**[MS-DNSP]:**

**Domain Name Service (DNS) Server Management Protocol**

**Intellectual Property Rights Notice for Open Specifications Documentation**

* **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
* **Copyrights**. This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
* **No Trade Secrets**. Microsoft does not claim any trade secret rights in this documentation.
* **Patents**. Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft [Open Specification Promise](http://go.microsoft.com/fwlink/?LinkId=214445) or the [Community Promise](http://go.microsoft.com/fwlink/?LinkId=214448). If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting [iplg@microsoft.com](mailto:iplg@microsoft.com).
* **Trademarks**. The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit [www.microsoft.com/trademarks](http://www.microsoft.com/trademarks).
* **Fictitious Names**. The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

**Reservation of Rights**. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

**Tools**. The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

**Revision Summary**

| Date | Revision History | Revision Class | Comments |
| --- | --- | --- | --- |
| 1/25/2008 | 0.1 | Major | MCPP Initial Availability. |
| 3/14/2008 | 0.1.1 | Editorial | Changed language and formatting in the technical content. |
| 5/16/2008 | 0.1.2 | Editorial | Changed language and formatting in the technical content. |
| 6/20/2008 | 1.0 | Major | Updated and revised the technical content. |
| 7/25/2008 | 1.0.1 | Editorial | Changed language and formatting in the technical content. |
| 8/29/2008 | 1.0.2 | Editorial | Changed language and formatting in the technical content. |
| 10/24/2008 | 2.0 | Major | Updated and revised the technical content. |
| 12/5/2008 | 3.0 | Major | Updated and revised the technical content. |
| 1/16/2009 | 4.0 | Major | Updated and revised the technical content. |
| 2/27/2009 | 5.0 | Major | Updated and revised the technical content. |
| 4/10/2009 | 6.0 | Major | Updated and revised the technical content. |
| 5/22/2009 | 7.0 | Major | Updated and revised the technical content. |
| 7/2/2009 | 8.0 | Major | Updated and revised the technical content. |
| 8/14/2009 | 9.0 | Major | Updated and revised the technical content. |
| 9/25/2009 | 10.0 | Major | Updated and revised the technical content. |
| 11/6/2009 | 11.0 | Major | Updated and revised the technical content. |
| 12/18/2009 | 12.0 | Major | Updated and revised the technical content. |
| 1/29/2010 | 13.0 | Major | Updated and revised the technical content. |
| 3/12/2010 | 14.0 | Major | Updated and revised the technical content. |
| 4/23/2010 | 15.0 | Major | Updated and revised the technical content. |
| 6/4/2010 | 16.0 | Major | Updated and revised the technical content. |
| 7/16/2010 | 17.0 | Major | Updated and revised the technical content. |
| 8/27/2010 | 18.0 | Major | Updated and revised the technical content. |
| 10/8/2010 | 19.0 | Major | Updated and revised the technical content. |
| 11/19/2010 | 20.0 | Major | Updated and revised the technical content. |
| 1/7/2011 | 21.0 | Major | Updated and revised the technical content. |
| 2/11/2011 | 22.0 | Major | Updated and revised the technical content. |
| 3/25/2011 | 22.0 | None | No changes to the meaning, language, or formatting of the technical content. |
| 5/6/2011 | 22.0 | None | No changes to the meaning, language, or formatting of the technical content. |
| 6/17/2011 | 22.1 | Minor | Clarified the meaning of the technical content. |
| 9/23/2011 | 23.0 | Major | Updated and revised the technical content. |
| 12/16/2011 | 24.0 | Major | Updated and revised the technical content. |
| 3/30/2012 | 24.0 | None | No changes to the meaning, language, or formatting of the technical content. |
| 7/12/2012 | 24.1 | Minor | Clarified the meaning of the technical content. |
| 10/25/2012 | 25.0 | Major | Updated and revised the technical content. |
| 1/31/2013 | 25.0 | None | No changes to the meaning, language, or formatting of the technical content. |
| 8/8/2013 | 26.0 | Major | Updated and revised the technical content. |
| 11/14/2013 | 27.0 | Major | Updated and revised the technical content. |
| 2/13/2014 | 27.0 | None | No changes to the meaning, language, or formatting of the technical content. |
| 5/15/2014 | 28.0 | Major | Updated and revised the technical content. |
| 6/30/2015 | 29.0 | Major | Significantly changed the technical content. |

Table of Contents

[1 Introduction 10](#_Toc423366306)

[1.1 Glossary 10](#_Toc423366307)

[1.2 References 17](#_Toc423366308)

[1.2.1 Normative References 18](#_Toc423366309)

[1.2.2 Informative References 21](#_Toc423366310)

[1.3 Overview 21](#_Toc423366311)

[1.4 Relationship to Other Protocols 22](#_Toc423366312)

[1.5 Prerequisites/Preconditions 24](#_Toc423366313)

[1.6 Applicability Statement 25](#_Toc423366314)

[1.7 Versioning and Capability Negotiation 25](#_Toc423366315)

[1.8 Vendor-Extensible Fields 25](#_Toc423366316)

[1.9 Standards Assignments 25](#_Toc423366317)

[2 Messages 27](#_Toc423366318)

[2.1 Transport 27](#_Toc423366319)

[2.1.1 Server Security Settings 27](#_Toc423366320)

[2.1.2 Client Security Settings 27](#_Toc423366321)

[2.2 Common Data Types 28](#_Toc423366322)

[2.2.1 DNS RPC Common Messages 28](#_Toc423366323)

[2.2.1.1 Enumerations and Constants 28](#_Toc423366324)

[2.2.1.1.1 DNS\_RPC\_TYPEID 28](#_Toc423366325)

[2.2.1.1.2 DNS\_RPC\_PROTOCOLS 32](#_Toc423366326)

[2.2.1.1.3 TRUSTPOINT\_STATE 33](#_Toc423366327)

[2.2.1.1.4 TRUSTANCHOR\_STATE 33](#_Toc423366328)

[2.2.1.2 Structures 34](#_Toc423366329)

[2.2.1.2.1 DNS\_RPC\_CURRENT\_CLIENT\_VER 34](#_Toc423366330)

[2.2.1.2.2 DNS\_RPC\_BUFFER 34](#_Toc423366331)

[2.2.1.2.3 DNS\_RPC\_UTF8\_STRING\_LIST 34](#_Toc423366332)

[2.2.1.2.4 DNS\_RPC\_UNICODE\_STRING\_LIST 35](#_Toc423366333)

[2.2.1.2.5 DNS\_RPC\_NAME\_AND\_PARAM 35](#_Toc423366334)

[2.2.1.2.6 DNSSRV\_RPC\_UNION 35](#_Toc423366335)

[2.2.2 Resource Record Messages 40](#_Toc423366336)

[2.2.2.1 Enumerations and Constants 40](#_Toc423366337)

[2.2.2.1.1 DNS\_RECORD\_TYPE 40](#_Toc423366338)

[2.2.2.1.2 DNS\_RPC\_NODE\_FLAGS 43](#_Toc423366339)

[2.2.2.2 Structures 44](#_Toc423366340)

[2.2.2.2.1 DNS\_RPC\_NAME 44](#_Toc423366341)

[2.2.2.2.2 DNS\_COUNT\_NAME 44](#_Toc423366342)

[2.2.2.2.3 DNS\_RPC\_NODE 45](#_Toc423366343)

[2.2.2.2.4 DNS\_RPC\_RECORD\_DATA 45](#_Toc423366344)

[2.2.2.2.4.1 DNS\_RPC\_RECORD\_A 46](#_Toc423366345)

[2.2.2.2.4.2 DNS\_RPC\_RECORD\_NODE\_NAME 46](#_Toc423366346)

[2.2.2.2.4.3 DNS\_RPC\_RECORD\_SOA 46](#_Toc423366347)

[2.2.2.2.4.4 DNS\_RPC\_RECORD\_NULL 47](#_Toc423366348)

[2.2.2.2.4.5 DNS\_RPC\_RECORD\_WKS 48](#_Toc423366349)

[2.2.2.2.4.6 DNS\_RPC\_RECORD\_STRING 48](#_Toc423366350)

[2.2.2.2.4.7 DNS\_RPC\_RECORD\_MAIL\_ERROR 49](#_Toc423366351)

[2.2.2.2.4.8 DNS\_RPC\_RECORD\_NAME\_PREFERENCE 49](#_Toc423366352)

[2.2.2.2.4.9 DNS\_RPC\_RECORD\_SIG 50](#_Toc423366353)

[2.2.2.2.4.10 DNS\_RPC\_RECORD\_RRSIG 50](#_Toc423366354)

[2.2.2.2.4.11 DNS\_RPC\_RECORD\_NSEC 51](#_Toc423366355)

[2.2.2.2.4.12 DNS\_RPC\_RECORD\_DS 52](#_Toc423366356)

[2.2.2.2.4.13 DNS\_RPC\_RECORD\_KEY 52](#_Toc423366357)

[2.2.2.2.4.14 DNS\_RPC\_RECORD\_DHCID 52](#_Toc423366358)

[2.2.2.2.4.15 DNS\_RPC\_RECORD\_DNSKEY 53](#_Toc423366359)

[2.2.2.2.4.16 DNS\_RPC\_RECORD\_AAAA 53](#_Toc423366360)

[2.2.2.2.4.17 DNS\_RPC\_RECORD\_NXT 53](#_Toc423366361)

[2.2.2.2.4.18 DNS\_RPC\_RECORD\_SRV 54](#_Toc423366362)

[2.2.2.2.4.19 DNS\_RPC\_RECORD\_ATMA 54](#_Toc423366363)

[2.2.2.2.4.20 DNS\_RPC\_RECORD\_NAPTR 55](#_Toc423366364)

[2.2.2.2.4.21 DNS\_RPC\_RECORD\_WINS 56](#_Toc423366365)

[2.2.2.2.4.22 DNS\_RPC\_RECORD\_WINSR 56](#_Toc423366366)

[2.2.2.2.4.23 DNS\_RPC\_RECORD\_TS 57](#_Toc423366367)

[2.2.2.2.4.24 DNS\_RPC\_RECORD\_NSEC3 57](#_Toc423366368)

[2.2.2.2.4.25 DNS\_RPC\_RECORD\_NSEC3PARAM 58](#_Toc423366369)

[2.2.2.2.4.26 DNS\_RPC\_RECORD\_TLSA 59](#_Toc423366370)

[2.2.2.2.4.27 DNS\_RPC\_RECORD\_UNKNOWN 59](#_Toc423366371)

[2.2.2.2.5 DNS\_RPC\_RECORD 59](#_Toc423366372)

[2.2.3 Address Information Messages 63](#_Toc423366373)

[2.2.3.1 Enumerations and Constants 63](#_Toc423366374)

[2.2.3.1.1 DNS\_IPVAL\_CONTEXT 63](#_Toc423366375)

[2.2.3.1.2 DNS\_IP\_VALIDATE\_RETURN\_FLAGS 64](#_Toc423366376)

[2.2.3.2 Structures 65](#_Toc423366377)

[2.2.3.2.1 IP4\_ARRAY 65](#_Toc423366378)

[2.2.3.2.2 DNS\_ADDR 65](#_Toc423366379)

[2.2.3.2.2.1 DNS ADDR 65](#_Toc423366380)

[2.2.3.2.2.2 DNS ADD USER 66](#_Toc423366381)

[2.2.3.2.3 DNS\_ADDR\_ARRAY 67](#_Toc423366382)

[2.2.3.2.4 DNS\_RPC\_IP\_VALIDATE 67](#_Toc423366383)

[2.2.4 Server Messages 68](#_Toc423366384)

[2.2.4.1 Enumerations and Constants 68](#_Toc423366385)

[2.2.4.1.1 DNS\_BOOT\_METHODS 68](#_Toc423366386)

[2.2.4.1.2 DNS\_NAME\_CHECK\_FLAGS 69](#_Toc423366387)

[2.2.4.2 Structures 69](#_Toc423366388)

[2.2.4.2.1 DNSSRV\_VERSION 69](#_Toc423366389)

[2.2.4.2.2 DNS\_RPC\_SERVER\_INFO 70](#_Toc423366390)

[2.2.4.2.2.1 DNS\_RPC\_SERVER\_INFO\_W2K 70](#_Toc423366391)

[2.2.4.2.2.2 DNS\_RPC\_SERVER\_INFO\_DOTNET 74](#_Toc423366392)

[2.2.4.2.2.3 DNS\_RPC\_SERVER\_INFO\_LONGHORN 76](#_Toc423366393)

[2.2.5 Zone Messages 77](#_Toc423366394)

[2.2.5.1 Enumerations and Constants 77](#_Toc423366395)

[2.2.5.1.1 DNS\_ZONE\_TYPE 77](#_Toc423366396)

[2.2.5.1.2 DNS\_ZONE\_SECONDARY\_SECURITY 77](#_Toc423366397)

[2.2.5.1.3 DNS\_ZONE\_NOTIFY\_LEVEL 78](#_Toc423366398)

[2.2.5.1.4 ZONE\_REQUEST\_FILTERS 78](#_Toc423366399)

[2.2.5.1.5 ZONE\_SKD\_ROLLOVER\_TYPE 79](#_Toc423366400)

[2.2.5.1.6 ZONE\_SKD\_ROLLOVER\_ACTION 79](#_Toc423366401)

[2.2.5.2 Structures 80](#_Toc423366402)

[2.2.5.2.1 DNS\_RPC\_ZONE 80](#_Toc423366403)

[2.2.5.2.1.1 DNS\_RPC\_ZONE\_W2K 80](#_Toc423366404)

[2.2.5.2.1.2 DNS\_RPC\_ZONE\_DOTNET 81](#_Toc423366405)

[2.2.5.2.2 DNS\_RPC\_ZONE\_FLAGS 81](#_Toc423366406)

[2.2.5.2.3 DNS\_RPC\_ZONE\_LIST 82](#_Toc423366407)

[2.2.5.2.3.1 DNS\_RPC\_ZONE\_LIST\_W2K 83](#_Toc423366408)

[2.2.5.2.3.2 DNS\_RPC\_ZONE\_LIST\_DOTNET 83](#_Toc423366409)

[2.2.5.2.4 DNS\_RPC\_ZONE\_INFO 84](#_Toc423366410)

[2.2.5.2.4.1 DNS\_RPC\_ZONE\_INFO\_W2K 84](#_Toc423366411)

[2.2.5.2.4.2 DNS\_RPC\_ZONE\_INFO\_DOTNET 86](#_Toc423366412)

[2.2.5.2.4.3 DNS\_RPC\_ZONE\_INFO\_LONGHORN 88](#_Toc423366413)

[2.2.5.2.5 DNS\_RPC\_ZONE\_SECONDARIES 89](#_Toc423366414)

[2.2.5.2.5.1 DNS\_RPC\_ZONE\_SECONDARIES\_W2K 90](#_Toc423366415)

[2.2.5.2.5.2 DNS\_RPC\_ZONE\_SECONDARIES\_DOTNET 90](#_Toc423366416)

[2.2.5.2.5.3 DNS\_RPC\_ZONE\_SECONDARIES\_LONGHORN 91](#_Toc423366417)

[2.2.5.2.6 DNS\_RPC\_ZONE\_DATABASE 91](#_Toc423366418)

[2.2.5.2.6.1 DNS\_RPC\_ZONE\_DATABASE\_W2K 91](#_Toc423366419)

[2.2.5.2.6.2 DNS\_RPC\_ZONE\_DATABASE\_DOTNET 92](#_Toc423366420)

[2.2.5.2.7 DNS\_RPC\_ZONE\_CREATE\_INFO 92](#_Toc423366421)

[2.2.5.2.7.1 DNS\_RPC\_ZONE\_CREATE\_INFO\_W2K 92](#_Toc423366422)

[2.2.5.2.7.2 DNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET 95](#_Toc423366423)

[2.2.5.2.7.3 DNS\_RPC\_ZONE\_CREATE\_INFO\_LONGHORN 96](#_Toc423366424)

[2.2.5.2.8 DNS\_RPC\_ZONE\_EXPORT\_INFO 97](#_Toc423366425)

[2.2.5.2.9 DNS\_RPC\_ENUM\_ZONES\_FILTER 97](#_Toc423366426)

[2.2.5.2.10 DNS\_RPC\_FORWARDERS 98](#_Toc423366427)

[2.2.5.2.10.1 DNS\_RPC\_FORWARDERS\_W2K 98](#_Toc423366428)

[2.2.5.2.10.2 DNS\_RPC\_FORWARDERS\_DOTNET 98](#_Toc423366429)

[2.2.5.2.10.3 DNS\_RPC\_FORWARDERS\_LONGHORN 99](#_Toc423366430)

[2.2.6 Zone Update Messages 99](#_Toc423366431)

[2.2.6.1 Enumerations and Constants 99](#_Toc423366432)

[2.2.6.1.1 DNS\_ZONE\_UPDATE 99](#_Toc423366433)

[2.2.6.1.2 KeySignScope 99](#_Toc423366434)

[2.2.6.1.3 ImportOpResult 100](#_Toc423366435)

[2.2.6.2 Structures 100](#_Toc423366436)

[2.2.6.2.1 DNS\_RPC\_SKD 100](#_Toc423366437)

[2.2.6.2.2 DNS\_RPC\_SKD\_LIST 102](#_Toc423366438)

[2.2.6.2.3 DNS\_RPC\_SKD\_STATE 102](#_Toc423366439)

[2.2.6.2.4 DNS\_RPC\_TRUST\_POINT 105](#_Toc423366440)

[2.2.6.2.5 DNS\_RPC\_TRUST\_POINT\_LIST 106](#_Toc423366441)

[2.2.6.2.6 DNS\_RPC\_TRUST\_ANCHOR 107](#_Toc423366442)

[2.2.6.2.7 DNS\_RPC\_TRUST\_ANCHOR\_LIST 108](#_Toc423366443)

[2.2.6.2.8 DNS\_RPC\_SIGNING\_VALIDATION\_ERROR 109](#_Toc423366444)

[2.2.6.2.9 DNS\_RPC\_ZONE\_DNSSEC\_SETTINGS 109](#_Toc423366445)

[2.2.6.2.10 DNS\_RPC\_ZONE\_SKD 111](#_Toc423366446)

[2.2.6.2.11 DNS\_RPC\_SKD\_STATE\_EX 111](#_Toc423366447)

[2.2.7 Application Directory Partition Messages 113](#_Toc423366448)

[2.2.7.1 Enumerations and Constants 113](#_Toc423366449)

[2.2.7.1.1 DNS\_RPC\_DP\_FLAGS 113](#_Toc423366450)

[2.2.7.2 Structures 114](#_Toc423366451)

[2.2.7.2.1 DNS\_RPC\_DP\_INFO 114](#_Toc423366452)

[2.2.7.2.2 DNS\_RPC\_DP\_REPLICA 115](#_Toc423366453)

[2.2.7.2.3 DNS\_RPC\_DP\_ENUM 116](#_Toc423366454)

[2.2.7.2.4 DNS\_RPC\_DP\_LIST 116](#_Toc423366455)

[2.2.7.2.5 DNS\_RPC\_ENLIST\_DP 116](#_Toc423366456)

[2.2.7.2.6 DNS\_RPC\_ZONE\_CHANGE\_DP 117](#_Toc423366457)

[2.2.8 AutoConfig Messages 118](#_Toc423366458)

[2.2.8.1 Enumerations and Constants 118](#_Toc423366459)

[2.2.8.1.1 DNS\_RPC\_AUTOCONFIG 118](#_Toc423366460)

[2.2.8.2 Structures 120](#_Toc423366461)

[2.2.8.2.1 DNS\_RPC\_AUTOCONFIGURE 120](#_Toc423366462)

[2.2.9 Logging Messages 120](#_Toc423366463)

[2.2.9.1 Enumerations and Constants 120](#_Toc423366464)

[2.2.9.1.1 DNS\_LOG\_LEVELS 120](#_Toc423366465)

[2.2.9.1.2 DNS\_EVENTLOG\_TYPES 121](#_Toc423366466)

[2.2.10 Server Statistics Messages 122](#_Toc423366467)

[2.2.10.1 Enumerations and Constants 122](#_Toc423366468)

[2.2.10.1.1 DNSSRV\_STATID\_TYPES 122](#_Toc423366469)

[2.2.10.2 Structures 123](#_Toc423366470)

[2.2.10.2.1 DNSSRV\_STAT\_HEADER 123](#_Toc423366471)

[2.2.10.2.2 DNSSRV\_STATS 124](#_Toc423366472)

[2.2.10.2.3 DNS\_SYSTEMTIME 124](#_Toc423366473)

[2.2.10.2.4 DNSSRV\_TIME\_STATS 125](#_Toc423366474)

[2.2.10.2.5 DNSSRV\_QUERY\_STATS 126](#_Toc423366475)

[2.2.10.2.6 DNSSRV\_QUERY2\_STATS 127](#_Toc423366476)

[2.2.10.2.7 DNSSRV\_RECURSE\_STATS 129](#_Toc423366477)

[2.2.10.2.8 DNSSRV\_DNSSEC\_STATS 136](#_Toc423366478)

[2.2.10.2.9 DNSSRV\_MASTER\_STATS 136](#_Toc423366479)

[2.2.10.2.10 DNSSRV\_SECONDARY\_STATS 139](#_Toc423366480)

[2.2.10.2.11 DNSSRV\_WINS\_STATS 143](#_Toc423366481)

[2.2.10.2.12 DNSSRV\_UPDATE\_STATS 143](#_Toc423366482)

[2.2.10.2.13 DNSSRV\_SKWANSEC\_STATS 147](#_Toc423366483)

[2.2.10.2.14 DNSSRV\_DS\_STATS 149](#_Toc423366484)

[2.2.10.2.15 DNSSRV\_MEMTAG\_STATS 153](#_Toc423366485)

[2.2.10.2.16 DNSSRV\_MEMORY\_STATS 154](#_Toc423366486)

[2.2.10.2.17 DNSSRV\_TIMEOUT\_STATS 158](#_Toc423366487)

[2.2.10.2.18 DNSSRV\_DBASE\_STATS 160](#_Toc423366488)

[2.2.10.2.19 DNSSRV\_RECORD\_STATS 161](#_Toc423366489)

[2.2.10.2.20 DNSSRV\_PACKET\_STATS 162](#_Toc423366490)

[2.2.10.2.21 DNSSRV\_NBSTAT\_STATS 164](#_Toc423366491)

[2.2.10.2.22 DNSSRV\_PRIVATE\_STATS 165](#_Toc423366492)

[2.2.10.2.23 DNSSRV\_ERROR\_STATS 168](#_Toc423366493)

[2.2.10.2.24 DNSSRV\_CACHE\_STATS 170](#_Toc423366494)

[2.2.11 Key Structures 171](#_Toc423366495)

[2.2.11.1 Enumerations and Constants 171](#_Toc423366496)

[2.2.11.1.1 Cryptographic Algorithm Name 171](#_Toc423366497)

[2.2.11.2 Structures 171](#_Toc423366498)

[2.2.11.2.1 RSA Key Pair 171](#_Toc423366499)

[2.2.11.2.2 ECDSA\_P256 Key Pair 172](#_Toc423366500)

[2.2.11.2.3 ECDSA\_P384 Key Pair 173](#_Toc423366501)

[2.2.11.2.4 Protection Key Identifier 174](#_Toc423366502)

[2.2.11.2.5 Protection Key Attributes 175](#_Toc423366503)

[2.2.11.2.6 Exported Key Pair 176](#_Toc423366504)

[2.2.12 Zone Statistics Messages 177](#_Toc423366505)

[2.2.12.1 Enumerations and Constants 177](#_Toc423366506)

[2.2.12.1.1 DNS\_ZONE\_STATS\_TYPE 177](#_Toc423366507)

[2.2.12.2 Structures 178](#_Toc423366508)

[2.2.12.2.1 DNSSRV\_ZONE\_TIME\_STATS 178](#_Toc423366509)

[2.2.12.2.2 DNSSRV\_ZONE\_QUERY\_STATS 178](#_Toc423366510)

[2.2.12.2.3 DNSSRV\_ZONE\_TRANSFER\_STATS 179](#_Toc423366511)

[2.2.12.2.4 DNSSRV\_ZONE\_UPDATE\_STATS 179](#_Toc423366512)

[2.2.12.2.5 DNS\_RPC\_ZONE\_STATS\_V1 180](#_Toc423366513)

[2.2.13 Zone Scope or Cache Scope Messages 180](#_Toc423366514)

[2.2.13.1 Enumerations and Constants 180](#_Toc423366515)

[2.2.13.2 Structures 180](#_Toc423366516)

[2.2.13.2.1 DNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST 180](#_Toc423366517)

[2.2.13.2.2 DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO 181](#_Toc423366518)

[2.2.13.2.2.1 DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1 181](#_Toc423366519)

[2.2.13.2.3 DNS\_RPC\_ZONE\_SCOPE\_INFO 181](#_Toc423366520)

[2.2.13.2.3.1 DNS\_RPC\_ZONE\_SCOPE\_INFO\_V1 181](#_Toc423366521)

[2.2.14 Server Scope Messages 182](#_Toc423366522)

[2.2.14.1 Structures 182](#_Toc423366523)

[2.2.14.1.1 DNS\_RPC\_ENUM\_SCOPE\_LIST 182](#_Toc423366524)

[2.2.15 Policies 182](#_Toc423366525)

[2.2.15.1 Enumerations and Constants 182](#_Toc423366526)

[2.2.15.1.1 Constants 182](#_Toc423366527)

[2.2.15.1.1.1 DNS\_RPC\_CRITERIA\_COMPARATOR 183](#_Toc423366528)

[2.2.15.1.1.2 DNS\_RPC\_POLICY\_CONDITION 184](#_Toc423366529)

[2.2.15.1.1.3 DNS\_RPC\_POLICY\_LEVEL 184](#_Toc423366530)

[2.2.15.1.1.4 DNS\_RPC\_POLICY\_ACTION\_TYPE 185](#_Toc423366531)

[2.2.15.1.1.5 DNS\_RPC\_POLICY\_TYPE 185](#_Toc423366532)

[2.2.15.1.1.6 DNS\_RPC\_CRITERIA\_ENUM 185](#_Toc423366533)

[2.2.15.2 Structures 186](#_Toc423366534)

[2.2.15.2.1 DNS\_RPC\_CLIENT\_SUBNET\_RECORD 186](#_Toc423366535)

[2.2.15.2.2 DNS\_RPC\_POLICY\_CONTENT 187](#_Toc423366536)

[2.2.15.2.3 DNS\_RPC\_POLICY\_CONTENT\_LIST 187](#_Toc423366537)

[2.2.15.2.4 DNS\_RPC\_CRITERIA 188](#_Toc423366538)

[2.2.15.2.5 DNS\_RPC\_POLICY 188](#_Toc423366539)

[2.2.15.2.6 DNS\_RPC\_POLICY\_NAME 189](#_Toc423366540)

[2.2.15.2.7 DNS\_RPC\_ENUMERATE\_POLICY\_LIST 190](#_Toc423366541)

[2.3 Directory Service Schema Elements 190](#_Toc423366542)

[2.3.1 Object Classes 192](#_Toc423366543)

[2.3.1.1 msDNS-ServerSettings 192](#_Toc423366544)

[2.3.2 Attributes 192](#_Toc423366545)

[2.3.2.1 dnsProperty 192](#_Toc423366546)

[2.3.2.1.1 Property Id 193](#_Toc423366547)

[2.3.2.1.2 DcPromo Flag 194](#_Toc423366548)

[2.3.2.2 dnsRecord 195](#_Toc423366549)

[2.3.2.3 msDNS-IsSigned 195](#_Toc423366550)

[2.3.2.4 msDNS-NSEC3OptOut 196](#_Toc423366551)

[2.3.2.5 msDNS-SigningKeys 196](#_Toc423366552)

[2.3.2.6 msDNS-SignWithNSEC3 196](#_Toc423366553)

[2.3.2.7 msDNS-NSEC3UserSalt 196](#_Toc423366554)

[2.3.2.8 msDNS-DNSKEYRecords 196](#_Toc423366555)

[2.3.2.9 msDNS-DSRecordSetTTL 196](#_Toc423366556)

[2.3.2.10 msDNS-NSEC3Iterations 197](#_Toc423366557)

[2.3.2.11 msDNS-PropagationTime 197](#_Toc423366558)

[2.3.2.12 msDNS-NSEC3CurrentSalt 197](#_Toc423366559)

[2.3.2.13 msDNS-RFC5011KeyRollovers 197](#_Toc423366560)

[2.3.2.14 msDNS-NSEC3HashAlgorithm 197](#_Toc423366561)

[2.3.2.15 msDNS-DSRecordAlgorithms 197](#_Toc423366562)

[2.3.2.16 msDNS-DNSKEYRecordSetTTL 197](#_Toc423366563)

[2.3.2.17 msDNS-MaintainTrustAnchor 197](#_Toc423366564)

[2.3.2.18 msDNS-NSEC3RandomSaltLength 197](#_Toc423366565)

[2.3.2.19 msDNS-SigningKeyDescriptors 197](#_Toc423366566)

[2.3.2.20 msDNS-SignatureInceptionOffset 202](#_Toc423366567)

[2.3.2.21 msDNS-ParentHasSecureDelegation 202](#_Toc423366568)

[2.3.2.22 msDNS-SecureDelegationPollingPeriod 202](#_Toc423366569)

[2.3.2.23 msDNS-KeymasterZones 202](#_Toc423366570)

[3 Protocol Details 203](#_Toc423366571)

[3.1 DnsServer Server Details 203](#_Toc423366572)

[3.1.1 Abstract Data Model 203](#_Toc423366573)

[3.1.1.1 DNS Server Configuration Information 207](#_Toc423366574)

[3.1.1.1.1 DNS Server Integer Properties 207](#_Toc423366575)

[3.1.1.1.2 DNS Server Address Array Properties 223](#_Toc423366576)

[3.1.1.1.3 DNS Server String Properties 223](#_Toc423366577)

[3.1.1.1.4 DNS Server String List Properties 224](#_Toc423366578)

[3.1.1.2 DNS Zone Configuration Information 224](#_Toc423366579)

[3.1.1.2.1 DNS Zone Integer Properties 224](#_Toc423366580)

[3.1.1.2.2 DNS Zone Address Array Properties 227](#_Toc423366581)

[3.1.1.2.3 DNS Zone String Properties 228](#_Toc423366582)

[3.1.1.2.4 DNS Record Configuration Information 228](#_Toc423366583)

[3.1.1.2.5 DNS Zone Scope or Cache Scope Configuration Information 228](#_Toc423366584)

[3.1.1.3 DNS Server Server Scope Configuration Information 228](#_Toc423366585)

[3.1.1.3.1 DNS Server Server Scope Integer Properties 229](#_Toc423366586)

[3.1.1.3.2 DNS Server Server Scope Address Array Properties 229](#_Toc423366587)

[3.1.2 Timers 229](#_Toc423366588)

[3.1.3 Initialization 229](#_Toc423366589)

[3.1.4 Message Processing Events and Sequencing Rules 233](#_Toc423366590)

[3.1.4.1 R\_DnssrvOperation (Opnum 0) 235](#_Toc423366591)

[3.1.4.2 R\_DnssrvQuery (Opnum 1) 265](#_Toc423366592)

[3.1.4.3 R\_DnssrvComplexOperation (Opnum 2) 267](#_Toc423366593)

[3.1.4.4 R\_DnssrvEnumRecords (Opnum 3) 276](#_Toc423366594)

[3.1.4.5 R\_DnssrvUpdateRecord (Opnum 4) 278](#_Toc423366595)

[3.1.4.6 R\_DnssrvOperation2 (Opnum 5) 280](#_Toc423366596)

[3.1.4.7 R\_DnssrvQuery2 (Opnum 6) 281](#_Toc423366597)

[3.1.4.8 R\_DnssrvComplexOperation2 (Opnum 7) 281](#_Toc423366598)

[3.1.4.9 R\_DnssrvEnumRecords2 (Opnum 8) 282](#_Toc423366599)

[3.1.4.10 R\_DnssrvUpdateRecord2 (Opnum 9) 283](#_Toc423366600)

[3.1.4.11 R\_DnssrvUpdateRecord3 (Opnum 10) 283](#_Toc423366601)

[3.1.4.12 R\_DnssrvEnumRecords3 (Opnum 11) 284](#_Toc423366602)

[3.1.4.13 R\_DnssrvOperation3 (Opnum 12) 284](#_Toc423366603)

[3.1.4.14 R\_DnssrvQuery3 (Opnum 13) 286](#_Toc423366604)

[3.1.5 Timer Events 287](#_Toc423366605)

[3.1.6 Other Local Events 287](#_Toc423366606)

[3.1.6.1 Three-phase authorization test 287](#_Toc423366607)

[3.1.6.2 Directory server security descriptors reading and caching 288](#_Toc423366608)

[3.1.6.3 dnsRecord in the Directory Server 288](#_Toc423366609)

[3.1.6.4 Modifying Directory Server Security Descriptors 288](#_Toc423366610)

[3.1.7 Key Processing Rules 289](#_Toc423366611)

[3.1.7.1 Constructing an Exported Key 289](#_Toc423366612)

[3.1.7.2 Importing an Exported Key 291](#_Toc423366613)

[3.1.8 DNS Policy 291](#_Toc423366614)

[3.1.8.1 Client Subnet Record 292](#_Toc423366615)

[3.1.8.2 DNS Policy Criteria 292](#_Toc423366616)

[3.1.8.3 DNS Policy Validation 293](#_Toc423366617)

[4 Protocol Examples 296](#_Toc423366618)

[4.1 Querying a DNS server DWORD property 296](#_Toc423366619)

[4.2 Modifying a DNS server DWORD property 296](#_Toc423366620)

[4.3 Creating a New Zone 297](#_Toc423366621)

[4.4 Enumerating Zones 297](#_Toc423366622)

[4.5 Creating and Deleting a DNS Record 298](#_Toc423366623)

[4.6 Creating a Zone Scope 299](#_Toc423366624)

[4.7 Deleting a Zone Scope 299](#_Toc423366625)

[4.8 Enumerating Zone Scopes 300](#_Toc423366626)

[4.9 Creating and Deleting a DNS Record in a Zone Scope 300](#_Toc423366627)

[4.10 Creating a Policy 301](#_Toc423366628)

[4.11 Updating a Policy 302](#_Toc423366629)

[4.12 Deleting a Policy 302](#_Toc423366630)

[4.13 Enumerating Policies 303](#_Toc423366631)

[4.14 Creating a Client Subnet Record 303](#_Toc423366632)

[4.15 Deleting a Client Subnet Record 304](#_Toc423366633)

[4.16 Enumerating Client Subnet Records 304](#_Toc423366634)

[5 Security 306](#_Toc423366635)

[5.1 Security Considerations for Implementers 306](#_Toc423366636)

[5.1.1 Security Considerations Specific to the DNS Server Management Protocol 306](#_Toc423366637)

[5.2 Index of Security Parameters 306](#_Toc423366638)

[6 Appendix A: Full IDL 307](#_Toc423366639)

[7 Appendix B: Product Behavior 339](#_Toc423366640)

[8 Change Tracking 369](#_Toc423366641)

[9 Index 375](#_Toc423366642)

# Introduction

The Domain Name Service (DNS) Server Management Protocol defines RPC interfaces that provide methods for remotely accessing and administering a DNS server. It is a client/server protocol based on RPC that is used in the configuration, management, and monitoring of a DNS server.

Sections 1.8, 2, and 3 of this specification are normative and can contain the terms MAY, SHOULD, MUST, MUST NOT, and SHOULD NOT as defined in [[RFC2119]](http://go.microsoft.com/fwlink/?LinkId=90317). Sections 1.5 and 1.9 are also normative but do not contain those terms. All other sections and examples in this specification are informative.

## Glossary

The following terms are specific to this document:

**access control list (ACL)**: A list of access control entries (ACEs) that collectively describe the security rules for authorizing access to some resource; for example, an object or set of objects.

**Active Directory**: A general-purpose network directory service. [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) also refers to the Windows implementation of a directory service. [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) stores information about a variety of objects in the network. Importantly, user accounts, computer accounts, groups, and all related credential information used by the Windows implementation of Kerberos are stored in [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90). [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) is either deployed as Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS). [[MS-ADTS]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ADTS%5d.pdf) describes both forms. For more information, see [[MS-AUTHSOD]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-AUTHSOD%5d.pdf) section 1.1.1.5.2, [**Lightweight Directory Access Protocol (LDAP)**](#gt_45643bfb-b4c4-432c-a10f-b98790063f8d) versions 2 and 3, Kerberos, and [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700).

**Active Directory domain**: A domain hosted on [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90). For more information, see [MS-ADTS].

**Active Directory domain controller promotion (DCPROMO)**: The act of causing a server to become a domain controller (DC).

**Active Directory forest**: See [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62).

**active refresh**: A self-generated DNS query for the DNSKEY records at a [**trust point**](#gt_34a102c7-7324-497c-b8d7-699067c619c0), for the purpose of automatically retrieving new [**trust anchors**](#gt_bfdbc40a-da75-45a3-a8bc-50cd4f2f9797) and removing revoked [**trust anchors**](#gt_bfdbc40a-da75-45a3-a8bc-50cd4f2f9797). See [[RFC5011]](http://go.microsoft.com/fwlink/?LinkId=225980).

**aging**: A concept in which a DNS server keeps track of time stamps for the last update of individual resource records. Duration from last [**time stamp**](#gt_391ec606-c265-48f2-aeeb-3245b5503121) to current time is considered as the age of the resource-record and this value is used for scavenging, a process for cleaning out not-recently used records.

**application directory partition**: An application NC.

**ASCII**: The American Standard Code for Information Interchange (ASCII) is an 8-bit character-encoding scheme based on the English alphabet. ASCII codes represent text in computers, communications equipment, and other devices that work with text. ASCII refers to a single 8-bit ASCII character or an array of 8-bit ASCII characters with the high bit of each character set to zero.

**authentication level**: A numeric value indicating the level of authentication or message protection that [**remote procedure call (RPC)**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) will apply to a specific message exchange. For more information, see [[C706]](http://go.microsoft.com/fwlink/?LinkId=89824) section 13.1.2.1 and [[MS-RPCE]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-RPCE%5d.pdf).

**authoritative**: A DNS server is [**authoritative**](#gt_ed54858d-02e4-4de3-b65b-e0b81c4185c7) for a portion of the DNS namespace if it hosts a primary or secondary [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) for that portion of the DNS namespace.

**autocreated zone**: A [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) that is created automatically by a DNS server, such as 0.in-addr.arpa, 127.in-addr.arpa or 255.in-addr.arpa.

**cache**: When a DNS server receives information from other servers, it stores the information for a certain amount of time in its own in-memory zones, also referred to as a DNS cache. This improves performance of domain name resolution and reduces DNS-related query traffic. The cache contains only nodes that have unexpired records and [**expired DNS records**](#gt_c0105e97-de24-448b-8514-78fd557e9164) that are not-yet-freed.

**cache scope**: A unique version of a cache [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) that can be created inside a DNS server cache. Resource records can then be added (and subsequently managed) in the cache scope. The cache scope behavior is the same as a DNS server cache.

**client subnet record**: A collection of [**IPv4**](#gt_0f25c9b5-dc73-4c3e-9433-f09d1f62ea8e) and [**IPv6**](#gt_64c29bb6-c8b2-4281-9f3a-c1eb5d2288aa) subnets grouped together. Each [**Client Subnet Record**](#gt_454a772d-d8fb-44b8-9b6d-39d624a813df) has a unique name.

