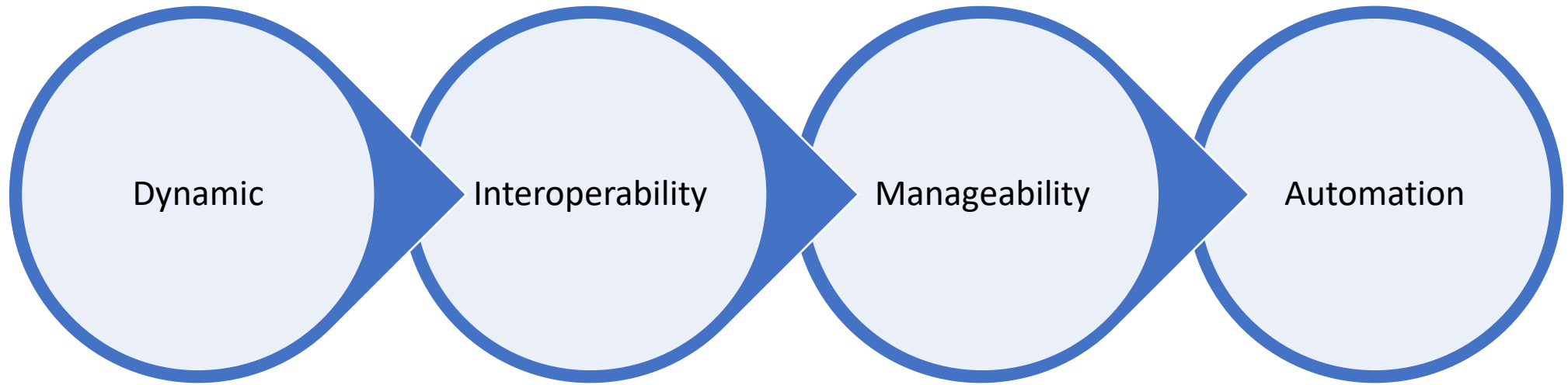


# DNSSEC in Windows DNS Server

---

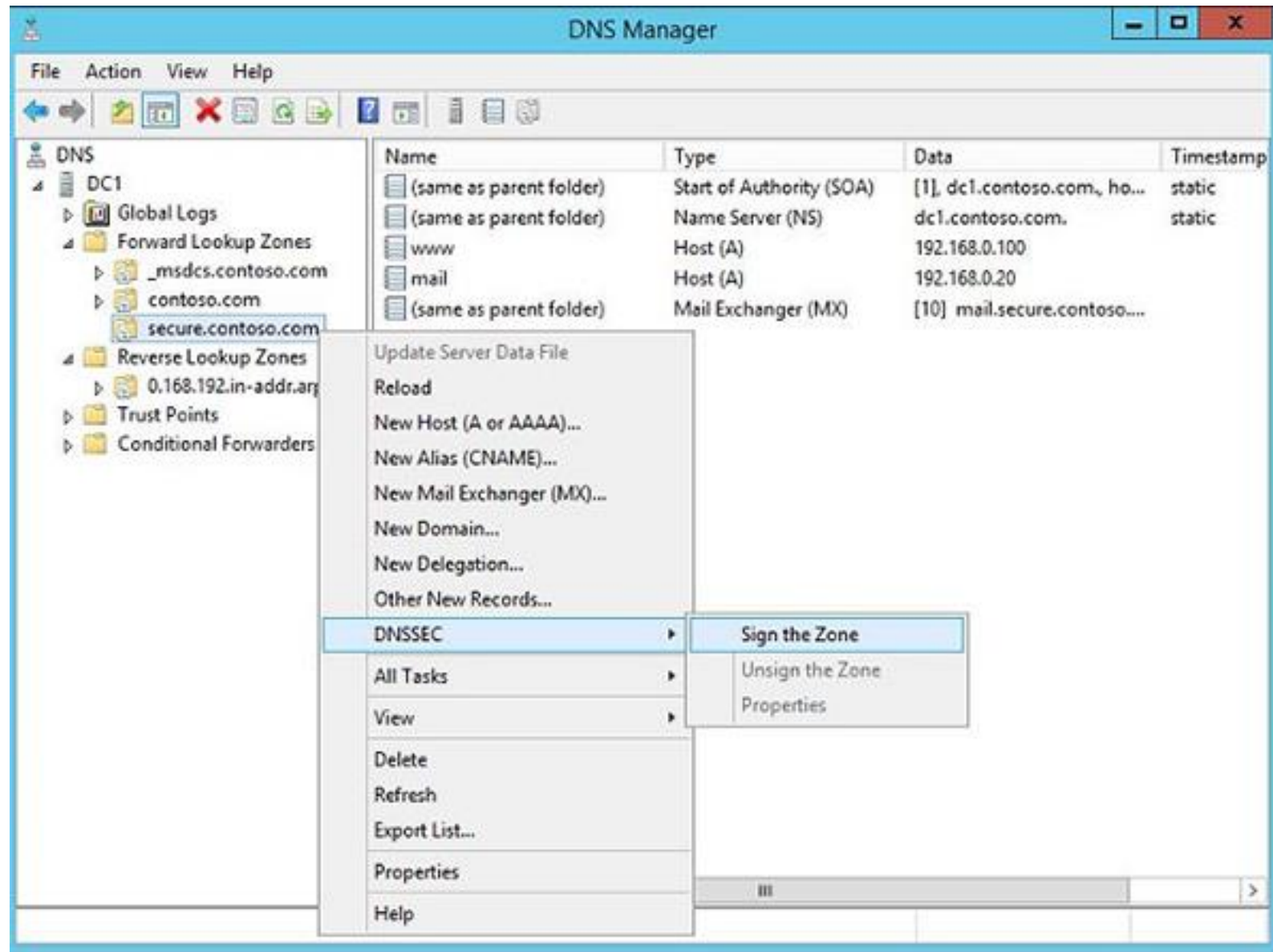
Kumar Ashutosh, Microsoft  
@krash0x35



Overview

# 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 Wizard ✕

**Key Master**  
Choose the Key Master for this zone. 

The Key Master is a DNS server that generates and manages cryptographic keys for a DNSSEC protected zone. Any authoritative DNS server that hosts a primary copy of the zone can be the Key Master.

By default, the current DNS server is chosen to be the Key Master. You can also choose another DNS server as the Key Master for this zone.

The DNS server DC1 is the Key Master.

Select another primary server as the Key Master:

# Zone Signing: Configure KSK

- Key signing keys (KSK) are used to sign other DNSKEY records

New Key Signing Key (KSK)

Guid

Guid: {00000000-0000-0000-0000-000000000000}

Key Generation

Generate new signing keys.

Use pre-generated keys

Use this key as active key:

Use this key as standby key:

Key Properties

Cryptographic algorithm: RSA/SHA-256

Key length (Bits): 2048

Select a key storage provider to generate and store keys: Microsoft Software Key Storage Prov

DNSKEY RRSET signature validity period (hours): 168

Replicate this private key to all DNS servers authoritative for this zone.  
(Applicable only to AD integrated zones)

Key Rollover

Enable automatic rollover

Rollover frequency (days): 755

Delay the first rollover by (days): 0

OK Cancel

# Zone Signing: Configure ZSK

- Zone signing keys (ZSK) are used to sign other records

New Zone Signing Key (ZSK)

Guid

Guid: {00000000-0000-0000-0000-000000000000}

