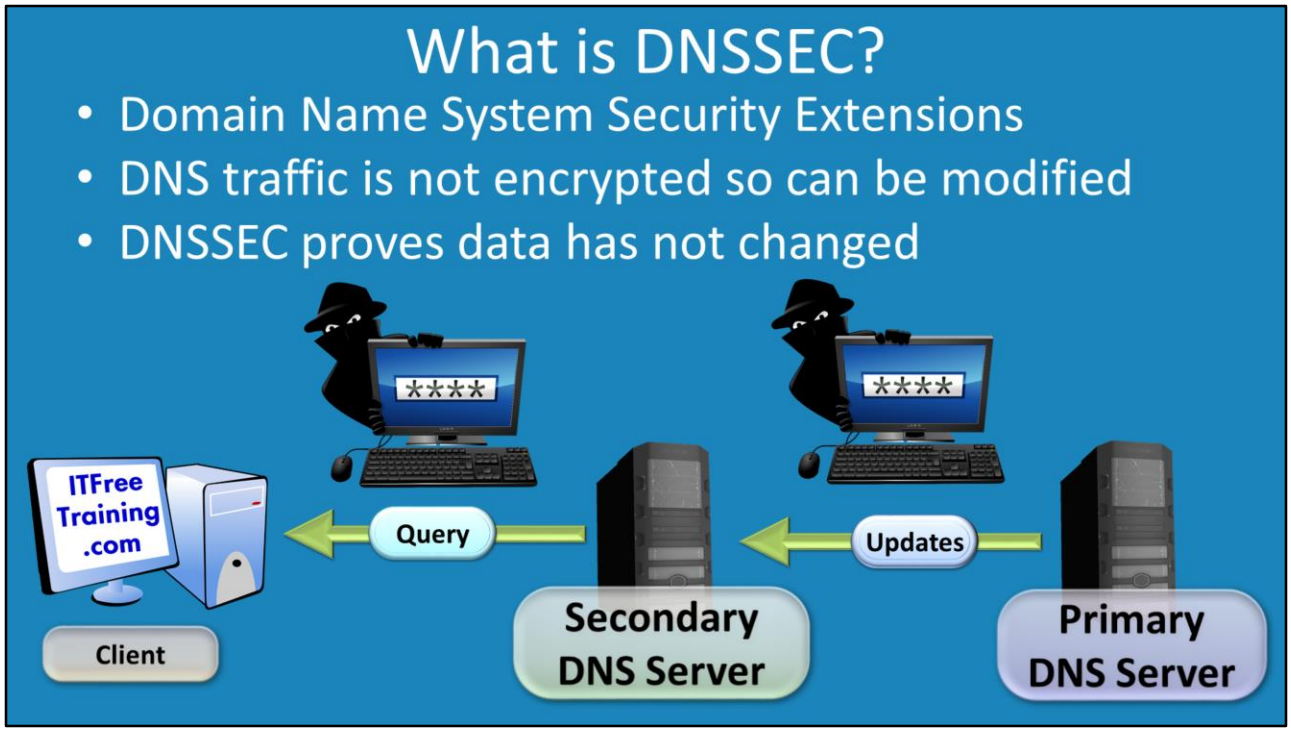
What's New In DNS for Windows 2012

For the free video please see
http://itfreetraining.com/dns#new2012

This video will look at the two new features that are included in DNS server for Windows Server 2012.