**Coordinated Universal Time (UTC)**: A high-precision atomic time standard that approximately tracks Universal Time (UT). It is the basis for legal, civil time all over the Earth. Time zones around the world are expressed as positive and negative offsets from UTC. In this role, it is also referred to as Zulu time (Z) and Greenwich Mean Time (GMT). In these specifications, all references to UTC refer to the time at UTC-0 (or GMT).

**crossRef object**: An object residing in the partitions container of the config NC that describes the properties of a naming context (NC), such as its domain naming service name, operational settings, and so on.

**delegation**: A name server (NS) record set in a parent [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) that lists the name servers [**authoritative**](#gt_ed54858d-02e4-4de3-b65b-e0b81c4185c7) for a delegated subzone.

**directory server**: A persistent storage for DNS [**zones**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) and records. A DNS server can access DNS data stored in a [**directory server**](#gt_04fd0982-6bb6-44f1-817e-795715049c50) using the [**LDAP**](#gt_45643bfb-b4c4-432c-a10f-b98790063f8d) protocol or a similar directory access mechanism.

**directory server security descriptors**: The set of [**security descriptors**](#gt_e5213722-75a9-44e7-b026-8e4833f0d350) read from the [**directory server**](#gt_04fd0982-6bb6-44f1-817e-795715049c50), encompassing the DNS Server Configuration Access Control List, Zone Access Control List, and the Application Directory Partition Access Control List.

**directory-server-integrated**: A DNS server is [**directory-server-integrated**](#gt_0f196310-8f7b-462b-af06-6d955831d6f9) if a [**local directory server**](#gt_7d2b136f-4948-4166-9a7b-dc39ff5d10f3) such as [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) resides in the same machine as the DNS Server.

**distinguished name (DN)**: A name that uniquely identifies an object by using the [**relative distinguished name (RDN)**](#gt_22198321-b40b-4c24-b8a2-29e44d9d92b9) for the object, and the names of container objects and domains that contain the object. The distinguished name (DN) identifies the object and its location in a tree.

**DNS domain partition**: An [**application directory partition**](#gt_68dc613a-d602-41ae-9acc-76ffe97877c4) stored in the [**directory server**](#gt_04fd0982-6bb6-44f1-817e-795715049c50) that is replicated to all DNS servers in the domain.

**DNS forest partition**: An [**application directory partition**](#gt_68dc613a-d602-41ae-9acc-76ffe97877c4) stored in the [**directory server**](#gt_04fd0982-6bb6-44f1-817e-795715049c50) that is replicated to all DNS servers in the forest.

**DNS Operations**: DNS Query Processing, DNS Zone Transfer, DNS Recursive Query, and DNS Update are collectively called [**DNS Operations**](#gt_8536bec5-df4d-4463-82bc-4434a7ea493f).

**DNS policy**: A group of processing rules, based on which a [**DNS Operation**](#gt_8536bec5-df4d-4463-82bc-4434a7ea493f) is controlled and allowed or denied access. A [**DNS Policy**](#gt_5076749f-34a6-48a6-b051-8968a55f4d7b) can be at a server level or at a specific [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df). A DNS Policy is specific to a [**DNS Operation**](#gt_8536bec5-df4d-4463-82bc-4434a7ea493f).

**DNS policy criteria**: A NULL-terminated [**Unicode string**](#gt_b069acb4-e364-453e-ac83-42d469bb339e) that states one of the processing rules of a [**DNS Policy**](#gt_5076749f-34a6-48a6-b051-8968a55f4d7b).

**Domain Name System (DNS)**: A hierarchical, distributed database that contains mappings of domain names (1) to various types of data, such as IP addresses. DNS enables the location of computers and services by user-friendly names, and it also enables the discovery of other information stored in the database.

**dynamic endpoint**: A network-specific server address that is requested and assigned at run time. For more information, see [C706].

**dynamic update**: A mechanism defined in [[RFC2136]](http://go.microsoft.com/fwlink/?LinkId=107017) by which updates for DNS records can be sent to the authoritative DNS server for a [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) through the DNS protocol.

**expired DNS record**: A DNS record stored in the [**cache**](#gt_2f48e305-acf2-470e-b481-a0b7cc5fae4f) whose age is greater than the value of its [**TTL**](#gt_185c4181-772d-4458-bb90-ab0e11370a1c).

**forest**: (1) One or more domains that share a common schema and trust each other transitively. An organization can have multiple [**forests**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62). A [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62) establishes the security and administrative boundary for all the objects that reside within the domains that belong to the [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62). In contrast, a domain establishes the administrative boundary for managing objects, such as users, groups, and computers. In addition, each domain has individual security policies and trust relationships with other domains.

(2) In the [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) directory service, a [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62) is a set of naming contexts (NCs) consisting of one schema NC, one config NC, and one or more domain NCs. Because a set of NCs can be arranged into a tree structure, a [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62) is also a set of one or several trees of NCs.

**forwarder**: The [**forwarder**](#gt_001ff1c1-e24f-4766-a5b1-a5802871054f) is the kernel-mode component of the router that is responsible for forwarding data from one router interface to the others. The [**forwarder**](#gt_001ff1c1-e24f-4766-a5b1-a5802871054f) also decides whether a packet is destined for local delivery, whether it is destined to be forwarded out of another interface, or both. There are two kernel-mode [**forwarders**](#gt_025cfacf-ebc5-4659-971a-ee2ab5903575): unicast and multicast.

**forwarders**: A DNS server that is designated to facilitate forwarding of queries for other DNS servers.

**FSMO role**: A set of objects that can be updated in only one naming context (NC) replica (the FSMO role owner's replica) at any given time. For more information, see [MS-ADTS] section 3.1.1.1.11. See also [**FSMO role owner**](#gt_de81e9fd-25f5-4e90-aadb-1d35c5e8a06b).

**FSMO role owner**: The domain controller (DC) holding the naming context (NC) replica in which the objects of a [**FSMO role**](#gt_73841222-e9d8-4dc1-83a1-206c75f4f90f) can be updated.

**full zone transfer (AXFR)**: A DNS protocol mechanism [[RFC1035]](http://go.microsoft.com/fwlink/?LinkId=90264) through which an entire copy of a DNS [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) can be transmitted to a remote DNS server.

**fully qualified domain name (FQDN)**: An unambiguous domain name (2) that gives an absolute location in the [**Domain Name System's (DNS)**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) hierarchy tree, as defined in [RFC1035] section 3.1 and [[RFC2181]](http://go.microsoft.com/fwlink/?LinkId=127732) section 11.

**global name zone (GNZ)**: A zone that provides single-label name resolution for large enterprise networks that do not deploy [**WINS**](#gt_bafb050b-b593-4517-8093-f721bd2378ac) and where using domain name suffixes to provide single-label name resolution is not practical.

**globally unique identifier (GUID)**: A term used interchangeably with [**universally unique identifier (UUID)**](#gt_c4813fc3-b2e5-4aa3-bde7-421d950d68d3) in Microsoft protocol technical documents (TDs). Interchanging the usage of these terms does not imply or require a specific algorithm or mechanism to generate the value. Specifically, the use of this term does not imply or require that the algorithms described in [[RFC4122]](http://go.microsoft.com/fwlink/?LinkId=90460) or [C706] must be used for generating the [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1). See also [**universally unique identifier (UUID)**](#gt_c4813fc3-b2e5-4aa3-bde7-421d950d68d3).

**glue record**: A record of type A or AAAA included in a zone to specify the IP address of a DNS server used in a delegation. The fully qualified domain name of each glue record will match the fully qualified domain name of an authoritative DNS server found in one of the NS records in the delegation.

**incremental zone transfer (IXFR)**: A DNS protocol mechanism [[RFC1995]](http://go.microsoft.com/fwlink/?LinkId=106956) through which a partial copy of a DNS [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) can be transmitted to a remote DNS server. An incremental zone transfer, or IXFR, is represented as a sequence of DNS record changes that can be applied to one image of a [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) to synchronize it with another image of a [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df).

**Interface Definition Language (IDL)**: The International Standards Organization (ISO) standard language for specifying the interface for remote procedure calls. For more information, see [C706] section 4.

**Internet Protocol version 4 (IPv4)**: An Internet protocol that has 32-bit source and destination addresses. IPv4 is the predecessor of IPv6.

**Internet Protocol version 6 (IPv6)**: A revised version of the Internet Protocol (IP) designed to address growth on the Internet. Improvements include a 128-bit IP address size, expanded routing capabilities, and support for authentication (2) and privacy.

**key master**: A DNS server that is responsible for generating and maintaining DNSSEC signing keys for one particular [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df).

**key rollover**: The process through which DNSSEC signing keys are updated as described in [[RFC4641]](http://go.microsoft.com/fwlink/?LinkId=225979) and [RFC5011].

**key signing key (KSK)**: A DNSKEY used to sign only the DNSKEY record set at the root of the [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df), as defined in [RFC4641].

**lame delegation**: A [**delegation**](#gt_32174781-13ee-48b0-8fc0-ef6bbe207573) in which none of the name servers listed in the [**delegation**](#gt_32174781-13ee-48b0-8fc0-ef6bbe207573) host the delegated subzone or respond to DNS queries.

**Lightweight Directory Access Protocol (LDAP)**: The primary access protocol for [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90). Lightweight Directory Access Protocol (LDAP) is an industry-standard protocol, established by the Internet Engineering Task Force (IETF), which allows users to query and update information in a directory service (DS), as described in [MS-ADTS]. The Lightweight Directory Access Protocol can be either version 2 [RFC1777] or version 3 [RFC3377].

**local directory server**: A [**directory server**](#gt_04fd0982-6bb6-44f1-817e-795715049c50) instance on the same host as the DNS server.

**local domain controller (DC)**: A domain controller (DC) on which the current method is executing.

**multizone operation**: An operation requested to be performed on a set of [**zones**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) with one or more particular properties, rather than on a single zone.

**multizone operation string**: A string indicating a property defining a set of [**zones**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) on which an operation is to be performed.

**naming context root (NC Root)**: The specific directory object referenced by the naming context dsname.

**Network Data Representation (NDR)**: A specification that defines a mapping from [**Interface Definition Language (IDL)**](#gt_73177eec-4092-420f-92c5-60b2478df824) data types onto octet streams. [**NDR**](#gt_9ebf9540-2c31-43bc-bc56-4a932faabf2d) also refers to the runtime environment that implements the mapping facilities (for example, data provided to [**NDR**](#gt_9ebf9540-2c31-43bc-bc56-4a932faabf2d)). For more information, see [MS-RPCE] and [C706] section 14.

**network mask**: A bit vector that, when logically AND-ed with an IP address, indicates the subnet to which an IP address belongs. Also known as net mask.

**node**: An entry identified by name in a DNS [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df). A [**node**](#gt_762051d8-4fdc-437e-af9d-3f4da77c3c7d) contains all of the DNS records sets associated with the name.

**nonkey master primary server**: In a file-backed signed zone, a nonkey master primary is a server that holds the primary copy of the signed zone. A nonkey master primary server can also do signature refreshes and Zone Signing using Zone Signing Keys but cannot generate or manage keys on its own.

**NoRefresh interval**: If an update which does not change the DNS data for a record set is received within the [**NoRefresh interval**](#gt_d826a56a-099e-41a2-8055-df5e0d2c51c6) then the DNS server will not update the timestamp on the record. This allows the DNS server to avoid unnecessary updates to the data store.

**online signing**: Refers to the process of signing and maintaining DNSSEC characteristics of a zone. Windows Server 2012 operating system and Windows Server 2012 R2 operating system support automatic DNSSEC signing of [**zones**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df).

**opnum**: An operation number or numeric identifier that is used to identify a specific [**remote procedure call (RPC)**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) method or a method in an interface. For more information, see [C706] section 12.5.2.12 or [MS-RPCE].

**primary DNS server**: A DNS server that holds a master authoritative copy of a particular zone's data in local persistent storage.

**primary server**: In a DHCPv4 server failover configuration, the [**primary server**](#gt_bb76b8f0-0929-47c8-a06a-d3f9a8761d93) in the failover relationship is the first server that is used when an attempt is made by a DHCP client to obtain an IP address and options. A server is primary in the context of a subnet. However, a [**primary server**](#gt_bb76b8f0-0929-47c8-a06a-d3f9a8761d93) for a given subnet can also be a secondary server for another subnet.

**primary zone**: A zone for which a master authoritative copy of data is held in persistent local storage or in a locally accessible [**directory server**](#gt_04fd0982-6bb6-44f1-817e-795715049c50). A zone stored in a [**directory server**](#gt_04fd0982-6bb6-44f1-817e-795715049c50) is a [**primary zone**](#gt_7205eedf-f027-4da5-8f65-18966a86a17a) for any DNS server that can retrieve a copy of it from its [**local directory server**](#gt_7d2b136f-4948-4166-9a7b-dc39ff5d10f3).

**read-only domain controller (RODC)**: A domain controller (DC) that does not accept originating updates. Additionally, an [**RODC**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870) does not perform outbound replication. An RODC cannot be the primary domain controller (PDC) for its domain.

**refresh interval**: If the [**NoRefresh interval**](#gt_d826a56a-099e-41a2-8055-df5e0d2c51c6) for a record has expired and the DNS server receives a DNS update that does not change the record data then the DNS server will commit a new timestamp to the data store. The combination of NoRefresh and [**refresh intervals**](#gt_ca2f2a4a-91f1-4547-809e-00bd8e41211c) allows a DNS server to maintain a relatively accurate record timestamp without unnecessary updates to the data store.

**relative distinguished name (RDN)**: The name of an object relative to its parent. This is the leftmost attribute-value pair in the [**distinguished name (DN)**](#gt_1175dd11-9368-41d5-98ed-d585f268ad4b) of an object. For example, in the [**DN**](#gt_1175dd11-9368-41d5-98ed-d585f268ad4b) "cn=Peter Houston, ou=NTDEV, dc=microsoft, dc=com", the [**RDN**](#gt_22198321-b40b-4c24-b8a2-29e44d9d92b9) is "cn=Peter Houston". For more information, see [[RFC2251]](http://go.microsoft.com/fwlink/?LinkId=90325).

**remote procedure call (RPC)**: A context-dependent term commonly overloaded with three meanings. Note that much of the industry literature concerning RPC technologies uses this term interchangeably for any of the three meanings. Following are the three definitions: (\*) The runtime environment providing remote procedure call facilities. The preferred usage for this meaning is "RPC runtime". (\*) The pattern of request and response message exchange between two parties (typically, a client and a server). The preferred usage for this meaning is "RPC exchange". (\*) A single message from an exchange as defined in the previous definition. The preferred usage for this term is "RPC message". For more information about RPC, see [C706].

**resource record (RR)**: A single piece of DNS data. Each [**resource record**](#gt_49c03845-ca86-48f5-9cbf-ab86c624aa29) consists of a DNS type, a DNS class, a time to live (TTL), and record data (RDATA) appropriate for the [**resource record's**](#gt_49c03845-ca86-48f5-9cbf-ab86c624aa29) DNS type.

**root directory system agent-specific entry (rootDSE)**: The logical root of a directory server, whose [**distinguished name (DN)**](#gt_1175dd11-9368-41d5-98ed-d585f268ad4b) is the empty string. In the [**Lightweight Directory Access Protocol (LDAP)**](#gt_45643bfb-b4c4-432c-a10f-b98790063f8d), the [**rootDSE**](#gt_29942b69-e0ed-4fe7-bbbf-1a6a3f9eeeb6) is a nameless entry (a [**DN**](#gt_1175dd11-9368-41d5-98ed-d585f268ad4b) with an empty string) containing the configuration status of the server. Access to this entry is typically available to unauthenticated clients. The [**rootDSE**](#gt_29942b69-e0ed-4fe7-bbbf-1a6a3f9eeeb6) contains attributes that represent the features, capabilities, and extensions provided by the particular server.

**root hints**: DNS [**root hints**](#gt_87238b98-87ff-4d10-bc86-06cd6b3bad5c) contain host information that is needed to resolve names outside of the [**authoritative**](#gt_ed54858d-02e4-4de3-b65b-e0b81c4185c7) DNS domains. It contains names and addresses of the root DNS servers.

**RPC transport**: The underlying network services used by the remote procedure call (RPC) runtime for communications between network nodes. For more information, see [C706] section 2.

**scavenging**: A regularly scheduled process in which the state of database records are changed if they have not been updated within a certain time interval, measured by the process that checks whether current time exceeds the record’s time stamp value.

**secondary DNS server**: A DNS server that holds an authoritative read-only copy of a particular zone's data. The copy is periodically copied from another authoritative DNS server. Each zone can have any number of secondary DNS servers.

**secondary zone**: A zone for which an authoritative read-only copy of data is hosted by a particular DNS server. The data for a secondary zone is periodically copied from another DNS server that is authoritative for the zone.

**secret key transaction authentication (TSIG)**: An authentication mechanism specified in [[RFC2845]](http://go.microsoft.com/fwlink/?LinkId=90388) for DNS [**dynamic updates**](#gt_dbff570c-a709-479a-980a-5b74ac7ab2e7) that uses a one-way hashing function to provide a cryptographically secure means of identifying each endpoint.

**secure delegation**: A delegation in a parent zone (name server (NS) record set), along with a signed delegation signer (DS) record set, signifying a delegation to a signed subzone.

**secure dynamic update**: A modification of the [**dynamic update**](#gt_dbff570c-a709-479a-980a-5b74ac7ab2e7) mechanism defined in [[RFC3645]](http://go.microsoft.com/fwlink/?LinkId=90440) by which updates for DNS records can be sent securely to the authoritative DNS server for a [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) through the DNS protocol.

**security context**: An abstract data structure that contains authorization information for a particular security principal in the form of a Token/Authorization Context (see [[MS-DTYP]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-DTYP%5d.pdf) section 2.5.2). A server uses the authorization information in a [**security context**](#gt_88d49f20-6c95-4b64-a52c-c3eca2fe5709) to check access to requested resources. A [**security context**](#gt_88d49f20-6c95-4b64-a52c-c3eca2fe5709) also contains a key identifier that associates mutually established cryptographic keys, along with other information needed to perform secure communication with another security principal.

**security descriptor**: A data structure containing the security information associated with a securable object. A [**security descriptor**](#gt_e5213722-75a9-44e7-b026-8e4833f0d350) identifies an object's owner by its security identifier (SID). If access control is configured for the object, its [**security descriptor**](#gt_e5213722-75a9-44e7-b026-8e4833f0d350) contains a discretionary access control list (DACL) with SIDs for the security principals who are allowed or denied access. Applications use this structure to set and query an object's security status. The [**security descriptor**](#gt_e5213722-75a9-44e7-b026-8e4833f0d350) is used to guard access to an object as well as to control which type of auditing takes place when the object is accessed. The [**security descriptor**](#gt_e5213722-75a9-44e7-b026-8e4833f0d350) format is specified in [MS-DTYP] section 2.4.6; a string representation of [**security descriptors**](#gt_e5213722-75a9-44e7-b026-8e4833f0d350), called SDDL, is specified in [MS-DTYP] section 2.5.1.

**security provider**: A pluggable security module that is specified by the protocol layer above the [**remote procedure call (RPC)**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) layer, and will cause the [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) layer to use this module to secure messages in a communication session with the server. The security provider is sometimes referred to as an authentication service. For more information, see [C706] and [MS-RPCE].

**security support provider (SSP)**: A dynamic-link library (DLL) that implements the [**Security Support Provider Interface (SSPI)**](#gt_fb216516-748b-4873-8bdd-64c5f4da9920) by making one or more security packages available to applications. Each security package provides mappings between an application's [**SSPI**](#gt_fb216516-748b-4873-8bdd-64c5f4da9920) function calls and an actual security model's functions. Security packages support security protocols such as Kerberos authentication and NTLM.

**Security Support Provider Interface (SSPI)**: A Windows-specific API implementation that provides the means for connected applications to call one of several security providers to establish authenticated connections and to exchange data securely over those connections. This is the Windows equivalent of Generic Security Services (GSS)-API, and the two families of APIs are on-the-wire compatible.

**serial number**: A field in the [**SOA**](#gt_0365bdcc-f1f5-4494-b57c-02c897b7ea8a) record [RFC1035] for a [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df). This value is used to compare different versions of [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df).

**server level policy**: A policy can be specified at each scope (subnet) or it can be specified global to the DHCP server. A policy which is global to the DHCP server is referred as a server-level policy and applies to all the scopes configured on the DHCP server.

**server scope**: A collection of DNS server settings with a unique name. The DNS server behavior is determined by the applied server scope.

**signing key descriptor (SKD)**: A collection of DNSSEC signing key characteristics such as algorithm, key length, and signature validity period that describe how DNSSEC signing keys and corresponding signatures should be generated and maintained by the DNS server.

**single-label name**: A domain name consisting of exactly one label [for example contoso. (an absolute name) or contoso (a relative name)]. When written in dotted-notation [[RFC1034]](http://go.microsoft.com/fwlink/?LinkId=90263), a [**single-label name**](#gt_711c326a-c3c3-4f78-9e92-b10b5581c59c) will contain at most one period (.).

**start of authority (SOA)**: Every [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) contains a [**SOA**](#gt_0365bdcc-f1f5-4494-b57c-02c897b7ea8a) record as defined in [RFC1035] section 3.3.13 and clarified in [RFC2181] section 7 at the beginning of the [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) that provides information relevant for a [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df).

**stub**: Used as specified in [C706] section 2.1.2.2. A [**stub**](#gt_4cef864e-5108-43a7-a631-68ffc7967546) that is used on the client is called a "client [**stub**](#gt_4cef864e-5108-43a7-a631-68ffc7967546)", and a [**stub**](#gt_4cef864e-5108-43a7-a631-68ffc7967546) that is used on the server is called a "server [**stub**](#gt_4cef864e-5108-43a7-a631-68ffc7967546)".

**stub zone**: A specialized version of a secondary [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df). A stub [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) contains only those resource records that are necessary to identify the [**authoritative**](#gt_ed54858d-02e4-4de3-b65b-e0b81c4185c7) DNS server for that [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df). A stub [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) consists of the [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) root [**SOA**](#gt_0365bdcc-f1f5-4494-b57c-02c897b7ea8a) [**resource record**](#gt_49c03845-ca86-48f5-9cbf-ab86c624aa29) [RFC1035] and [RFC2181], [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) root NS resource records [RFC1035], and glue [**resource records**](#gt_49c03845-ca86-48f5-9cbf-ab86c624aa29) for the [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) root [**SOA**](#gt_0365bdcc-f1f5-4494-b57c-02c897b7ea8a) and NS records.

**time stamp**: An integer value representing the number of hours that have elapsed since midnight (00:00:00), January 1, 1601 UTC.

**Time-To-Live (TTL)**: The time duration for which a Server Object is available.

**tombstone**: An inactive DNS node which is not considered to be part of a DNS [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) but has not yet been deleted from the [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) database in the [**directory server**](#gt_04fd0982-6bb6-44f1-817e-795715049c50). [**Tombstones**](#gt_9d8e0963-13fa-4e19-a97f-7ce6bc90d20f) may be permanently deleted from the [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) once they reach a certain age. [**Tombstones**](#gt_9d8e0963-13fa-4e19-a97f-7ce6bc90d20f) are not used for DNS [**zones**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) that are not stored in the [**directory server**](#gt_04fd0982-6bb6-44f1-817e-795715049c50). A node is a tombstone if its dnsTombstoned attribute has been set to "TRUE".

**trust anchor**: A DNSKEY (public key) or DS (public key hash) record that is presumed to be authentic (that is trusted); a DNSKEY or DS record that is in the "TrustAnchors" zone. A DS [**trust anchor**](#gt_bfdbc40a-da75-45a3-a8bc-50cd4f2f9797) cannot be used in a DNSSEC proof, but it can serve as an authentication of a retrieved DNSKEY record, allowing it to become a DNSKEY [**trust anchor**](#gt_bfdbc40a-da75-45a3-a8bc-50cd4f2f9797).

**trust point**: An [**FQDN**](#gt_1769aec9-237e-44ed-9014-1abb3ec6de6e) that has one or more [**trust anchors**](#gt_bfdbc40a-da75-45a3-a8bc-50cd4f2f9797); a point in the DNS namespace from which a DNSSEC proof can begin, via the presumption of trust anchor authenticity; a node in the "TrustAnchors" zone that contains a DS or DNSKEY record.

**Unicode string**: A Unicode 8-bit string is an ordered sequence of 8-bit units, a Unicode 16-bit string is an ordered sequence of 16-bit code units, and a Unicode 32-bit string is an ordered sequence of 32-bit code units. In some cases, it may be acceptable not to terminate with a terminating null character. Unless otherwise specified, all [**Unicode strings**](#gt_b069acb4-e364-453e-ac83-42d469bb339e) follow the [**UTF-16LE**](#gt_69864bcc-33be-41c9-9486-e18618ee3dd0) encoding scheme with no Byte Order Mark (BOM).

**universally unique identifier (UUID)**: A 128-bit value. UUIDs can be used for multiple purposes, from tagging objects with an extremely short lifetime, to reliably identifying very persistent objects in cross-process communication such as client and server interfaces, manager entry-point vectors, and [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) objects. UUIDs are highly likely to be unique. UUIDs are also known as [**globally unique identifiers (GUIDs)**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) and these terms are used interchangeably in the Microsoft protocol technical documents (TDs). Interchanging the usage of these terms does not imply or require a specific algorithm or mechanism to generate the UUID. Specifically, the use of this term does not imply or require that the algorithms described in [RFC4122] or [C706] must be used for generating the UUID.

**User Datagram Protocol (UDP)**: The connectionless protocol within TCP/IP that corresponds to the transport layer in the ISO/OSI reference model.

**UTF-16LE**: The Unicode Transformation Format - 16-bit, Little Endian encoding scheme. It is used to encode Unicode characters as a sequence of 16-bit codes, each encoded as two 8-bit bytes with the least-significant byte first.

**UTF-8**: A byte-oriented standard for encoding Unicode characters, defined in the Unicode standard. Unless specified otherwise, this term refers to the UTF-8 encoding form specified in [[UNICODE5.0.0/2007]](http://go.microsoft.com/fwlink/?LinkId=154659) section 3.9.

**Windows Internet Name Service (WINS)**: A name service for the NetBIOS protocol, particularly designed to ease transition to a TCP/IP based network. The Microsoft implementation of an NBNS server.

**Windows Internet Name Service Reverse Lookup (WINS-R)**: A form of reverse lookup performed by the DNS server using NBSTAT [[RFC1002]](http://go.microsoft.com/fwlink/?LinkId=90261) lookups to map IPv4 addresses to single-label names.

**zone**: A domain namespace is divided up into several sections called zones [RFC1034] and [RFC2181]. A [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) represents authority over a portion of the DNS namespace, excluding any subzones that are below [**delegations**](#gt_32174781-13ee-48b0-8fc0-ef6bbe207573).

**zone scope**: A unique version of a [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) that can be created inside an existing zone. Resource records can then be added (and subsequently managed) to the zone scope.

**zone signing key (ZSK)**: A DNSKEY used to sign all of the records in a zone, as defined in [RFC4641].

**zone transfer**: A DNS protocol mechanism [RFC1035] by which a full or partial copy of a DNS [**zone**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df) can be transmitted from one DNS server to another.

**MAY, SHOULD, MUST, SHOULD NOT, MUST NOT:** These terms (in all caps) are used as defined in [[RFC2119]](http://go.microsoft.com/fwlink/?LinkId=90317). All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

## References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the [Errata](http://msdn.microsoft.com/en-us/library/dn781092.aspx).

### Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com). We will assist you in finding the relevant information.

[ATMA] Technical Committee, ATM Forum, "ATM Name System Specification Version 1.0", [http://www.ipmplsforum.org/ftp/pub/approved-specs/af-saa-0069.000.pdf](http://go.microsoft.com/fwlink/?LinkId=107028)

[C706] The Open Group, "DCE 1.1: Remote Procedure Call", C706, August 1997, [https://www2.opengroup.org/ogsys/catalog/c706](http://go.microsoft.com/fwlink/?LinkId=89824)

[DRAFT-DNSSEC-ECDSA] Hoffman, P., and Wijngaards, W., "Elliptic Curve DSA for DNSSEC", draft-hoffman-dnssec-ecdsa-04, December 2010, [http://tools.ietf.org/html/draft-hoffman-dnssec-ecdsa-04.txt](http://go.microsoft.com/fwlink/?LinkId=229294)

[FIPS186] FIPS PUBS, "Digital Signature Standard (DSS)", FIPS PUB 186-3, June 2009, [http://csrc.nist.gov/publications/fips/fips186-3/fips\_186-3.pdf](http://go.microsoft.com/fwlink/?LinkId=89869)

[FIPS197] FIPS PUBS, "Advanced Encryption Standard (AES)", FIPS PUB 197, November 2001, [http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf](http://go.microsoft.com/fwlink/?LinkId=89870)

[IANA-DNSSECAN] IANA, "Domain Name System Security (DNSSEC) Algorithm Numbers", [http://www.iana.org/assignments/dns-sec-alg-numbers](http://go.microsoft.com/fwlink/?LinkId=225982)

[IANA-DNS] IANA, "Domain Name System (DNS) Parameters", April 2009, [http://www.iana.org/assignments/dns-parameters](http://go.microsoft.com/fwlink/?LinkId=148574)

[IANA-PROTO-NUM] IANA, "Protocol Numbers", February 2007, [http://www.iana.org/assignments/protocol-numbers](http://go.microsoft.com/fwlink/?LinkId=89889)

[IANAPORT] IANA, "Service Name and Transport Protocol Port Number Registry", November 2006, [http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml](http://go.microsoft.com/fwlink/?LinkId=89888)

[MS-ADA1] Microsoft Corporation, "[Active Directory Schema Attributes A-L](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ADA1%5d.pdf)".

[MS-ADA2] Microsoft Corporation, "[Active Directory Schema Attributes M](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ADA2%5d.pdf)".

[MS-ADA3] Microsoft Corporation, "[Active Directory Schema Attributes N-Z](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ADA3%5d.pdf)".

[MS-ADSC] Microsoft Corporation, "[Active Directory Schema Classes](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ADSC%5d.pdf)".

[MS-ADTS] Microsoft Corporation, "[Active Directory Technical Specification](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ADTS%5d.pdf)".

[MS-DTYP] Microsoft Corporation, "[Windows Data Types](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-DTYP%5d.pdf)".

[MS-ERREF] Microsoft Corporation, "[Windows Error Codes](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ERREF%5d.pdf)".

[MS-GKDI] Microsoft Corporation, "[Group Key Distribution Protocol](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-GKDI%5d.pdf)".

[MS-NRPC] Microsoft Corporation, "[Netlogon Remote Protocol](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-NRPC%5d.pdf)".

[MS-RPCE] Microsoft Corporation, "[Remote Procedure Call Protocol Extensions](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-RPCE%5d.pdf)".

[MS-WINSRA] Microsoft Corporation, "[Windows Internet Naming Service (WINS) Replication and Autodiscovery Protocol](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-WINSRA%5d.pdf)".

[RFC1034] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, November 1987, [http://www.ietf.org/rfc/rfc1034.txt](http://go.microsoft.com/fwlink/?LinkId=90263)

[RFC1035] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, November 1987, [http://www.ietf.org/rfc/rfc1035.txt](http://go.microsoft.com/fwlink/?LinkId=90264)

[RFC1183] Everhart, C., Mamakos, L., Ullman, R. and Mockapetris, P., "New DNS RR Definitions", RFC 1183, October 1990, [http://www.ietf.org/rfc/rfc1183.txt](http://go.microsoft.com/fwlink/?LinkId=106947)

[RFC1738] Berners-Lee, T., Masinter, L., and McCahill, M., Eds., "Uniform Resource Locators (URL)", RFC 1738, December 1994, [http://www.ietf.org/rfc/rfc1738.txt](http://go.microsoft.com/fwlink/?LinkId=90287)

[RFC1876] Davis, C., Vixie, P., Goodwin, T., et al., "A Means for Expression Location Information in the Domain Name System", RFC 1876, January 1996, [http://www.ietf.org/rfc/rfc1876.txt](http://go.microsoft.com/fwlink/?LinkId=106954)

[RFC1982] Elz, R., and Bush, R., "Serial Number Arithmetic", RFC 1982, August 1996, [http://www.ietf.org/rfc/rfc1982.txt](http://go.microsoft.com/fwlink/?LinkId=184551)

[RFC1995] Ohta, M., "Incremental Zone Transfer in DNS", RFC 1995, August 1996, [http://www.ietf.org/rfc/rfc1995.txt](http://go.microsoft.com/fwlink/?LinkId=106956)

[RFC1996] Vixie, P., "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)", RFC 1996, August 1996, [http://www.ietf.org/rfc/rfc1996.txt](http://go.microsoft.com/fwlink/?LinkId=106957)

[RFC2065] Eastlake, D., and Kaufman, C., "Domain Name System Security Extensions", RFC 2065, January 1997, [http://www.ietf.org/rfc/rfc2065.txt](http://go.microsoft.com/fwlink/?LinkId=106958)

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, [http://www.rfc-editor.org/rfc/rfc2119.txt](http://go.microsoft.com/fwlink/?LinkId=90317)

[RFC2136] Thomson, S., Rekhter Y. and Bound, J., "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997, [http://www.ietf.org/rfc/rfc2136.txt](http://go.microsoft.com/fwlink/?LinkId=107017)

[RFC2181] Elz, R., and Bush, R., "Clarifications to the DNS Specification", RFC 2181, July 1997, [http://www.ietf.org/rfc/rfc2181.txt](http://go.microsoft.com/fwlink/?LinkId=127732)

[RFC2308] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", RFC 2308, March 1998, [http://www.ietf.org/rfc/rfc2308.txt](http://go.microsoft.com/fwlink/?LinkId=187326)

[RFC2535] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999, [http://tools.ietf.org/html/rfc2535.txt](http://go.microsoft.com/fwlink/?LinkId=107021)

[RFC2671] Vixie, P., "Extension mechanism for DNS", RFC 2671, August 1999, [http://www.ietf.org/rfc/rfc2671.txt](http://go.microsoft.com/fwlink/?LinkId=107022)

[RFC2672] Crawford, M., and Fermilab, "Non-Terminal DNS Name Redirection", RFC 2672, August 1999, [http://www.ietf.org/rfc/rfc2672.txt](http://go.microsoft.com/fwlink/?LinkId=132207)

[RFC2782] Gulbrandsen, A., Vixie, P., and Esibov, L., "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000, [http://www.ietf.org/rfc/rfc2782.txt](http://go.microsoft.com/fwlink/?LinkId=90381)

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake III, D., and Wellington, B., "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000, [http://www.ietf.org/rfc/rfc2845.txt](http://go.microsoft.com/fwlink/?LinkId=90388)

[RFC2915] Mealling, M., and Daniel, R., "The Naming Authority Pointer (NAPTR) DNS Resource Record", RFC 2915, September 2000, [http://www.ietf.org/rfc/rfc2915.txt](http://go.microsoft.com/fwlink/?LinkId=107024)

[RFC2930] Eastlake III, D., "Secret Key Establishment for DNS (TKEY RR)", RFC 2930, September 2000, [http://www.ietf.org/rfc/rfc2930.txt](http://go.microsoft.com/fwlink/?LinkId=90397)

[RFC2931] Eastlake, D., "DNS Request and Transaction Signature (SIG (0) s)", RFC 2931, September 2000, [http://www.ietf.org/rfc/rfc2931.txt](http://go.microsoft.com/fwlink/?LinkId=107025)

[RFC3403] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database", RFC 3403, October 2002, [http://www.ietf.org/rfc/rfc3403.txt](http://go.microsoft.com/fwlink/?LinkId=107026)

[RFC3447] Jonsson, J. and Kaliski, B., "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003, [http://www.ietf.org/rfc/rfc3447.txt](http://go.microsoft.com/fwlink/?LinkId=90422)

[RFC3565] Schaad, J., "Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)", RFC 3565, July 2003, [http://www.ietf.org/rfc/rfc3565.txt](http://go.microsoft.com/fwlink/?LinkId=229738)

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and Souissi, M., "DNS Extensions to Support IP version 6", RFC 3596, October 2003, [http://www.ietf.org/rfc/rfc3596.txt](http://go.microsoft.com/fwlink/?LinkId=107027)

[RFC3597] Gustafsson, A., "Handling of Unknown DNS Resource Record (RR) Types", RFC3597, September 2003, [http://www.ietf.org/rfc/rfc3597.txt](http://go.microsoft.com/fwlink/?LinkID=532820)

[RFC3629] Yergeau, F., "UTF-8, A Transformation Format of ISO 10646", STD 63, RFC 3629, November 2003, [http://www.ietf.org/rfc/rfc3629.txt](http://go.microsoft.com/fwlink/?LinkId=90439)

[RFC3645] Kwan, S., Garg, P., Gilroy, J., Esibov, L., Westhead, J., and Hall, R., "Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)", RFC 3645, October 2003, [http://www.ietf.org/rfc/rfc3645.txt](http://go.microsoft.com/fwlink/?LinkId=90440)

[RFC3852] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3852, July 2004, [http://www.ietf.org/rfc/rfc3852.txt](http://go.microsoft.com/fwlink/?LinkId=90445)

[RFC4033] Arends, R., Austein, R., Lason, M., et al., "DNS Security Introduction and Requirements", RFC 4033, March 2005, [http://www.ietf.org/rfc/rfc4033.txt](http://go.microsoft.com/fwlink/?LinkId=107051)

[RFC4034] Arends, R., Austein, R., Lason, M., et al., "Resource Records for the DNS Security Extensions", RFC 4034, March 2005, [http://www.ietf.org/rfc/rfc4034.txt](http://go.microsoft.com/fwlink/?LinkId=107052)

[RFC4035] Arends, R., Austein, R., Lason, M., et al., "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005, [http://www.ietf.org/rfc/rfc4035.txt](http://go.microsoft.com/fwlink/?LinkID=107053)

[RFC4511] Sermersheim, J., "Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, June 2006, [http://www.rfc-editor.org/rfc/rfc4511.txt](http://go.microsoft.com/fwlink/?LinkId=157505)

[RFC4641] Kolkman, O., and Gieben, R., "DNSSEC Operational Practices", RFC 4641, September 2006, [http://www.ietf.org/rfc/rfc4641.txt](http://go.microsoft.com/fwlink/?LinkId=225979)

[RFC4701] Stapp, M., Lemon, T., and Gustafsson, A., "A DNS Resource Record (RR) for Encoding Dynamic Host Configuration Protocol (DHCP) Information (DHCID RR)", RFC 4701, October 2006, [http://www.ietf.org/rfc/rfc4701.txt](http://go.microsoft.com/fwlink/?LinkId=125431)

[RFC5011] StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", RFC 5011, September 2007, [http://www.ietf.org/rfc/rfc5011.txt](http://go.microsoft.com/fwlink/?LinkId=225980)

[RFC5084] Housley, R., "Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS)", RFC 5084, November 2007, [http://www.ietf.org/rfc/rfc5084.txt](http://go.microsoft.com/fwlink/?LinkId=229742)

[RFC5155] Laurie, B., Sisson, G., Arends, R., and Blacka, D., "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, March 2008, [http://www.ietf.org/rfc/rfc5155.txt](http://go.microsoft.com/fwlink/?LinkId=225981)

[RFC6698] Hoffman, P. and Schlyter, J, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC6698, August 2012, [http://www.ietf.org/rfc/rfc6698.txt](http://go.microsoft.com/fwlink/?LinkId=532821)

[SP800-38D] National Institute of Standards and Technology., "Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", November 2007, [http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf](http://go.microsoft.com/fwlink/?LinkId=186038)

[UNICODE5.0.0/2007] The Unicode Consortium, "Unicode 5.0.0", 2007, [http://www.unicode.org/versions/Unicode5.0.0/](http://go.microsoft.com/fwlink/?LinkId=154659)

[X690] ITU-T, "Information Technology - ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", Recommendation X.690, July 2002, [http://www.itu.int/rec/T-REC-X.690/en](http://go.microsoft.com/fwlink/?LinkId=90593)

### Informative References

[MSDN-RPC] Microsoft Corporation, "Remote Procedure Call", [http://msdn.microsoft.com/en-us/library/aa378651.aspx](http://go.microsoft.com/fwlink/?LinkId=90075)

[MSKB-2919355] Microsoft Corporation, "Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 Update: April 2014", [http://support.microsoft.com/kb/2919355](http://go.microsoft.com/fwlink/?LinkId=397642)

## Overview

The DNS Server Management Protocol is a client/server protocol that is used to remotely query, monitor and configure DNS server settings, its [**zones**](#gt_e6a86700-c17d-4513-8f4f-5aacaff014df), and [**resource records**](#gt_49c03845-ca86-48f5-9cbf-ab86c624aa29). The protocol allows a client to access DNS server settings and properties and also to enumerate all DNS data stored on the server (DNS zones and DNS records).

