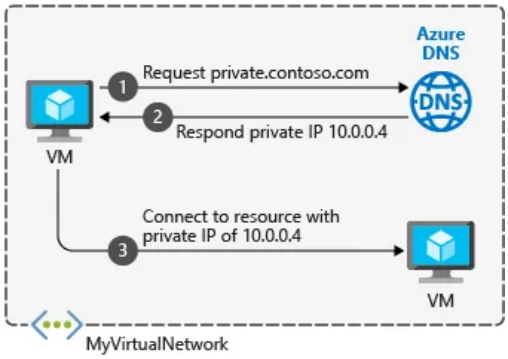
Architecture of Azure Private DNS and name lookup in Azure

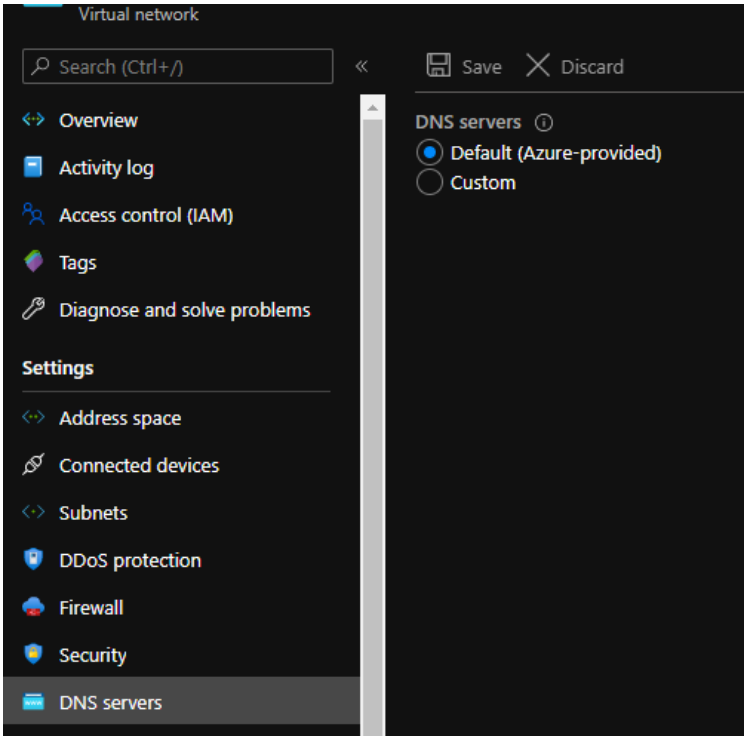
Posted by Marius Sandbu July 13, 2020 in Uncategorized



With the latest addition of DNS Proxy to Azure Firewall (https://docs.microsoft.com/en-us/azure/firewall/dns-settings) and looking at some of the questions I get on this blog I guess it was time to write a bit about how DNS lookup works within Microsoft Azure.

How does DNS lookup work within Microsoft Azure?

Azure provides internal name resolution for VMs and role instances (including app services) for all services that reside within a virtual network. When setting up a virtual network it will by default use the internal Azure DNS service.



Subscribe to msandbu.org via Email

Enter your email address to subscribe to this blog and receive notifications of new posts by email.

Join 452 other subscribers

Email Address

Subscribe

Recent Posts

Technology predictions for 2021

Troubleshoot Networking in Microsoft Azure

Migrate to WVD and Beyond

Microsoft Azure coming to Sweden and Denmark

What is AIOps and why should I care?

Now as you might know within each subnet Azure also reserves the first 4 IP addresses to Azure related services, so for instance if we have a 10.0.0.0/16 subnet the x.x.x.2, x.x.x.3: Is reserved by Azure to map the Azure DNS Server IPs to the VNet space.

