

# HA Provisioning failed - NSG Rules

Last updated by | Hamza Aqel | Oct 26, 2022 at 2:33 AM PDT

High availability Features of Azure Database for PostgreSQL - Flexible Server require ability to send\receive traffic to destination ports 5432, 6432 within Azure virtual network subnet where Azure Database for PostgreSQL - Flexible Server is deployed , as well as to Azure storage for log archival. If you create Network Security Groups (NSG) to deny traffic flow to or from your Azure Database for PostgreSQL - Flexible Server within the subnet where its deployed, please make sure to allow traffic to destination ports 5432 and 6432 within the subnet, and also to Azure storage by using service tag Azure Storage as a destination

So if the customer has NSG rule defined to allow the traffic from certain IP addresses , make sure to include allow subnet IP range in PostgreSQL server's inbound NSG rules and try again. Below is the recommened NSG setup and how it should looks like:

Inbound:

- delegated subnet , any port <-> delegated subnet , port 5432,6432

Outbound:

- delegated subnet , any port <-> delegated subnet , port 5432,6432

- delegated subnet , any port <-> azure storage service tag, port 443, port 80

Inbound Security Rules						
100	Port 8080	22,6432	Any	92.253.31.218	Any	✓ Allow
110	AllowCidrBlockCustom5432...	5432,6432	Any	10.2.1.0/24	10.2.1.0/24	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny
Outbound Security Rules						
120	AllowCidrBlockCustom5432...	5432,6432	TCP	10.2.1.0/24	10.2.1.0/24	✓ Allow
121	StorageRule	80,443	Any	10.2.1.0/24	Storage	✓ Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow

For failed HA provision PG flex servers , you can use the below TSG to check whether the customer subnet has NSG conflict or not :

From ASC Properties -- > Server Info , get the vnet integrated name:

+	Paired Region	NORTHEUROPE
+	Cluster Short Name	ProdWeu1a
+	Virtual Machine Name	d78f7cb0f4fd
+	Virtual Machine ID	[REDACTED]3A4CE
+	Virtual Machine State	Succeeded
+	Resource Uri	/subscriptions/[REDACTED]4b77ae49f05c/resourceGroups/HaqelResGrp/providers/Micros
+	Create Time	7/6/2021 10:42:57 PM
+	Microsoft Subscription Id	[REDACTED]b99BC59E6
+	Microsoft Management Service Cluster	tr1428.westeurope1-a.worker.database.windows.net
+	Vnet Injected	Yes
-	Vnet Name	haqelvnet1
	Property Name	Vnet Name
	Property Value	haqelvnet1
+	Vnet Resource Group	HaqelResGrp
+	Vnet Subscription ID	[REDACTED]9F05C
+	Vnet State	Succeeded
+	Subnet Name	default
+	Subnet State	Succeeded
+	Dns Name	
+	Private Dns Zone Name	
+	Is Customer Private Dns Zone	
+	BYOK	BYOK Not Attempted

Search in ASC explorer for that VNET name :

+

Add subscription

haqelvnet1

Completed loading live data for subscription 5198ed8e-c2e9-482d-ae9d-d58607fed53b

Show additional status

routeTables

serviceEndpointPolicies

virtualNetworks

appservice1

appservice2

australia1

australia2

azure\_mariadb\_vnet

bulkloadvnet1

dbipervnet

HaqelResGrp-vnet

HaqelResGrpVnet211

HaqelResGrpVnet344

HaqelResGrpVnet474

HaqelResGrpVnet546

HaqelResGrpVnet540

haqelvnet1

haqelvnet2

haqelvnet3

hmzpriv1

magenoapp2vnet

magento1vnet

magentoapp1vnet

magentoprxyvnet

magproxyvnet1

mustafaVNET

mustafavnet2

mustafavnet3

Microsoft.Network/virtualNetworks

Properties

Operations

Diagnostics

Connected Resources

Insights

Resource Change History

Access Control

Azure Monitor Metrics

Health

Properties

Subnets

Peerings

Properties

Resource Id

/subscriptions/[REDACTED]05c/resourceGroups/HAQELRESGRP/providers/Microsoft.Network/virtualNetworks/HAQELVNET1

Name

haqelvnet1

Location

westeurope

Edge Zone

N/A

Resource Group

HaqelResGrp

Resource Guid

198966c5-59a7-4c03-b375-bb92efc774ce

Full Name

haqelvnet1

Created Time

07/06/2021 22:31:39

Last Modified Time

07/06/2021 22:43:02

Last Operation Id

746f7513-bb2d-4334-9757-40597efc4b9c

Last Operation Type

Microsoft.WindowsAzure.Networking.Nrp.Frontend.Operations.Csm.PutSubnetOperation

Provisioning State

Succeeded

Address Prefixes

10.24.0.0/16

VnetId

198966c5-59a7-4c03-b375-bb92efc774ce

VNet Peerings

N/A

Contains Accelerated Networking VMs

N/A

Enable DDoS Protection

False

DDoS Protection Plan

N/A

DNS Servers

Default (Azure-Provided)

DNS Names

N/A

Allocation Committed IPs

N/A

Allocation Goal IPs

N/A

Previous Allocation Goals IPs

N/A

Go to subnet, and check the NSG Rules :

