Active Directory integrated with DNS in Azure.

Active Directory, or AD, is a directory service that was developed by Microsoft specifically for use in Windows domain networks. It is a set of processes and services that are common to the Windows Server operating systems that are most often used. Active Directory keeps a database of user accounts, computers, and other resources, and it also provides authentication and authorization resources. These three features allow administrators to regulate who on a network may access what.

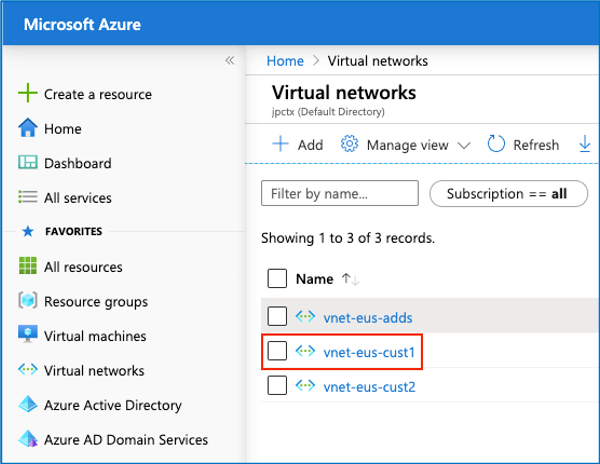
The acronym "DNS" refers to the Domain Name System, which is a hierarchical and decentralized naming system for Internet and network-based computers, services, and other resources that are connected over a network. It translates between domain names (such as "www.microsoft.com") and the numeric IP addresses ("207.46.197.32) that computers use to interact with one another. It serves as the backbone of the modern Internet and translates between the two.

Misconfigured settings and poor maintenance procedures lead to Active Directory's poor performance. Domain configuration DNS settings may be managed at either the branch or the headquarters site. The connection and bandwidth of each site must be considered while planning the two sites' differences. There is a simulation of what would happen if all domain controllers were to be disabled. No matter whether method is used, the DNS Server settings must always be configured in Active Directory (Alonso et al, 2016). The loopback IP on a domain controller should only be set up as a secondary DNS Server. Additionally, it is highly recommended that you have more than one domain controller in your environment. Having just one domain controller creates a vulnerable spot for network identities.

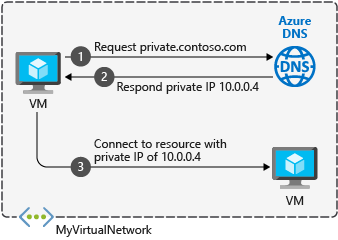
Active Directory's domain controllers may be located using the DNS. The DNS is implemented as a structural component of Active Directory. Active Directory's domain name conventions are also included in the design of AC domains via the Domain Name System. Three of AC's primary components are wholly reliant on the DNS (Chandramouli et al., 2009). DNS objects include the domain controller locator, Active Directory domain names, and the Active Directory AC directory. DNS zones and resource records depict the logical organization of Active Directory data inside DNS.

***Replication topologies***

When creating a new Azure DNS zone, it is a must to specify a unique DNS name for the zone. This name becomes the root of the DNS namespace for the zone, and all DNS records in the zone must be relative to this root. For example, if someone creates a zone named contoso.com, then the zone can contain DNS records for www.contoso.com, mail.contoso.com, and so on.



