Fehlerbehebung bei Cloud OnRamp-Problemen in Microsoft Azure

Inhalt

Einleitung

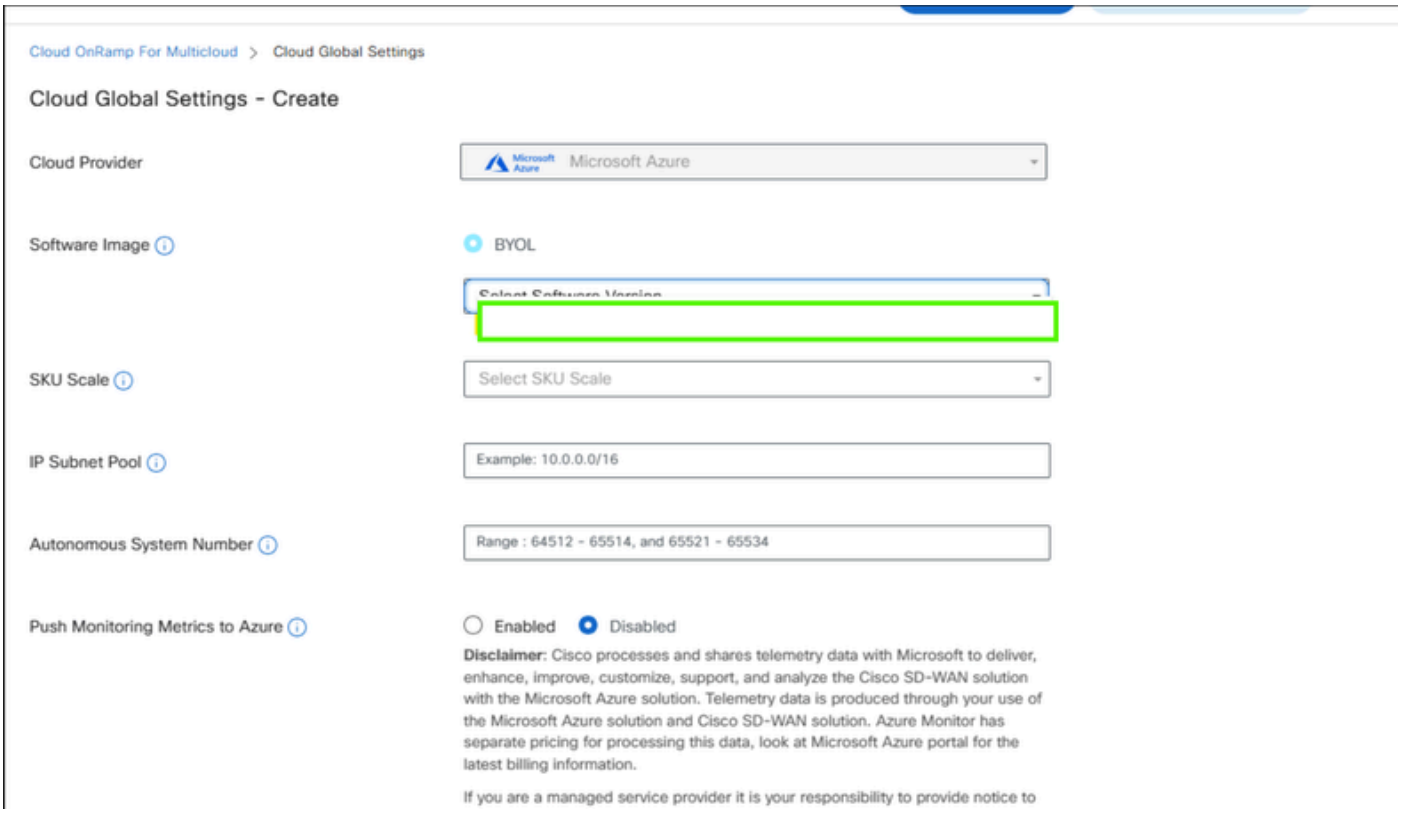
In diesem Dokument werden einige der häufigsten Probleme bei der Bereitstellung von Cloud Gateways in Azure von vManage Cloud on Ramp beschrieben.

