Troubleshoot Azure Active Directory for PostgreSQL flexible server

Last updated by | Hamza Aqel | Mar 31, 2023 at 4:54 AM PDT

Contents

Setup

This document will guide you how to setup AAD on Azure database for flexible server.

Prerequisites:

Configure network requirements

Azure AD is a multitenant application. It requires outbound connectivity to perform certain operations, like adding Azure AD admin groups. Additionally, you need network rules for Azure AD connectivity to work, depending on your network topology:

- Public access (allowed IP addresses): No extra network rules are required.
- Private access (virtual network integration):

You need an outbound network security group (NSG) rule to allow virtual network traffic to only reach the AzureActiveDirectory service tag. Optionally, if you're using a proxy, you can add a new firewall rule to allow HTTP/S traffic to reach only the AzureActiveDirectory service tag.

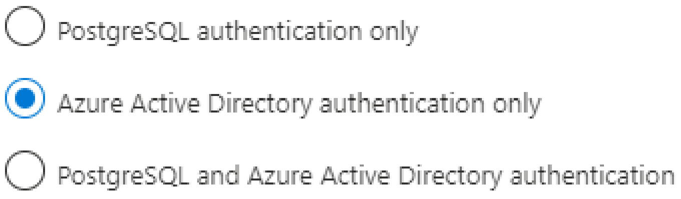
At the end of this TSG, you will see a sample of the above configuration in ASC.

Validating if flexible server has AAD enabled.

Notes:

```
There can be cases where we do not have access to customer's tenant but AAD remains enabled (aad_auth_tenant_i
SO please make sure customer run this command:
New-AzureADServicePrincipal -Appld 5657e26c-cc92-45d9-bc47-9da6cfdb4ed9
```

AAD enabled only

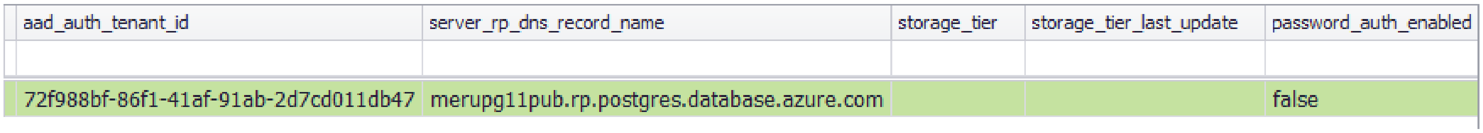


○ PostgreSQL authentication only

● Azure Active Directory authentication only

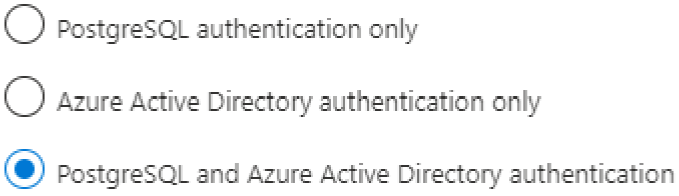
○ PostgreSQL and Azure Active Directory authentication

To validate if server has AAD auth is enabled only and no PostgreSQL authentication enabled, in XTS view orcasbreadth\orcasbreadth servers.xts, value of aad_auth_tenant_id should not be null and password authentication should be false:



aad_auth_tenant_id	server_rp_dns_record_name	storage_tier	storage_tier_last_update	password_auth_enabled
72f988bf-86f1-41af-91ab-2d7cd011db47	merupg11pub.rp.postgres.database.azure.com			false

AAD and PostgreSQL authentication:

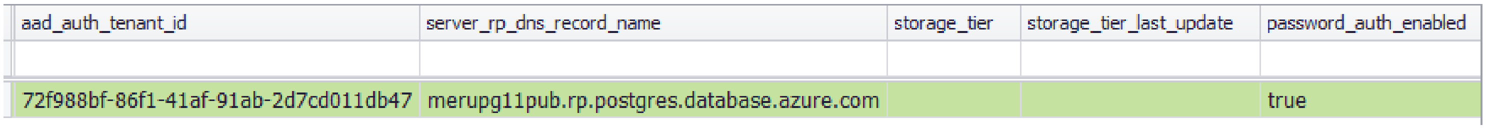


○ PostgreSQL authentication only

○ Azure Active Directory authentication only

● PostgreSQL and Azure Active Directory authentication

To validate if server has AAD and PostgreSQL authentication are enabled, in XTS view orcasbreadth\orcasbreadth servers.xts, value of aad_auth_tenant_id should not be null and password authentication should be true:



aad_auth_tenant_id	server_rp_dns_record_name	storage_tier	storage_tier_last_update	password_auth_enabled
72f988bf-86f1-41af-91ab-2d7cd011db47	merupg11pub.rp.postgres.database.azure.com			true

