PROVINCIE UTRECHT

Azure Assessment

18-06-2025

Finaal

Inhoudsopgave

1 ALGEMEEN

1.1 DOEL VAN HET DOCUMENT

Dit document beschrijft de resultaten van een Azure Assessment uitgevoerd door Inspark op verzoek van de Provincie Utrecht.

1.2 AANNAMES VOOR DOCUMENTEN

Het document is bedoeld voor lezers met basiskennis van Azure en bekendheid met het concept van Azure Enterprise-scale landing zones.

1.3 DOELEN

De beoordeling is gericht op het presenteren van de bevindingen, het geven van toelichting waar nodig, het formuleren van aanbevelingen en het vaststellen van mogelijke vervolgstappen.

1.4 DRAAGWIJDTE

Deze beoordeling richt zich op de implementatie van een Azure Enterprise-scale landing zone binnen de Entra ID-tenant van provincieutrecht.onmicrosoft.com.
Deze beoordeling is voornamelijk gericht op de principes van de landingszone. Tijdens de beoordeling komen de volgende onderdelen aan bod:

Ontwerpgebieden	Meer informatie
Azure-facturerings- en AD-tenant	Azure-factureringsaanbiedingen en Active Directorytenants - Cloud Adoption Framework | Microsoft Leren
Identiteits- en toegangsbeheer	Ontwerpgebied Azure-identiteits- en toegangsbeheer - Cloud Adoption Framework | Microsoft Leren
Organisatie van hulpbronnen	Overzicht van het ontwerpgebied van resourceorganisaties - Cloud Adoption Framework | Microsoft Leren
Netwerktopologie en connectiviteit	Overzicht van netwerktopologie en connectiviteit voor Azure - Cloud Adoption Framework | Microsoft Leren
Beheer	Beheer voor Azure-omgevingen - Cloud Adoption Framework | Microsoft Leren
Azure-beheer	Ontwerpgebied voor Azure-governance - Cloud Adoption Framework | Microsoft Leren
Azure-beveiliging	Beveiligingsontwerp in Azure - Cloud Adoption Framework | Microsoft Leren

1.5 BUITEN HET TOEPASSINGSGEBIED

• Evaluatie van de inhoud van toepassingen op VM's / containers / web-apps of andere zakelijke toepassingen.

2 MANAGEMENT SAMENVATTING

2.1 INTRODUCTIE

De Provincie Utrecht heeft InSpark gevraagd een Azure Assessment uit te voeren, ter ondersteuning van de verkenning naar migratie van de huidige on-premises omgeving naar Microsoft Azure. Dit assessment heeft als doel om inzicht te geven in optimalisatiemogelijkheden, een migratiestrategie te formuleren en het toekomstige beheer van de cloudomgeving te structureren.

2.2 RESULTATEN

De beoordeling is uitgevoerd op basis van de Azure Review Checklist, waarin de relevante ontwerpgebieden en best practices van het Microsoft Cloud Adoption Framework (CAF) zijn toegepast. Tijdens deze beoordeling zijn interviews gehouden met betrokkenen van de Provincie Utrecht om aanvullende context te verkrijgen. In totaal zijn er 33 bevindingen geconstateerd, verspreid over 8 ontwerpgebieden. InSpark heeft de belangrijkste aandachtspunten geselecteerd en voorzien van aanbevelingen. Een overzicht van de technische onderbouwing is opgenomen in hoofdstuk 1.4.1.

De Azure-omgeving van de Provincie Utrecht bevat momenteel zeven abonnementen, waarvan er meerdere nog niet actief worden gebruikt. Deze versnippering kan leiden tot een gebrek aan overzicht, suboptimale kostenstructuren en inconsistent beheer.

Daarnaast is vastgesteld dat identity en access management slechts gedeeltelijk is ingericht. Zo ontbreekt een consistent RBAC-model en worden er geen voorwaardelijke toegangsregels afgedwongen via Microsoft Entra ID. Dit verhoogt het risico op ongecontroleerde toegang tot kritieke resources.

Ook ontbreekt een centrale logging- en monitoringstructuur. Hierdoor is het moeilijk om afwijkingen of beveiligingsincidenten tijdig te detecteren en adequaat op te volgen.

De aanbeveling is om een solide fundament op te zetten op basis van het CAF. Dit fundament moet dienen als de technische en organisatorische basis voor de migratie van workloads vanuit de huidige on-premises omgeving naar Azure. Hierdoor kunnen deze workloads snel, veilig en kostenefficiënt worden overgezet en beheerd binnen een goed georganiseerde cloudomgeving.

Door gebruik te maken van Enterprise-scale landingszones, Azure Policy en centrale monitoring via onder andere Microsoft Defender for Cloud, kan de Provincie Utrecht toewerken naar een schaalbare en beheersbare Azure-omgeving die voldoet aan de eisen op het gebied van governance, beveiliging en operationeel beheer.

Deze aanpak maakt het tevens mogelijk om duidelijke rolverdeling toe te passen, resourcegebruik inzichtelijk te maken, en structurele verbeteringen door te voeren in beheer en beveiliging.

Bovendien legt deze benadering de basis voor toekomstige automatisering via DevOps en ondersteunt het een continu verbeterproces door regelmatige evaluaties en optimalisaties van de cloudomgeving.

2.3 VOLGENDE STAPPEN

Het opzetten van een robuuste Azure-omgeving die is afgestemd op het CAF is cruciaal voor de Provincie Utrecht om zowel huidige als toekomstige uitdagingen aan te gaan. Deze aanbeveling richt zich op het belang van het opzetten van een fundament, landingszones, beleid, Role-Based Access Control (RBAC) en netwerkconfiguratie.

Fundament en landingszones
Een fundament en landingszones vormen de ruggengraat van een goed gestructureerde Azure-omgeving. Ze bieden een gestandaardiseerde en schaalbare architectuur die toekomstige groei en veranderingen ondersteunt. Door het opzetten van een solide fundament kan de Provincie Utrecht een consistente en herhaalbare omgeving creëren die voldoet aan de best practices van het CAF. Landingszones helpen bij het organiseren van middelen en het implementeren van governance- en beveiligingsmaatregelen vanaf het begin.
Met toegewezen landingszones voor connectiviteit, identiteit en beheer wordt de omgeving verder geoptimaliseerd voor betrouwbaarheid, efficiënt beheer en verbeterde beveiliging. Dit zorgt ervoor dat de infrastructuur robuust en schaalbaar is en in staat is om te voldoen aan de veranderende behoeften van de organisatie.

Beleid
Het implementeren van beleid is essentieel voor het onderhouden van governance en compliance binnen de Azure-omgeving. Beleid zorgt ervoor dat resources voldoen aan bedrijfs- en beveiligingsnormen, waardoor risico's worden geminimaliseerd en naleving van regelgeving wordt gegarandeerd. Door gebruik te maken van beleid kan de Provincie Utrecht automatische controles en handhaving implementeren, wat leidt tot een beter beheerde en veiligere omgeving.

Op rollen gebaseerde toegangscontrole (RBAC)
RBAC is een cruciaal onderdeel van identiteits- en toegangsbeheer. Het stelt de Provincie Utrecht in staat om toegangsrechten te beheren op basis van de rol van een gebruiker binnen de organisatie, waardoor het risico op ongeoorloofde toegang wordt geminimaliseerd. Het implementeren van een consistent RBAC-model verbetert de beveiliging en het beheer van de Azure-omgeving door ervoor te zorgen dat gebruikers alleen toegang hebben tot de resources die ze nodig hebben voor hun werkzaamheden.

Netwerkconfiguratie
Een goed ingerichte netwerkconfiguratie is essentieel voor de beveiliging en prestaties van de Azure-omgeving. Dit omvat het segmenteren van het netwerk, het configureren van netwerkbeveiligingsgroepen (NSG's) en het implementeren van Azure Firewall. Deze maatregelen beschermen de cloudomgeving tegen bedreigingen en zorgen voor een efficiënte en veilige communicatie tussen resources.

Belang voor nu en de toekomst
Het opzetten van het CAF met een fundament, landingszones, beleid, RBAC en netwerkconfiguratie is niet alleen belangrijk voor de huidige behoeften van de Provincie Utrecht, maar ook voor de toekomst. Het zorgt voor een schaalbare en flexibele omgeving die kan meegroeien met de organisatie. Bovendien helpt het de kosten te optimaliseren, de operationele efficiëntie te verbeteren en ervoor te zorgen dat wordt voldaan aan industrienormen en -voorschriften. Door deze maatregelen te implementeren, kan de Provincie Utrecht een goed beheerde, veilige en kosteneffectieve Azure-omgeving creëren die klaar is voor toekomstige uitdagingen en innovaties.

Schaalbaarheid en flexibiliteit
Het implementeren van het CAF met een fundament, landingszones, policies, RBAC en netwerkconfiguratie is essentieel voor de Provincie Utrecht om een veilige, schaalbare en efficiënte Azure-omgeving te realiseren. Deze maatregelen bieden een solide basis die de organisatie helpt middelen te optimaliseren, de beveiliging en governance te verbeteren en zich voor te bereiden op toekomstige groei en veranderingen.

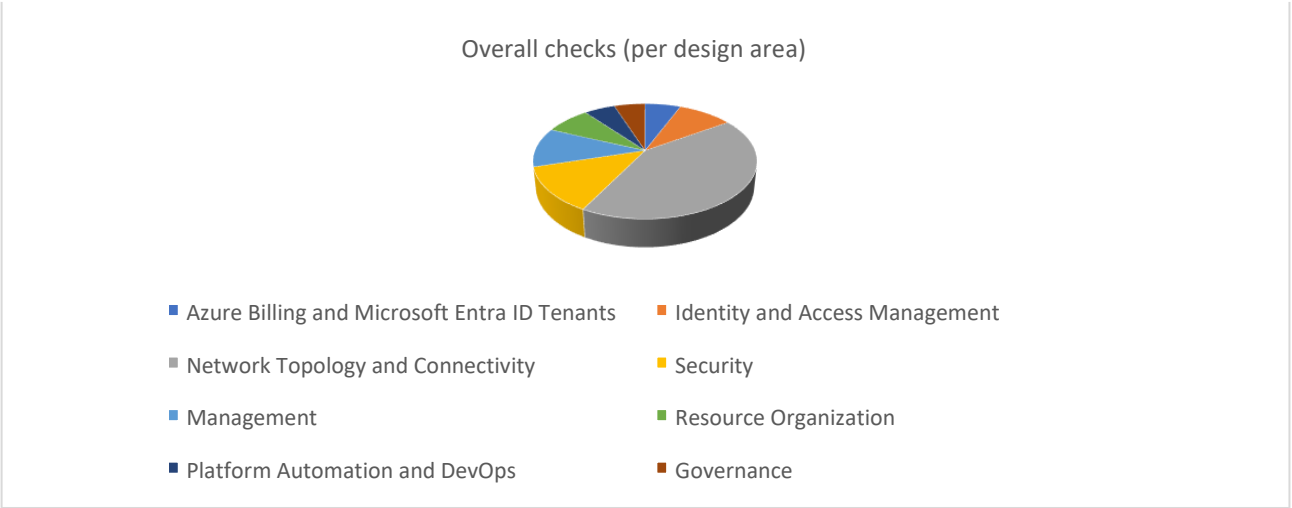
3 SAMENVATTING VAN HET ASSESSMENT

De beoordeling heeft verschillende ontwerpgebieden met verschillende controle-items met een ernst. Tijdens de beoordeling worden de checklistitems beoordeeld als een checklistitem toepasbaar is op de huidige geïmplementeerde configuratie en voldoet aan de best practices van het CAF en InSpark.

Legenda:

Strengheid	Beschrijving
Niet geverifieerd	Artikel is niet geverifieerd. Een paar redenen kunnen niet binnen het bereik vallen of items kunnen niet worden beoordeeld omdat er niet genoeg machtigingen zijn.
Open	Het item wordt beoordeeld, maar voldoet niet aan de best practices op basis van Cloud Adoption Framework (CAF).
Volledig gevuld	Het item wordt beoordeeld en voldoet volledig aan de best practices op basis van Cloud Adoption Framework (CAF).
Niet vereist	Het item hoeft niet te worden beoordeeld in de beoordeling.
Niet van toepassing	Het item is niet van toepassing in de omgeving wat zal worden beoordeeld.

De resultaten van de beoordeling leiden tot 33 openstaande items met een ernst hoog, InSpark vond ook een aantal items waarvan we betwijfelen of er in het verleden wel de juiste ontwerpkeuzes zijn gemaakt. De resultaten zijn beschikbaar in de onderstaande tabel op basis van ernst.



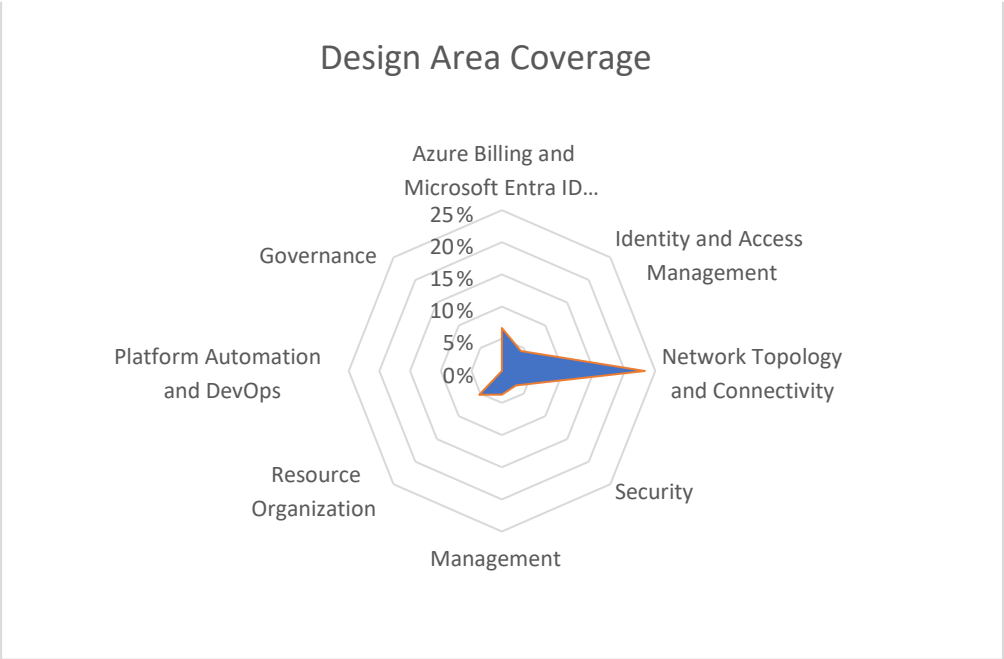
Figuur 01 – Algemeen statusoverzicht van de ontwerpgebieden

Strengheid	Niet geverifieerd	Open	Vervuld	Niet vereist	N.V.T	Totaal
Hoog	9	33	7	1	21	71
Gemiddeld	-	-	-	-	-	0
Laag	-	-	-	-	-	0
	0	**33**	**7**	**1**	**21**	**62**

In de volgende paragrafen beschrijft InSpark een selectie van de bevindingen, gecategoriseerd op ontwerpgebied.

3.1 DEKKING VAN HET ONTWERPGEBIED

De beslissingen die worden genomen binnen dit assessment, hebben directe invloed op het fundament van het Azure-platform, waarop alle landingszones zijn gebaseerd. De ontwerpgebieden zijn gemarkeerd met de letters "A" tot en met "I", die de hiërarchische opbouw van de resourceorganisatie binnen de conceptuele architectuur van het platform illustreren.



Figuur 02 – Algemeen statusoverzicht van de dekkingsgebieden van het ontwerp

In de onderstaande paragrafen wordt elk ontwerpgebied nader toegelicht, evenals de onderdelen die tijdens deze beoordeling zijn geëvalueerd. Ter verduidelijking zijn de ontwerpgebieden onderverdeeld in twee subdimensies: ontwerpgebieden die betrekking hebben op de IT-omgeving, en ontwerpgebieden met betrekking tot compliance.

3.2 ONTWERPGEBIEDEN VOOR CLOUDOMGEVING

De ontwerpgebieden met betrekking tot de IT-omgeving richten zich op de kerncomponenten van de cloudomgeving. In de onderstaande paragrafen worden deze gebieden nader toegelicht.

