**Azure Hub and Spoke VNets - Private Endpoints and Private DNS Zones**

[April 08, 2022](https://joe.blog.freemansoft.com/2022/04/azure-hub-and-spoke-private-dns-zones.html)

Azure makes it simple to access *Azure Cloud Services* from your processes in Azure over the public network.  Things become a little more complicated when you implement the best practice of restricting access to your Azure Services to only your Azure networks (VNets).  This simple action drags in *Private Link Endpoints* and *Private DNS Zones*.   
  
Enterprises typically then layer on multiple *Virtual Networks (VNets)*for management and control purposes. This VNET Hub and Spoke architecture is pretty common though Microsoft has recently been advising customers to implement HUB and Spoke more through subnets than VNets. This reduces VNet sprawl and the amount of peering and other network magic required

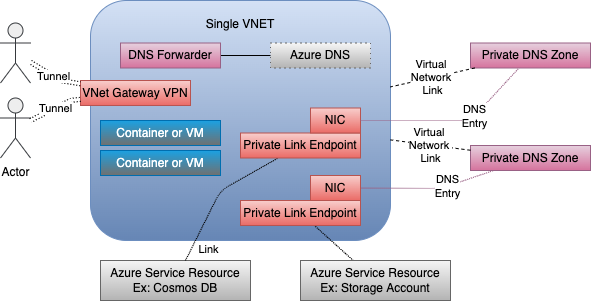
*See YouTube video links below*

**Private Endpoints / Private DNS Zones**

Azure Standard Sevices can be restricted from the Public Internet to your private *Virtual Network*(VNet) through the use of *Private Link Endpoints*(PLE). The PLEs essentially create private connections from a *Network Interface Card*(NIC) in your VNet to the Azure Service.

* Each service asset has its own Private Link Endpoint and corresponding NIC.
* A DNS entry is created for that NIC using an [Azure standard domain name](https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-dns).
* The DNS entry is managed through a [Private DNS Zone](https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.Network%2FprivateDnsZones).
* The Private DNS Zone is joined to your VNet through a *Virtual Network Link*. A Private DNS Zone's Virtual Network Links can be managed in the Azure Portal.
* Processes in that VNET can access the resource PLE via DNS name using the [standard Azure VNet DNS service](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances) available on the well-known address in each VNET.

Each Azure service type has its own domain naming standard and corresponding Private DNS Zone.

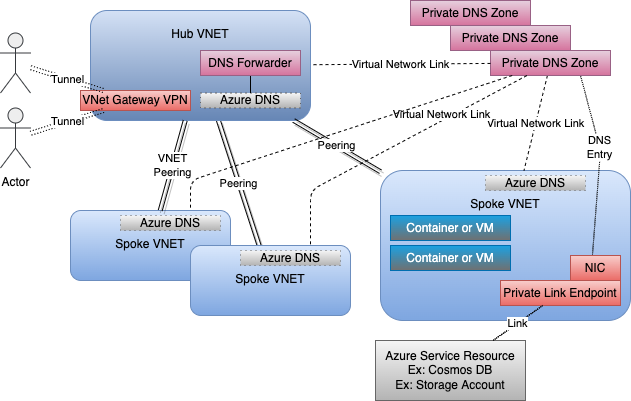
[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEikHlhCC9fD2xvhhFzvzeafKldR213NPxUjgaWm3N8s0ux9L4f_bEVUf7yGH1EvrXR1dkk2bsnzl1td8qcRCJ1KJBv7EcHQn_DmVa3YJRLRf6vw0lGaa1_By_BpE7RnGIP0ZeBhyt8slY6nY6Vc4psS2SeUSMJ0Jr7X-PQ1rJYlB8KmOnXBvQYNBQICTg/s591/Azure%20VNet%20DNS%20and%20PL%20One%20VNET.png)

This VNet also includes a *Point to Site (P2S)*VPN on the *VNet Gateway*. Remote processes communicate with Azure resources over the VPN tunnel.  A *DNS forwarder* is provisioned in the VNET and attached to the VPN Gateway.  The downloaded VPN configuration files include references to the *DNS Forwarder.*External processes then use that *DNS Forwarder*as their DNS server when looking up Azure names.

**Private Link Endpoint / DNS / Hub and Spoke VNets**

This same behavior can be extended across peered VNets. It is pretty standard in the networking world to organize networks around a *hub and spoke* topology.  There is typically a hub VNet that contains management resources and gateways or peerings off to any resources outside this grouping.  Worker or Spoke VNets connect to the hub.  Resources in the spoke VNets talk to resources in other VNets by transiting through the hub. The current *Landing Zone* pattern is an extension of this.

* Peering relationships are set up between the Hub Vnet and each connected Spoke.
* Private DNS Zone resources are declared in a centralized resource group rather than in one of the Resource Groups dedicated to Spoke assets.
* Azure services are exposed in a given Spoke using the same pattern used for a single VNet with *Private Endpoints* and *Private DNS Zones* that are connected to the Spoke VNet DNS via *Virtual Network Links*.
* Private Link NIC DNS entries from all the Spokes are stored in the same share Private DNS Zones.
* The Private DNS Zones are linked to all the VNets.  Really to all the VNets where that asset may be accessed from.

[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi8dUJdwhYqS_LdmQfIEoFf33IGXLAujnvq_uGBrf8DFwpd9JcpF7_Df9yNFSSsovovPJ41Ikmb1TpvFzLTh7i-X5lqz3M7e8KHCk2JMlx4WWKTSlrJ20mG4GBPpu77hlPKFyHhvScuTqqBZIhpw_U4EFOhUS0D_wPJoItRJhXDCbbtyW1LEGCgjjUOUw/s631/Azure%20VNet%20DNS%20and%20Private%20Links.png)

The DNS Forwarder presented to VPN Clients is linked to the standard VNet Azure DNS Server.  That server knows about the *Private DNS Zone*severs.  This means the programs on the VPN have access to the DNS entries for all of the *Private Endpoints* or other resources in all the Spoke VNets.

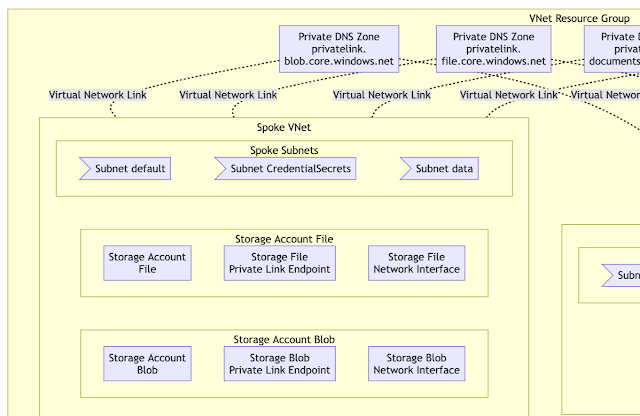
**Videos**

* Part 1: Single VNET: <https://youtu.be/OducMRDoLCo>
* Part 2: Hub and Spoke VNet <https://youtu.be/J-KQkoq--FU>

**Example Project on GitHub**

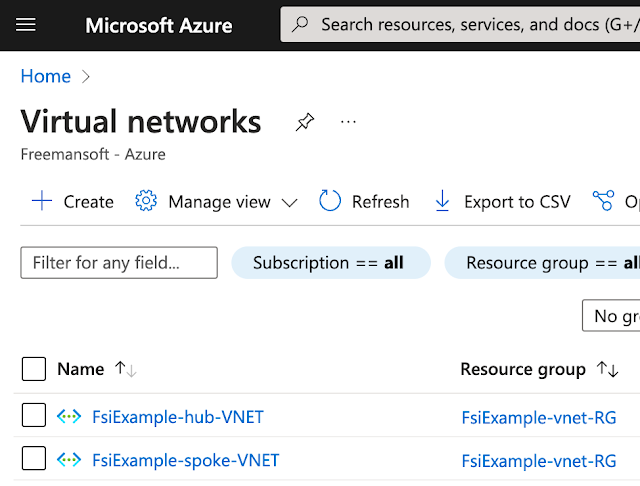
This picture comes from the README of <https://github.com/freemansoft/vnet-p2s-vpn-bastion-azure>. It shows multiple *Private DNS Zones*, one for each type of Azure Service resource that exists in this project.  Each Zone is exposed to the Spoke VNet over a Virtual Network Link, as described in the Azure Portal.

The Spoke VNet contains multiple subnets.  Some of those subnets have *Private Link Endpoints* terminating in them.  Those PLEs DNS entries are registered with the corresponding *Private DNS Zones*.  This means compute and other resources in that VNET can find the resource by name.

The same DNS is linked to the *Hub VNet.*This means processes on the hub VNet can also see the PLE DNS names.   
  
[](https://blogger.googleusercontent.com/img/a/AVvXsEhZ0ufRrHmaBDXhQihixs95fHfZHqNAZ2f-i205qTXvGNMLN4RnzZffnlydtBNsfEmc3LihDhDMHxqUjpysZs_vViat10gWTFQL6DWZdDl6fotVrlPbk69IbGZAL684inuQ62zt6fvrtUkPOaOK6OSTli79MAY6ZN4laqXnjGtuz28VaOxH_T9uk7nNVg)

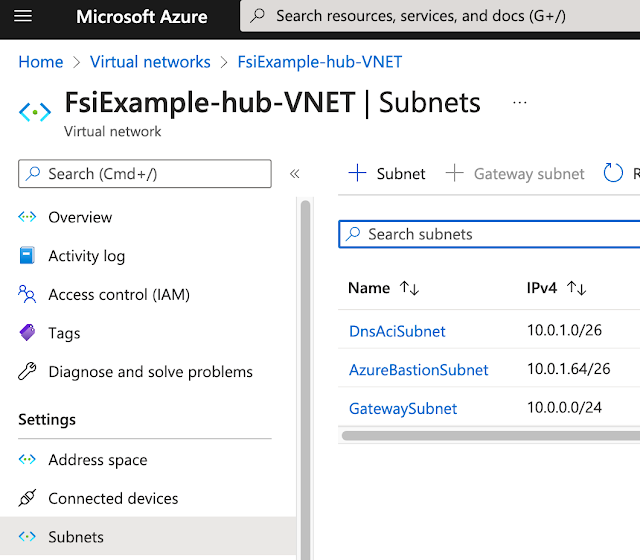
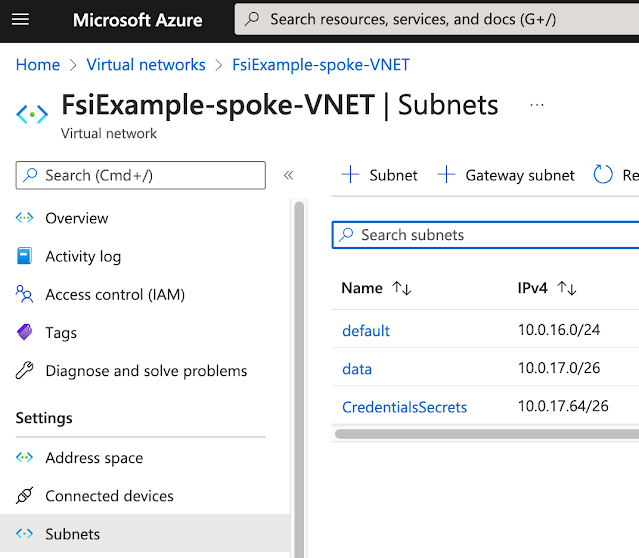
The screenshots in the rest of this blog are from Infrastructure configured via this GitHub Project <https://github.com/freemansoft/vnet-p2s-vpn-bastion-azure>

**Hub and Spoke VNets**

Our sample network has two VNets.  One Hub and one Spoke.  
  
[](https://blogger.googleusercontent.com/img/a/AVvXsEiyYMVCchH0SQlypybYlun95TfFkcmL7HWBD988gE4tz5u-YzB2ib37ws4OMv6Gv5EltX-8KwnO_nOAPahK4UR8BNFS5SZR1v60Ox0SnJkW-j0RDnqhpEqL3kiCzkl-NIWNoI8ikwyg6GGQ5huaFT7KSKLfxwZz7TglFUt2wDvbh1Tzbzz20EvTeb8IyA)