Problem

Bei der Konfiguration von Cisco SD-WAN Cloud OnRamp für Microsoft Azure ist das Feld zur Auswahl von Software-Images für cEdge-Geräte in den globalen Einstellungen von vManage leer, wodurch die Bereitstellung von cEdge-Instanzen in Azure Cloud verhindert wird.

Symptome:

- Die Softwareversion von cEdge, die für die zukünftige Implementierung im Azure Cloud-Feld unter vManage > Cloud OnRamp For Multicloud > Cloud Global Settings geplant ist, ist leer.
- Anfängliche Admin-Tech-Protokolle können Azure-Fehler anzeigen: "AuthorizationFailed" (Autorisierung fehlgeschlagen) mit einer Meldung, die darauf hinweist, dass der Client nicht autorisiert ist, eine Microsoft.Network/networkVirtualApplianceSkus/read-Aktion auszuführen.
- In Administrator-Tech-Protokollen kann RetryError angezeigt werden: HTTPSConnectionPool(...) Max. Anzahl von Wiederholungen überschritten mit URL: ... (Ausgelöst durch Antwortfehler "zu viele 502 Fehlerantworten"), wenn vManage versucht, Network Virtual Appliance (NVA) SKUs from management.azure.com abzurufen.



Sie finden dieses Protokoll im Pfad /var/log/nms/containers/cloudagent-v2/cloudagent.log und es zeigt an, dass die Berechtigungsebene im Azure-Konto falsch ist.

```
[2025-07-18T04:14:53UTC+0000:140226169132800:ERROR:ca-
v2:azure_resource_helper.py:351] Fehler beim Abrufen von Ressourcen für {
"cloudType": "AZURE",
"Konto-ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
"Kontoname": "<Kontoname>",
"Region": "Eastus2",
Typ: "NVA_SKUS"
}:Azure-Fehler: Autorisierung fehlgeschlagen
Nachricht: Der Client "yyyyyyyyy-yyyyy-yyyyyyyyyyy" mit der Objekt-ID "yyyyyyyyy-yyyyy-yyyyy-
yyyyyyyyyyy" verfügt nicht über die Berechtigung zum Ausführen der Aktion <<<<< nicht
ausreichend

"Microsoft.Network/networkVirtualApplianceSkus/read" über "/subscriptions/xxxxxxxx-xxxx-xxxx-
xxxx-xxxxxxxxxxx/providers/Microsoft.Network/networkVirtualApplianceSkus/ciscosdwan", oder
der Bereich ist ungültig. Wenn Sie kürzlich Zugriff erhalten haben, aktualisieren Sie Ihre
Anmeldeinformationen.
[2025-07-18T04:14:53UTC+0000:140226169132800:INFO:ca-v2:grpc_service.py:1011]
Rückgabe der GetAzureResourceInfo-Antwort: {
"mcText": {
"TenantId": "<Tenanname>",
"ctxId": "zzzzzzzz-zzzz-zzzz-zzzz-zzzz-zzzzzzzzzz"
},
Status: {
```

"Code": OK

}

}

Dieses Protokoll befindet sich im gleichen Pfad /var/log/nms/containers/cloudagent-v2/cloudagent.log. Es zeigt an, dass mehrere Ressourcengruppen in Azure konfiguriert wurden.

[2025-09-01T04:07:35UTC+0000:140226169132800:ERROR:ca-v2:azure_resource_helper.py:351] Fehler beim Abrufen von Ressourcen für {

"cloudType": "AZURE",

"Konto-ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

"Kontoname": "<Kontoname>",

"Region": "Eastus2",

Typ: "NVA_SKUS"

}:Fehler in Anforderung., RetryError: HTTPSConnectionPool(host='management.azure.com', port=443): Max. Anzahl von Wiederholungen überschritten mit URL: /subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/providers/Microsoft.Network/networkVirtualApplianceSkus/ciscosdwan?api-version=2020-05-01 (Ausgelöst durch ResponseError('zu viele 502 Fehlerantworten'))

[2025-09-01T04:07:35UTC+0000:140226169132800:INFO:ca-v2:grpc_service.py:1011] Rückgabe der GetAzureResourceInfo-Antwort: {

"mcText": {

"TenantId": "<Tenanname>",

"ctxId": "zzzzzzzz-zzzz-zzzz-zzzz-zzzz-zzzzzzzzzz"

},

Status: {

"Code": OK

}

}

In vManage ist dies eines der allgemeinen Protokolle, die angezeigt werden, wenn die Aufgabe

bereitgestellt wird, nachdem dem Konto in Azure die Berechtigungsebene zugewiesen wurde. Der Kontotyp ist jedoch nicht Enterprise.

[27. August 2025, 19:46:46 UTC] Erstellen eines MultiCloud-Gateways: <Kontoname>

[27. August 2025, 19:46:47 UTC] Ressourcengruppe erfolgreich abgerufen: <Kontoname> aus der Cloud

[27. August 2025, 19:46:47 UTC] Erstellen eines Speicherkontos unter "Ressourcengruppe": <Kontoname

[27. August 2025, 19:46:49 UTC] Speicherkonto unter Ressourcengruppe: Fehler beim Erstellen von <Ko

[27. August 2025, 19:46:49 Uhr UTC] Weitere Informationen: Azure-Fehler: AnforderungNichtZulässigDur

Nachricht: Die Ressource 'lcoix7mu7rcrswtdkyj0jsyw' wurde von der Richtlinie nicht zugelassen. Richtlinie xxxxxxxxxxxx)","id":"/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/providers/Microsoft.Authorizati

"policyDefinition":{"name":"Der öffentliche Zugriff auf das Speicherkonto sollte untersagt werden","id":"/pro auf den Kontotyp in Azure ist nicht korrekt, Abonnement muss Enterprise sein

"policySetDefinition":{"name":"Microsoft Cloud Security Benchmark","id":"/providers/Microsoft.Authorizatio

Ziel: lcoix7mu7rcrswtdkyj0jsyw

Zusätzliche Informationen:

Typ: Richtlinienverletzung

Info: {

"evaluationDetails": {

"evaluierteAusdrücke": [

{

Ergebnis: "Wahr",

"AusdruckKind": "Feld",

Ausdruck: "Typ"

Pfad: "Typ"

"expressionValue": "Microsoft.Storage/storage-Konten",

"targetValue": "Microsoft.Storage/storage-Konten",

"Operator": "Gleich"

},

```
            {
               Ergebnis: "Falsch",
               "AusdruckKind": "Feld",
               Ausdruck: "id",
               Pfad: "id",
               "expressionValue": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/resourceGr
               "targetValue": "/resourceGroups/aro-",
               "Operator": "Enthält"
            },
            {
               Ergebnis: "Falsch",
               "AusdruckKind": "Feld",
               Ausdruck: "Microsoft.Storage/storageAccounts/allowBlobPublicAccess",
               Pfad: "properties.allowBlobPublicAccess",
               "targetValue": "Falsch",
               "Operator": "Gleich"
            }
         ]
      },
      "policyDefinitionId" "/providers/Microsoft.Authorization/policyDefinitions/yyyyyyy-yyyy-yyyyy-yy
      "policySetDefinitionId" "/providers/Microsoft.Authorization/policySetDefinitions/zzzzzz-zzzz-zzz
      "policyDefinitionReferenceId": "StorageDisallowPublicAccess",
      "policySetDefinitionName": ‚zzzzzzzz-zzzz-zzzz-zzzz-zzzz-zzzzzzzzzz‘,
      "policySetDefinitionDisplayName": "Microsoft Cloud Security Benchmark",
      "policySetDefinitionVersion" "57.53.0",
      "policyDefinitionName": "yyyyyyyyyy-yyyyy-
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
```

```
            "policyDefinitionDisplayName": "Der öffentliche Zugriff auf Speicherkonten sollte untersagt wer
            "policyDefinitionVersion": "3.1.1",
            "policyDefinitionEffect": "Verweigern",
            "policyAssignmentId": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/providers/Micros
            "policyAssignmentName": "SecurityCenterIntegrated",
            "policyAssignmentDisplayName": "ASC-Standard (Abonnement: xxxxxxxx-xxxx-xxxx-xxxx-xxx
            "policyAssignmentScope" "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
            "policyAssignmentParameters": {
                "disallowPublicBlobAccessEffect": "leugnen"
            },
            "policyExemptionIds": [],
            "policyEnrollmentIds": []
        }
[27-Aug-2025 19:46:49 UTC] Rolling back changes made...
[27. August 2025, 19:46:49 Uhr UTC] Rollback abgeschlossen
[27-Aug-2025 19:46:49 UTC] Interner Fehler beim Erstellen oder Abrufen des Speicherkontos
```


