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:

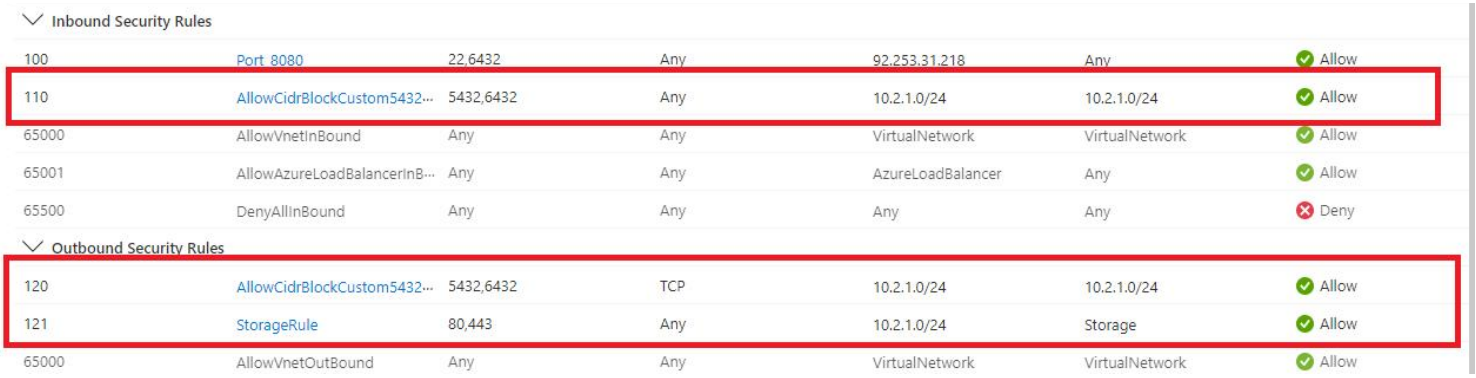
Inbound:

- 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

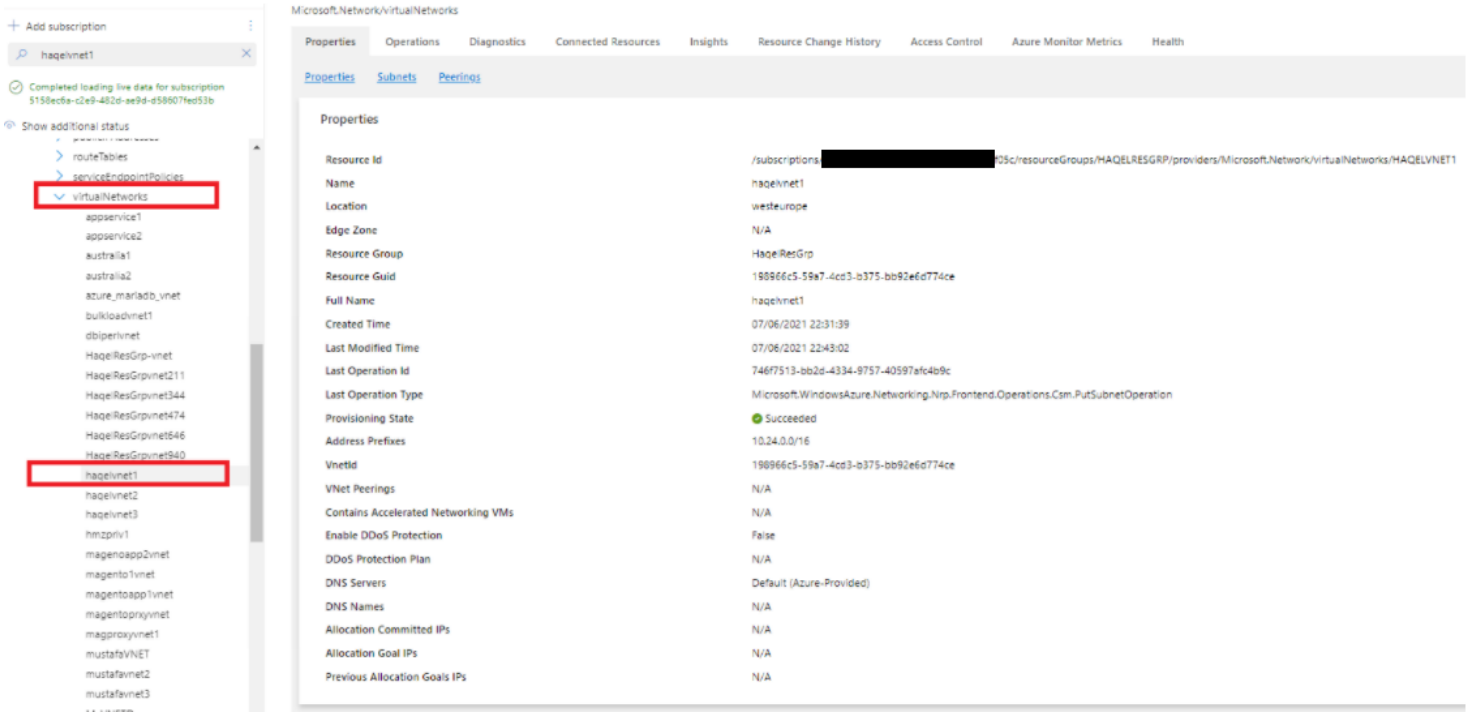
120	AllowCidrBlockCustom5432...	5432,6432	TCP	10.2.1.0/24	10.2.1.0/24	Allow
121	StorageRule	80,443	Any	10.2.1.0/24	Storage	Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow

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

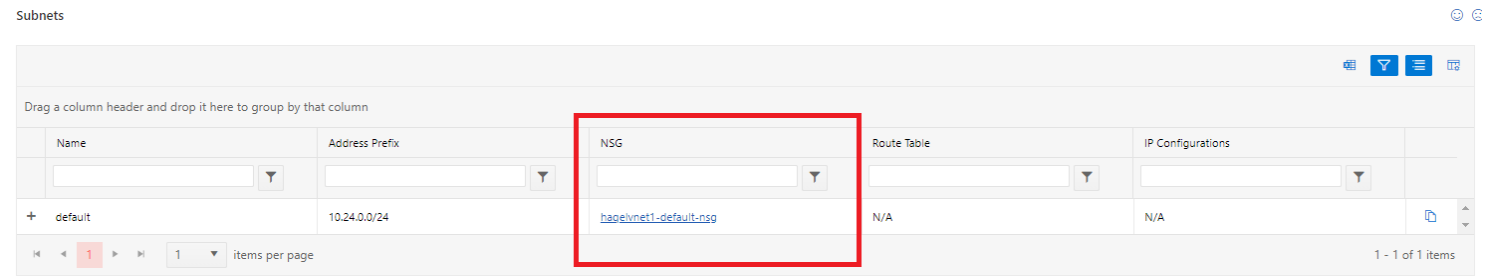
From ASC Properties -- > Server Info , get the vnet integrated name:

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
PropertyName: Vnet Name	
PropertyValue: haqelvnet1	
Vnet Resource Group	HaqelResGrp
Vnet Subscription ID	[redacted]49F05C
Vnet State	Succeeded
Subnet Name	default
Subnet State	Succeeded
Dns Name	
Private Dns Zone Name	
Is Customer Private Dns Zone	
BYOK	BYOK Not Attempted