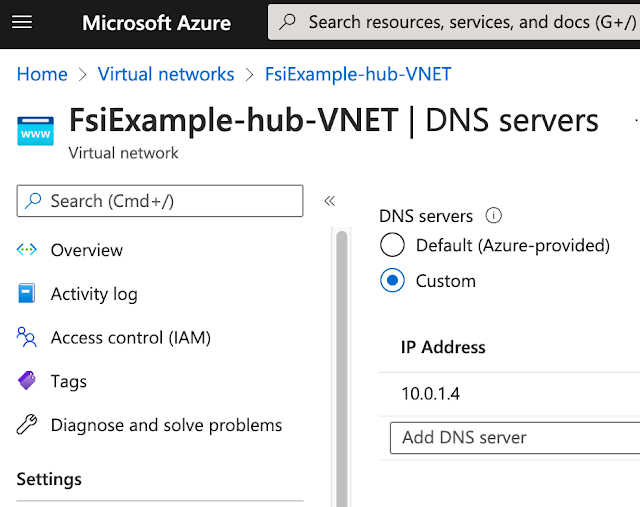
**Subnets on the two VNets**

Each VNet has its own subnet.  Our Hub VNet has 3 network management and governance subnets.

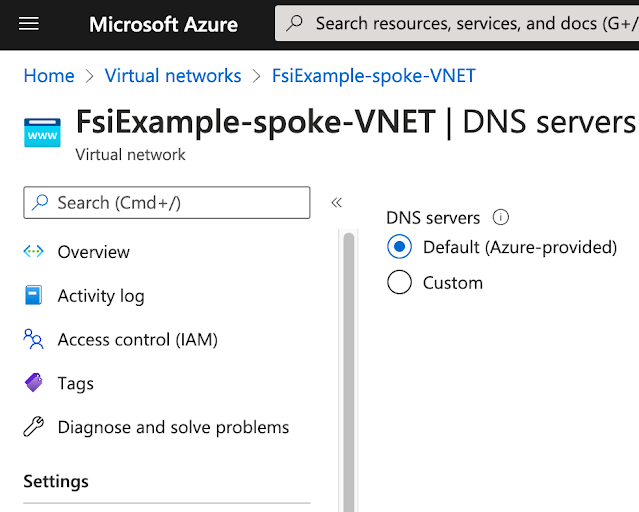
[](https://blogger.googleusercontent.com/img/a/AVvXsEhEivnxrK5gAwdEMzZVOtkJt0VDcYuMPNCryez0Kq6Kpv8D2RmjBff_1NVY884ifuEDnUle_eSmgzdoMtGiqcUELANVYiX6kbnYGSWAjSHLaqlXy8bbMZNnKxiRBQ_XkHRIKhsKx5spfr6fJjwfOsZWhhIh_YBbv61jQ3axxO2Nrrkj6gvkb71c1kX9PQ)  
  
  
The Spoke Vnet has compute, data, and secrets subnets.  The data and CredentialsSecrets subnets will contain Private Link Endpoints for our data and Key Vault Azure services  
  
[](https://blogger.googleusercontent.com/img/a/AVvXsEjqiBMUC9uhO1R8uvSs7IpCXfSP560TaW_MB9WYBOu2LEE5cEwQ1Rk0ay4CEGeiXzIdj8T1uz_7B7WgS-fm4hr_r4iLkvSI1bsXgLADcJmSFpwMvm6TmhD350rkOuvzztZv9_xeZZFyz66H7uAxQItDcN5pBo2Gci0IzJcgBRFKv1X_YiTV_PIQ3SEJUA)