Subnets

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

Name	Address Prefix	NSG	Route Table	IP Configurations
default	10.24.0.0/24	<a href="#">hagelvmnet1-default-nsg</a>	N/A	N/A

1 - 1 of 1 items

Click on NSG name :

Security Rules

↑ Direction.searchableText

Name	Access	Protocol	Priority	Source Address Prefix	Source Port Range	Source Application S...	Destination Address ...	Destination Port Ran...	Destination Applicat...	
Inbound										
+ CASG-Rule-101	Allow	*	101	VirtualNetwork	*	N/A	*	*	N/A	
+ CASG-Rule-102	Allow	*	102	CorpNetPublic	*	N/A	*	*	N/A	
+ CASG-Rule-103	Allow	*	103	CorpNetSaw	*	N/A	*	*	N/A	
+ CASG-Rule-104	Deny	*	104	Internet	*	N/A	*	13, 17, 19, 22, 23, 53, 69, 111, 119, 123, 135, 137, 138, 139, 161, 162, 389, 445, 512, 514, 593, 636, 873, 1433, 1434, 1900, 2049, 2301, 2381, 3268, 3306, 3389, 4333, 5353, 5432, 5800, 5900, 5985, 5986, 6379, 7000, 7001, 7199, 9042, 9160, 9300, 11211, 16379, 26379, 27017	N/A	

1 - 4 of 4 items

check the Security Rules , if the customer define any rules to allow traffic from certain IP addresses for this subnet , please recommend the customer to add Inbound/Outbound rules for POstgreSQL ports 5432 and 6432 , for example :

3014	Allow_PostgreSQL_to_PostgreSQL	5432,6432	TCP	10.129.140.0/24	10.129.140.0/24	Allow
------	--------------------------------	-----------	-----	-----------------	-----------------	-------

but on the above case here , no need to add as there is no rules defined for any IP addresses

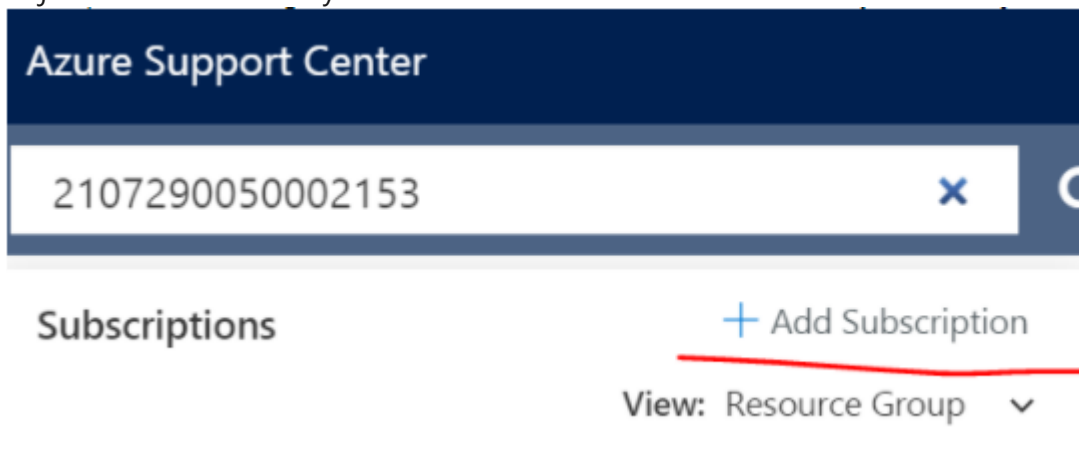
Or you can use the below alternative way to get the same information above, and especially if the server was dropped :

1. open ASC for this Ticket .
2. Click on "Resource Explorer" from ASC. This will load the server details.
3. Run the below query in orcasbreadth\orcasbreadth-adhocquery.xts.

```
select vnet.network_name, vnet.delegated_virtual_network_subscription_id, vnet.delegated_virtual_network_resou
from [dbo].[entity_delegated_virtual_network] vnet, [dbo].[entity_delegated_subnet] subnet, [dbo].[entity_dnc_
where vnet.id = subnet.delegated_virtual_network_entity_id
and subnet.id = nc.delegated_subnet_entity_id
and nc.orcas_instance_id = sr.orcas_instance_id
and sr.server_name = '<server_name>';
```

If above doesn't return anything, which can happen in case the server is already dropped, go to orcasbreadth\orcasbreadth crud.xts view and find the UpsertServerManagementOperationV2 operation based on your server name, then select Operational Parameters tab from the bottom panel. All the parameters needed in step 4 and step 5 can be located here.

4. Check if the delegated\_virtual\_network\_subscription\_id is the same as the server subscription in ASC. If it's the same, use the resource group and VNET name info from step 3 to locate the VNET from ASC. Otherwise add the VNET subscription in ASC using below link, then locate the VNET in the same way. Put in the jurisdiction reasonably.



5. Once you find the VNET, go to the Subnet section, use the subnet name from step 3 to locate the subnet. You can view NSG rule from here. If there is NSG on this subnet, you should be able to click on it and review the detailed rules.

Subnets

Drag a column header and drop it here to group by that column				
Name	Address Prefix	NSG	Route Table	IP Configurations
aks-australiaeast-prod-bogong-k8s-service	172.16.16.0/20	N/A	N/A	N/A

1 - 1 of 1 items