Windows DNS Server

Mehmet Akcin
Microsoft Corporation

Agenda

Overview

DNSSEC

Performance

More…

Overview

Windows DNS Footprint

- Widely deployed in enterprises that have Active Directory environment
- Fair presence in the resolver space
- Great alternative for diverse operations

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 ISC's BIND.

Ease of Use

- Full AD integration as well as support for file backed persistence
- Graphical User interface
- Full scripting support via Powershell
- Dnscmd
- IPAM integration for A/AAAA record management and service monitoring

More Features

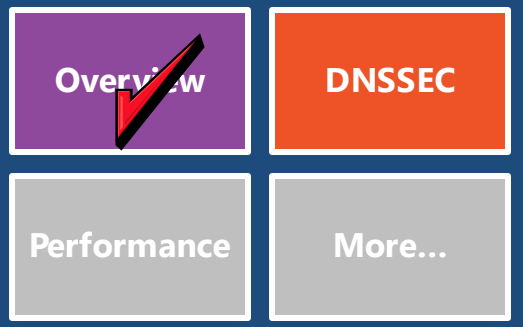
- Conditional Forwarding
  - A conditional forwarder is a DNS server on a network that forwards DNS queries according to the DNS domain name in the query.
- Stub Zones
  - A stub zone is a copy of a zone that contains only those resource records that are necessary to identify the authoritative DNS servers 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
- Source Port Randomization
- WINS and DNSSEC coexistence