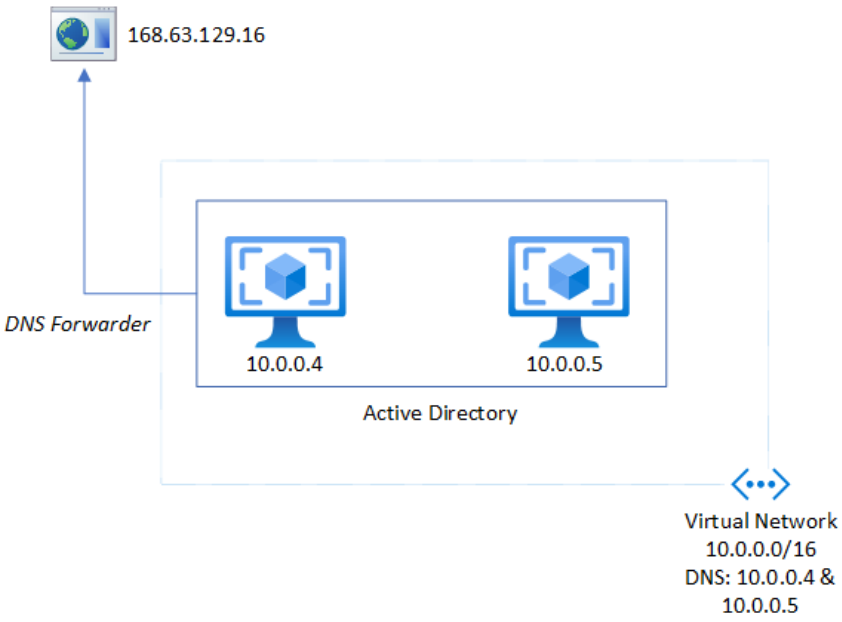
When you setup a virtual machine within this VNET it will automatically get assigned IP by a DHCP service and DNS lookup services by an internal IP address 168.63.129.16. This IP address is an internal VIP address by Microsoft (Which is only available internally from wtihin Azure) https://docs.microsoft.com/en-us/azure/virtual-network/what-is-ip-address-168-63-129-16 (*Traffic should not be blocked to this IP address, this address is static and will not change*)

You can also change the DNS Server scope on a virtual network, but this will not affect other virtual networks that are peered or otherwise connected to the virtual network using VPN or ExpressRoute.

When it comes to providing DNS Servces in Azure, there are a couple of options.

- **Azure built-in DNS (**Does not provide any ability to change or update record)
- **DNS Server running IaaS** (Provides full flexibility, but requires that you have virtual machines that running to deliver DNS services)
- **DNS Proxy** (Having a virtual machine or service which can provide DNS services for services in Azure but authoritative DNS servers are outside of Azure)
- **Azure DNS Private Zones** (An internal DNS Service in Azure which can provide DNS lookup within a virtual network, allows you to manage records in Azure)

