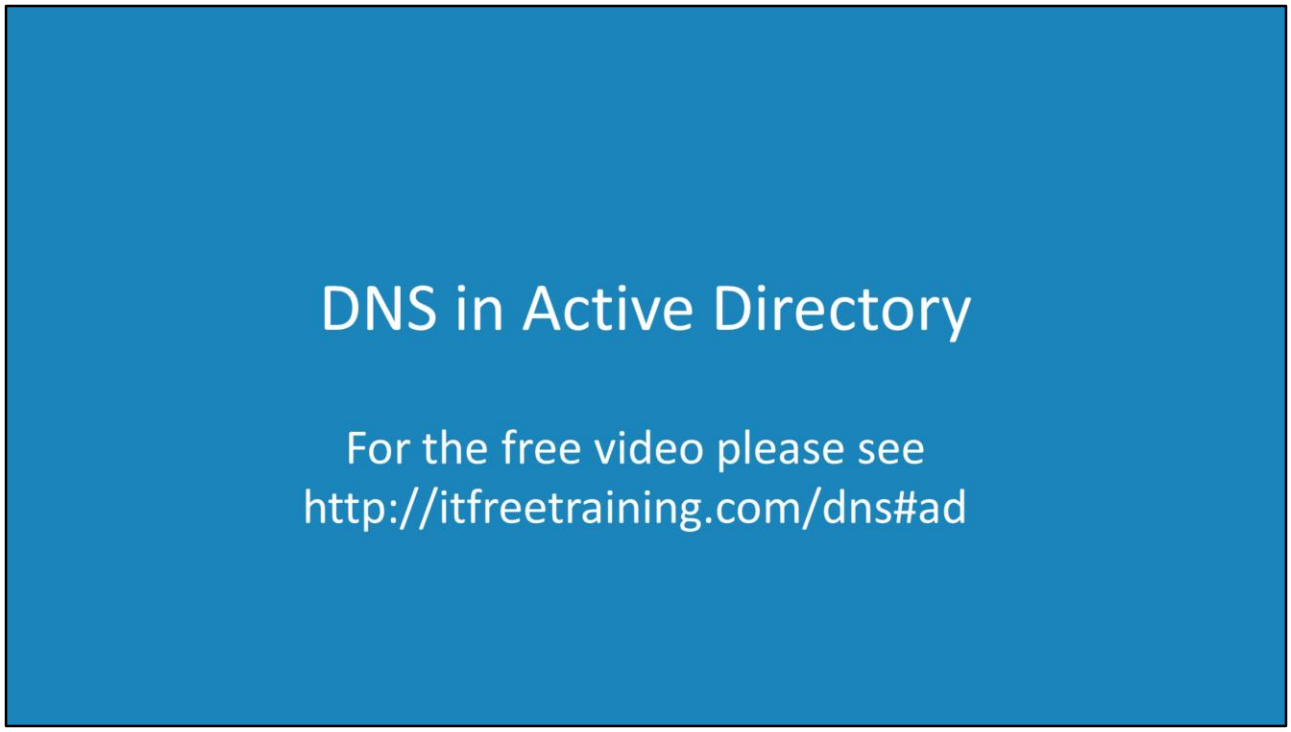
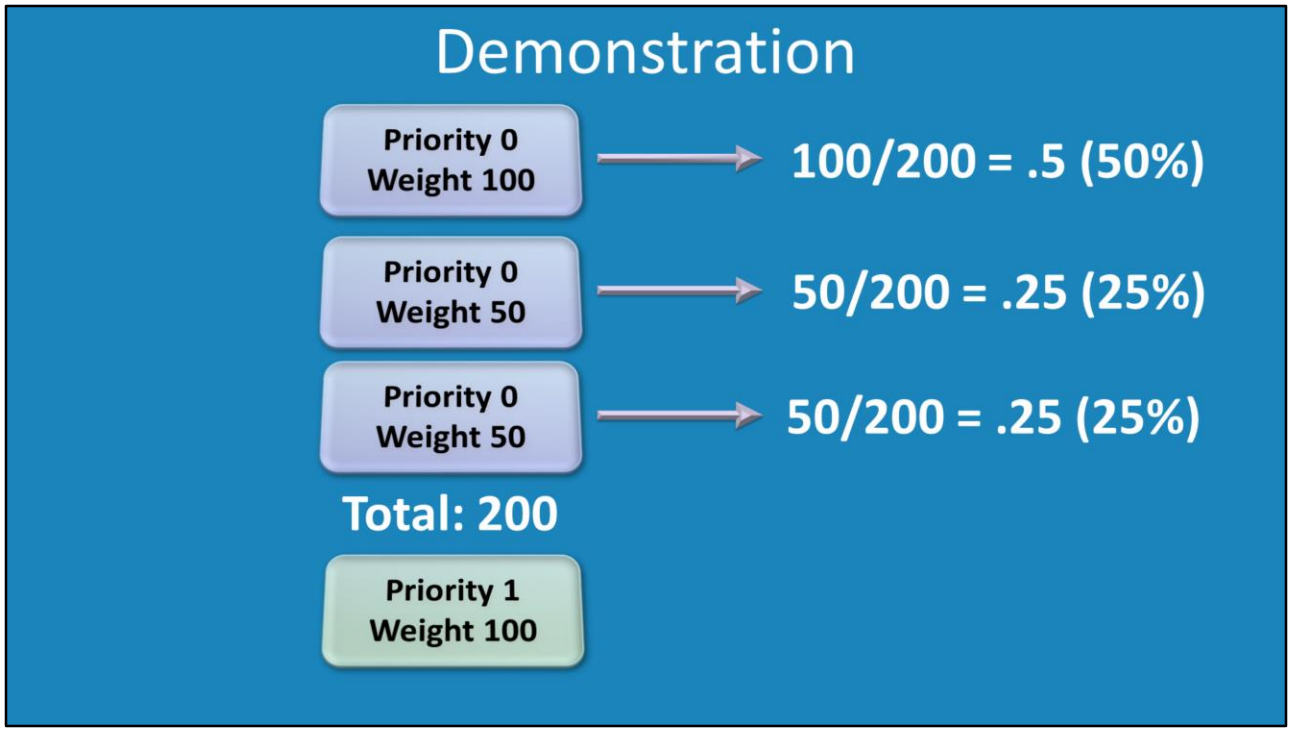


