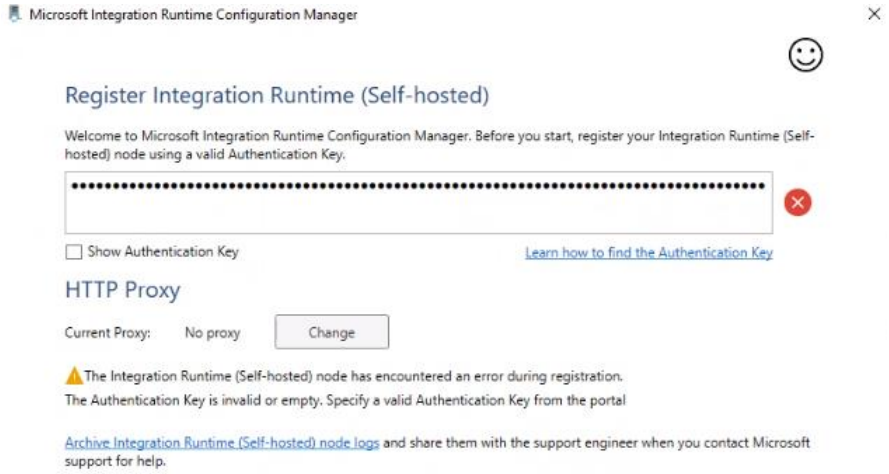
"The Authentication key is invalid or empty" after disabling public network access for Data Factory

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

Contents

Issue

Self Hosted integration runtime throwing error "The Authentication key is invalid or empty" after disabling public network access for Data Factory.



Root Cause

Disabling public connectivity and establishing a private endpoint. But it still doesn't seem to be connecting, most likely the DNS resolution issue. The DNS name of ADF is resolving to a public IP even after created a DNS record in Azure Private Link.

Steps to verify the cause

1. Check whether the Customer has created Azure VM in the same VNET as Data Factory private endpoint.

2. a) Psping or Ping from Azure VM to Data Factory FQDN it resolved to a public IP. Command: - psping.exe <dataFactoryName>.<region>.datafactory.azure.net:443 (Replace ADF name and region)

   Note: - 443 is not required but PSPING command requires a port to be specified.

   Or

   b) Command: - ping <dataFactoryName>.<region>.datafactory.azure.net (Replace ADF name and region)

3. Both the above commands would resolve to a ADF public IP based on region specified.

```
C:\Users\M9600211\Downloads\PSTools>psping.exe adf-pe[redacted].net:443

PsPing v2.10 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

TCP connect to [redacted]443:
5 iterations (warmup 1) ping test:
Connecting to [redacted] (warmup): from 10.0.0.119:65216: 84.88ms
Connecting to [redacted]: from [redacted] 82.67ms
Connecting to [redacted]: from [redacted] 81.27ms
Connecting to [redacted]: from [redacted] 82.82ms
Connecting to [redacted]: from [redacted] 78.99ms

TCP connect statistics for 20.42.64.0:443:
  Sent = 4, Received = 4, Lost = 0 (0% loss),
  Minimum = 78.99ms, Maximum = 82.82ms, Average = 81.44ms
```

Resolution

(before using the resolution, kindly perform the step to verify if the cause)

If the response of above command resolved network connection to a public IP and not a private IP as below (xx.xx.xx.0 is a public IP, verified from "Service Tags" file for public cloud)

```
C:\Users\M9600211\Downloads\PSTools>p[redacted]t.eastus.datafactory.azure.net:443

PsPing v2.10 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

TCP connect to [redacted]:443:
```

Then ask customer to follow the document [Azure Private Link for Azure Data Factory] to configure the private DNS zone/server to resolve DF FQDN to private IP address. This is same for all service which support private link.

If customer does not want to configure the private DNS zone/server as public document required, then this is temp workaroud for customer. However, we recommend our customer to leverage the custom DNS as long term solution.

1. Change the host file in windows and map private IP (ADF Private endpoint) to ADF FQDN
   - In Azure VM, navigate to path "C:\Windows\System32\drivers\etc\hosts" and open the host file in a text editor like Notepad (ADMIN MODE REQUIRED).
   - Add a line at the end as shown below, where "10.3.0.9" is private IP i.e. ADF Private endpoint and "xxx-xx-test.eastus.datafactory.azure.net" is FQDN for ADF. Save and close the host file after making the above changes.

