

Solucionar problemas de Cloud OnRamp en Microsoft Azure

Contenido

[Introducción](#)

[Problema](#)

[Solución](#)

[Información Relacionada](#)

Introducción

Este documento describe algunos de los problemas comunes de la implementación de gateways de nube en Azure desde vManage Cloud on Ramp.

Problema

Al configurar Cisco SD-WAN Cloud OnRamp para Microsoft Azure, el campo de selección de imagen de software para dispositivos cEdge aparece vacío en vManage Global Settings, lo que impide la implementación de instancias de cEdge en Azure Cloud.

Síntomas:

- La versión de software de cEdge que está programada para su futura implementación en el campo Nube de Azure en vManage > Cloud OnRamp For Multicloud > Cloud Global Settings está en blanco.
- Los registros iniciales de admin-tech pueden mostrar el error de Azure: "AuthorizationFailed" con un mensaje que indica que el cliente carece de autorización para realizar la acción Microsoft.Network/networkVirtualApplianceSkus/read.
- Los registros de tecnología de administración pueden mostrar RetryError: HTTPSConnectionPool(...) Se superaron los reintentos máximos con la dirección URL: ... (Causado por el error de respuesta "demasiadas respuestas de error 502") cuando vManage intenta recuperar las SKU de dispositivos virtuales de red (NVA) from management.azure.com.

Cloud OnRamp For Multicloud > Cloud Global Settings

Cloud Global Settings - Create

Cloud Provider Microsoft Azure

Software Image BYOL

Select Software Version

SKU Scale Select SKU Scale

IP Subnet Pool Example: 10.0.0.0/16

Autonomous System Number Range : 64512 - 65514, and 65521 - 65534

Push Monitoring Metrics to Azure Enabled Disabled

Disclaimer: Cisco processes and shares telemetry data with Microsoft to deliver, enhance, improve, customize, support, and analyze the Cisco SD-WAN solution with the Microsoft Azure solution. Telemetry data is produced through your use of the Microsoft Azure solution and Cisco SD-WAN solution. Azure Monitor has separate pricing for processing this data, look at Microsoft Azure portal for the latest billing information.

If you are a managed service provider it is your responsibility to provide notice to

Puede encontrar este registro en la ruta de acceso /var/log/nms/containers/cloudagent-v2/cloudagent.log y muestra que el nivel de privilegio es incorrecto en la cuenta de Azure.

```
[2025-07-18T04:14:53UTC+0000:140226169132800:ERROR:ca-
v2:azure_resource_helper.py:351] Error al obtener recursos para {
"cloudType": "AZURE",
"accountId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
"accountName": "<account_name>",
"región": "eastus2",
"tipo": "NVA_SKUS"
}:Error de Azure: Error de autorización
Mensaje: El cliente 'yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyy' con el id de objeto 'yyyyyy-yyyy-yyyy-
yyyy-yyyy-yyyyyyyy' no tiene autorización para realizar la acción <<<< Confirma que los
privilegios no son suficientes

'Microsoft.Network/networkVirtualApplianceSkus/read' sobre el ámbito '/subscriptions/xxxxxxxx-
xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Network/networkVirtualApplianceSkus/ciscosdwan' o el ámbito
no es válido. Si el acceso se ha concedido recientemente, actualice sus credenciales.
[2025-07-18T04:14:53UTC+0000:140226169132800:INFO:ca-v2:grpc_service.py:1011]
Devolviendo GetAzureResourceInfo Respuesta: {
"mcCtxt": {
"tenantId": "<nombre del arrendatario>",
"ctxId": "zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzz"
},
"estado": {
```

```
"código": "OK"
```

```
}
```

```
}
```

Este registro se puede encontrar en la misma ruta /var/log/nms/containers/cloudagent-v2/cloudagent.log y muestra que se han configurado varios grupos de recursos en Azure.

```
[2025-09-01T04:07:35UTC+0000:140226169132800:ERROR:ca-  
v2:azure_resource_helper.py:351] Error al obtener recursos para {
```

```
"cloudType": "AZURE",
```

```
"accountId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx",
```

```
"accountName": "<account_name>",
```

```
"región": "eastus2",
```

```
"tipo": "NVA_SKUS"
```

```
};Error en la solicitud., RetryError: HTTPSPool(host='management.azure.com',  
puerto=443): Se excedieron los reintentos máximos con la dirección URL:  
/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-  
xxxxxxxxxxxxxx/providers/Microsoft.Network/networkVirtualApplianceSkus/ciscosdwan?api-  
version=2020-05-01 (Causado por ResponseError('too many 502 error response'))
```

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

```
"mcCtx": {
```

```
"tenantId": "<nombre del arrendatario>",
```

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

```
},
```

```
"estado": {
```

```
"código": "OK"
```

```
}
```

```
}
```

Desde vManage, este es uno de los registros comunes que se muestran cuando se implementa la

tarea después de asignar la cuenta de Azure con el nivel de privilegio; sin embargo, el tipo de cuenta no es Enterprise.

[27 de agosto de 2025, 19:46:46 UTC] Creación de un gateway de nube múltiple: <account name>

[27 de agosto de 2025, 19:46:47 UTC] Grupo de recursos obtenido correctamente: <account name> desde la nube

[27 de agosto de 2025, 19:46:47 UTC] Creación de una cuenta de almacenamiento en el grupo de recursos: <account name> en la nube

[27 de agosto de 2025, 19:46:49 UTC] Cuenta de almacenamiento en el grupo de recursos: <account name> no se pudo crear en la nube

[27-ago-2025 19:46:49 UTC] Detalles adicionales: Error de Azure: RequestDisallowedByPolicy

Mensaje: La directiva no permitió el recurso 'lcoix7mu7rcrswtdkyj0jsyw'. Identificadores de políticas: [{"policyAssignment":{"name":"ASC predeterminado (suscripción: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx)","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","version":"3.1.1"}, <<<< Se refiere a que el tipo de cuenta en Azure no es correcto, la suscripción debe ser Enterprise

"policySetDefinition":{"name":"evaluación de la seguridad en la nube de Microsoft","id":"/providers/Microsoft.Authorization/policySetDefinitions/zzzzzzzz-zzzz-zzzz-zzzzzzzzz","version":"57.53.0"}}].