Key Properties

Cryptographic algorithm: RSA/SHA-256

Key length (Bits): 1024

Select a key storage provider to generate and store keys: Microsoft Software Key Storage Prov

DNSKEY signature validity period (hours): 168

DS signature validity period (hours): 168

Zone record validity period (hours): 240

Key Rollover

Enable automatic rollover

Rollover frequency (days): 90

Delay the first rollover by (days): 0

OK Cancel

# Zone Signing: Denial of Existence

- NSEC
- NSEC3

## Zone Signing Wizard

**Next Secure (NSEC)**  
NSEC and NSEC3 resource records provide authenticated denial of existence.

Choose NSEC or NSEC3 for authenticated denial of existence.

Use NSEC3

Iterations:

Generate and use a random salt of length:

Use opt-out to cover unsigned delegations

(Recommended for zones with many unsigned delegations)

Use NSEC

< Back   Next >   Cancel

# Zone Signing: Trust Anchors

- A trust anchor (or trust “point”) is a public cryptographic key for a signed zone.
- Delegation Signer (DS)
- DNSKEY

**Zone Signing Wizard**

**Trust Anchors (TAs)**  
Configure distribution of trust anchors and rollover keys.

Enable the distribution of trust anchors for this zone.

If this is also a domain controller, trust anchors for this zone will be distributed to all other DNS servers running on domain controllers in the forest. If this DNS server is not a domain controller, a trust anchor for this zone will be added only to the local trust anchor store. Selecting this option enables DNSSEC validation for this zone on all the servers where trust anchors are distributed.


Enable automatic update of trust anchors on key rollover (RFC 5011).



