DNSSEC in Windows DNS Server

Kumar Ashutosh, Microsoft
Windows DNS Server

- Widely deployed in enterprises
- Fair presence in the DNS resolver space
- Standards compliant and interoperable
- Secure and scalable
Microsoft introduced support for DNSSEC in Windows 2008 R2…

- Ability to sign zones offline and host signed zones
- Validation of signed responses
- Support for NSEC
DNSSEC in Windows DNS Server

- Latest RFCs
  - NSEC3 Support
  - RSA/SHA-2, ECDSA Signing
  - Automated Trust Anchor rollover
- Support for 3rd Party Key Management
- Support for Online Zone Signing.
  - Sign/unsign/change DNSSEC settings on a live zone
  - Add/remove records dynamically on a signed zone
- Improved DNS/DNSSEC server performance
- Trust Anchor Management
  - Root Trust Anchor Management
  - Managing Zone specific Trust Anchors
  - Signed Delegations
  - RFC 5011 for Automated, authenticated and authorized update of Trust Anchors

DNSSEC in Windows DNS Server
DNSSEC in Windows DNS Server

ENABLING ENTERPRISE DNSSEC ROLLOUT

Interoperability

Dynamic

Manageability

Automation

Complete Powershell Support
DNSSEC in Windows Server

ENABLING ENTERPRISE DNSSEC ROLLOUT

- Automated re-signing on static and dynamic updates
- Automated key rollovers
- Automated signature refresh
- Automated updating of secure delegations
- Automated distribution and updating of Trust Anchors - RFC 5011
Signing a zone

- DNS Manager wizard walks admin through signing process
- Generates Keys for signing zone on the first Server.
  - Support for CNG compliant third party KSPs
- Signs it's own copy of the zone
## Key Master Role

- Single location for all key generation and management
  - Responsible for automated key rollover
- Administrator designates one server to be the key master
  - First DNSSEC server becomes

### DNSSEC

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Status</th>
<th>DNSSEC Status</th>
<th>Key Master</th>
</tr>
</thead>
<tbody>
<tr>
<td>_msdcs.corp.contoso.com</td>
<td>Active Directory-Integrated Primary</td>
<td>Running</td>
<td>Not Signed</td>
<td>DNS-DC2.corp.contoso.com</td>
</tr>
<tr>
<td>com</td>
<td>Standard Primary</td>
<td>Running</td>
<td>Signed</td>
<td></td>
</tr>
<tr>
<td>corp.contoso.com</td>
<td>Active Directory-Integrated Primary</td>
<td>Running</td>
<td>Not Signed</td>
<td></td>
</tr>
<tr>
<td>DinnerNow.com</td>
<td>Standard Primary</td>
<td>Running</td>
<td>Signed</td>
<td></td>
</tr>
</tbody>
</table>
Signing entire zone

- Private zone signing keys replicate automatically to all DCs hosting the zone through AD replication
- Each zone owner signs its own copy of the zone when it receives the key
  - Only Server 2012+ DCs will sign their copy of the zone
Updating zone data

1. Client sends dynamic update to any authoritative DNS server
2. That DNS server updates its own copy of the zone and generates signatures
3. The unsigned update is replicated to all other authoritative servers
4. Each DNS server adds the update to its copy of the zone and generates signatures
5. The DNSSEC settings of zone can also be updated
Key Rollover Process

- Zone Signing Key Rollover:
  - Uses Pre-Publish Mechanism

- Key Singing Key Rollover:
  - Uses Double Signature Mechanism

- Trust Anchor Management: RFC 5011 and Hold Down Time

- Key Retirals
Key Management has low TCO

- Automated key rollovers
  - Key rollover frequency is configured per zone
  - Key master automatically generates new keys
  - Secure delegations from the parent are also automatically updated
  - Manual Rollovers are also available

- Signatures stay up-to-date
  - New records are signed automatically when zone data changes
  - Static and dynamic updates
  - NSEC records are kept up to date

- More