Objetivo: lcoix7mu7rcrswtdkyj0jsyw

Información adicional:

Tipo: ViolaciónDePolítica

INFO: {

"evaluacióndetalles": {

"expresiones evaluadas": [

{

"resultado": "Verdadero",

"expressionKind": "Campo",

"expresión": "tipo",

```
        "trayecto": "tipo",

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

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

        "operador": "Es igual a"
    },
    {

        "resultado": "Falso",

        "expressionKind": "Campo",

        "expresión": "id",

        "trayecto": "id",

        "expressionValue": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/resourceGroups/<nombre de cuenta>/providers/Microsoft.Storage/storageAccounts/lcoix7mu7rcrswtdkyj0jsyw",

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

        "operador": "Contiene"
    },
    {

        "resultado": "Falso",

        "expressionKind": "Campo",

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

        "trayecto": "properties.allowBlobPublicAccess",

        "targetValue": "falso",

        "operador": "Es igual a"
    }
]

},

    "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/yyyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyy",
```

```
"policySetDefinitionId":  
"/providers/Microsoft.Authorization/policySetDefinitions/zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzz",  
"policyDefinitionReferenceId": "StorageDisallowPublicAccess",  
"policySetDefinitionName": "zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzz",  
"policySetDefinitionDisplayName": "Referencia de seguridad en la nube de Microsoft",  
"policySetDefinitionVersion": "57.53.0",  
"policyDefinitionName": "yyyyyyyy-yyy-yyy-yyy-yyyyyyyyyy",  
"policyDefinitionDisplayName": "No se debe permitir el acceso público a la cuenta de  
almacenamiento",  
"policyDefinitionVersion": "3.1.1",  
"policyDefinitionEffect": "denegar",  
"policyAssignmentId": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-  
xxxxxxxxxxxxx/providers/Microsoft.Authorization/policyAssignments/SecurityCenterBuiltIn",  
"policyAssignmentName": "SecurityCenterBuiltIn",  
"policyAssignmentDisplayName": "ASC predeterminado (suscripción: xxxxxxxx-xxxx-  
xxxx-xxxx-xxxxxxxxxxxx)",  
"policyAssignmentScope": "/suscripciones/xxxxxxxx-xxxx-xxxx-xxxx-xxxx-  
xxxxxxxxxxxx",  
"policyAssignmentParameters": {  
  "disallowPublicBlobAccessEffect": "denegar"  
},  
"policyExemptionIds": [],  
"policyEnrollmentIds": []  
}
```

[27-ago-2025 19:46:49 UTC] Revirtiendo los cambios realizados...

[27-ago-2025 19:46:49 UTC] Reversión completada

[27-ago-2025 19:46:49 UTC] Error interno al crear o recuperar la cuenta de almacenamiento

Causas potenciales:

1. Privilegios de Azure insuficientes: incluso si la cuenta de Azure está vinculada correctamente y tiene derechos de colaborador, vManage requiere permisos específicos. Para leer las SKU de dispositivos virtuales de red, puede que falten o que estén configuradas de forma incorrecta.

2. Varios grupos de recursos de Azure: la documentación de Cisco para la integración de Azure vWAN especifica que solo se permite un grupo de recursos para la configuración de Cloud OnRamp. Si hay varios grupos de recursos antiguos o redundantes, Azure puede generar demasiadas respuestas de error 502 cuando vManage intenta consultar las SKU disponibles.

Solución

1. Compruebe los permisos de Azure:

- Asegúrese de que la aplicación de Azure o la entidad de servicio vinculada a vManage tiene los permisos necesarios para leer las SKU de dispositivos virtuales de red. La acción específica es Microsoft.Network/networkVirtualApplianceSkus/read.
- Si los permisos se concedieron o modificaron recientemente, actualice las credenciales en vManage o Azure.
- Estos pasos se documentan en la Guía de la solución Cisco Cloud onRamp para Multi-Cloud Azure Version2 en la sección Comprobación de los permisos de suscripción de Azure.

2. Administrar grupos de recursos de Azure:

- Revise su suscripción de Azure para ver si hay grupos de recursos antiguos o redundantes relacionados con Cisco SD-WAN Cloud OnRamp.
- Según la documentación de Cisco, solo se permite un grupo de recursos para la integración de Azure vWAN. Elimine todos los grupos de recursos antiguos, asegurándose de que sólo quede el activo y el necesario. Se ha observado que esta acción resuelve errores, demasiadas respuestas de error 502.

Información Relacionada

- [Guía de configuración de Cisco Catalyst SD-WAN Cloud OnRamp, Cisco IOS XE Catalyst SD-WAN versión 17.x](#) Este documento detalla las restricciones, incluido el requisito de grupo de recursos único para la integración de Azure vWAN.
- [Ampliación de Cisco SD-WAN Fabric a Azure con Cisco Cloud on Ramp para varias nubes:](#) Esta guía puede proporcionar más detalles sobre la comprobación de la suscripción de Azure y los permisos para la integración.
- [Problema relacionado con la CLI de Azure \(para el contexto de errores 502\)](#): Aunque no es un documento directo de Cisco, este problema de GitHub proporciona información sobre respuestas de error 502 similares de la API de Azure, que pueden ser relevantes para el comportamiento subyacente de Azure.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).