Kusto

Deployment Troubleshooting - Creating Admin/Principle

- Get failed deployment correlationID , then run:

```
HttpIncomingRequests
| where correlationId == 'CORRELATIONID'
| where targetUri contains "azureAsyncOperation"
| project targetUri, RoleLocation
```

After getting requestID (Asyncoperation), check OrcasbreadthRp for any errors:

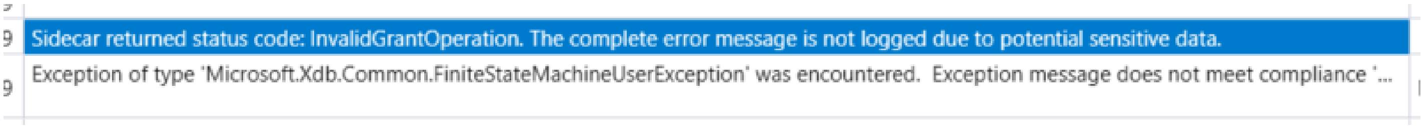
in our example above, asyncID was '36a16853-de89-4f97-9a53-06565276a300':

```
 https://management.azure.com/subscriptions/1138e852-151e-49b4-a635-
435c9b07a189/providers/Microsoft.DBforPostgreSQL/locations/eastus/azureAsyncOperation/36a16853-de89-4f97-
9a53-06565276a300?api-version=2022-03-08-privatepreview
```

- Check Message output for request_id above in MonOrcasBreadthRp, example below:

```
MonOrcasBreadthRp
| where request_id  == toupper('36A16853-DE89-4F97-9A53-06565276A300')
| where TIMESTAMP >= start_time and TIMESTAMP <= end_time
| project TIMESTAMP, message, stack_trace ,state, old_state, new_state, operation_parameters
| order by TIMESTAMP asc
```

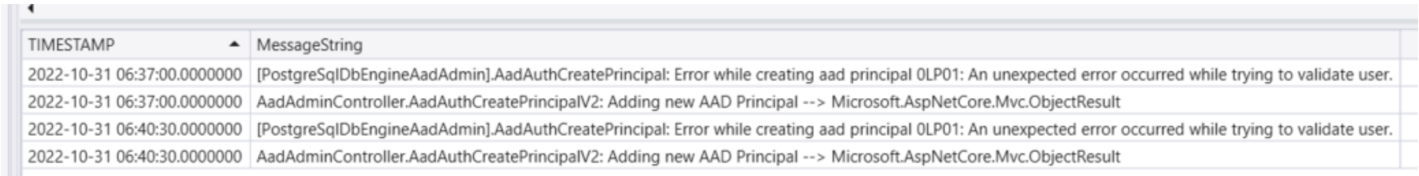
If message is not clear or you had a non-clear error, please check below tables:



```
9 Sidecar returned status code: InvalidGrantOperation. The complete error message is not logged due to potential sensitive data.
9 Exception of type 'Microsoft.Xdb.Common.FiniteStateMachineUserException' was encountered.  Exception message does not meet compliance '...
```

- Check OBvmagentsidecarpgsql:

```
OBvmagentsidecarpgsql
| where LogicalServerName == 'postgrytest'
| where TIMESTAMP >= start_time and TIMESTAMP <= end_time
| where MessageString contains "AadAuthCreatePrincipal"
| project  TIMESTAMP,  MessageString
```



TIMESTAMP	MessageString
2022-10-31 06:37:00.0000000	[PostgreSqlDbEngineAadAdmin].AadAuthCreatePrincipal: Error while creating aad principal 0LP01: An unexpected error occurred while trying to validate user.
2022-10-31 06:37:00.0000000	AadAdminController.AadAuthCreatePrincipalV2: Adding new AAD Principal --> Microsoft.AspNetCore.Mvc.ObjectResult
2022-10-31 06:40:30.0000000	[PostgreSqlDbEngineAadAdmin].AadAuthCreatePrincipal: Error while creating aad principal 0LP01: An unexpected error occurred while trying to validate user.
2022-10-31 06:40:30.0000000	AadAdminController.AadAuthCreatePrincipalV2: Adding new AAD Principal --> Microsoft.AspNetCore.Mvc.ObjectResult

