

Aansluitvoorwaarden Azure Landing Zones



Document gegevens

Onderwerp		
Versie status	0.91	Concept
Bestandsnaam	Aansluitvoorwaarden voor Azure Landing Zones	

***Dit document beschrijft de aansluitvoorwaarden zoals deze gelden per oktober 2025.
Omdat de Azure Landing Zone voortdurend in ontwikkeling is, zullen de aansluitvoorwaarden in de toekomst worden aangevuld en aangepast in lijn met deze ontwikkelingen.***

Introductie

Wat dit document is

Dit document biedt aansluitvoorwaarden voor externe partijen, waaronder leveranciers die gebruik moeten maken van de functies van de Azure Landing Zone van NWO.

Wat dit document niet is

Dit document is geen technische how-to voor de daadwerkelijke integratie van een product in de Azure Landing Zone, maar geeft alleen de voorwaarden daarvoor.

Doelgroep

De aansluitvoorwaarden zijn bedoeld voor externe partijen, waaronder leveranciers die vanuit een aanbesteding of goedgekeurde wijziging gebruik willen maken van de Azure Landing Zone van NWO.

Inhoud

Introductie	3
Wat dit document is	3
Wat dit document niet is	3
Doelgroep	3
1. Inleiding	5
2. Aansluitvoorwaarden	5
Aansluitvoorwaarde 1: Deploymentstandaarden	5
Aansluitvoorwaarde 2: Kostenbeheer	5
Aansluitvoorwaarde 3: Monitoring en logging	6
Aansluitvoorwaarde 4: Lifecycle management	6
Aansluitvoorwaarde 5: Documentatie en naamconventie	6
Aansluitvoorwaarde 6: Identiteit en toegang	6
Aansluitvoorwaarde 7: Netwerkconfiguratie	6
Aansluitvoorwaarde 8: Beveiliging	6
Aansluitvoorwaarde 9: Compliance en governance	7
3. Verantwoordelijkheden	7
5. Anders	7

1. Inleiding

De twee Azure Landing Zones “ALZ’s”, brengen voor NWO een robuuste en schaalbare cloudomgeving waarmee in brede zin continuïteit wordt gegeven aan softwareoplossingen.

NWO heeft twee landing zones: productie en non-productie waarbij productie- en acceptatieomgevingen worden gefaciliteerd door de productie landing zone en test- en ontwikkelomgevingen door de non-productie landing zone. Dit bevordert de betrouwbaarheid en veiligheid van de cloudomgeving.

Dit document biedt externe partijen, waaronder leveranciers een set aansluitvoorwaarden om eerdergenoemde doelstellingen te kunnen handhaven.

2. Aansluitvoorwaarden

Deze aansluitvoorwaarden geven aan waar workloads van leveranciers zich in de ALZ’s aan moeten houden:

Aansluitvoorwaarde 1: Deploymentstandaarden

- Per subscriptie wordt een sleutelkluis ingericht en in gebruik genomen;
- Gebruik Infrastructure as Code – geen handmatige wijzigingen in de productie portal;
- CI/CD pipelines worden gebruikt voor de productieomgeving;
- De productie omgeving wordt uitgerold naar een eigen subscription in de productie-ALZ;
- Toegang tot de tenant wordt verleend op basis van RBAC en MFA;
- Er wordt gewerkt op basis van Zerotrust;
- Het maken van een ITSM koppeling tussen het ITSM systeem van opdrachtgever en opdrachtnemer is mogelijk;
- Niet standaard wijzigingen worden afgestemd met de productowner van het team Technologieplatformen en volgen het wijzigingsproces van NWO;
- De Service Bus of Event Grid services worden gebruikt om een gestandaardiseerde en betrouwbare integratie tussen softwaresystemen te realiseren;
- Data blijft binnen de tenant van NWO, tenzij anders overeengekomen;
- Alle wijzigingen in de Azure Landingzones m.b.t. productie moeten worden gedocumenteerd en vereisen een plan van aanpak en een risico- en impactanalyse;
- Er worden geen koppelingen naar externe omgevingen gelegd zonder goedkeuring van NWO.