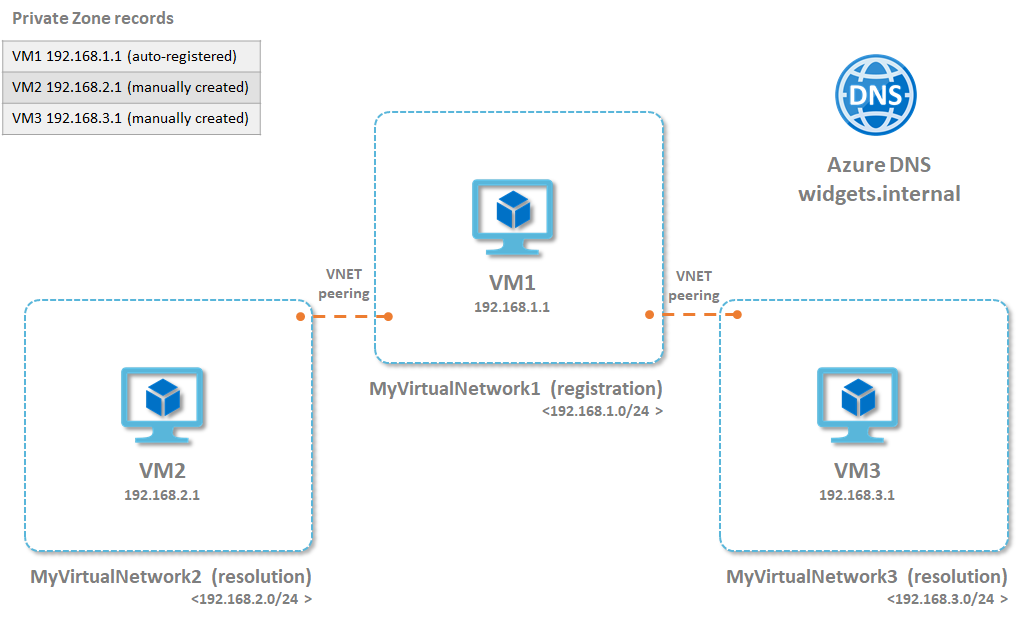
The pathways that domain controllers in a forest use to make identical copies of the directory that have their conventional index partitions synchronized are referred to as the "Active Directory replication topology." Replications must take place nonstop if one wants to have any hope of ensuring that the data in the available directory are constantly correct. When it comes to Active Directory (AD), replication often takes place across domains for the purpose of keeping track of and ensuring that any changes, such as those made to user passwords, are reflected in all domains that are relevant to the system (Brian Desmond, 2008).



When choosing a replication topology to implement into place, the available network speeds are one of the factors that are considered. The process of replication is made easier by faster speeds. Its usefulness is mostly seen in LAN environments. A slowdown caused by discrimination in wide-area networks. To correctly define and implement the replication topology, all the physical domains need to be connected to the local area network (LAN) and represented in Active Directory (AD) as site objects. The ability to conduct searches inside the system is facilitated because of this.

There are two completely different kinds of replication topologies. Intra-site replication and inter-site replication are two topologies that fall within this category. Domain controllers located at each site in the system work together to do an analysis of the system's topology and to establish the replication connections that are required for an inter-site replication architecture. The local domain controller at each site is responsible for performing this operation of replication (Manaois, 2010). Replication happens across identical domains when the intra-site topology is used, and domain controllers are the ones that construct the replications. The primary difference lies in the fact that the replication process takes place in different domains during an inter-site replication topology, while it takes place within the same domain during an intra-site replication topology.

When creating a DNS zone in Azure, one can configure it to use Active Directory integration. This allows Azure to act as a secondary DNS server for the Active Directory domain. After enabling Active Directory integration, Azure will automatically create and manage DNS records for the domain and will update these records when changes are made in Active Directory. This makes it easy to keep your DNS records up-to-date and ensures that domain name can be resolved by DNS clients on the Internet.



To create a DNS zone in Azure, you will need to use the Azure portal, or the Azure CLI.

In the Azure portal, select All services from the left-hand menu, and then select DNS Zones from the list of services.

Click the Add button to create a new DNS zone.

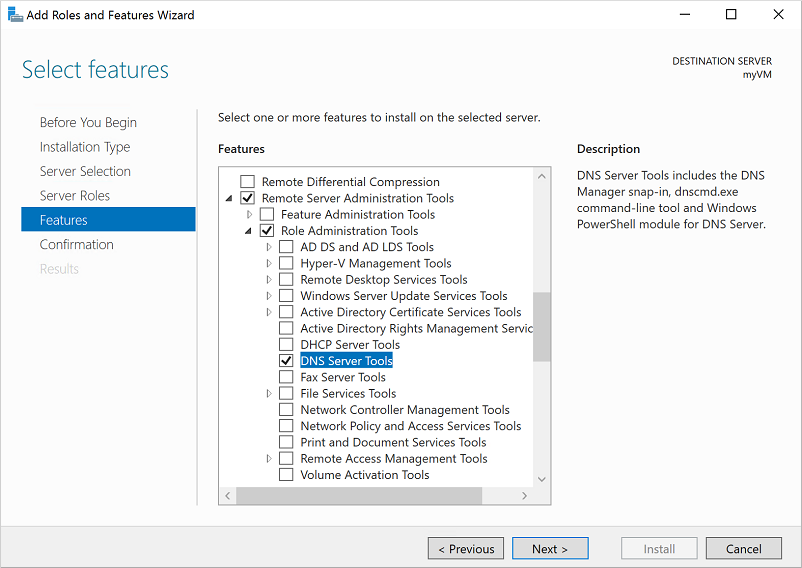
Enter a name for your DNS zone. This can be any valid domain name. For example, you could use the name of your company, or the name of your website.