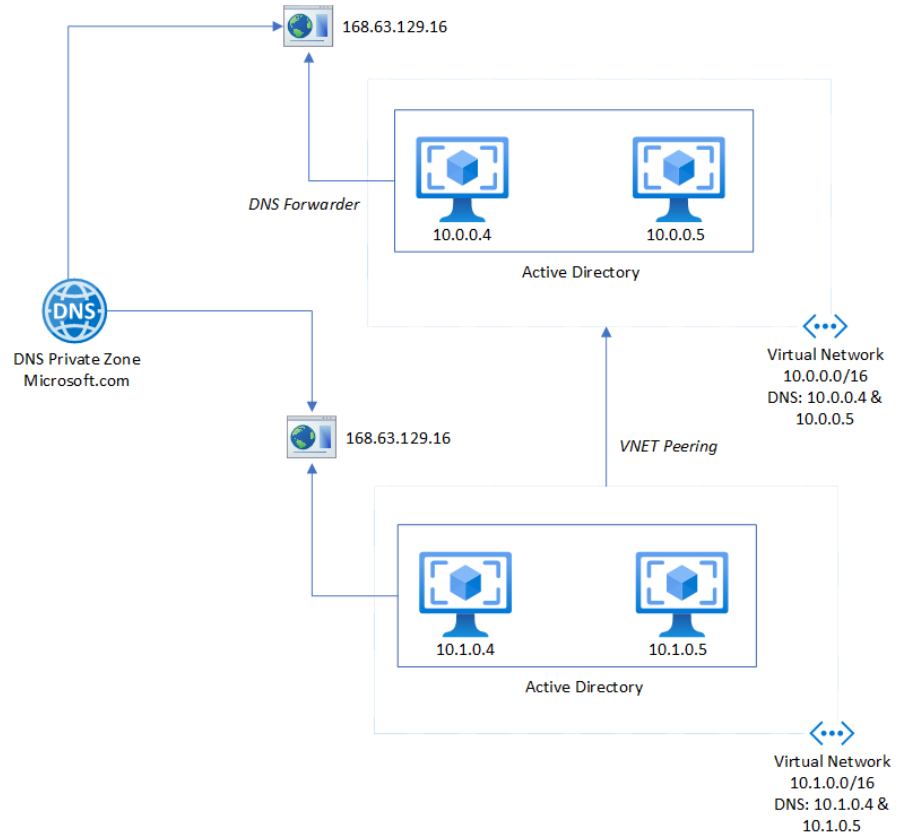
So for instance if you want to setup your own active directory domain within Azure also running DNS, you would need to setup those at DNS servers for the virtual network and then define 168.63.129.16 as a DNS forwarder to allow for external lookup outside of your local active directory domain.



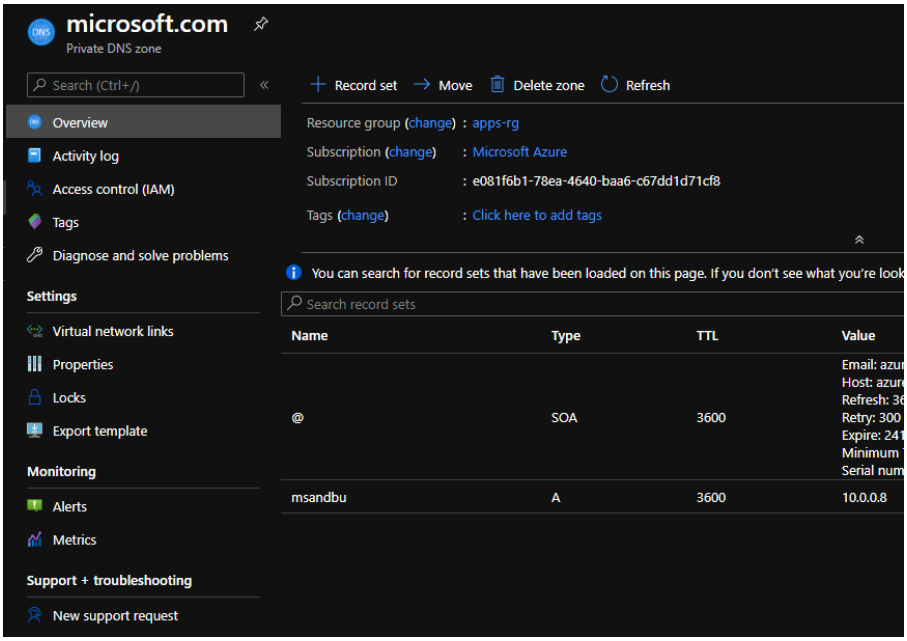
If you want to have the flexibility to create your own records but do not require/want an DNS servers you can use Azure DNS Private Zones, which essentially adds an DNS records on top of the regular Azure DNS service which is available on the same Virtual IP 168.63.129.16 which is also scoped on the VNET level, which means that DNS Private Zones are not supported across VNET Peering. However a DNS Private Zone can be linked to multiple

virtual network which allows you to provide the same DNS records across mulitple virtual networks.

Now since private DNS Zones are only available within a virtual network it means that you can define any type of DNS Zone and attach it to the virtual network. For instance you can use Microsoft.com as a DNS private Zone



Link it to a virtual network and use that for name resolution. If I add msandbu as an A record under microsoft.com and link this to a virtual network where DNS servers are setup using the default settings

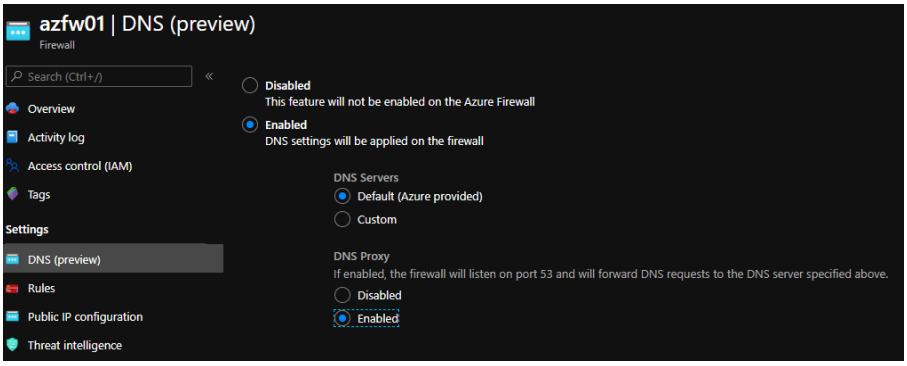


The VM and or service would send a DNS Query to the local VIP 168.63.129.16 and it would see which DNS Private Zones are linked to the virtual network and find the record

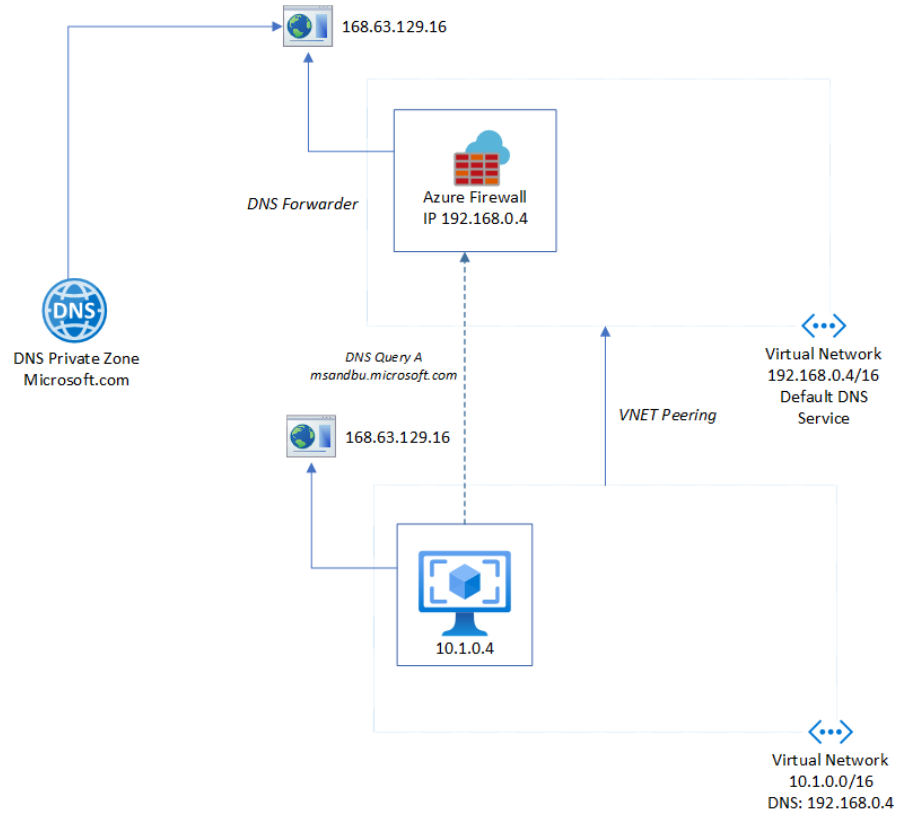
```
C:\Users\msandbu>nslookup msandbu.microsoft.com
Server:  UnKnown
Address:  168.63.129.16

Non-authoritative answer:
Name:    msandbu.microsoft.com
Address:  10.0.0.8


C:\Users\msandbu>
```