The DNS Server Management Protocol is a simple protocol with no state shared across [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) method calls. Each RPC method call contains one complete request. Output from one method call can be used as input to another call but the DNS Server Management Protocol does not provide for locking of DNS data across method calls. For example, a client may enumerate DNS zones with one call and then retrieve the properties of one or more of the enumerated DNS zones with another call, but no guarantee is made that the zone has not been deleted by another DNS Server Management Protocol client between these two method calls.

When the DNS server is [**directory server-integrated**](#gt_0f196310-8f7b-462b-af06-6d955831d6f9), some client requests may require or trigger [**Lightweight Directory Access Protocol (LDAP)**](#gt_45643bfb-b4c4-432c-a10f-b98790063f8d) requests from the DNS server to the [**local directory server**](#gt_7d2b136f-4948-4166-9a7b-dc39ff5d10f3) or another directory server.

In particular, the DNS Server may use the "defaultNamingContext" of the directory server's [**rootDSE**](#gt_29942b69-e0ed-4fe7-bbbf-1a6a3f9eeeb6), a [**DNS domain partition**](#gt_24873c07-a6aa-4d4b-8064-fa64dff80204) named "DnsDomainZones", or a [**DNS forest partition**](#gt_6e0d87be-b750-4025-9241-0d1ba904f1f8) named "DnsForestZones" to store zone information and zone records. (See section [2.3](#Section_74db40e109174ecb863d9bce5165ebf3) for a discussion of the schemas used to store this information.) A DNS Server integrated with a directory server creates and automatically enlists itself in these default [**application directory partitions**](#gt_68dc613a-d602-41ae-9acc-76ffe97877c4). Alternatively, zone information and zone records may be stored in additional application directory partitions, which can be created (and removed) by the DNS Server Management Protocol client in order to control the granularity of zone replication. Zones created in these additional application directory partitions will only be visible to directory servers enlisted in those partitions, thus allowing for granular control over replication.

A typical remote management involves the client querying or setting the configuration parameters of the DNS server. The client may also enumerate DNS zones and the DNS records stored in one or more zones. The client can modify the configuration of the DNS server as required. The client can also add, delete, or modify DNS zones or the DNS records held in zones as required. For example, a remote management client can:

* Set or retrieve the server's [**forwarders**](#gt_025cfacf-ebc5-4659-971a-ee2ab5903575).
* Set or retrieve various DNS server settings.
* Create or modify zones.
* Create or modify zone records.

This usually involves sending a request to the DNS server specifying the type of operation (get, set and execute are examples of types of operations) to perform and any specific parameters that are associated with that operation. The DNS server responds to the client with the result of the operation.

The following diagram shows an example of a remote client creating a zone on the DNS server using the DNS server Management Protocol. The client sends a request to the server with the operation type and parameters. The server responds with a success or an error.

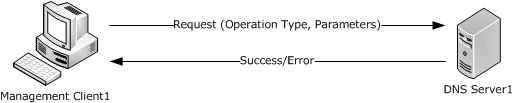


Figure : DNS Server Management Protocol

## Relationship to Other Protocols

The DNS Server Management Protocol relies on RPC [[MS-RPCE]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-RPCE%5d.pdf) as a transport. It is used to manage servers that implement DNS [[RFC1035]](http://go.microsoft.com/fwlink/?LinkId=90264), [[RFC1183]](http://go.microsoft.com/fwlink/?LinkId=106947), [[RFC1876]](http://go.microsoft.com/fwlink/?LinkId=106954), [[RFC1995]](http://go.microsoft.com/fwlink/?LinkId=106956), [[RFC1996]](http://go.microsoft.com/fwlink/?LinkId=106957), [[RFC2065]](http://go.microsoft.com/fwlink/?LinkId=106958), [[RFC2136]](http://go.microsoft.com/fwlink/?LinkId=107017), [[RFC2535]](http://go.microsoft.com/fwlink/?LinkId=107021), [[RFC2671]](http://go.microsoft.com/fwlink/?LinkId=107022), [[RFC2672]](http://go.microsoft.com/fwlink/?LinkId=132207), [[RFC2782]](http://go.microsoft.com/fwlink/?LinkId=90381), [[RFC2845]](http://go.microsoft.com/fwlink/?LinkId=90388), [[RFC2915]](http://go.microsoft.com/fwlink/?LinkId=107024), [[RFC2931]](http://go.microsoft.com/fwlink/?LinkId=107025), [[RFC3596]](http://go.microsoft.com/fwlink/?LinkId=107027), [[RFC4034]](http://go.microsoft.com/fwlink/?LinkId=107052), and [[RFC4701]](http://go.microsoft.com/fwlink/?LinkId=125431). It also interacts with the Netlogon protocol [[MS-NRPC]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-NRPC%5d.pdf).

The following diagram illustrates the relationship of the DNS Server Management Protocol and how it relates to RPC [MS-RPCE].

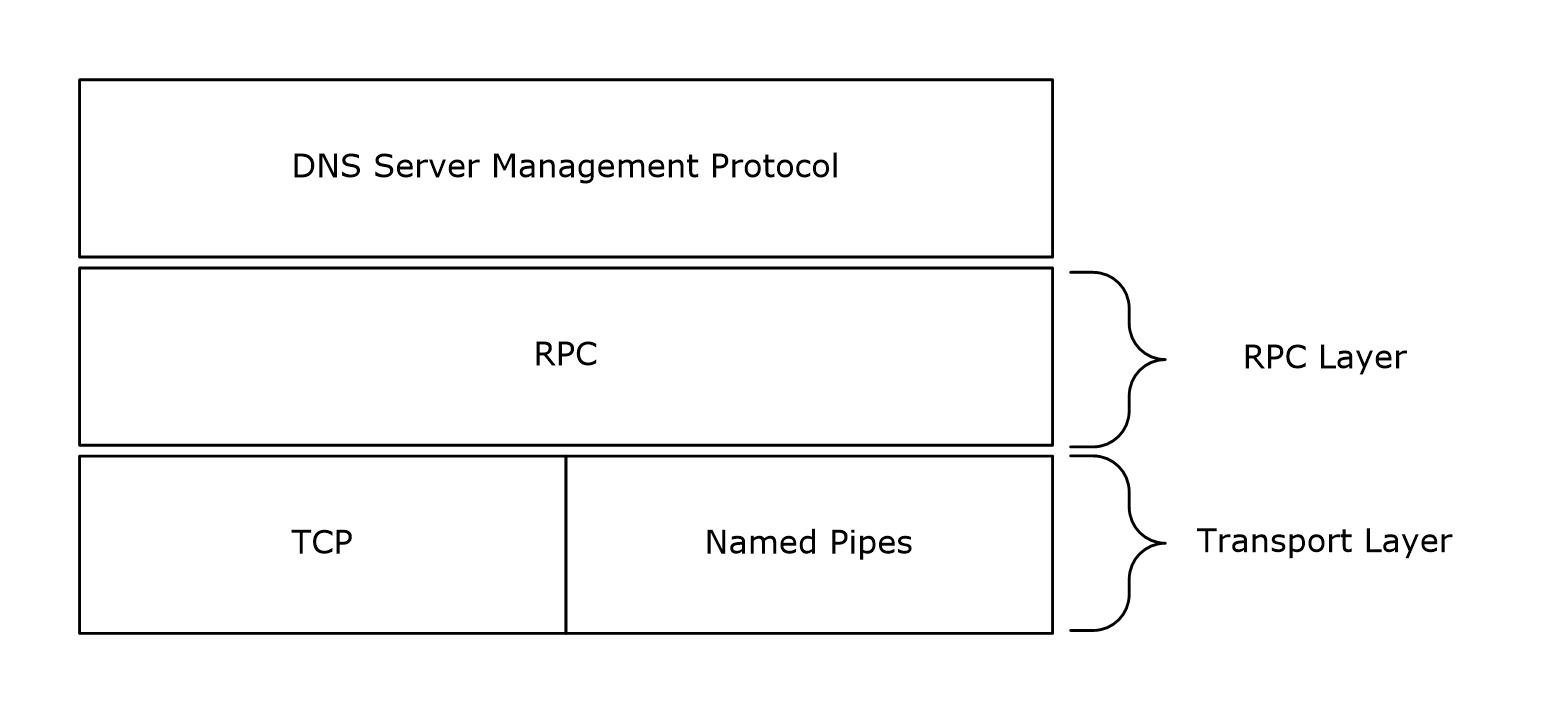


Figure : How the DNS Server Management Protocol uses RPC

The DNS server relies on the LDAP protocol [[RFC4511]](http://go.microsoft.com/fwlink/?LinkId=157505) to retrieve and modify DNS information when it is stored in a directory server. In this case, the DNS server is the client of the LDAP protocol, acting on behalf of and impersonating (using RPC impersonation), the client of the DNS Server Management Protocol. LDAP's relationship with other protocols is covered in [RFC4511] section 5. Note that although an LDAP provider may support transports other than TCP, the DNS server is required to open LDAP connections specifying the TCP transport using port 389.

The following diagram shows the relationship of the DNS Server Management Protocol to LDAP and TCP:

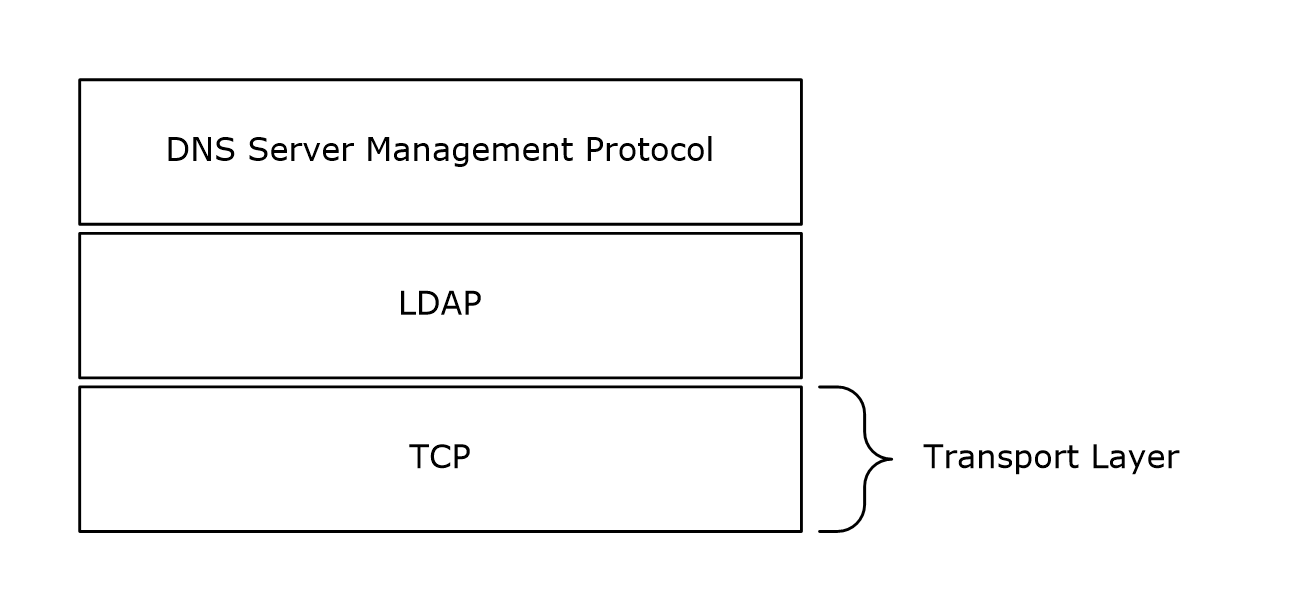


Figure : How the DNS Server Management Protocol uses LDAP

The following diagram illustrates the interaction between DNS Server Management Protocol Clients, DNS Servers, and directory servers.

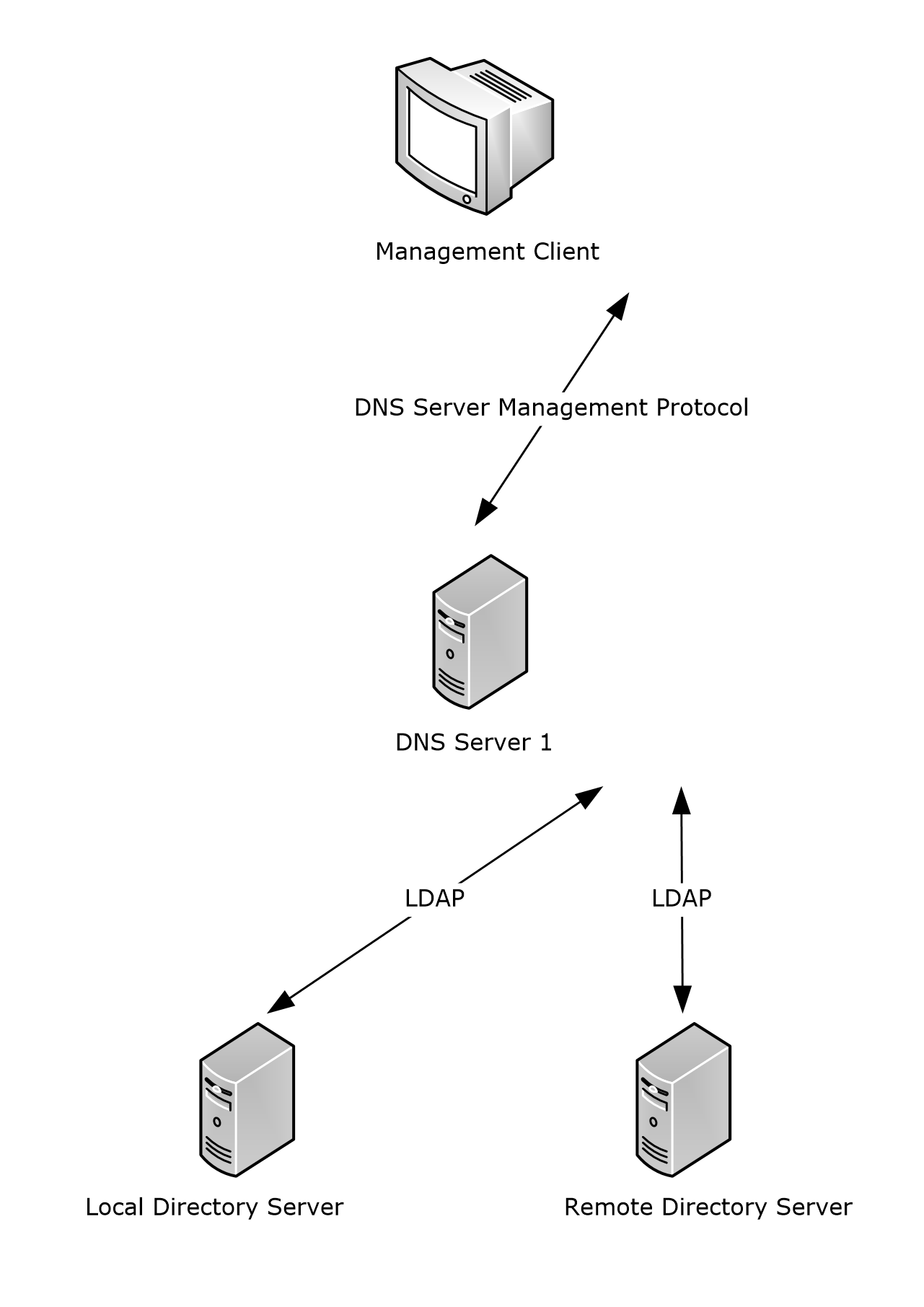


Figure : Relationship between DNS Server Management Protocol Clients, DNS Servers, and Directory Servers

## Prerequisites/Preconditions

This protocol is implemented on top of RPC and, as a result, has the prerequisites identified in [[MS-RPCE]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-RPCE%5d.pdf).

The DNS Server Management Protocol assumes that a client has obtained the name of a server that supports this protocol before the protocol is invoked. It also assumes that if a local directory server is available, the DNS server will establish an LDAP session to it and has appropriate credentials for requests. If no local directory server is available, or if a connection cannot be established, the DNS server operates only with zones loaded from files in the local file system rather than with zones replicated in the directory service, and operations requiring a directory service will fail.

All LDAP operations described in this protocol are performed with the local directory server unless otherwise stated. Consistency of DNS data stored in the local directory server is not guaranteed, since complete or partial updates to the LDAP directory can be replicated to the local directory server at any time. The protocol assumes that the DNS server polls the local directory server for changes that need to be synchronized with the in-memory zones.

## Applicability Statement

This protocol is applicable when an application needs to remotely configure a DNS server. It is not applicable to scenarios with multiple clients simultaneously managing a DNS server, if the ability to prevent interference is required.

## Versioning and Capability Negotiation

This document covers versioning issues in the following areas:

* Supported Transports: The DNS Server Management Protocol uses the RPC protocol as a transport and multiple [**RPC transports**](#gt_c2eeb200-3cd0-4916-966e-d7d6bff1737a).
* Protocol Versions: This protocol has a version number of 5.0.
* Security and Authentication Methods: Authentication and security are provided as specified in [[MS-RPCE]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-RPCE%5d.pdf).

The DNS server requests the principal name for the [**security provider**](#gt_05fd3925-0672-4f24-9dd9-2b9d441eb333) available on the system. Then Providers, for whom a principal name was obtained, are registered as supported authenticating mechanism for RPC calls. An RPC client using TCP, immediately after creating a binding attempts to negotiate authentication using RPC\_C\_AUTHN\_GSS\_NEGOTIATE and [**authentication level**](#gt_bfb9708e-9d05-4f79-8969-ef63f73aa434) as RPC\_C\_AUTHN\_LEVEL\_PKT\_INTEGRITY as specified in sections [2.1.1](#Section_cafd4f91def54329ac8566eab1b67eec) and [2.1.2](#Section_6ba440f3eae24d8e85a1e62b6030bc8f).

* Localization: This protocol passes text strings in various methods. Localization considerations for such strings are specified where relevant.
* Capability Negotiation: The DNS Server Management Protocol does not support negotiation of the protocol version to use. Instead, this protocol uses only the protocol version number specified in the [**IDL**](#gt_73177eec-4092-420f-92c5-60b2478df824) for versioning and capability negotiation. It should be noted that the present version of the IDL includes a client version input parameter (*dwClientVersion*) for some of the method calls (section [2.2.1.2.1](#Section_a237781bb048495d844b10ffb38df2a8)). This parameter allows the server to provide responses conforming to earlier versions of certain data structures associated with those method calls, while allowing extensibility of the present version of the protocol.

## Vendor-Extensible Fields

This protocol uses Win32 error codes as defined in [[MS-ERREF]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ERREF%5d.pdf) section 2.2. Vendors should reuse those values with their indicated meaning.  Choosing any other value runs the risk of a collision in the future.

## Standards Assignments

The following parameters are private Microsoft assignments.

| Parameter | Value | Reference |
| --- | --- | --- |
| RPC Interface [**UUID**](#gt_c4813fc3-b2e5-4aa3-bde7-421d950d68d3) for DNS | 50ABC2A4-574D-40B3-9D66-EE4FD5FBA076 | [[C706]](http://go.microsoft.com/fwlink/?LinkId=89824) section A.2.5 |
| Named Pipe name | \PIPE\DNSSERVER |  |

# Messages

The following sections specify how the DNS Server Management Protocol messages are transported and what common data types are used.

## Transport

All implementations MUST support the RPC over TCP protocol sequence (ncacn\_ip\_tcp), as specified in [[MS-RPCE]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-RPCE%5d.pdf), with [**dynamic endpoints**](#gt_46da887f-3f66-4941-a854-e51c52cf4c56). Implementations MAY[<1>](#Appendix_A_1) also support the RPC over named pipes protocol sequence (ncacn\_np), as specified in [MS-RPCE], with named pipe name \PIPE\DNSSERVER. The choice of transport for any given communication is up to the client application or higher-layer protocol.

The protocol MUST use the following UUID:

DnsServer: 50ABC2A4-574D-40B3-9D66-EE4FD5FBA076

The protocol MUST use an IDL version of 5.0.

### Server Security Settings

The DNS Server Management Protocol uses [**Security Support Provider Interface (SSPI)**](#gt_fb216516-748b-4873-8bdd-64c5f4da9920) security provided by RPC, as specified in [[MS-RPCE]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-RPCE%5d.pdf) section 3.3.1.5.2 for sessions using TCP as the transport protocol. The server SHOULD register the following as security providers:

* RPC\_C\_AUTHN\_GSS\_NEGOTIATE
* RPC\_C\_AUTHN\_GSS\_KERBEROS
* RPC\_C\_AUTHN\_WINNT

The DNS server MUST allow only authenticated access to RPC clients. The DNS server MUST NOT allow anonymous RPC clients. The DNS RPC server MUST perform a three-phase authorization test to ensure that the client is authorized to perform the specific RPC operation. The three-phase authorization test is specified in section [3.1.6.1](#Section_7ba0801d74f1499e81a300231ef31952). If the server is [**directory server**](#gt_04fd0982-6bb6-44f1-817e-795715049c50) integrated, the server MUST cache [**directory server security descriptors**](#gt_a1e2e723-b87f-499c-a03e-ebd98eed4620) until the next LDAP read operation that reads them and perform LDAP read operations for security descriptors as specified in section [3.1.6.2](#Section_22c0c227816b4cc88a60644a7985a8ce).

The DNS server can support up to 1,234 concurrent RPC calls.

The DNS server MUST limit access to only clients that negotiate an authentication level higher than that of RPC\_C\_AUTHN\_LEVEL\_NONE (see [MS-RPCE] section 2.2.1.1.8).

### Client Security Settings

The DNS RPC client SHOULD use a [**security support provider (SSP)**](#gt_e0edad22-1b0e-42f3-8e51-50f8aa30b29a) over RPC as specified in [[MS-RPCE]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-RPCE%5d.pdf), for sessions using TCP as RPC transport protocol. A client SHOULD authenticate using:

* RPC\_C\_AUTHN\_GSS\_NEGOTIATE

A client using TCP as the RPC transport requests RPC\_C\_AUTHN\_LEVEL\_PKT\_INTEGRITY authentication with the DNS server.

For negotiating RPC security, the DNS RPC client uses the following parameters:

* The client SHOULD[<2>](#Appendix_A_2) request mutual authentication by requesting the RPC\_C\_QOS\_CAPABILITIES\_MUTUAL\_AUTH capability. The client MAY additionally request the RPC\_C\_QOS\_CAPABILITIES\_IGNORE\_DELEGATE\_FAILURE capability.
* The identity tracking type is set to RPC\_C\_QOS\_IDENTITY\_STATIC.
* The impersonation type is set to RPC\_C\_IMP\_LEVEL\_IMPERSONATE, indicating that the server can impersonate the client; the client MAY instead specify RPC\_C\_IMP\_LEVEL\_DELEGATE.[<3>](#Appendix_A_3)

## Common Data Types

In addition to RPC base types and definitions specified in [[C706]](http://go.microsoft.com/fwlink/?LinkId=89824) and [[MS-RPCE]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-RPCE%5d.pdf), additional data types are defined below. This protocol also uses the types WORD and DWORD defined in [[MS-DTYP]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-DTYP%5d.pdf).

All multi-byte integer values in the messages declared in this section use little-endian byte order unless otherwise noted.

All fields designated as Unicode strings MUST be implemented using [**UTF-16LE**](#gt_69864bcc-33be-41c9-9486-e18618ee3dd0) strings as defined in [[UNICODE5.0.0/2007]](http://go.microsoft.com/fwlink/?LinkId=154659) section 2.6.

### DNS RPC Common Messages

#### Enumerations and Constants

##### DNS\_RPC\_TYPEID

The DNS Server Management Protocol RPC methods use a generic and extensible data structure of type [DNSSRV\_RPC\_UNION (section 2.2.1.2.6)](#Section_b61a872746b14981a6b3a1d4b92b67c4), which is a union of pointers to different data types. A DNS\_RPC\_TYPEID value is used to specify what data is being stored in an instance of the DNSSRV\_RPC\_UNION structure. The DNS\_RPC\_TYPEID enumeration combined with a DNSSRV\_RPC\_UNION structure allow the DNS RPC interface to communicate many different types of DNS server configuration and data in a single structure. The type of data carried inside the union is qualified by one of the following values:

| Constant/value | Description |
| --- | --- |
| DNSSRV\_TYPEID\_ANY  0xFFFFFFFF | Type is invalid. |
| DNSSRV\_TYPEID\_NULL  0x00000000 | No data is provided. |
| DNSSRV\_TYPEID\_DWORD  0x00000001 | A DWORD value. |
| DNSSRV\_TYPEID\_LPSTR  0x00000002 | A pointer to null-terminated [**UTF-8**](#gt_409411c4-b4ed-4ab6-b0ee-6d7815f85a35) [[RFC3629]](http://go.microsoft.com/fwlink/?LinkId=90439) string. |
| DNSSRV\_TYPEID\_LPWSTR  0x00000003 | A pointer to a null-terminated [**Unicode string**](#gt_b069acb4-e364-453e-ac83-42d469bb339e). |
| DNSSRV\_TYPEID\_IPARRAY  0x00000004 | A pointer to an [IP4\_ARRAY](#Section_588ae29671bf402f999686ecee39dc29). This structure is used to specify a list of [**IPv4**](#gt_0f25c9b5-dc73-4c3e-9433-f09d1f62ea8e) addresses. |
| DNSSRV\_TYPEID\_BUFFER  0x00000005 | A pointer to a [DNS\_RPC\_BUFFER (section 2.2.1.2.2)](#Section_cd4d047c3e894bc2b1651dc60ba538d5). This structure is used to hold a generic buffer of the DNS server information. Interpretation of the buffer depends upon the request. |
| DNSSRV\_TYPEID\_SERVER\_INFO\_W2K  0x00000006 | A pointer to a structure of type [DNS\_RPC\_SERVER\_INFO\_W2K (section 2.2.4.2.2.1)](#Section_130bd2ca07644ea6996553ca15dd6ed2). This structure is used to specify general DNS server state and configuration. |
| DNSSRV\_TYPEID\_STATS  0x00000007 | A pointer to a structure of type [DNSSRV\_STATS (section 2.2.10.2.2)](#Section_c4dd5c55f4344b968bb59d69e28ec7c2). The structure exposes internal statistics and counters. |
| DNSSRV\_TYPEID\_FORWARDERS\_W2K  0x00000008 | A pointer to a structure of type [DNS\_RPC\_FORWARDERS\_W2K (section 2.2.5.2.10.1)](#Section_7c71bbd3a46d4f8ebca79bc9e153454f). This structure specifies the set of DNS servers this DNS server will forward unresolved queries to. |
| DNSSRV\_TYPEID\_ZONE\_W2K  0x00000009 | A pointer to a structure of type [DNS\_RPC\_ZONE\_W2K (section 2.2.5.2.1.1)](#Section_6b6e834ae08e432ca9a78ced1422a688). This structure is used to specify basic information about a DNS zone. |
| DNSSRV\_TYPEID\_ZONE\_INFO\_W2K  0x0000000A | A pointer to a structure of type [DNS\_RPC\_ZONE\_INFO\_W2K (section 2.2.5.2.4.1)](#Section_e86515440fbb40388232375ff2d8a55e). This structure is used to specify detailed DNS zone information. |
| DNSSRV\_TYPEID\_ZONE\_SECONDARIES\_W2K  0x0000000B | A pointer to a structure of type [DNS\_RPC\_ZONE\_SECONDARIES\_W2K (section 2.2.5.2.5.1)](#Section_0961e81f542f48c78043bd420d104101). This structure is used to specify information about the secondary servers for a primary DNS zone. |
| DNSSRV\_TYPEID\_ZONE\_DATABASE\_W2K  0x0000000C | A pointer to a structure of type [DNS\_RPC\_ZONE\_DATABASE\_W2K (section 2.2.5.2.6.1)](#Section_660c4d3d6049422b912a7bf9129e7ed6). This structure specifies how a DNS zone is stored in persistent storage. |
| DNSSRV\_TYPEID\_ZONE\_TYPE\_RESET\_W2K  0x0000000D | This value is not used. |
| DNSSRV\_TYPEID\_ZONE\_CREATE\_W2K  0x0000000E | A pointer to a structure of type [DNS\_RPC\_ZONE\_CREATE\_INFO\_W2K (section 2.2.5.2.7.1)](#Section_780eba2615ea43d3a2b377ed9ab00690). This structure is used to specify parameters required when creating a new DNS zone. |
| DNSSRV\_TYPEID\_NAME\_AND\_PARAM  0x0000000F | A pointer to a structure of type [DNS\_RPC\_NAME\_AND\_PARAM (section 2.2.1.2.5)](#Section_408e91b91e534631a0515e097394f8d8). This is a general purpose structure used to associate a parameter name with a DWORD value. |
| DNSSRV\_TYPEID\_ZONE\_LIST\_W2K  0x00000010 | A pointer to a structure of type [DNS\_RPC\_ZONE\_LIST\_W2K (section 2.2.5.2.3.1)](#Section_f457cf9e14e04195a8fd2c93bc7f1f6d). This structure is used to enumerate zones. |
| DNSSRV\_TYPEID\_ZONE\_RENAME  0x00000011 | This value is not used. |
| DNSSRV\_TYPEID\_ZONE\_EXPORT  0x00000012 | A pointer to a structure of type [DNS\_RPC\_ZONE\_EXPORT\_INFO (section 2.2.5.2.8)](#Section_563518e385464d3c88c8f9b001beaa6e). This structure is used to specify how to export a zone to a file. |
| DNSSRV\_TYPEID\_SERVER\_INFO\_DOTNET  0x00000013 | A pointer to a structure of type [DNS\_RPC\_SERVER\_INFO\_DOTNET (section 2.2.4.2.2.2)](#Section_84f3331d499d49fe9f61ab4c5dde6377). This structure is used to specify general DNS server state and configuration. |
| DNSSRV\_TYPEID\_FORWARDERS\_DOTNET  0x00000014 | A pointer to a structure of type [DNS\_RPC\_FORWARDERS\_DOTNET (section 2.2.5.2.10.2)](#Section_4356fa2462664bb2ac5e519b6afe9237). This structure specifies the set of DNS servers this DNS server will forward unresolved queries to. |
| DNSSRV\_TYPEID\_ZONE  0x00000015 | A pointer to a structure of type [DNS\_RPC\_ZONE (section 2.2.5.2.1)](#Section_f22773cabfbf46a58042fbda1f3c4ad2). This structure is used to specify basic information and a DNS zone. |
| DNSSRV\_TYPEID\_ZONE\_INFO\_DOTNET  0x00000016 | A pointer to a structure of type [DNS\_RPC\_ZONE\_INFO\_DOTNET (section 2.2.5.2.4.2)](#Section_45b100df57c24c8486de00b69d742372). This structure is used to specify detailed information about a DNS zone. |
| DNSSRV\_TYPEID\_ZONE\_SECONDARIES\_DOTNET  0x00000017 | A pointer to a structure of type [DNS\_RPC\_ZONE\_SECONDARIES\_DOTNET (section 2.2.5.2.5.2)](#Section_f3f440eb6ff5419ca9ff7ed6aafc937a). This structure is used to specify information about the secondary servers for a primary DNS zone. |
| DNSSRV\_TYPEID\_ZONE\_DATABASE  0x00000018 | A pointer to a structure of type [DNS\_RPC\_ZONE\_DATABASE (section 2.2.5.2.6)](#Section_fc8b181af8b84953992e8102008d23cd). This structure specifies how a DNS zone is stored in persistent storage. |
| DNSSRV\_TYPEID\_ZONE\_TYPE\_RESET\_DOTNET  0x00000019 | This value is not used. |
| DNSSRV\_TYPEID\_ZONE\_CREATE\_DOTNET  0x0000001A | A pointer to a structure of type [DNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET](#Section_f0a445761d3f43ccbece07ae958f5b36). This structure is used to specify parameters required when creating a new DNS zone. |
| DNSSRV\_TYPEID\_ZONE\_LIST  0x0000001B | A pointer to a structure of type [DNS\_RPC\_ZONE\_LIST (section 2.2.5.2.3)](#Section_e43b2e88e3d54e909c0708d2f2dc57ed). This structure is used to enumerate zones. |
| DNSSRV\_TYPEID\_DP\_ENUM  0x0000001C | A pointer to a structure of type [DNS\_RPC\_DP\_ENUM (section 2.2.7.2.3)](#Section_324a939828c6463f93f68505904dc738). This structure is used to specify basic information about an application directory partition. |
| DNSSRV\_TYPEID\_DP\_INFO  0x0000001D | A pointer to a structure of type [DNS\_RPC\_DP\_INFO (section 2.2.7.2.1)](#Section_bd2a817d6a6940d3befc0c198a9c6e80). This structure specifies detailed information about a single application directory partition. |
| DNSSRV\_TYPEID\_DP\_LIST  0x0000001E | A pointer to a structure of type [DNS\_RPC\_DP\_LIST (section 2.2.7.2.4)](#Section_56b1d38f78964632b7dc0913ff3ef9b1). This structure is used to enumerate application directory partitions. |
| DNSSRV\_TYPEID\_ENLIST\_DP  0x0000001F | A pointer to a structure of type [DNS\_RPC\_ENLIST\_DP (section 2.2.7.2.5)](#Section_7f445256e1694f1ea244d4223fbdf604). This structure is used to request enlistment changes for an application directory partition. |
| DNSSRV\_TYPEID\_ZONE\_CHANGE\_DP  0x00000020 | A pointer to a structure of type [DNS\_RPC\_ZONE\_CHANGE\_DP (section 2.2.7.2.6)](#Section_6dc9428b7a6f4112a3dc7d250d2b06b4). This structure is used to request that a DNS zone be moved from one application directory partition to another. |
| DNSSRV\_TYPEID\_ENUM\_ZONES\_FILTER  0x00000021 | A pointer to a structure of type [DNS\_RPC\_ENUM\_ZONES\_FILTER (section 2.2.5.2.9)](#Section_b2c763771c5042f483c6b514a1a7e65e). This structure is used to filter DNS zones during enumeration. |
| DNSSRV\_TYPEID\_ADDRARRAY  0x00000022 | A pointer to a structure of type [DNS\_ADDR\_ARRAY (section 2.2.3.2.3)](#Section_56ba5fabf304486699a44f1c1f9247a3). This structure is used to specify a list of IPv4 or [**IPv6**](#gt_64c29bb6-c8b2-4281-9f3a-c1eb5d2288aa) addresses. |
| DNSSRV\_TYPEID\_SERVER\_INFO  0x00000023 | A pointer to a structure of type [DNS\_RPC\_SERVER\_INFO (section 2.2.4.2.2)](#Section_ac444baf4bf94f36912e3041d4c46361). This structure is used to specify general DNS server state and configuration. |
| DNSSRV\_TYPEID\_ZONE\_INFO  0x00000024 | A pointer to a structure of type [DNS\_RPC\_ZONE\_INFO (section 2.2.5.2.4)](#Section_5e6b44a913c44c3aa7a2b5576016c3cf). This structure is used to specify detailed information about a DNS zone. |
| DNSSRV\_TYPEID\_FORWARDERS  0x00000025 | A pointer to a structure of type [DNS\_RPC\_FORWARDERS (section 2.2.5.2.10)](#Section_83f4bfffc5fb4029aad305b3d7f4ef40). This structure specifies the set of DNS servers this DNS server will forward unresolved queries to. |
| DNSSRV\_TYPEID\_ZONE\_SECONDARIES  0x00000026 | A pointer to a structure of type [DNS\_RPC\_ZONE\_SECONDARIES (section 2.2.5.2.5)](#Section_2e5897350d8943c4a463212857482882). This structure is used to specify information about the secondary servers for a primary DNS zone. |
| DNSSRV\_TYPEID\_ZONE\_TYPE\_RESET  0x00000027 | This value is not used. |
| DNSSRV\_TYPEID\_ZONE\_CREATE  0x00000028 | A pointer to a structure of type [DNS\_RPC\_ZONE\_CREATE\_INFO (section 2.2.5.2.7)](#Section_f79e7455e26643d3ab2bf8e75aacfefa). This structure is used to specify parameters required when creating a new DNS zone. |
| DNSSRV\_TYPEID\_IP\_VALIDATE  0x00000029 | A pointer to a structure of type [DNS\_RPC\_IP\_VALIDATE (section 2.2.3.2.4)](#Section_2a367e0b5a8245d6aa77fbf407ed8d61). This structure is used to request IP validation and to return the results of IP validation. |
| DNSSRV\_TYPEID\_AUTOCONFIGURE  0x0000002A | A pointer to a structure of type [DNS\_RPC\_AUTOCONFIGURE (section 2.2.8.2.1)](#Section_414cf6fba8884c5591a46f77dff66cbe). This structure is used to request DNS server autoconfiguration. |
| DNSSRV\_TYPEID\_UTF8\_STRING\_LIST  0x0000002B | A pointer to a structure of type [DNS\_RPC\_UTF8\_STRING\_LIST (section 2.2.1.2.3)](#Section_8c593fe61a074140992c71f97f929ba3). This structure is used to represent a list of UTF-8 [RFC3629] strings. |
| DNSSRV\_TYPEID\_UNICODE\_STRING\_LIST  0x0000002C | A pointer to a structure of type [DNS\_RPC\_UNICODE\_STRING\_LIST (section 2.2.1.2.4)](#Section_ad7d4230cccf41589287328eb753e716). This structure is used to represent a list of Unicode strings. |
| DNSSRV\_TYPEID\_SKD  0x0000002D | A pointer to a structure of type [DNS\_RPC\_SKD (section 2.2.6.2.1)](#Section_f7b0ad424cae40fd87c882af83824639). This structure is used to specify detailed [**signing key descriptor**](#gt_621e5d7b-d764-4196-b838-b52bf82b9380) information. |
| DNSSRV\_TYPEID\_SKD\_LIST  0x0000002E | A pointer to a structure of type [DNS\_RPC\_SKD\_LIST (section 2.2.6.2.2)](#Section_6a715b5cf8c24b26923bca23cca2bd57). This structure is used to enumerate signing key descriptors. |
| DNSSRV\_TYPEID\_SKD\_STATE  0x0000002F | A pointer to a structure of type [DNS\_RPC\_SKD\_STATE (section 2.2.6.2.3)](#Section_b211f98844044c14b293bafd114b0eb6). This structure is used to specify detailed signing key descriptor state information. |
| DNSSRV\_TYPEID\_SIGNING\_VALIDATION\_ERROR  0x00000030 | A pointer to a structure of type [DNS\_RPC\_SIGNING\_VALIDATION\_ERROR (section 2.2.6.2.8)](#Section_b9b7d8ba458b4c589ae5c9616a52aa4a). This structure is used to specify signing key descriptor validation error information. |
| DNSSRV\_TYPEID\_TRUST\_POINT\_LIST  0x00000031 | A pointer to a structure of type [DNS\_RPC\_TRUST\_POINT\_LIST (section 2.2.6.2.5)](#Section_4a950c7f5f734b0eb0d2c467dde70976). This structure is used to enumerate [**trust points**](#gt_34a102c7-7324-497c-b8d7-699067c619c0). |
| DNSSRV\_TYPEID\_TRUST\_ANCHOR\_LIST  0x00000032 | A pointer to a structure of type [DNS\_RPC\_TRUST\_ANCHOR\_LIST (section 2.2.6.2.7)](#Section_b70ad9a4fb654fea80f3eef09cbc54b9). This structure is used to enumerate [**trust anchors**](#gt_bfdbc40a-da75-45a3-a8bc-50cd4f2f9797). |
| DNSSRV\_TYPEID\_ZONE\_SIGNING\_SETTINGS  0x00000033 | A pointer to a structure of type [DNS\_RPC\_ZONE\_DNSSEC\_SETTINGS (section 2.2.6.2.9)](#Section_a6027a0db9364702b72c51bc0634ed19). This structure is used to specify the DNSSEC settings for file-backed zones. |
| DNSSRV\_TYPEID\_ZONE\_SCOPE\_ENUM  0x00000034 | A pointer to a structure of type [DNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST (section 2.2.13.2.1)](#Section_fe6fb7243db047ba9b00852703f430c4). This structure is used to enumerate [**zone scopes**](#gt_bbe7722c-420e-48e7-b4bb-9838ff07b9e6) or [**cache scopes**](#gt_0ceb8c41-16c7-4dd0-8307-d977c30cbbc4). |
| DNSSRV\_TYPEID\_ZONE\_STATS  0x00000035 | A pointer to a structure of type [DNS\_RPC\_ZONE\_STATS\_V1 (section 2.2.12.2.5)](#Section_d0ac5580a8464e5aa526c5e17c00e15d). This structure is used to enumerate the zone statistics. |
| DNSSRV\_TYPEID\_ZONE\_SCOPE\_CREATE  0x00000036 | A pointer to a structure of type [DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1 (section 2.2.13.2.2.1)](#Section_cbe779f029b94a6199fba1d9115d590f). This structure is used to create the zone scope or cache scope. |
| DNSSRV\_TYPEID\_ZONE\_SCOPE\_INFO  0x00000037 | A pointer to a structure of type [DNS\_RPC\_ZONE\_SCOPE\_INFO\_V1 (section 2.2.13.2.3.1)](#Section_7dc5c61adb9b4704a287a9713f24b0c6). This structure is used to get the zone scope or cache scope information. |
| DNSSRV\_TYPEID\_SCOPE\_ENUM  0x00000038 | A pointer to a structure of type [DNS\_RPC\_ENUM\_SCOPE\_LIST (section 2.2.14.1.1)](#Section_eb2f8d9cf68e44389fddd7e9ec1a52bd). The structure is used to enumerate the [**server scopes**](#gt_b20e1dd4-e2fb-44d4-8508-9d9c8ac7ebd7) configured on the DNS server. |

Clients and servers of the DNS Server Management Protocol SHOULD[<4>](#Appendix_A_4) support all values above.