Active Directory requires DNS in order to operate. This videos looks at how Active Directory uses DNS and thus improves your understanding of how to support Active Directory and ensures your DNS infrastructure will support the requirements for Active Directory.

Copyright 2013 © http://ITFreeTraining.com



Demonstration

To access DNS Manager, open Server Manager and select DNS from the tools menu. The DNS records required for Active Directory are located under Forward Lookup zones under the DNS name of your domain. There are a number of different containers in here. The DNS records in each container have different uses to clients on the network.

_tcp container

This container contains services that are available via TCP or reliable transport. The container contains 4 different types of records. These are _gc, _kerberos, _kpasswd and _ldap. These allow clients to find services on the network by searching for these records. For example, if a client wants to find a global catalog server, it will look for the DNS records _gc. Under _tcp, this will contain all the global catalog servers that are available in the domain. A client needs to query this container using DNS and this will give the client a service record for a global catalog server in the domain. The default DNS server setting will attempt to return a global catalog server in the same network as the client. The _kerberos records are used by the client to locate servers on the network that can perform Kerberos authentication. The _kpasswd records tell the client where a server is that can perform Kerberos password changes. The _ldap tells the client where servers are located on the network that can perform Ldap lookups.

_udp container contains the same kind of records as _tcp, however these services are contactable with the UDP protocol.

