

Problemen met Cloud OnRamp oplossen in Microsoft Azure

Inhoud

[Inleiding](#)

[Probleem](#)

[Oplossing](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft enkele van de meest voorkomende problemen bij het implementeren van Cloud Gateways in de Azure van vManage Cloud on Ramp.

Probleem

Bij het configureren van Cisco SD-WAN Cloud OnRamp voor Microsoft Azure wordt het selectieveld Software Image voor cEdge-apparaten leeg weergegeven in de algemene instellingen van vManage, waardoor de implementatie van cEdge-instanties in Azure Cloud wordt voorkomen.

Symptomen:

- De softwarerelease van cEdge die is gepland voor toekomstige implementatie op het Azure Cloud-veld in vManage > Cloud OnRamp for Multicloud > Cloud Global Settings is leeg.
- Initiële admin-tech-logs kunnen Azure Error: "AuthorizationFailed" weergeven met een bericht dat aangeeft dat de client geen autorisatie heeft om Microsoft.Network/networkVirtualApplianceSkus/read-actie uit te voeren.
- Admin-tech-logs kunnen RetryError: HTTPSConnectionPool(...) weergeven Max. aantal pogingen overschreden met URL: ... (Veroorzaakt door de responsfout "te veel 502-foutreacties") wanneer vManage probeert Network Virtual Appliance (NVA) SKU's op te halen van management.azure.com.

Dit log is te vinden in hetzelfde pad `/var/log/nms/containers/cloudagent-v2/cloudagent.log` en laat zien dat er verschillende brongroepen zijn geconfigureerd in Azure.

```
[2025-09-01T04:07:35UTC+0000:140226169132800:ERROR:ca-v2:azure_resource_helper.py:351] Er zijn geen bronnen opgehaald voor {  
  
    "cloudType": "AZURE",  
  
    "accountId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx",  
  
    "accountName": "<account_name>",  
  
    "region": "eastus2",  
  
    "type": "NVA_SKUS"  
  
}: Fout opgetreden in aanvraag., RetryError:  
HTTPSConnectionPool(host='management.azure.com', poort=443): Max. aantal herhalingen  
overschreden met URL: /subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-  
xxxxxxxxxxxxxx/providers/Microsoft.Network/networkVirtualApplianceSkus/ciscosdwan?api-  
version=2020-05-01 (veroorzaakt door ResponseError('too many 502 error responses'))
```

```
[2025-09-01T04:07:35UTC+0000:140226169132800:INFO:ca-v2:grpc_service.py:1011]  
Terugkerende GetAzureResourceInfo Response: {  
  
    "mcCtxt": {  
  
        "tenantId": "<naam huurder>",  
  
        "ctxId": "zzzzzzzzzz-zzzz-zzzz-zzzzzzzzzzzzzzzzzzzzz"  
  
    }  
  
    "status": {  
  
        "code": "OK"  
  
    }  
  
}
```

Van vManage is dit een van de gebruikelijke logs die worden weergegeven wanneer de taak wordt geïmplementeerd nadat de account in Azure is toegewezen met het voorkeursniveau; het type account is echter niet Enterprise.

[27-Aug-2025 19:46:46 UTC] MultiCloud Gateway maken: <accountnaam>

[27-Aug-2025 19:46:47 UTC] Succesvol opgehaalde Resource Group: <accountnaam> uit de cloud

[27-Aug-2025 19:46:47 UTC] Opslagaccount maken onder Brongroep: <accountnaam> in de cloud

[27-Aug-2025 19:46:49 UTC] Opslagaccount onder brongroep: <accountnaam> is niet gemaakt in de clou

[27-Aug-2025 19:46:49 UTC] Aanvullende details: Azure Error: RequestDisallowedByPolicy

Bericht: Resource 'lcoix7mu7rcrswtdkyj0jsyw' werd door het beleid afgewezen. Beleidsidentificatoren:

```
[{"policyAssignment":{"name":"ASC Default (abonnement: xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxxxx)","id":"/subscriptions/xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/providers/Microsoft.Authorization/policyAssignments/SecurityCenterBuiltIn"},
```

```
"policyDefinition":{"name":"Storage account public access should be disallowed","id":"/providers/Microsoft.Authorization/policyDefinitions/yyyyyyyyyy-yyyyyy-yyyyyy-yyyyyyyyyy","version":"3.1.1"}}, <<<< Het verwijst naar accounttype in Azure is niet correct, abonnement n Enterprise zijn
```

```
"policySetDefinition":{"name":"Microsoft cloud security benchmark","id":"/providers/Microsoft.Authorization/policySetDefinitions/zzzzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzzzzzzzzzz","version":"57.53.0"}]".
```

Doel: lcoix7mu7rcrswtdkyj0jsyw

Aanvullende informatie:

Type: Beleidsovertreding

Info: {

```
"evaluationDetails": {
```

```
"evaluatedExpressions": [
```

{

```
"resultaat": "Waar",
```

```
"expressionKind": "Field",
```

```
"expressie": "type",
```

```
"pad": "type"
```

```
"expressionValue": "Microsoft.Storage/storageAccounts",
```