##### DNS\_RPC\_PROTOCOLS

DNS\_RPC\_PROTOCOLS is a DWORD value that specifies types of RPC protocols supported by the DNS server. For more details about this type, see section 2.1 in [[MS-RPCE]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-RPCE%5d.pdf).

| Constant/value | Description |
| --- | --- |
| DNS\_RPC\_USE\_TCPIP  0x00000001 | The server allows clients to connect using RPC over TCP/IP. |
| DNS\_RPC\_USE\_NAMED\_PIPE  0x00000002 | The server allows clients to connect using RPC over named pipes. |
| DNS\_RPC\_USE\_LPC  0x00000004 | An implementation-specific mode of communicating with a client on the same machine. [<5>](#Appendix_A_5) |
| DNS\_RPC\_USE\_ALL\_PROTOCOLS  0xFFFFFFFF | The server allows clients to connect using any of the above RPC mechanisms. |

##### TRUSTPOINT\_STATE

The TRUSTPOINT\_STATE enumeration identifies the current state of the life cycle of a DNSSEC trust point. The state of the trust point is determined by the states of its trust anchors and is given for informational purposes only; it does not affect the DNS or LDAP protocol.

| Constant/value | Description |
| --- | --- |
| TRUSTPOINT\_STATE\_INITIALIZED  0x00000000 | Indicates a trust point that has no trust anchors but has child nodes that do have trust anchors. |
| TRUSTPOINT\_STATE\_DSPENDING  0x00000001 | Indicates a trust point that has only DS trust anchors and is therefore ineffective for DNSSEC operations. |
| TRUSTPOINT\_STATE\_ACTIVE  0x00000002 | Indicates a trust point that has one or more DNSKEY trust anchors. Queries covered by this trust point will be validated using the DNSKEY trust anchors. |
| TRUSTPOINT\_STATE\_DELETE\_PENDING  0x00000003 | Indicates a trust point containing only revoked DNSKEY trust anchors. When the [[RFC5011]](http://go.microsoft.com/fwlink/?LinkId=225980) remove-hold-down time is exceeded for all revoked trust anchors, this trust point will be deleted. |

##### TRUSTANCHOR\_STATE

The TRUSTANCHOR\_STATE enumeration identifies the current state of the life cycle of a DNSSEC trust anchor. All states other than TRUSTANCHOR\_STATE\_DSPENDING and TRUSTANCHOR\_STATE\_DSINVALID correspond to the states given in [[RFC5011]](http://go.microsoft.com/fwlink/?LinkId=225980) section 4.2. Only the TRUSTANCHOR\_STATE\_VALID and TRUSTANCHOR\_STATE\_MISSING trust anchors affect the DNS protocol (by acting as a DNSSEC trust anchor). None of the states affect the LDAP protocol [[RFC4511]](http://go.microsoft.com/fwlink/?LinkId=157505).

| Constant/value | Description |
| --- | --- |
| TRUSTANCHOR\_STATE\_DSPENDING  0x00000001 | Indicates a DS trust anchor that can be replaced by the DNSKEY trust anchor that matches the hash of the DS trust anchor after the next [RFC5011] active refresh. |
| TRUSTANCHOR\_STATE\_DSINVALID  0x00000002 | Indicates a DS trust anchor that matches a DNSKEY record that is not valid as a trust anchor because the SEP flag is not set or because the algorithm is unsupported. |
| TRUSTANCHOR\_STATE\_ADDPEND  0x00000003 | Indicates a DNSKEY trust anchor that has not exceeded the [RFC5011] add-hold-down time. This trust anchor may become a valid trust anchor after the hold-down time has been exceeded. |
| TRUSTANCHOR\_STATE\_VALID  0x00000004 | Indicates a DNSKEY trust anchor that has exceeded the [RFC5011] add-hold-down time, has been matched to (and has replaced) a DS trust anchor, or has been added by the administrator. This trust anchor is trusted for DNSSEC operations, and a copy exists in the TrustAnchors zone. |
| TRUSTANCHOR\_STATE\_MISSING  0x00000005 | Indicates a DNSKEY trust anchor that is valid but was not seen in the last [RFC5011] active refresh. This trust anchor is trusted for DNSSEC operations, and a copy exists in the TrustAnchors zone. |
| TRUSTANCHOR\_STATE\_REVOKED  0x00000006 | Indicates a DNSKEY trust anchor that has been revoked by the authoritative zone administrator according to [RFC5011]. This trust anchor will be deleted when the [RFC5011] remove-hold-down time is exceeded. |

#### Structures

##### DNS\_RPC\_CURRENT\_CLIENT\_VER

This structure specifies version number information of the DNS RPC client. This version number is used by RPC clients to identify the requested RPC structures' version to the server so that the server can treat the request appropriately. This structure is defined as (in host byte order):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| DNS RPC Client Major Version | | | | | | | | | | | | | | | | DNS RPC Client Minor Version | | | | | | | | | | | | | | | |

**DNS RPC Client Major Version (2 bytes):** The major version number for the DNS RPC client. This MUST have a value from the following set:

| Value | Meaning |
| --- | --- |
| 0x0000 | Client requests RPC structures that do not require specific version numbers. |
| 0x0006 | Client requests RPC structures associated with version 6. |
| 0x0007 | Client requests RPC structures associated with version 7. |

**DNS RPC Client Minor Version (2 bytes):** The minor version number for the DNS RPC client. Senders MUST set this to zero and receivers MUST ignore it.

##### DNS\_RPC\_BUFFER

DNS\_RPC\_BUFFER defines a structure that contains a set of a specific type of structures. The DNS Server Management Protocol uses this structure to return information from the server, while processing R\_DnssrvComplexOperation2 (section [3.1.4.8](#Section_d28e3ba85742417dad6d2e0139ab2ad9)) method calls with operation type "Statistics".

1. typedef struct \_DnssrvRpcBuffer {
2. DWORD dwLength;
3. [size\_is(dwLength)] BYTE Buffer[];
4. } DNS\_RPC\_BUFFER,
5. \*PDNS\_RPC\_BUFFER;

**dwLength:**  The length, in bytes, of the data stored in Buffer.

**Buffer:**  A variable length array of bytes of length specified by dwLength. The buffer can contain one or more DNS\_RPC\_NODE structures (section [2.2.2.2.3](#Section_cb5539fa67fd40e09ea5468ecc56bd66)). Each DNS\_RPC\_NODE contains the length of that node such that the DNS\_RPC\_BUFFER dwLength may be larger to indicate multiple DNS\_RPC\_NODE structures.

##### DNS\_RPC\_UTF8\_STRING\_LIST

DNS\_RPC\_UTF8\_STRING\_LIST defines a structure that contains a list of null-terminated UTF-8 strings. This structure is used by the DNS Server Management Protocol while processing R\_DnssrvOperations2 (section [3.1.4.6](#Section_8c0522b197fb4fa7b4e22c55c0afb0e7)) and R\_DnssrvQuery2 (section [3.1.4.7](#Section_a90a44f0f64e44b09e35a7fc49f6adea)) method calls, with operations type "GlobalQueryBlockList".

1. typedef struct \_DnsRpcUtf8StringList {
2. [range(0,10000)] DWORD dwCount;
3. [size\_is(dwCount), string] char\* pszStrings[];
4. } DNS\_RPC\_UTF8\_STRING\_LIST,
5. \*PDNS\_RPC\_UTF8\_STRING\_LIST;

**dwCount:**  The number of strings present in the pszStrings array.

**pszStrings:**  A variable length array of pointers to null-terminated UTF-8 strings.

##### DNS\_RPC\_UNICODE\_STRING\_LIST

DNS\_RPC\_UNICODE\_STRING\_LIST defines a structure that contains a list of null-terminated Unicode strings. This structure is used by the DNS Server Management Protocol while processing the [R\_DnssrvComplexOperation2 (section 3.1.4.8)](#Section_d28e3ba85742417dad6d2e0139ab2ad9) method call, with operations of type "EnumerateKeyStorageProviders".

1. typedef struct \_DnsRpcUnicodeStringList {
2. [range(0,10000)] DWORD dwCount;
3. [size\_is(dwCount), string] char\* pwszStrings[];
4. } DNS\_RPC\_UNICODE\_STRING\_LIST,
5. \*PDNS\_RPC\_UNICODE\_STRING\_LIST;

**dwCount:**  The number of strings present in the pwszStrings array.

**pwszStrings:**  A variable-length array of pointers to null-terminated Unicode strings.

##### DNS\_RPC\_NAME\_AND\_PARAM

DNS\_RPC\_NAME\_AND\_PARAM defines the structure that contains information about a simple server property that takes a DWORD value. The DNS Server Management Protocol uses this structure to exchange information about various properties that take an integer value, while processing the R\_DnssrvOperation2 (section [3.1.4.6](#Section_8c0522b197fb4fa7b4e22c55c0afb0e7)) method call with operation types "ResetDwordProperty", "DeleteNode", and "DeleteRecordSet".

1. typedef struct \_DnssrvRpcNameAndParam {
2. DWORD dwParam;
3. [string] char\* pszNodeName;
4. } DNS\_RPC\_NAME\_AND\_PARAM,
5. \*PDNS\_RPC\_NAME\_AND\_PARAM;

**dwParam:**  The requested new value for the server property specified by pszNodeName.

**pszNodeName:**  Pointer to a null-terminated UTF-8 string that specifies the name of the server property.

##### DNSSRV\_RPC\_UNION

Note: Some of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview in the Product Behavior appendix.

DNSSRV\_RPC\_UNION specifies a collection of all possible messages structures that can be exchanged between a client and server communicating using the DNS Server Management Protocol. This is used by the R\_DnssrvOperation2 (section [3.1.4.6](#Section_8c0522b197fb4fa7b4e22c55c0afb0e7)), R\_DnssrvQuery2 (section [3.1.4.7](#Section_a90a44f0f64e44b09e35a7fc49f6adea)) and R\_DnssrvComplexOperation2 (section [3.1.4.8](#Section_d28e3ba85742417dad6d2e0139ab2ad9)) method calls. The exact message format inside DNSSRV\_RPC\_UNION is identified by an accompanying DNS\_RPC\_TYPEID (section [2.2.1.1.1](#Section_c49b8142a36441c8914a7675a573b5e4)) value. Clients and servers of the DNS Server Management Protocol SHOULD[<6>](#Appendix_A_6) support all members of DNSSRV\_RPC\_UNION.

1. typedef
2. [switch\_type(DWORD)]
3. union \_DnssrvSrvRpcUnion {
4. [case(DNSSRV\_TYPEID\_NULL)]
5. PBYTE Null;
6. [case(DNSSRV\_TYPEID\_DWORD)]
7. DWORD Dword;
8. [case(DNSSRV\_TYPEID\_LPSTR)]
9. [string] char\* String;
10. [case(DNSSRV\_TYPEID\_LPWSTR)]
11. [string] wchar\_t\* WideString;
12. [case(DNSSRV\_TYPEID\_IPARRAY)]
13. PIP4\_ARRAY IpArray;
14. [case(DNSSRV\_TYPEID\_BUFFER)]
15. PDNS\_RPC\_BUFFER Buffer;
16. [case(DNSSRV\_TYPEID\_SERVER\_INFO\_W2K)]
17. PDNS\_RPC\_SERVER\_INFO\_W2K ServerInfoW2K;
18. [case(DNSSRV\_TYPEID\_STATS)]
19. PDNSSRV\_STATS Stats;
20. [case(DNSSRV\_TYPEID\_FORWARDERS\_W2K)]
21. PDNS\_RPC\_FORWARDERS\_W2K ForwardersW2K;
22. [case(DNSSRV\_TYPEID\_ZONE\_W2K)]
23. PDNS\_RPC\_ZONE\_W2K ZoneW2K;
24. [case(DNSSRV\_TYPEID\_ZONE\_INFO\_W2K)]
25. PDNS\_RPC\_ZONE\_INFO\_W2K ZoneInfoW2K;
26. [case(DNSSRV\_TYPEID\_ZONE\_SECONDARIES\_W2K)]
27. PDNS\_RPC\_ZONE\_SECONDARIES\_W2K SecondariesW2K;
28. [case(DNSSRV\_TYPEID\_ZONE\_DATABASE\_W2K)]
29. PDNS\_RPC\_ZONE\_DATABASE\_W2K DatabaseW2K;
30. [case(DNSSRV\_TYPEID\_ZONE\_CREATE\_W2K)]
31. PDNS\_RPC\_ZONE\_CREATE\_INFO\_W2K ZoneCreateW2K;
32. [case(DNSSRV\_TYPEID\_NAME\_AND\_PARAM)]
33. PDNS\_RPC\_NAME\_AND\_PARAM NameAndParam;
34. [case(DNSSRV\_TYPEID\_ZONE\_LIST\_W2K)]
35. PDNS\_RPC\_ZONE\_LIST\_W2K ZoneListW2K;
36. [case(DNSSRV\_TYPEID\_SERVER\_INFO\_DOTNET)]
37. PDNS\_RPC\_SERVER\_INFO\_DOTNET ServerInfoDotNet;
38. [case(DNSSRV\_TYPEID\_FORWARDERS\_DOTNET)]
39. PDNS\_RPC\_FORWARDERS\_DOTNET ForwardersDotNet;
40. [case(DNSSRV\_TYPEID\_ZONE)]
41. PDNS\_RPC\_ZONE Zone;
42. [case(DNSSRV\_TYPEID\_ZONE\_INFO\_DOTNET)]
43. PDNS\_RPC\_ZONE\_INFO\_DOTNET ZoneInfoDotNet;
44. [case(DNSSRV\_TYPEID\_ZONE\_SECONDARIES\_DOTNET)]
45. PDNS\_RPC\_ZONE\_SECONDARIES\_DOTNET SecondariesDotNet;
46. [case(DNSSRV\_TYPEID\_ZONE\_DATABASE)]
47. PDNS\_RPC\_ZONE\_DATABASE Database;
48. [case(DNSSRV\_TYPEID\_ZONE\_CREATE\_DOTNET)]
49. PDNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET ZoneCreateDotNet;
50. [case(DNSSRV\_TYPEID\_ZONE\_LIST)]
51. PDNS\_RPC\_ZONE\_LIST ZoneList;
52. [case(DNSSRV\_TYPEID\_ZONE\_EXPORT)]
53. PDNS\_RPC\_ZONE\_EXPORT\_INFO ZoneExport;
54. [case(DNSSRV\_TYPEID\_DP\_INFO)]
55. PDNS\_RPC\_DP\_INFO DirectoryPartition;
56. [case(DNSSRV\_TYPEID\_DP\_ENUM)]
57. PDNS\_RPC\_DP\_ENUM DirectoryPartitionEnum;
58. [case(DNSSRV\_TYPEID\_DP\_LIST)]
59. PDNS\_RPC\_DP\_LIST DirectoryPartitionList;
60. [case(DNSSRV\_TYPEID\_ENLIST\_DP)]
61. PDNS\_RPC\_ENLIST\_DP EnlistDirectoryPartition;
62. [case(DNSSRV\_TYPEID\_ZONE\_CHANGE\_DP)]
63. PDNS\_RPC\_ZONE\_CHANGE\_DP ZoneChangeDirectoryPartition;
64. [case(DNSSRV\_TYPEID\_ENUM\_ZONES\_FILTER)]
65. PDNS\_RPC\_ENUM\_ZONES\_FILTER EnumZonesFilter;
66. [case(DNSSRV\_TYPEID\_ADDRARRAY)]
67. PDNS\_ADDR\_ARRAY AddrArray;
68. [case(DNSSRV\_TYPEID\_SERVER\_INFO)]
69. PDNS\_RPC\_SERVER\_INFO ServerInfo;
70. [case(DNSSRV\_TYPEID\_ZONE\_CREATE)]
71. PDNS\_RPC\_ZONE\_CREATE\_INFO ZoneCreate;
72. [case(DNSSRV\_TYPEID\_FORWARDERS)]
73. PDNS\_RPC\_FORWARDERS Forwarders;
74. [case(DNSSRV\_TYPEID\_ZONE\_SECONDARIES)]
75. PDNS\_RPC\_ZONE\_SECONDARIES Secondaries;
76. [case(DNSSRV\_TYPEID\_IP\_VALIDATE)]
77. PDNS\_RPC\_IP\_VALIDATE IpValidate;
78. [case(DNSSRV\_TYPEID\_ZONE\_INFO)]
79. PDNS\_RPC\_ZONE\_INFO ZoneInfo;
80. [case(DNSSRV\_TYPEID\_AUTOCONFIGURE)]
81. PDNS\_RPC\_AUTOCONFIGURE AutoConfigure;
82. [case(DNSSRV\_TYPEID\_UTF8\_STRING\_LIST)]
83. PDNS\_RPC\_UTF8\_STRING\_LIST Utf8StringList;
84. [case(DNSSRV\_TYPEID\_UNICODE\_STRING\_LIST)]
85. PDNS\_RPC\_UNICODE\_STRING\_LIST UnicodeStringList;
86. [case(DNSSRV\_TYPEID\_SKD)]
87. PDNS\_RPC\_SKD Skd;
88. [case(DNSSRV\_TYPEID\_SKD\_LIST)]
89. PDNS\_RPC\_SKD\_LIST SkdList;
90. [case(DNSSRV\_TYPEID\_SKD\_STATE)]
91. PDNS\_RPC\_SKD\_STATE SkdState;
92. [case(DNSSRV\_TYPEID\_SIGNING\_VALIDATION\_ERROR)]
93. PDNS\_RPC\_SIGNING\_VALIDATION\_ERROR SigningValidationError;
94. [case(DNSSRV\_TYPEID\_TRUST\_POINT\_LIST)]
95. PDNS\_RPC\_TRUST\_POINT\_LIST TrustPointList;
96. [case(DNSSRV\_TYPEID\_TRUST\_ANCHOR\_LIST)]
97. PDNS\_RPC\_TRUST\_ANCHOR\_LIST TrustAnchorList;
98. [case(DNSSRV\_TYPEID\_ZONE\_SIGNING\_SETTINGS)]
99. PDNS\_RPC\_ZONE\_DNSSEC\_SETTINGS ZoneDnsSecSettings;
100. [case(DNSSRV\_TYPEID\_ZONE\_SCOPE\_ENUM)]
101. PDNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST ZoneScopeList;
102. [case(DNSSRV\_TYPEID\_ZONE\_STATS)]
103. PDNS\_RPC\_ZONE\_STATS ZoneStats;
104. [case(DNSSRV\_TYPEID\_ZONE\_SCOPE\_CREATE)]
105. PDNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO ScopeCreate;
106. [case(DNSSRV\_TYPEID\_ZONE\_SCOPE\_INFO)]
107. PDNS\_RPC\_ZONE\_SCOPE\_INFO ScopeInfo;
108. [case(DNSSRV\_TYPEID\_SCOPE\_ENUM)]
109. PDNS\_RPC\_ENUM\_SCOPE\_LIST ScopeList;
110. [case(DNSSRV\_TYPEID\_CLIENT\_SUBNET\_RECORD)]
111. PDNS\_RPC\_CLIENT\_SUBNET\_RECORD SubnetList;
112. [case(DNSSRV\_TYPEID\_POLICY)]
113. PDNS\_RPC\_POLICY pPolicy;
114. [case(DNSSRV\_TYPEID\_POLICY\_NAME)]
115. PDNS\_RPC\_POLICY\_NAME pPolicyName;
116. [case(DNSSRV\_TYPEID\_POLICY\_ENUM)]
117. PDNS\_RPC\_ENUMERATE\_POLICY\_LIST pPolicyList;
118. } DNSSRV\_RPC\_UNION;

**Null:**  No data is provided.

**Dword:**  Data is a DWORD value.

**String:**  A pointer to a null-terminated UTF-8 string or a NULL pointer.

**WideString:**  A pointer to a null-terminated Unicode string or a NULL pointer.

**IpArray:**  An array of IPv4 addresses in IP4\_ARRAY (section [2.2.3.2.1](#Section_588ae29671bf402f999686ecee39dc29)) format.

**Buffer:**  A pointer to a DNS\_RPC\_BUFFER (section [2.2.1.2.2](#Section_cd4d047c3e894bc2b1651dc60ba538d5)).

**ServerInfoW2K:**  A pointer to a structure of type DNS\_RPC\_SERVER\_INFO\_W2K (section [2.2.4.2.2](#Section_ac444baf4bf94f36912e3041d4c46361)). This structure is used to specify general DNS server state and configuration.

**Stats:**  A pointer to a structure of type DNSSRV\_STAT (section [2.2.10.2.2](#Section_c4dd5c55f4344b968bb59d69e28ec7c2)). The structure exposes internal statistics and counters.

**ForwardersW2K:**  A pointer to a structure of type DNS\_RPC\_FORWARDERS\_W2K (section [2.2.5.2.10.1](#Section_7c71bbd3a46d4f8ebca79bc9e153454f)). This structure specifies the set of DNS servers this DNS server will forward unresolved queries to.

**ZoneW2K:**  A pointer to a structure of type DNS\_RPC\_ZONE\_W2K (section [2.2.5.2.1](#Section_f22773cabfbf46a58042fbda1f3c4ad2)). This structure is used to specify basic information about a DNS zone.

**ZoneInfoW2K:**  A pointer to a structure of type DNS\_RPC\_INFO\_W2K (section [2.2.5.2.4](#Section_5e6b44a913c44c3aa7a2b5576016c3cf)). This structure is used to specify detailed DNS zone information.

**SecondariesW2K:**  A pointer to a structure of type DNS\_RPC\_ZONE\_SECONDARIES\_W2K (section [2.2.5.2.5](#Section_2e5897350d8943c4a463212857482882)). This structure is used to specify information about the secondary servers for a primary DNS zone.

**DatabaseW2K:**  A pointer to a structure of type DNS\_RPC\_ZONE\_DATABASE\_W2K (section [2.2.5.2.6](#Section_fc8b181af8b84953992e8102008d23cd)). This structure specifies how a DNS zone is stored in persistent storage.

**ZoneCreateW2K:**  A pointer to a structure of type DNS\_RPC\_ZONE\_CREATE\_INFO\_W2K (section [2.2.5.2.9](#Section_b2c763771c5042f483c6b514a1a7e65e)). This structure is used to specify parameters required when creating a new DNS zone.

**NameAndParam:**  A pointer to a structure of type DNS\_RPC\_NAME\_AND\_PARAM (section [2.2.1.2.5](#Section_408e91b91e534631a0515e097394f8d8)). This is a general purpose structure used to associate a parameter name with a DWORD value.

**ZoneListW2K:**  A pointer to a structure of type DNS\_RPC\_ZONE\_LIST\_W2K (section 2.2.1.2.5). This structure is used to enumerate zones.

**ServerInfoDotNet:**  A pointer to a structure of type DNS\_RPC\_SERVER\_INFO\_DOTNET (section 2.2.4.2.2). This structure is used to specify general DNS server state and configuration.

**ForwardersDotNet:**  A pointer to a structure of type DNS\_RPC\_FORWARDERS\_DOTNET (section [2.2.5.2.10.2](#Section_4356fa2462664bb2ac5e519b6afe9237)). This structure specifies the set of DNS servers this DNS server will forward unresolved queries to.

**Zone:**  A pointer to a structure of type DNS\_RPC\_ZONE (section 2.2.5.2.1). This structure is used to specify basic information about a DNS zone.

**ZoneInfoDotNet:**  A pointer to a structure of type DNS\_RPC\_ZONE\_INFO\_DOTNET (section 2.2.5.2.4). This structure is used to specify detailed DNS zone information.

**SecondariesDotNet:**  A pointer to a structure of type DNS\_RPC\_ZONE\_SECONDARIES\_DOTNET (section 2.2.5.2.5). This structure is used to specify information about the secondary servers for a primary DNS zone.

**Database:**  A pointer to a structure of type DNS\_RPC\_ZONE\_DATABASE (section 2.2.5.2.6). This structure specifies how a DNS zone is stored in persistent storage.

**ZoneCreateDotNet:**  A pointer to a structure of type DNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET (section 2.2.5.2.9). This structure is used to specify parameters required when creating a new DNS zone.

**ZoneList:**  A pointer to a structure of type DNS\_RPC\_ZONE\_LIST (section [2.2.5.2.3](#Section_e43b2e88e3d54e909c0708d2f2dc57ed)). This structure is used to enumerate zones.

**ZoneExport:**  A pointer to a structure of type DNS\_RPC\_ZONE\_EXPORT\_INFO (section [2.2.5.2.8](#Section_563518e385464d3c88c8f9b001beaa6e)). This structure is used to specify how a zone is exported to file.

**DirectoryPartition:**  A pointer to a structure of type DNS\_RPC\_DP\_INFO (section [2.2.7.2.1](#Section_bd2a817d6a6940d3befc0c198a9c6e80)). This structure specifies detailed information about a single application directory partition.

**DirectoryPartitionEnum:**  A pointer to a structure of type DNS\_RPC\_DP\_ENUM (section [2.2.7.2.3](#Section_324a939828c6463f93f68505904dc738)). This structure is used to specify basic information about an application directory partition.

**DirectoryPartitionList:**  A pointer to a structure of type DNS\_RPC\_DP\_LIST (section [2.2.7.2.4](#Section_56b1d38f78964632b7dc0913ff3ef9b1)). This structure is used to enumerate the Application Directory Partition Table.

**EnlistDirectoryPartition:**  A pointer to a structure of type DNS\_RPC\_ENLIST\_DP (section [2.2.7.2.5](#Section_7f445256e1694f1ea244d4223fbdf604)). This structure is used to request enlistment changes for an application directory partition.

**ZoneChangeDirectoryPartition:**  A pointer to a structure of type DNS\_RPC\_ZONE\_CHANGE\_DP (section [2.2.7.2.6](#Section_6dc9428b7a6f4112a3dc7d250d2b06b4)). This structure is used to request that a DNS zone be moved from one application directory partition to another.

**EnumZonesFilter:**  A pointer to a structure of type DNS\_RPC\_ENUM\_ZONES\_FILTER (section 2.2.5.2.9). This structure is used to filter DNS zones during enumeration.

**AddrArray:**  A pointer to a structure of type DNS\_ADDR\_ARRAY (section [2.2.3.2.3](#Section_56ba5fabf304486699a44f1c1f9247a3)). This structure is used to specify a list of IPv4 or IPv6 addresses.

**ServerInfo:**  A pointer to a structure of type DNS\_RPC\_SERVER\_INFO (section 2.2.4.2.2). This structure is used to specify general DNS server state and configuration.

**ZoneCreate:**  A pointer to a structure of type DNS\_RPC\_ZONE\_CREATE\_INFO (section 2.2.5.2.9). This structure is used to specify parameters required when creating a new DNS zone.

**Forwarders:**  A pointer to a structure of type DNS\_RPC\_FORWARDERS (section [2.2.5.2.10](#Section_83f4bfffc5fb4029aad305b3d7f4ef40)). This structure specifies the set of DNS servers this DNS server will forward unresolved queries to.

**Secondaries:**  A pointer to a structure of type DNS\_RPC\_ZONE\_SECONDARIES (section 2.2.5.2.5). This structure is used to specify information about the secondary servers for a primary DNS zone.

**IpValidate:**  A pointer to a structure of type [DNS\_RPC\_IP\_VALIDATE (section 2.2.3.2.4)](#Section_2a367e0b5a8245d6aa77fbf407ed8d61). This structure is used to request IP validation and to return the results of IP validation.

**ZoneInfo:**  A pointer to a structure of type DNS\_RPC\_ZONE\_INFO (section 2.2.5.2.4). This structure is used to specify detailed DNS zone information.

**AutoConfigure:**  A pointer to a structure of type DNS\_AUTOCONFIGURE (section [2.2.8.2.1](#Section_414cf6fba8884c5591a46f77dff66cbe)). This structure is used to request DNS server autoconfiguration.

**Utf8StringList:**  A pointer to a structure of type DNS\_RPC\_UTF8\_STRING\_LIST (section [2.2.1.2.3](#Section_8c593fe61a074140992c71f97f929ba3)). This structure is used to represent a list of UTF-8 [[RFC3629]](http://go.microsoft.com/fwlink/?LinkId=90439) strings.

**UnicodeStringList:**  A pointer to a structure of type [DNS\_RPC\_UNICODE\_STRING\_LIST](#Section_ad7d4230cccf41589287328eb753e716) (section 2.2.1.2.4). This structure is used to represent a list of Unicode strings.

**Skd:**  A pointer to a structure of type [DNS\_RPC\_SKD](#Section_f7b0ad424cae40fd87c882af83824639) (section 2.2.6.2.1). This structure is used to specify detailed signing key descriptor information.

**SkdList:**  A pointer to a structure of type [DNS\_RPC\_SKD\_LIST](#Section_6a715b5cf8c24b26923bca23cca2bd57) (section 2.2.6.2.2). This structure is used to enumerate signing key descriptors.

**SkdState:**  A pointer to a structure of type [DNS\_RPC\_SKD\_STATE](#Section_b211f98844044c14b293bafd114b0eb6) (section 2.2.6.2.3). This structure is used to specify detailed signing key descriptor state information.

**SigningValidationError:**  A pointer to a structure of type [DNS\_RPC\_SIGNING\_VALIDATION\_ERROR](#Section_b9b7d8ba458b4c589ae5c9616a52aa4a) (section 2.2.6.2.8). This structure is used to specify signing key descriptor validation error information.

**TrustPointList:**  A pointer to a structure of type [DNS\_RPC\_TRUST\_POINT\_LIST](#Section_4a950c7f5f734b0eb0d2c467dde70976) (section 2.2.6.2.5). This structure is used to enumerate trust points.

**TrustAnchorList:**  A pointer to a structure of type [DNS\_RPC\_TRUST\_ANCHOR\_LIST](#Section_b70ad9a4fb654fea80f3eef09cbc54b9) (section 2.2.6.2.7). This structure is used to enumerate trust anchors.

**ZoneDnsSecSettings:**  A pointer to a structure of type [DNS\_RPC\_ZONE\_DNSSEC\_SETTINGS (section 2.2.6.2.9)](#Section_a6027a0db9364702b72c51bc0634ed19). This structure is used to list the DNSSEC settings of a zone.

**ZoneScopeList:**  A pointer to a structure of type [DNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST (section 2.2.13.2.1)](#Section_fe6fb7243db047ba9b00852703f430c4). This structure is used to enumerate zone scopes in a specified zone or cache scopes in a cache zone.

**ZoneStats:**  A pointer to a structure of type [DNS\_RPC\_ZONE\_STATS\_V1 (section 2.2.12.2.5)](#Section_d0ac5580a8464e5aa526c5e17c00e15d). This structure is used to enumerate the zone statistics.

**ScopeCreate:**  A pointer to a structure of type [DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1 (section 2.2.13.2.2.1)](#Section_cbe779f029b94a6199fba1d9115d590f). This structure is used to create a zone scope or cache scope.

**ScopeInfo:**  A pointer to a structure of type [DNS\_RPC\_ZONE\_SCOPE\_INFO\_V1 (section 2.2.13.2.3.1)](#Section_7dc5c61adb9b4704a287a9713f24b0c6). This structure is used to specify detailed DNS zone scope or cache scope information.

**ScopeList:**  A pointer to a structure of type [DNS\_RPC\_ENUM\_SCOPE\_LIST (section 2.2.14.1.1)](#Section_eb2f8d9cf68e44389fddd7e9ec1a52bd). This structure is used to retrieve all the server scopes configured on the DNS server.

**SubnetList:**  A pointer to a structure of type [DNS\_RPC\_CLIENT\_SUBNET\_RECORD (section 2.2.15.2.1)](#Section_c8b7e015035f424d90bef1c5f0b60eab). This structure is used to retrieve details of a [**client subnet record**](#gt_454a772d-d8fb-44b8-9b6d-39d624a813df) in the DNS server.

**pPolicy:**  A pointer to a structure of type [DNS\_RPC\_POLICY (section 2.2.15.2.5)](#Section_89be092dec014ab384e45a56622f9de8). This structure is used to retrieve details of a [**DNS Policy**](#gt_5076749f-34a6-48a6-b051-8968a55f4d7b) in the DNS server.

**pPolicyName:**  A pointer to a structure of type [DNS\_RPC\_POLICY\_NAME (section 2.2.15.2.6)](#Section_c97d6de9ddf44579bdece242bccb349d). This structure is used while enumerating DNS Policies in a DNS server per level.

**pPolicyList:**  A pointer to a structure of type [DNS\_RPC\_ENUMERATE\_POLICY\_LIST (section 2.2.15.2.7)](#Section_e1c7065259a844eb844a1cda0b1453b8). This structure contains a list of DNS\_RPC\_POLICY\_NAME structures.

### Resource Record Messages

#### Enumerations and Constants

##### DNS\_RECORD\_TYPE

Note: Some of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview in the Product Behavior appendix.

The DNS\_RECORD\_TYPE is a 16-bit integer value that specifies DNS record types that can be enumerated by the DNS server.

| Constant/value | Description |
| --- | --- |
| DNS\_TYPE\_ZERO  0x0000 | An empty record type ([[RFC1034]](http://go.microsoft.com/fwlink/?LinkId=90263) section 3.6 and [[RFC1035]](http://go.microsoft.com/fwlink/?LinkId=90264) section 3.2.2). |
| DNS\_TYPE\_A  0x0001 | An A record type, used for storing an IP address ([RFC1035] section 3.2.2). |
| DNS\_TYPE\_NS  0x0002 | An [**authoritative**](#gt_ed54858d-02e4-4de3-b65b-e0b81c4185c7) name-server record type ([RFC1034] section 3.6 and [RFC1035] section 3.2.2). |
| DNS\_TYPE\_MD  0x0003 | A mail-destination record type ([RFC1035] section 3.2.2). |
| DNS\_TYPE\_MF  0x0004 | A mail forwarder record type ([RFC1035] section 3.2.2). |
| DNS\_TYPE\_CNAME  0x0005 | A record type that contains the canonical name of a DNS alias ([RFC1035] section 3.2.2). |
| DNS\_TYPE\_SOA  0x0006 | A [**Start of Authority (SOA)**](#gt_0365bdcc-f1f5-4494-b57c-02c897b7ea8a) record type ([RFC1035] section 3.2.2). |
| DNS\_TYPE\_MB  0x0007 | A mailbox record type ([RFC1035] section 3.2.2). |
| DNS\_TYPE\_MG  0x0008 | A mail group member record type ([RFC1035] section 3.2.2). |
| DNS\_TYPE\_MR  0x0009 | A mail-rename record type ([RFC1035] section 3.2.2). |
| DNS\_TYPE\_NULL  0x000A | A record type for completion queries ([RFC1035] section 3.2.2). |
| DNS\_TYPE\_WKS  0x000B | A record type for a well-known service ([RFC1035] section 3.2.2). |
| DNS\_TYPE\_PTR  0x000C | A record type containing [**FQDN**](#gt_1769aec9-237e-44ed-9014-1abb3ec6de6e) pointer ([RFC1035] section 3.2.2). |
| DNS\_TYPE\_HINFO  0x000D | A host information record type ([RFC1035] section 3.2.2). |
| DNS\_TYPE\_MINFO  0x000E | A mailbox or mailing list information record type ([RFC1035] section 3.2.2). |
| DNS\_TYPE\_MX  0x000F | A mail-exchanger record type ([RFC1035] section 3.2.2). |
| DNS\_TYPE\_TXT  0x0010 | A record type containing a text string ([RFC1035] section 3.2.2). |
| DNS\_TYPE\_RP  0x0011 | A responsible-person record type [[RFC1183]](http://go.microsoft.com/fwlink/?LinkId=106947). |
| DNS\_TYPE\_AFSDB  0x0012 | A record type containing AFS database location [RFC1183]. |
| DNS\_TYPE\_X25  0x0013 | An X25 PSDN address record type [RFC1183]. |
| DNS\_TYPE\_ISDN  0x0014 | An ISDN address record type [RFC1183]. |
| DNS\_TYPE\_RT  0x0015 | A route through record type [RFC1183]. |
| DNS\_TYPE\_SIG  0x0018 | A cryptographic public key signature record type [[RFC2931]](http://go.microsoft.com/fwlink/?LinkId=107025). |
| DNS\_TYPE\_KEY  0x0019 | A record type containing public key used in DNSSEC [[RFC2535]](http://go.microsoft.com/fwlink/?LinkId=107021). |
| DNS\_TYPE\_AAAA  0x001C | An IPv6 address record type [[RFC3596]](http://go.microsoft.com/fwlink/?LinkId=107027). |
| DNS\_TYPE\_LOC  0x001D | A location information record type [[RFC1876]](http://go.microsoft.com/fwlink/?LinkId=106954). |
| DNS\_TYPE\_NXT  0x001E | A next-domain record type [[RFC2065]](http://go.microsoft.com/fwlink/?LinkId=106958). |
| DNS\_TYPE\_SRV  0x0021 | A server selection record type [[RFC2782]](http://go.microsoft.com/fwlink/?LinkId=90381). |
| DNS\_TYPE\_ATMA  0x0022 | An Asynchronous Transfer Mode (ATM) address record type [[ATMA]](http://go.microsoft.com/fwlink/?LinkId=107028). |
| DNS\_TYPE\_NAPTR  0x0023 | An NAPTR record type [[RFC2915]](http://go.microsoft.com/fwlink/?LinkId=107024). |
| DNS\_TYPE\_DNAME  0x0027 | A DNAME record type [[RFC2672]](http://go.microsoft.com/fwlink/?LinkId=132207). |
| DNS\_TYPE\_DS  0x002B | A DS record type [[RFC4034]](http://go.microsoft.com/fwlink/?LinkId=107052). |
| DNS\_TYPE\_RRSIG  0x002E | An RRSIG record type [RFC4034]. |
| DNS\_TYPE\_NSEC  0x002F | An NSEC record type [RFC4034]. |
| DNS\_TYPE\_DNSKEY  0x0030 | A DNSKEY record type [RFC4034]. |
| DNS\_TYPE\_DHCID  0x0031 | A DHCID record type [[RFC4701]](http://go.microsoft.com/fwlink/?LinkId=125431). |
| DNS\_TYPE\_NSEC3  0x0032 | An NSEC3 record type [[RFC5155]](http://go.microsoft.com/fwlink/?LinkId=225981). |
| DNS\_TYPE\_NSEC3PARAM  0x0033 | An NSEC3PARAM record type [RFC5155]. |
| DNS\_TYPE\_TLSA  0x0034 | A TLSA record type [[RFC6698]](http://go.microsoft.com/fwlink/?LinkId=532821). |
| DNS\_TYPE\_ALL  0x00FF | A query-only type requesting all records [RFC1035]. |
| DNS\_TYPE\_WINS  0xFF01 | A record type containing [**WINS**](#gt_bafb050b-b593-4517-8093-f721bd2378ac) forward lookup data [[MS-WINSRA]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-WINSRA%5d.pdf). |
| DNS\_TYPE\_WINSR  0xFF02 | A record type containing WINS reverse lookup data [MS-WINSRA]. |

An implementation SHOULD[<7>](#Appendix_A_7) support all the preceding record types.

Other type values that are not explicitly defined in the preceding table MUST be enumerable, including values defined by [[IANA-DNS]](http://go.microsoft.com/fwlink/?LinkId=148574).

##### DNS\_RPC\_NODE\_FLAGS

Note: Some of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview in the Product Behavior appendix.

DNS\_RPC\_NODE\_FLAGS enumerates the possible property values for the DNS\_RPC\_NODE and DNS\_RPC\_RECORD structures, which MUST have dwFlags field set to any combination of following possible values. These flags are used to indicate special properties of DNS records and to request special handling of DNS records during enumeration and modification operations.

| Constant/value | Description |
| --- | --- |
| DNS\_RPC\_FLAG\_CACHE\_DATA  0x80000000 | Data is from the DNS [**cache**](#gt_2f48e305-acf2-470e-b481-a0b7cc5fae4f). |
| DNS\_RPC\_FLAG\_ZONE\_ROOT  0x40000000 | Data is from enumeration performed at a zone-root. Applicable for dwFlags in DNS\_RPC\_NODE (section [2.2.2.2.3](#Section_cb5539fa67fd40e09ea5468ecc56bd66)). |
| DNS\_RPC\_FLAG\_AUTH\_ZONE\_ROOT  0x20000000 | Data is from enumeration performed at an authoritative zone-root. Applicable for dwFlags in DNS\_RPC\_NODE (section 2.2.2.2.3). |
| DNS\_RPC\_FLAG\_ZONE\_DELEGATION  0x10000000 | Data is from enumeration performed at a [**node**](#gt_762051d8-4fdc-437e-af9d-3f4da77c3c7d) that is represents in a delegated subzone. Applicable for dwFlags in DNS\_RPC\_NODE (section 2.2.2.2.3). |
| DNS\_RPC\_FLAG\_RECORD\_DEFAULT\_TTL  0x08000000 | Record SHOULD use zone default [**TTL**](#gt_185c4181-772d-4458-bb90-ab0e11370a1c) value. Applicable for dwFlags in DNS\_RPC\_RECORD (section [2.2.2.2.5](#Section_ac7939811c6043b8be59cdbb5c4ecb8a)). |
| DNS\_RPC\_FLAG\_RECORD\_TTL\_CHANGE  0x04000000 | This flag is set in case of update record to update TTL value for the record. Applicable for dwFlags in DNS\_RPC\_RECORD (section 2.2.2.2.5). |
| DNS\_RPC\_FLAG\_RECORD\_CREATE\_PTR  0x02000000 | This flag is set when adding or deleting a record. Applicable for dwFlags in DNS\_RPC\_RECORD (section 2.2.2.2.5). |
| DNS\_RPC\_FLAG\_NODE\_STICKY  0x01000000 | This flag is set when enumerating a node that is at the domain root. Applicable for dwFlags in DNS\_RPC\_NODE (section 2.2.2.2.3). |
| DNS\_RPC\_FLAG\_NODE\_COMPLETE  0x00800000 | This flag is set when requested enumeration is completed with the buffer being returned. Applicable for dwFlags in DNS\_RPC\_NODE (section 2.2.2.2.3). |
| DNS\_RPC\_FLAG\_SUPPRESS\_NOTIFY  0x00010000 | This flag is set when updated record to disable zone-update notifications for a zone. Applicable for dwFlags in DNS\_RPC\_RECORD (section 2.2.2.2.5). |
| DNS\_RPC\_FLAG\_AGING\_ON  0x00020000 | This flag is set when updating a record to enable or disable [**aging**](#gt_0288f9f1-b244-4551-8638-a2280001b531) for a record. Applicable for dwFlags in DNS\_RPC\_RECORD (section 2.2.2.2.5). |
| DNS\_RPC\_FLAG\_OPEN\_ACL  0x00040000 | This flag is set when updating a record to disable access control for a record. Applicable for dwFlags in DNS\_RPC\_RECORD (section 2.2.2.2.5). |
| DNS\_RPC\_FLAG\_RECORD\_WIRE\_FORMAT  0x00100000 | This flag is set when adding a resource record of an unknown type ([[RFC3597]](http://go.microsoft.com/fwlink/?LinkID=532820) section 2). Applicable for dwFlags in DNS\_RPC\_RECORD (section 2.2.2.2.5). |
| DNS\_RPC\_FLAG\_SUPPRESS\_RECORD\_UPDATE\_PTR  0x00200000 | This flag is set when replacing a resource record. Applicable for dwFlags in DNS\_RPC\_RECORD (section 2.2.2.2.5). |

An implementation SHOULD[<8>](#Appendix_A_8) support all of the preceding flags.

#### Structures

##### DNS\_RPC\_NAME

The DNS\_RPC\_NAME structure is used to specify an FQDN, a DNS label, or another string in an RPC buffer by the DNS server. See section [3.1.6.3](#Section_6ad921057d2b4350ae8f80e99c09013e) for the handling of this structure in the directory server.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| cchNameLength | | | | | | | | dnsName (variable) | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**cchNameLength (1 byte):** The length, in bytes, of the string stored in the dnsName member. To represent an empty string, cchNameLength MUST be zero and dnsName MUST be empty. The length of this structure will always be 4-byte aligned so there may be 0-3 bytes of padding at the end of this field. The pad bytes are not included in the cchNameLength count.

**dnsName (variable):** A UTF-8 string with length given by cchNameLength. The string MUST NOT be null-terminated. This string can represent a fully qualified domain name (FQDN) or any other string.

##### DNS\_COUNT\_NAME

The DNS\_COUNT\_NAME structure is used to specify an FQDN in an LDAP message.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Length | | | | | | | | LabelCount | | | | | | | | RawName (variable) | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Length (1 byte):** The length, in bytes, of the string stored in the RawName member, including null termination. To represent an empty string, Length MUST be zero, LabelCount MUST be zero, and RawName MUST be empty.

**LabelCount (1 byte):** The count of DNS labels in the RawName member.

**RawName (variable):** A string containing an FQDN in which a 1-byte label length count for the subsequent label has been inserted before the first label and in place of each "." delimiter. The string MUST be null-terminated. The maximum length of the string, including the null terminator, is 256 bytes.

##### DNS\_RPC\_NODE

DNS\_RPC\_NODE defines a structure that is used as a header for a list of DNS\_RPC\_RECORD structures (section [2.2.2.2.5](#Section_ac7939811c6043b8be59cdbb5c4ecb8a)) returned by the DNS server inside a DNS\_RPC\_BUFFER (section [2.2.1.2.2](#Section_cd4d047c3e894bc2b1651dc60ba538d5)) while processing the R\_DnssrvEnumRecords2 (section [3.1.4.9](#Section_0d236e5899444cdfae98f92460202e29)).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| wLength | | | | | | | | | | | | | | | | wRecordCount | | | | | | | | | | | | | | | |
| dwFlags | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwChildCount | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dnsNodeName (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**wLength (2 bytes):** The length of this structure, in bytes, including the fixed size elements plus the length of the dnsNodeName element. The length of this structure will always be 4-byte aligned so there may be 0-3 bytes of padding at the end of the structure. The pad bytes are included in the wLength count.

**wRecordCount (2 bytes):** The number of DNS\_RPC\_RECORD structures that follow this node structure.

**dwFlags (4 bytes):** The properties of the DNS\_RPC\_NODE structure.

**dwChildCount (4 bytes):** The total number of children nodes below this node in the DNS record database.

**dnsNodeName (variable):** The name of this node in DNS\_RPC\_NAME (section [2.2.2.2.1](#Section_3fd41adcc69e407b979e721251403132)) format.

##### DNS\_RPC\_RECORD\_DATA

DNS\_RPC\_RECORD\_DATA defines a collection of possible resource record structures that are available on the DNS server. This is used by the DNS server while responding to R\_DnssrvEnumRecords2 (section [3.1.4.9](#Section_0d236e5899444cdfae98f92460202e29)) method call to return resource record information inside a DNS\_RPC\_RECORD ([2.2.2.2.5](#Section_ac7939811c6043b8be59cdbb5c4ecb8a)) structure that in turn is encapsulated inside a DNS\_RPC\_BUFFER (section [2.2.1.2.2](#Section_cd4d047c3e894bc2b1651dc60ba538d5)) structure. It is similarly used as input to the R\_DnssrvUpdateRecord (section [3.1.4.5](#Section_37eea10100b8495899ebde8cda4b8417)) and R\_DnssrvUpdateRecord2 (section [3.1.4.10](#Section_8f50ae96d87f4fdb85265a86cea25837)) method calls.

The DNS\_RPC\_RECORD\_DATA MUST be specified in one of the type-specific formats defined in a section that follows, where the type is indicated by the **wType** value in the DNS\_RPC\_RECORD (section 2.2.2.2.5) structure. Further, for each DNS\_RECORD\_TYPE (section [2.2.2.1.1](#Section_39b03b89226440638198d62f62a6441a)) that the server supports, the server MUST support the corresponding DNS\_RPC\_RECORD\_DATA subtype.

###### DNS\_RPC\_RECORD\_A

The DNS\_RPC\_RECORD\_A structure contains an IPv4 address. This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| IPv4 Address | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**IPv4 Address (4 bytes):** An IPv4 address in network byte order.

###### DNS\_RPC\_RECORD\_NODE\_NAME

The DNS\_RPC\_RECORD\_NODE\_NAME structure contains information about a DNS record of any of the following types:[<9>](#Appendix_A_9)

* DNS\_TYPE\_PTR
* DNS\_TYPE\_NS
* DNS\_TYPE\_CNAME
* DNS\_TYPE\_DNAME
* DNS\_TYPE\_MB
* DNS\_TYPE\_MR
* DNS\_TYPE\_MG
* DNS\_TYPE\_MD
* DNS\_TYPE\_MF

This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| nameNode (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**nameNode (variable):** The FQDN of this node in [DNS\_RPC\_NAME (section 2.2.2.2.1)](#Section_3fd41adcc69e407b979e721251403132) format.

###### DNS\_RPC\_RECORD\_SOA

The DNS\_RPC\_RECORD\_SOA structure contains information about an SOA record (section 3.3.13 in [[RFC1035]](http://go.microsoft.com/fwlink/?LinkId=90264)). This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| dwSerialNo | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwRefresh | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwRetry | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwExpire | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwMinimumTtl | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| namePrimaryServer (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Zone Administrator Email (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**dwSerialNo (4 bytes):** The [**serial number**](#gt_9902897a-67ab-4c95-a910-a96bea8ad76e) of the SOA record.

**dwRefresh (4 bytes):** The interval, in seconds, at which a [**secondary DNS server**](#gt_85ec490e-c7d1-4b6d-80b3-23320e7e1c9d) attempts to contact the [**primary DNS server**](#gt_c5f78ae9-df7c-47ee-92f5-5e4f92198cd0) for getting an update.

**dwRetry (4 bytes):** The interval, in seconds, at which a secondary DNS server retries to check with the primary DNS server in case of failure.

**dwExpire (4 bytes):** The duration, in seconds, that a secondary DNS server continues attempts to get updates from the primary DNS server and if still unsuccessful assumes that the primary DNS server is unreachable.

**dwMinimumTtl (4 bytes):** The minimum duration, in seconds, for which record data in the zone is valid.

**namePrimaryServer (variable):** The FQDN of the primary DNS server for this zone in DNS\_RPC\_NAME (section [2.2.2.2.1](#Section_3fd41adcc69e407b979e721251403132)) format.

**Zone Administrator Email (variable):** The contact email address for the zone administrators in a structure of type DNS\_RPC\_NAME (section 2.2.2.2.1).

###### DNS\_RPC\_RECORD\_NULL

The DNS\_RPC\_RECORD\_NULL structure contains information for any record for which there is no more specific [DNS\_RPC\_RECORD](#Section_ac7939811c6043b8be59cdbb5c4ecb8a) structure. This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| bData (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**bData (variable):** An array of data. The sender can provide any data in this array.

###### DNS\_RPC\_RECORD\_WKS

The DNS\_RPC\_RECORD\_WKS structure contains the information for the well known services supported by a host, as defined in section 3.4.2 [[RFC1035]](http://go.microsoft.com/fwlink/?LinkId=90264). This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| ipAddress | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| chProtocol | | | | | | | | bBitMask (variable) | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**ipAddress (4 bytes):** The IPv4 address of the server that provides the service.

**chProtocol (1 byte):** The IP protocol number as specified in [[IANA-PROTO-NUM]](http://go.microsoft.com/fwlink/?LinkId=89889).

**bBitMask (variable):** A list of service names (specified as "keywords" in the "WELL KNOWN PORT NUMBERS" section of [[IANAPORT]](http://go.microsoft.com/fwlink/?LinkId=89888)) or port number if service name is unknown as an [**ASCII**](#gt_79fa85ca-ac61-467c-b819-e97dc1a7a599) character string in DNS\_RPC\_NAME (section [2.2.2.2.1](#Section_3fd41adcc69e407b979e721251403132)) format. If more than one port is listed for a single combination of service name and IP protocol number, then only the first such port number is indicated when that service name is used. Each service name or port MUST be separated by a single space character, and the string MUST be terminated by a single null character. Each port number specified MUST be less than or equal to 1024. The terminating null character MUST be included in the **cchNameLength** field of the DNS\_RPC\_NAME (section 2.2.2.2.1) structure.

###### DNS\_RPC\_RECORD\_STRING

The DNS\_RPC\_RECORD\_STRING structure contains information about a DNS record of any of the following types:

* DNS\_TYPE\_HINFO
* DNS\_TYPE\_ISDN
* DNS\_TYPE\_TXT
* DNS\_TYPE\_X25
* DNS\_TYPE\_LOC

This packet contains one or more instances of stringData, depending upon the type listed above. This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| stringData (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**stringData (variable):** Each stringData member contains the host name value for a node in DNS\_RPC\_NAME (section [2.2.2.2.1](#Section_3fd41adcc69e407b979e721251403132)) structure.

###### DNS\_RPC\_RECORD\_MAIL\_ERROR

The DNS\_RPC\_RECORD\_MAIL\_ERROR structure contains information about a DNS record of any of the following types:

* DNS\_TYPE\_MINFO
* DNS\_TYPE\_RP

This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| nameMailBox (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ErrorMailBox (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**nameMailBox (variable):** A structure of type DNS\_RPC\_NAME (section [2.2.2.2.1](#Section_3fd41adcc69e407b979e721251403132)) containing the RMAILBX value specified in section 3.3.7 of [[RFC1035]](http://go.microsoft.com/fwlink/?LinkId=90264) for an MINFO record, or the mbox-dname value specified in section 2.2 of [[RFC1183]](http://go.microsoft.com/fwlink/?LinkId=106947) for an RP record.

**ErrorMailBox (variable):** A structure of type DNS\_RPC\_NAME (section 2.2.2.2.1) containing the EMAILBX value specified in section 3.3.7 of [RFC1035] for an MINFO record, or the txt-dname value specified in section 2.2 of [RFC1183] for an RP record.

###### DNS\_RPC\_RECORD\_NAME\_PREFERENCE

The DNS\_RPC\_RECORD\_NAME\_PREFERENCE structure specifies information about a DNS record of any of the following types:

* DNS\_TYPE\_MX
* DNS\_TYPE\_AFSDB
* DNS\_TYPE\_RT

This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| wPreference | | | | | | | | | | | | | | | | nameExchange (variable) | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**wPreference (2 bytes):** The preference value for the DNS server that holds the record.

**nameExchange (variable):** The FQDN of the server hosting the mail-exchange and specified in DNS\_RPC\_NAME (section [2.2.2.2.1](#Section_3fd41adcc69e407b979e721251403132)) format.

###### DNS\_RPC\_RECORD\_SIG

The DNS\_RPC\_RECORD\_SIG structure contains information about cryptographic public key signatures as specified in section 4 of [[RFC2535]](http://go.microsoft.com/fwlink/?LinkId=107021).[<10>](#Appendix_A_10) This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| wTypeCovered | | | | | | | | | | | | | | | | chAlgorithm | | | | | | | | chLabelCount | | | | | | | |
| dwOriginalTtl | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwSigExpiration | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwSigInception | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| wKeyTag | | | | | | | | | | | | | | | | nameSigner (variable) | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SignatureInfo (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**wTypeCovered (2 bytes):** The type covered value for SIG RR as specified in section 4.1 of [RFC2535].

**chAlgorithm (1 byte):** The algorithm value for SIG RR as specified in section 4.1 of [RFC2535].

**chLabelCount (1 byte):** The total number of labels present in the name of the record signed by the SIG RR as specified in section 4.1 of [RFC2535].

**dwOriginalTtl (4 bytes):** The original TTL value of the record signed by the SIG RR as specified in section 4.1 of [RFC2535].

**dwSigExpiration (4 bytes):** The signature expiration time as specified in section 4.1 of [RFC2535].

**dwSigInception (4 bytes):** The signature inception time as specified in section 4.1 of [RFC2535].

**wKeyTag (2 bytes):** The key tag value for SIG RR as specified in section 4.1 of [RFC2535].

**nameSigner (variable):** Pointer to a structure of type [DNS\_RPC\_NAME](#Section_3fd41adcc69e407b979e721251403132) (section 2.2.2.2.1) containing the FQDN of the originating host for this record.

**SignatureInfo (variable):** Binary signature information as specified in section 4.1 of [RFC2535].

###### DNS\_RPC\_RECORD\_RRSIG

The DNS\_RPC\_RECORD\_RRSIG structure contains information about cryptographic public key signatures as specified in section 3 of [[RFC4034]](http://go.microsoft.com/fwlink/?LinkId=107052).[<11>](#Appendix_A_11) This record MUST be formatted as follows.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| wTypeCovered | | | | | | | | | | | | | | | | chAlgorithm | | | | | | | | chLabelCount | | | | | | | |
| dwOriginalTtl | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwSigExpiration | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwSigInception | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| wKeyTag | | | | | | | | | | | | | | | | nameSigner (variable) | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SignatureInfo (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**wTypeCovered (2 bytes):** The type covered value for RRSIG RR as specified in section 3.1 of [RFC4034].

**chAlgorithm (1 byte):** The algorithm value for RRSIG RR as specified in section 3.1 of [RFC4034].

**chLabelCount (1 byte):** The total number of labels present in the name of the record signed by the RRSIG RR as specified in section 3.1 of [RFC4034].

**dwOriginalTtl (4 bytes):** The original TTL value of the record signed by the RRSIG RR as specified in section 3.1 of [RFC4034].

**dwSigExpiration (4 bytes):** The signature expiration time as specified in section 3.1 of [RFC4034].

**dwSigInception (4 bytes):** The signature inception time as specified in section 3.1 of [RFC4034].

**wKeyTag (2 bytes):** The tag value for RRSIG RR as specified in section 3.1 of [RFC4034].

**nameSigner (variable):** A structure of type [DNS\_RPC\_NAME](#Section_3fd41adcc69e407b979e721251403132) (section 2.2.2.2.1) containing the FQDN of the originating host for this record.

**SignatureInfo (variable):** Binary signature information as specified in section 3.1 of [RFC4034].

###### DNS\_RPC\_RECORD\_NSEC

The DNS\_RPC\_RECORD\_NSEC structure contains the next FQDN in the zone as specified in section 4 of [[RFC4034]](http://go.microsoft.com/fwlink/?LinkId=107052).[<12>](#Appendix_A_12) This record MUST be formatted as follows.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| nameSigner (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NSECBitmap (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**nameSigner (variable):** A structure of type [DNS\_RPC\_NAME](#Section_3fd41adcc69e407b979e721251403132) (section 2.2.2.2.1) containing the FQDN of the originating host for this record.

**NSECBitmap (variable):** Bitmap of types present at this node as specified in section 4 of [RFC4034].

###### DNS\_RPC\_RECORD\_DS

The DNS\_RPC\_RECORD\_DS structure contains a public key associated with an FQDN as specified in section 5 of [[RFC4034]](http://go.microsoft.com/fwlink/?LinkId=107052).[<13>](#Appendix_A_13) This record MUST be formatted as follows.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| wKeyTag | | | | | | | | | | | | | | | | chAlgorithm | | | | | | | | chDigestType | | | | | | | |
| bDigest (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**wKeyTag (2 bytes):** The key tag of the DNSKEY record referred to by this DS record, as specified in section 5 of [RFC4034].

**chAlgorithm (1 byte):** Algorithm value of the DNSKEY record referred to by this DS record, as specified in section 5 of [RFC4034].

**chDigestType (1 byte):** The digest algorithm that was used to construct this DS record, as specified in section 5 of [RFC4034].

**bDigest (variable):** An array of bytes containing the digest value as specified of section 5 in [RFC4034].

###### DNS\_RPC\_RECORD\_KEY

The DNS\_RPC\_RECORD\_KEY structure contains a public key associated with an FQDN as specified in section 3 of [[RFC2535]](http://go.microsoft.com/fwlink/?LinkId=107021).[<14>](#Appendix_A_14) This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| wFlags | | | | | | | | | | | | | | | | chProtocol | | | | | | | | chAlgorithm | | | | | | | |
| bKey (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**wFlags (2 bytes):** Flags value for the key RR as specified in section 3.1 of [RFC2535].

**chProtocol (1 byte):** Protocol value for the key RR as specified in section 3.1 of [RFC2535].

**chAlgorithm (1 byte):** Algorithm value for the key RR as specified in section 3.1 of [RFC2535].

**bKey (variable):** An array of bytes containing the key value as specified of section 3.1 in [RFC2535].

###### DNS\_RPC\_RECORD\_DHCID

The DNS\_RPC\_RECORD\_DHCID structure contains a public key associated with an FQDN as specified in section 3 of [[RFC2535]](http://go.microsoft.com/fwlink/?LinkId=107021).[<15>](#Appendix_A_15) This record MUST be formatted as follows.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| bDHCID (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**bDHCID (variable):** An opaque DHCID record as specified in section 3 in [[RFC4701]](http://go.microsoft.com/fwlink/?LinkId=125431).

###### DNS\_RPC\_RECORD\_DNSKEY

The DNS\_RPC\_RECORD\_DNSKEY structure contains a public key associated with an FQDN as specified in section 2 of [[RFC4034]](http://go.microsoft.com/fwlink/?LinkId=107052).[<16>](#Appendix_A_16) This record MUST be formatted as follows.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| wFlags | | | | | | | | | | | | | | | | chProtocol | | | | | | | | chAlgorithm | | | | | | | |
| bKey (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**wFlags (2 bytes):** Flags value for the key RR as specified in section 2.1 of [RFC4034].

**chProtocol (1 byte):** Protocol value for the key RR as specified in section 2.1 of [RFC4034].

**chAlgorithm (1 byte):** Algorithm value for the key RR as specified in section 2.1 of [RFC4034].

**bKey (variable):** An array of bytes containing the key value as specified of section 2.1 in [RFC4034].

###### DNS\_RPC\_RECORD\_AAAA

The DNS\_RPC\_RECORD\_AAAA structure contains IPv6 address information. This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| ipv6Address (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**ipv6Address (16 bytes):** An IPv6 address member holds an IPv6 address, in network byte order.

###### DNS\_RPC\_RECORD\_NXT

The DNS\_RPC\_RECORD\_NXT specifies a NXT resource record as specified in section 5.1 of [[RFC2535]](http://go.microsoft.com/fwlink/?LinkId=107021).[<17>](#Appendix_A_17) This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| wNumRecordTypes | | | | | | | | | | | | | | | | wTypeWords (variable) | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| nextName (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**wNumRecordTypes (2 bytes):** The number of 16-bit unsigned integers in the variable sized wTypeWords array. This value MUST be greater than 1.

**wTypeWords (variable):** An array for of 16-bit unsigned integers in little-endian byte order for that contains a variable sized bit-mask value for types present in this record, as specified in section 5.2 of [RFC2535]. The most significant bit of the first integer corresponds to type zero and MUST be zero. If there is a second 16-bit unsigned integer present in the array, the most significant bit of the second integer corresponds to type 16, and so on.

**nextName (variable):** A DNS\_RPC\_NAME (section [2.2.2.2.1](#Section_3fd41adcc69e407b979e721251403132)) containing next name information, as specified in section 5.2 of [RFC2535].

###### DNS\_RPC\_RECORD\_SRV

The DNS\_RPC\_RECORD\_SRV specifies an SRV resource record as specified in [[RFC2782]](http://go.microsoft.com/fwlink/?LinkId=90381). This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| wPriority | | | | | | | | | | | | | | | | wWeight | | | | | | | | | | | | | | | |
| wPort | | | | | | | | | | | | | | | | nameTarget (variable) | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**wPriority (2 bytes):** The priority of the target host as specified in [RFC2782].

**wWeight (2 bytes):** The relative weight for the target host as specified in [RFC2782].

**wPort (2 bytes):** The port number for the service on the target host as specified in [RFC2782].

**nameTarget (variable):** The FDQN of the server that hosts this service in DNS\_RPC\_NAME (section [2.2.2.2.1](#Section_3fd41adcc69e407b979e721251403132)) format, as specified in [RFC2782].

###### DNS\_RPC\_RECORD\_ATMA

The DNS\_RPC\_RECORD\_ATMA specifies a resource record that contains ATM address information as specified in [[ATMA]](http://go.microsoft.com/fwlink/?LinkId=107028). This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| chFormat | | | | | | | | bAddress (variable) | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**chFormat (1 byte):** The format of the address as specified in section 5.2 of [ATMA].

**bAddress (variable):** The ATM address of the node to which this resource record pertains (see section 5.2 of [ATMA]).

###### DNS\_RPC\_RECORD\_NAPTR

The DNS\_RPC\_RECORD\_NAPTR specifies a NAPTR resource record as specified in section 4 of [[RFC3403]](http://go.microsoft.com/fwlink/?LinkId=107026).[<18>](#Appendix_A_18) This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| wOrder | | | | | | | | | | | | | | | | wPreference | | | | | | | | | | | | | | | |
| nameFlags (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| nameService (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| nameSubstitution (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| nameReplacement (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**wOrder (2 bytes):** A value that specifies the order in which the NAPTR record is processed, as specified in section 4.1 in [RFC3403].

**wPreference (2 bytes):** The preference given to this NAPTR record, as specified in section 4.1 in [RFC3403].

**nameFlags (variable):** Pointer to a structure of type DNS\_RPC\_NAME (section [2.2.2.2.1](#Section_3fd41adcc69e407b979e721251403132)) containing the string flags value as specified in section 4.1 in [RFC3403].

**nameService (variable):** Pointer to a structure of type DNS\_RPC\_NAME (section 2.2.2.2.1) containing service parameters value for NAPTR to control the rewriting and interpretation of the field in the record, as specified in section 4.1 in [RFC3403].

**nameSubstitution (variable):** Pointer to a structure of type DNS\_RPC\_NAME (section 2.2.2.2.1) containing a substitution expression value for the NAPTR record, as specified in section 4.1 in [RFC3403].

**nameReplacement (variable):** Pointer to a structure of type DNS\_RPC\_NAME (section 2.2.2.2.1) containing a replacement expression value for the NAPTR record, as specified in section 4.1 in [RFC3403].

###### DNS\_RPC\_RECORD\_WINS

The DNS\_RPC\_RECORD\_WINS specifies a WINS resource record. This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| dwMappingFlag | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwLookupTimeout | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwCacheTimeout | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| cWinsServerCount | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| aipWinsServers (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**dwMappingFlag (4 bytes):** The scope of the WINS record lookups. This value MUST be set to 0x00000000 or any combination of the following:

| Value | Meaning |
| --- | --- |
| DNS\_WINS\_FLAG\_SCOPE  0x80000000 | Server forwards lookup requests to remote WINS servers. |
| DNS\_WINS\_FLAG\_LOCAL  0x00010000 | Server performs WINS lookups locally. |

**dwLookupTimeout (4 bytes):** The duration, in seconds, for which the server waits to receive a response from a remote DNS server.

**dwCacheTimeout (4 bytes):** The duration, in seconds, for which the server keeps this record in its cache before considering it stale.

**cWinsServerCount (4 bytes):** The number of WINS server addresses in this record. The value of this field MUST be at least one.

**aipWinsServers (variable):** An array of IPv4 addresses in network byte order with length given by cWinsServerCount.

###### DNS\_RPC\_RECORD\_WINSR

The DNS\_RPC\_RECORD\_WINSR specifies a [**Windows Internet Name Service Reverse Lookup (WINS-R)**](#gt_5b990252-86cc-4c08-b06b-49d703ea4d18) resource record. This record MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| dwMappingFlag | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwLookupTimeout | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwCacheTimeout | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| nameResultDomain (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**dwMappingFlag (4 bytes):** The scope of the WINS-R record lookups. This value MUST be set to zero or any combination of the following:

| Value | Meaning |
| --- | --- |
| DNS\_WINS\_FLAG\_SCOPE  0x80000000 | Server forwards lookup requests to remote WINS servers. |
| DNS\_WINS\_FLAG\_LOCAL  0x00010000 | Server performs WINS lookups locally. |

**dwLookupTimeout (4 bytes):** The duration, in seconds, for which server waits to receive a response from a remote DNS server.

**dwCacheTimeout (4 bytes):** The duration, in seconds, for which server keeps this record in its cache before considering it stale.

**nameResultDomain (variable):** Pointer to a structure of type DNS\_RPC\_NAME (section [2.2.2.2.1](#Section_3fd41adcc69e407b979e721251403132)) containing a domain name suffix that will be appended to a [**single-label name**](#gt_711c326a-c3c3-4f78-9e92-b10b5581c59c) obtained from a WINS-R lookup.

###### DNS\_RPC\_RECORD\_TS

The DNS\_RPC\_RECORD\_TS specifies information for a node that has been [**tombstoned**](#gt_9d8e0963-13fa-4e19-a97f-7ce6bc90d20f).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| EntombedTime | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**EntombedTime (8 bytes):** The time at which this node was tombstoned, represented as the number of 100-nanosecond intervals since midnight (00:00:00), January 1, 1601 UTC.

###### DNS\_RPC\_RECORD\_NSEC3

The DNS\_RPC\_RECORD\_NSEC3 structure specifies an NSEC3 resource record as specified in [[RFC5155]](http://go.microsoft.com/fwlink/?LinkId=225981) section 3.[<19>](#Appendix_A_19) This record MUST be formatted as follows.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| chAlgorithm | | | | | | | | bFlags | | | | | | | | wIterations | | | | | | | | | | | | | | | |
| bSaltLength | | | | | | | | bHashLength | | | | | | | | salt (variable) | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| nextHashedOwnerName (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| bitmaps (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**chAlgorithm (1 byte):** A value that specifies the cryptographic hash algorithm used to construct the hash value, as specified in [RFC5155] section 3.1.

**bFlags (1 byte):** A value that specifies NSEC3 processing flags, as specified in [RFC5155] section 3.1.

**wIterations (2 bytes):** A value that specifies the number of additional times the hash function has been performed, as specified in [RFC5155] section 3.1.

**bSaltLength (1 byte):** A value that specifies the length of the salt field, in octets.

**bHashLength (1 byte):** A value that specifies the length of the nextHashedOwnerName field, in octets.

**salt (variable):** A value that specifies the salt to be appended to the original owner name before hashing, as specified in [RFC5155] section 3.1.

**nextHashedOwnerName (variable):** A value that specifies the next hashed owner name in hash order, as specified in [RFC5155] section 3.1.

**bitmaps (variable):** A value that specifies the DNS types that exist at the original owner name of the NSEC3 record, as specified in [RFC5155] section 3.1.

###### DNS\_RPC\_RECORD\_NSEC3PARAM

The DNS\_RPC\_RECORD\_NSEC3PARAM structure specifies an NSEC3PARAM resource record as specified in [[RFC5155]](http://go.microsoft.com/fwlink/?LinkId=225981) section 3.[<20>](#Appendix_A_20) This record MUST be formatted as follows.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| chAlgorithm | | | | | | | | bFlags | | | | | | | | wIterations | | | | | | | | | | | | | | | |
| bSaltLength | | | | | | | | salt (variable) | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**chAlgorithm (1 byte):** A value that specifies the cryptographic hash algorithm used to construct the hash value, as specified in [RFC5155] section 4.1.

**bFlags (1 byte):** A value that specifies NSEC3 processing flags, as specified in [RFC5155] section 3.1.

**wIterations (2 bytes):** A value that specifies the number of additional times the hash function has been performed, as specified in [RFC5155] section 4.1.

**bSaltLength (1 byte):** A value that specifies the length of the salt field, in octets.

**salt (variable):** A value that specifies the salt to be appended to the original owner name before hashing, as specified in [RFC5155].

###### DNS\_RPC\_RECORD\_TLSA

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The DNS\_RPC\_RECORD\_TLSA structure SHOULD[<21>](#Appendix_A_21) specify a TLSA resource record as defined in [[RFC6698]](http://go.microsoft.com/fwlink/?LinkId=532821) section 2. This record MUST be formatted as follows.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| bCertUsage | | | | | | | | bSelector | | | | | | | | bMatchingType | | | | | | | | bCertificateAssociationData | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**bCertUsage (1 byte)**: Specifies the association used to match the certificate presented during TLS handshake ([RFC6698] section 2.1.1).

**bSelector (1 byte)**: Specifies the part of the TLS certificate which will be matched against the TLS association data ([RFC6698] section 2.1.2.

**bMatchingType (1 byte)**: Specifies how the certificate association is presented ([RFC6698] section 2.1.3).

**bCertificateAssociationData (variable)**: Specifies the certificate association data that is to be matched ([RFC6698] section 2.1.4).

###### DNS\_RPC\_RECORD\_UNKNOWN

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The DNS\_RPC\_RECORD\_UNKNOWN structure SHOULD[<22>](#Appendix_A_22) specify a resource record of unknown type ([[RFC3597]](http://go.microsoft.com/fwlink/?LinkID=532820) section 2). This record MUST be formatted as follows.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| bData … | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**bData (variable)**: Specifies the unknown record data. The data MUST be in the format in which it will be returned in the response message for a DNS query.

##### DNS\_RPC\_RECORD

Note: Some of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview in the Product Behavior appendix.

The DNS\_RPC\_RECORD structure is used to specify a single DNS record's parameters and data. This structure is returned by the DNS server in response to an R\_DnssrvEnumRecords2 (section [3.1.4.9](#Section_0d236e5899444cdfae98f92460202e29)) method call.

1. typedef struct \_DnssrvRpcRecord {
2. WORD wDataLength;
3. WORD wType;
4. DWORD dwFlags;
5. DWORD dwSerial;
6. DWORD dwTtlSeconds;
7. DWORD dwTimeStamp;
8. DWORD dwReserved;
9. [size\_is(wDataLength)] BYTE Buffer[];
10. } DNS\_RPC\_RECORD,
11. \*PDNS\_RPC\_RECORD,
12. DNS\_FLAT\_RECORD,
13. \*PDNS\_FLAT\_RECORD;

**wDataLength:**  The total size of the variable buffer, in bytes. Note that the DNS\_RPC\_RECORD structure is always 4-byte aligned, which means there may be 0-3 bytes of padding at the end of the structure. The pad bytes are not included in the wDataLength count.

**wType:**  The type of the resource record, as specified in section [2.2.2.1.1](#Section_39b03b89226440638198d62f62a6441a) DNS\_RECORD\_TYPE.

**dwFlags:**  Resource record properties. This field can contain one of the RANK\* flags in the low-order bits and one of the DNS\_RPC\_FLAGS\* in the high-order bits.

| Value | Meaning |
| --- | --- |
| RANK\_CACHE\_BIT  0x00000001 | The record came from the cache. |
| RANK\_ROOT\_HINT  0x00000008 | The record is a preconfigured root hint. |
| RANK\_OUTSIDE\_GLUE  0x00000020 | This value is not used. |
| RANK\_CACHE\_NA\_ADDITIONAL  0x00000031 | The record was cached from the additional section of a non-authoritative response. |
| RANK\_CACHE\_NA\_AUTHORITY  0x00000041 | The record was cached from the authority section of a non-authoritative response. |
| RANK\_CACHE\_A\_ADDITIONAL  0x00000051 | The record was cached from the additional section of an authoritative response. |
| RANK\_CACHE\_NA\_ANSWER  0x00000061 | The record was cached from the answer section of a non-authoritative response. |
| RANK\_CACHE\_A\_AUTHORITY  0x00000071 | The record was cached from the authority section of an authoritative response. |
| RANK\_GLUE  0x00000080 | The record is a [**glue record**](#gt_5aa9e7c0-e2fd-45f3-9edd-076147deba0a) in an authoritative zone. |
| RANK\_NS\_GLUE  0x00000082 | The record is a [**delegation**](#gt_32174781-13ee-48b0-8fc0-ef6bbe207573) (type NS) record in an authoritative zone. |
| RANK\_CACHE\_A\_ANSWER  0x000000c1 | The record was cached from the answer section of an authoritative response. |
| RANK\_ZONE  0x000000f0 | The record comes from an authoritative zone. |
| DNS\_RPC\_FLAG\_ZONE\_ROOT  0x40000000 | The record is at the root of a zone (not necessarily a zone hosted by this server; the record could have come from the cache). |
| DNS\_RPC\_FLAG\_AUTH\_ZONE\_ROOT  0x20000000 | The record is at the root of a zone that is locally hosted on this server. |
| DNS\_RPC\_FLAG\_CACHE\_DATA  0x80000000 | The record came from the cache. |
| DNS\_RPC\_FLAG\_RECORD\_WIRE\_FORMAT  0x00100000 | The record SHOULD[<23>](#Appendix_A_23) be treated as a resource record of unknown type ([[RFC3597]](http://go.microsoft.com/fwlink/?LinkID=532820) section 2) by the DNS server. |

**dwSerial:**  This MUST be set to 0x00000000 when sent by the client or server, and ignored on receipt by the server or client.

