Microsoft

Windows DNS Server
DNSSEC support and Performance

Kumar Ashutosh
Microsoft Corporation

Agenda

Overview

DNSSEC

Performance

More…

Overview

Windows DNS Footprint

- Widely deployed in enterprises
- Fair presence in the DNS resolver space
- The Windows DNS Client is ubiquitous

Standards and Interoperability

- A RFC compliant DNS Server
- Interoperable with other DNS Server implementations
  - Because the DNS Server service is RFC-compliant and it can use standard DNS data file and resource record formats, it can successfully work with most other DNS server implementations, such as those that use BIND software.

Ease of Use

- Graphical User Interface
- Full scripting support via Powershell
- Dnscmd
- IPAM integration for A/AAAA record management

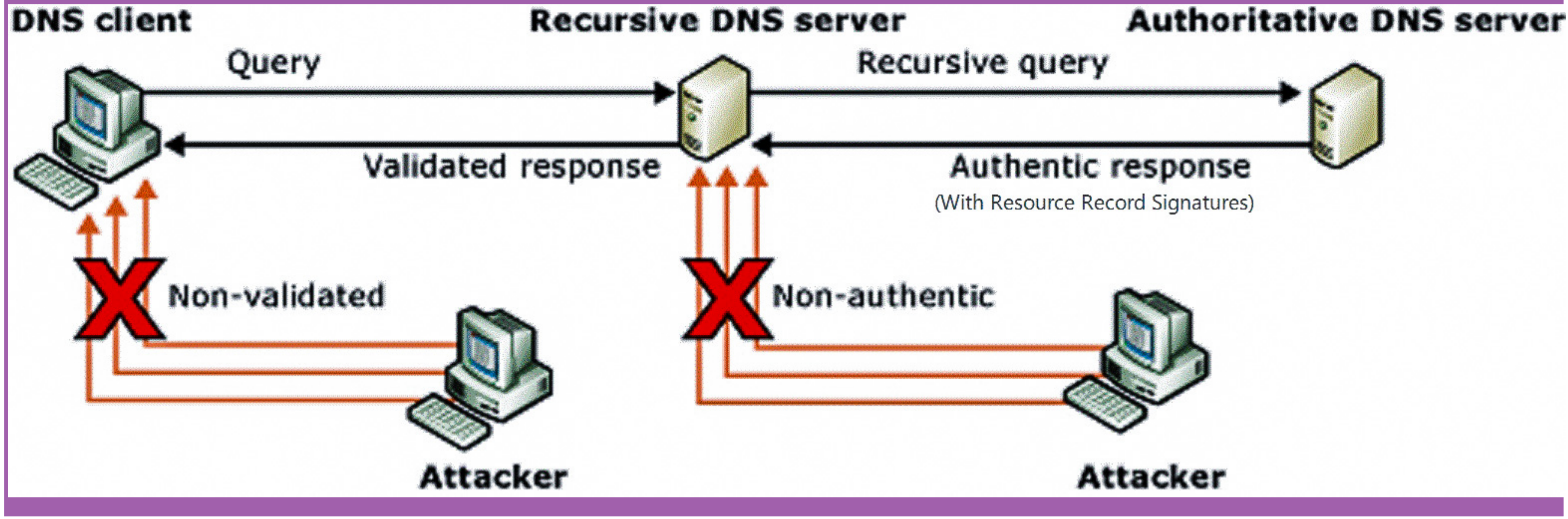
More Features

- Conditional Forwarding
  - A conditional forwarder is a DNS server on a network that forwards DNS queries according to the DNS domain name in the query.
- Stub Zones
  - A stub zone is a copy of a zone that contains only those resource records that are necessary to identify the authoritative DNS servers for that zone. A stub zone keeps a DNS server that hosts a parent zone updated with the authoritative DNS servers for its child zone. This helps maintain DNS name resolution efficiency
- Zone Transfers
  - AXFR and IXFR

More Features

- Dynamic Update
  - Integrated with DHCP
  - Secure dynamic updates in AD environment
- Dynamic re-ordering of forwarders
  - Server now picks the forwarder that is responsive over the ones that are not responsive
  - Basically, unresponsive forwarders are dropped to the bottom of the list for successive queries
- WINS and DNSSEC coexistence

DNSSEC


DNS client
Recursive DNS server
Authoritative DNS server
Query
Recursive query
Validated response
Authentic response
(With Resource Record Signatures)
Non-validated
Non-authentic
Attacker
Attacker

DNSSEC in Windows

Overview ✓ | DNSSEC
Performance | More…

- 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 Server 2012 R2

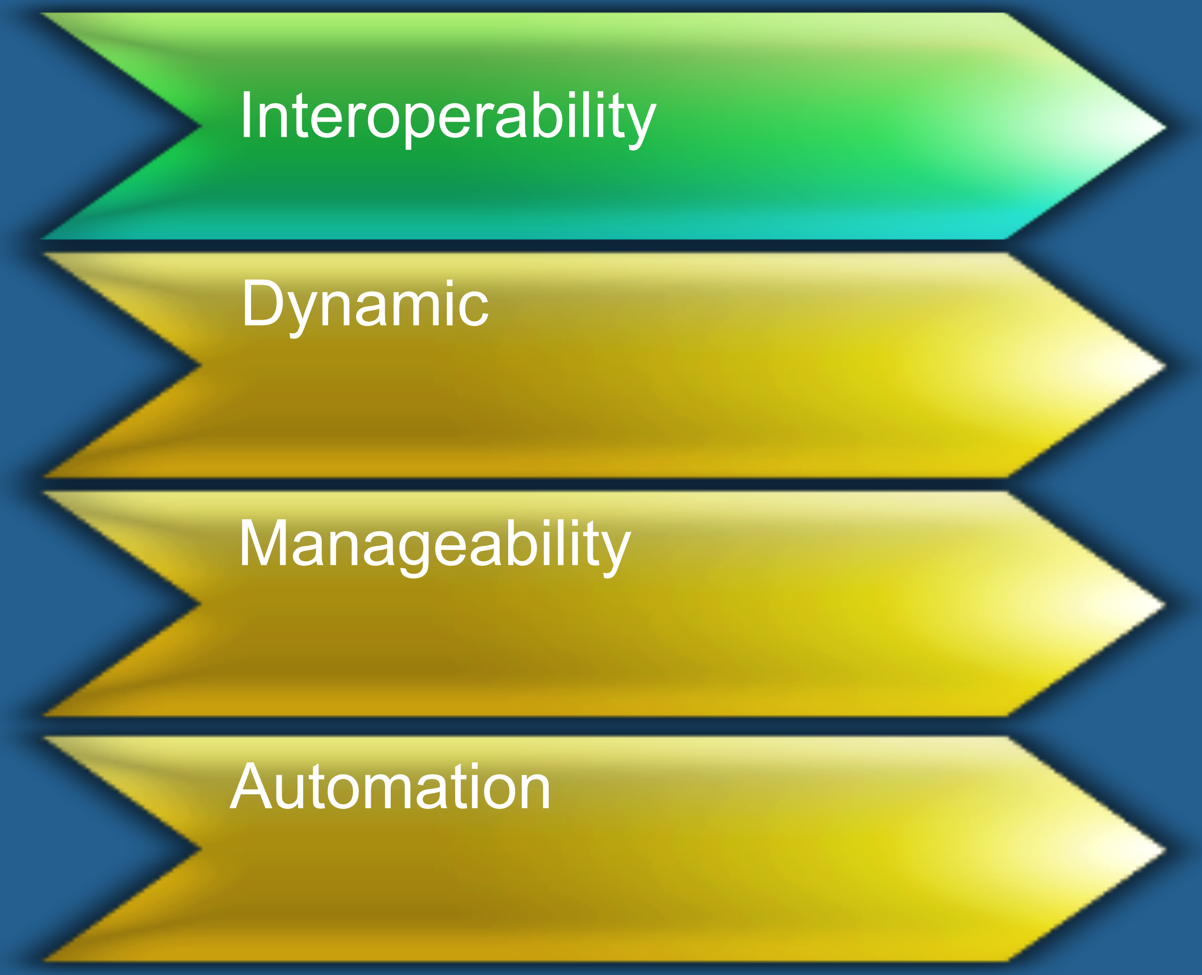
Overview ✓

DNSSEC

Performance

More…

ENABLING ENTERPRISE DNSSEC ROLLOUT



Interoperability

Dynamic

Manageability

Automation

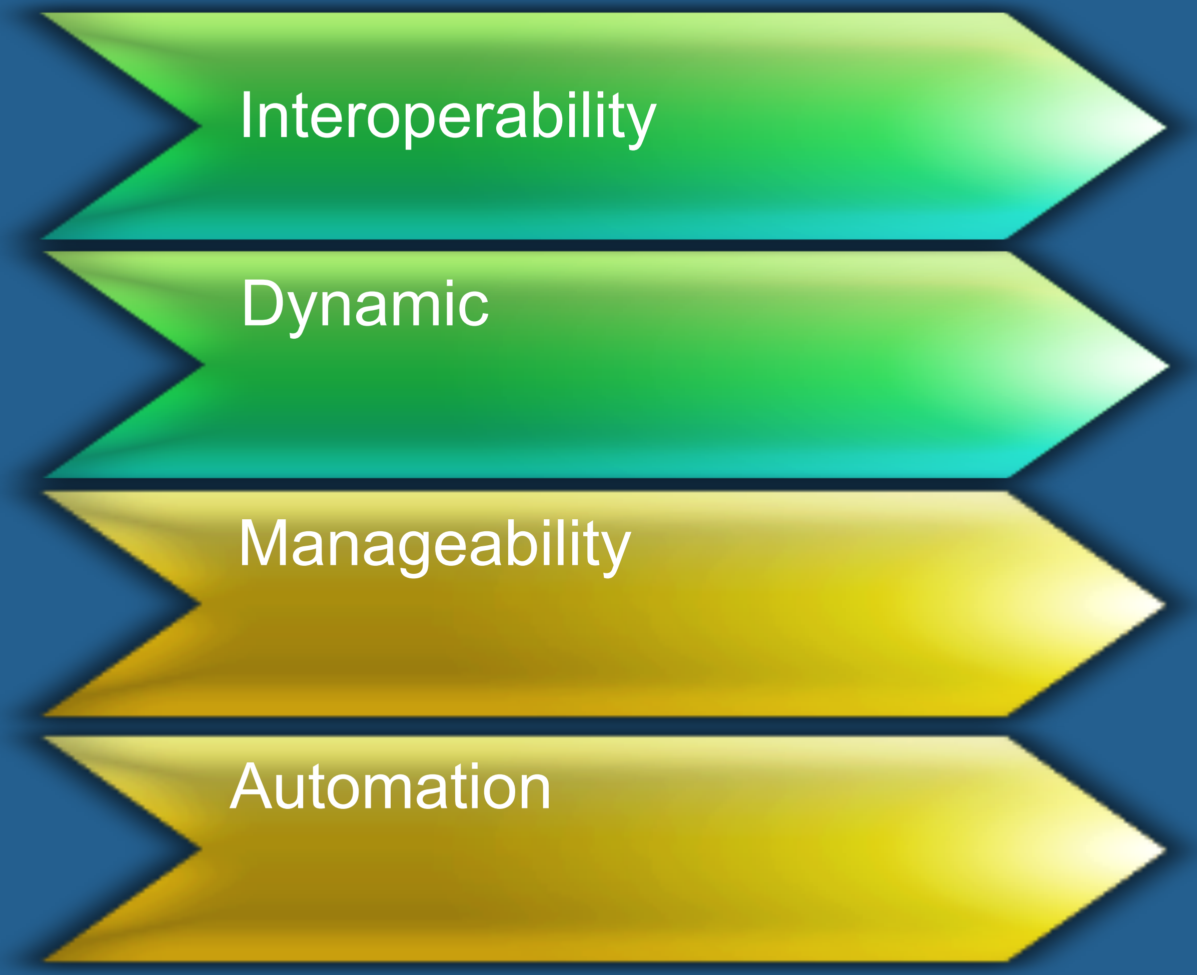
- Latest RFCs
  - NSEC3 Support
  - RSA/SHA-2, ECDSA Signing
  - Automated Trust Anchor rollover
- Support for 3rd Party Key Management

