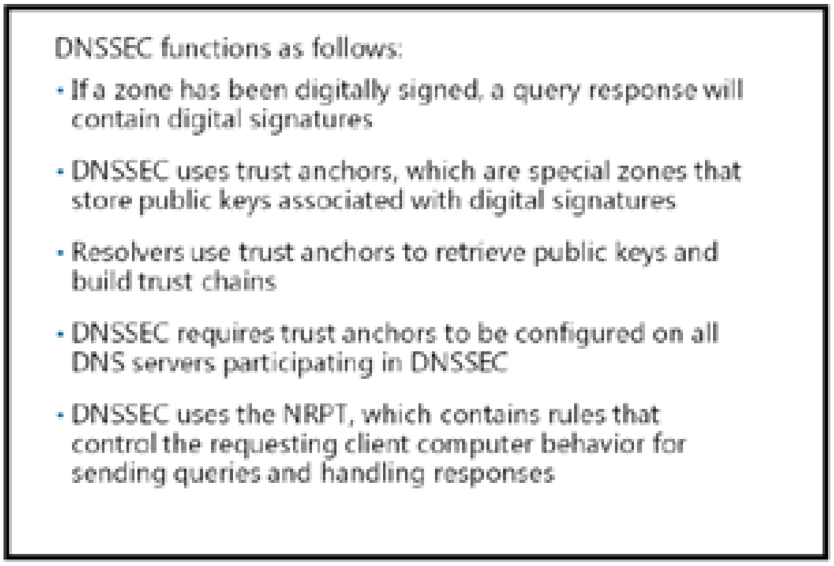
DNSSEC enables a DNS zone and all records in the zone to be signed cryptographically such that client computers can validate the DNS response. DNS is often subject to various attacks, such as spoofing and cache-tampering. DNSSEC helps protect against these threats and provides a more secure DNS infrastructure.

How DNSSEC Works



DNSSEC functions as follows:

- If a zone has been digitally signed, a query response will contain digital signatures
- DNSSEC uses trust anchors, which are special zones that store public keys associated with digital signatures
- Resolvers use trust anchors to retrieve public keys and build trust chains
- DNSSEC requires trust anchors to be configured on all DNS servers participating in DNSSEC
- DNSSEC uses the NRPT, which contains rules that control the requesting client computer behavior for sending queries and handling responses

Intercepting and tampering with an organization’s DNS query response is a common attack method. If malicious users can alter responses from DNS servers, or send spoofed responses to point client computers to their own servers, they can gain access to sensitive information. Any service that relies on DNS for the initial connection—such as e-commerce web servers and email servers—are vulnerable. DNSSEC protects clients that are making DNS queries from accepting false DNS responses.

When a DNS server that is hosting a digitally signed zone receives a query, it returns the digital signatures along with the requested records. A resolver or another server can obtain the public key of the public/private key pair from a trust anchor, and then validate that the responses are authentic and have not been tampered with. To do this, the resolver or server must be configured with a trust anchor for the signed zone or for a parent of the signed zone.

Trust Anchors

A *trust anchor* is an authoritative entity that is represented by a public key. The TrustAnchors zone stores preconfigured public keys that are associated with a specific zone. In DNS, the trust anchor is the DNSKEY or DS resource record. Client computers use these records to build trust chains. You must configure a trust anchor from the zone on every domain DNS server to validate responses from that signed zone. If the DNS server is a domain controller, then Active Directory–integrated zones can distribute the trust anchors.

Name Resolution Policy Table

The Name Resolution Policy Table (NRPT) contains rules that control the DNS client behavior for sending DNS queries and processing the responses from those queries. For example, a DNSSEC rule prompts the client computer to check for validation of the response for a particular DNS domain suffix. As a best practice, Group Policy is the preferred method of configuring the NRPT. If there is no NRPT present, the client computer accepts responses without validating them.

Deploying DNSSEC

To deploy DNSSEC:

1. Install Windows Server 2012 and assign the DNS role to the server. Typically, a domain controller also acts as the DNS server. However, this is not a requirement.
2. Sign the DNS zone by using the DNSSEC Configuration Wizard, which is located in the DNS console.
3. Configure trust anchor distribution points.
4. Configure the NRPT on the client computers.

Assigning the DNS Server Role

To assign the DNS server role, in the Server Manager Dashboard, use the Add Roles and Features Wizard. You can also add this role can when you add the AD DS role.