**dwTtlSeconds:**  The duration, in seconds, after which this record will expire.

**dwTimeStamp:**  The [**time stamp**](#gt_391ec606-c265-48f2-aeeb-3245b5503121), in hours, for the record when it received the last update.

**dwReserved:**  This value MUST be set to 0x00000000 when sent by the client and ignored on receipt by the server.

**Buffer:**  Record data in DNS\_RPC\_RECORD\_DATA (section [2.2.2.2.4](#Section_38b873927f614e3092639f0fb832d084)) format where type is specified by the value **wType**.[<24>](#Appendix_A_24)

| Value | Meaning |
| --- | --- |
| DNS\_TYPE\_ZERO  0x0000 | DNS\_RPC\_RECORD\_TS |
| DNS\_TYPE\_A  0x0001 | DNS\_RPC\_RECORD\_A |
| DNS\_TYPE\_NS  0x0002 | DNS\_RPC\_RECORD\_NODE\_NAME |
| DNS\_TYPE\_MD  0x0003 | DNS\_RPC\_RECORD\_NODE\_NAME |
| DNS\_TYPE\_MF  0x0004 | DNS\_RPC\_RECORD\_NODE\_NAME |
| DNS\_TYPE\_CNAME  0x0005 | DNS\_RPC\_RECORD\_NODE\_NAME |
| DNS\_TYPE\_SOA  0x0006 | DNS\_RPC\_RECORD\_SOA |
| DNS\_TYPE\_MB  0x0007 | DNS\_RPC\_RECORD\_NODE\_NAME |
| DNS\_TYPE\_MG  0x0008 | DNS\_RPC\_RECORD\_NODE\_NAME |
| DNS\_TYPE\_MR  0x0009 | DNS\_RPC\_RECORD\_NODE\_NAME |
| DNS\_TYPE\_NULL  0x000A | DNS\_RPC\_RECORD\_NULL |
| DNS\_TYPE\_WKS  0x000B | DNS\_RPC\_RECORD\_WKS |
| DNS\_TYPE\_PTR  0x000C | DNS\_RPC\_RECORD\_NODE\_NAME |
| DNS\_TYPE\_HINFO  0x000D | DNS\_RPC\_RECORD\_STRING |
| DNS\_TYPE\_MINFO  0x000E | DNS\_RPC\_RECORD\_MAIL\_ERROR |
| DNS\_TYPE\_MX  0x000F | DNS\_RPC\_RECORD\_NAME\_PREFERENCE |
| DNS\_TYPE\_TXT  0x0010 | DNS\_RPC\_RECORD\_STRING |
| DNS\_TYPE\_RP  0x0011 | DNS\_RPC\_RECORD\_MAIL\_ERROR |
| DNS\_TYPE\_AFSDB  0x0012 | DNS\_RPC\_RECORD\_NAME\_PREFERENCE |
| DNS\_TYPE\_X25  0x0013 | DNS\_RPC\_RECORD\_STRING |
| DNS\_TYPE\_ISDN  0x0014 | DNS\_RPC\_RECORD\_STRING |
| DNS\_TYPE\_RT  0x0015 | DNS\_RPC\_RECORD\_NAME\_PREFERENCE |
| DNS\_TYPE\_SIG  0x0018 | DNS\_RPC\_RECORD\_SIG |
| DNS\_TYPE\_KEY  0x0019 | DNS\_RPC\_RECORD\_KEY |
| DNS\_TYPE\_AAAA  0x001C | DNS\_RPC\_RECORD\_AAAA |
| DNS\_TYPE\_NXT  0x001E | DNS\_RPC\_RECORD\_NXT |
| DNS\_TYPE\_SRV  0x0021 | DNS\_RPC\_RECORD\_SRV |
| DNS\_TYPE\_ATMA  0x0022 | DNS\_RPC\_RECORD\_ATMA |
| DNS\_TYPE\_NAPTR  0x0023 | DNS\_RPC\_RECORD\_NAPTR |
| DNS\_TYPE\_DNAME  0x0027 | DNS\_RPC\_RECORD\_NODE\_NAME |
| DNS\_TYPE\_DS  0x002B | DNS\_RPC\_RECORD\_DS |
| DNS\_TYPE\_RRSIG  0x002E | DNS\_RPC\_RECORD\_RRSIG |
| DNS\_TYPE\_NSEC  0x002F | DNS\_RPC\_RECORD\_NSEC |
| DNS\_TYPE\_DNSKEY  0x0030 | DNS\_RPC\_RECORD\_DNSKEY |
| DNS\_TYPE\_DHCID  0x0031 | DNS\_RPC\_RECORD\_DHCID |
| DNS\_TYPE\_NSEC3  0x0032 | DNS\_RPC\_RECORD\_NSEC3 |
| DNS\_TYPE\_NSEC3PARAM  0x0033 | DNS\_RPC\_RECORD\_NSEC3PARAM |
| DNS\_TYPE\_TLSA  0x0034 | DNS\_RPC\_RECORD\_TLSA |
| DNS\_TYPE\_WINS  0xFF01 | DNS\_RPC\_RECORD\_WINS |
| DNS\_TYPE\_WINSR  0xFF02 | DNS\_RPC\_RECORD\_WINSR |

Other type values that are not explicitly defined in the preceding table MUST be enumerable, including values defined by [[IANA-DNS]](http://go.microsoft.com/fwlink/?LinkId=148574), and they MUST use the DNS\_RPC\_RECORD\_NULL (section [2.2.2.2.4.4](#Section_308da71d67db4a0b96b1d0120aaf0017)) structure. If the **dwFlags** field is set to DNS\_RPC\_FLAG\_RECORD\_WIRE\_FORMAT, the DNS\_RPC\_RECORD\_UNKNOWN (section [2.2.2.2.4.27](#Section_48645c7312e84b60baf7c28f80a14ac4)) structure MUST be used for all resource record types.

### Address Information Messages

#### Enumerations and Constants

##### DNS\_IPVAL\_CONTEXT

DNS\_IPVAL\_CONTEXT is a DWORD value that specifies possible context values for IP validation. This is used to populate the dwContext field in DNS\_RPC\_IP\_VALIDATE (section [2.2.3.2.4](#Section_2a367e0b5a8245d6aa77fbf407ed8d61)). The DNS server MUST use this value to determine the type of validation that SHOULD[<25>](#Appendix_A_25) be performed for IP address specified in DNS\_RPC\_IP\_VALIDATE (section 2.2.3.2.4).

| Constant/value | Description |
| --- | --- |
| DNS\_IPVAL\_DNS\_SERVERS  0x00000000 | Validate that IP addresses are reachable and operational by the DNS servers. |
| DNS\_IPVAL\_DNS\_ROOTHINTS  0x00000001 | Validate that IP addresses are suitable as root-hints. |
| DNS\_IPVAL\_DNS\_FORWARDERS  0x00000002 | Validate that IP addresses are server level forwarders. |
| DNS\_IPVAL\_DNS\_ZONE\_MASTERS  0x00000003 | Validate that IP addresses are remote DNS servers hosting a zone, named as pointed to by pszContextName in the DNS\_RPC\_IP\_VALIDATE (section 2.2.3.2.4). |
| DNS\_IPVAL\_DNS\_DELEGATIONS  0x00000004 | Validate that IP addresses are remote DNS servers are name-server for the delegated zone, named as pointed to by **pszContextName** in the DNS\_RPC\_IP\_VALIDATE (section 2.2.3.2.4). |

##### DNS\_IP\_VALIDATE\_RETURN\_FLAGS

DNS\_IP\_VALIDATE\_RETURN\_FLAGS is a DWORD value that specifies the results of IP validation performed by the DNS server. This value will be used by the DNS server to populate the Flags field within each DNS\_ADDR structure (section [2.2.3.2.2](#Section_835c236a4d354a1ebc4cf5eb27bfb06d)) present in the DNS\_ADDR\_ARRAY (section [2.2.3.2.3](#Section_56ba5fabf304486699a44f1c1f9247a3)) structure which in turn is present inside the returned DNS\_RPC\_IP\_VALIDATE structure (section [2.2.3.2.4](#Section_2a367e0b5a8245d6aa77fbf407ed8d61))[<26>](#Appendix_A_26).

| Constant/value | Description |
| --- | --- |
| ERROR\_SUCCESS  0x00000000 | The remote IP address is valid. |
| DNS\_IPVAL\_INVALID\_ADDR  0x00000001 | Remote IP address is not a valid IP address. |
| DNS\_IPVAL\_UNREACHABLE  0x00000002 | Remote IP address is not reachable. |
| DNS\_IPVAL\_NO\_RESPONSE  0x00000003 | Remote IP address does not appear to be hosting a DNS server. |
| DNS\_IPVAL\_NOT\_AUTH\_FOR\_ZONE  0x00000004 | Remote IP address is not authoritative for the required zone, specified by pszContextName in the DNS\_RPC\_IP\_VALIDATE (section 2.2.3.2.4). |
| DNS\_IPVAL\_UNKNOWN\_ERROR  0x000000FF | The DNS server encountered an unknown error occurred while validating IP address. |
| DNS\_IPVAL\_NO\_TCP  0x80000000 | Indicated that remote IP address, responds to UDP DNS messages, but does not respond to TCP DNS messages. |

#### Structures

##### IP4\_ARRAY

The IP4\_ARRAY structure is used to represent an array of IPv4 addresses. This structure cannot represent IPv6 addresses.

1. typedef struct \_IP4\_ARRAY {
2. DWORD AddrCount;
3. [size\_is(AddrCount)] DWORD AddrArray[];
4. } IP4\_ARRAY,
5. \*PIP4\_ARRAY;

**AddrCount:**  The number of IPv4 addresses present in the AddrArray member.

**AddrArray:**  An array of IPv4 addresses. An IPv4 address is represented as a 32-bit unsigned integer in network byte order.

An empty IP4\_ARRAY is represented by **AddrCount** set to zero and **AddrArray** unused. Senders of an empty IP4\_ARRAY MUST set **AddrArray** to a single entry containing binary zeros, and receivers MUST ignore it.

##### DNS\_ADDR

This DNS\_ADDR structure is used to represent an IP address. The IP address may be either IPv4 or IPv6.

1. typedef struct \_DnsAddr {
2. CHAR MaxSa[32];
3. DWORD DnsAddrUserDword[8];
4. } DNS\_ADDR,
5. \*PDNS\_ADDR;

**MaxSa:**  This field MUST be constructed as specified in [DNS ADDR](#Section_aea3ba9bde484f0ea4c84f7c89404b99).

**DnsAddrUserDword:**  This field MUST be constructed as specified in [DNS ADD USER](#Section_6e041c763b55480a84fbfeebcb0cc9db).

Any field not specified above MUST be set to zero by the sender and ignored by the receiver.

###### DNS ADDR

An IPv4 or IPv6 addressed used by [DNS\_ADDR](#Section_835c236a4d354a1ebc4cf5eb27bfb06d) **MaxSa** field.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Address Family | | | | | | | | | | | | | | | | Port Number | | | | | | | | | | | | | | | |
| IPv4 Address | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IPv6 Address (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Padding | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Address Family (2 bytes):** This MUST be set to 0x0002 if this is an IPv4 address or 0x0017 if this is an IPv6 address.

0x0002

0x0017

**Port Number (2 bytes):** Senders MUST set this to zero, and receivers MUST ignore it.

**IPv4 Address (4 bytes):** An IPv4 address in network byte order value for the host pointed to by DNS\_ADDR structure.

**IPv6 Address (16 bytes):** An IPv6 address in network byte order value for the host pointed to by DNS\_ADDR structure.

**Padding (8 bytes):** Senders MUST set this to zero, and receivers MUST ignore it.

###### DNS ADD USER

Used by [DNS\_ADDR](#Section_835c236a4d354a1ebc4cf5eb27bfb06d) **DnsAddrUserDword** field.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| SockaddrLength | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SubnetLength | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Flags | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Padding (20 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**SockaddrLength (4 bytes):** The length of valid data in the socket address structure present above this field.

**SubnetLength (4 bytes):** Senders MUST set this to 0x00000000 and receivers MUST ignore this value.

**Flags (4 bytes):** Clients MUST set to 0x00000000. Senders will use this field to indicate the results of IP validation for this IP address, where it has a format as follows (in host byte order):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| T | Zero | | | | | | | RTT | | | | | | | | | | | | validationStatus | | | | | | | | | | | |

**T (1 bit):** If set, DNS over UDP is available from the remote DNS server but DNS over TCP is not available.

**Zero (7 bits):** Reserved. Senders MUST set these bits to zero and receivers MUST ignore them.

**RTT (12 bits):** Round trip time to the remote DNS server for a UDP query, measured in units of 10 milliseconds.

**validationStatus (12 bits):** The result of the DNS UDP validation attempt. This field MUST be set to one of the DNS\_IP\_VALIDATE\_RETURN\_FLAGS (section [2.2.3.1.2](#Section_f9f3901a862f4bdba7c4963dae44c13e)).

**Padding (20 bytes):** This can be any value and MUST be ignored.

##### DNS\_ADDR\_ARRAY

The DNS\_ADDR\_ARRAY structure is used to represent an array of DNS\_ADDR (section [2.2.3.2.2](#Section_835c236a4d354a1ebc4cf5eb27bfb06d)) structures. The DNS Server Management Protocol uses this structure to exchange lists of mixed IPv4 and IPv6 addresses between client and server.

1. typedef struct \_DnsAddrArray {
2. DWORD MaxCount;
3. DWORD AddrCount;
4. DWORD Tag;
5. WORD Family;
6. WORD WordReserved;
7. DWORD Flags;
8. DWORD MatchFlag;
9. DWORD Reserved1;
10. DWORD Reserved2;
11. [size\_is(AddrCount )] DNS\_ADDR AddrArray[];
12. } DNS\_ADDR\_ARRAY,
13. \*PDNS\_ADDR\_ARRAY;

**MaxCount:**  The actual number of IP addresses that are present in the AddrArray member.

**AddrCount:**  Must be set to the same value as MaxCount.

**Tag:**  This field is unused. Senders MUST set the value to zero and receivers MUST ignore it.

**Family:**  The family of addresses present in the array, such as AF\_INET or AF\_INET6. If this field is not specified, then addresses with all families may be present.

**WordReserved:**  This field is unused. Senders MUST set the value to zero and receivers MUST ignore it.

**Flags:**  This field is unused. Senders MUST set the value to zero and receivers MUST ignore it.

**MatchFlag:**  This field is unused. Senders MUST set the value to zero and receivers MUST ignore it.

**Reserved1:**  This field is unused. Senders MUST set the value to zero and receivers MUST ignore it.

**Reserved2:**  This field is unused. Senders MUST set the value to zero and receivers MUST ignore it.

**AddrArray:**  An array of DNS\_ADDR (section 2.2.3.2.2) structures. The number of elements in this array is specified by the AddrCount member.

An empty DNS\_ADDR\_ARRAY is represented by **AddrCount** set to zero. Senders of an empty DNS\_ADR\_ARRAY MUST set the other fields' values to zero (including a single entry in **AddrArray**, which is set to binary zeros), and receivers MUST ignore them.

##### DNS\_RPC\_IP\_VALIDATE

The DNS\_RPC\_IP\_VALIDATE structure is used to request that the DNS server validate a number of IP addresses. This can be used by clients to determine if an IP address is suitable for use as a DNS server in the context specified by the dwContext member (see below). This structure is to request IP validation while processing the [R\_DnssrvComplexOperation2 (section 3.1.4.8)](#Section_d28e3ba85742417dad6d2e0139ab2ad9) method call with operation type IpValidate.

1. typedef struct \_DnsRpcIPValidate {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. DWORD dwContext;
5. DWORD dwReserved1;
6. [string] char\* pszContextName;
7. PDNS\_ADDR\_ARRAY aipValidateAddrs;
8. } DNS\_RPC\_IP\_VALIDATE,
9. \*PDNS\_RPC\_IP\_VALIDATE;

**dwRpcStructureVersion:**  The DNS management structure version number. This value MUST be set to 0x00000001.

**dwReserved0:**  This field is unused. The client MUST set this value to zero and the server MUST ignore it.

**dwContext:**  The context or purpose for which addresses present in aipValidateAddrs MUST be validated by the DNS server. This field MUST be set to one of the following values:

| Value | Meaning |
| --- | --- |
| DNS\_IPVAL\_DNS\_SERVERS  0x00000000 | Validate that IP addresses are reachable and operational by the DNS servers. |
| DNS\_IPVAL\_DNS\_ROOTHINTS  0x00000001 | Validate that IP addresses are suitable as [**root hints**](#gt_87238b98-87ff-4d10-bc86-06cd6b3bad5c). |
| DNS\_IPVAL\_DNS\_FORWARDERS  0x00000002 | Validate that IP addresses are server level forwarders. |
| DNS\_IPVAL\_DNS\_ZONE\_MASTERS  0x00000003 | Validate that IP addresses are remote DNS servers hosting a zone, named as pointed to by pszContextName. |
| DNS\_IPVAL\_DNS\_DELEGATIONS  0x00000004 | Validate that IP addresses are remote DNS servers are name-server for the delegated zone, named as pointed to by **pszContextName**. |

**dwReserved1:**  This field is unused. The client MUST set this to zero and the server MUST ignore it.

**pszContextName:**  A pointer to a null-terminated ASCII character string that specifies a zone name. The use of this zone name is specified by the dwContext member.

**aipValidateAddrs:**  A pointer to a [DNS\_ADDR\_ARRAY structure (section 2.2.3.2.3)](#Section_56ba5fabf304486699a44f1c1f9247a3) contains a list of IP addresses to be validated by the DNS server.

### Server Messages

#### Enumerations and Constants

##### DNS\_BOOT\_METHODS

The DNS\_BOOT\_METHODS is an 8-bit integer value that specifies the sources of information from which the DNS server obtains information at boot time. Following are possible values for this:

| Constant/value | Description |
| --- | --- |
| BOOT\_METHOD\_UNINITIALIZED  0x00 | Server obtains the boot information, the list of zones to load, and populates its database in the following order, until successful: from a file-based persistent storage, or from the directory server, or from the persistent copy of the DNS Zone Table. [<27>](#Appendix_A_27) |
| BOOT\_METHOD\_FILE  0x01 | Server obtains boot information, the list of zones to load, and populates its database from a file based persistent storage. |
| BOOT\_METHOD\_REGISTRY  0x02 | Server obtains boot information, the list of zones to load, and populates its database from the local persistent copy of the DNS Zone Table. |
| BOOT\_METHOD\_DIRECTORY  0x03 | Server obtains boot information, the list of zones to load, and populates its database from the local persistent copy of the DNS Zone Table for zones located in local persistent storage, and from the directory server for zones persistently stored in the directory server. |

##### DNS\_NAME\_CHECK\_FLAGS

The DNS server enforces different levels of syntax checking for FQDNs. DNS\_NAME\_CHECK\_FLAGS is a DWORD value that specifies the configured level of syntax checking for FQDNs. DNS [[RFC1034]](http://go.microsoft.com/fwlink/?LinkId=90263) and [[RFC2181]](http://go.microsoft.com/fwlink/?LinkId=127732) requires that all FQDNs meet the following basic criteria:

* Total length no longer than 255 characters.
* Each label is less than 63 characters.
* No two consecutive "." characters.

The name check value MUST be set to one of the following allowed values to modify basic FQDN validity checking:

| Constant/value | Description |
| --- | --- |
| DNS\_ALLOW\_RFC\_NAMES\_ONLY  0x00000000 | The DNS server accepts FQDNs that only contain the ASCII characters "a-z", "A-Z", and "0-9". Names that begin with "." or contain two consecutive "." characters are rejected. The name can contain zero or one "\*", but this character MUST appear as the first character in the name if it is present. |
| DNS\_ALLOW\_NONRFC\_NAMES  0x00000001 | The DNS server accepts any printable ASCII character in an FQDN. |
| DNS\_ALLOW\_MULTIBYTE\_NAMES  0x00000002 | The DNS server accepts all characters specified above and also UTF-8 [[RFC3629]](http://go.microsoft.com/fwlink/?LinkId=90439) characters in FQDNs. |
| DNS\_ALLOW\_ALL\_NAMES  0x00000003 | The DNS server does not restrict the set of characters that may appear in FQDNs. |

#### Structures

##### DNSSRV\_VERSION

The DNSSRV\_VERSION is used to store detailed version information of the operating system running on the DNS server. This structure is used by the DNS server to populate the **dwVersion** field in the DNS\_RPC\_SERVER\_INFO structure (section [2.2.4.2.2](#Section_ac444baf4bf94f36912e3041d4c46361)).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Service Pack Version | | | | | | | | | | | | | | | | OS Minor Version | | | | | | | | OS Major Version | | | | | | | |

**Service Pack Version (2 bytes):** The implementation-specific revision number of the DNS server's operating system. [<28>](#Appendix_A_28)

**OS Minor Version (1 byte):** The minor OS version number for the DNS server.

**OS Major Version (1 byte):** The major OS version number for the DNS server.

##### DNS\_RPC\_SERVER\_INFO

The DNS\_RPC\_SERVER\_INFO structure contains information about the DNS server's configuration and state. There are different versions of the DNS\_RPC\_SERVER\_INFO structure. The DNS server MUST use one of the structures corresponding to the value of the **dwClientVersion** field in DNS Server Management Protocol method calls (section [3.1.4](#Section_bdffbbf3e31b49ba8b8d8abde125a9d8)) as shown in the following table. If the method call does not specify the value of **dwClientVersion**, the DNS\_RPC\_SERVER\_INFO\_W2K version of the structure MUST be used.

| Value | Structure |
| --- | --- |
| 0x00000000 | DNS\_RPC\_SERVER\_INFO\_W2K (section [2.2.4.2.2.1](#Section_130bd2ca07644ea6996553ca15dd6ed2)) |
| 0x00060000 | DNS\_RPC\_SERVER\_INFO\_DOTNET (section [2.2.4.2.2.2](#Section_84f3331d499d49fe9f61ab4c5dde6377)) |
| 0x00070000 | DNS\_RPC\_SERVER\_INFO\_LONGHORN (section [2.2.4.2.2.3](#Section_12233dd4dd644b1c95fd6a566e529ac9)) |

###### DNS\_RPC\_SERVER\_INFO\_W2K

1. typedef struct \_DnsRpcServerInfoW2K {
2. DWORD dwVersion;
3. UCHAR fBootMethod;
4. BOOLEAN fAdminConfigured;
5. BOOLEAN fAllowUpdate;
6. BOOLEAN fDsAvailable;
7. [string] char\* pszServerName;
8. [string] wchar\_t\* pszDsContainer;
9. PIP4\_ARRAY aipServerAddrs;
10. PIP4\_ARRAY aipListenAddrs;
11. PIP4\_ARRAY aipForwarders;
12. PDWORD pExtension1;
13. PDWORD pExtension2;
14. PDWORD pExtension3;
15. PDWORD pExtension4;
16. PDWORD pExtension5;
17. DWORD dwLogLevel;
18. DWORD dwDebugLevel;
19. DWORD dwForwardTimeout;
20. DWORD dwRpcProtocol;
21. DWORD dwNameCheckFlag;
22. DWORD cAddressAnswerLimit;
23. DWORD dwRecursionRetry;
24. DWORD dwRecursionTimeout;
25. DWORD dwMaxCacheTtl;
26. DWORD dwDsPollingInterval;
27. DWORD dwScavengingInterval;
28. DWORD dwDefaultRefreshInterval;
29. DWORD dwDefaultNoRefreshInterval;
30. DWORD dwReserveArray[10];
31. BOOLEAN fAutoReverseZones;
32. BOOLEAN fAutoCacheUpdate;
33. BOOLEAN fRecurseAfterForwarding;
34. BOOLEAN fForwardDelegations;
35. BOOLEAN fNoRecursion;
36. BOOLEAN fSecureResponses;
37. BOOLEAN fRoundRobin;
38. BOOLEAN fLocalNetPriority;
39. BOOLEAN fBindSecondaries;
40. BOOLEAN fWriteAuthorityNs;
41. BOOLEAN fStrictFileParsing;
42. BOOLEAN fLooseWildcarding;
43. BOOLEAN fDefaultAgingState;
44. BOOLEAN fReserveArray[15];
45. } DNS\_RPC\_SERVER\_INFO\_W2K,
46. \*PDNS\_RPC\_SERVER\_INFO\_W2K;

**dwVersion:**  The operating system version of the DNS server in DNSSRV\_VERSION (section [2.2.4.2.1](#Section_abf93ed679384564b21486762a1c4dea)).

**fBootMethod:**  The method by which the DNS server obtains information at the start time. This MUST be set to one of the possible values as specified in DNS\_BOOT\_METHODS (section [2.2.4.1.1](#Section_dc737abd3e844814a62a9398c770f28f)).

**fAdminConfigured:**  A Boolean field that specifies whether the DNS server has been configured by an administrator. On a fresh installed server this value MUST be set to FALSE. This value MUST be set to TRUE whenever a zone is created, or a record is modified, or an [**Active Directory domain controller promotion (DCPROMO)**](#gt_25515bcc-3293-4709-b3c4-cfd1a0b4e70f) configures the DNS server.

**fAllowUpdate:**  A Boolean field that indicates whether the DNS server allows dynamic DNS updates. This field MUST be set to FALSE if the server does not allow dynamic zone-updates, otherwise set to TRUE.

**fDsAvailable:**  A Boolean field that specifies whether a directory server is available to the DNS server. It MUST be set to FALSE, if the server does not have access to a directory server.

**pszServerName:**  A pointer to a null-terminated UTF-8 string that contains the FQDN of the DNS server.

**pszDsContainer:**  A pointer to a null-terminated Unicode string that points to the DNS server's container path as a [**distinguished name (DN)**](#gt_1175dd11-9368-41d5-98ed-d585f268ad4b) in the directory server. If no directory server is configured, this value MUST be set to NULL. This value is synthesized by the server by concatenating a constant container [**relative distinguished name (RDN)**](#gt_22198321-b40b-4c24-b8a2-29e44d9d92b9) and the result of an LDAP search operation to retrieve the "defaultNamingContext" of the [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) server's rootDSE.[<29>](#Appendix_A_29)

**aipServerAddrs:**  The list of IP addresses that are available on the server.

**aipListenAddrs:**  The list of IP addresses that are explicitly configured by the administrator on the DNS server that listens for the DNS requests. If this value is set to NULL then the server listens to all available IP addresses.

**aipForwarders:**  The list of remote DNS servers to which this DNS server will forward unresolved DNS requests.

**pExtension1:**  Reserved for future use and MUST be ignored by receiver.

**pExtension2:**  Reserved for future use and MUST be ignored by receiver.

**pExtension3:**  Reserved for future use and MUST be ignored by receiver.

**pExtension4:**  Reserved for future use and MUST be ignored by receiver.

**pExtension5:**  Reserved for future use and MUST be ignored by receiver.

**dwLogLevel:**  This indicates which DNS packets will be logged and how they will be logged. This field MUST be set to either zero or a combination (by bitwise OR) of the possible values as specified under DNS\_LOG\_LEVELS (section [2.2.9.1.1](#Section_fc6275bab4d34e81941703d004369075)). If this value is set to zero, then no logging will be performed for DNS packets.

**dwDebugLevel:**  Unused. Receivers MUST ignore.

**dwForwardTimeout:**  The time interval, in seconds, for which the DNS server waits for a response from each server in the forwarders list.

**dwRpcProtocol:**  This value indicates what RPC protocols this DNS server will accept connections on. This value MUST be set to any combination of values specified in DNS\_RPC\_PROTOCOLS (section [2.2.1.1.2](#Section_cbae04989a604455977845476f7331f5)).

**dwNameCheckFlag:**  The level of domain name checking and validation enforced by the DNS server. This value MUST be set one of the allowed values that are specified in DNS\_NAME\_CHECK\_FLAGS (section [2.2.4.1.2](#Section_914badedbfe04e249150197b7ea2ba5d)).

**cAddressAnswerLimit:**  The configured value for the maximum number of type A IP address resource records that the DNS server can insert in the answer section of a response to a UDP query of type A. If this value is set to 0x00000000 then the DNS server MUST NOT enforce any artificial limit on number of records in a response and if response becomes larger than the DNS UDP packet size then the truncation bit MUST be set [[RFC1035]](http://go.microsoft.com/fwlink/?LinkId=90264). If this property value is not 0x00000000 and the DNS server is unable to add the specified number of records to the response message due to message size limitations, it MUST return as many records as will fit in the message and the truncation bit MUST NOT be set. The DNS server MUST NOT enforce this limit if the query is not of type A. If the value of this property is not 0x00000000 the DNS server MUST enforce this limit for UDP queries and MUST NOT enforce this limit for TCP queries. If the **LocalNetPriority** property value is set to TRUE, the DNS server first orders the address records as per the **LocalNetPriority** property and then MUST select the first **cAddressAnswerLimit** type A records in this sorted list for inclusion in the response. The value MUST be either zero or between 0x00000005 and 0x0000001C inclusive.

**dwRecursionRetry:**  The time-interval, in seconds, for which the DNS server waits before it retries a recursive query to the remote DNS server from which it did not receive a response. The values MUST be between 1 and 15 seconds inclusive.

**dwRecursionTimeout:**  The time-interval, in seconds, for which the DNS server waits for a recursive query-response from a remote DNS server. The values MUST be between 1 and 15 seconds inclusive.

**dwMaxCacheTtl:**  The maximum time duration, in seconds, for which the DNS server will cache a resource record obtained from a remote server in a successful query response. The values for this MUST be between 0 to 30 days (but specified in seconds) inclusive.

**dwDsPollingInterval:**  The interval, in seconds, at which the DNS server will poll a directory server to obtain updated information for any changes that may have occurred to zones loaded in the server. The values MUST be between 30 and 3600 seconds inclusive.

**dwScavengingInterval:**  The [**scavenging**](#gt_345c3de7-adfa-4386-9ba5-f5f572af489c) interval, in hours, on the DNS server. This is the interval at which the server will execute the cleanup of stale DNS records. The value MUST be between 0 and 8760 hours (1 year). If this value is zero then scavenging is disabled.

**dwDefaultRefreshInterval:**  The default value of the [**refresh interval**](#gt_ca2f2a4a-91f1-4547-809e-00bd8e41211c), in hours, for new zones created on the DNS server. For any [**primary zone**](#gt_7205eedf-f027-4da5-8f65-18966a86a17a) created on the server by default this value is used as the refresh interval.

**dwDefaultNoRefreshInterval:**  The default value of the [**NoRefresh interval**](#gt_d826a56a-099e-41a2-8055-df5e0d2c51c6), in hours, for new zones created on the DNS server. For any primary zone created on the server by default this value is used as the NoRefresh interval.

**dwReserveArray:**  This value is reserved for future use and MUST be ignored by the receiver. Senders MUST set this to zero and receivers MUST ignore it.

**fAutoReverseZones:**  A Boolean value that indicates whether the DNS server is configured to automatically create standard reverse lookup zones at boot time.

**fAutoCacheUpdate:**  A Boolean value that indicates whether the DNS server is configured to automatically write-back cached root hints and delegation data to persistent storage.

**fRecurseAfterForwarding:**  A Boolean value that indicates whether the DNS server is configured to use recursion in addition to forwarding. If this value is TRUE (0x01) then if the DNS server does not have any forwarders configured or if fowarders are unreachable then it MUST return failure, otherwise it MUST perform normal recursive processing for this query as specified in section 4.3.1 [[RFC1034]](http://go.microsoft.com/fwlink/?LinkId=90263).

**fForwardDelegations:**  A Boolean value indicates whether or not the DNS server will forward queries about delegated subzones to servers outside of its authoritative zone. If this value is set to TRUE, then the DNS server forwards all name queries about delegated subzones to forwarding servers in other zones; otherwise it will send such queries within its authoritative zone to the corresponding subzone only.

**fNoRecursion:**  A Boolean value that indicates whether the DNS server will perform recursive resolution for queries. If this value is TRUE then recursion MUST NOT be performed even if the Recursion Desired (RD) bit (section 4.1.1 of [RFC1035]) is set in the DNS query packet header. If this value is FALSE then recursion will be performed as per [RFC1035].

**fSecureResponses:**  A Boolean value that indicates if the DNS server needs to screen DNS records received in remote query responses against the zone of authority for the remote server to prevent cache pollution. If it is set to TRUE, the DNS server caches only the records that are in zone of authority for the remote server that was queried. When set to FALSE, all records in the cache are saved.

**fRoundRobin:**  A Boolean value that indicates if the DNS server is configured to rotate the order of DNS records it returns for a given name. If this value is set to FALSE no round robin will be performed and DNS records will be returned in static, arbitrary order.

**fLocalNetPriority:**  A Boolean value that indicates if the DNS server is configured to prioritize address records in a response based on the IP address of the DNS client that submitted the query. If this is set to TRUE the DNS server will return address records in the order of their closeness to the querying client's IP address by applying the [**network mask**](#gt_44652747-fc40-48ea-a0d6-7650b6e4a3aa) pointed to by LocalNetPriorityNetMask. If this value is set to 0 then the DNS server returns records in the order in which they are obtained from the database.

**fBindSecondaries:**  A Boolean value that indicates if the DNS server allows [**zone transfers**](#gt_67ea3c5b-6b1e-40a3-ac20-3f7eaf056504) to secondary DNS servers running older non-Microsoft software. If this value is set to TRUE the DNS server sends zone transfer to secondaries via a slower mechanism, with one resource record in each message.

**fWriteAuthorityNs:**  A Boolean value that indicates if the DNS server is enabled to write NS records in the authority section of all successful authoritative responses. If this value is TRUE then NS records will be included in the authority section of responses, otherwise NS records will only be included in referral responses.

**fStrictFileParsing:**  A Boolean value that indicates if the DNS server is configured to perform strict file parsing. When this value is set to TRUE and a record parsing error is detected server will quit after indicating error. If this value is FALSE parsing errors will cause that specific record to be ignored and the server will continue to load the rest of the database.

**fLooseWildcarding:**  A Boolean value that indicates if the DNS server is configured to perform loose wildcarding [RFC1035], otherwise it returns FALSE. When a server does not find a resource record that matches the name and type specified in the query in the authoritative zone, then it searches for related wildcard records, (section 4.3.3 [RFC1034]), if configured to perform loose wildcarding will return the first node it finds that has matching resource-record type, whereas if it is not then it will return the first node that has any resource record.

**fDefaultAgingState:**  A Boolean value that indicates if the default value of ageing state for new primary zones created on the DNS server. For any primary zone created on the server this value is used as its default aging state. If this is FALSE then timestamps of records in the zone will not be tracked whereas when this value is TRUE then the timestamps of records in the zone will be tracked.

**fReserveArray:**  Reserved for future use. These values MUST be ignored by receiver.

###### DNS\_RPC\_SERVER\_INFO\_DOTNET

All fields have same definition as specified in DNS\_RPC\_SERVER\_INFO\_W2K (section [2.2.4.2.2.1](#Section_130bd2ca07644ea6996553ca15dd6ed2)), with the following exceptions:[<30>](#Appendix_A_30)

1. typedef struct \_DnsRpcServerInfoDotNet {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. DWORD dwVersion;
5. UCHAR fBootMethod;
6. BOOLEAN fAdminConfigured;
7. BOOLEAN fAllowUpdate;
8. BOOLEAN fDsAvailable;
9. [string] char\* pszServerName;
10. [string] wchar\_t\* pszDsContainer;
11. PIP4\_ARRAY aipServerAddrs;
12. PIP4\_ARRAY aipListenAddrs;
13. PIP4\_ARRAY aipForwarders;
14. PIP4\_ARRAY aipLogFilter;
15. [string] wchar\_t\* pwszLogFilePath;
16. [string] char\* pszDomainName;
17. [string] char\* pszForestName;
18. [string] char\* pszDomainDirectoryPartition;
19. [string] char\* pszForestDirectoryPartition;
20. [string] char\* pExtensions[6];
21. DWORD dwLogLevel;
22. DWORD dwDebugLevel;
23. DWORD dwForwardTimeout;
24. DWORD dwRpcProtocol;
25. DWORD dwNameCheckFlag;
26. DWORD cAddressAnswerLimit;
27. DWORD dwRecursionRetry;
28. DWORD dwRecursionTimeout;
29. DWORD dwMaxCacheTtl;
30. DWORD dwDsPollingInterval;
31. DWORD dwLocalNetPriorityNetMask;
32. DWORD dwScavengingInterval;
33. DWORD dwDefaultRefreshInterval;
34. DWORD dwDefaultNoRefreshInterval;
35. DWORD dwLastScavengeTime;
36. DWORD dwEventLogLevel;
37. DWORD dwLogFileMaxSize;
38. DWORD dwDsForestVersion;
39. DWORD dwDsDomainVersion;
40. DWORD dwDsDsaVersion;
41. DWORD dwReserveArray[4];
42. BOOLEAN fAutoReverseZones;
43. BOOLEAN fAutoCacheUpdate;
44. BOOLEAN fRecurseAfterForwarding;
45. BOOLEAN fForwardDelegations;
46. BOOLEAN fNoRecursion;
47. BOOLEAN fSecureResponses;
48. BOOLEAN fRoundRobin;
49. BOOLEAN fLocalNetPriority;
50. BOOLEAN fBindSecondaries;
51. BOOLEAN fWriteAuthorityNs;
52. BOOLEAN fStrictFileParsing;
53. BOOLEAN fLooseWildcarding;
54. BOOLEAN fDefaultAgingState;
55. BOOLEAN fReserveArray[15];
56. } DNS\_RPC\_SERVER\_INFO\_DOTNET,
57. \*PDNS\_RPC\_SERVER\_INFO\_DOTNET;

**dwRpcStructureVersion:**  The DNS management structure version number. The following are possible values:

| Value | Meaning |
| --- | --- |
| 0x00000001 | Structure is of type DNS\_SERVER\_INFO\_DOTNET. |
| 0x00000002 | Structure is of type DNS\_SERVER\_INFO\_LONGHORN. |

**dwReserved0:**  This field is reserved for future use. Senders MUST set this to zero and it MUST be ignored by receiver.

**aipLogFilter:**  The list of IP addresses used for debug log filtering. The DNS server will log DNS traffic that is sent to or received from for these IP addresses and will not log DNS traffic to or from other IP addresses. If this value is set to NULL then the DNS server will not perform IP filtering when logging DNS traffic.

**pwszLogFilePath:**   A pointer to a null-terminated Unicode string that contains an absolute pathname or relative pathname or filename for the operational log file on the DNS server. If this value is set to NULL, the log SHOULD be logged to an implementation specific log file.

**pszDomainName:**  A pointer to a null-terminated UTF-8 string that contains the name of the directory server domain to which the DNS server belongs if directory server is available. This value will be NULL if no directory server is available.

**pszForestName:**  A pointer to a null-terminated UTF-8 string that contains the name of the directory server forest to which the DNS server belongs if directory server is available. This value will be NULL if no directory server is available.

**pszDomainDirectoryPartition:**  A pointer to a null-terminated UTF-8 string that contains the base name for the domain wide DNS application directory partition.

**pszForestDirectoryPartition:**   A pointer to a null-terminated UTF-8 string that contains the base name for the forest-wide DNS application directory partition.

**pExtensions:**  Reserved for future use. Senders MUST set this to NULL and it MUST be ignored by the receiver.

**dwLocalNetPriorityNetMask:**  The net mask used by the DNS server to prioritize address records in responses when the server is configured to enforce LocalNetPriority as mentioned above.

