Scope Activity: Restricting Authoring and Execution of Scope Activity to CorpNet

Last updated by | Ranjith Katukojwala | Mar 7, 2023 at 11:35 AM PST

Contents

WHAT

ADF will be adding a restriction to authoring and execution of Scope Activity only from Corpnet

Note: The Scope Activity can only be used by Microsoft Internal Tenants only

WHY

Security guidelines enforced from ADLA/S teams.

[Note that as of early 2022 this restriction is in the process of being removed]

WHAT DOES IT MEAN TO CUSTOMERS

1. Any data factory that has pipeline with Scope Activity, can only be accessed from Microsoft Corpnet.
2. All clients (UX/SDK/Powershell) must be in Corpnet

REFERENCE DOCUMENTS

The following document provides a lot more info regarding this process. It also talks about access methods.

[Datalake Scope Activity Doc](#) ⧉

This document is the base for a series of discussions on how the Cosmos to ADLA/S process works

[Cosmos upgrade doc](#) ⧉

WHAT HAPPENS TO MY EXISTING RUNS WITH SCOPE ACTIVITY

Existing Pipeline Runs will fail with error "Data Factory is not authorized to use Scope Activity;"

Scope is an internal facing activity and due to security requirements, it can only be run from within Microsoft IP addresses. To use Scope Activity, user will have to add a GlobalParameter to their factory { "name" :

"ADFScopeSupport", "value" : "true" }. After this global parameter is added, all calls to their factory must originate from Microsoft IP addresses (GET calls are still allowed), if not they will fail with the error **"Client IP not authorized to access the API. ClientIPNotAuthorized"**.

If ADF resources are cached in the browser, you might see some things appear to load and others not, but the resources that load are not coming from our servers. If you test with an Incognito window, you should see no resources coming through from Azure.

HOW DO I ACCESS IP RESTRICTED DATA FACTORIES OVER VPN

Please note that VPN connections are NOT considered to be within Corpnet.

If you need to access IP restricted data factories remotely, you may be able to route traffic to [management.azure.com](#) ⊡ over your corpnet VPN connection. Keep in mind this can fix ADF access but cause other issues so proceed with caution:

1. Open an administrative command prompt
2. Run 'nslookup [management.azure.com](#) ⊡' and make note of the IP address listed
3. Run 'ipconfig' to get your MSFTVPN IP address
4. Add a route rule to force all traffice to [management.azure.com](#) ⊡ via VPN with 'route -p add <<nslookupip>> mask 255.255.255.255 <<Your MSFTVP IPv4 address>>'
5. Test access to Data Factory in an InPrivate window to avoid caching issues

If this causes any issues, you can undo this by running 'route -p delete <<nslookupip>>'

Alternatively, you can get reliable access to ADF via a Remote Desktop. You can request one here: [https://microsoft.sharepoint.com/sites/Security_Tools_Services/SitePages/WindowsVirtualDesktop/CSEO-Windows-Virtual-Desktop-Pilot.aspx](#) ⊡

Please look at [Datalake Scope Activity Doc](#) ⊡ for more information.

How good have you found this content?

😊 🙁