If error similar to below was raised

Scenario 1: Failed to create Azure AD Principal. Reason - 0LP01: An unexpected error occurred while trying to validate user

Then the issue is one of the following issues: >

1. serviceprinciple was not added <**No need to run this from the customer side, after the GA this prerequisite has been removed** >

   ```
   Step 1: Connect-AzureAD -Tenantld <customer tenant id>
   Step 2: New-AzureADServicePrincipal -Appld 5657e26c-cc92-45d9-bc47-9da6cfdb4ed9
   ```

   You can validate if service principle was not added using above validations.

2. The token for the VM has expired, in this case, you need to refresh token. (**internal only**)

To check VM token expiry please run (Please note this will require running CAS commands):

```
 Invoke-OrcasBreadthExecuteScriptWithRunCommand -OrcasInstanceId 11111111-1111-1111-1111-111111111111 -
AzureVmRunCommandScriptName "cat_050_aad_parameters_conf"
```

```
 pgaadauth.graph_access_token_expires_on = '2022-10-21_08-27-34-683' # Saved on: 2022-10-20_08-27-35-863
```

If pgaadauth.graph_access_token_expires_on was less than today then please run:

```
 Set-AadGraphAccessTokenOnVm -CustomerSubscriptionId 00000000-0000-0000-0000-000000000000 -
CustomerResourceGroup rg_name -ServerName server_name -UpdateTokenViaRunCommand $true
```

Note

```
 If you have no permissions to execute above please contact EEE
```

Scenario 2: Error while creating aad principal Internal server error occured ... Timeout during reading attempt

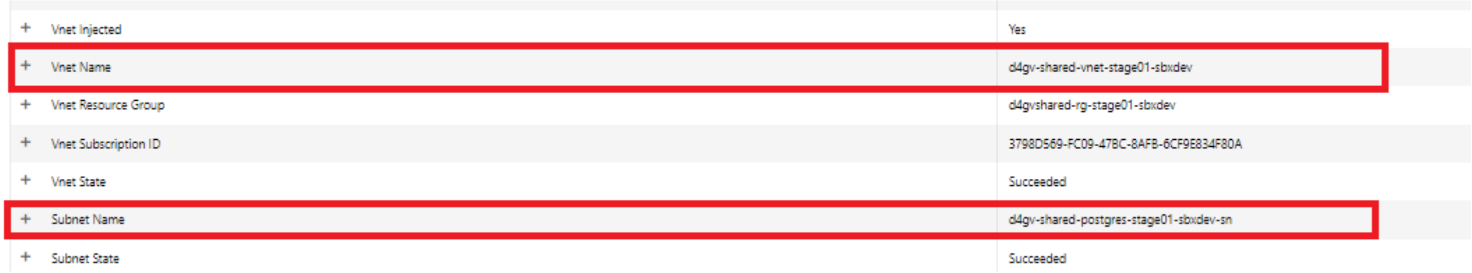
```
OBvmagentsidecarpgsql
| where LogicalServerName == "pgflexservername"
| where TIMESTAMP >= start_time and TIMESTAMP <= end_time
| where MessageString contains "AadAuthCreatePrincipal"
| project TIMESTAMP,MessageString
```

```
[PostgreSqlDbEngineAadAdmin].AadAuthCreatePrincipal: Error while creating aad principal Internal server error
 ---> Npgsql.NpgsqlException (0x80004005): Exception while reading from stream
 ---> System.TimeoutException: Timeout during reading attempt
   at Npgsql.NpgsqlConnector.<ReadMessage>g__ReadMessageLong|194_0(NpgsqlConnector connector, Boolean async, D
   at Npgsql.NpgsqlDataReader.NextResult(Boolean async, Boolean isConsuming, CancellationToken cancellationTok
   at Npgsql.NpgsqlCommand.ExecuteReader(CommandBehavior behavior, Boolean async, CancellationToken cancellati
   at Npgsql.NpgsqlCommand.ExecuteReader(CommandBehavior behavior, Boolean async, CancellationToken cancellati
   at Npgsql.NpgsqlCommand.ExecuteNonQuery(Boolean async, CancellationToken cancellationToken)
   at VmAgent.SideCar.Postgres.Services.PostgresDataHandler.ExecuteNonQueryWithPiiContent(PostgresConnectOptio
   --- End of inner exception stack trace ---
   at System.Threading.Tasks.Task.Wait(Int32 millisecondsTimeout, CancellationToken cancellationToken)
   at System.Threading.Tasks.Task.Wait()
   at VmAgent.SideCar.Postgres.Services.PostgreSqlDbEngineAadAdmin.AadAuthCreatePrincipal(AadAuthCreatePrincip
```