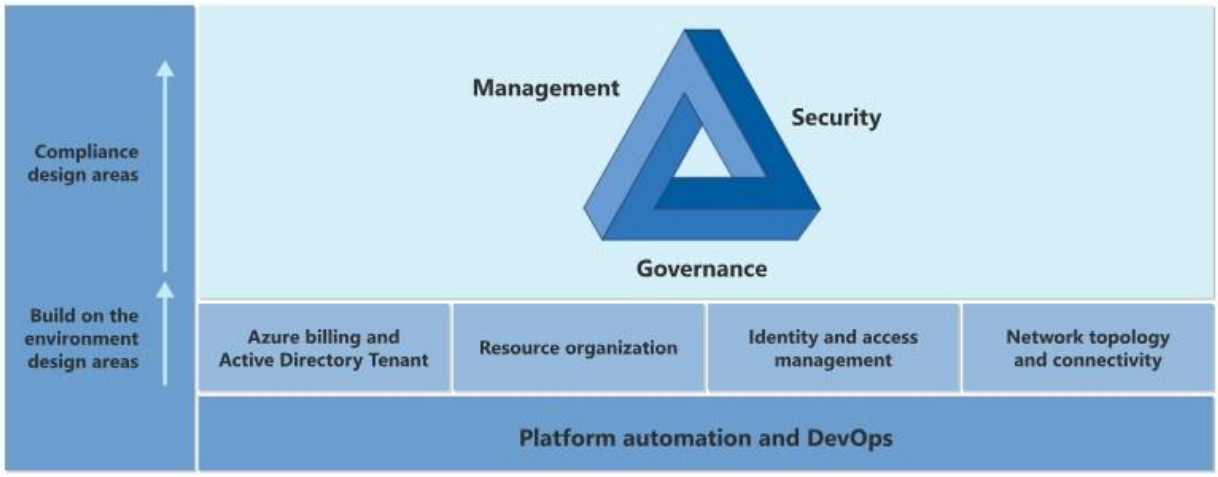
Ontwerpgebied	Doelstelling
Azure-facturering en Entra ID-tenant	Zorgen voor een correct ingerichte tenant, juiste inschrijvingen en geconfigureerde facturering als fundament voor een beheersbare en conforme cloudomgeving
Identiteits- en toegangsbeheer	Het implementeren van een veilige en schaalbare identity-structuur die toegang regelt op basis van principes zoals least privilege en Zero Trust.
Organisatie van resources	Het opzetten van een hiërarchische structuur van managementgroepen en abonnementen die schaalbaar governance en operationeel beheer mogelijk maakt
Netwerktopologie en connectiviteit	Het ontwerpen van een veilige, performante en uitbreidbare netwerkstructuur die aansluit op hybride behoeften en cloudstandaarden.

3.3 ONTWERPGEBIEDEN VOOR NALEVING

Beveiliging, governance en compliance zijn essentiële ontwerpgebieden bij het opzetten van een Azure-omgeving. Ze vormen de basis voor een stabiel, veilig en beheersbaar platform en zorgen ervoor dat er robuuste processen en controles aanwezig zijn voor continue naleving.

De combinatie van automatiseringstools en procesmatige inrichting speelt een sleutelrol bij het waarborgen van operationele continuïteit, het detecteren van afwijkingen en het kunnen reageren op incidenten. Dit ondersteunt zowel dagelijks beheer als strategische verbetering.

Naarmate de cloudomgeving van de Provincie Utrecht zich verder ontwikkelt, ontstaan er nieuwe aandachtspunten en vereisten die vragen om continue verfijning binnen de nalevingsgerichte ontwerpgebieden. Dit vereist focus op onderliggende architectuurkeuzes die bijdragen aan beheersbaarheid, herstelbaarheid en compliance.



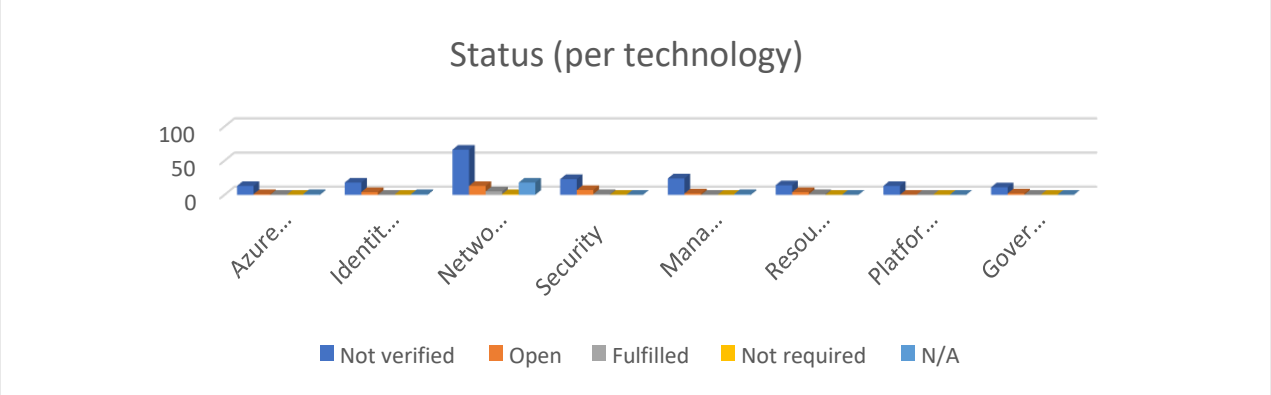
Afbeelding 03 – Ontwerpgebieden van het framework voor cloudadoptie

Ontwerpgebied	Doelstelling
Platform automatisering en DevOps	Het inzetten van gestandaardiseerde tooling en Infrastructure as Code (IaC) om implementatieprocessen van landingszones en resources betrouwbaar en schaalbaar te maken.
Beheer	Het borgen van zichtbaarheid en controle over de cloudomgeving door middel van logging, monitoring, herstelstrategieën en naleving van operationele standaarden..
Azure Governance	Het automatiseren van de controle en handhaving van beleidsregels (Azure Policy) ter ondersteuning van consistente naleving van organisatorische en wettelijke richtlijnen
Azure Security	Het implementeren van beveiligingsmaatregelen en processen die de cloudomgeving beschermen tegen bedreigingen, ongeautoriseerde toegang en datalekken.