Then configure the primary zones on the DNS server. After a zone is signed, any new DNS servers in Windows Server 2012 automatically receive the DNSSEC parameters.

Signing the Zone

The following signing options are available:

- **Configure the zone signing parameters**. This option guides you through the steps and enables you to set all values for the key signing key (KSK) and the zone signing key (ZSK).
- **Sign the zone with parameters of an existing zone**. This option enables you to keep the same values and options as another signed zone.
- **Use recommended settings**. This option signs the zone by using the default values.

  Note: Zones can also be unsigned by using the DNSSEC management user interface to remove zone signatures.

Configuring Trust Anchor Distribution Points

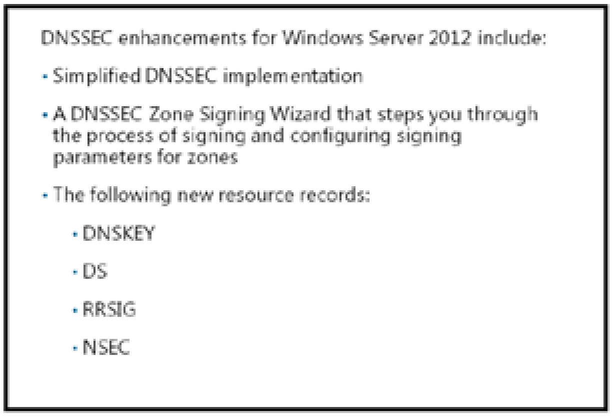
If the zone is Active Directory–integrated, and if all domain controllers are running Windows Server 2012, you can select to distribute the trust anchors to all the servers in the forest. Make this selection with caution because the wizard turns on DNSSEC validation. If you enable DNS trust anchors without thorough testing, you could cause DNS outages. If trust anchors are required on computers that are not domain-joined—for example, a DNS server in the perimeter network (also known as screened subnet)—then you should enable automated key rollover.

Note: A key rollover is the act of replacing one key pair with another at the end of a key's effective period.

Configuring NRPT on Client Computers

The DNS client computer only performs DNSSEC validation on domain names where the NRPT has configured the DNS client computer to do so. A client computer that is running Windows 7 is DNSSEC–aware, but it does not perform validation. Instead, it relies on the security-aware DNS server to perform validation on its behalf.

New DNSSEC Features for Windows Server 2012



DNSSEC enhancements for Windows Server 2012 include:

- Simplified DNSSEC implementation
- A DNSSEC Zone Signing Wizard that steps you through the process of signing and configuring signing parameters for zones
- The following new resource records:
  - DNSKEY
  - DS
  - RRSIG
  - NSEC

Windows Server 2012 has simplified DNSSEC implementation. Although DNSSEC was supported in Windows Server 2008 R2, most of the configuration and administration tasks were performed manually, and zones were signed when they were offline.

DNSSEC Zone Signing Wizard

Windows Server 2012 includes a DNSSEC Zone Signing Wizard to simplify the configuration and signing process, and to enable online signing. The wizard allows you to choose the zone signing parameters as indicated in the previous topic. If you choose to configure the zone signing settings rather than using parameters from an existing zone or using default values, you can use the wizard to configure settings such as:

- KSK options
- ZSK options
- Trust anchor distribution options
- Signing and polling parameters

New Resource Records

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 Secure)	When the DNS response has no data to provide to the client, this 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.

Demonstration: Configuring DNSSEC

In this demonstration, you will see how to use the Zone Signing Wizard in the DNS console to configure DNSSEC.

Demonstration Steps Configure DNSSEC

1. Sign in on **LON-DC1** as **Adatum\Administrator** with a password of **Pa$$w0rd**.
2. Start the **DNS** console.
3. Use the DNSSEC Zone Signing Wizard to sign the Adatum.com zone.
4. Choose to customize zone signing parameters.
5. Ensure that DNS server LON-DC1 is the Key Master.
6. Add the **Key Signing Key** by accepting default values for the new key.
7. Add the **Zone Signing Key** by accepting the default values for the new key.
8. Choose to use **NSCE3** with default values.
9. Do not choose to enable the distribution of trust anchors for this zone.
10. Accept the default values for **signing** and **polling**.
11. Verify that the DNSKEY resource records were created in the **Trust Points zone**.
12. Use the Group Policy Management Console (GPMC) to configure NRPT. Create a rule that enables DNSSEC for the Adatum.com suffix, and that requires DNS client computers to verify that the name and address data is validated.