**DNS Forwarders**

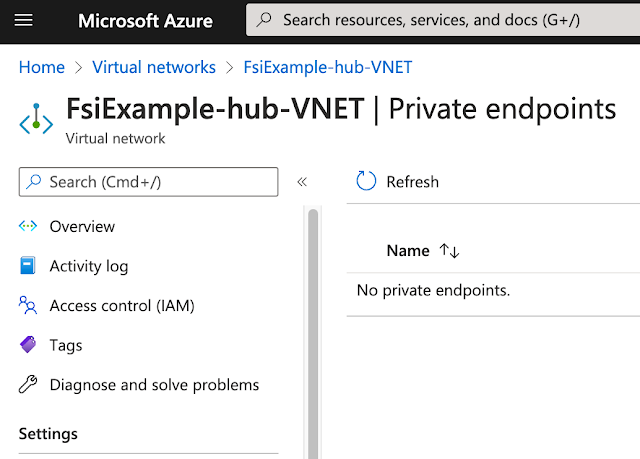
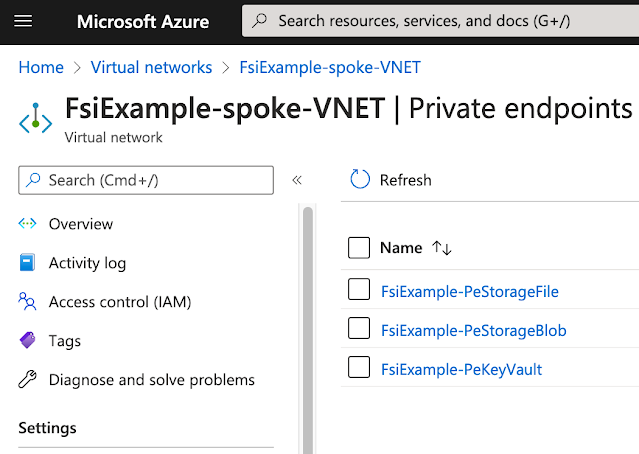
The Hub VNet contains a VPN gateway.  This means it needs a DNS Forwarder to provide internal Azure DNS IP address resolution for processes across the VNet.

[](https://blogger.googleusercontent.com/img/a/AVvXsEgtZAZbkC8HHUl99xR98w16TZ3zxkL0NTJQSdi5QL_5MjHE3tHi8obIOq1PYsJQ0xxSYuKrjPH99NBFJuaCgFJApxS8csPP5D22wkQ7jZb5n-QvAfnRDLGLv2KOMYFzA07_3ZRxEs47r34r-4vGgZeZzgHypzmgJh933LTn6Y-UIgsNK8aST9cRpGlyZQ)

Spoke VNets use standard Azure DNS services.

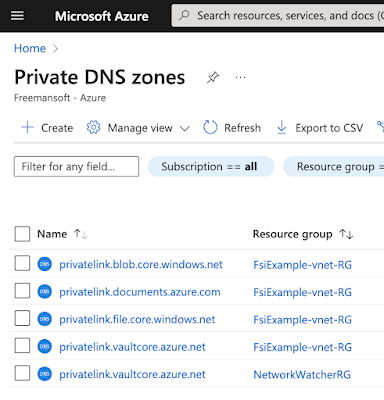
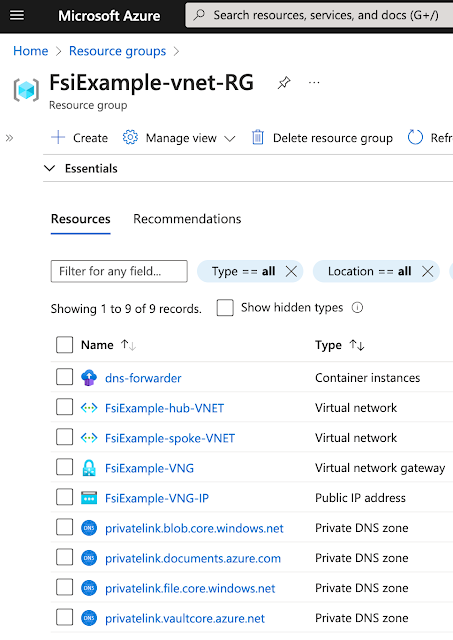
[](https://blogger.googleusercontent.com/img/a/AVvXsEjJ4iQB1QvaqXxPmB2rVj93EZwuvafB7LKGQOWrq7qNnvPZrY2xnLKZkHYanRoLxfe9g1Zc0mCRo9rm9HbkHmeawrzkw_o9DlKlle55MvQuc5z4pxHdUBAy4J8N5RGzo-D8CH5brRXLlPYcWS0IWUQt6zEd2tKdj3yUTIdoDbretRWhpTtR0ysfy9VdZw)

**Private Endpoints**

We don't have any *Private Endpoints* in the Hub VNet.  A real network would have Key Vault, Storage or other services used for management and governance.  
  
