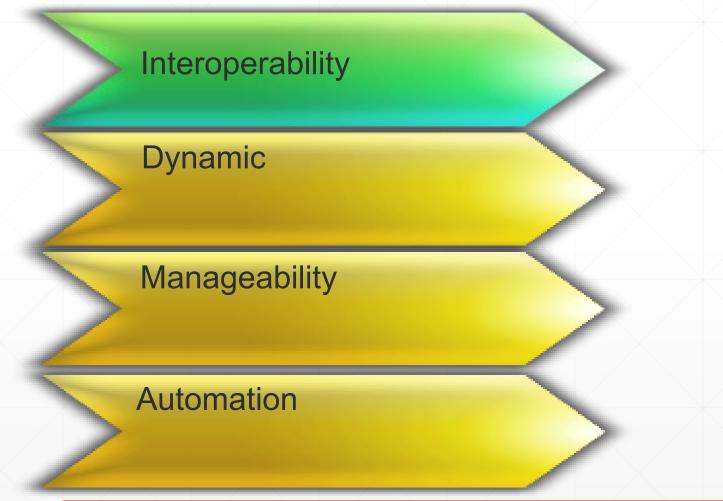
Kumar Ashutosh, Microsoft

Windows DNS Server

- Widely deployed in enterprises
- Fair presence in the DNS resolver space
- Standards compliant and interoperable
- Secure and scalable

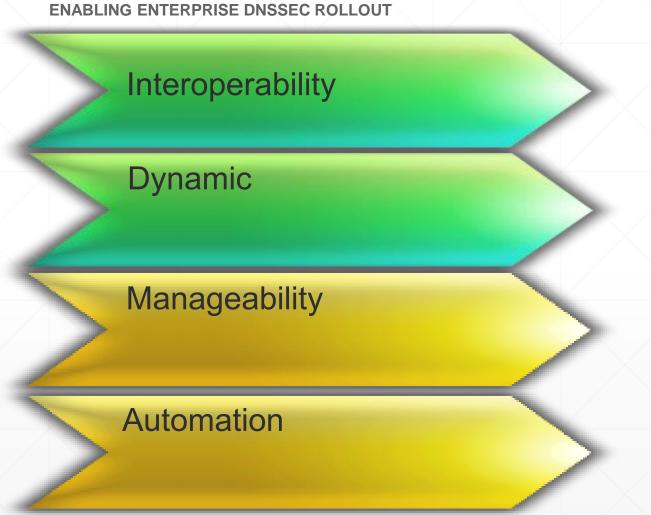
- Microsoft introduced support for DNSSEC in Windows 2008 R2…
 - Ability to sign zones offline and host signed zones
 - Validation of signed responses
 - Support for NSEC