DNSSEC in Windows Server 2012 R2

Overview ✓ | DNSSEC

Performance | More…

ENABLING ENTERPRISE DNSSEC ROLLOUT



- 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 Server 2012 R2

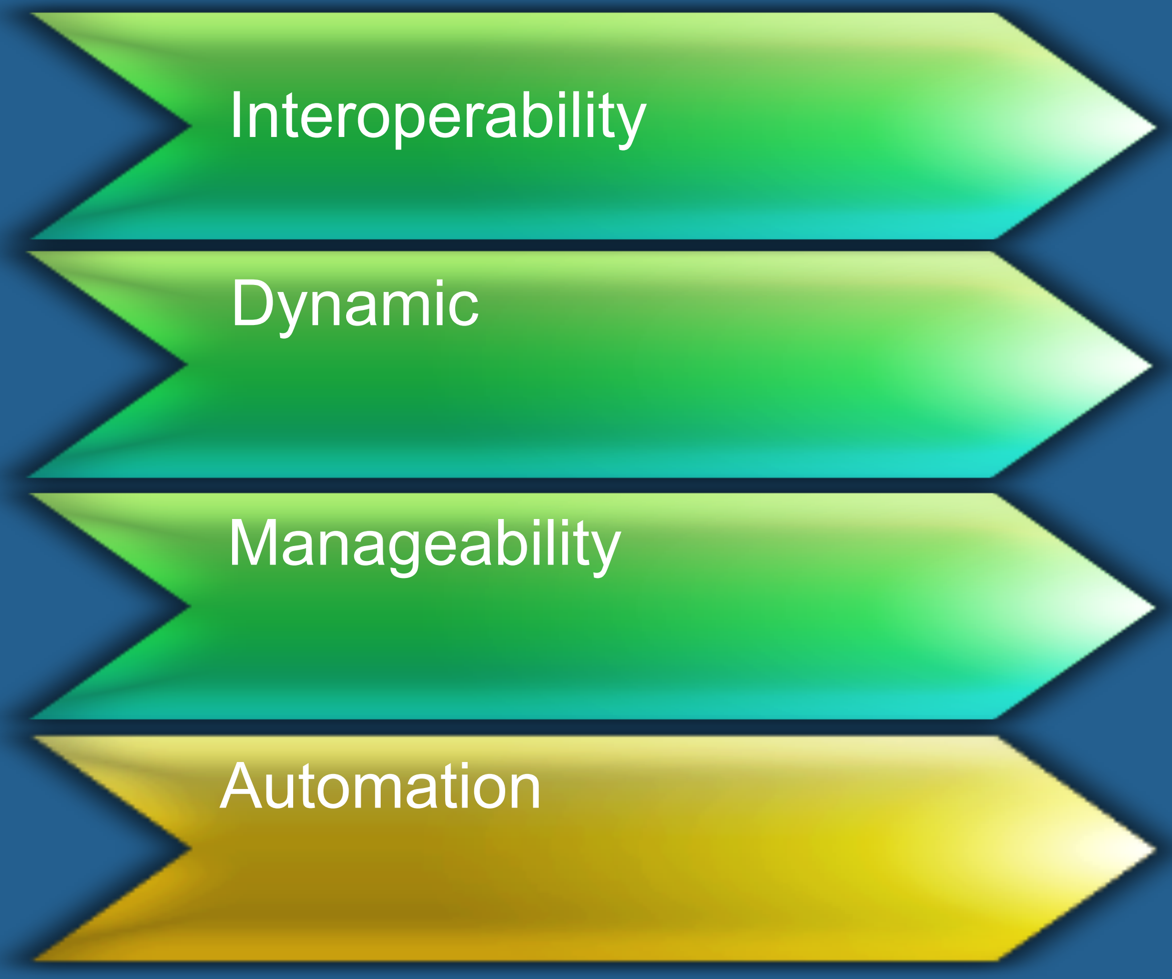
Overview ✓

DNSSEC

Performance

More…

ENABLING ENTERPRISE DNSSEC ROLLOUT

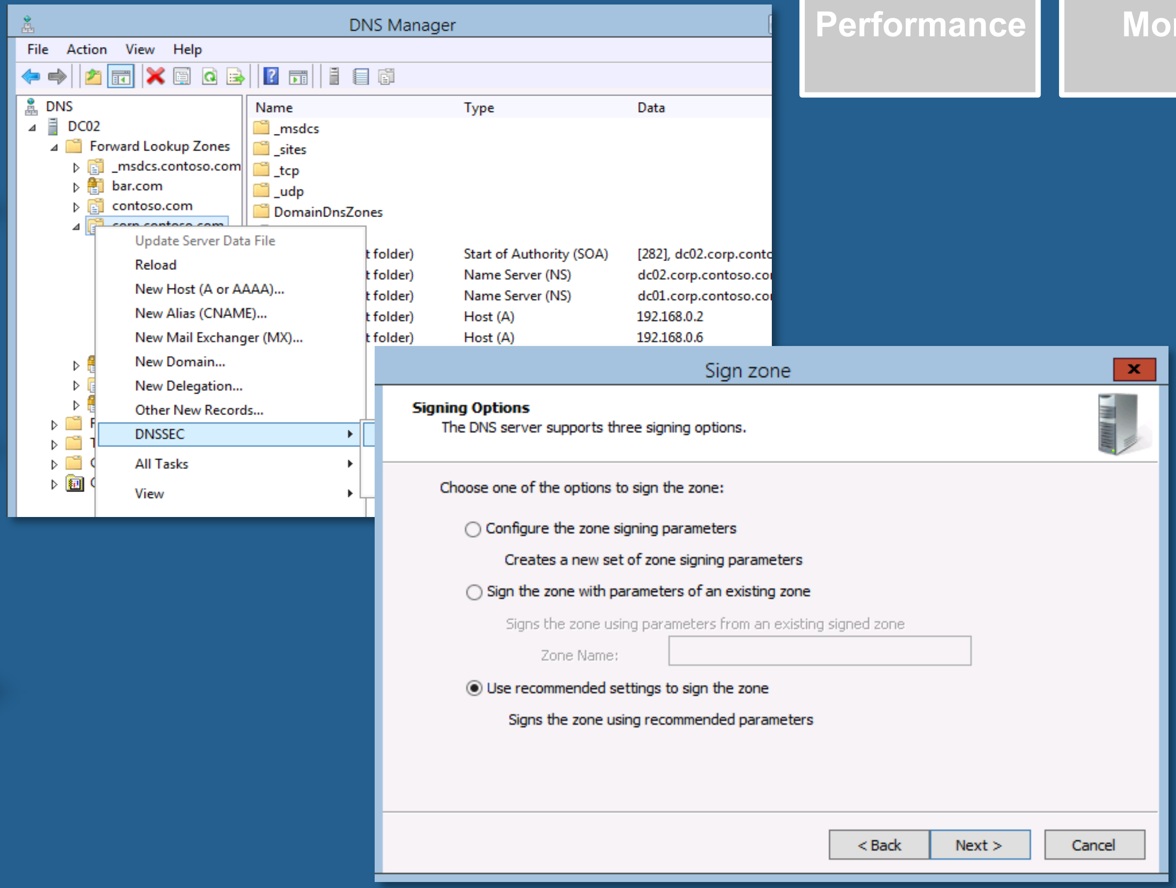


Interoperability

Dynamic

Manageability

Automation



Sign zone

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:

● Use recommended settings to sign the zone

Signs the zone using recommended parameters

< Back | Next > | Cancel

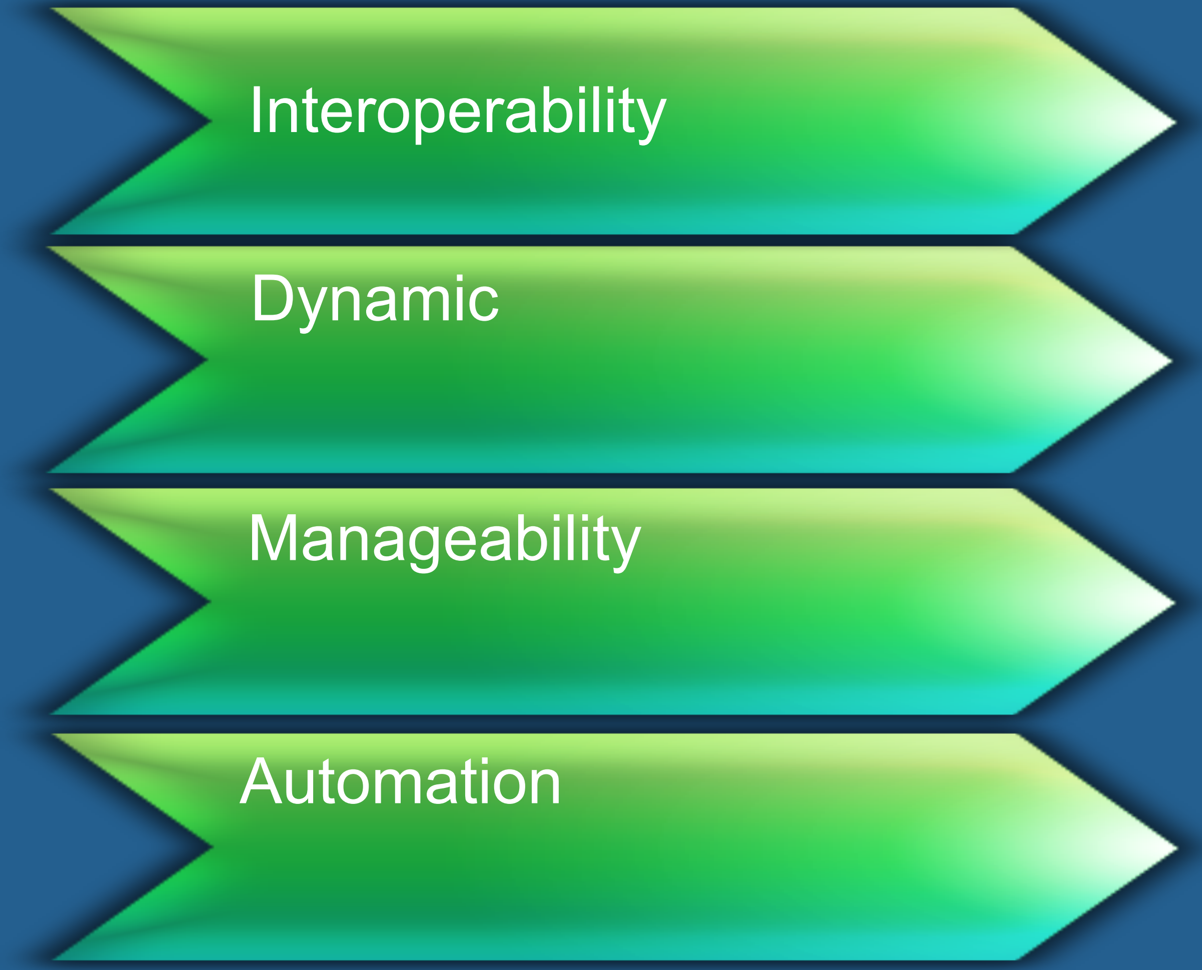
Complete Powershell Support

DNSSEC in Windows Server 2012 R2

Overview ✓ | DNSSEC

Performance | More…

ENABLING ENTERPRISE DNSSEC ROLLOUT



Interoperability

Dynamic

Manageability

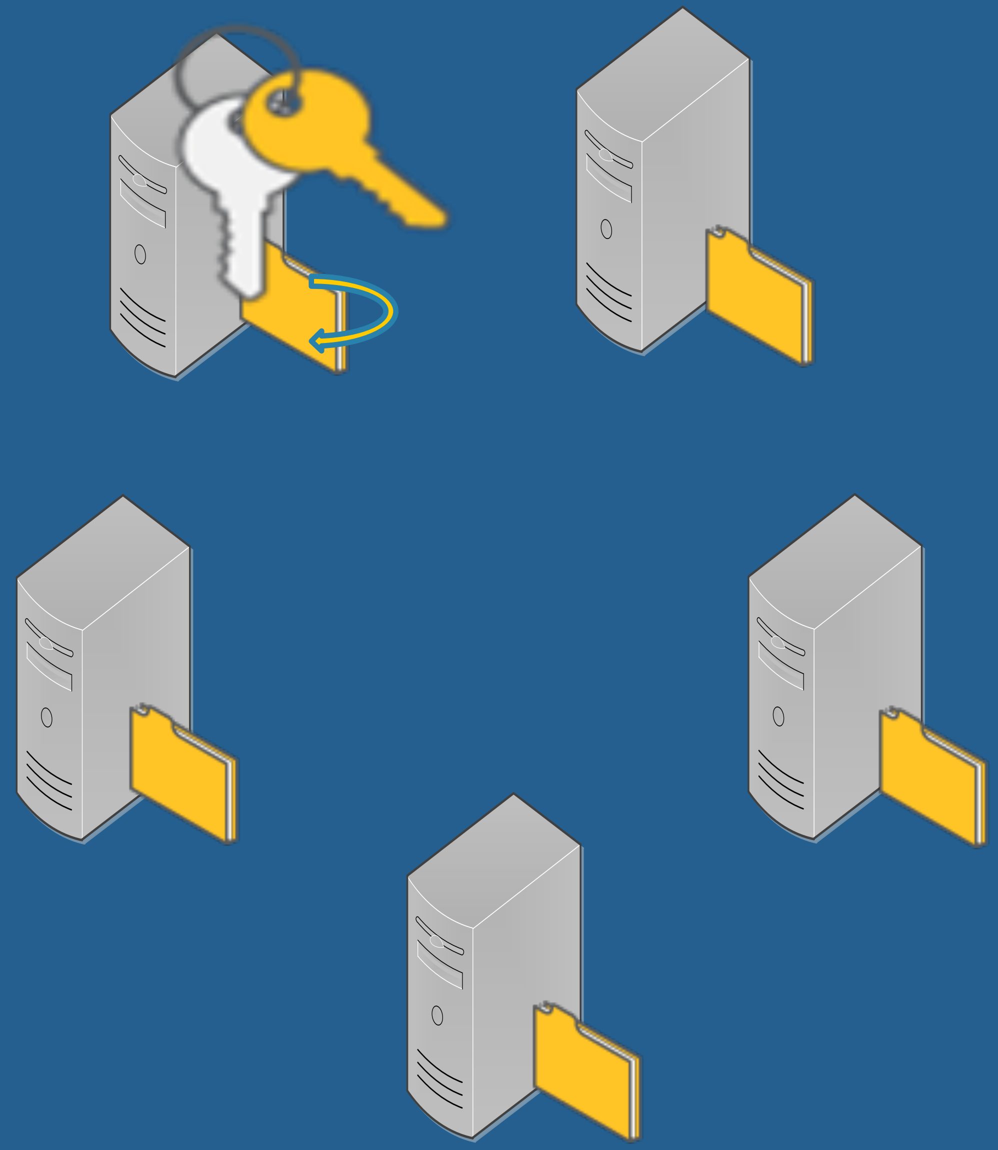
Automation

- 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

