Troubleshoot Cloud OnRamp Issues in Microsoft Azure

Contents

Introduction

This document describes some of the common problems at deploying Cloud Gateways in the Azure from vManage Cloud on Ramp.

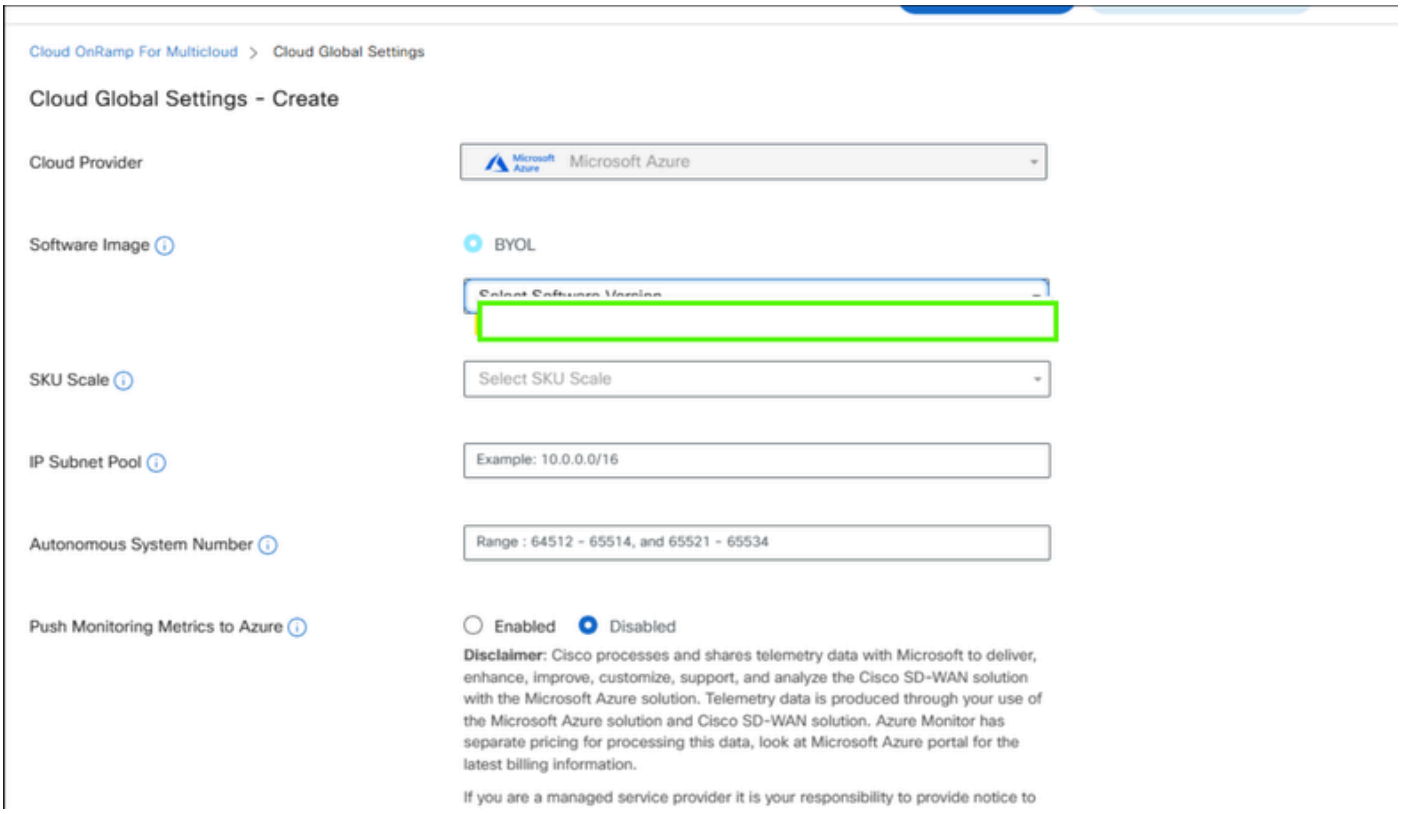
Problem

When configuring Cisco SD-WAN Cloud OnRamp for Microsoft Azure, the Software Image selection field for cEdge devices appears empty in vManage Global Settings, preventing the deployment of cEdge instances in Azure Cloud.