ENABLING ENTERPRISE DNSSEC ROLLOUT

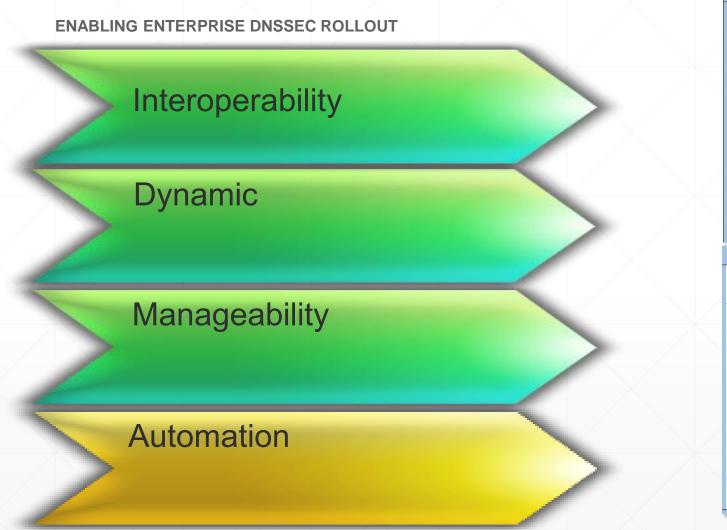


Latest RFCs

- 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



File Action View Help Image: State of Action View Help Image: State of Authority (SOA) [282], dc02.corp.contex Image: State of Authority (SOA) Image: State of Authority (SOA) [282], dc02.corp.contex dc02.corp.contex Image: State of Authority (SOA) Image: State of Authority (SOA) Image: State of Authority (SOA) (282], dc02.corp.contex Image: State of Authority (SOA) Image: State of Authority (SOA) Image: State of Authority (SOA) (282], dc02.corp.contex Image: State of Authority (SOA) Image: State of Authority (SOA) Image: State of Authority (SOA) (282], dc02.corp.contex Image: State of Authority (SOA) Image: State of Authority (SOA) Image: State of Authority (SOA) (282], dc02.corp.contex Image: State of Authority (SOA) Image: State o	*	D	NS Manag	er	I
DNS Name Type Data Image: Second					
NMS Type Data Image: Source of the options to sign the zone:	🤙 🔿 🎽 📰 🗶 🖻 🗔 📑		- Fi		
Image: Construction of the properties of the properti				Time	Dete
Forward Lockup Zones				Туре	Data
Image: contros oconsection in the properties of the p					
Image: Server Data File Folder) Name Server (NS) (d2.corp.contros.cord) New Hot (A or AAAA) Folder) Name Server (NS) (d2.corp.contros.cord) New Hot (A or AAAA) Folder) Name Server (NS) (d2.corp.contros.cord) New Hot (A or AAAA) Folder) Host (A) 192168.0.2 New Alias (CNAMB) Host (A) 192168.0.2 192168.0.3 New Hoil Exchanger (MX) Host (A) 192168.0.3 192168.0.3 New Hoil Exchanger (MX) Host (A) 192168.0.3 192168.0.3 New Hoil Exchanger (MX) Unsign the Zone 192168.0.3 192168.0.3 New Dornain Host (A) 192168.0.3 192168.0.3 New Dornain Host (A) 192168.0.3 192168.0.3 New Dornain Worster New Secords 192168.0.3 192168.0.3 Nusser Commer Secords Nusser New Secords 192168.0.3 192168.0.3 Nusser Secords Nusser New Secords 192168.0.3 192168.0.3 Commer Secords Nusser New Secords 192168.0.3 192168.0.3 Configure the zone signing parameters New Secords 1921					
Windowskie Communications Windowskie folder Stat of Authority (SOA) [282], do2.corp.contesis.c	þ 打 bar.com				
Update Server Data File if older) Stat of Authority (SOA) [282], dc02.corp.conteso.cod New Host (A or AAAA) folder) Name Server (NS) dc02.corp.conteso.cod New Mail Exchanger (MX) folder) Name Server (NS) dc01.corp.conteso.cod New Mail Exchanger (MX) folder) Host (A) 192168.0.2 New Mail Exchanger (MX) Host (A) 192168.0.2 idde.corp.conteso.cod New Delegation Host (A) 192168.0.134 idde.corp.conteso.cod Other New Records Host (A) 192168.0.2 idde.corp.conteso.cod Other New Records Host (A) 192168.0.134 idde.corp.conteso.cod Other New Records Host (A) 192168.0.2 idde.corp.conteso.cod Other New Records Host (A) 192168.0.2 idde.corp.conteso.cod Other New Records Using the Zone 192168.0.2 idde.corp.conteso		DomainDnsZc	ones		
Reload tolder) Start of Authority (SOA) (282), dd2.corp.contoso.cor New Host (A or AAAA) tolder) Name Server (NS) dd0.corp.contoso.cor New Alits (CNAME) tolder) Host (A) 192168.0.2 New Mail Exchanger (MX) tolder) Host (A) 192168.0.13 New Mail Exchanger (MX) tolder) Host (A) 192168.0.13 New Delegation Host (A) 192168.0.2 192168.0.2 Other New Records Host (A) 192168.0.3 192168.0.3 New Delegation Other New Records 192168.0.5 192168.0.5 DNSSEC Sign the Zone 192168.0.5 192168.0.5 DNSSEC Sign the Zone 192168.0.5 192168.0.5 New Delegation Unsign the Zone 192168.0.5 192168.0.5 DNSSEC Sign the Zone 192168.0.5 192168.0.5 Sign to configure the sone signing options. Sign to configure the zone signing parameters 192168.0.5 Configure the zone signing parameters Creates a new set of zone signing parameters Creates a new set of zone signing parameters Sign the zone using parameters from an existing signed zone Zone Nam		a File			
