New DNS Resource Records and other New Enhancements

DNS response validation is achieved by associating a private/public key pair (as generated by the administrator) with a DNS zone, and then defining additional DNS resource records to sign and publish keys. Resource records distribute the public key while the private key remains on the server. When the client requests validation, DNSSEC adds data to the response that enables the client to authenticate the response.

The following table describes the new resource records in Windows Server 2012.

Resource record	**Purpose**
DNSKEY	This record publishes the public key for the zone. It checks the authority of a response against the private key held by the DNS server. These keys require periodic replacement through key rollovers. Windows Server 2012 supports automated key rollovers. Every zone has multiple DNSKEY's that are then broken down to the ZSK and KSK.
DS (Delegation Signer)	This record is a delegation record that contains the hash of the public key of a child zone. This record is signed by the parent zone's private key. If a child zone of a signed parent is also signed, the DS records from the child must be manually added to the parent so that a chain of trust can be created.
RRSIG (Resource Record Signature)	This record holds a signature for a set of DNS records. It is used to check the authority of a response.
NSEC (Next	When the DNS response has no data to provide to the client, this

Resource record	Purpose
Secure)	record authenticates that the host does not exist.
NSEC3	This record is a hashed version of the NSEC record, which prevents alphabet attacks by enumerating the zone.

Other New Enhancements

Other enhancements for Windows Server 2012 include:

- Support for DNS dynamic updates in DNSSEC signed zones.
- Automated trust anchor distribution through AD DS.
- Windows PowerShell–based command-line interface for management and scripting.