# Zone Signing: Signaling And Polling

**Zone Signing Wizard** ✕

**Signing and Polling Parameters**  
Configure values for DNSSEC signing and polling.



DS record generation algorithm:

DS record TTL (seconds):

DNSKEY record TTL (seconds):

Secure delegation polling period (hours):

Signature inception (hours):

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

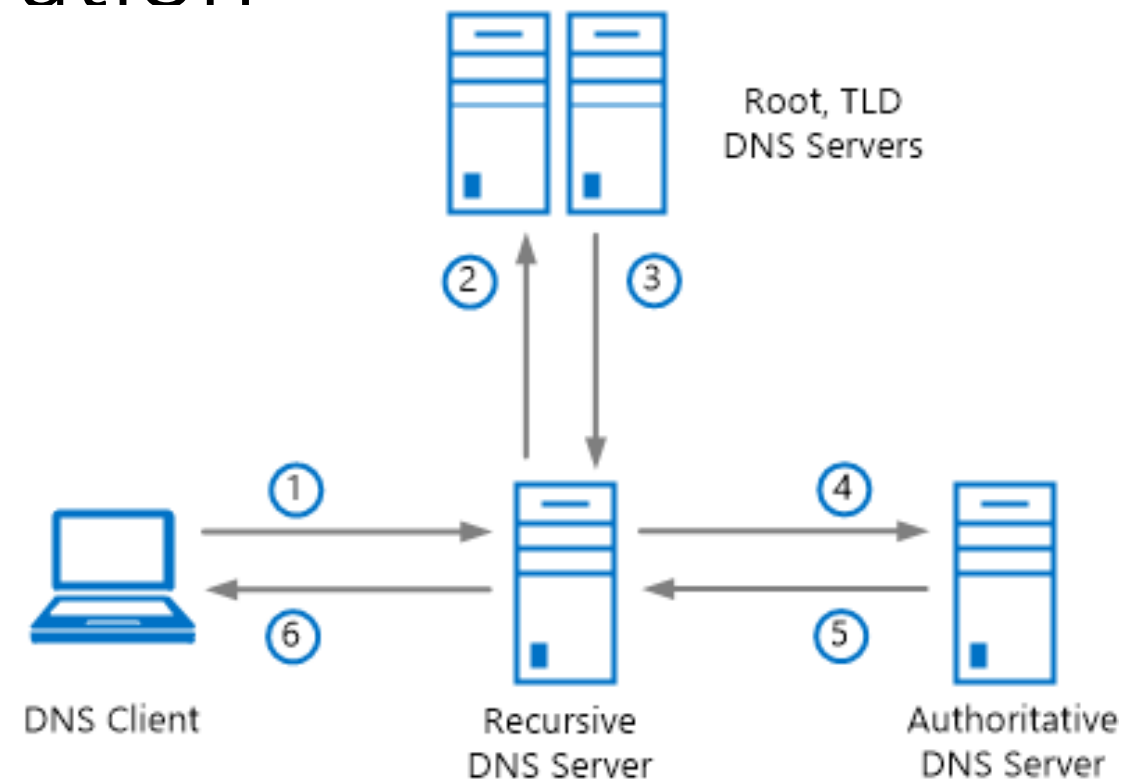
- `Import-DnsServerTrustAnchor -KeySetFile "\\File1\DNSKeys\keyset-secure.contoso.com"`

## Add Root Trust Anchor

- `Add-DnsServerTrustAnchor -Root`

# Verify DNSSEC: Demonstration

Step	Query-response	Optional DNSSEC data
1	A DNS client sends a DNS query to a recursive DNS server.	The DNS client can indicate that it is DNSSEC-aware (DO=1).
2	The recursive DNS server sends a DNS query to the root and top-level domain (TLD) DNS servers.	The recursive DNS server can indicate that it is DNSSEC-aware (DO=1).
3	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.	Authoritative servers for the parent zone can indicate that the child zone is signed using DNSSEC and include a secure delegation (DS record).
4	The recursive DNS server sends a DNS query to the authoritative DNS server for the zone.	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.
5	The authoritative DNS server returns a DNS response to the recursive DNS server, providing the resource record data.	The authoritative DNS server can include DNSSEC signatures in the form of RRSIG records in the DNS response, for use in validation.
6	The recursive DNS server returns a DNS response to the DNS client, providing the resource record data.	The recursive DNS server can indicate whether or not the DNS response was validated (AD=1) using DNSSEC.



# Thank You

For more details visit:

[https://technet.microsoft.com/en-us/library/dn593694\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn593694(v=ws.11).aspx)