*hosts - Notepad

File Edit Format View Help

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      [redacted]      rhino.acme.com          # source server
#      [redacted]      x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       [redacted]0.0.1       localhost
#       ::1             localhost
      [redacted]      [redacted].datafactory.azure.net
```

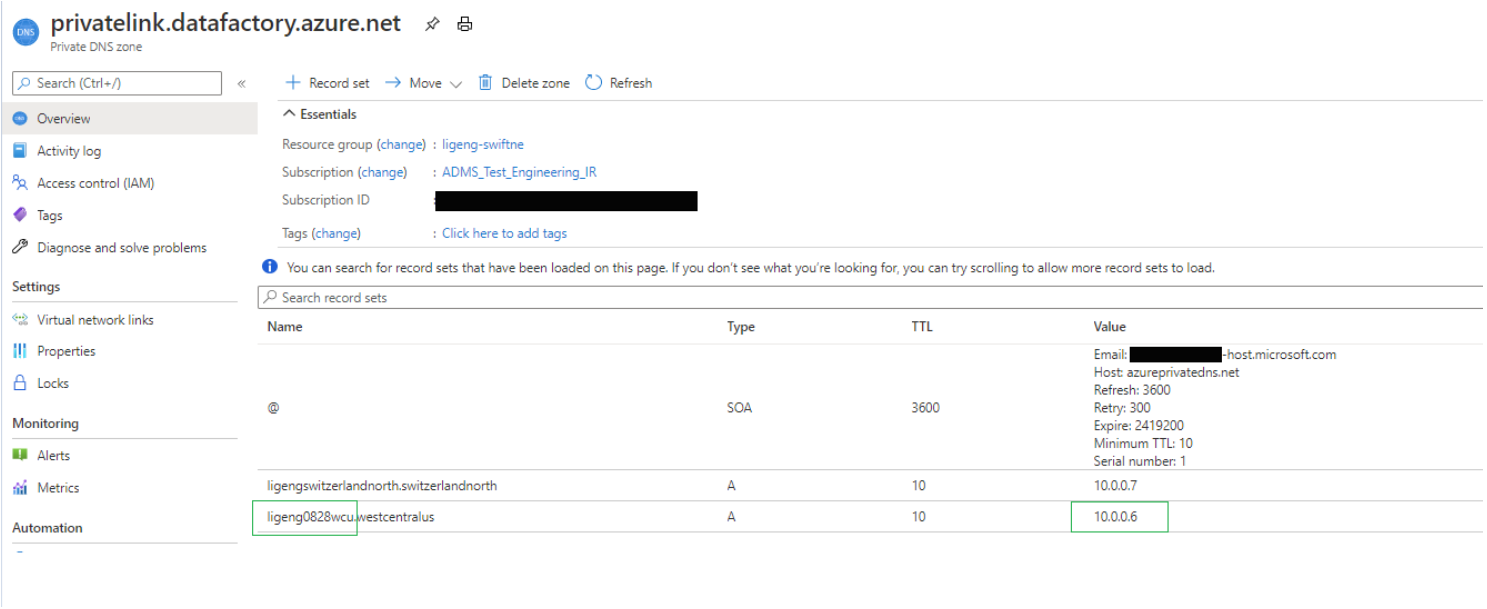
2. Rerun the same commands given above and the response will contain a private IP i.e. customer's ADF Private endpoint.

```
C:\Users\M9600211\Downloads\PSTools>psping.exe [redacted] s.datafactory.azure.net:443