4 STATUS VAN DE ONTWERPGEBIEDEN

In de volgende secties beschrijven we in meer detail de resultaten van de beoordeling van elk ontwerpgebied, InSpark heeft tijdens de beoordeling focus op items met configuratie-impact of beveiligings gerelateerde risico's en markeert die items met de status open en de ernst hoog.

Het doel is om dieper in te gaan op de meest kritische items die aandacht behoeven. In de volgende stappen wil InSpark enkele technische ontwerpbeslissingen en configuraties bespreken en verbeteren.



Figuur 04 – Algemeen statusoverzicht van elk ontwerpgebied

4.1 IDENTITEITS- EN TOEGANGSBEHEER

Voor een veilige en beheersbare Azure-omgeving is het essentieel om het identiteits- en toegangsbeheer goed in te richten. Hieronder worden acht strategieën aanbevolen die bijdragen aan een solide security-architectuur:

1. **Role-Based Access Control (RBAC):**
- **Afstemming**: Zorg voor een RBAC-model dat aansluit op het cloudgovernancemodel. Wijs rollen toe op het niveau van beheergroepen en abonnementen om de toegang tot resources zorgvuldig te beheren.

2. **Beleid voor voorwaardelijke toegang via Microsoft Entra ID:**
- **Afdwinging**: Microsoft Entra ID-beleid voor voorwaardelijke toegang afdwingen voor elke gebruiker met rechten voor Azure-omgevingen.

3. **Multi-factor authenticatie (MFA):**
- **Afdwinging**: Dwing meervoudige verificatie af voor elke gebruiker met rechten voor de Azure-omgevingen.

4. **Gedelegeerde verantwoordelijkheden:**
- **Toegangsbeheer**: Dwing gecentraliseerde en gedelegeerde verantwoordelijkheden af om resources te beheren die in de landingszone worden ingezet, op basis van rol- en beveiligingsvereisten.

5. **Active Directory-domain controllers:**
- **Implementatie**: Gebruik bij het implementeren van Active Directory-domain controllers een locatie met beschikbaarheidszones en implementeer ten minste twee VM's in deze zones. Als beschikbaarheidszones niet beschikbaar zijn, implementeert u deze in een beschikbaarheidsset.

6. **Toegang in noodgevallen (Break-glass accounts):**

- **Breaking-Glass-account**: Implementeer noodtoegangs- of break-glass-accounts om accountvergrendeling voor de hele tenant te voorkomen. MFA wordt in oktober 2024 standaard ingeschakeld voor alle gebruikers. Het wordt aanbevolen om deze accounts bij te werken met behulp van passkey (FIDO2) of om verificatie op basis van certificaten voor MFA te configureren. Update naar de standaardinstellingen voor beveiliging MFA. Update naar de standaardinstellingen voor beveiliging MFA

7. **Segmentatie van identiteitsnetwerken:**

- **Segmentatie**: Configureer segmentatie van het identiteitsnetwerk door het gebruik van een virtueel netwerk en peer terug naar de hub. Deze instelling biedt verificatie binnen de landingszone van de toepassing.

8. **Sessieconfiguratie van Microsoft Entra ID:**

- **Controle**: Controleer of sessiegedrag binnen Microsoft Entra ID juist is geconfigureerd. Ongebruikelijk lange sessies kunnen wijzen op een verkeerde configuratie van sessiecookies of sessieduurinstellingen.
- **Aanbeveling**: Herzie de configuratie van sessie-instellingen binnen Microsoft Entra ID en stem deze af op het beveiligingsbeleid van de Provincie Utrecht. Dit voorkomt langdurige of ongewenste actieve sessies en verhoogt de algehele beveiligingshouding.

Door deze strategieën te implementeren, kan de Provincie Utrecht de beveiliging en het toegangsbeheer binnen Azure aanzienlijk verbeteren en een schaalbare en conforme IAM structuur realiseren.

Subgebied	Checklist item	Prioriteit	Status
Identiteit	Dwing een RBAC-model af dat is uitgelijnd met uw cloudbesturingsmodel. Bereik en wijs toe in beheergroepen en abonnementen.	Hoog	Openen
Microsoft Entra ID en hybride identiteit	Dwing Microsoft Entra ID voorwaardelijke toegangsbeleid af voor elke gebruiker met rechten op Azure-omgevingen.	Hoog	Openen
Identiteit	Dwing meervoudige verificatie af voor elke gebruiker met rechten voor de Azure-omgevingen.	Hoog	Openen
Identiteit	Dwing gecentraliseerde en gedelegeerde verantwoordelijkheden af voor het beheer van middelen die in de landingszone worden ingezet, op basis van rol- en beveiligingsvereisten.	Hoog	Openen
Landingszones	Wanneer u Active Directory-domain controleers implementeert, gebruikt u een locatie met beschikbaarheidszones en implementeert u ten minste twee VM's in deze zones. Als deze niet beschikbaar is, implementeert u deze in een beschikbaarheidsset.	Hoog	Openen
Veiligheid	Implementeer een noodtoegangs- of break-glass-accounts om accountvergrendeling voor de hele huurder te voorkomen. MFA is in oktober 2024 standaard ingeschakeld voor alle gebruikers. We raden u aan deze accounts bij te werken om passkey (FIDO2) te gebruiken of verificatie op basis van certificaten voor MFA te configureren.	Hoog	Openen
Veiligheid	Configureer identiteitsnetwerksegmentatie door het gebruik van een virtueel netwerk en peer terug naar de hub. Authenticatie bieden binnen de landingszone van de applicatie (verouderd).	Hoog	Openen