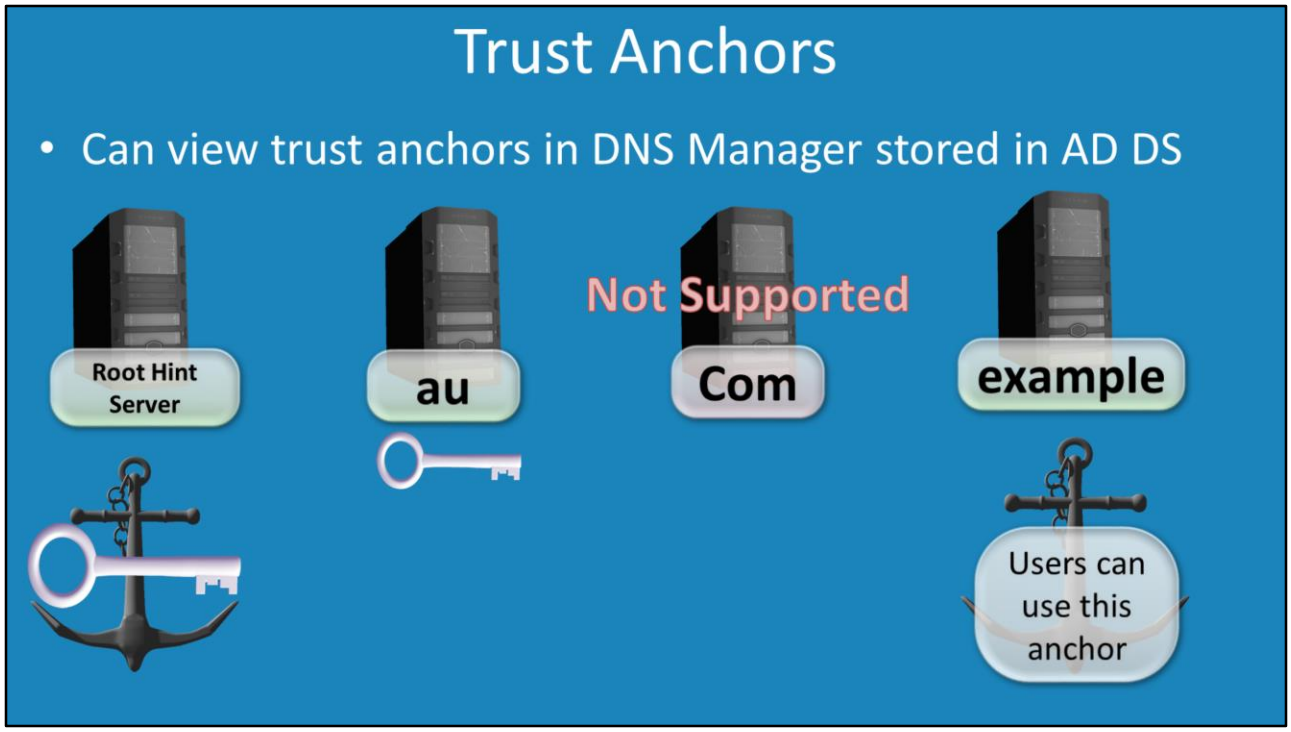
What's new in DNS in 2012
Windows Server 2012 across the board adds additional administration features to PowerShell. With DNS in Windows Server 2012, features have been added that allow all functionally that can be performed with the graphical DNS Manager to be performed using PowerShell. The DNS role itself can also be added or removed using the command prompt.

DNSSEC was available in Windows Server 2008 but in Windows Server 2012 additional features have been added.



What is DNSSEC?