DNSSEC

DNSSEC in Windows

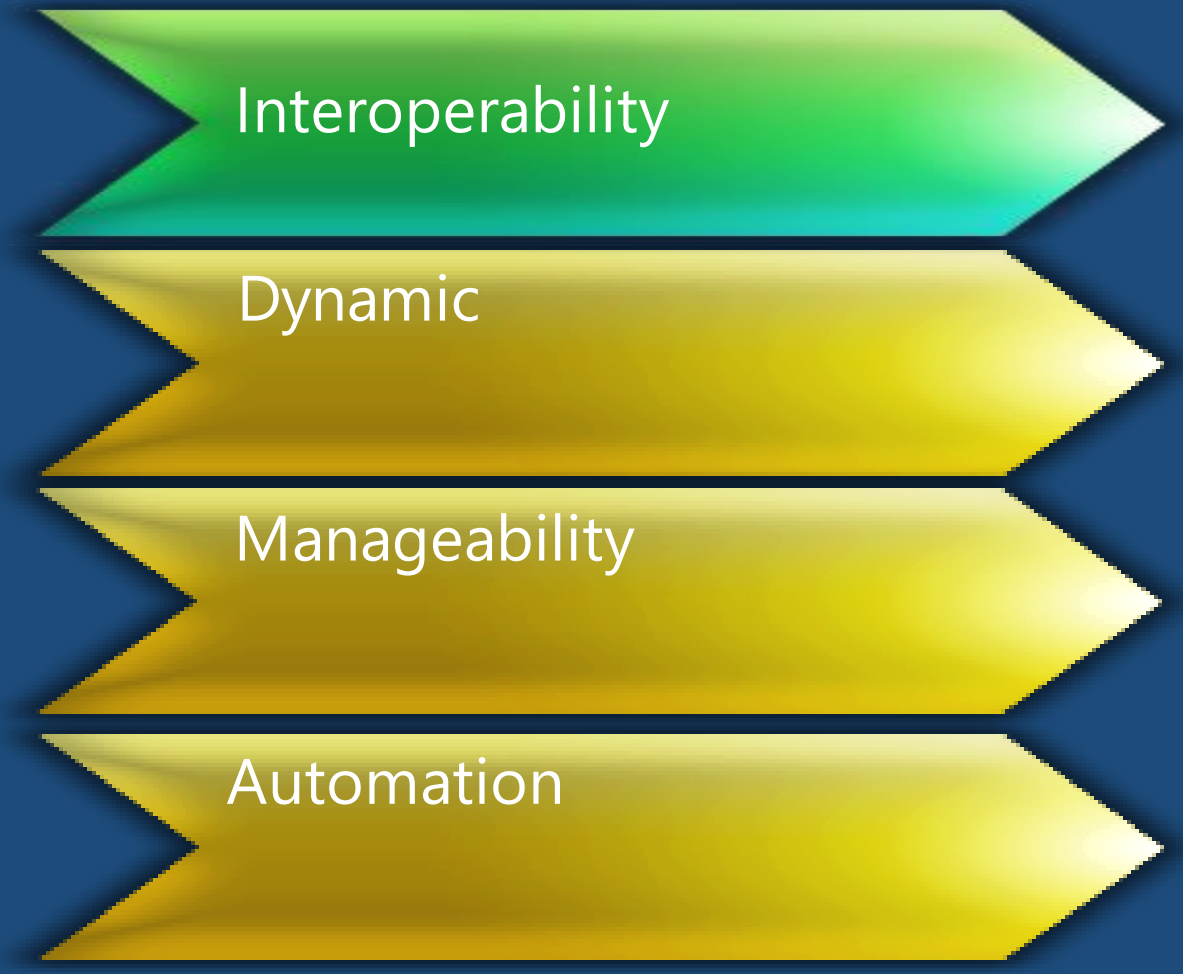


- Microsoft introduced support for DNSSEC in Windows 2008 R2…
  - Ability to sign zones offline and host signed zones
  - Validation of signed responses
  - Support for NSEC