It should be noted that with DNS Private Zones are only available within a virtual network. So if you have a scenario where you have a hybrid network with resouces on-premises that would not be able to lookup resources in a Private DNS Zone directly. The only way that they would be able to lookup resources within a DNS Private Zone would be if used together with a DNS Proxy or that your authoritative DNS Servers are running in Azure which can communicate with 168.63.129.16. The same would apply to VNET Peering.

Now this is where the Azure Firewall DNS Proxy service comes in, since this allows your Azure Firewall to act as an DNS Proxy.



So to demonstrate how this would work. We have two virtual networks, where a DNS Private Zone is linked to one of my virtual networks. This virtual network has the native DNS service configured. We have another virtual network that is peered with the first one, by default VM's in VNET 2 are not able to resolve records on VNET1 because DNS Private Zones are not linked and not available across peered networks. This scenario would also apply for networks that are on-premises as well. Where the Azure Firewall IP can be a conditional forwarder to forward DNS requests to azure records.



In this scenario, the VM on 10.1.0.4 would send a DNS request to its defined DNS service which is the Azure Firewall 192.168.0.4 on the other site of the peered network, which would in turn send the DNS request to its local VIP where the DNS Private Zone is configured where the A record is configured

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : reddog.microsoft.com
   Link-local IPv6 Address . . . . . : fe80::215c:e717:b448:ab24%4
   IPv4 Address. . . . . . . . . . . : 10.1.0.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.0.1

C:\Users\msandbu>nslookup msandbu.microsoft.com
Server:  UnKnown
Address:  192.168.0.4