Mögliche Ursachen:

1. Unzureichende Azure-Berechtigungen: Auch wenn das Azure-Konto erfolgreich verknüpft ist und über Mitwirkerrechte verfügt, sind von vManage bestimmte Berechtigungen erforderlich. Zum Lesen von SKUs der virtuellen Network Appliance kann diese fehlen oder falsch konfiguriert sein.

2. Mehrere Azure-Ressourcengruppen: In der Cisco Dokumentation für die Azure vWAN-Integration wird angegeben, dass nur eine Ressourcengruppe für die Cloud OnRamp-Einrichtung zulässig ist. Wenn vManage versucht, verfügbare SKUs abzufragen, können mehrere alte oder redundante Ressourcengruppen zu zu vielen 502 Fehlerantworten von Azure führen.

Lösung

1. Azure-Berechtigungen überprüfen:

- Stellen Sie sicher, dass die mit vManage verknüpfte Azure-Anwendung oder der mit

vManage verknüpfte Dienstprinzipal über die erforderlichen Berechtigungen zum Lesen der SKUs der virtuellen Netzwerkappliance verfügt. Die spezifische Aktion ist "Microsoft.Network/networkVirtualApplianceSkus/read".
- Wenn kürzlich Berechtigungen gewährt oder geändert wurden, aktualisieren Sie die Anmeldeinformationen in vManage oder Azure.
- Diese Schritte werden im Cisco Cloud onRamp for Multi-Cloud Azure Version2 Solution Guide im Abschnitt Azure Subscription-Berechtigungen überprüfen dokumentiert.

2. Azure-Ressourcengruppen verwalten:

- Überprüfen Sie Ihr Azure-Abonnement auf alle alten oder redundanten Ressourcengruppen im Zusammenhang mit Cisco SD-WAN Cloud OnRamp.
- Laut Cisco-Dokumentation ist nur eine Ressourcengruppe für die Azure vWAN-Integration zulässig. Löschen Sie alle alten Ressourcengruppen, und stellen Sie sicher, dass nur die aktive und die erforderliche Ressourcengruppe erhalten bleibt. Diese Aktion wurde beobachtet, um Fehler zu beheben, zu viele 502 Fehlerantworten.

Zugehörige Informationen

- Cisco Catalyst SD-WAN Cloud OnRamp Konfigurationsleitfaden, Cisco IOS XE Catalyst SD-WAN Version 17.x In diesem Dokument werden die Einschränkungen beschrieben, einschließlich der Anforderung einer einzelnen Ressourcengruppe für die Azure vWAN-Integration.
- Erweiterung der Cisco SD-WAN-Fabric auf Azure mit Cisco Cloud onRamp für Multi-Cloud: Dieser Leitfaden kann weitere Details zum Überprüfen des Azure-Abonnements und der Berechtigungen für die Integration enthalten.
- Zugehöriges Azure CLI-Problem (bei Kontext zu 502-Fehlern): Obwohl es sich nicht um ein direktes Dokument von Cisco handelt, bietet dieses GitHub-Problem Einblicke in ähnliche 502-Fehlerantworten von Azure API, die für das zugrunde liegende Azure-Verhalten relevant sein können.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.