[Storage] The remote server returned an error: (403) Forbidden

Last updated by | Jackie Huang | Jan 4, 2022 at 12:24 AM PST
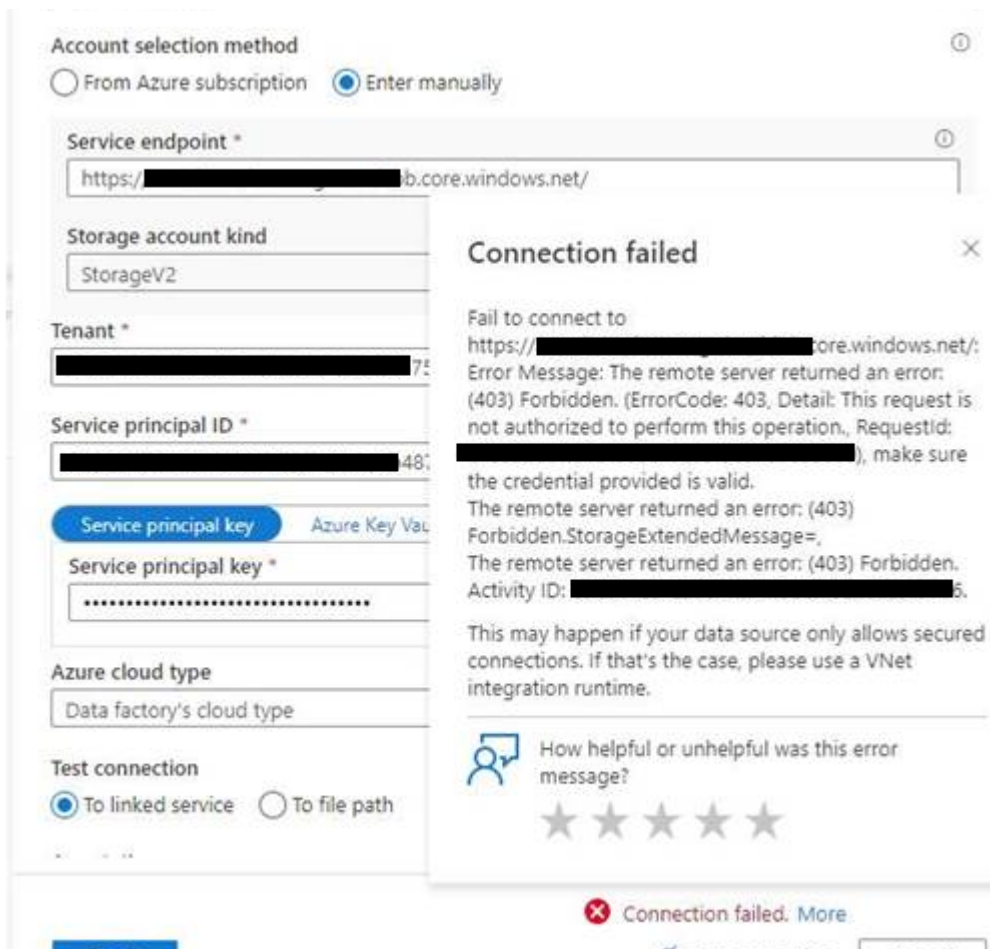
Contents

Issue

Customer facing issues in creating Linked Service for storage account. Getting error:

Fail to connect to <StorageURL>: Error Message: The remote server returned an error: (403) Forbidden. (ErrorCode: 403, Detail: This request is not authorized to perform this operation.

Investigation

- In this case, Storage Account was in a different tenant, and Data Factory in another tenant.

- Customer was using Managed Identity, which does not support cross-tenant.

Resolution

1. If the service principal is in Tenant A in your scenario cross tenant should work.
2. Azure IR and storage should be in the same region.
3. Service principal and storage should be in the same tenant
4. Static IP does not work for storage if storage and compute in same region
5. You will need to create IR in different region so internal IP will not be used
6. Another thing is with the Service principal "Allow trusted service" does not work.
7. Because Trusted Service can only be used with the Managed Identity but Managed Identity does not support in cross tenant.

Workaround to use is:

You will need to create an Azure IR in a different region, then make storage linked service use the specified Azure Integration Runtime, in this way, ADF copy activity will not auto resolve the region, but use the Azure Integration Runtime region, and this will make the compute and storage in different region, and IP whitelist will work in this case as cross region communication will use compute public IP address.

Links:

1. https://supportability.visualstudio.com/AzureVMPOD/_wiki/wikis/AzureVMPOD/265582/Azure_Storage_Firewall-and-Virtual-Networks?anchor=**how-to-onboard-my-service-with-azure-storage-firewall-and-vnet%3F**
2. This doc talks about how to setup VNET Configure Azure Storage firewalls and virtual networks | Microsoft Docs for a storage account.
3. https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security#grant-access-from-an-internet-ip-range ⧉
4. https://docs.microsoft.com/en-us/azure/data-factory/azure-integration-runtime-ip-addresses ⧉
5. When connecting to Azure Storage account, IP network rules have no effect on requests originating from the Azure integration runtime in the same region as the storage account.

Additional Information:

- **Icm References:** Icm Link ⧉
- **Author:** v-pasir
- **Reviewer:** vimals
- **Keywords:**

How good have you found this content?

🙂 🙁