Non-authoritative answer:
Name:    msandbu.microsoft.com
Address:  10.0.0.8
```

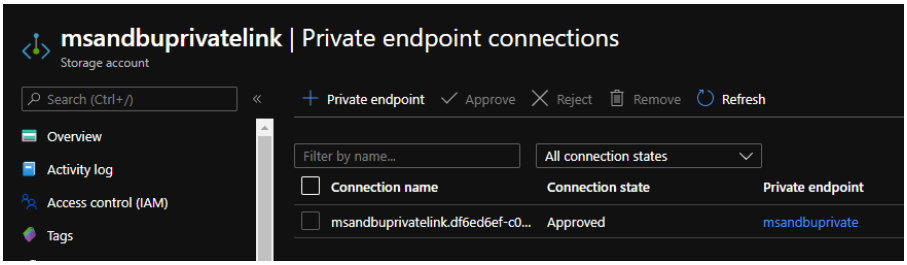
Private Link and Private Endpoints

Private Endpoints are essentially PaaS Services which are only available from within a virtual network. You can read more about them here –> https://docs.microsoft.com/en-us/azure/private-link/private-link-overview but since they are available from within a VNET it means that services inside the VNET needs to be able to find those resources, that's why when you configure a private endpoint they will automatically be added to a Private DNS Zone. If you try to resolve the name of the PaaS service outside of the VNET you will only get the public IP and not be able to connect to the PaaS Service.

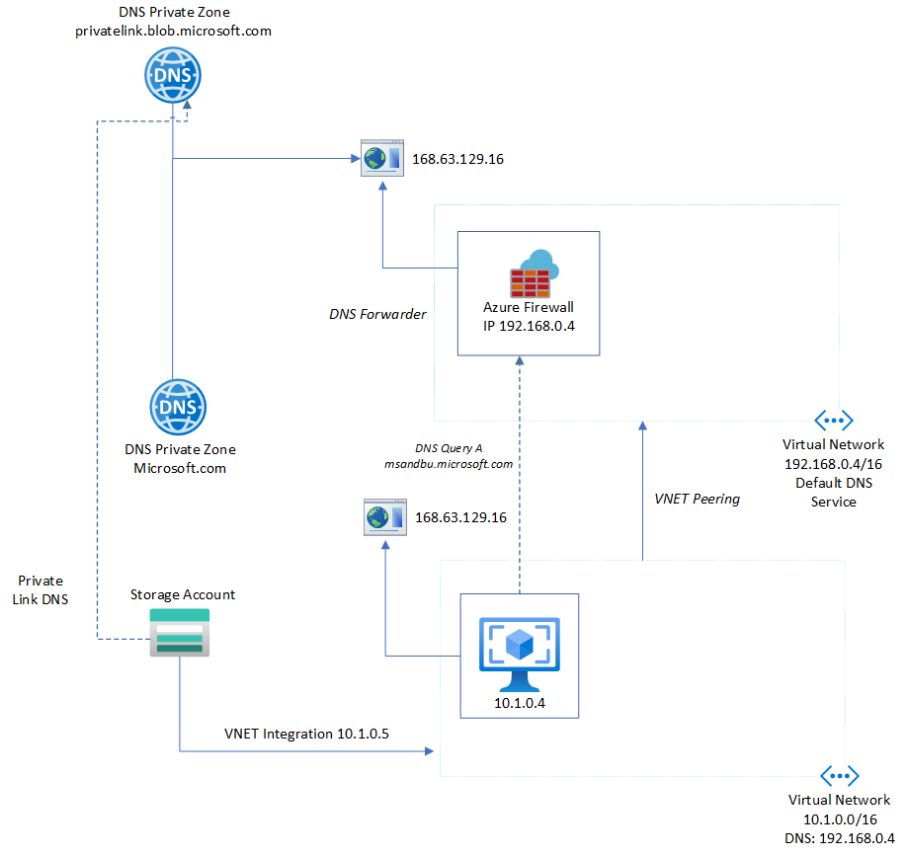
With the scenario above the Private Link would create its own DNS Private Zone according to the DNS Prefix in the article above. The DNS Zone would then be attached to the same virtual network as the other DNS Private Zones. As long as the domain names are unique you can attach up to 1,000 DNS zones per virtual network https://docs.microsoft.com/en-

us/azure/azure-resource-manager/management/azure-subscription-service-limits#azure-dns-limits

If I would add a storage account using a Private Endpoint and attach that endpoint to the virtual network where the VM is running. The DNS Private Zone is attached to the virtual network where the Azure Firewall is running to allow for DNS lookup to work against the private zone.



This means that services within that are using the Azure Firewall as DNS service would be able to resolve that PaaS IP. The PaaS service would be available from the VNET where it is attached.

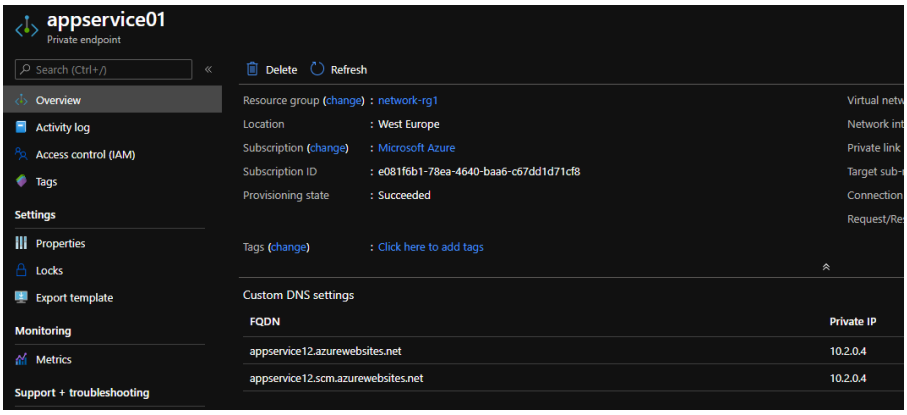


App Services and DNS Lookup

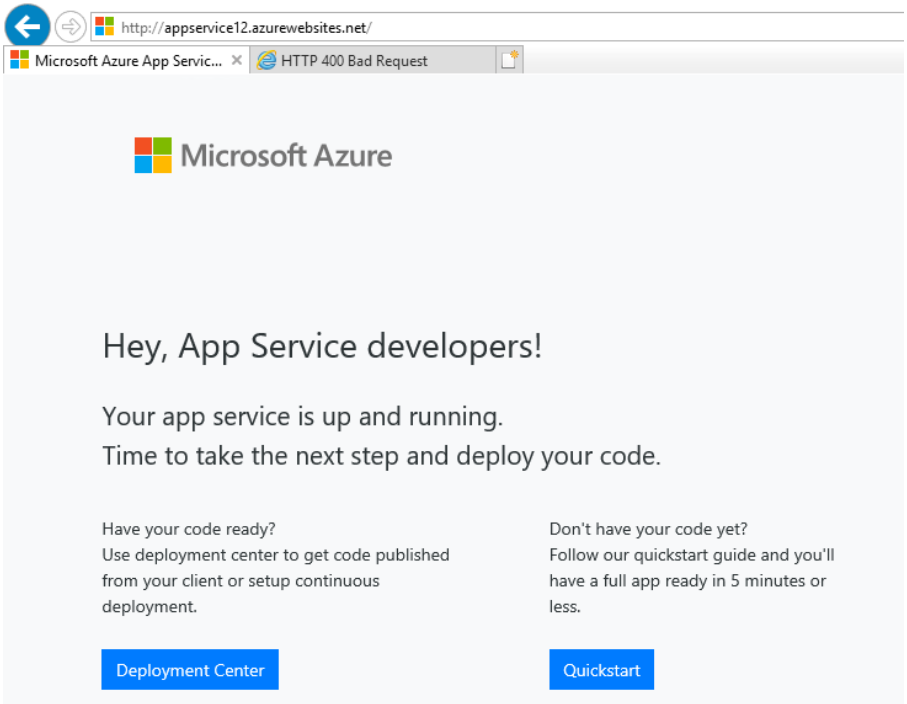