Symptoms:

- The software release of cEdge that is scheduled for future implementation on Azure Cloud field in **vManage > Cloud OnRamp For Multicloud > Cloud Global Settings** is blank.

- Initial admin-tech logs can show Azure Error: "AuthorizationFailed" with a message indicating the client lacks authorization to perform Microsoft.Network/networkVirtualApplianceSkus/read action.
- Admin-tech logs can show RetryError: HTTPSConnectionPool(...) Max retries exceeded with url: ... (Caused by Response Error "too many 502 error responses") when vManage attempts to retrieve Network Virtual Appliance (NVA) SKUs from management.azure.com.



You can find this log in the path **/var/log/nms/containers/cloudagent-v2/cloudagent.log** and it shows that privilege level is incorrect in Azure account.

```
[2025-07-18T04:14:53UTC+0000:140226169132800:ERROR:ca-v2:azure_resource_helper.py:351] Failed to get resources for {
"cloudType": "AZURE",
"accountId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
"accountName": “<account_name>“,
"region": "eastus2",
"type": "NVA_SKUS"
}:Azure Error: AuthorizationFailed
Message: The client 'yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy' with object id 'yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy' does not have authorization to perform action <<<< It confirms that privileges are not sufficient

'Microsoft.Network/networkVirtualApplianceSkus/read' over scope '/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/providers/Microsoft.Network/networkVirtualApplianceSkus/ciscosdwan' or the scope is invalid. If access was recently granted, please refresh your credentials.
[2025-07-18T04:14:53UTC+0000:140226169132800:INFO:ca-v2:grpc_service.py:1011] Returning GetAzureResourceInfo Response: {
"mcCtxt": {
"tenantId": "<tenan name>",
"ctxId": "zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzzz"
},
"status": {
"code": "OK"

  }

}
```

This log can be found in the same path **/var/log/nms/containers/cloudagent-v2/cloudagent.log** ant it shows that several resource groups have been configured in Azure.

```
[2025-09-01T04:07:35UTC+0000:140226169132800:ERROR:ca-v2:azure_resource_helper.py:351] Failed to get resources for {

 "cloudType": "AZURE",

 "accountId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",

 "accountName": "<account_name>",

 "region": "eastus2",

 "type": "NVA_SKUS"

}:Error occurred in request., RetryError: HTTPSConnectionPool(host='management.azure.com', port=443): Max retries exceeded with url: /subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/providers/Microsoft.Network/networkVirtualApplianceSkus/ciscosdwan?api-version=2020-05-01 (Caused by ResponseError('too many 502 error responses'))

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

 "mcCtxt": {

  "tenantId": "<tenan name>",

  "ctxId": "zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzzz"

 },

 "status": {

  "code": "OK"

 }

}
```

From vManage, this is one of the common logs shown when the task is deployed after the account in Azure was assigned with the privilege level; however, the type of account is not Enterprise.

```
[27-Aug-2025 19:46:46 UTC] Creating MultiCloud Gateway: <account name>

[27-Aug-2025 19:46:47 UTC] Successfully fetched Resource Group: <account name> from the cloud

[27-Aug-2025 19:46:47 UTC] Creating Storage Account under Resource Group: <account name> in the cloud

[27-Aug-2025 19:46:49 UTC] Storage Account under resource group: <account name> failed to get created in the cloud
```

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

Message: Resource 'lcoix7mu7rcrswtdkyj0jsyw' was disallowed by policy. Policy identifiers: '[{"policyAssignment":{"name":"ASC Default (subscription: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx)","id":"/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/providers/Microsoft.Authorization/policyAssignments/SecurityCenterBuiltIn"},

"policyDefinition":{"name":"Storage account public access should be disallowed","id":"/providers/Microsoft.Authorization/policyDefinitions/yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy","version":"3.1.1"}, <<<< **It refers to account type in Azure is not correct, subscription must be Enterprise**

"policySetDefinition":{"name":"Microsoft cloud security benchmark","id":"/providers/Microsoft.Authorization/policySetDefinitions/zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzzz","version":"57.53.0"}}]'.