"targetValue": "Microsoft.Storage/storageAccounts"

```
"operator": "Equals"
```

}

{

```
        "resultaat": "onwaar",

        "expressionKind": "Field",

        "Expressie": "ID",

        pad: id,

        "expressionValue": "/abonnements/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/<accountnaam>/providers/Microsoft.Storage/storageAccounts/lcoix7mu7rcr

        "targetValue": "/resourceGroups/aro-",

        "operator": "Bevat"
    }

    {

        "resultaat": "onwaar",

        "expressionKind": "Field",

        "expression": "Microsoft.Storage/storageAccounts/allowBlobPublicAccess",

        "path": "properties.allowBlobPublicAccess",

        "targetValue": "false",

        "operator": "Equals"

    }

]

}

"policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/yyyyyyyyyy-yyyyy-yyy

"policySetDefinitionId": "/providers/Microsoft.Authorization/policySetDefinitions/zzzzzzzz-zzzz-
zzzzzzzzzzzzzzzzzz",

"policyDefinitionReferenceId": "StorageDisallowPublicAccess",

"policySetDefinitionName": "zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzzzz",

"policySetDefinitionDisplayName": "Microsoft cloud security benchmark",

"policySetDefinitionVersion": "57.53.0",

"policyDefinitionName": "yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy",
```

```
"policyDefinitionDisplayName": "Openbare toegang tot opslagaccount moet worden geweigerd",
"policyDefinitionVersion": "3.1.1",
"policyDefinitionEffect": "ontkennen",
"policyAssignmentId": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx/providers/Microsoft.Authorization/policyAssignments/SecurityCenterBuiltIn",
"policyAssignmentName": "SecurityCenterBuiltIn",
"policyAssignmentDisplayName": "ASC Default (abonnement: xxxxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxxxxxxxx)",
"policyAssignmentScope": "/abonnements/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx",
"policyAssignmentParameters": {
  "disallowPublicBlobAccessEffect": "deny"
}
"policyExemptionIds": [],
"policyEnrollmentIds": []
}
```

[27-Aug-2025 19:46:49 UTC] Terugdraaiende wijzigingen...

[27-aug-2025 19:46:49 UTC] Terugdraaiing voltooid

[27-Aug-2025 19:46:49 UTC] Interne fout bij het maken of ophalen van een opslagaccount

Mogelijke oorzaken:

1. Onvoldoende Azure-bevoegdheden: Zelfs als de Azure-account met succes is gekoppeld en bijdragerrechten heeft, zijn specifieke machtigingen vereist door vManage. Als u de SKU's van Network Virtual Appliance wilt lezen, kan deze ontbreken of onjuist zijn geconfigureerd.
2. Meerdere Azure Resource Groups: Cisco-documentatie voor Azure vWAN-integratie geeft aan dat slechts één brongroep is toegestaan voor de installatie van Cloud OnRamp. Het hebben van meerdere oude of redundante brongroepen kan leiden tot te veel 502-foutreacties van Azure wanneer vManage probeert beschikbare SKU's te bevragen.

Oplossing

1. Azure-machtigingen controleren:

- Ervoor zorgen dat de Azure-toepassing of -service die is gekoppeld aan vManage de nodige machtigingen heeft om de SKU's van Network Virtual Appliance te lezen. De specifieke actie is `Microsoft.Network/networkVirtualApplianceSkus/read`.
- Als er onlangs machtigingen zijn verleend of gewijzigd, kunt u referenties vernieuwen binnen vManage of Azure.
- Deze stappen zijn gedocumenteerd in de Cisco Cloud onRamp for Multi-Cloud Azure Version2 Solution Guide in het gedeelte Controleer Azure Subscription Permissions.

2. Azure-brongroepen beheren:

- Controleer uw Azure-abonnement voor alle oude of redundante brongroepen met betrekking tot Cisco SD-WAN Cloud OnRamp.
- Volgens de documentatie van Cisco is slechts één brongroep toegestaan voor de Azure vWAN-integratie. Verwijder alle oude brongroepen en zorg ervoor dat alleen de actieve en noodzakelijke groepen overblijven. Deze actie is waargenomen om de fout op te lossen, te veel 502 foutreacties.

Gerelateerde informatie

- [Cisco Catalyst SD-WAN Cloud OnRamp Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x](#) Dit document bevat beperkingen, waaronder de vereiste voor één brongroep voor Azure vWAN-integratie.
- [De Cisco SD-WAN Fabric uitbreiden naar Azure met Cisco Cloud onRamp voor Multi-Cloud](#): deze handleiding kan meer informatie geven over het controleren van Azure-abonnementen en -machtigingen voor de integratie.
- [Gerelateerd Azure CLI-probleem \(voor context op 502-fouten\)](#): Hoewel het geen direct Cisco-document is, biedt dit GitHub-probleem inzicht in vergelijkbare 502-foutreacties van Azure API, die relevant kunnen zijn voor het onderliggende Azure-gedrag.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.