In certain scenarios you might need to have App Service be able to connect either to on-premises resources or other services residing within Azure running as virtual machines. App Services have a couple of ways to integrate with a Virtual network, either using

- VNET Integration
- Hybrid Connections
- Private Endpoints

All of these options above support DNS lookup to resources residing on-premises or other networks. VNET Integration means that a service is still available publically and able to connect to internal services in a virtual network. Hybrid Connections are usefull if you don't want to connect virtual networks together and you want to allow communication between an app service and a specific database engine. And lastly you have Private Endpoints which is currently in public preview as of (13/07/2020) this means that the service is only available internally in the virtual network. When you add a app service with an private endpoint it will automatially add the app service and the SCM as part of the private endpoint (It will not automatically add the IP to a Private DNS Zone) so you would need to define the IP's of the Private Endpoint to a hosts file to map the FQDN of App Services.



when connecting to the service from a VM in another peered network you can access the endpoint using the FQDN after adding the record to the hosts file



Share this:

Related

Things you need to consider before using Azure AD Domain Services
June 30, 2019
Similar post

Troubleshoot Networking in Microsoft Azure
December 16, 2020
In "azure"

Azure Private links and Endpoints
November 12, 2019
Similar post

AZURE DNS | AZURE PRIVATE DNS | AZURE PUBLIC DNS | DNS PROXY AZURE FIREWALL | PRIVATE DNS ZONES

You May Also Like

Technology predictions for 2021

Troubleshoot Networking in Microsoft Azure

About the Author: Marius Sandbu

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Post Comment

Notify me of follow-up comments by email.

Notify me of new posts by email.