**dwLastScavengeTime:**  The timestamp at which the last scavenging cycle was executed on the DNS server. If this value is set to 0 then no scavenging cycle has been run since the server was last started.

**dwEventLogLevel:**  This value indicates what level of events will be logged by the DNS server. This value MUST be set to one of the combination of the possible values for this defined in DNS\_EVENTLOG\_TYPES (section [2.2.9.1.2](#Section_9422eb05ebf54b86ac1be79ebf2e3b37)).

**dwLogFileMaxSize:**   The maximum allowed size, in bytes, for the log file.

**dwDsForestVersion:**   This value indicates the directory server [**forest (2)**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62) version being used by the DNS server, stored in the ForceForestBehaviorVersion property.

**dwDsDomainVersion:**  This value indicates the directory server domain version being used by the [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) server, stored in the ForceDomainBehaviorVersion property.

**dwDsDsaVersion:**   This value indicates the directory server local server version being used by the DNS server, stored in the ForceDsaBehaviorVersion property.

###### DNS\_RPC\_SERVER\_INFO\_LONGHORN

All fields have same definition as specified in section DNS\_RPC\_SERVER\_INFO\_DOTNET (section [2.2.4.2.2.2](#Section_84f3331d499d49fe9f61ab4c5dde6377) ), with the following exceptions:[<31>](#Appendix_A_31)

1. typedef struct \_DnsRpcServerInfoLonghorn {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. DWORD dwVersion;
5. UCHAR fBootMethod;
6. BOOLEAN fAdminConfigured;
7. BOOLEAN fAllowUpdate;
8. BOOLEAN fDsAvailable;
9. [string] char\* pszServerName;
10. [string] wchar\_t\* pszDsContainer;
11. PDNS\_ADDR\_ARRAY aipServerAddrs;
12. PDNS\_ADDR\_ARRAY aipListenAddrs;
13. PDNS\_ADDR\_ARRAY aipForwarders;
14. PDNS\_ADDR\_ARRAY aipLogFilter;
15. [string] wchar\_t\* pwszLogFilePath;
16. [string] char\* pszDomainName;
17. [string] char\* pszForestName;
18. [string] char\* pszDomainDirectoryPartition;
19. [string] char\* pszForestDirectoryPartition;
20. [string] char\* pExtensions[6];
21. DWORD dwLogLevel;
22. DWORD dwDebugLevel;
23. DWORD dwForwardTimeout;
24. DWORD dwRpcProtocol;
25. DWORD dwNameCheckFlag;
26. DWORD cAddressAnswerLimit;
27. DWORD dwRecursionRetry;
28. DWORD dwRecursionTimeout;
29. DWORD dwMaxCacheTtl;
30. DWORD dwDsPollingInterval;
31. DWORD dwLocalNetPriorityNetMask;
32. DWORD dwScavengingInterval;
33. DWORD dwDefaultRefreshInterval;
34. DWORD dwDefaultNoRefreshInterval;
35. DWORD dwLastScavengeTime;
36. DWORD dwEventLogLevel;
37. DWORD dwLogFileMaxSize;
38. DWORD dwDsForestVersion;
39. DWORD dwDsDomainVersion;
40. DWORD dwDsDsaVersion;
41. BOOLEAN fReadOnlyDC;
42. DWORD dwReserveArray[3];
43. BOOLEAN fAutoReverseZones;
44. BOOLEAN fAutoCacheUpdate;
45. BOOLEAN fRecurseAfterForwarding;
46. BOOLEAN fForwardDelegations;
47. BOOLEAN fNoRecursion;
48. BOOLEAN fSecureResponses;
49. BOOLEAN fRoundRobin;
50. BOOLEAN fLocalNetPriority;
51. BOOLEAN fBindSecondaries;
52. BOOLEAN fWriteAuthorityNs;
53. BOOLEAN fStrictFileParsing;
54. BOOLEAN fLooseWildcarding;
55. BOOLEAN fDefaultAgingState;
56. BOOLEAN fReserveArray[15];
57. } DNS\_RPC\_SERVER\_INFO\_LONGHORN,
58. \*PDNS\_RPC\_SERVER\_INFO\_LONGHORN,
59. DNS\_RPC\_SERVER\_INFO,
60. \*PDNS\_RPC\_SERVER\_INFO;

**fReadOnlyDC:**   A **Boolean** value that indicates whether the DNS server has access to a directory server that is running in read-only mode, that is, whether the server does not accept directory server write operations. The DNS server detects whether this is the case by reading the **supportedCapabilities** attribute of the server's "rootDse" object, looking for LDAP\_CAP\_ACTIVE\_DIRECTORY\_PARTIAL\_SECRETS\_OID. (See [[MS-ADTS]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ADTS%5d.pdf), section 3.1.1.3.2.10.)

### Zone Messages

#### Enumerations and Constants

##### DNS\_ZONE\_TYPE

DNS\_ZONE\_TYPE is an 8-bit integer value that specifies the type of a zone. An implementation SHOULD[<32>](#Appendix_A_32) support following values.

| Constant/value | Description |
| --- | --- |
| DNS\_ZONE\_TYPE\_CACHE  0x00 | This zone is used to store all cached DNS records received from remote DNS servers during normal query processing. |
| DNS\_ZONE\_TYPE\_PRIMARY  0x01 | The DNS server is a primary DNS server for this zone. |
| DNS\_ZONE\_TYPE\_SECONDARY  0x02 | The DNS server is acting as a secondary DNS server for this zone. |
| DNS\_ZONE\_TYPE\_STUB  0x03 | Zone is a [**stub zone**](#gt_55a705e5-1ca3-4001-8d6d-c5ae08fdcdeb), that is, it contains only those resource records that are necessary to identify authoritative DNS servers for that zone. |
| DNS\_ZONE\_TYPE\_FORWARDER  0x04 | The DNS server is a forwarder for this zone, that is, the server does not have authoritative information for resource records in this zone. |
| DNS\_ZONE\_TYPE\_SECONDARY\_CACHE  0x05 | This zone is used to hold cached records for some implementation specific purpose. |

##### DNS\_ZONE\_SECONDARY\_SECURITY

DNS\_ZONE\_SECONDARY\_SECURITY is a 32-bit integer value that enumerates the types of security settings that are enforced by the master DNS server to honor zone transfer requests for this zone.

| Constant/value | Description |
| --- | --- |
| ZONE\_SECSECURE\_NO\_SECURITY  0x00000000 | No security enforcement for secondaries, that is, any zone transfer request will be honored. |
| ZONE\_SECSECURE\_NS\_ONLY  0x00000001 | Zone transfer request will be honored from the remote servers, which are in the list of name servers for this zone. |
| ZONE\_SECSECURE\_LIST\_ONLY  0x00000002 | Zone transfer request will be honored from the remote servers, which are explicitly configured by IP addresses in the **aipSecondaries** field in the DNS\_RPC\_ZONE\_INFO structure (section [2.2.5.2.4](#Section_5e6b44a913c44c3aa7a2b5576016c3cf)). |
| ZONE\_SECSECURE\_NO\_XFER  0x00000003 | No zone transfer requests will be honored. |

##### DNS\_ZONE\_NOTIFY\_LEVEL

DNS\_ZONE\_NOTIFY\_LEVEL is a DWORD value that enumerates the levels of notification settings that can be configured on a master DNS server to send out notifications to secondaries about any changes to this zone, so that they can initiate a zone transfer to get updated zone information.

| Constant/value | Description |
| --- | --- |
| ZONE\_NOTIFY\_OFF  0x00000000 | The Master DNS server does not send any zone notifications. |
| ZONE\_NOTIFY\_ALL\_SECONDARIES  0x00000001 | The Master DNS server sends zone notifications to all secondary servers for this zone, either they are listed as name-servers for this zone or they are present explicitly in the zone notify list for this zone. (DNS notify [[RFC1996]](http://go.microsoft.com/fwlink/?LinkId=106957) is a mechanism in which the primary DNS server for a zone notifies secondary servers about any changes in the zone.) |
| ZONE\_NOTIFY\_LIST\_ONLY  0x00000002 | The Master DNS server sends zone notifications only to those remote servers which are explicitly configured by IP addresses in the **aipNotify** field in the DNS\_RPC\_ZONE\_INFO structure (section [2.2.5.2.4](#Section_5e6b44a913c44c3aa7a2b5576016c3cf)). |

##### ZONE\_REQUEST\_FILTERS

ZONE\_REQUEST\_FILTERS is a 32-bit integer value that specifies possible selection filter types for zone selection. An implementation SHOULD[<33>](#Appendix_A_33) support all values.

| Constant/value | Description |
| --- | --- |
| ZONE\_REQUEST\_PRIMARY  0x00000001 | Consider primary zones. |
| ZONE\_REQUEST\_SECONDARY  0x00000002 | Consider [**secondary zones**](#gt_718c47c0-e274-4946-a0e7-f31aa03a1bc1). |
| ZONE\_REQUEST\_CACHE  0x00000004 | Consider cache zones. |
| ZONE\_REQUEST\_AUTO  0x00000008 | Consider the [**autocreated zones**](#gt_439a7fee-e146-458f-9869-ce2f8983bd0b). These are zones with the AutoCreated flag (section [2.2.5.2.2](#Section_015f97afba5048bbaf444a542f3ff44a)) turned on. |
| ZONE\_REQUEST\_FORWARD  0x00000010 | Consider zones whose names do not end with the "arpa" label. |
| ZONE\_REQUEST\_REVERSE  0x00000020 | Consider zones whose names end with the "arpa" label. |
| ZONE\_REQUEST\_FORWARDER  0x00000040 | Consider forwarder zones. |
| ZONE\_REQUEST\_STUB  0x00000080 | Consider stub zones. |
| ZONE\_REQUEST\_DS  0x00000100 | Consider zones that are directory server integrated. |
| ZONE\_REQUEST\_NON\_DS  0x00000200 | Consider zones that are not directory server integrated (that is, zones that are either persistently stored in local storage or are zones of type DNS\_ZONE\_TYPE\_CACHE or DNS\_ZONE\_TYPE\_SECONDARY\_CACHE (section [2.2.5.1.1](#Section_27e138a7110c44a4afcbb95f35f00306))). |
| ZONE\_REQUEST\_DOMAIN\_DP  0x00000400 | Consider zones that are stored in the domain application directory partition. |
| ZONE\_REQUEST\_FOREST\_DP  0x00000800 | Consider zones that are stored in the forest application directory partition. |
| ZONE\_REQUEST\_CUSTOM\_DP  0x00001000 | Consider zones that are stored in a custom application directory partition, where the application directory partition name is specified by **pszPartitionFqdn** in the DNS\_RPC\_ENUM\_ZONES\_FILTER (section [2.2.5.2.9](#Section_b2c763771c5042f483c6b514a1a7e65e)) structure. |
| ZONE\_REQUEST\_LEGACY\_DP  0x00002000 | Consider zones that are stored in the default application directory partition. |

##### ZONE\_SKD\_ROLLOVER\_TYPE

ZONE\_SKD\_ROLLOVER\_TYPE is a 32-bit integer value that specifies possible [**key rollover**](#gt_bba25ad2-df77-44a6-80ce-527528948f8e) types for a signing key descriptor. An implementation SHOULD[<34>](#Appendix_A_34) support all values.

| Constant/value | Description |
| --- | --- |
| DNS\_ROLLOVER\_TYPE\_PREPUBLISH  0x00000000 | A method of key rollover in which the new key is published in the zone before it will be used. See [[RFC4641]](http://go.microsoft.com/fwlink/?LinkId=225979) section 4.2. |
| DNS\_ROLLOVER\_TYPE\_DOUBLE\_SIGNATURE  0x00000001 | A method of key rollover in which data is signed by both old and new keys simultaneously for a period of time. See [RFC4641] section 4.2. |

##### ZONE\_SKD\_ROLLOVER\_ACTION

ZONE\_SKD\_ROLLOVER\_ACTION is a 32-bit integer value that specifies possible key rollover actions for a signing key descriptor. An implementation SHOULD[<35>](#Appendix_A_35) support all values.

| Constant/value | Description |
| --- | --- |
| DNS\_ROLLOVER\_ACTION\_DEFAULT  0x00000000 | The server MUST never send this value. The client MUST send this value to indicate that no change to the current key rollover behavior is desired. |
| DNS\_ROLLOVER\_ACTION\_NORMAL  0x00000001 | The server will perform a normal key rollover the next time the keys for this signing key descriptor are rolled over. |
| DNS\_ROLLOVER\_ACTION\_REVOKE\_STANDBY  0x00000002 | The server will revoke the standby key for this signing key descriptor as defined by [[RFC5011]](http://go.microsoft.com/fwlink/?LinkId=225980) the next time the keys for this signing key descriptor are rolled over. This rollover action applies only to signing key descriptors representing [**key signing keys**](#gt_33a6e1a7-8ac7-4d38-b25a-75b2ccae8311) (those whose "fIsKSK" property as described in section [2.2.6.2.1](#Section_f7b0ad424cae40fd87c882af83824639) is set to 0x00000001). |
| DNS\_ROLLOVER\_ACTION\_RETIRE  0x00000003 | The server will retire this signing key descriptor and remove all signatures associated with it the next time the keys for this signing key descriptor are rolled over. |

#### Structures

##### DNS\_RPC\_ZONE

The DNS\_RPC\_ZONE structure contains basic information about a zone present on the DNS server. There are different versions of the DNS\_RPC\_ZONE structure. The DNS server MAY[<36>](#Appendix_A_36) decide to use one of these structures depending upon the value of the **dwClientVersion** field in DNS Server Management Protocol method calls (section [3.1.4](#Section_bdffbbf3e31b49ba8b8d8abde125a9d8)) as follows in the table provided. If the method call does not specify the value of **dwClientVersion**, the DNS\_RPC\_ZONE\_W2K version of the structure MUST be used.

| Value | Structure |
| --- | --- |
| 0x00000000 | DNS\_RPC\_ZONE\_W2K (section [2.2.5.2.1.1](#Section_6b6e834ae08e432ca9a78ced1422a688)) |
| 0x00060000 or 0x00070000 | DNS\_RPC\_ZONE\_DOTNET (section [2.2.5.2.1.2](#Section_64c5005d2a5546cc8453af393bb27bb9)) |

###### DNS\_RPC\_ZONE\_W2K

1. typedef struct \_DnssrvRpcZoneW2K {
2. [string] wchar\_t\* pszZoneName;
3. DNS\_RPC\_ZONE\_FLAGS Flags;
4. UCHAR ZoneType;
5. UCHAR Version;
6. } DNS\_RPC\_ZONE\_W2K,
7. \*PDNS\_RPC\_ZONE\_W2K;

**pszZoneName:**  A pointer to a null-terminated Unicode string that contains zone-name.

**Flags:**  Zone flags as specified in section [2.2.5.2.2](#Section_015f97afba5048bbaf444a542f3ff44a).

**ZoneType:**  The zone type. This MUST be set to one of the allowed DNS\_ZONE\_TYPE section [2.2.5.1.1](#Section_27e138a7110c44a4afcbb95f35f00306).

**Version:**  The RPC protocol version. It MUST be set to 0x32.

###### DNS\_RPC\_ZONE\_DOTNET

All fields have same definition as specified in section DNS\_RPC\_ZONE\_W2K (section [2.2.5.2.1.1](#Section_6b6e834ae08e432ca9a78ced1422a688)), with the following exceptions:

1. typedef struct \_DnssrvRpcZoneDotNet {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. [string] wchar\_t\* pszZoneName;
5. DNS\_RPC\_ZONE\_FLAGS Flags;
6. UCHAR ZoneType;
7. UCHAR Version;
8. DWORD dwDpFlags;
9. [string] char\* pszDpFqdn;
10. } DNS\_RPC\_ZONE\_DOTNET,
11. \*PDNS\_RPC\_ZONE\_DOTNET,
12. DNS\_RPC\_ZONE,
13. \*PDNS\_RPC\_ZONE;

**dwRpcStructureVersion:**  The DNS management structure version number. This value MUST be set to 0x00000001.

**dwReserved0:**  This field is reserved for future use. Senders set this to an arbitrary value and receivers MUST ignore it.

**dwDpFlags:**  Application directory partition flags for this zone. This MUST be set to one of the combination of the DNS\_RPC\_DP\_FLAGS (section [2.2.7.1.1](#Section_27e378aad4d743de8b343e5b957a7130)). If this zone is not stored in the directory server this value MUST be 0x00000000.

**pszDpFqdn:**  A pointer to a null-terminated UTF-8 string that specifies the FQDN of the application directory partition in which this zone is stored in the directory server. If this zone is not stored in the directory server this value MUST be NULL.

If the DNS RPC client sends an older version of DNS\_RPC\_ZONE structure, that is, DNS\_RPC\_ZONE\_W2K (section 2.2.5.2.1.1), then the DNS RPC server MUST construct a current version of DNS\_RPC\_ZONE structure, that is, DNS\_RPC\_ZONE\_DOTNET, using the following steps:

1. Copy the same value for fields that are common to input and the current version of the DNS\_RPC\_ZONE structures.
2. The dwRpcStructureVersion field MUST be set to "1".
3. All other fields that are defined only in DNS\_RPC\_ZONE\_DOTNET and are not defined in DNS\_RPC\_ZONE (section [2.2.5.2.1](#Section_f22773cabfbf46a58042fbda1f3c4ad2)), MUST be set to "0".

##### DNS\_RPC\_ZONE\_FLAGS

DNS\_RPC\_ZONE\_FLAGS is a bit-mask value used by the DNS\_RPC\_ZONE structure (section [2.2.5.2.1](#Section_f22773cabfbf46a58042fbda1f3c4ad2)) to indicate zone properties and state.

This type is declared as follows:

1. typedef DWORD DNS\_RPC\_ZONE\_FLAGS, \*PDNS\_RPC\_ZONE\_FLAGS;

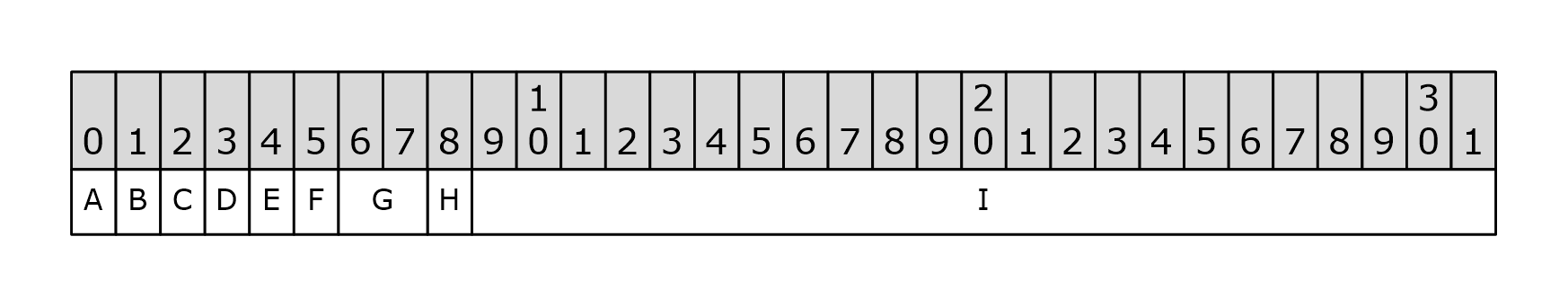


Figure : DNS\_RPC\_ZONE\_FLAGS Bit-Mask

**A (Paused)**: If set to 1, indicates that this zone is currently administratively paused. The DNS server will not use this zone to respond to queries, will not accept updates in this zone, and will suspend all other functions related to this zone. The default value for this flag is 0.

**B (Shutdown)**: If set to 1, indicates that an error occurred that caused the DNS server to be unable to load a complete copy of the zone into memory. For primary zones, the DNS server MUST set this flag to 1 if an error occurred while loading the zone or its records from persistent storage. If the zone is directory server-integrated, the DNS server MUST retry loading the zone at an interval specified by the "DsPollingInterval" property (section [3.1.1.1](#Section_c4833797156c4c48a380d40dd1760eb9)) and set this flag to zero if a subsequent loading attempt succeeds. If the server is not directory server-integrated the DNS server MUST NOT automatically retry loading the zone. For secondary and stub zones, the DNS server MUST set this flag to 1 if zone transfer was refused by all of the master servers or if zone transfer could not be successfully completed. The DNS server MUST retry zone transfer as specified by [[RFC1034]](http://go.microsoft.com/fwlink/?LinkId=90263) and set this flag to zero if a subsequent zone transfer attempt succeeds. The default value of this field MUST be 1 and the value MUST be set to zero if the zone is successfully loaded during initialization (section [3.1.3](#Section_007efcd2295546dda59ef83ae88f4678)).

**C (Reverse)**: If set to 1, indicates that this is a reverse lookup zone.

**D (AutoCreated)**: If set to 1, indicates that zone was auto-created. A DNS server MAY automatically create certain zones at boot time which are flagged as "AutoCreated". Such zones are never written to persistent storage, and the DNS Server MUST NOT perform any DNS Server Management Protocol RPC operations on such zones.[<37>](#Appendix_A_37)

**E (DsIntegrated)**: If set to 1, indicates that zone is stored in a directory server.

**F (Aging)**: If set to 1, indicates that zone has aging enabled for resource records.

**G (Update)**: The type of updates that are supported on this zone. This value MUST be set to one of the possible value from DNS\_ZONE\_UPDATE (section [2.2.6.1.1](#Section_d4b84209f00c478f80d78dd0f1633d9e)).

**H (ReadOnly)**: If set to 1, indicates that this zone is operating in read-only mode. The DNS server SHOULD[<38>](#Appendix_A_38) support read-only zones. If the DNS server supports read-only zones, it MUST set this flag to 1 if the zone is loaded from a directory server that is read-only, and in all other cases it MUST set the flag to 0.

**I (Unused)**: MUST be set to zero when sent and MUST be ignored on receipt.

##### DNS\_RPC\_ZONE\_LIST

The DNS\_RPC\_ZONE\_LIST structure contains the information about a list of zones present on the DNS server. There are different versions of the DNS\_RPC\_ZONE\_LIST structure. The DNS server SHOULD[<39>](#Appendix_A_39) use one of these structures depending upon the passed-in value for the **dwClientVersion** field in DNS Server Management Protocol method calls (section [3.1.4](#Section_bdffbbf3e31b49ba8b8d8abde125a9d8)) as shown in the following table. If the method call does not specify the value of **dwClientVersion**, the DNS\_RPC\_ZONE\_LIST\_W2K version of the structure MUST be used.

| Value | Structure |
| --- | --- |
| 0x00000000 | DNS\_RPC\_ZONE\_LIST\_W2K (section [2.2.5.2.3.1](#Section_f457cf9e14e04195a8fd2c93bc7f1f6d)) |
| 0x00060000 | DNS\_RPC\_ ZONE\_LIST\_DOTNET (section [2.2.5.2.3.2](#Section_24366c193f664ddab3a533a79417661f)) |
| 0x00070000 | DNS\_RPC\_ ZONE\_LIST\_DOTNET (section 2.2.5.2.3.2) |

###### DNS\_RPC\_ZONE\_LIST\_W2K

1. typedef struct \_DnssrvRpcZoneListW2K {
2. [range(0,500000)] DWORD dwZoneCount;
3. [size\_is(dwZoneCount)] PDNS\_RPC\_ZONE\_W2K ZoneArray[];
4. } DNS\_RPC\_ZONE\_LIST\_W2K,
5. \*PDNS\_RPC\_ZONE\_LIST\_W2K;

**dwZoneCount:**  The number of zones present in the array of zones pointed to by ZoneArray.

**ZoneArray:**  An array of structures of type DNS\_RPC\_ZONE (section [2.2.5.2.1.1](#Section_6b6e834ae08e432ca9a78ced1422a688)). Each element of the array represents one zone.

###### DNS\_RPC\_ZONE\_LIST\_DOTNET

All fields have same definition as specified in section DNS\_RPC\_ZONE\_LIST\_W2K (section [2.2.5.2.3.1](#Section_f457cf9e14e04195a8fd2c93bc7f1f6d)), with the following exceptions:

1. typedef struct \_DnssrvRpcZoneListDotNet {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. [range(0,500000)] DWORD dwZoneCount;
5. [size\_is(dwZoneCount)] PDNS\_RPC\_ZONE\_DOTNET ZoneArray[];
6. } DNS\_RPC\_ZONE\_LIST\_DOTNET,
7. \*PDNS\_RPC\_ZONE\_LIST\_DOTNET,
8. DNS\_RPC\_ZONE\_LIST,
9. \*PDNS\_RPC\_ZONE\_LIST;

**dwRpcStructureVersion:**  The DNS management structure version number. This MUST be set to 0x00000001.

**dwReserved0:**  This field is reserved for future use. Senders can send an arbitrary value and receivers MUST ignore it.

If the DNS RPC client sends an older version of DNS\_RPC\_ZONE\_LIST structure, that is, DNS\_RPC\_ZONE\_LIST\_W2K (section 2.2.5.2.3.1), then the DNS RPC server MUST construct a current version of DNS\_RPC\_ZONE\_LIST structure, that is, DNS\_RPC\_ZONE\_LIST\_DOTNET, using the following steps:

1. Copy the same value for the fields that are common to input and the current version of DNS\_RPC\_ZONE\_LIST structures.
2. The dwRpcStructureVersion field MUST be set to "1".
3. The value for the ZoneArray field MUST be obtained from the input structure as DNS\_RPC\_ZONE\_W2K (section [2.2.5.2.1.1](#Section_6b6e834ae08e432ca9a78ced1422a688)) array elements and each MUST be converted using the steps specified in section DNS\_RPC\_ZONE\_DOTNET (section [2.2.5.2.1.2](#Section_64c5005d2a5546cc8453af393bb27bb9)), and then assigned to the ZoneArray field in the DNS\_RPC\_ZONE\_LIST\_DOTNET structure.
4. All other fields that are defined only in DNS\_RPC\_ZONE\_LIST\_DOTNET and are not defined in DNS\_RPC\_ZONE\_LIST\_W2K (section 2.2.5.2.3.1), MUST be set to "0".

##### DNS\_RPC\_ZONE\_INFO

The DNS\_RPC\_ZONE\_INFO structure contains the detailed information about a zone present on the DNS server. The DNS server uses this structure to return information about a zone while responding to R\_DnssrvQuery2 (section [3.1.4.7](#Section_a90a44f0f64e44b09e35a7fc49f6adea)) method calls with operation type "ZoneInfo". There are different versions of DNS\_RPC\_ZONE\_INFO. The DNS server MUST use the structures corresponding to the passed-in value for the **dwClientVersion** field in DNS Server Management Protocol method calls (section [3.1.4](#Section_bdffbbf3e31b49ba8b8d8abde125a9d8)) in the following table, or if the method call does not specify the value of **dwClientVersion**, the DNS\_RPC\_ZONE\_ INFO\_W2K version of the structure MUST be used.

| Value | Structure |
| --- | --- |
| 0x00000000 | DNS\_RPC\_ZONE\_INFO\_W2K (section [2.2.5.2.4.1](#Section_e86515440fbb40388232375ff2d8a55e)) |
| 0x00060000 | DNS\_RPC\_ ZONE\_INFO\_DOTNET (section [2.2.5.2.4.2](#Section_45b100df57c24c8486de00b69d742372)) |
| 0x00070000 | DNS\_RPC\_ ZONE\_INFO\_LONGHORN (section [2.2.5.2.4.3](#Section_23a085bfd81445e3943f8bbdc32a5dae)) |

###### DNS\_RPC\_ZONE\_INFO\_W2K

1. typedef struct \_DnsRpcZoneInfoW2K {
2. [string] char\* pszZoneName;
3. DWORD dwZoneType;
4. DWORD fReverse;
5. DWORD fAllowUpdate;
6. DWORD fPaused;
7. DWORD fShutdown;
8. DWORD fAutoCreated;
9. DWORD fUseDatabase;
10. [string] char\* pszDataFile;
11. PIP4\_ARRAY aipMasters;
12. DWORD fSecureSecondaries;
13. DWORD fNotifyLevel;
14. PIP4\_ARRAY aipSecondaries;
15. PIP4\_ARRAY aipNotify;
16. DWORD fUseWins;
17. DWORD fUseNbstat;
18. DWORD fAging;
19. DWORD dwNoRefreshInterval;
20. DWORD dwRefreshInterval;
21. DWORD dwAvailForScavengeTime;
22. PIP4\_ARRAY aipScavengeServers;
23. DWORD pvReserved1;
24. DWORD pvReserved2;
25. DWORD pvReserved3;
26. DWORD pvReserved4;
27. } DNS\_RPC\_ZONE\_INFO\_W2K,
28. \*PDNS\_RPC\_ZONE\_INFO\_W2K;

**pszZoneName:**  A pointer to a null-terminated Unicode string that contains a zone name.

**dwZoneType:**  The zone type. This MUST be set to one of the allowed values as specified in DNS\_ZONE\_TYPE (section [2.2.5.1.1](#Section_27e138a7110c44a4afcbb95f35f00306)).

**fReverse:**  A Boolean value where TRUE (0x00000001) indicates this is a reverse lookup zone and FALSE (0x00000000) indicates this is a forward lookup zone.

**fAllowUpdate:**  A value that indicates what kind [**dynamic updates**](#gt_dbff570c-a709-479a-980a-5b74ac7ab2e7) are allowed for this zone. This MUST be set to one of the following values:

| Constant/value | Descriptiom |
| --- | --- |
| ZONE\_UPDATE\_OFF 0x00000000 | No updates are allowed for the zone. |
| ZONE\_UPDATE\_UNSECURE0x00000001 | All updates (secure and unsecure) are allowed for the zone. |
| ZONE\_UPDATE\_SECURE0x00000002 | The zone only allows secure updates, that is, DNS packet MUST have a TSIG [[RFC2845]](http://go.microsoft.com/fwlink/?LinkId=90388) present in the additional section. |

**fPaused:**  A Boolean value indicates whether zone operations are currently paused. TRUE indicates that the DNS server does not use this zone to answer queries or accept updates. FALSE indicates that the zone is handled normally.

**fShutdown:**  A Boolean value that indicates whether this zone is currently shut down.

**fAutoCreated:**  A Boolean value that indicates whether this zone was autocreated by the DNS server at boot time.

**fUseDatabase:**  A Boolean value that indicates whether this zone is stored in a directory server.

**pszDataFile:**  A pointer to a null-terminated UTF-8 character string that specifies the name (with no path) of the zone file for a file-based zone or NULL if this zone is not stored in a file.

**aipMasters:**  A pointer to a structure of type IP4\_ARRAY (section [2.2.3.2.1](#Section_588ae29671bf402f999686ecee39dc29)) that specifies a list of IPv4 addresses of the remote DNS servers that can be sources of information for this zone to perform zone transfers by a secondary. This value is applicable for secondary, stub and forwarder zones only and MUST be NULL for all other zone types.

**fSecureSecondaries:**  The secondary security settings configured for a zone on the master DNS server. The DNS server MUST respond to zone transfer requests from a secondary server according to the behavior description corresponding to this flag's value as specified in DNS\_ZONE\_SECONDARY\_SECURITY (section [2.2.5.1.2](#Section_751e1cf8c97f41c5ae499a674398d0f3)). This value MUST be set to one of the allowed values as specified in DNS\_ZONE\_SECONDARY\_SECURITY (section 2.2.5.1.2).

**fNotifyLevel:**  This parameter is ignored, and for dwZoneType parameter setting DNS\_ZONE\_TYPE\_PRIMARY (specified in section 2.2.5.1.1) and for DNS servers that are not directory service-integrated, the zone notification setting is set to ZONE\_NOTIFY\_ALL\_SECONDARIES. Otherwise, it is set to ZONE\_NOTIFY\_LIST\_ONLY, as specified in section [2.2.5.1.3](#Section_343f4212ad8a47908aa77c5bc15f7bd2).

**aipSecondaries:**  A pointer to a structure of type IP4\_ARRAY (section 2.2.3.2.1) that specifies a list of IPv4 addresses of the remote DNS servers that are secondary DNS servers for this zone, or NULL if there are no secondary DNS servers. If fSecureSecondaries is set to ZONE\_SECSECURE\_LIST\_ONLY then only zone transfers from IP addresses in this list will be honored.

**aipNotify:**  A pointer to a structure of type IP4\_ARRAY (section 2.2.3.2.1) that specifies a list of IPv4 addresses of the remote DNS servers that are secondaries for this zone, for which this DNS server is acting as master and the DNS server will send zone notifications to these secondary servers, as directed by the value of fNotifyLevel above.

**fUseWins:**  A Boolean value that indicates whether WINS resource record lookup is enabled for this forward lookup zones.

**fUseNbstat:**  A Boolean value that indicates whether WINS-R resource record lookup is enabled for this reverse lookup zones.

**fAging:**  A Boolean value where TRUE (0x00000001) indicates that aging is enabled for resource records in this zone, so the time-stamps of records in the zone will be updated when server receives dynamic update request for that record; whereas FALSE(0x00000000) indicates, that the time-stamps of the records in the zone will not be updated.

**dwNoRefreshInterval:**  The time interval, in hours, that is configured as NoRefresh interval value for this zone. This value determines the time interval between the last update of a record's time-stamp and the earliest instance when that time-stamp can be refreshed.

**dwRefreshInterval:**  The time interval, in hours, that is configured as the refresh interval value for this zone. Records that have not been refreshed by the expiration of this interval are eligible to be removed during the next scavenging cycle performed by the DNS server.

**dwAvailForScavengeTime:**  The time interval, in hours, that is available before the scheduled next scavenging cycle for this zone.

**aipScavengeServers:**  A pointer to a structure of type IP4\_ARRAY (section 2.2.3.2.1) that specifies a list of IPv4 addresses of the DNS servers that will perform scavenging for this zone. This value is applicable for zones of type DNS\_ZONE\_TYPE\_PRIMARY (section DNS\_ZONE\_TYPE) only. If this value is NULL then there are no restrictions on which DNS server may perform scavenging for this zone.

**pvReserved1:**  Reserved for future use. Server MUST set to zero and receiver MUST ignore this value.

**pvReserved2:**  Reserved for future use. Server MUST set to zero and receiver MUST ignore this value.

**pvReserved3:**  Reserved for future use. Server MUST set to zero and receiver MUST ignore this value.

**pvReserved4:**  Reserved for future use. Server MUST set to zero and receiver MUST ignore this value.

###### DNS\_RPC\_ZONE\_INFO\_DOTNET

All fields have same definition as specified in section DNS\_RPC\_ZONE\_INFO\_W2K (section [2.2.5.2.4.1](#Section_e86515440fbb40388232375ff2d8a55e)), with the following exceptions:

1. typedef struct \_DnsRpcZoneInfoDotNet {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. [string] char\* pszZoneName;
5. DWORD dwZoneType;
6. DWORD fReverse;
7. DWORD fAllowUpdate;
8. DWORD fPaused;
9. DWORD fShutdown;
10. DWORD fAutoCreated;
11. DWORD fUseDatabase;
12. [string] char\* pszDataFile;
13. PIP4\_ARRAY aipMasters;
14. DWORD fSecureSecondaries;
15. DWORD fNotifyLevel;
16. PIP4\_ARRAY aipSecondaries;
17. PIP4\_ARRAY aipNotify;
18. DWORD fUseWins;
19. DWORD fUseNbstat;
20. DWORD fAging;
21. DWORD dwNoRefreshInterval;
22. DWORD dwRefreshInterval;
23. DWORD dwAvailForScavengeTime;
24. PIP4\_ARRAY aipScavengeServers;
25. DWORD dwForwarderTimeout;
26. DWORD fForwarderSlave;
27. PIP4\_ARRAY aipLocalMasters;
28. DWORD dwDpFlags;
29. [string] char\* pszDpFqdn;
30. [string] wchar\_t\* pwszZoneDn;
31. DWORD dwLastSuccessfulSoaCheck;
32. DWORD dwLastSuccessfulXfr;
33. DWORD dwReserved1;
34. DWORD dwReserved2;
35. DWORD dwReserved3;
36. DWORD dwReserved4;
37. DWORD dwReserved5;
38. [string] char\* pReserved1;
39. [string] char\* pReserved2;
40. [string] char\* pReserved3;
41. [string] char\* pReserved4;
42. } DNS\_RPC\_ZONE\_INFO\_DOTNET,
43. \*PDNS\_RPC\_ZONE\_INFO\_DOTNET;

**dwRpcStructureVersion:**  The DNS server management structure version number. This value SHOULD[<40>](#Appendix_A_40) be set to 0x00000001.

**dwReserved0:**  Reserved for future use. Server will set to zero and receiver MUST ignore this value.

**dwForwarderTimeout:**  (4 bytes): The forwarder timeout value for a zone, in seconds. This is the number of seconds the DNS server waits for response from a remote DNS server for a forwarded query. This value is applicable for zones of type DNS\_ZONE\_TYPE\_FORWARDER (section [2.2.5.1.1](#Section_27e138a7110c44a4afcbb95f35f00306)). For all other zone types, senders MUST set this value to zero and receivers MUST ignore it.

**fForwarderSlave:**  A Boolean value indicating whether the DNS server is not allowed to perform recursion while resolving names for this zone. The DNS server MUST fail queries after getting failure from all forwarded servers, if the value is TRUE (0x00000001). Otherwise normal recursion MUST be performed. This value is applicable for zones of type DNS\_ZONE\_TYPE\_FORWARDER (section 2.2.5.1.1). For all other zone types, senders MUST set this value to zero and receivers MUST ignore it.

**aipLocalMasters:**  A pointer to a structure of type [IP4\_ARRAY (section 2.2.3.2.1)](#Section_588ae29671bf402f999686ecee39dc29) that specifies a list of IPv4 addresses of primary DNS servers for this zone. If this value is not NULL then it overrides the master servers list configured in the directory server.

**dwDpFlags:**  Flag value that specifies information about the application directory partition in which this zone is stored. This MUST be set to any combination of the [DNS\_RPC\_DP\_FLAGS (section 2.2.7.1.1)](#Section_27e378aad4d743de8b343e5b957a7130) or zero if this zone is not stored in a directory server.

**pszDpFqdn:**  A pointer to a null-terminated UTF-8 string that specifies the FQDN of the application directory partition in which this zone is stored. If the zone is not stored in an application directory partition this value MUST be NULL.

**pwszZoneDn:**  Pointer to a null-terminated Unicode string that specifies the distinguished name for the zone if the zone is stored the directory server. This field is applicable for directory server integrated zones only. The value MUST be NULL if this zone is not stored in the directory server.

**dwLastSuccessfulSoaCheck:**  The time-stamp at which last SOA record was received successfully from the primary DNS server for this zone. This field is applicable only for zones which are secondary or non-authoritative. For all other zones this value MUST be set to zero by senders and MUST be ignored by receivers.

**dwLastSuccessfulXfr:**  The time-stamp at which last zone transfer was completed successfully from the primary DNS server for this zone. This field is applicable only for zones which are secondary or non-authoritative. For all other zones this value MUST be set to zero by senders and MUST be ignored by receivers.