Target: lcoix7mu7rcrswtdkyj0jsyw

Additional Information:

Type: PolicyViolation

Info: {

"evaluationDetails": {

"evaluatedExpressions": [

{

"result": "True",

"expressionKind": "Field",

"expression": "type",

"path": "type",

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

"targetValue": "Microsoft.Storage/storageAccounts",

"operator": "Equals"

},

{

"result": "False",

"expressionKind": "Field",

"expression": "id",

"path": "id",

"expressionValue": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-

```
xxxxxxxxxxxx/resourceGroups/<account
name>/providers/Microsoft.Storage/storageAccounts/lcoix7mu7rcrswtdkyj0jsyw",

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

                    "operator": "Contains"

                },

                {

                    "result": "False",

                    "expressionKind": "Field",

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

                    "path": "properties.allowBlobPublicAccess",

                    "targetValue": "false",

                    "operator": "Equals"

                }

            ]

        },

        "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/yyyyyyyy-yyyy-
yyyy-yyyy-yyyyyyyyyyyy",

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

        "policyDefinitionReferenceId": "StorageDisallowPublicAccess",

        "policySetDefinitionName": "zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzzz",

        "policySetDefinitionDisplayName": "Microsoft cloud security benchmark",

        "policySetDefinitionVersion": "57.53.0",

        "policyDefinitionName": "yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy",

        "policyDefinitionDisplayName": "Storage account public access should be disallowed",

        "policyDefinitionVersion": "3.1.1",

        "policyDefinitionEffect": "deny",

        "policyAssignmentId": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Authorization/policyAssignments/SecurityCenterBuiltIn",

        "policyAssignmentName": "SecurityCenterBuiltIn",

        "policyAssignmentDisplayName": "ASC Default (subscription: xxxxxxxx-xxxx-xxxx-xxxx-
```

xxxxxxxxxxxx)",

"policyAssignmentScope": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",

"policyAssignmentParameters": {

"disallowPublicBlobAccessEffect": "deny"

},

"policyExemptionIds": [],

"policyEnrollmentIds": []

}

[27-Aug-2025 19:46:49 UTC] Rolling back changes made...

[27-Aug-2025 19:46:49 UTC] Rollback completed

[27-Aug-2025 19:46:49 UTC] Internal error in creating or fetching Storage Account

Potential Causes:

1. Insufficient Azure Privileges: Even if the Azure account is successfully linked and has contributor rights, specific permissions are required by vManage. To read Network Virtual Appliance SKUs, it can be missing or incorrectly configured.

2. Multiple Azure Resource Groups: Cisco documentation for Azure vWAN integration specifies that only one resource group is allowed for the Cloud OnRamp setup. Having multiple old or redundant resource groups can lead to, too many 502 error responses, from Azure when vManage tries to query available SKUs.

Solution

1. Verify Azure Permissions:

- Ensure the Azure application or service principal linked to vManage has the necessary permissions to read Network Virtual Appliance SKUs. The specific action is Microsoft.Network/networkVirtualApplianceSkus/read.
- If permissions were recently granted or modified, refresh credentials within vManage or Azure.
- These steps are documented in the **Cisco Cloud onRamp for Multi-Cloud Azure Version2 Solution Guide** in section **Check Azure Subscription Permissions**.

2. Manage Azure Resource Groups:

- Review your Azure subscription for any old or redundant resource groups related to Cisco SD-WAN Cloud OnRamp.
- As per Cisco documentation, only one resource group is allowed for the Azure vWAN integration. Delete all old resource groups, ensuring only the active and necessary one remains. This action has been observed to resolve error, too many 502 error responses.

Related Information

- Cisco Catalyst SD-WAN Cloud OnRamp Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x This document details restrictions, including the single resource group requirement for Azure vWAN integration.
- Extending the Cisco SD-WAN Fabric into Azure with Cisco Cloud onRamp for Multi-Cloud: This guide can provide further details on checking Azure subscription and permissions for the integration.
- Related Azure CLI Issue (for context on 502 errors): While not a direct Cisco document, this GitHub issue provides insight into similar 502 error responses from Azure API, which can be relevant to the underlying Azure behavior.