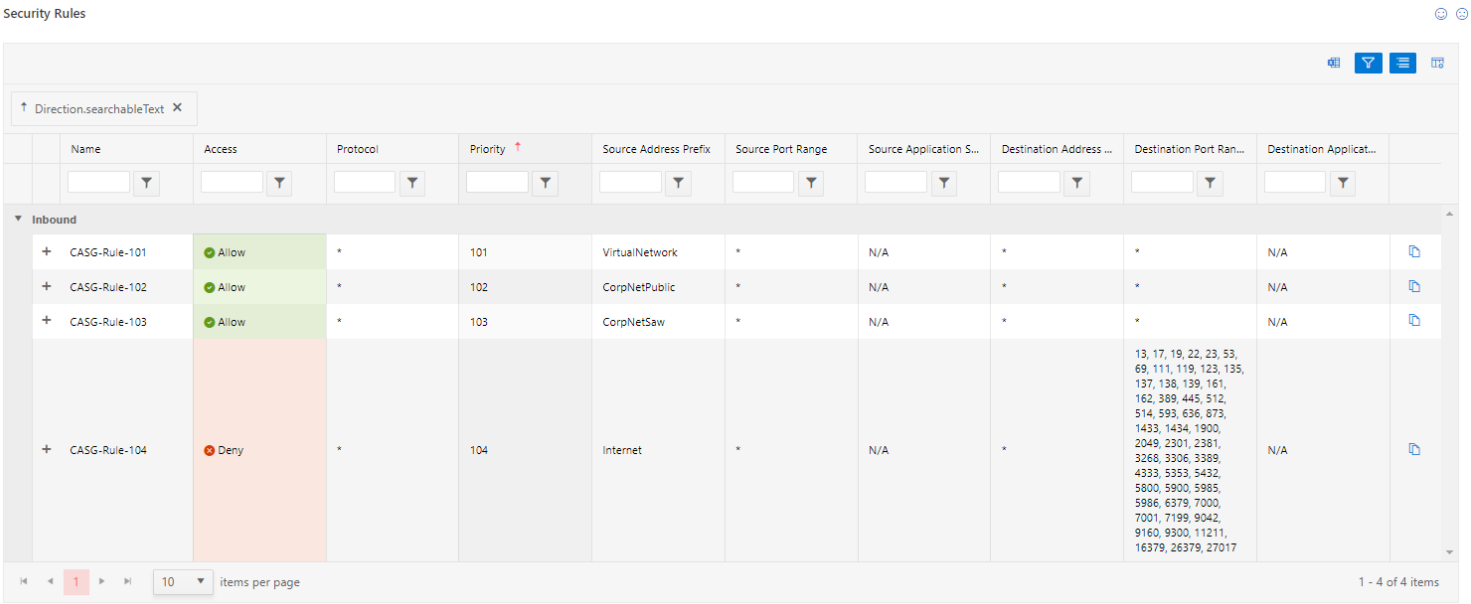
Search in ASC explorer for that VNET name :



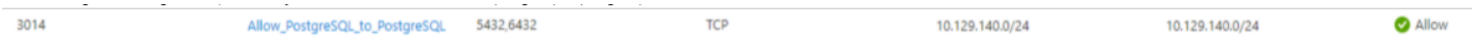
Go to subnet, and check the NSG Rules :



Click on NSG name :



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 :



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

---

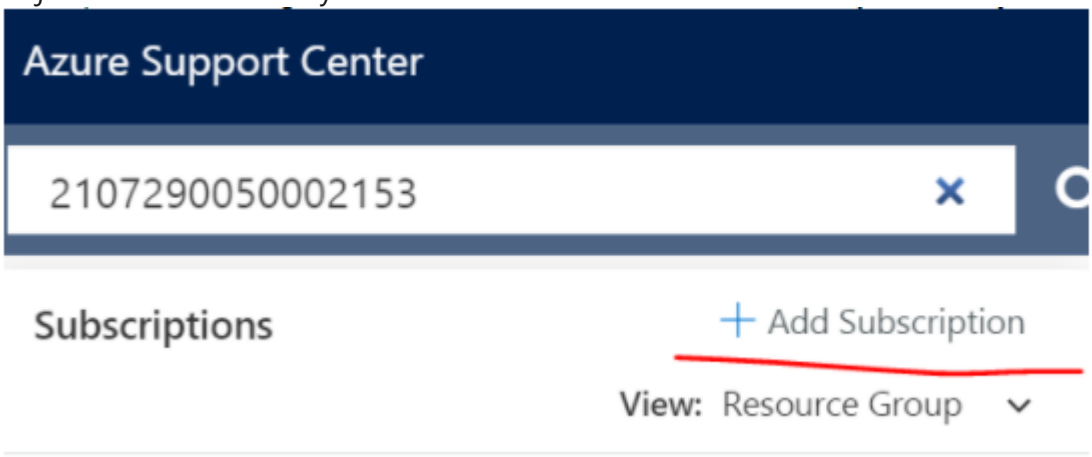
Or you can use the below alternative way to get the same information above, and especially if the server was dropped :

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-adhoccmsquery.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.