New Host (A or AAAA) tfolder) Name Server (NS) dd02.corp.contoso.cor New Alias (CNAME) tfolder) Name Server (NS) dd01.corp.contoso.cor New Mail Exchanger (MX) tfolder) Host (A) 192168.0.3 New Domain Host (A) 192168.0.3 192168.0.3 New Delgation Host (A) 192168.0.3 192168.0.3 Other New Records Host (A) 192168.0.3 192168.0.3 Mew Johnson Unsign the Zone 192168.0.3 192168.0.3 Mew Johnson Sign the Zone 192168.0.3 192168.0.3 Mew Johnson Unsign the Zone 192168.0.3 192168.0.3 Mew Johnson Exerce Signing parameters Sign the Zone signing parameters Sign the zone signing parameters <			t folder)		[282], dc02.corp.contc
New Alias (CNAME) troider) Name server (ns) ubd1.comp.com/sob.com New Mailas (CNAME) troider) Host (A) 192168.0.2 New Domain Host (A) 192168.0.34 New Delegation Host (A) 192168.0.2 Other New Records Host (A) 192168.0.4 DNSSEC Sign the Zone 192168.0.4 DNSSEC Sign the Zone 192168.0.4 Properties 192168.0.4 192168.0.4 Properties 192168.0.4 192168.0.5 Sign the Zone 192168.0.4 192168.0.5 Properties 192168.0.4 192168.0.5 Sign the Zone 192168.0.5 192168.0.5 New New Records Unsign the Zone 192168.0.5 View Properties 192168.0.5 192168.0.5 Sign the Zone signing options. Sign the Zone signing parameters Sign the Zone signing parameters Sign the zone signing parameters Configure the zone signing parameters of an existing signed zone Zone Name: Signs the zone using percommended parameters Signs the zone using recommended parameters Signs the zone using recommended parameters Signs the				· · ·	
New Mail Exchanger (MX) folder) Host (A) 192168.0.6 New Domain Host (A) 192168.0.134 New Delegation Other New Records 192168.0.2 DNSSEC Sign the Zone 192168.0.3 DNSSEC Sign the Zone 192168.0.3 DNSSEC Unsign the Zone 192168.0.3 DNSSEC Bign 20ne 192168.0.3 View Properties 192168.0.3 DISSEC Bign 20ne 192168.0.3 View Host (A) 192168.0.3 DISSEC Bign 20ne 192168.0.3 View Host (A) 192168.0.3 DISSEC Bign the Zone 192168.0.3 Distant Example Host (A) 192168.0.3 Distant Wiew New		-			
New Domain Host (A) 192168.0134 New Delegation Other New Records 192168.0.6 DNSSEC Sign the Zone 192168.0.6 DNSSEC Sign the Zone 192168.0.6 New Delegation Unsign the Zone 192168.0.5 New Delegation New Delegation 192168.0.5 Sign Tom New Delegation 192168.0.5 New Delegation New Delegation 192168.0.5 Sign Tom New Delegation 192168.0.5 Sign Tom New Delegation 192168.0.5 Sign Tom New Delegation 192168.0.7 Componention New Delegation 192168.0.5 Sign Tom New Delegation 192168.0.5 Choose one of the options to sign the zone Creates a new set of zone signing parameters Creates a new set of zone signing parameters Cone Name: New Name New Name N					
Hew Outdati Host (A) 192168.014 New Delegation Other New Records 192168.0.6 DNSSEC Sign the Zone 192168.0.4 New View Unsign the Zone 192168.0.4 New View Properties 192168.0.4 New View New View New View New View Properties 192168.0.4 New View New View New View New View New View New View New View New View New View New View New View New View Sign to come of the options to sign the zone: Creates a new set of zone signing parameters Creates a new set of zone signing parameters Sign the zone with parameters of an existing zone Sign the zone using parameters from an existing signed zone Zone Name: Outer Name: New Yiew New Yiew New Yiew New Yiew Other Name: New Yiew New Yiew <t< td=""><th></th><td>Jer (MX)</td><td>t tolder)</td><td></td><td></td></t<>		Jer (MX)	t tolder)		
Wew Delegation Host (A) 192168.0.2 DNSEC Sign the Zone 192168.0.4 DVISIT Unsign the Zone 192168.0.4 DVISIT Host (A) 192168.0.5 DVISIT Host (A) 192168.0.5 DVISIT Host (A) 192168.0.5 DVISIT Host (A) 192168.0.7	P U				
Other New Records 192168.0.5 DNSSEC Sign the Zone Wiew Unsign the Zone Properties 192168.0.4 192168.0.7 192168.0.7 Sign Zone X Signing Options Image: Construction of the options to sign the zone The DNS server supports three signing options. Image: Configure the zone signing parameters Choose one of the options to sign the zone Creates a new set of zone signing parameters Creates a new set of zone signing parameters Signs the zone with parameters of an existing zone Signs the zone using parameters from an existing signed zone Zone Name: Use recommended settings to sign the zone Signs the zone using recommended parameters Signs the zone using recommended parameters Signs the zone using recommended parameters	. 4				