DNSSEC in Windows Server 2012 R2

Overview ✓ | DNSSEC | Performance | More…

ENABLING ENTERPRISE DNSSEC ROLLOUT

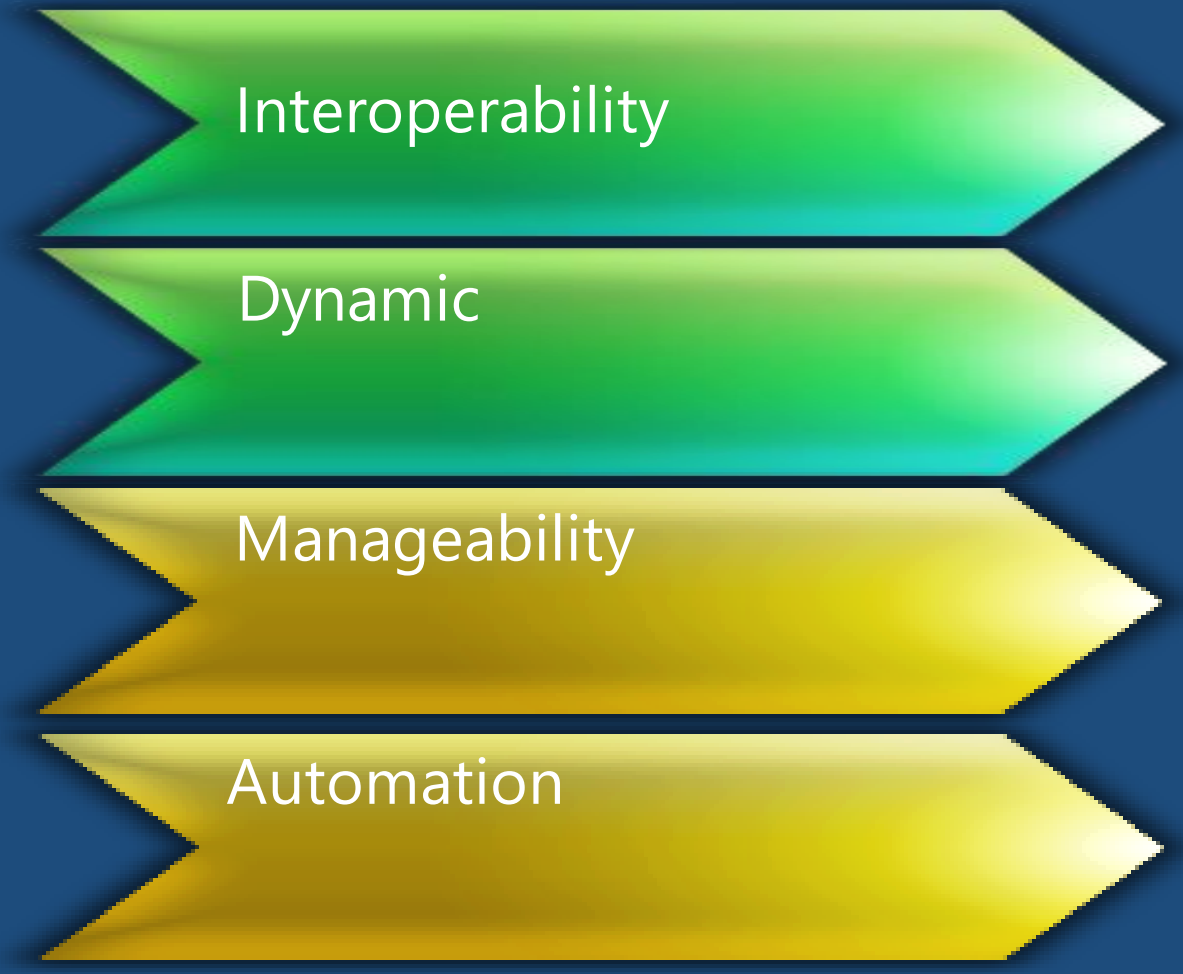


- Latest RFCs
  - NSEC3 Support
  - RSA/SHA-2, ECDSA Signing
  - Automated Trust Anchor Rollover
- Support for 3rd Party Key Management (HSMs)

DNSSEC in Windows Server 2012 R2

Overview | DNSSEC | Performance | More…

ENABLING ENTERPRISE DNSSEC ROLLOUT



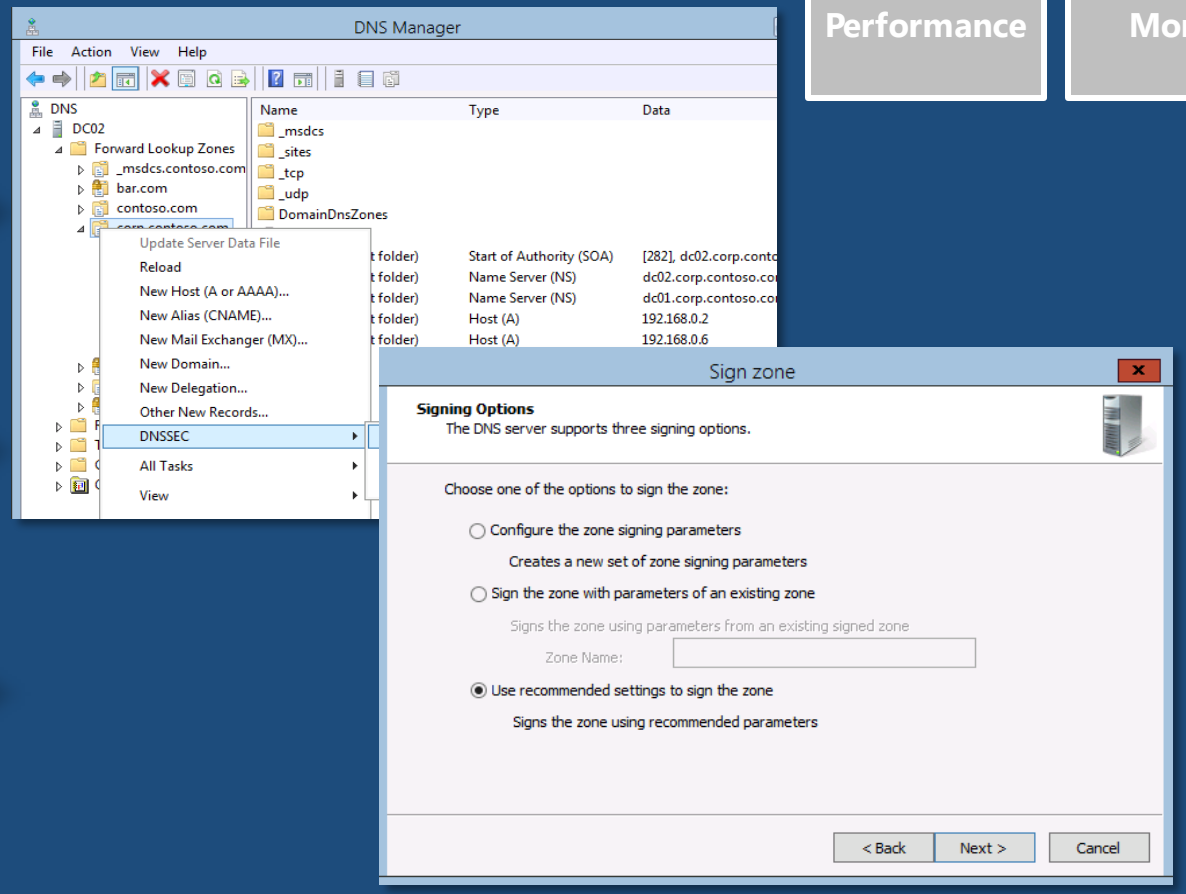
- Support for Online Zone Signing.
  - Sign/unsign/change DNSSEC settings on a live zone
  - Add/remove records dynamically on a signed zone
- Active Directory Integrated
  - Support for dynamic updates
  - Preserving the multi-master DNS model
  - Leverage AD for secure key distribution and Trust Anchor distribution
- Dynamic Update support is available for file backed zones as well
- Improved DNS/DNSSEC server performance