Aansluitvoorwaarde 2: Kostenbeheer

- Azure-workloads dienen te worden ingericht en beheerd conform de FinOps-principes. Daarbij moeten de volgende aspecten worden meegenomen:
 - Kosten moeten kunnen worden toegewezen aan de juiste afdeling, applicatie of project (via tags);
 - Resources worden voorzien van tags t.b.v. kostenbeheer waarbij de leverancier een eigen tag krijgt;
 - Alerts en policies worden ingesteld t.b.v. kostenbeheer;
 - Kosten en verbruik moeten zichtbaar zijn in via een dashboard;
 - Workloads worden zodanig ingericht dat onnodige kosten worden voorkomen.

Aansluitvoorwaarde 3: Monitoring en logging

- Applicaties integreren met de centrale monitoring van NWO. Deze monitoring is gebaseerd op Azure Monitoring i.c.m. een Log Analytics Workspace;
- Alerts zijn ingesteld voor resources die productieverstoringen of hoge kosten kunnen veroorzaken.

Aansluitvoorwaarde 4: Lifecycle management

- Resources hebben een eigen lifecycle (zoals die voor de automatische verwijdering van een testomgeving);
- Versie N-1 wordt gehanteerd;
- Azure backup en disaster recovery zijn ingericht conform een RTO van 5 uur en een RPO van 2 uur voor "Het nieuwe financieringssysteem".

Aansluitvoorwaarde 5: Documentatie en naamconventie

- Documentatie van policies, netwerk, toegang en deployment zijn beschikbaar voor NWO en volgen de naamconventie van NWO volgens het format:
<YYYYMMDD> <projectnummer/Naam product/Naam product team> <titel-document> <versie>;
- De naamconventie en versiebeheer van Git is als volgt:
 - Branch: git branch <categorie/referentie/korte-uitleg>
 - Commit: git commit -m <categorie: aanpassing 1; aanpassing 2>
- De naamconventie van Azureonderdelen volgen de best practices van Microsoft.

Aansluitvoorwaarde 6: Identiteit en toegang

- Gebruik van Entra ID voor authenticatie;
- RBAC wordt toegepast op resources in Azure;
- MFA verplicht voor beheerderaccounts;
- Privileged Identity Management (PIM) wordt toegepast;
- Identity Access Management (IAM) wordt toegepast.

Aansluitvoorwaarde 7: Netwerkconfiguratie

- Om communicatie tussen het productnetwerk (spoke) en de Azure Landing Zone (hub) mogelijk te maken, moet er een (peering) verbinding worden opgezet;
- Zonder centrale firewall, Network Security Gateway is er geen directe toegang tot het internet;
- Domain Name Service moet integreren met de centrale name resolution (ook wel bekend als DNS);
- Er wordt gewerkt binnen netwerksegmentatie, met als doel het opdelen van resources, netwerken en/of applicaties in geïsoleerde segmenten.

Aansluitvoorwaarde 8: Beveiliging

- Workloads houden zich aan de beveiligingseisen zoals beschreven in de aanbestedingsdocumenten van "Het nieuwe financieringssysteem";

- Logging en monitoring t.b.v. beveiliging zijn actief via resp. Log Analytics en Azure Monitoring van NWO;
- Functionele koppelingen naar Azure Lighthouse, kunnen alleen tot stand worden gebracht middels goedkeuring van NWO en volgen lifecyclemanagement;
- Microsoft Defender for Cloud is standaard onderdeel van de deployments in de subscription.

Aansluitvoorwaarde 9: Compliance en governance

- Alleen de goedgekeurde regio “West-Europe” mag gebruikt worden;
- Management Groups worden gebruikt om toegang, beleid en naleving centraal te beheren binnen de omgeving, ongeacht het aantal subscriptions;
- Governance policies zijn toegepast via Azure Policy en Blueprints;
- Leverancier committeert zich aan IT Service Management processen volgens IT4IT van NWO. De in-scope processen en de bijbehorende vereisten zijn beschreven in de aanbestedingsdocumenten “Het nieuwe financieringssysteem”.

3. Verantwoordelijkheden

De verantwoordelijkheden van de leverancier en NWO zijn:

1. De beschikbaarheid en het faciliteren van het Azure platform zijn de verantwoordelijkheden van NWO;
2. Het volgen van de aansluitvoorwaarden zijn de verantwoordelijkheden van de leverancier;
3. De leverancier is verantwoordelijk voor alles wat in de subscription plaatsvindt in lijn met het beleid van NWO.

5. Anders

Ten behoeve van een efficiënte samenwerking kunnen externe ontwikkelteams met beperkte toegangsrechten gebruik maken van de Azure DevOps-omgeving van NWO.