Azure storage 403 or 502 or 504 issue in lookup activity execution

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

Contents

- Issue
- Root Cause
- Action
- Resolution

Issue

Customer try to run lookup activity at self-hosted IR, linked IR or Azure IR while meeting following error message:

- Type=Microsoft.WindowsAzure.Storage.StorageException,Message=The remote server returned an error: (502) Bad Gateway
- Type=Microsoft.WindowsAzure.Storage.StorageException,Message=The remote server returned an error: (403) Forbidden.StorageExtendedMessage=This request is not authorized to perform this operation.
- Type=Microsoft.WindowsAzure.Storage.StorageException,Message=Unable to connect to the remote server,Source=Microsoft.WindowsAzure.Storage,Type=System.Net.WebException,Message=Unable to connect to the remote server, Message=No connection could be made because the target machine actively refused it 13.82.152.48:443

Root Cause

- If the customer is using self-hosted IR to run lookup activity and meet up error, mostly the connectivity issue could be caused by the following factors:
  - Proxy setting in the self-hosted IR's node
  - Firewall setting in the self-hosted IR's node

Action

1. Get the issue storage account by below kusto query.

```
CustomLogEvent
| where ActivityId == "failed activity id"
| where * contains "Create read-write SAS of container"
```

<LogProperties><Text>Create read-write SAS of container '7dcf912c-10d0-4ee0-89fa-5d00fcfee667' in account 'transfereustorage2' with expiry time: 3000 seconds. </Text></LogProperties>

In this case, **transfereustorage2** is the blocked one.

Ask customer to check the configuration on IR machine with following steps one by one:

- Login the physical IR machine.
- Start network trace: *netsh trace start capture=yes level=5 tracefile=c:%computername%nettrace.etl scenario=netconnection*
- Test connection: *Test-NetConnection blob-storage -port 443 (For example, Test-NetConnection transfereustorage2.blob.core.windows.net -port 443)*
- Stop network trace: *netsh trace stop*
- Get IP details: *ipconfig /all*
- Copy the whole output and save it as one file.

Resolution

Suggest the customer to change the proxy, firewall, network setting based on up test result and public doc.

- Self-hosted IR Ports and Firewalls
- Specific connectors doc which may have endpoint or ports requirements. E.g. ADLS connector.

2. If the customer is using Azure IR to run lookup activity and meet up error, suggest the customer to try disabling the data store's firewall setting, for example, run lookup activity with Azure blob, ADLS Gen1 or ADLS Gen2 as data source.

- If succeeded after disable firewall setting, check the following known issues. If it is a new issue, contact PG team for further help.
  - In general, the firewall setting shouldn't rely on the whitelisted IP address ranges, as Azure IR uses dynamic IP addresses.
  - For **Azure Storage (Blob, Table, File) and ADLS Gen 2**, the customer needs to disable the firewall setting.
    - If firewall setting is must have, (before the V-Net is available) the customer needs to set up the self-hosted IR and white list those nodes' IP address.
  - For **ADLS Gen1**, the customer can turn on the firewall with setting "Allow access to Azure services" enabled. If it fails, there is a known issue in ADLS side that certain account with preview features may have connectivity issues.
- If still fails, contact PG team.

Additional Information:

- **Icm References:**
- **Author:** zhanyu
- **Reviewer:** chargu; vimals
- **Micro-service:** Transfer Web, Self-hosted IR, Azure IR, Task Management Service
- **Keywords:**

How good have you found this content?