[](https://blogger.googleusercontent.com/img/a/AVvXsEjfzmAoPySqYHsE7zPwfGbKUUk715Ps3HACFxVdrxPTE_7KSq5IpnY5a67XMjABG2ghRwZgbrUKLzY-jOtEOBB4IyvTubC2q6bSAmsBNIBY_NvJ5XyINhyJxi02e21Ps6xyqNQXunQtMJlpHYmOe1Mijt3MFFWi8F1BJfq1q9vOLO-Ux4gamjMTycwn2Q)  
  
  
The Spoke VNet contains Private Endpoints for Storage Accounts and Key Vaults.  
  
[](https://blogger.googleusercontent.com/img/a/AVvXsEguu3OfTED-aDW1-KQjgCRV3RFpvDM6brnppfaJ-MOhS95JGiBIjCrKi_G6xehpG1Uutx-bnYyMSnC0odrDB8FgBQG5BSD4HcGvNGswPPGndDJJmavDdNI-xz9r_jQU5_BSm6h4mmdfTLVcPa_FuHFdvXu6_4jEiwX1NFoU95NXYnxB0e1yxmWCHG9yjw)

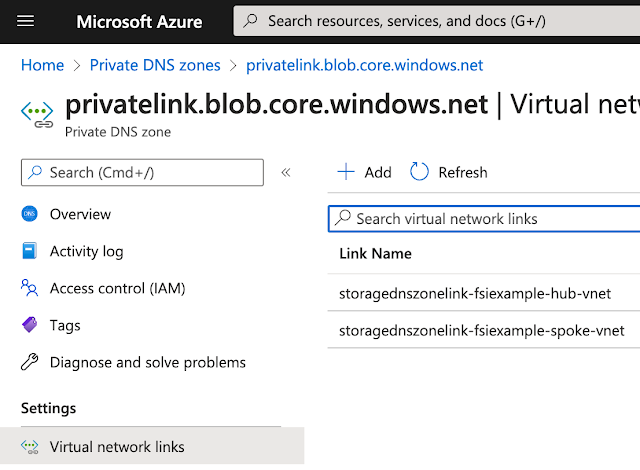
**Private DNS Zones**

Private DNS Zones are created for each of the Azure Service types, and associated DNS Zone, we expect to provision access via Private Endpoints.  All of the Private DNS Zones are put in the same Resource Group to ensure that we don't end up with disjoint Private DNS Zones for the same domain.

[](https://blogger.googleusercontent.com/img/a/AVvXsEiHYu2BBwjPWp_WZ9o_zYe35Pulyrz371laprI8NeYA9mki4EpfQdBx7szZiOSiACw78fnvtZTmgg4_Y7bC7YKuWN4iD_ddD0A8fAnyHCo3kQi0Rsw6q94B-dgmRV7wzKA9j1hZxSbIZHG5YmVjTMIFcfeQipIUuflMxCuFr5s6mVxnPpFWFk76vN5xXQ)  
  
The project has a core Resource Group that contains our VNET, DNS Forwarder VPN Gatway and all the Private DNS Zones.  
  
[](https://blogger.googleusercontent.com/img/a/AVvXsEiKZcFV-3peN0M11zwrG80ecLFXsLfleIPoM3-M9HAoFVC7hkMhJoD3d7x_9NZDttN0VuFkM7fvV6QI0-52SDBcSnAkZvLrvU27n1it9TxWjCd4rM2u6AYQsnqnqeLO9Q27omf0veCtIK8sRcP-BMS37WGbrDcSz6TqTc60l0tv-uJLFSm-tD5x4Gawfg)