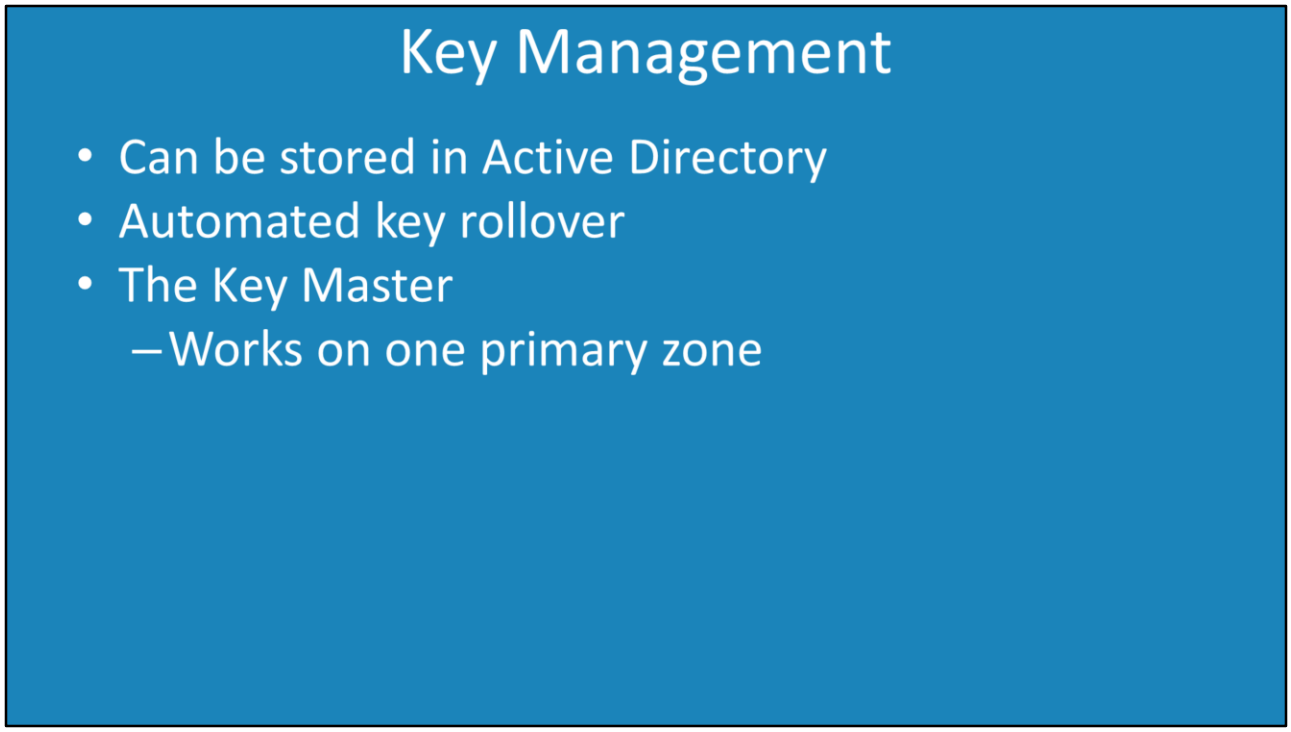
DNSSEC stands for Domain Name System Security Extensions. DNS replicates data between each other and this data is not encrypted so an attacker could potentially modify this data when it travels over the internet. DNSSEC provides a way to test the data that has been transferred that it has not been modified. It also provides a method for checking the identification of a DNS server so an attacker cannot create their own DNS server and disguise it as an authoritative DNS Server. In a lot of companies they will use VPN connections or other secure connections like IPSec to secure data travelling over the internet. If this is the case, even though the DNS traffic itself is not encrypted, the tunnel it is travelling over is encrypted and thus prevents it from being modified by an attacker. The next issue is that if an attacker did create a fake DNS server, DNSSEC provides a method for the client to check that the DNS server is a legitimate DNS server. This is performed by DNSSEC adding a signature to the DNS record when it is given to the client. This means the DNS record itself is still not encrypted but can be checked against the signature.



Trust Anchors
A trust anchor in DNS is a point where the trust model starts. In the case of certificates you have a root CA which forms the root of the trust model. DNSSEC likewise has a trust anchor that is at the top of the DNS hierarchy, each DNS server in the hierarchy is chained to this trust anchor. The problem occurs in that a DNS server may not support DNSSEC which is in the chain. When this occurs the chain for trust if broken and the DNS data cannot be considered secure.

When the chain of trust is broken, an administrator may decide to add their own trust anchor. For example, the chain of trust may be broken at the last server which is the ISP's DNS server. If the connection back to the ISP is secure, the administrator may not consider this to be a problem. If this is the case, a new trust anchor can be added to the client computer to allow them to use DNSSEC even though a complete chain of trust is not available back to the root hint server.

The ability to add trust anchors was present in Windows Server 2008, however with Windows Server 2012 you can now see these trust anchors in DNS Manager making them easy to administer.



Key Management
In order to use DNSSEC there are a number of keys that need to be managed. In Windows Server 2008 this was more of a manual process. In Windows server 2012 this is more automated. Firstly a key must be changed after a certain amount of time in order to have good security. The longer you have the same key, the higher the probability that it could be hacked. Windows Server 2012 has a feature called automated key rollover which makes this process automatic.

Windows Server 2012 also comes with a feature called The Key Master. This allows DNSSEC keys to be stored in the one primary zone making administration a lot simpler.

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
"What's New in DNS Server in Windows Server 2012" http://technet.microsoft.com/en-us/library/dn305897.aspx
"Overview of DNSSEC" http://technet.microsoft.com/en-us/library/jj200221.aspx
"Securing the Root: The root of the problem, creating a trust anchor(s)" http://www.internetgovernance.org/2007/04/18/securing-the-root-the-root-of-the-problem-creating-a-trust-anchors