Overview ✓ | DNSSEC

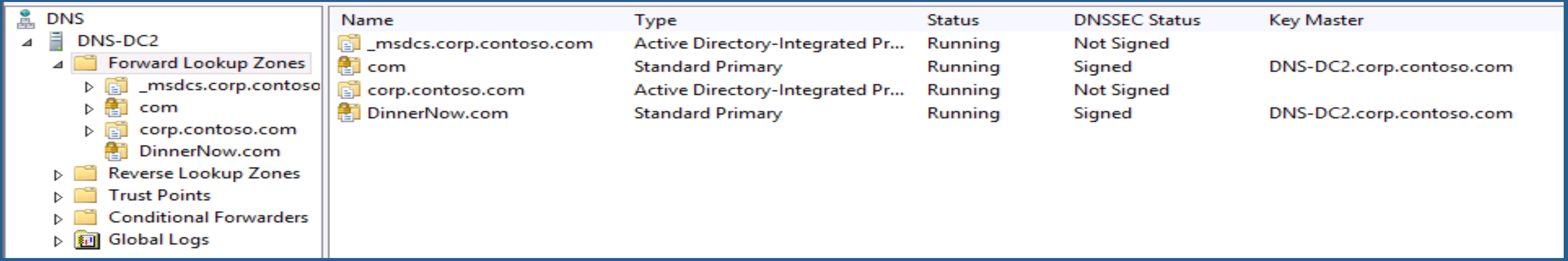
Performance | More…



- 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 KM



Name	Type	Status	DNSSEC Status	Key Master
_msdcs.corp.contoso.com	Active Directory-Integrated Pr...	Running	Not Signed	
com	Standard Primary	Running	Signed	DNS-DC2.corp.contoso.com
corp.contoso.com	Active Directory-Integrated Pr...	Running	Not Signed	
DinnerNow.com	Standard Primary	Running	Signed	DNS-DC2.corp.contoso.com