4.2 NETWERKTOPOLOGIE EN CONNECTIVITEIT

Houd rekening met de volgende aanbevelingen om een efficiënt, veilig en centraal beheerd netwerk in uw Azure-omgeving te waarborgen:

1. **Gedeelde netwerkdiensten:**
   - **ExpressRoute-gateways, VPN-gateways en Azure Firewall:** Implementeer gedeelde netwerkservices, waaronder ExpressRoute-gateways, VPN-gateways en Azure Firewall (of NVA's van partners) in het virtuele netwerk van de centrale hub. Voeg indien nodig ook DNS-services toe om een betrouwbare naamomzetting en netwerkfunctionaliteit te waarborgen.

2. **Openbare IP-adressen:**
   - **Beleidstoewijzing:** Zorg voor een beleid dat het direct koppelen van openbare IPadressen aan virtuele machines voorkomt. Gebruik uitzonderingen alleen waar nodig, bijvoorbeeld voor specifieke VM's met een legitieme internetrol. Dit minimaliseert blootstelling aan het internet en verhoogt de algehele beveiliging.

3. **Azure Firewall:**
   - **Verkeersbeheer:** Gebruik Azure Firewall voor controle over uitgaand verkeer naar internet, niet-HTTP/S inkomende verbindingen en oost-west-verkeer (tussen subnetten of VNets), indien de organisatie dit vereist.
   - **Geavanceerde beveiligingsfuncties:** Schakel Azure Firewall Premium in voor functionaliteiten zoals TLS-inspectie, intrusion detection & prevention (IDPS), en URLfiltering. Hiermee wordt dieper inzicht verkregen in verkeer en bedreigingen.

4. **Route tabellen:**
   - **Subnetconfiguratie:** Voor subnetten in VNets die niet zijn aangesloten op Virtual WAN, maakt u gebruik van aangepaste routetabellen om verkeer via Azure Firewall of een NVA te laten verlopen. Gebruik een /26-adresblok voor het Azure Firewall-subnet voor voldoende IP-capaciteit en toekomstbestendige uitbreiding.

5. **Monitoring en registratie:**
   - **Integratie met Azure Monitor:** Koppel Azure Firewall aan Azure Monitor en activeer diagnostische logging. Hiermee worden logbestanden en metrische gegevens opgeslagen en geanalyseerd. Deze inzichten helpen bij het detecteren van ongewenst verkeer en ondersteunen een proactieve beveiligingsaanpak.

Door deze strategieën te implementeren, kan de Provincie Utrecht een goed beheerde, kostenefficiënte en veilige Azure-omgeving realiseren met volledige controle over netwerkverkeer, toegangsbeheer en risicobeheersing.

Subgebied	Checklist item	Prioriteit	Status
Hub en spaak	Implementeer gedeelde netwerkservices, waaronder ExpressRoute-gateways, VPNgateways en Azure Firewall of NVA's van partners in het virtuele netwerk van de centrale hub. Implementeer indien nodig ook DNS-services.	Hoog	Openen
Internet	Plan hoe u de configuratie en strategie van uw netwerk voor uitgaand verkeer kunt beheren vóór de aanstaande ingrijpende wijziging. Op 30 september 2025 wordt de standaard uitgaande toegang voor nieuwe implementaties buiten gebruik gesteld en zijn alleen expliciete toegangsconfiguraties toegestaan.	Hoog	Openen
Internet	Zorg ervoor dat er een beleidstoewijzing is om openbare IP-adressen te weigeren die rechtstreeks zijn gekoppeld aan virtuele machines. Gebruik uitsluitingen als openbare IP's nodig zijn op specifieke VM's.	Hoog	Openen
Firewall	Gebruik Azure Firewall voor het beheren van uitgaand Azure-verkeer naar internet, nietHTTP/S-inkomende verbindingen en het filteren van oost/west-verkeer (als de organisatie dit vereist).	Hoog	Openen

Firewall	Gebruik Azure Firewall Premium om aanvullende beveiligingsfuncties in te schakelen.	Hoog	Openen
Firewall	Voor subnetten in VNets die niet zijn verbonden met Virtual WAN, koppelt u een routetabel zodat internetverkeer wordt omgeleid naar Azure Firewall of een Virtual Network Appliance.	Hoog	Openen
Segmentatie	Gebruik een /26-voorvoegsel voor uw Azure Firewall-subnetten.	Hoog	Openen
Firewall	Integreer Azure Firewall met Azure Monitor en schakel diagnostische logboekregistratie in om firewalllogboeken en metrische gegevens op te slaan en te analyseren.	Hoog	Openen
Segmentatie	Vertrouw niet op de standaardregels voor binnenkomend binnenkomend verkeer van NSG met behulp van de VirtualNetwork-servicetag om de connectiviteit te beperken.	Hoog	Openen

4.3 BEVEILIGING

Beveiliging is een essentieel onderdeel van elke cloudadoptiestrategie, zoals benadrukt in het CAF. Door robuuste beveiligingsmaatregelen te implementeren, kunnen gevoelige gegevens worden beschermd, wordt voldaan aan industrienormen en worden risico's op incidenten geminimaliseerd.