Such errors are mostly happening in servers with Private access (virtual network integration), make sure:

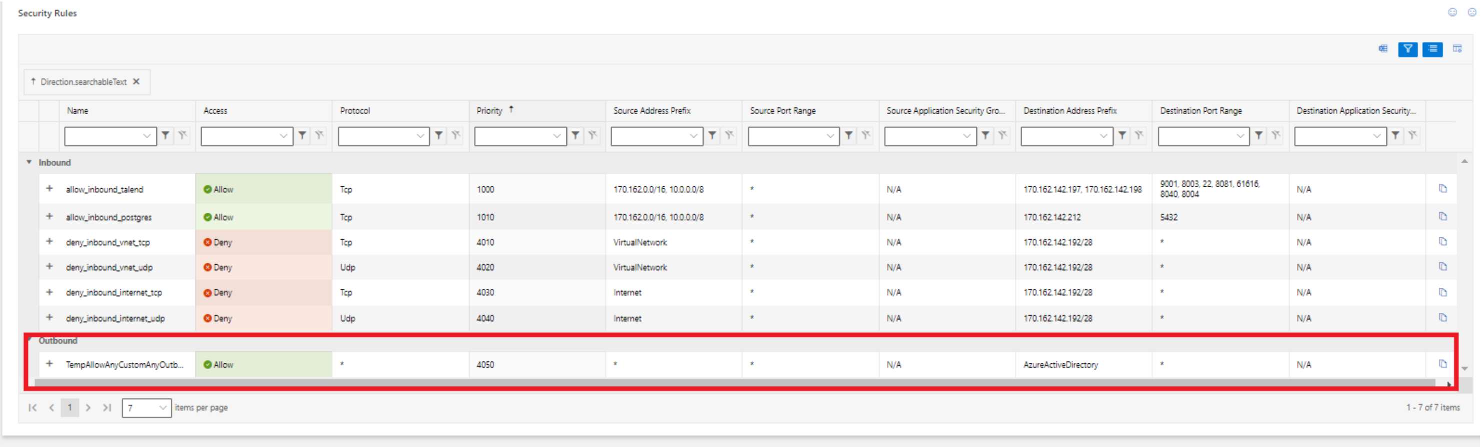
- If the customer has NSG rules, make sure an outbound network security group (NSG) rule exists to allow virtual network traffic to only reach the AzureActiveDirectory service tag:

Go to the Vnet/subnet that is used for that server, you can find them in ASC - properties tab:



+ Vnet Injected	Yes
+ Vnet Name	d4gv-shared-vnet-stage01-sbxdev
+ Vnet Resource Group	d4gvshared-rg-stage01-sbxdev
+ Vnet Subscription ID	3798D569-FC09-47BC-8AFB-6CF9E834F80A
+ Vnet State	Succeeded
+ Subnet Name	d4gv-shared-postgres-stage01-sbxdev-sn
+ Subnet State	Succeeded

and go to the subnet:



