

# Linked Service for Office 365 with Firewall Enabled

Last updated by | Graziani Orcai | Jun 20, 2022 at 7:22 AM PDT

## ISSUE

Customer is trying to run a copy activity with Office 365 (Microsoft Graph) as a source, and has Firewall enabled on his sink (storage – Blob or ADLS), and it fails with error:

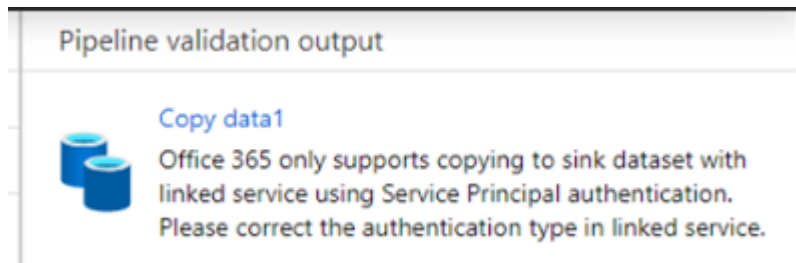
ADLS Gen2 operation failed for: Storage operation '' on container XXXX get failed with 'Operation returned an invalid status code 'Forbidden''. Possible root causes: (1). It's possible because the service principal or managed identity don't have enough permission to access the data. (2). It's possible because some IP address ranges of Azure Data Factory are not allowed by your Azure Storage firewall settings.

## CAUSE


By design – several limitations.

## TROUBLESHOOTING STEPS

If customer has an Office 365 Linked Service/Microsoft Graph Dataset as a source in a copy activity, he MUST use Service Principal as an authentication: [Datasets, regions, and sinks supported by Microsoft Graph Data Connect - Microsoft Graph | Microsoft Docs](#) 





Also, if cx wants to use in his ADLS Gen2 account Firewall enable +

Allow Azure services on the trusted services list to access this storage account, he MUST use Managed identity: [Copy and transform data in Azure Data Lake Storage Gen2 - Azure Data Factory & Azure Synapse | Microsoft Docs](#) 

- If want to use the public Azure integration runtime to connect to the Data Lake Storage Gen2 by leveraging the **Allow trusted Microsoft services to access this storage account** option enabled on Azure Storage firewall, you must use managed identity authentication.


So, in a scenario where customer wants to have the firewall enabled on his storage, and take advantage of the « Allow Azure services on the trusted services» option, but wants to run a copy activity with Microsoft Graph as a source and storage as a sink, he will face an impasse, where his only option will be to use the Service Principal, but he will have to whitelist the IPs on the firewall, instead of using the Allow trusted services.

Nevertheless, if Storage Account is in same region as ADF, the IPs won't have effect - this is a known issue: [Azure Integration Runtime IP addresses - Azure Data Factory | Microsoft Docs](#) 


In that case, customer will face another impasse, which is only solved by using a storage account in another region, different then ADF region, but both ADF and Storage must be in the list of regions supported by Microsoft Graph: [Datasets, regions, and sinks supported by Microsoft Graph Data Connect - Microsoft Graph | Microsoft Docs](#) 


## SOLUTION:

In conclusion, if customer is trying to copy data from Microsoft Graph (Office 365) to a Storage (sink), and have Firewall enabled in his storage with the option Allow Azure services on the trusted services list to access this storage account enabled, he MUST create a storage in a region covered by Microsoft Graph, but different then ADF region, and whitelist all the Data Factory region IPs in the Storage Firewall, and use Service Principal as authentication method for the Linked Service.

More information: Datasets, regions, and sinks supported by Microsoft Graph Data Connect: [Datasets, regions, and sinks supported by Microsoft Graph Data Connect - Microsoft Graph | Microsoft Docs](#) 

Azure Data Lake Storage Gen2 Linked Service: [Copy and transform data in Azure Data Lake Storage Gen2 - Azure Data Factory & Azure Synapse | Microsoft Docs](#) 

Azure Integration Runtime IP addresses: [Azure Integration Runtime IP addresses - Azure Data Factory | Microsoft Docs](#) 

Azure IP Ranges and Service Tags – Public Cloud: [Download Azure IP Ranges and Service Tags – Public Cloud from Official Microsoft Download Center](#) 

**How good have you found this content?**