Aangezien de Provincie Utrecht voornemens is om workloads naar Azure te migreren, is het belangrijk om tijdig passende beveiligingsstrategieën te evalueren en toe te passen. Hieronder volgen concrete aanbevelingen:

1. Microsoft Defender for Cloud

- **Huidige resources:** Schakel Defender for Cloud Workload Protection Plans in voor alle actieve abonnementen om brede bescherming te bieden. De huidige eindpuntbescherming met Kaspersky kan in Azure worden vervangen door Microsoft Defender for Endpoint voor optimale integratie.
- **Toekomstige workloads:** Neem Defender for Cloud standaard op in toekomstige implementaties om direct vanaf de start beveiligingsmaatregelen af te dwingen.

2. Opslagaccounts en TLS

- **Soft delete containers:** Schakel de functie 'voorlopig verwijderen' in voor containers, zodat verwijderde gegevens eenvoudig kunnen worden hersteld.
- **TLS 1.2:** Stel TLS 1.2 als minimumvereiste in op alle opslagaccounts om te zorgen dat alleen veilige clients toegang krijgen.

3. Beheer van Microsoft Entra ID-accounts

- **Gescheiden accounts:** Gebruik afzonderlijke beheerdersaccounts voor beheeracties in Azure en reserveer persoonlijke accounts voor dagelijks werk. Dit verkleint de kans op ongeoorloofde wijzigingen en verhoogt de controleerbaarheid.

4. Eindpuntbeveiliging

- **IaaS-servers:** Activeer endpoint protection op alle IaaS-servers om deze te beschermen tegen malware en andere bedreigingen.

5. Azure Key Vault

- **Beveiligde opslag van geheimen:** Implementeer Azure Key Vault voor het opslaan van wachtwoorden, API-keys en andere gevoelige informatie. Dit voorkomt dat geheimen onveilig worden opgeslagen in code of configuratiebestanden.

Door deze maatregelen te implementeren, creëert de Provincie Utrecht een veilige, goed beschermde en compliant Azure-omgeving. De inzet van Microsoft Defender, soft delete, TLSstandaarden, gescheiden accounts en Key Vault dragen bij aan een stevig beveiligingsfundament dat klaar is voor verdere automatisering via DevOps en Infrastructureas-Code (IaC).

Subgebied	Checklist item	Prioriteit	Status
Operaties	Schakel Defender Cloud Workload Protection Plans in voor Azure-resources op alle abonnementen.	Hoog	Openen
Operaties	Schakel voorlopig verwijderen van containers in voor het opslagaccount om een verwijderde container en de inhoud ervan te herstellen.	Hoog	Openen
Veilige bevoorrechte toegang	Afzonderlijke bevoegde beheerdersaccounts voor Azure-beheertaken.	Hoog	Openen
Operaties	Schakel eindpuntbeveiliging in op IaaS-servers.	Hoog	Openen
Versleuteling en sleutels	Gebruik Azure Key Vault om uw geheimen en referenties op te slaan.	Hoog	Openen

4.4 ORGANISATIE VAN HULPBRONNEN

4.4.1 KOSTENBEHEERSING EN GOVERNANCE

Effectief kostenbeheer en governance zijn cruciale pijlers van een succesvolle cloudadoptiestrategie, zoals onderstreept door het CAF. Kostenbeheer helpt om middelen efficiënt te gebruiken, onnodige uitgaven te vermijden en investeringen in Azure te optimaliseren. Governance biedt tegelijkertijd een gestructureerde aanpak voor het beheren en controleren van cloudresources, waarbij naleving van beleidsregels en standaarden gewaarborgd wordt.

Gezien de geplande migratie van workloads naar Azure is het voor de Provincie Utrecht belangrijk om strategieën toe te passen die zowel kostenefficiëntie als effectief resourcemanagement ondersteunen. Een van de aanbevolen maatregelen is het gebruik van gereserveerde instanties. Door virtuele machines vooraf te reserveren voor één of drie jaar, kunnen aanzienlijke kostenbesparingen worden gerealiseerd. De korting wordt automatisch toegepast op actieve resources die overeenkomen met de reservering, waardoor handmatige toewijzing overbodig is.

Op dit moment maakt de Provincie Utrecht gebruik van Veeam voor het back-uppen van onpremises servers. Voor de cloudomgeving adviseren wij over te stappen op Azure Backup. Indien er wettelijke verplichtingen zijn voor langdurige gegevensbewaring met Veeam, kan overwogen worden om de back-updata te verplaatsen naar een Azure Storage-account.

Een ander belangrijk aspect van governance is het invoeren van een consistente naamgevingsconventie voor Azure-resources. Dit vergemakkelijkt herkenning, beheer en rapportage. We raden aan om Microsoft's best practices voor naming standards toe te passen.

Daarnaast speelt beleid een essentiële rol in het afdwingen van beveiliging en compliance. Door gebruik te maken van Azure Policy en – waar nodig – aangepaste beleidsregels, kunnen beveiligingsvereisten effectief worden geïmplementeerd en beheertaken worden gestroomlijnd. Het is belangrijk om resource-eigenaren bewust te maken van hun verantwoordelijkheden rondom toegang, kostenbeheer en beleidsnaleving.