PsPing v2.10 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

TCP connect to [redacted]
```

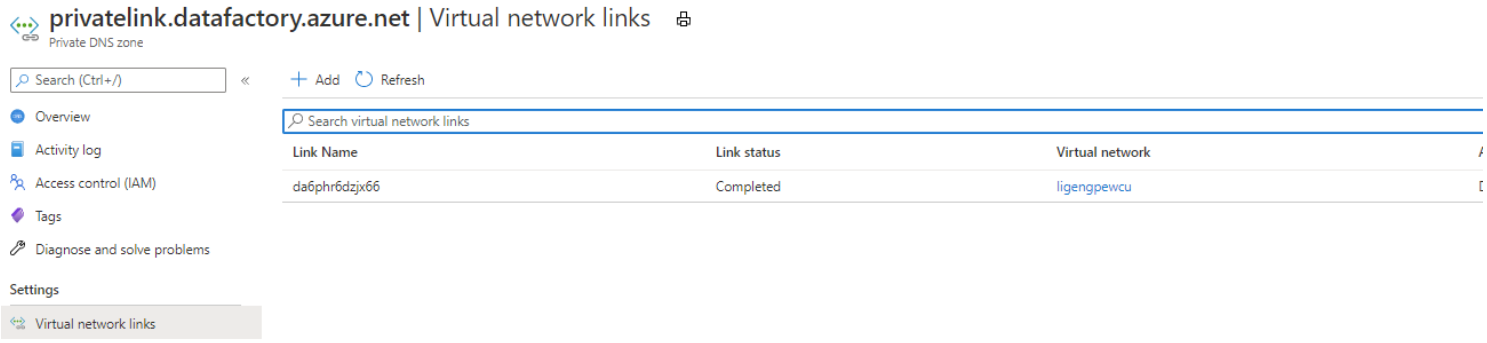
3. Try registering the SHIR again and it should succeed.

How to find private IP for ADF private endpoint and validate private DNS zone is configured,

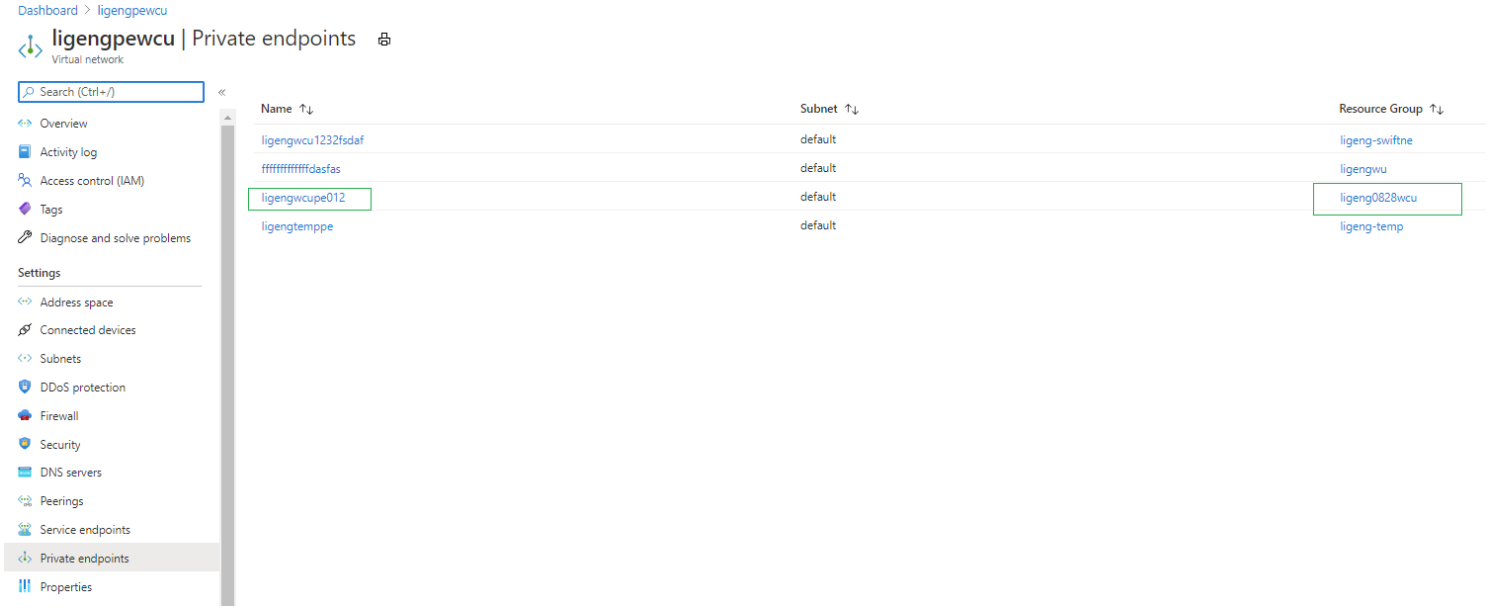
1. In Azure portal under the resource group where customer created ADF PE, a private link resource will be created with name "privatelink.datafactory.azure.net" which contains private IP with respective ADF FQDN



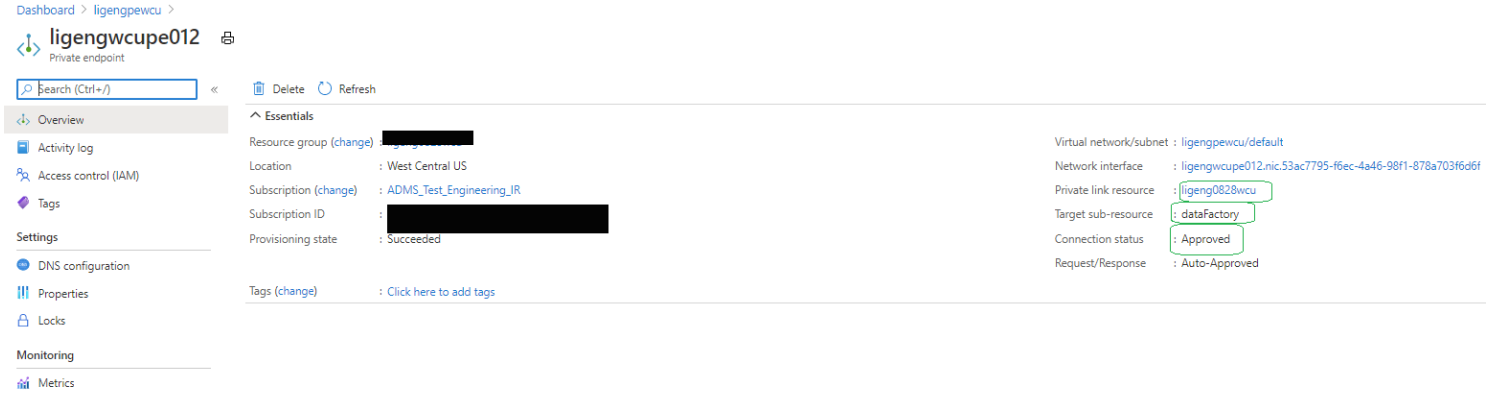
2. In Virtual network links page, make sure Virtual Network used by private endpoint is added,



3. Click the linked under Virtual Network, and click Private Endpoints to see all PE, click the PE used by specified DF



4. You should see below information,



If user have configured private DNS zone and the DF FQDN is still not resolved to private IP address, work with network team on this.

Reference

120101424005318