DNSSEC in Windows Server 2012 R2

Overview | DNSSEC | Performance | More…

ENABLING ENTERPRISE DNSSEC ROLLOUT

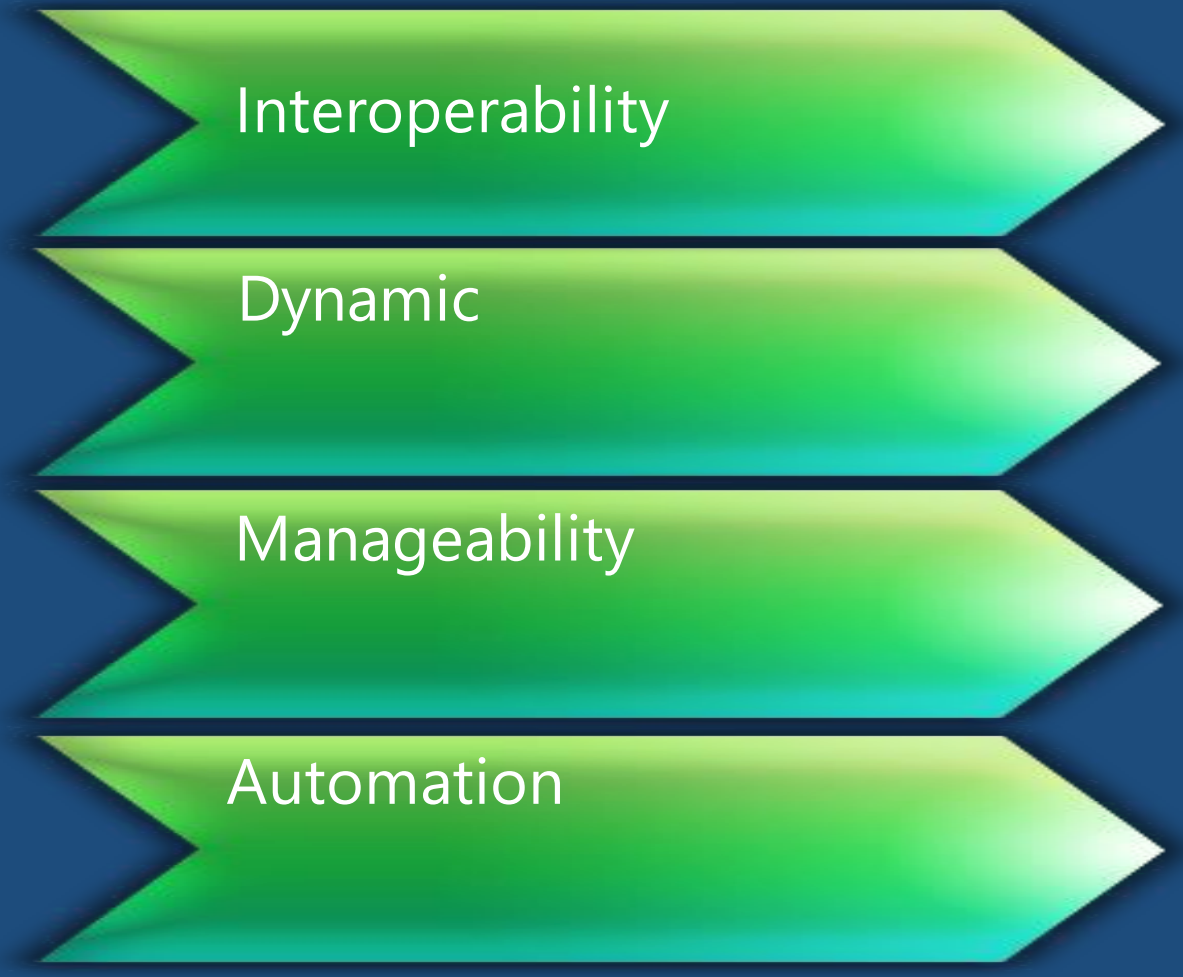
- Interoperability
- Dynamic
- Manageability
- Automation