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

Overview ✓
DNSSEC
Performance
More…

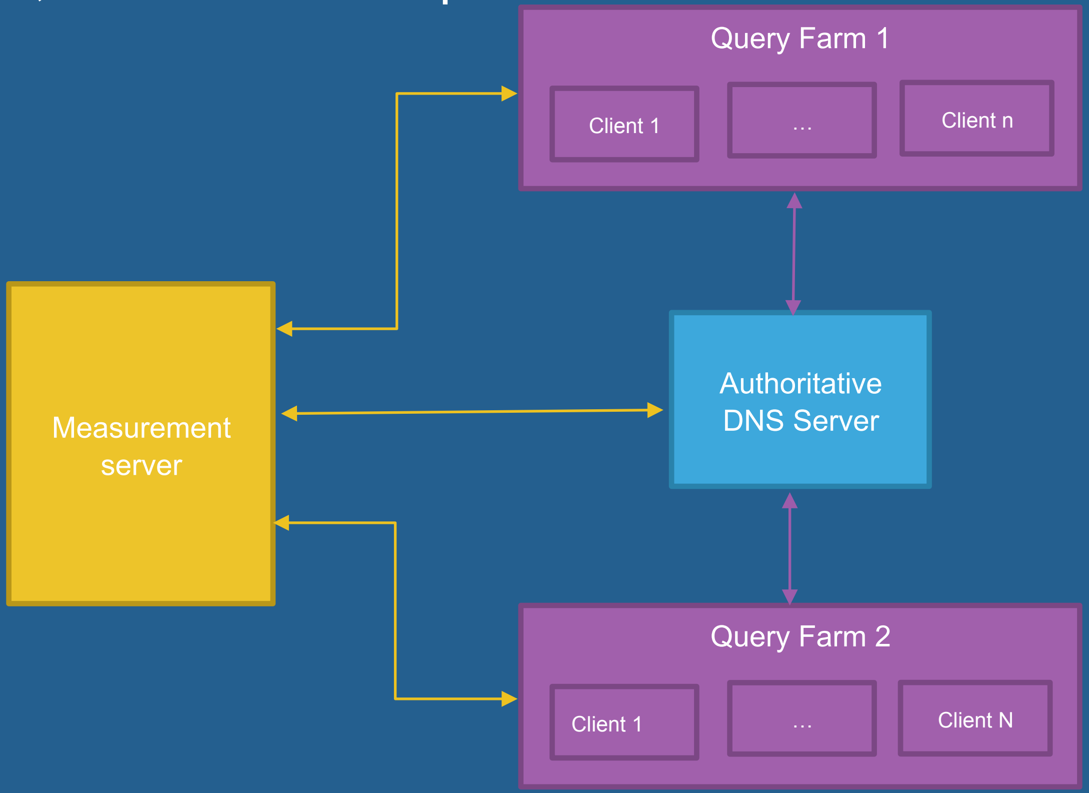
- Automated key rollovers
  - Key rollover frequency is configured per zone
  - Key master automatically generates new keys
  - Secure delegations from the parent are also automatically updated
  - Manual Rollovers are also available

- 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

Performance

DNS performance-Test Model

- Multiple Client Query Farms: Each client in these farms sends randomized queries (+ve and -ve) to the auth server. Each farm publishes its query sent/ query received counts
- Authoritative server : Publishes its query sent/query received counts
- Measurement server : Observes these counts and collects statistics.
- 5 zones, 100K A records per zone



Processor(s):	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	
	Maximum speed:	2.30 GHz
	Sockets:	2
	Cores:	12
	Logical processors:	24
	Virtualization:	Enabled
	L1 cache:	768 KB
	L2 cache:	3.0 MB
	L3 cache:	30.0 MB
Total Physical Memory:	80 GB	
Network Card(s):	Broadcom NetXtreme Gigabit Ethernet	

