DNS Security Extensions (DNSSEC)

One major issue that you must always look at is keeping your DNS safe. Think about it, DNS is a database of computer names and IP addresses. As a hacker, if I control DNS, I can control your company. In organizations that do not support extra security like IPSec, DNS security is even more important. This is where DNSSEC can help.

Windows Server 2012 can use a suite of extensions that will help add security to DNS, and that suite is called *Domain Name System Security Extensions (DNSSEC)*, which was introduced in Windows Server 2008 R2. The DNSSEC protocol allows your DNS servers to be secure by validating DNS responses. DNSSEC secures your DNS resource records by accompanying the records with a digital signature.

To allow your DNS resource records to receive digital signatures, DNSSEC is applied to your DNS server by a procedure called *zone signing*. This process begins when a DNS resolver initiates a DNS query for a resource record in a signed DNS zone. When a response is returned, a digital signature (RRSIG) accompanies the response and this allows the response to be verified. If the verification is successful, then the DNS resolver knows that the data has not been modified or tampered with in any way.

Once you implement a zone with DNSSEC, all the records that are contained within that zone get individually signed. Since all of the records in the zone get individually signed, this gives administrators the ability to add, modify, or delete records without resigning the entire zone. The only requirement is to resign any updated records.

Trust Anchors

Trust anchors are an important part of the DNSSEC process because trust anchors allow the DNS servers to validate the DNSKEY resource records. *Trust anchors* are preconfigured public keys that are linked to a DNS zone. For a DNS server to perform validation, one or more trust anchors must be configured. If you are running an Active Directory Integrated zone, trust anchors can be stored in the Active Directory Domain Services directory partition of the forest. If you decide to store the trust anchors in the directory partition, then all DNS servers that reside on a domain controller get a copy of this trust anchor. On DNS servers that reside on stand-alone servers, trust anchors are stored in a file called TrustAnchors.dns. If your servers are running Windows Server 2012, then you can view trust anchors in the DNS Manager Console tree in the Trust Points container. You can also use Windows PowerShell or Dnscmd.exe to view trust anchors. Windows PowerShell is the recommended command-line method

for viewing trust anchors. The following line is a PowerShell command to view the trust anchors for Contoso.com.

```
get-dnsservertrustanchor sec.contoso.com
```

DNSSEC Clients

Windows 7, Windows 8, Windows Server 2008 R2, and Windows Server 2012 are all DNS clients that receive a response to a DNS query, examine the response, and then evaluate whether or not the response has been validated by a DNS server. The DNS client itself is nonvalidating, and the DNS client relies on the local DNS server to indicate that validation was successful. If the server doesn’t perform validation, then the DNS client service can be configured to return no results.