DNSSEC ign the Zone 192168.0.3 All Tasks Unsign the Zone 192168.0.4 View Properties 192168.0.7 Sign to EXAMPLE Host (A) 192168.0.7 Signing Options Image: Configure the zone signing options. Image: Configure the zone signing parameters Choose one of the options to sign the zone: Configure the zone signing parameters Creates a new set of zone signing parameters Sign the zone with parameters of an existing zone Signs the zone with parameters of an existing signed zone Zone Name: Image: Construction of the cone using recommended parameters Signs the zone using recommended parameters		ls			
Image: Normalized Structure Properties 192168.0.5 View Properties 192168.0.7 Sign zone Signing Options The DNS server supports three signing options. Choose one of the options to sign the zone: Choose one of the options to sign the zone: Configure the zone signing parameters Creates a new set of zone signing parameters Creates a new set of zone signing parameters Signs the zone with parameters of an existing zone Signs the zone using parameters from an existing signed zone Zone Name: Image: Signs the zone using recommended parameters Signs the zone using recommended parameters Signs the zone using recommended parameters	DNSSEC	•	Sign th	e Zone	
View Host (A) 192.168.0.7 Sign zone X Signing Options Image: Configure the signing options. Choose one of the options to sign the zone: Configure the zone signing parameters Creates a new set of zone signing parameters Creates a new set of zone signing parameters Signs the zone with parameters of an existing zone Signs the zone using parameters from an existing signed zone Zone Name: Image: Construction of the zone using recommended parameters Signs the zone using recommended parameters Signs the zone using recommended parameters	All Tasks	•	Unsign	the Zone	192.168.0.4
Host (A) 192:168.0.7 Sign zone Signing Options The DNS server supports three signing options. Choose one of the options to sign the zone: Choose one of the options to sign the zone: Configure the zone signing parameters Creates a new set of zone signing parameters Creates a new set of zone signing parameters Sign the zone with parameters of an existing zone Signs the zone using parameters from an existing signed zone Zone Name: Image: Image:	▶ 💼 🤇 Minur		Proper	ties	192.168.0.5
Signing Options The DNS server supports three signing options. Choose one of the options to sign the zone: Configure the zone signing parameters Creates a new set of zone signing parameters Sign the zone with parameters of an existing zone Signs the zone using parameters from an existing signed zone Zone Name: Image:	view			Host (A)	192.168.0.7
 Configure the zone signing parameters Creates a new set of zone signing parameters Sign the zone with parameters of an existing zone Signs the zone using parameters from an existing signed zone Zone Name: Use recommended settings to sign the zone Signs the zone using recommended parameters 					
Creates a new set of zone signing parameters Sign the zone with parameters of an existing zone Signs the zone using parameters from an existing signed zone Zone Name: Signs the zone using recommended parameters Signs the zone using recommended parameters		-			
 Sign the zone with parameters of an existing zone Signs the zone using parameters from an existing signed zone Zone Name: Use recommended settings to sign the zone Signs the zone using recommended parameters 					
Signs the zone using parameters from an existing signed zone Zone Name: © Use recommended settings to sign the zone Signs the zone using recommended parameters					
Zone Name: (Use recommended settings to sign the zone Signs the zone using recommended parameters			-		
Signs the zone using recommended parameters	Zone Name	;			
	Use recommended s	ettings to sign the	e zone		
< Back Next > Cancel	Signs the zone u	sing recommended	d parameters	4	
< Back Next > Cancel					
< Back Next > Cancel					
				< Back Next	> Cancel