Copyright 2013 © http://ITFreeTraining.com

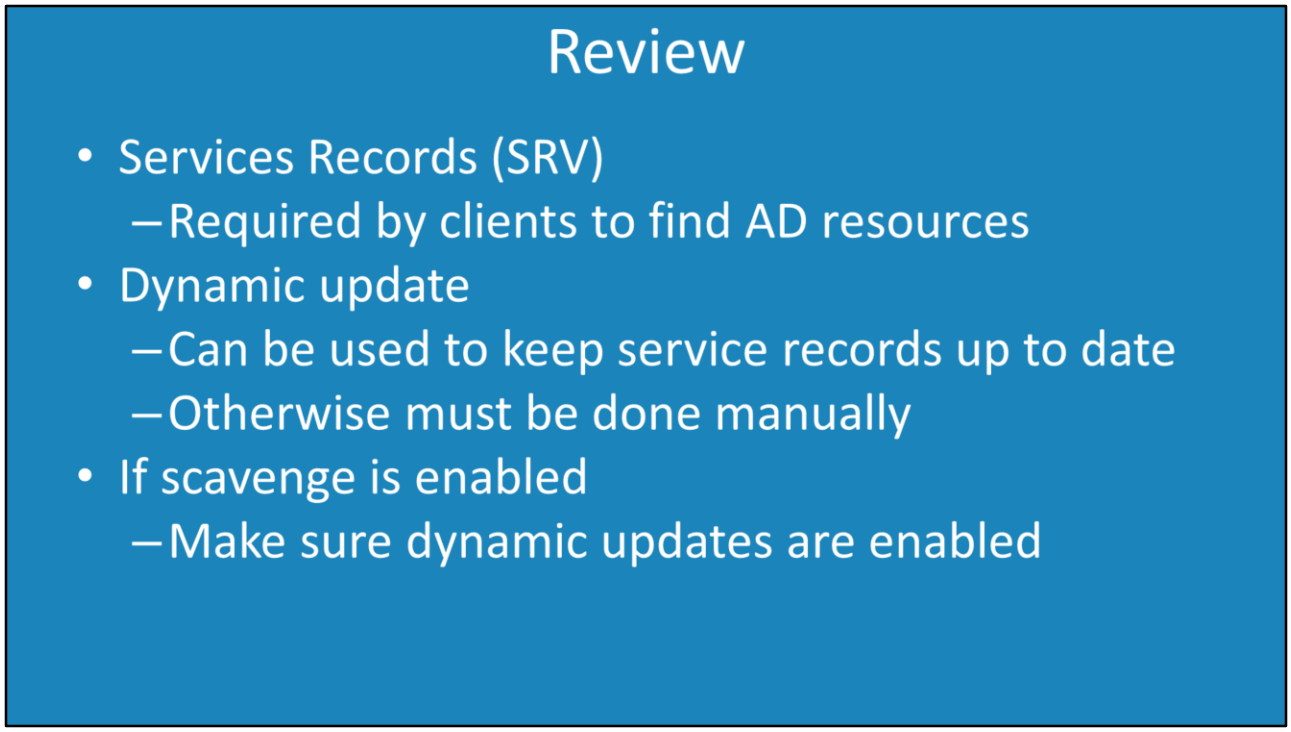
Service records properties
Priority: When two or more records exist with the same name than the DNS record will be used with the lowest priority.
Weight: When two or more records exist that have the same lowest priority, the weight value is used to determine which record is used. For example, if one record had a value of 20 and the other 80, the first record would use 2 out of 10 requests and the second, 8 out of 10 records.
Port: The port number is the port the service can be contacted on.

Dynamic update and DNS
When services like Active Directory Domain Services starts up, it will automatically attempt to register service records in DNS. If you do not have dynamic updates enabled and you have scavenging enabled, the Active Directory DNS records will eventually be removed. Since the services records have been removed, clients will not be able to find Active Directory resources on the network. If you want to check if dynamic updates are enabled, open the properties of the zone file and make sure that dynamic updates is not disabled on the general tab.

DomainDNSZones and ForestDNSZones
These two containers contains DNS records that are relevant for the domain and forest.

_msdcs zone
This is a Microsoft specific zone that contains resource service records for the domain or forest. This zone contains DNS service records that are registered by Microsoft based services. Since there are other non-Microsoft Directory Services that use service records, in order for a client to be sure that it is obtaining service records for a Microsoft solution, a Microsoft only zone is required. This zone is available at the forest level and thus Domain Controllers can obtain service records for all Domain Controllers in the forest. Using this information, they can create replication that works at the domain and forest level.

Copyright 2013 © http://ITFreeTraining.com



Review
Clients query a DNS server in order to obtain service records. These services records contain the location of servers on the network that provide particular services. For example, let's say the client needed to locate a Domain Controller to log on to the network. If you have dynamic updates enabled, DNS will be automatically updated when you make changes to a Domain Controller, for example changing its IP Address or making it a global catalog server. If you want service records to be removed automatically, for example you want service records to be removed for a Domain Controller automatically when the a Domain Controller is removed from the network, you need to ensure that scavenging is enabled on the DNS server. This will remove the DNS records for the Domain Controller that has been removed from the network automatically, however if you do enable scavenging, make sure that dynamic updates is also enabled otherwise all service records will eventually be removed from DNS and the clients will not be able to locate Active Directory resources on the network.

See http://YouTube.com/ITFreeTraining or http://itfreetraining.com for our always free training videos. This is only one video from the many free courses available on YouTube.

References
"MCTS 70-640 Configuring Windows Server 2008 Active Directory Second edition" pg 480
"Active Directory SRV Records" http://www.petri.co.il/active_directory_srv_records.htm
"How DNS Support for Active Directory Works" http://technet.microsoft.com/en-us/library/cc759550(WS.10).aspx

Copyright 2013 © http://ITFreeTraining.com