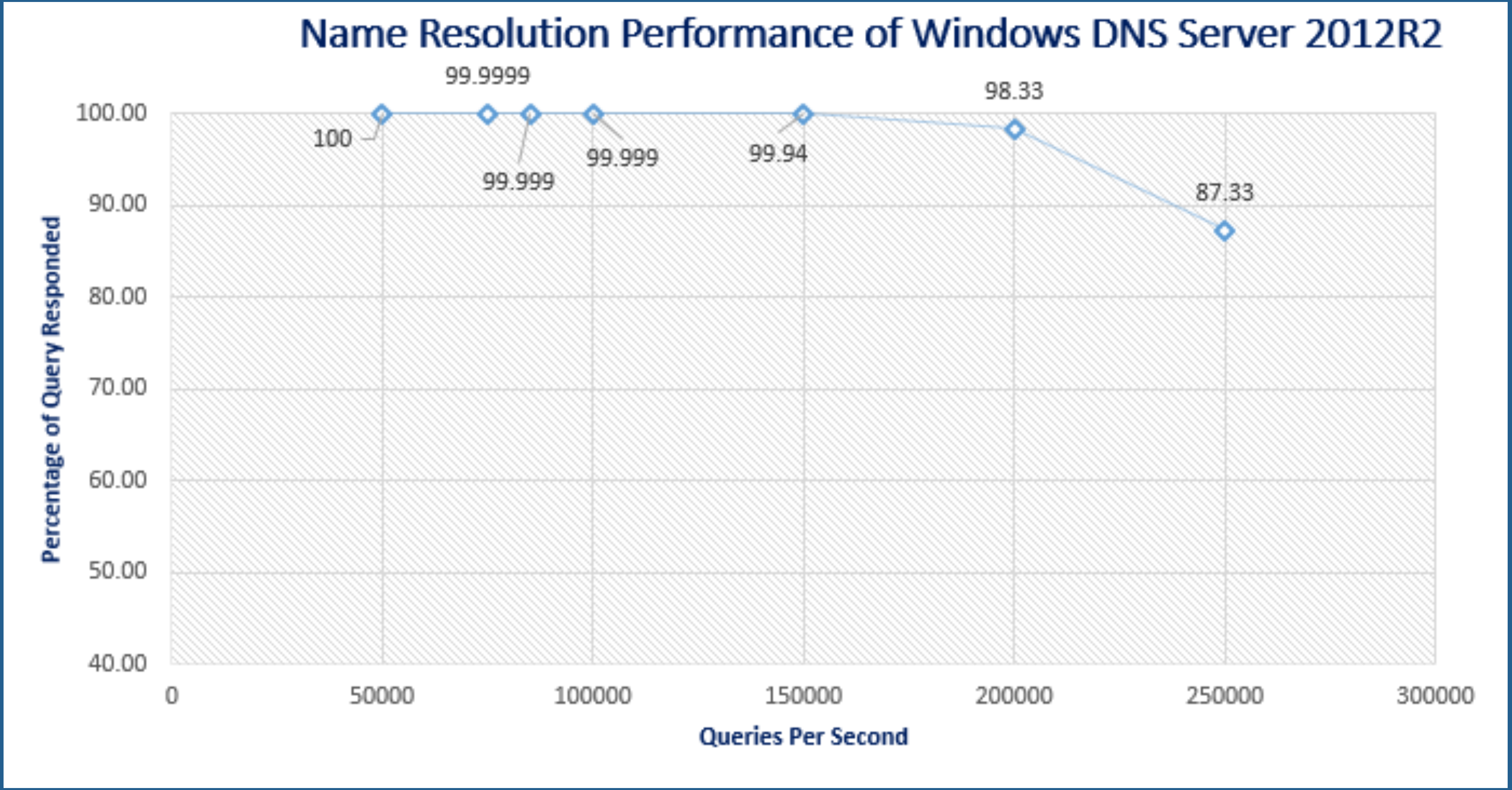
DNS performance

Overview ✓

DNSSEC ✓

Performance

More…



DNSSEC performance

- The DNSSEC performance for authoritative server with signed zones is similar to a server with unsigned zones
- The data transmitted is however larger and hence more network throughput is required.

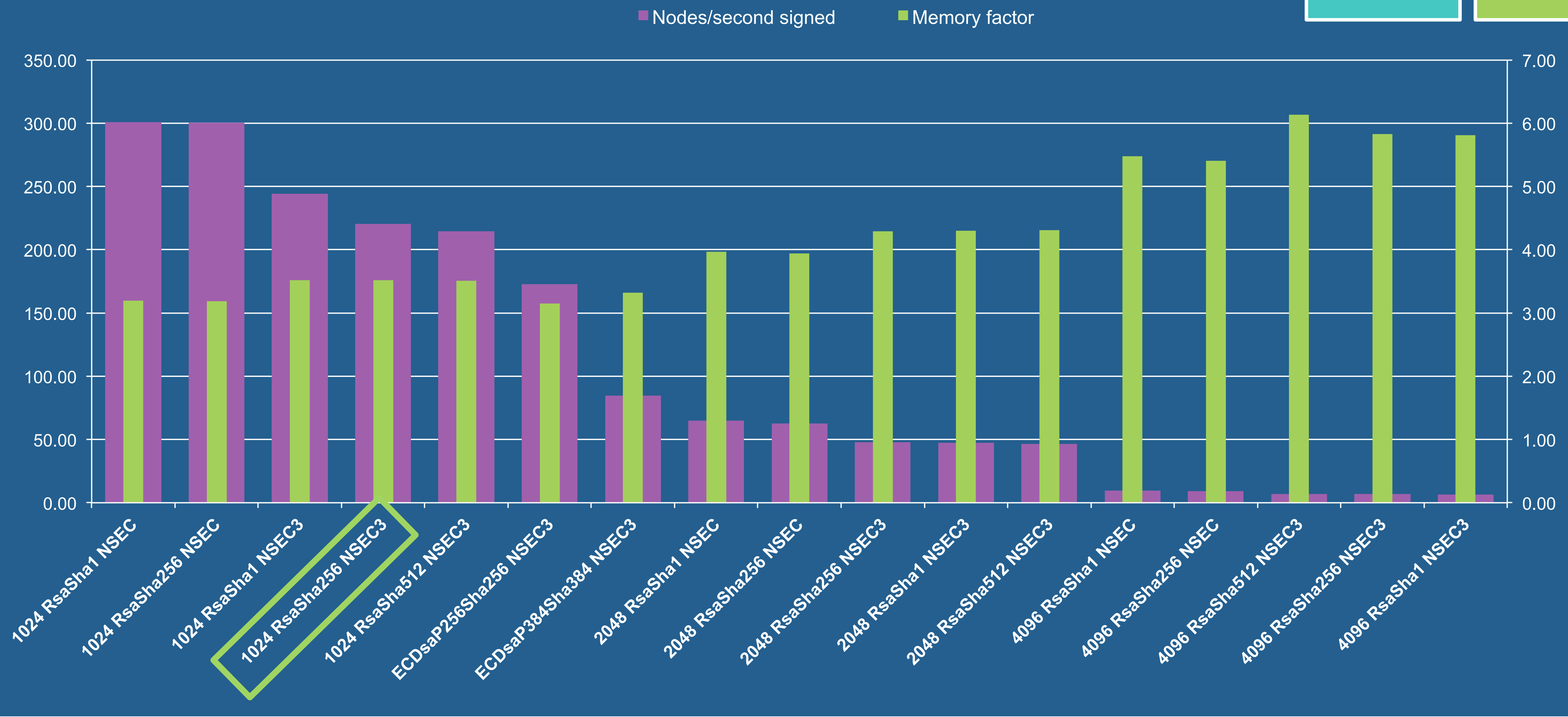
DNSSEC signing performance

Overview ✓

DNSSEC ✓

Performance

More…



Tuning DNS Server for performance

Following slides are recommendations based on a server with following configuration. The setting may differ from hardware to hardware:

Processor(s):Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz (Dell PowerEdge R720)

Maximum speed	:	2.30 GHz
Sockets	:	2
Cores	:	12
Logical processors	:	12
Virtualization	:	Disabled
L1 cache	:	768 KB
L2 cache	:	3.0 MB
L3 cache	:	30.0 MB

Total Physical Memory:	80 GB
Network Card(s):	Broadcom NetXtreme Gigabit Ethernet

Tuning DNS Server for performance

Firewall

- For serving queries at high rate, explicitly enable below firewall rule

```
New-NetFirewallRule -DisplayName <String> -Direction Inbound -Action Allow -Protocol UDP -LocalPort 53 -LocalOnlyMapping $true -Enabled True
```

- Enabling this rule is recommended for authoritative and resolver server and does not require service/server restart
- Ensure below firewall rules are present and enabled (created at time of server role installation)
  - Firewall rule for DNS process to send outbound communication should be set to allowed
  - Firewall rule set to allow for DNS to listen on Port 53 for TCP/UDP

Tuning DNS Server for performance

CPU Cores

- DNS service creates UDP Receive threads based on total logical cores present in system. e.g. for 64 logical core system DNS service will create 64 UDP receive threads
- When MS-DNS server is deployed on machines where total cores (logical / physical) are more than 12, UDP Thread count should be set to 8. This gives us high QPS with most optimum utilization of CPU.

Reg key name	*: UdpRecvThreadCount*
Type	*: REG_DWORD*
Path	*: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters*
Value	*: Number of threads in decimal, requires service restart*

- This setting is applicable on authoritative and resolver server and requires service restart

Tuning DNS Server for performance

Overview ✓

DNSSEC ✓

Performance

More…

NIC Settings

- NIC level setting and should be done for each NIC if there are more than one NIC dedicated for DNS
- Receive buffer size: Set it to maximum.

```
Set-NetAdapterAdvancedProperty -Name <NIC Name> -DisplayName "Receive Buffers" -DisplayValue "Maximum"
```

- Enabling RSS on NIC is recommended, below command can be used to enable it:

```
Enable-NetAdapterRss -Name “NIC1”
```

Tuning DNS Server for performance

RSS Settings

- Simply enabling RSS, enables with default settings. Below operations can be used to fine tune it:
  - Set Profile for dynamic load balancing

    ```
    Set-NetAdapterRss -name NIC1 -Profile NUMAStatic
    ```
  - Set number of queue

    ```
    Set-NetAdapterRss -name NIC1 -NumberOfReceiveQueues <Max it can support>
    ```

    (Set with high value, say 64 and PS output will show maximum it can support, then use that value)
  - Total number of Cores to be used concurrently by RSS

    ```
    Set-NetAdapterRss -Name NIC1 -MaxProcessors 6
    ```

    (Assuming DNS service is only high load service running in system, dedicating half i.e. 6 cores to RSS)
  - Dedicate specific cores to RSS

    ```
    Set-NetAdapterRss -name NIC1 -BaseProcessorNumber  6 -MaxProcessorNumber 11
    ```

    (Assume we have total 12 cores, cores number from 6 to 11 will be dedicated to RSS. Rest are free for DNS server)

Tuning DNS Server for performance

Set Processor Affinity

- Idea is to assign logical cores to DNS where RSS is not associated.
- Affinity setting is valid only till life time of process, so after service restart this has to be done again
- It may require to put a PS script for setting it up automatically, , e.g.

```
PS C:\> $var = Get-Process DNS
PS C:\> $var.ProcessorAffinity =  (Sum of cores to be dedicated for DNS)
                                  0001 = 1 ( CPU 1)      00010000 = 16 ( CPU 5)
                                  0010 = 2 ( CPU 2)     00100000 = 32 (CPU 6)
                                  0100 = 4 ( CPU 3 )    01000000 = 64 (CPU 7)
                                  1000 = 8 ( CPU 4 )     . . . . .
```

- Continuing from previous example for settings cores for RSS, out of 12 cores, last 6 were dedicated for RSS, so first 6 can be dedicated for DNS. From table above

```
$var.ProcessorsAffinity=63 (1+2+4+8+16+32)
```

Tuning DNS Server for performance

Other Settings

- Power plan should be set for maximum performance and not conservative
- **Multiple IP address binding for DNS server**
  - Seen Optimal performance (>30%) when DNS server is listening to 2 IP addresses and queries are received on both of these IP addresses

Tuning DNS Server for performance

Overview ✓ | DNSSEC ✓

Performance | More…

Recursion Settings

- **Timeout**
  - Determines the number of seconds that a DNS server waits before it stops trying to contact a remote server.
  - The default setting is 15 seconds.
  - We recommend that you increase this value when recursion occurs over a slow link.
- **Retry Interval**
  - Specifies elapsed seconds before a DNS server retries a recursive lookup
  - Default value = 3 seconds
  - If a DNS server contacts a remote DNS server over a slow link and retries the lookup before it gets a response, you can raise the retry interval to be slightly longer than the observed response time.

Overview ✓	DNSSEC ✓
Performance ✓	More... ✓

Summary

- Easy to deploy
- Smart defaults
- Automated management for day to day operations
- Standards compliant
- High Performance
- Contacts:
  - mailto:dns_msft@outlook.com : WINDOWS DNS TEAM
  - Windows DNS Server Users Mailing List : Mailing List
  - mailto:dns@microsoft.com : DNS Operations @ Microsoft
  - Microsoft.com/dns

Questions

Suggestions

Feedback

?

Microsoft