Complete Powershell Support

DNSSEC in Windows Server 2012 R2

ENABLING ENTERPRISE DNSSEC ROLLOUT

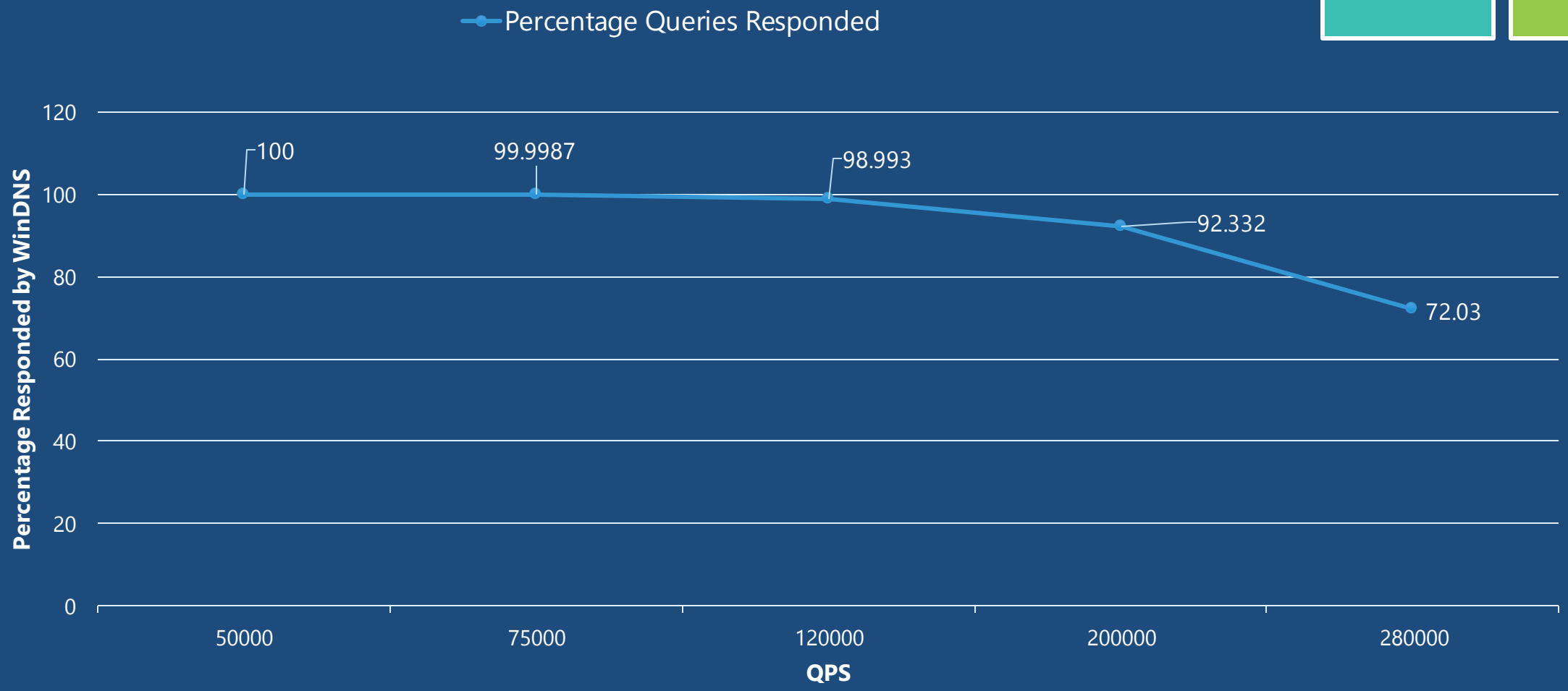


- Automated **re-signing** on static and dynamic updates
- Automated **key rollovers**
- Automated **signature refresh**
- Automated **updating of secure delegations**
- Automated **distribution and updating of Trust Anchors - RFC 5011**

