DNSSEC in Windows DNS Server

Kumar Ashutosh, Microsoft
@krash0x35
Overview

- Dynamic
- Interoperability
- Manageability
- Automation
Zone Signing

- Choose the Key Master
- Signing keys
- KSK configuration
- ZSK configuration
- NSEC
- Trust anchors
- Signing and polling
- Summary
Zone Signing: Select Key Master

- Single location for all key generation and management
- Responsible for automated key rollover
Zone Signing: Configure KSK

- Key signing keys (KSK) are used to sign other DNSKEY records
Zone Signing: Configure ZSK

- Zone signing keys (ZSK) are used to sign other records
Zone Signing: Denial of Existence

- NSEC
- NSEC3
A trust anchor (or trust “point”) is a public cryptographic key for a signed zone.

- Delegation Signer (DS)
- DNSKEY
Zone Signing: Signaling And Polling

- DS record generation algorithm: SHA-1 and SHA-256
- DS record TTL (seconds): 3600
- DNSKEY record TTL (seconds): 3600
- Secure delegation polling period (hours): 12
- Signature inception (hours): 1
  Offset from current time when the signature is created.
Flexibility

- Chose your Keys
- Dynamic unsign/re-sign
- Change Properties
- DDNS with DNSSEC
- AD/Non-AD
- Primary Secondary
- DNSSEC with Traffic Management
- Chose your Key Store
Powershell Automation

Sign with Default

- Invoke-DnsServerZoneSign -ZoneName secure.contoso.com –SignWithDefault -Force

Customize your parameters

- PS C:\> Reset-DnsServerZoneKeyMasterRole -ZoneName fabrikam.com -KeyMasterServer dc2.contoso.com -SeizeRole -Force
- PS C:\> Set-DnsServerDnsSecZoneSetting -ZoneName fabrikam.com -DenialOfExistence NSec
- PS C:\> Add-DnsServerSigningKey -ZoneName fabrikam.com -Type KeySigningKey -CryptoAlgorithm RsaSha1 -KeyLength 2048
- PS C:\> Add-DnsServerSigningKey -ZoneName fabrikam.com -Type ZoneSigningKey -CryptoAlgorithm RsaSha1 -KeyLength 1024
- PS C:\> Invoke-DnsServerZoneSign -ZoneName fabrikam.com -Force
Distribute Trust Anchors

Export a Trust Point

- Export-DnsServerDnsSecPublicKey -ComputerName DC2.contoso.com -ZoneName secure.contoso.com -Path "\Myshare\keys"
- Export-DnsServerDnsSecPublicKey -ComputerName DC2.contoso.com -ZoneName secure.contoso.com -Path "\Myshare\keys" -DigestType sha1

Import a Trust Point

- Import-DnsServerTrustAnchor -KeySetFile "\File1\DNSKeys\keyset-secure.contoso.com"

Add Root Trust Anchor

- Add-DnsServerTrustAnchor -Root
**Verify DNSSEC: Demonstration**

<table>
<thead>
<tr>
<th>Step</th>
<th>Query-response</th>
<th>Optional DNSSEC data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A DNS client sends a DNS query to a recursive DNS server.</td>
<td>The DNS client can indicate that it is DNSSEC-aware (DO=1).</td>
</tr>
<tr>
<td>2</td>
<td>The recursive DNS server sends a DNS query to the root and top-level domain (TLD) DNS servers.</td>
<td>The recursive DNS server can indicate that it is DNSSEC-aware (DO=1).</td>
</tr>
<tr>
<td>3</td>
<td>The root and TLD servers return a DNS response to the recursive DNS server providing the IP address of the authoritative DNS server for the zone.</td>
<td>Authoritative servers for the parent zone can indicate that the child zone is signed using DNSSEC and include a secure delegation (DS record).</td>
</tr>
<tr>
<td>4</td>
<td>The recursive DNS server sends a DNS query to the authoritative DNS server for the zone.</td>
<td>The recursive DNS server can indicate that it is DNSSEC-aware (DO=1) and capable of validating signed resource records (CD=1) to be sent in the response.</td>
</tr>
<tr>
<td>5</td>
<td>The authoritative DNS server returns a DNS response to the recursive DNS server, providing the resource record data.</td>
<td>The authoritative DNS server can include DNSSEC signatures in the form of RRSIG records in the DNS response, for use in validation.</td>
</tr>
<tr>
<td>6</td>
<td>The recursive DNS server returns a DNS response to the DNS client, providing the resource record data.</td>
<td>The recursive DNS server can indicate whether or not the DNS response was validated (AD=1) using DNSSEC.</td>
</tr>
</tbody>
</table>
Thank You

For more details visit: