegevens van klanten bekend zijn bij het bedrijf. Om te voorkomen dat de bestanden in de verkeerde handen komen kun je meerdere dingen toepassen.

- RBAC, om ervoor te zorgen dat medewerkers niet zomaar bij alle bestanden kunnen maar alleen de bestanden die ze nodig hebben.
- Download beveiliging, om te zorgen dat heel belangrijke bestanden niet zomaar gedownload kunnen worden en dat bij de andere bestanden je een extra waarschuwing krijgt over het downloaden.
- Mogelijkheid tot downloaden bepaalde bestands types uitzetten.

Netwerk

Een belangrijk onderdeel van de cloud omgeving is het netwerk in de cloud. Daarom zijn er een aantal dingen waar we rekening mee moeten houden voor de beveiliging.

- Gasten netwerk splitsen van de andere netwerken zodat zij niet bij de servers of werkplekken kunnen.
- Zeer beperkt firewall regels aanmaken zodat er niet teveel dingen open staan naar het internet.
- Ook zou je voor de netwerken met zeer gevoelige informatie kunnen verplichten dat je alleen met een VPN kan ik loggen en niet vanaf elk willekeurig netwerk

Inloggen

Om het inloggen in de cloud omgeving beter te beveiligen zou je een aantal maatregelen kunnen toepassen zodat niet iedereen zomaar kan ik loggen.

- MFA, een handige manier om te voorkomen dat iemand inlogt zonder dat die dat mag is het gebruik van 2 staps verificatie. Hierdoor kan alleen de persoon van wie het account is inloggen doordat hij/zij een bericht krijgt met een code die je moet invullen.
- Wachtwoord policy, je kunt een wachtwoord policy aanmaken zodat de wachtwoorden van gebruikers aan bepaalde eisen moeten voldoen. Zoals een hoofdletter, een cijfer, een teken en minimaal 12 tekens lang.
- Ook kun je verschillende soorten admin accounts aanmaken zodat een hacker nog minder kan, dus voor de accounts die de servers bedienen een ander wachtwoord dan voor de accounts die op de workstations worden gebruikt. Zodat als de hacker in de workstations kan hij niet ook automatisch bij de servers kan.

Monitoring

Een belangrijk onderdeel van een veilig netwerk is ook het monitoren van het netwerk en in de gaten houden of er pogingen tot hacken worden gedaan. Hier bij kun je op een aantal dingen letten.

- Monitoren van de mails die medewerkers ontvangen, dit kun je doen om te voorkomen dat ze op een phising link drukken waardoor hun inlog gegevens gestolen kunnen worden.
- Ook kun je logs bij houden van wat medewerkers doen met bestanden zoals, downloaden, verplaatsen, openen of verwijderen. Dit zodat je voorkomt dat de bestanden gedownload worden en dan vervolgens gedeeld worden met mensen van buiten het bedrijf

Onderhoud

een belangrijk onderdeel van veiligheid is onderhoud, als je niet zorgvuldig bent met je onderhoud kunnen er problemen ontstaan.

- Regelmatig updaten van server zodat deze de nieuwste beveiligingen hebben.
- GPO aanmaken zodat alle workstations automatisch geupdate worden zodat deze ook de beste beveiliging hebben.

6. Implementatieplanning

6.1 Stappenplan

Fase	Stappen	Tijdlijn	Mijlpaal
Sprint 1 – Oriëntatiefase	**Routers geconfigureerd. Servers en werkplekken verbonden met de routers**	**Week 1/2**	**Alle servers en werkplekken hebben internet**
Sprint 2 – Start bouwen oude omgeving – projectplan maken – starten aan PPDIOO	**Servers inrichten met de juiste services. Werkplekken verbinden met domein**	**Week 3/6**	**De servers hebben de juiste services en werkplekken verbonden met domein**
Sprint 3 – Verder bouwen oude omgeving en technisch ontwerp verder uitbreiden en PPDIOO af maken			
Sprint 4 – Afronden oude omgeving			
Sprint 5 – Start migreren naar cloud en nieuwe omgeving vormgeven			
Sprint 6 – Naar de cloud gemigreerd zijn en puntjes op de i zetten			
Sprint 7 – Afronden nieuwe omgeving en opleveren			

6.2 Teststrategie

Beschrijf de testprocedures en validatiecriteria.

6.3 Risicoanalyse en mitigatie

Nr.	Risico's	Maatregelen
1.	Cyberaanvallen en datalekken	- installeer sterke firewalls - Gebruik encryptie - Train medewerkers in herkennen van spam - Beveilig wifi en scheid gast netwerk
2.	Systeemuitval	- Zorg voor redundante systemen - Test noodprocedures - Maak dagelijks back-ups - Gebruik UPS voor belangrijke systemen
3.	Onvoldoende updates en onderhoud	- Stel updatebeleid op en automatiseer updates - Controleer regelmatig status hardware
4.	Gasten als risico	- Beperk toegang van gasten tot interne systemen - Gebruik unieke, tijdelijke toegangscodes voor wifi en huisjestoegang die na vertrek verlopen

7. Documentatie en Onderhoud

7.1 Monitoring en beheer
Omschrijf monitoringtools en procedures voor proactief beheer.

7.2 Wijzigingsbeheer
Geef richtlijnen voor documentatie van wijzigingen in de ICT-omgeving.

7.3 Back-up en herstel
Beschrijf back-upstrategieën en disaster recovery-plannen.

8. Conclusie en Aanbevelingen

Geef een samenvatting van het ontwerp en eventuele aanbevelingen voor de toekomst.

Bijlagen

Voeg hier relevante schema’s, diagrammen en aanvullende documentatie toe.