Performance

DNS performance

Overview ✓ | DNSSEC ✓ | Performance | More…

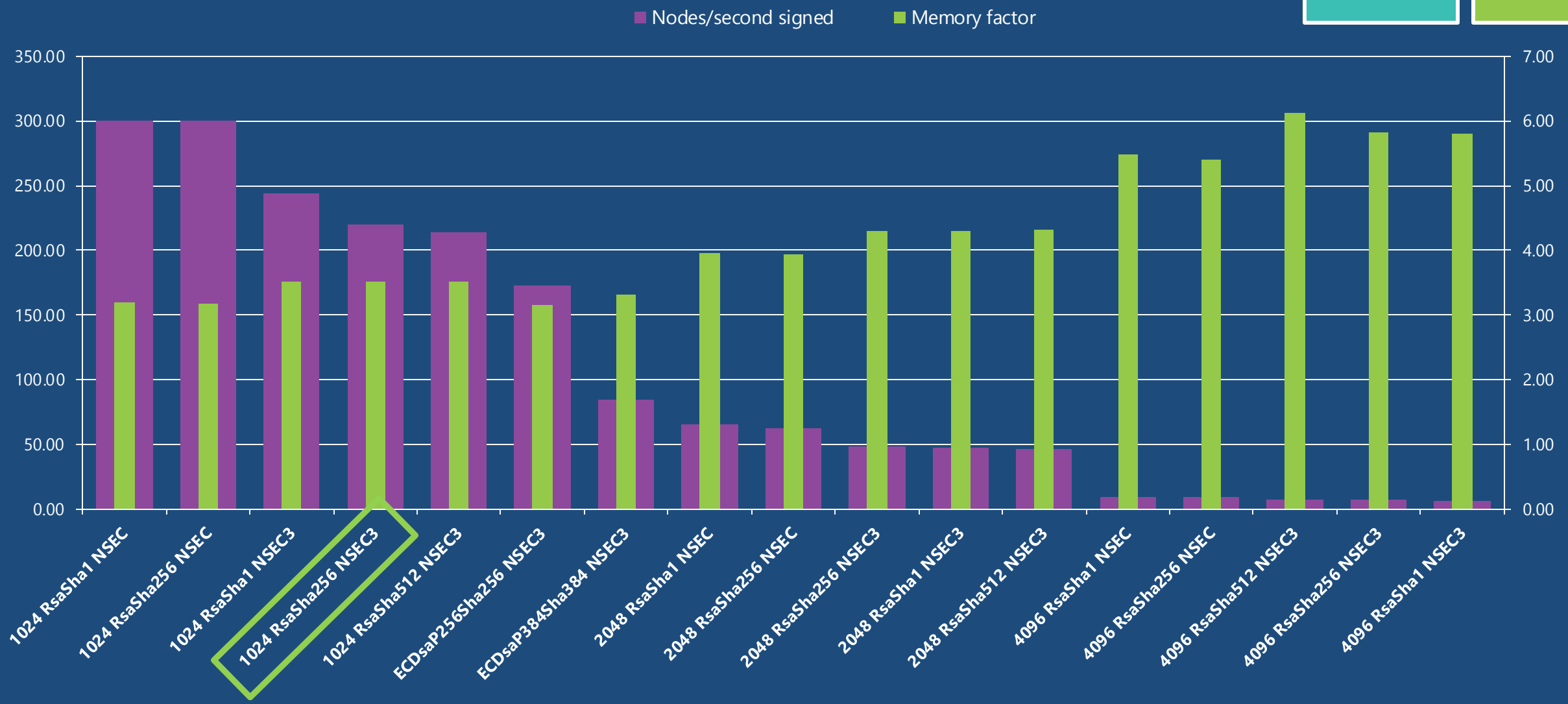


DNSSEC performance

- 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…



Summary

- Easy to deploy
- Smart defaults
- Automated management for day to day operations
- IETF RFC compliant
- High Performance
- Documentation available in 10 languages
- Join WinDNS Users Discussion list
  - http://lists.msft.net
  - See you at DNS-OARC in Los Angeles, CA

Questions

Suggestions

Feedback

?