Complete Powershell Support

ENABLING ENTERPRISE DNSSEC ROLLOUT

Interoperability

Dynamic

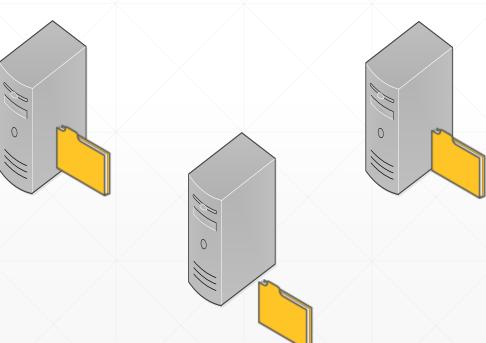
Manageability

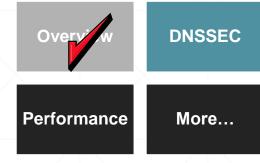
Automation

- 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

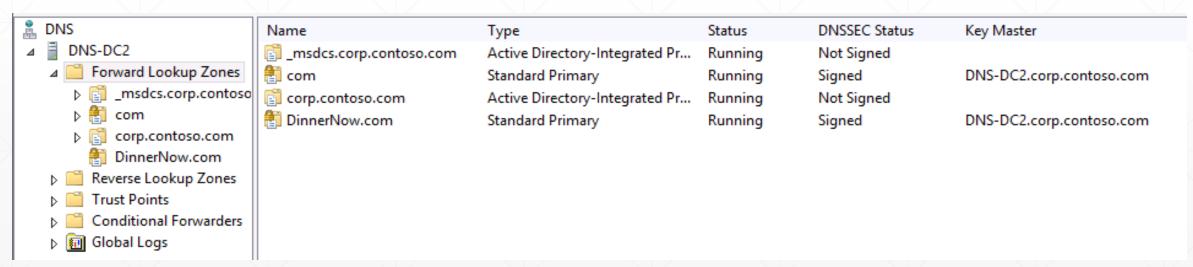
DNSSEC

More...

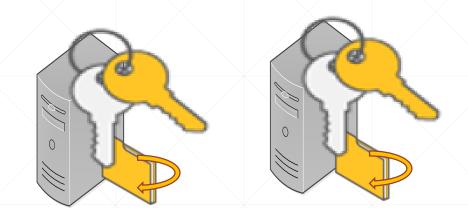
Over

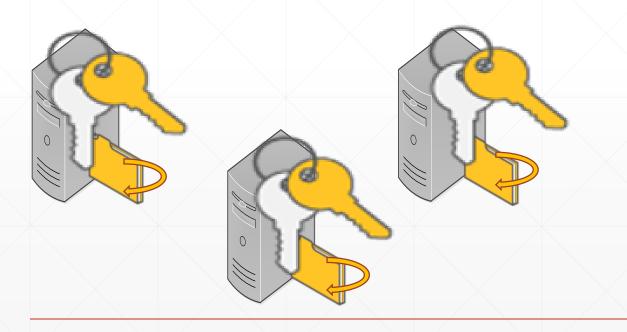
Performance

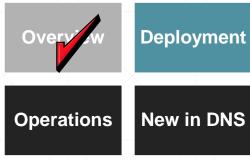
- Administrator designates one server to be the key master
 - First DNSSEC server becomes



Signing entire zone

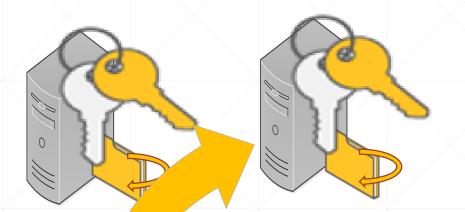


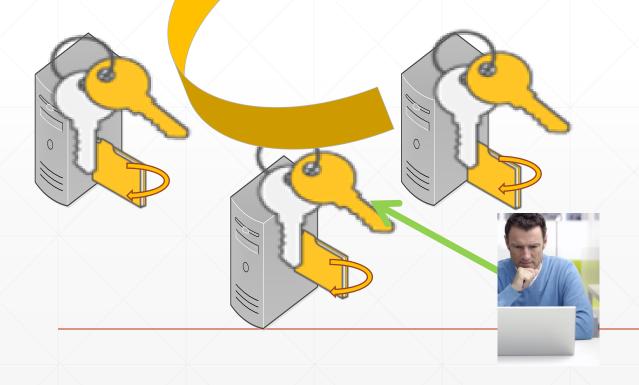


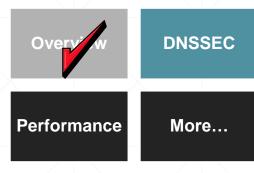


- Private zone signing keys replicate automatically to all DCs hosting the zone through AD replication
- Each zone owner signs its own copy of the zone when it receives the key
 - Only Server 2012+ DCs will sign their copy of the zone

Updating zone data

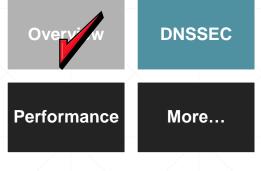






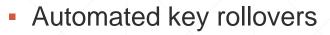
- 1. Client sends dynamic update to any authoritative DNS server
- 2. That DNS server updates its own copy of the zone and generates signatures
- 3. The *unsigned* update is replicated to all other authoritative servers
- 4. Each DNS server adds the update to its copy of the zone and generates signatures
- 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



- 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

DNSSEC

More...

Performance



© 2012 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.