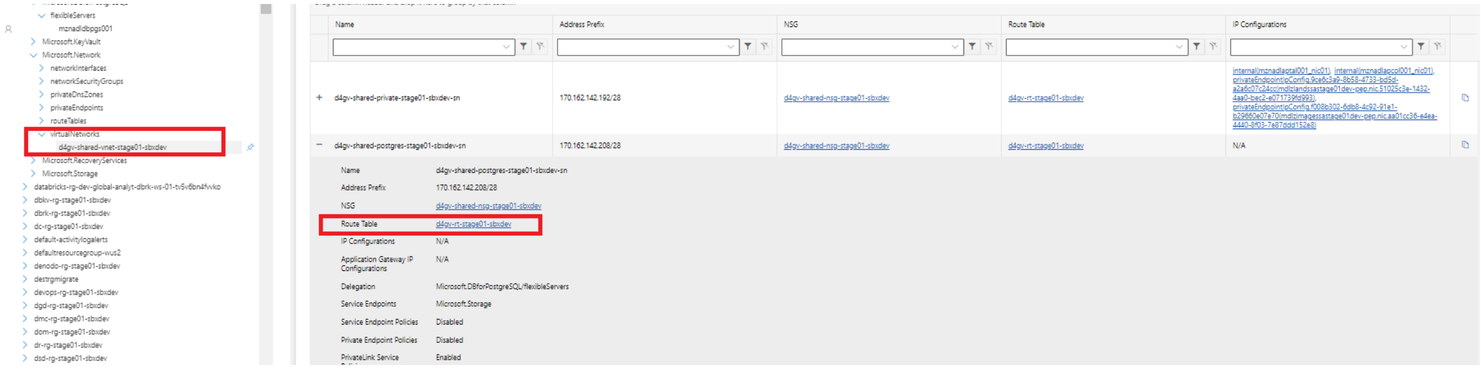
Security Rules

↑ Direction.searchableText ✕

Name	Access	Protocol	Priority ↑	Source Address Prefix	Source Port Range	Source Application Security Gro...	Destination Address Prefix	Destination Port Range	Destination Application Security...
Inbound									
allow_inbound_talend	Allow	Tcp	1000	170.162.0.0/16, 10.0.0.0/8	*	N/A	170.162.142.197, 170.162.142.198	9001, 8003, 22, 8081, 61616, 8040, 8004	N/A
allow_inbound_postgres	Allow	Tcp	1010	170.162.0.0/16, 10.0.0.0/8	*	N/A	170.162.142.212	5432	N/A
deny_inbound_vnet_tcp	Deny	Tcp	4010	VirtualNetwork	*	N/A	170.162.142.192/28	*	N/A
deny_inbound_vnet_udp	Deny	Udp	4020	VirtualNetwork	*	N/A	170.162.142.192/28	*	N/A
deny_inbound_internet_tcp	Deny	Tcp	4030	Internet	*	N/A	170.162.142.192/28	*	N/A
deny_inbound_internet_udp	Deny	Udp	4040	Internet	*	N/A	170.162.142.192/28	*	N/A
Outbound									
TempAllowAnyCustomAnyOutb...	Allow	*	4050	*	*	N/A	AzureActiveDirectory	*	N/A