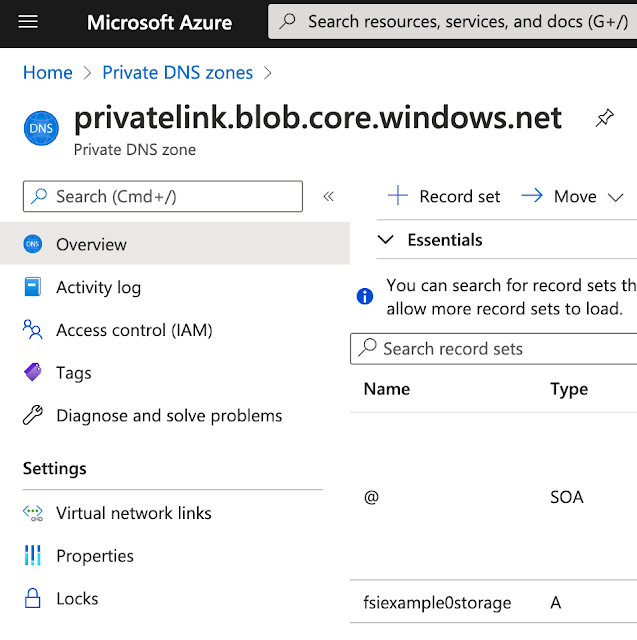
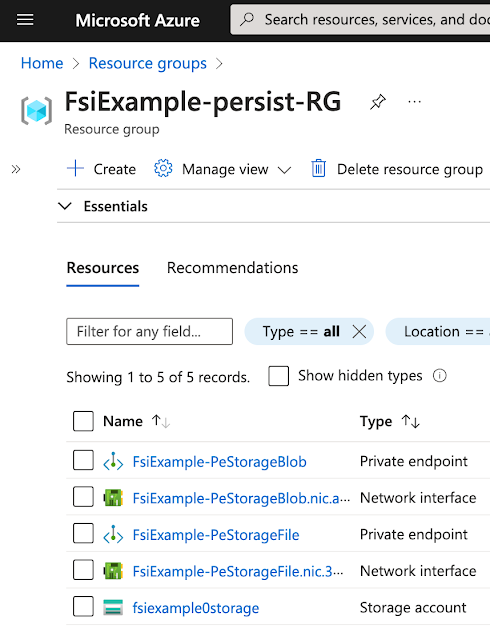
**Private DNS Zone Links to VNETs**

Private DNS Zones are exposed into VNets via *Virtual Network Links*.  A link is created from the DNS Zone to each VNet where the resource may need to be accessed via DNS name.  In this example, we create a link to *every* VNet, hub, and spoke.

[](https://blogger.googleusercontent.com/img/a/AVvXsEiLwx9cYGF2pIO2eWqa_EH-a_qba7RxzTE-N5HAfdxwb722_8uNEaeYfcnh7H8vmyNIF7wG75nHSHkZKG8qH-yuLWZYFIq-7lACl1WcJoL6ZcIwm-RNboL3Lcif1MEhMVknJ6EzxIl6ITnJAIQabuWYFPqwdweoPT7_XlBolu0ntpU9KrtukC73_rh5Wg)

**Private DNS Zone DNS Private Link Entries**

A DNS entry is created for every Private Endpoint.  Microsoft has standardized the domain name for Private Links by Azure resource types.  All of the Azure Storage blob resources end up in the *blob.core.windows.net* domain.  The sample has a single blob resource so there is only one DNS entry in the *Private DNS Zone*DNS server for that domain.

[](https://blogger.googleusercontent.com/img/a/AVvXsEjLKg4P7frajgvFAVyH7EQDiAVXfxXNROfdvo8Q7aJRr35ceeO3qsvbGdSP62nQzw9QLaAgOh8M901VKwK0Q_sTTyUQA3SAxMsfYoZHVDofYWIHJwd2fhh6GdlBZJT4OGp6k-R_Ukeq2E42xdmxz_KphrKIGYuHQb64zrEjpdAQ3pJf6dU-qLnk63PlUA)  
We've exposed both blob and file for this Storage Account. This means we created *Private Endpoints* for both *file* and *blob.*  There will be two DNS entries each in its associated zone.  
  
[](https://blogger.googleusercontent.com/img/a/AVvXsEjvDveKblbf-xG6BjO6pK5SR1R2Yw6eThHISLwqgdS4aOn1Di9xmyVWPnCMqiwi_QhuUk8fCoLMnjrN3bYDJaCPZJH2BekdCD4Ae_x-IhiajR6_oPWoYmiTQJ9pPr53AHXlgNFq0rLLrBnds4Eg7FR5X2W_tEhBW95mpXPSnyeiGBs9-yGkd28e9fW2Pg)

**Conclusion**

This was a short description of how VNets, peering, Private Endpoints, and multi-VNet DNS work.  Leave feedback if you think one of these sections could use more explanation.