Click the Create button to create your DNS zone.

Once your DNS zone has been created, you will need to configure it to use Active Directory integration.

To do this, select the DNS zone that you just created, and then click the Configure button.

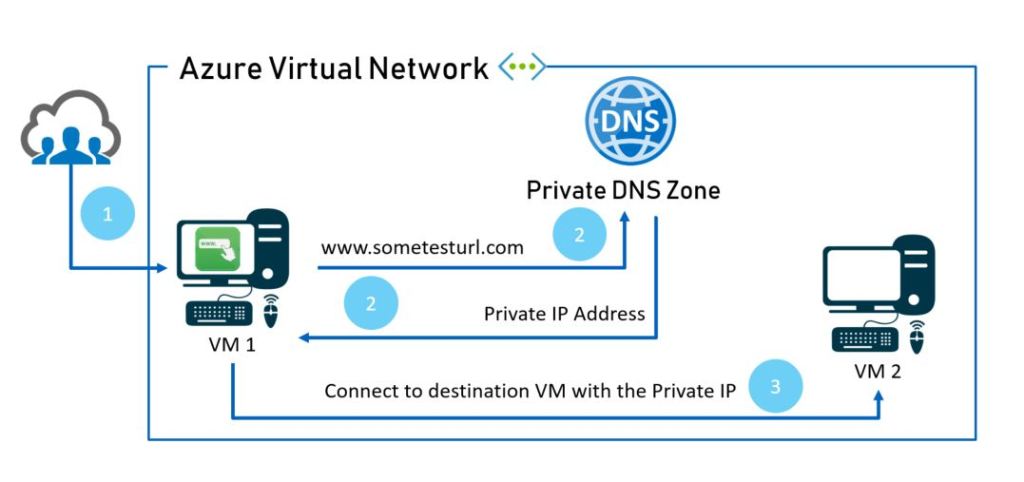
In the Configure DNS Zone blade, select the Active Directory Integration option, and then click the Save button.



Once Active Directory integration has been enabled, Azure will automatically create and manage DNS records for your domain. These records will be updated whenever changes are made in Active Directory.

If you need to manually add or remove DNS records, you can do so by selecting the DNS zone, and then clicking the Records button.

In the DNS Records blade, you will see a list of all the DNS records that have been created for your domain.



To add a new DNS record, click the Add button.

In the Add DNS Record blade, select the type of DNS record that you want to create.

Enter the name of the record, and then enter the value for the record.

Click the Save button to save the DNS record.

To delete a DNS record, select the record from the list, and then click the Delete button.

You will need to confirm the deletion, and then the DNS record will be deleted.

**References**

Alonso, R., Monroy, R., & Trejo, L. (2016). Mining IP to Domain Name Interactions to Detect DNS Flood Attacks on Recursive DNS Servers. Sensors, 16(8), 1311. http://dx.doi.org/10.3390/s16081311

Brian Desmond, J. R.-N. (2008). *Active Directory: Designing, Deploying, and Running Active Directory.* O'Reilly Media, Inc.

Chandramouli, R. & Rose, S. (2009). Open Issues in Secure Domain Name System (DNS) Deployment. IEEE Security & Privacy Magazine. <http://dx.doi.org/10.1109/msp.2009.113>

Manaois, S. (2010, March 2). *Microsoft SharePoint*. Retrieved from What are Intra Site and Inter Site?: <https://social.technet.microsoft.com/Forums/sharepoint/en-US/6f108dd5-759b-4fb8-8292-832be4eb20f6/what-are-intra-site-and-inter-site?forum=winserverDS>