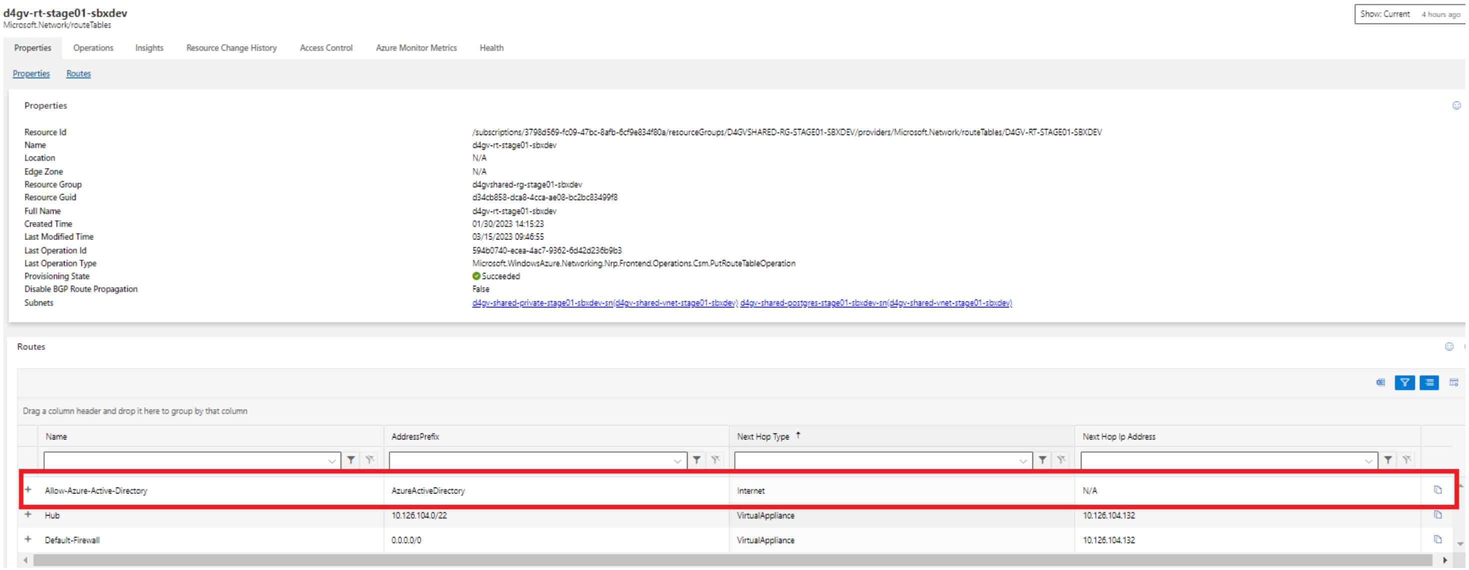
7 items per page 1 - 7 of 7 items

- Some customers might have some route tables :



Name	Address Prefix	NSG	Route Table	IP Configurations
d4gv-shared-private-stage01-sbxdev-sn	170.162.142.192/28	d4gv-shared-nsg-stage01-sbxdev	d4gv-rt-stage01-sbxdev	internal(mznadlaptal001_nic01), internal(mznadlapcol001_nic01), privateEndpointIpConfig.9ce6c3a9-8b58-4733-bd5d-a2a6c07c24cc(mdlzlandssastage01dev-pep.nic.51025c3e-1432-4aa0-bec2-e071739fd993), privateEndpointIpConfig.f008b302-6db8-4c92-91e1-b29660e07e70(mdlzimagessastage01dev-pep.nic.aa01cc36-e4ea-4440-8f03-7e87ddd152e8)
d4gv-shared-postgres-stage01-sbxdev-sn	170.162.142.208/28	d4gv-shared-nsg-stage01-sbxdev	d4gv-rt-stage01-sbxdev	N/A

Name	d4gv-shared-postgres-stage01-sbxdev-sn
Address Prefix	170.162.142.208/28
NSG	d4gv-shared-nsg-stage01-sbxdev
Route Table	d4gv-rt-stage01-sbxdev
IP Configurations	N/A
Application Gateway IP Configurations	N/A
Delegation	Microsoft.DBforPostgreSQL/flexibleServers
Service Endpoints	Microsoft.Storage
Service Endpoint Policies	Disabled
Private Endpoint Policies	Disabled
PrivateLink Service	Enabled



d4gv-rt-stage01-sbxdev
Microsoft.Network/routeTables

Properties

Resource Id	/subscriptions/3798d569-fc09-47bc-8afb-6cf9e834f80a/resourceGroups/D4GVSHARED-RG-STAGE01-SBXDEV/providers/Microsoft.Network/routeTables/D4GV-RT-STAGE01-SBXDEV
Name	d4gv-rt-stage01-sbxdev
Location	N/A
Edge Zone	N/A
Resource Group	d4gvshared-rg-stage01-sbxdev
Resource Guid	d34cb858-dca8-4cca-ae08-bc2bc83499f8
Full Name	d4gv-rt-stage01-sbxdev
Created Time	01/30/2023 14:15:23
Last Modified Time	03/15/2023 09:46:55
Last Operation Id	594b0740-ecea-4ac7-9362-6d42d236b9b3
Last Operation Type	Microsoft.WindowsAzure.Networking.Nrp.Frontend.Operations.Csm.PutRouteTableOperation
Provisioning State	Succeeded
Disable BGP Route Propagation	False
Subnets	d4gv-shared-private-stage01-sbxdev-sn(d4gv-shared-vnet-stage01-sbxdev) d4gv-shared-postgres-stage01-sbxdev-sn(d4gv-shared-vnet-stage01-sbxdev)

Routes

Drag a column header and drop it here to group by that column

Name	AddressPrefix	Next Hop Type ↑	Next Hop Ip Address
Allow-Azure-Active-Directory	AzureActiveDirectory	Internet	N/A
Hub	10.126.104.0/22	VirtualAppliance	10.126.104.132
Default-Firewall	0.0.0.0/0	VirtualAppliance	10.126.104.132

To resolve the problem customer should either:

Option 1. Create a Route table rule with destination service tag "AzureActiveDirectory" and next hop "Internet" as in the above example.

Option 2. Configure your Firewall deployment to allow traffic to MS Graph API. For Azure Firewall, that would be using the same "AzureActiveDirectory" service tag.

Authentication troubleshooting

For now Monpglogs will show password failure but no AAD specific errors.
All messages are logged to PII tables due to security reasons, PG are looking into this to see if they can change anything, workitem ↗.