Tot slot adviseren wij het gebruik van tagging om kosten toe te wijzen aan workloads, het selecteren van de juiste Azure-regio's, en het afdwingen van veilige standaarden zoals TLS 1.2 voor opslagaccounts.

Door deze maatregelen te integreren – waaronder gereserveerde instanties, kosten- en taggingstructuren, beleid, namingconventies en moderne back-upstrategieën – kan de Provincie Utrecht een goed beheerde, veilige en kostenefficiënte Azure-omgeving realiseren.

Observaties
Onderbenut licentieprogramma Gebruik een programma voor gereserveerde exemplaren voor Azure-resources. Besparen met Azure-reserveringen - Microsoft Cost Management | Microsoft Leren
Naamgevingsconventies maken het voor u en uw team gemakkelijker om het doel en de functie van elke bron te begrijpen. Wanneer u een resource met de naam myapp-prod-vm-weu tegenkomt, weet u onmiddellijk dat het een virtuele productiemachine is in de regio West-Europa. Uw naamgevingsconventie definiëren - Cloud Adoption Framework | Microsoft Leren
Maak een uitgebreid kostenbeheerplan door het proces 'Beheerde cloudkosten' te volgen. Door tags toe te passen op uw resources, krijgt u een duidelijk overzicht van hoeveel een workload kost en verbruikt binnen Azure. Kosten groeperen en toewijzen met behulp van tag-overname - Microsoft Cost Management | Microsoft Leren
Maak strategisch gebruik van Azure Policy, definieer besturingselementen voor uw omgeving en gebruik Policy Initiatives om gerelateerd beleid te groeperen. Overzicht van Azure Policy - Azure Policy | Microsoft Leren
Beheer beleidstoewijzingen op het hoogst passende niveau, met uitzonderingen op de laagste niveaus, indien nodig.

Subgebied	Checklist item	Prioriteit	Status
Naamgeving en taggen	Gebruik een goed gedefinieerd naamgevingsschema voor resources, zoals Microsoft Best Practice Naming Standards.	Hoog	Openen
Abonnementen	Dwing een proces af om resource-eigenaren bewust te maken van hun rollen en verantwoordelijkheden, toegang te krijgen tot beoordeling, budgetbeoordeling, beleidsnaleving en indien nodig te herstellen.	Hoog	Openen
Abonnementen	Gebruik waar nodig gereserveerde instanties om de kosten te optimaliseren en de beschikbare capaciteit in doelregio's te garanderen.	Hoog	Openen
Abonnementen	Als onderdeel van uw cloudadoptie implementeert u een gedetailleerd kostenbeheerplan met behulp van het proces 'Beheerde cloudkosten'.	Hoog	Openen
Abonnementen	Zorg ervoor dat tags worden gebruikt voor facturering en kostenbeheer.	Hoog	Openen
Contreien	Selecteer de juiste Azure-regio('s) voor uw implementatie. Azure is een cloudplatform op wereldwijde schaal dat wereldwijde dekking biedt in vele regio's en regio's.	Hoog	Openen

4.4.2 PLATFORMAUTOMATISERING EN DEVOPS

InSpark adviseert de Provincie Utrecht om vanaf het begin te investeren in DevOps en Infrastructure as Code (IaC). Omdat er momenteel nog geen workloads zijn uitgerold in Azure, is dit het ideale moment om een geautomatiseerd en schaalbaar fundament op te zetten. Het toepassen van IaC biedt niet alleen controle en herhaalbaarheid, maar voorkomt ook technische schuld bij toekomstige uitbreidingen.

Hoewel het opzetten van een IaC-omgeving initieel uitdagend kan zijn, biedt Microsoft hiervoor concrete ondersteuning in de vorm van Azure Verified Modules (AVM). Dit zijn door Microsoft gevalideerde sjablonen met ingebouwde best practices. Ze worden actief onderhouden en geüpdatet, waardoor het onderhoud van eigen templates aanzienlijk wordt verminderd.

De voordelen van automatisering via Azure Automation:

- Schaalbaarheid: Processen kunnen op grote schaal worden uitgerold, wat essentieel is voor toekomstige groei en centrale beheersbaarheid.
- Consistentie: Azure Automation zorgt voor uniforme configuratie en beheer, zowel in Azure- als hybride omgevingen.
- Volledige controle: De gehele levenscyclus van workloads — van implementatie tot decommissioning — kan gestructureerd worden beheerd.
- Kostenoptimalisatie: Door automatisch resources te starten of te stoppen op basis van gebruik (bijvoorbeeld in ontwikkel- of testomgevingen), kunnen operationele kosten aanzienlijk worden verlaagd.

Door nu te investeren in een DevOps-strategie ondersteund door IaC en Azure Automation, legt de Provincie Utrecht een toekomstbestendig fundament voor veilige, efficiënte en beheersbare cloudoperaties.

Subgebied	Checklist item	Prioriteit	Status
DevOps team topologieën	Zorg ervoor dat u een multifunctioneel DevOps-platformteam hebt om uw Azure Landing Zone-architectuur te bouwen, te beheren en te onderhouden.		
Levenscyclus van ontwikkeling	Zorg ervoor dat er een versiebeheersysteem wordt gebruikt voor de broncode van applicaties en dat er een IaC wordt ontwikkeld. Microsoft raadt Git aan.		
Ontwikkelingsstrategie	Integreer beveiliging in het reeds gecombineerde proces van ontwikkeling en operaties in DevOps om risico's in het innovatieproces te beperken.		
Veiligheid	Integreer beveiliging in het reeds gecombineerde proces van ontwikkeling en operaties in DevOps om risico's in het innovatieproces te beperken.		