**dwReserved1:**  Reserved for future use. Server MUST set to zero and receiver MUST ignore this value.

**dwReserved2:**  Reserved for future use. Server MUST set to zero and receiver MUST ignore this value.

**dwReserved3:**  Reserved for future use. Server MUST set to zero and receiver MUST ignore this value.

**dwReserved4:**  Reserved for future use. Server MUST set to zero and receiver MUST ignore this value.

**dwReserved5:**  Reserved for future use. Server MUST set to zero and receiver MUST ignore this value.

**pReserved1:**  Reserved for future use. Server MUST set to zero and receiver MUST ignore this value.

**pReserved2:**  Reserved for future use. Server MUST set to zero and receiver MUST ignore this value.

**pReserved3:**  Reserved for future use. Server MUST set to zero and receiver MUST ignore this value.

**pReserved4:**  Reserved for future use. Server MUST set to zero and receiver MUST ignore this value.

###### DNS\_RPC\_ZONE\_INFO\_LONGHORN

All fields have same definition as specified in section DNS\_RPC\_ZONE\_INFO\_DOTNET (section [2.2.5.2.4.2](#Section_45b100df57c24c8486de00b69d742372)), with the following exceptions:

1. typedef struct \_DnsRpcZoneInfoLonghorn {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. [string] char\* pszZoneName;
5. DWORD dwZoneType;
6. DWORD fReverse;
7. DWORD fAllowUpdate;
8. DWORD fPaused;
9. DWORD fShutdown;
10. DWORD fAutoCreated;
11. DWORD fUseDatabase;
12. [string] char\* pszDataFile;
13. PDNS\_ADDR\_ARRAY aipMasters;
14. DWORD fSecureSecondaries;
15. DWORD fNotifyLevel;
16. PDNS\_ADDR\_ARRAY aipSecondaries;
17. PDNS\_ADDR\_ARRAY aipNotify;
18. DWORD fUseWins;
19. DWORD fUseNbstat;
20. DWORD fAging;
21. DWORD dwNoRefreshInterval;
22. DWORD dwRefreshInterval;
23. DWORD dwAvailForScavengeTime;
24. PDNS\_ADDR\_ARRAY aipScavengeServers;
25. DWORD dwForwarderTimeout;
26. DWORD fForwarderSlave;
27. PDNS\_ADDR\_ARRAY aipLocalMasters;
28. DWORD dwDpFlags;
29. [string] char\* pszDpFqdn;
30. [string] wchar\_t\* pwszZoneDn;
31. DWORD dwLastSuccessfulSoaCheck;
32. DWORD dwLastSuccessfulXfr;
33. DWORD fQueuedForBackgroundLoad;
34. DWORD fBackgroundLoadInProgress;
35. BOOL fReadOnlyZone;
36. DWORD dwLastXfrAttempt;
37. DWORD dwLastXfrResult;
38. } DNS\_RPC\_ZONE\_INFO\_LONGHORN,
39. \*PDNS\_RPC\_ZONE\_INFO\_LONGHORN,
40. DNS\_RPC\_ZONE\_INFO,
41. \*PDNS\_RPC\_ZONE\_INFO;

**dwRpcStructureVersion:**  The DNS server management structure version number. It SHOULD[<41>](#Appendix_A_41) be set to 0x00000002.

**aipMasters:**  A pointer to a structure of type DNS\_ADDR\_ARRAY (section [2.2.3.2.3](#Section_56BA5FABF304486699A44F1C1F9247A3)) that specifies a list of IP addresses of the remote DNS servers that can be sources of information for this zone on which to perform zone transfers by a secondary. This value is applicable for secondary, stub and forwarder zones only and MUST be NULL for all other zone types.

**aipSecondaries:**  A pointer to a structure of type DNS\_ADDR\_ARRAY (section 2.2.3.2.3) that specifies a list of IP addresses of the remote DNS servers that are secondary DNS servers for this zone, or NULL if there are no secondary DNS servers. If **fSecureSecondaries** is set to ZONE\_SECSECURE\_LIST\_ONLY, then only zone transfers from IP addresses in this list will be honored.

**aipNotify:**  A pointer to a structure of type DNS\_ADDR\_ARRAY (section 2.2.3.2.3) that specifies a list of IP addresses of the remote DNS servers that are secondaries for this zone, for which this DNS server is acting as master and the DNS server will send zone notifications to these secondary servers, as directed by the value of **fNotifyLevel** above.

**aipScavengeServers:**  A pointer to a structure of type DNS\_ADDR\_ARRAY (section 2.2.3.2.3) that specifies a list of IP addresses of the DNS servers that will perform scavenging for this zone. This value is applicable for zones of type DNS\_ZONE\_TYPE\_PRIMARY (section [2.2.5.1.1](#Section_27E138A7110C44A4AFCBB95F35F00306)) only. If this value is NULL then there are no restrictions on which DNS server may perform scavenging for this zone.

**aipLocalMasters:**  A pointer to a structure of type DNS\_ADDR\_ARRAY (section 2.2.3.2.3) that specifies a list of IP addresses of primary DNS servers for this zone. If this value is not NULL then it overrides the masters servers list configured in the directory server.

**fQueuedForBackgroundLoad:**  This MUST be set to 0x00000001 if this zone is has not yet been loaded from persistent storage.

**fBackgroundLoadInProgress:**  This MUST be set to 0x00000001 if this zone is currently being loaded from persistent storage, or 0x00000000 if it has been loaded.

**fReadOnlyZone:**  This MUST be set to 0x00000001 if this zone is backed by a read-only store that will not accept write operations, or 0x00000000 if not.

**dwLastXfrAttempt:**  The time-stamp at which last zone transfer was attempted by a DNS server. This field is applicable only for zones which are secondary or not-authoritative. For all other zones senders MUST set this value to zero and receivers MUST ignore it.

**dwLastXfrResult:**  The result of the last zone transfer attempted by server. This field is applicable only for zones which are secondary or not-authoritative, and in this case it MUST be either a Win32 error code, or 0xFFFFFFFF to indicate that a zone transfer is currently in progress. For all other zones senders MUST set this value to zero and receivers MUST ignore it.

##### DNS\_RPC\_ZONE\_SECONDARIES

The DNS\_RPC\_ZONE\_SECONDARIES structure contains the information about the secondary DNS servers for a zone. There are different versions of the DNS\_RPC\_ZONE\_SECONDARIES structure. The DNS server MUST use the structure corresponding to the value of the *dwClientVersion* in DNS Server Management Protocol method calls (section [3.1.4](#Section_bdffbbf3e31b49ba8b8d8abde125a9d8)) as in the following table, or if the method call does not specify the value of *dwClientVersion*, the DNS\_RPC\_ZONE\_SECONDARIES\_W2K version of the structure MUST be used.

| Value | Structure |
| --- | --- |
| 0x00000000 | DNS\_RPC\_ZONE\_SECONDARIES\_W2K (section [2.2.5.2.5.1](#Section_0961e81f542f48c78043bd420d104101)) |
| 0x00060000 | DNS\_RPC\_ ZONE\_SECONDARIES\_DOTNET (section [2.2.5.2.5.2](#Section_f3f440eb6ff5419ca9ff7ed6aafc937a)) |
| 0x00070000 | DNS\_RPC\_ ZONE\_SECONDARIES\_LONGHORN (section [2.2.5.2.5.3](#Section_bf91cfc1da7c48f4bb5ff708ad305f3c)) |

###### DNS\_RPC\_ZONE\_SECONDARIES\_W2K

1. typedef struct \_DnssrvRpcZoneSecondariesW2K {
2. DWORD fSecureSecondaries;
3. DWORD fNotifyLevel;
4. PIP4\_ARRAY aipSecondaries;
5. PIP4\_ARRAY aipNotify;
6. } DNS\_RPC\_ZONE\_SECONDARIES\_W2K,
7. \*PDNS\_RPC\_ZONE\_SECONDARIES\_W2K;

**fSecureSecondaries:**  The secondary security settings configured for this zone. The DNS server MUST respond to zone transfer requests from a secondary server according to the behavior corresponding to the value of the flag, as described in DNS\_ZONE\_SECONDARY\_SECURITY (section [2.2.5.1.2](#Section_751e1cf8c97f41c5ae499a674398d0f3)). This value MUST be set to one of the allowed values as specified in DNS\_ZONE\_SECONDARY\_SECURITY (section 2.2.5.1.2).

**fNotifyLevel:**  The settings for sending zone notifications for this zone. The DNS server MUST send notify messages to secondary servers as specified by the entry corresponding to the value of this flag, as shown in the table in section [2.2.5.1.3](#Section_343f4212ad8a47908aa77c5bc15f7bd2). This flag's value MUST be set to one of the allowed values as specified in DNS\_ZONE\_ NOTIFY\_LEVEL (section 2.2.5.1.3).

**aipSecondaries:**  The list of IPv4 addresses of remote DNS servers that are permitted to perform zone transfers for this zone. The DNS server will honor zone transfer requests from these secondary servers, as specified by fSecureSecondaries above.

**aipNotify:**  The list of IPv4 addresses of the remote DNS servers that will be sent notification messages when records in this zone change, as directed by fNotifyLevel above.

###### DNS\_RPC\_ZONE\_SECONDARIES\_DOTNET

All fields have same definition as specified in section DNS\_RPC\_ZONE\_SECONDARIES\_W2K (section [2.2.5.2.5.1](#Section_0961e81f542f48c78043bd420d104101)), with the following exceptions:

1. typedef struct \_DnssrvRpcZoneSecondariesDotNet {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. DWORD fSecureSecondaries;
5. DWORD fNotifyLevel;
6. PIP4\_ARRAY aipSecondaries;
7. PIP4\_ARRAY aipNotify;
8. } DNS\_RPC\_ZONE\_SECONDARIES\_DOTNET,
9. \*PDNS\_RPC\_ZONE\_SECONDARIES\_DOTNET;

**dwRpcStructureVersion:**  The DNS server management structure version number. It MUST be set to 0x00000001

**dwReserved0:**  Reserved for future use. Sender MUST set to zero and receiver MUST ignore this value.

###### DNS\_RPC\_ZONE\_SECONDARIES\_LONGHORN

All fields have same definition as specified in section DNS\_RPC\_ZONE\_SECONDARIES\_DOTNET (section [2.2.5.2.5.2](#Section_f3f440eb6ff5419ca9ff7ed6aafc937a)), with the following exceptions:

1. typedef struct \_DnssrvRpcZoneSecondariesLonghorn {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. DWORD fSecureSecondaries;
5. DWORD fNotifyLevel;
6. PDNS\_ADDR\_ARRAY aipSecondaries;
7. PDNS\_ADDR\_ARRAY aipNotify;
8. } DNS\_RPC\_ZONE\_SECONDARIES\_LONGHORN,
9. \*PDNS\_RPC\_ZONE\_SECONDARIES\_LONGHORN,
10. DNS\_RPC\_ZONE\_SECONDARIES,
11. \*PDNS\_RPC\_ZONE\_SECONDARIES;

**dwRpcStructureVersion:**  The DNS server management structure version number. It MUST be set to 0x00000002.

**aipSecondaries:**  A pointer to a structure of type DNS\_ADDR\_ARRAY (section [2.2.3.2.3](#Section_56ba5fabf304486699a44f1c1f9247a3)) that specifies a list of IP addresses of remote DNS servers that are permitted to perform zone transfers for this zone. The DNS server will honor zone transfer requests from these secondary servers, as directed by the value of fSecureSecondaries above.

**aipNotify:**  A pointer to a structure of type DNS\_ADDR\_ARRAY (section 2.2.3.2.3) that specifies a list of IP addresses of the remote DNS servers that be sent notification messages when records in this zone change, as directed by fNotifyLevel above.

##### DNS\_RPC\_ZONE\_DATABASE

The DNS\_RPC\_ZONE\_DATABASE structure contains information about the persistent data store for a zone on the DNS server. There are different versions of the DNS\_RPC\_ZONE\_DATABASE structure. The DNS server MUST use the structure corresponding to the value of *dwClientVersion* in DNS Server Management Protocol method calls (section [3.1.4](#Section_bdffbbf3e31b49ba8b8d8abde125a9d8)) as shown in the following table, or if the method call does not specify the value of *dwClientVersion*, the DNS\_RPC\_ZONE\_DATABASE\_W2K (section [2.2.5.2.6.1](#Section_660c4d3d6049422b912a7bf9129e7ed6)) version of the structure MUST be used.

| Value | Structure |
| --- | --- |
| 0x00000000 | DNS\_RPC\_ZONE\_DATABASE\_W2K (section 2.2.5.2.6.1) |
| 0x00060000 | DNS\_RPC\_ZONE\_DATABASE\_DOTNET (section [2.2.5.2.6.2](#Section_05778fae86d1414dbdf799479bb1ac15)) |
| 0x00070000 | DNS\_RPC\_ZONE\_DATABASE\_DOTNET (section 2.2.5.2.6.2) |

###### DNS\_RPC\_ZONE\_DATABASE\_W2K

1. typedef struct \_DnssrvRpcZoneDatabaseW2K {
2. DWORD fDsIntegrated;
3. [string] char\* pszFileName;
4. } DNS\_RPC\_ZONE\_DATABASE\_W2K,
5. \*PDNS\_RPC\_ZONE\_DATABASE\_W2K;

**fDsIntegrated:**  This MUST be set TRUE (0x00000001) if the zone is stored in a directory server, or FALSE (0x00000000) if not.

0x00000001

0x00000000

**pszFileName:**  A pointer to a null-terminated UTF-8 string that specifies the name of the file in which this zone is stored, or NULL if this zone is to be stored in a directory server or in a file with the default file name for the zone.

###### DNS\_RPC\_ZONE\_DATABASE\_DOTNET

All fields have same definition as specified in section DNS\_RPC\_ZONE\_DATABASE\_W2K (section [2.2.5.2.6.1](#Section_660c4d3d6049422b912a7bf9129e7ed6)), with the following exceptions:

1. typedef struct \_DnssrvRpcZoneDatabaseDotNet {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. DWORD fDsIntegrated;
5. [string] char\* pszFileName;
6. } DNS\_RPC\_ZONE\_DATABASE\_DOTNET,
7. \*PDNS\_RPC\_ZONE\_DATABASE\_DOTNET,
8. DNS\_RPC\_ZONE\_DATABASE,
9. \*PDNS\_RPC\_ZONE\_DATABASE;

**dwRpcStructureVersion:**  The DNS management structure version number. This MUST be set to 0x00000001.

**dwReserved0:**  Reserved for future use. The sender MUST set this value to 0x00000000 and it MUST be ignored by the receiver.

##### DNS\_RPC\_ZONE\_CREATE\_INFO

The DNS\_RPC\_ZONE\_CREATE\_INFO structure contains information required to create a zone or reset a zone's information on the DNS server. There are different versions of the DNS\_RPC\_ZONE\_CREATE\_INFO structure. The DNS server MUST use the structure corresponding to the value of *dwClientVersion* in DNS Server Management Protocol method calls (section [3.1.4](#Section_bdffbbf3e31b49ba8b8d8abde125a9d8)) as shown in the following table, or if the method call does not specify the value of *dwClientVersion*, the DNS\_RPC\_ZONE\_CREATE\_INFO\_W2K version of the structure MUST be used.

| Value | Structure |
| --- | --- |
| 0x00000000 | DNS\_RPC\_ZONE\_CREATE\_INFO\_W2K (section [2.2.5.2.7.1](#Section_780eba2615ea43d3a2b377ed9ab00690)) |
| 0x00060000 | DNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET (section [2.2.5.2.7.2](#Section_f0a445761d3f43ccbece07ae958f5b36)) |
| 0x00070000 | DNS\_RPC\_ZONE\_CREATE\_INFO\_LONGHORN (section [2.2.5.2.7.3](#Section_5646cf31c0d242d88ef8ab2b69feb37b)) |

###### DNS\_RPC\_ZONE\_CREATE\_INFO\_W2K

typedef struct \_DnsRpcZoneCreateInfo {

1. [string] char\* pszZoneName;
2. DWORD dwZoneType;
3. DWORD fAllowUpdate;
4. DWORD fAging;
5. DWORD dwFlags;
6. [string] char\* pszDataFile;
7. DWORD fDsIntegrated;
8. DWORD fLoadExisting;
9. [string] char\* pszAdmin;
10. PIP4\_ARRAY aipMasters;
11. PIP4\_ARRAY aipSecondaries;
12. DWORD fSecureSecondaries;
13. DWORD fNotifyLevel;
14. [string] char\* pvReserved1;
15. [string] char\* pvReserved2;
16. [string] char\* pvReserved3;
17. [string] char\* pvReserved4;
18. [string] char\* pvReserved5;
19. [string] char\* pvReserved6;
20. [string] char\* pvReserved7;
21. [string] char\* pvReserved8;
22. DWORD dwReserved1;
23. DWORD dwReserved2;
24. DWORD dwReserved3;
25. DWORD dwReserved4;
26. DWORD dwReserved5;
27. DWORD dwReserved6;
28. DWORD dwReserved7;
29. DWORD dwReserved8;
30. } DNS\_RPC\_ZONE\_CREATE\_INFO\_W2K,
31. \*PDNS\_RPC\_ZONE\_CREATE\_INFO\_W2K;

**pszZoneName:**  As specified in section [2.2.5.2.4.1](#Section_e86515440fbb40388232375ff2d8a55e).

**dwZoneType:**  The zone type. This MUST be set to one of the allowed values specified in DNS\_ZONE\_TYPE (section [2.2.5.1.1](#Section_27e138a7110c44a4afcbb95f35f00306)), and it MUST NOT be either DNS\_ZONE\_TYPE\_CACHE or DNS\_ZONE\_TYPE\_SECONDARY\_CACHE.

**fAllowUpdate:**  As specified in section 2.2.5.2.4.1.

**fAging:**  As specified in section 2.2.5.2.4.1.

**dwFlags:**  The zone creation behavior that the DNS server is to follow while creating the zone. This field is only used when the operation is **ZoneCreate**. The DNS server MUST ignore the value of this field when the operation is **ZoneTypeReset**. This field MUST be set to any combination of the following values:

| Value | Meaning |
| --- | --- |
| DNS\_ZONE\_LOAD\_OVERWRITE\_MEMORY  0x00000010 | If **dwZoneType** is not set to the value DNS\_ZONE\_TYPE\_PRIMARY (section 2.2.5.1.1), then this flag MUST be ignored. Otherwise, the DNS server MUST attempt to find and load the zone database from persistent storage instead of creating a new empty zone database. If the value of fDsIntegrated is 0x00000001 then the DNS server MUST search for a pre-existing zone database in the directory server, otherwise the DNS server MUST search for a pre-existing zone database in a file. If a pre-existing zone database is not found then it continues with zone creation, however if a pre-existing zone database is found but could not be loaded, the DNS server MUST fail the operation and return an error. |
| DNS\_ZONE\_CREATE\_FOR\_DCPROMO  0x00001000 | If this flag is set, the DNS server MUST create the zone such that it is directory server-integrated and stored in the DNS domain partition. |
| DNS\_ZONE\_CREATE\_FOR\_DCPROMO\_FOREST  0x00004000 | If this flag is set, the DNS server MUST create the zone such that it is directory server-integrated and stored in the DNS forest partition. |

**pszDataFile:**  As specified in section 2.2.5.2.4.1.

**fDsIntegrated:**  A value of 0x00000001 indicates that the zone is to be created to use the directory server for persistent storage, and 0x00000000 indicates it is not. If this is set to 0x00000001 the caller MUST specify the application directory partition information in pszDpFqdn (section [2.2.5.2.7.2](#Section_f0a445761d3f43ccbece07ae958f5b36)); in this case the DNS server MUST ignore the value of pszDataFile.

**fLoadExisting:**  If the operation is **ZoneCreate** this field is interpreted as a Boolean value. If set to TRUE this has the same effect as specifying DNS\_ZONE\_LOAD\_OVERWRITE\_MEMORY in the **dwFlags** field above. If the operation is **ZoneTypeReset** this field may be set to one of the following values but the DNS server MUST ignore the value of this field if **fDsIntegrated** is not TRUE or **dwZoneType** is not DNS\_ZONE\_TYPE\_PRIMARY (section 2.2.5.1.1).

| Value | Meaning |
| --- | --- |
| DNS\_ZONE\_LOAD\_OVERWRITE\_MEMORY  0x00000010 | The server MUST attempt to find and load the zone database from persistent storage instead of retaining the existing in-memory zone database by searching for a pre-existing zone database in the directory server. If a pre-existing zone database is not found, then the server MUST fail the operation and return an error. |
| DNS\_ZONE\_LOAD\_OVERWRITE\_DS  0x00000020 | If this flag is set and if the zone already exists in the database, then the server MUST overwrite the existing zone database with current in-memory zone database. |

**pszAdmin:**  A pointer to a null-terminated UTF-8 string containing the administrator's email name (in the format specified in [[RFC1035]](http://go.microsoft.com/fwlink/?LinkId=90264) section 8) or NULL to cause the DNS server to use a default value "hostmaster", followed by the name of the zone. This value MUST be used to populate the zone administrator email field in the SOA record in the new zone.

**aipMasters:**  As specified in section 2.2.5.2.4.1.

**aipSecondaries:**  As specified in section 2.2.5.2.4.1.

**fSecureSecondaries:**  As specified in section 2.2.5.2.4.1.

**fNotifyLevel:**  As specified in section 2.2.5.2.4.1.

**pvReserved1:**  MUST be set to zero when sent and MUST be ignored on receipt.

**pvReserved2:**  MUST be set to zero when sent and MUST be ignored on receipt.

**pvReserved3:**  MUST be set to zero when sent and MUST be ignored on receipt.

**pvReserved4:**  MUST be set to zero when sent and MUST be ignored on receipt.

**pvReserved5:**  MUST be set to zero when sent and MUST be ignored on receipt.

**pvReserved6:**  MUST be set to zero when sent and MUST be ignored on receipt.

**pvReserved7:**  MUST be set to zero when sent and MUST be ignored on receipt.

**pvReserved8:**  MUST be set to zero when sent and MUST be ignored on receipt.

**dwReserved1:**  MUST be set to zero when sent and MUST be ignored on receipt.

**dwReserved2:**  MUST be set to zero when sent and MUST be ignored on receipt.

**dwReserved3:**  MUST be set to zero when sent and MUST be ignored on receipt.

**dwReserved4:**  MUST be set to zero when sent and MUST be ignored on receipt.

**dwReserved5:**  MUST be set to zero when sent and MUST be ignored on receipt.

**dwReserved6:**  MUST be set to zero when sent and MUST be ignored on receipt.

**dwReserved7:**  MUST be set to zero when sent and MUST be ignored on receipt.

**dwReserved8:**  MUST be set to zero when sent and MUST be ignored on receipt.

###### DNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET

All fields have same definition as specified in section DNS\_RPC\_ZONE\_CREATE\_INFO\_W2K (section [2.2.5.2.7.1](#Section_780eba2615ea43d3a2b377ed9ab00690)), with the following exceptions:

1. typedef struct \_DnsRpcZoneCreateInfoDotNet {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. [string] char\* pszZoneName;
5. DWORD dwZoneType;
6. DWORD fAllowUpdate;
7. DWORD fAging;
8. DWORD dwFlags;
9. [string] char\* pszDataFile;
10. DWORD fDsIntegrated;
11. DWORD fLoadExisting;
12. [string] char\* pszAdmin;
13. PIP4\_ARRAY aipMasters;
14. PIP4\_ARRAY aipSecondaries;
15. DWORD fSecureSecondaries;
16. DWORD fNotifyLevel;
17. DWORD dwTimeout;
18. DWORD fRecurseAfterForwarding;
19. DWORD dwDpFlags;
20. [string] char\* pszDpFqdn;
21. DWORD dwReserved[32];
22. } DNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET,
23. \*PDNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET;

**dwRpcStructureVersion:**  As specified in section [2.2.5.2.4.2](#Section_45b100df57c24c8486de00b69d742372).

**dwReserved0:**  As specified in section 2.2.5.2.4.2.

**dwTimeout:**  Equivalent to dwForwarderTimeout specified in section 2.2.5.2.4.2.

**fRecurseAfterForwarding:**  Equivalent to fForwarderSlave specified in section 2.2.5.2.4.2.

**dwDpFlags:**  As specified in section 2.2.5.2.4.2. However, only the following values can be used and of these values more than one MUST NOT be specified: "DNS\_DP\_LEGACY", "DNS\_DP\_DOMAIN\_DEFAULT", and "DNS\_DP\_FOREST\_DEFAULT". This field is set to zero if the zone is not to be created to use the directory server for persistent storage. The DNS server returns an error if any value not listed above is specified or if more than one of the allowable values are specified.

**pszDpFqdn:**  As specified in section 2.2.5.2.4.2.

**dwReserved:**  MUST be set to zero when sent and MUST be ignored on receipt.

If the DNS RPC client sends an older version of DNS\_RPC\_ZONE\_CREATE\_INFO structure such as DNS\_RPC\_ZONE\_CREATE\_INFO\_W2K (section 2.2.5.2.7.1), then the DNS RPC server MUST construct a current version of DNS\_RPC\_ZONE\_CREATE\_INFO structure such as DNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET, using steps as specified below:

1. Copy the same value for fields that are common to input and current version of DNS\_RPC\_ZONE\_CREATE\_INFO structures.
2. dwRpcStructureVersion field MUST be set to 1.
3. All other fields that are defined only in DNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET and are not defined in DNS\_RPC\_ZONE\_CREATE\_INFO\_W2K (section 2.2.5.2.7.1), MUST be set to 0.

###### DNS\_RPC\_ZONE\_CREATE\_INFO\_LONGHORN

All fields have same definition as specified in section DNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET (section [2.2.5.2.7.2](#Section_f0a445761d3f43ccbece07ae958f5b36)), with the following exceptions:

1. typedef struct \_DnsRpcZoneCreateInfoLonghorn {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. [string] char\* pszZoneName;
5. DWORD dwZoneType;
6. DWORD fAllowUpdate;
7. DWORD fAging;
8. DWORD dwFlags;
9. [string] char\* pszDataFile;
10. DWORD fDsIntegrated;
11. DWORD fLoadExisting;
12. [string] char\* pszAdmin;
13. PDNS\_ADDR\_ARRAY aipMasters;
14. PDNS\_ADDR\_ARRAY aipSecondaries;
15. DWORD fSecureSecondaries;
16. DWORD fNotifyLevel;
17. DWORD dwTimeout;
18. DWORD fRecurseAfterForwarding;
19. DWORD dwDpFlags;
20. [string] char\* pszDpFqdn;
21. DWORD dwReserved[32];
22. } DNS\_RPC\_ZONE\_CREATE\_INFO\_LONGHORN,
23. \*PDNS\_RPC\_ZONE\_CREATE\_INFO\_LONGHORN,
24. DNS\_RPC\_ZONE\_CREATE\_INFO,
25. \*PDNS\_RPC\_ZONE\_CREATE\_INFO;

**dwRpcStructureVersion:**  As specified in section [2.2.5.2.4.3](#Section_23a085bfd81445e3943f8bbdc32a5dae).

**aipMasters:**  As specified in section 2.2.5.2.4.3.

**aipSecondaries:**  As specified in section 2.2.5.2.4.3.

If the DNS RPC client sends an older version of DNS\_RPC\_ZONE\_CREATE\_INFO structure such as DNS\_RPC\_ZONE\_CREATE\_INFO\_W2K (section [2.2.5.2.7.1](#Section_780eba2615ea43d3a2b377ed9ab00690)) or DNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET (section 2.2.5.2.7.2), then the DNS RPC server MUST construct a current version of DNS\_RPC\_ZONE\_CREATE\_INFO structure such as DNS\_RPC\_ZONE\_CREATE\_INFO\_LONGHORN, using steps as specified below:

1. Copy the same value for fields that are common to input and current version of DNS\_RPC\_ZONE\_CREATE\_INFO structures.
2. dwRpcStructureVersion field MUST be set to 2.
3. The values for aipMasters and aipSecondaries fields MUST be obtained from input structure as IP4\_ARRAY type and MUST be converted to DNS\_ADDR\_ARRAY type, and then assigned to aipMasters and aipSecondaries fields in the DNS\_RPC\_ZONE\_CREATE\_INFO\_LONGHORN structure.

**Note**  DNS\_RPC\_ZONE\_CREATE\_INFO\_W2K (section 2.2.5.2.7.1) and DNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET (section 2.2.5.2.7.2), do not support IPv6 address list of **aipMasters** and **aipSecondaries**.

1. All other fields that are defined only in DNS\_RPC\_ZONE\_CREATE\_INFO\_LONGHORN and are not defined in DNS\_RPC\_ZONE\_CREATE\_INFO\_W2K (section 2.2.5.2.7.1) or DNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET (section 2.2.5.2.7.2) structure MUST be set to 0.

##### DNS\_RPC\_ZONE\_EXPORT\_INFO

The DNS\_RPC\_ZONE\_EXPORT\_INFO structure contains the information file to which a zone is exported on the DNS server.[<42>](#Appendix_A_42)

1. typedef struct \_DnssrvRpcZoneExport {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. [string] char\* pszZoneExportFile;
5. } DNS\_RPC\_ZONE\_EXPORT\_INFO,
6. \*PDNS\_RPC\_ZONE\_EXPORT\_INFO;

**dwRpcStructureVersion:**  The structure version number; this MUST be set to 0x00000001.

**dwReserved0:**  MUST be set to zero when sent and MUST be ignored on receipt

**pszZoneExportFile:**  A pointer to a null-terminated UTF-8 string that specifies the name of the file to which a zone is exported by the DNS server.

##### DNS\_RPC\_ENUM\_ZONES\_FILTER

The DNS\_RPC\_ENUM\_ZONES\_FILTER structure specifies zone filtering criteria.

1. typedef struct \_DnsRpcEnumZonesFilter {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. DWORD dwFilter;
5. [string] char\* pszPartitionFqdn;
6. [string] char\* pszQueryString;
7. [string] char\* pszReserved[6];
8. } DNS\_RPC\_ENUM\_ZONES\_FILTER,
9. \*PDNS\_RPC\_ENUM\_ZONES\_FILTER;

**dwRpcStructureVersion:**  The structure version number; this MUST be set to 0x00000001.

**dwReserved0:**  MUST be set to zero when sent and MUST be ignored on receipt.

**dwFilter:**  A filter value that specifies the zone types that are to be selected as part of the output zone list. This value MUST be set to any combination of the ZONE\_REQUEST\_FILTERS (section [2.2.5.1.4](#Section_f4cf1f3e7d134010a9155223dcabc15d)).

**pszPartitionFqdn:**  A pointer to a null-terminated UTF-8 string that specifies the distinguished name for an application directory partition location from which the server is to enumerate zones; if this is NULL then zone enumeration is not restricted based on the application directory partition.

**pszQueryString:**  Reserved for future use. Server MUST set to zero and receiver MUST ignore this value.

**pszReserved:**  Reserved for future use. Server MUST set to zero and receiver MUST ignore this value.

##### DNS\_RPC\_FORWARDERS

The DNS\_RPC\_FORWARDERS structure contains information about forwarders configured on the DNS server. There are different versions of the DNS\_RPC\_FORWARDERS structure. The DNS server MUST use the structures corresponding to the value of *dwClientVersion* in DNS Server Management Protocol method calls (section [3.1.4](#Section_bdffbbf3e31b49ba8b8d8abde125a9d8)) in the following table, or if the method call does not specify the value of *dwClientVersion*, the DNS\_RPC\_FORWARDERS\_W2K version of the structure MUST be used.

| Value | Structure |
| --- | --- |
| 0x00000000 | DNS\_RPC\_FORWARDERS\_W2K (section [2.2.5.2.10.1](#Section_7c71bbd3a46d4f8ebca79bc9e153454f)) |
| 0x00060000 | DNS\_RPC\_FORWARDERS\_DOTNET (section [2.2.5.2.10.2](#Section_4356fa2462664bb2ac5e519b6afe9237)) |
| 0x00070000 | DNS\_RPC\_FORWARDERS\_LONGHORN (section [2.2.5.2.10.3](#Section_2b015323fedd4bf8bcc40df5da06450f)) |

###### DNS\_RPC\_FORWARDERS\_W2K

1. typedef struct \_DnssrvRpcForwardersW2K {
2. DWORD fRecurseAfterForwarding;
3. DWORD dwForwardTimeout;
4. PIP4\_ARRAY aipForwarders;
5. } DNS\_RPC\_FORWARDERS\_W2K,
6. \*PDNS\_RPC\_FORWARDERS\_W2K;

**fRecurseAfterForwarding:**  A value of 0x00000001 indicates that the DNS server is configured to use normal recursion for name resolution if forwarders are not configured or are unreachable; a value of 0x00000000 indicates it is not.

**dwForwardTimeout:**  The time-interval, in seconds, for which the DNS server waits for a response from each server in the forwarders list. No restrictions are applied to the range for the **dwForwardTimeout** member when modifying its value through this structure. If **dwForwardTimeout** is set to zero, then the server SHOULD[<43>](#Appendix_A_43) reset the forward timeout to the default value, 3 minutes (180 seconds).

**aipForwarders:**  The list of IP addresses that will be used as forwarders by the DNS server.

###### DNS\_RPC\_FORWARDERS\_DOTNET

All fields have same definition as specified in section DNS\_RPC\_FORWARDERS\_W2K (section [2.2.5.2.10.1](#Section_7c71bbd3a46d4f8ebca79bc9e153454f)), with the following exceptions:

1. typedef struct \_DnssrvRpcForwardersDotNet {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. DWORD fRecurseAfterForwarding;
5. DWORD dwForwardTimeout;
6. PIP4\_ARRAY aipForwarders;
7. } DNS\_RPC\_FORWARDERS\_DOTNET,
8. \*PDNS\_RPC\_FORWARDERS\_DOTNET;

**dwRpcStructureVersion:**  The structure version number. It MUST be set to 0x00000001.

**dwReserved0:**  MUST be set to zero when sent and MUST be ignored on receipt.

###### DNS\_RPC\_FORWARDERS\_LONGHORN

All fields have same definition as specified in section DNS\_RPC\_FORWARDERS\_DOTNET (section [2.2.5.2.10.2](#Section_4356fa2462664bb2ac5e519b6afe9237)), with the following exceptions:

1. typedef struct \_DnssrvRpcForwardersLonghorn {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. DWORD fRecurseAfterForwarding;
5. DWORD dwForwardTimeout;
6. PDNS\_ADDR\_ARRAY aipForwarders;
7. } DNS\_RPC\_FORWARDERS\_LONGHORN,
8. \*PDNS\_RPC\_FORWARDERS\_LONGHORN,
9. DNS\_RPC\_FORWARDERS,
10. \*PDNS\_RPC\_FORWARDERS;

**dwRpcStructureVersion:**  The structure version number. It MUST be set to 0x00000002.

**aipForwarders:**  A pointer to a structure of type DNS\_ADDR\_ARRAY (section [2.2.3.2.3](#Section_56ba5fabf304486699a44f1c1f9247a3)) specifies a list of IP addresses that will be used as forwarders by the DNS server.

### Zone Update Messages

#### Enumerations and Constants

##### DNS\_ZONE\_UPDATE

A DNS\_ZONE\_UPDATE value is a 2-bit value that indicates the type of dynamic update that is allowed for a zone.

| Constant/value | Description |
| --- | --- |
| ZONE\_UPDATE\_OFF  0x0 | No updates are allowed for the zone. |
| ZONE\_UPDATE\_UNSECURE  0x1 | All updates (secure and unsecure) are allowed for the zone. |
| ZONE\_UPDATE\_SECURE  0x2 | The zone only allows secure updates, that is, the DNS packet MUST have a [**TSIG**](#gt_b6d1e111-4a70-48b1-b302-06372bafec14) [[RFC2845]](http://go.microsoft.com/fwlink/?LinkId=90388) present in the additional section. |

##### KeySignScope

KeySignScope [<44>](#Appendix_A_44) defines the scope of the key in a signed zone. It is used to indicate different signing and publishing scopes of the key.

| Constant/value | Description |
| --- | --- |
| SIGN\_SCOPE\_DEFAULT  0x00000000 | The key is used for its default purpose: If the signing key descriptor's **fIsKSK** field is set to 0x00000001, the key is used to sign only DNSKEY records in the zone. If the signing key descriptor's **fIsKSK** field is set to 0x00000000, the key is used to sign all records in the zone. |
| SIGN\_SCOPE\_DNSKEY\_ONLY  0x00000001 | The key is used to sign only DNSKEY records in the zone. |
| SIGN\_SCOPE\_ALL\_RECORDS  0x00000002 | The key is used to sign all records in the zone. |
| SIGN\_SCOPE\_ADD\_ONLY  0x00000003 | The key is published as a DNSKEY in the zone, but it is not used to sign any records. |
| SIGN\_SCOPE\_DO\_NOT\_PUBLISH  0x00000004 | The key is not published to the zone and is not used to sign any records. |
| SIGN\_SCOPE\_REVOKED  0x00000005 | The key is published as a DNSKEY in the zone with its Revoked bit ([[RFC5011]](http://go.microsoft.com/fwlink/?LinkId=225980) section 2.1) set. It is used to sign DNSKEY records. |

##### ImportOpResult

ImportOpResult[<45>](#Appendix_A_45) defines the operations to be executed when the DNS\_RPC\_ZONE\_DNSSEC\_SETTINGS is imported on a zone.

| Constant/value | Description |
| --- | --- |
| IMPORT\_STATUS\_NOOP  0x0 | No change was detected in the imported signing settings or the signing settings of the zone. |
| IMPORT\_STATUS\_SIGNING\_READY  0x1 | The zone is marked for re-signing. |
| IMPORT\_STATUS\_UNSIGNING\_READY  0x2 | The zone is marked for unsigning. |
| IMPORT\_STATUS\_CHANGED  0x3 | The change was detected in signing settings imported and were incorporated, but no re-signing or unsigning is required. |

#### Structures

##### DNS\_RPC\_SKD

The DNS\_RPC\_SKD structure specifies a signing key descriptor.

1. typedef struct \_DnssrvRpcSigningKeyDescriptor {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. GUID Guid;
5. [string] wchar\_t\* pwszKeyStorageProvider;
6. BOOL fStoreKeysInDirectory;
7. BOOL fIsKSK;
8. BYTE bSigningAlgorithm;
9. DWORD dwKeyLength;
10. DWORD dwInitialRolloverOffset;
11. DWORD dwDNSKEYSignatureValidityPeriod;
12. DWORD dwDSSignatureValidityPeriod;
13. DWORD dwStandardSignatureValidityPeriod;
14. DWORD dwRolloverType;
15. DWORD dwRolloverPeriod;
16. DWORD dwNextRolloverAction;
17. DWORD dwReserved;
18. } DNS\_RPC\_SKD,
19. \*PDNS\_RPC\_SKD;

**dwRpcStructureVersion:**  The structure version number; this MUST be set to 0x00000001.

**dwReserved0:**  MUST be set to zero when sent and MUST be ignored on receipt.

**Guid:**  A unique identifier for this signing key descriptor.

**pwszKeyStorageProvider:**  The Key Storage Provider that will be used to generate and store keys for this signing key descriptor.

**fStoreKeysInDirectory:**  A value of 0x00000001 indicates that the DNS server exports keys generated for this signing key descriptor and stores them on the DNS zone object in Active Directory. A value of 0x00000000 indicates that the DNS server stores keys in self-signed certificates in the local machine certificate store.

**fIsKSK:**  A value of 0x00000001 indicates that this signing key descriptor describes a key signing key; a value of 0x00000000 indicates a zone signing key [[RFC4641]](http://go.microsoft.com/fwlink/?LinkId=225979).

**bSigningAlgorithm:**  The cryptographic algorithm used to generate signing keys. The DNS server SHOULD[<46>](#Appendix_A_46) support all values given by [[IANA-DNSSECAN]](http://go.microsoft.com/fwlink/?LinkId=225982) and [[DRAFT-DNSSEC-ECDSA]](http://go.microsoft.com/fwlink/?LinkId=229294).

**dwKeyLength:**  The length, in bits, of cryptographic signing keys. This value MUST be ignored if the signing algorithm does not have variable key length.

**dwInitialRolloverOffset:**  The amount of time, in seconds, to delay the first scheduled key rollover for this signing key descriptor. The value SHOULD be limited to the range 0x00000000 to 0x00278D00 (30 days), inclusive, but it can be any value. The default value SHOULD be 0x00000000, and the value zero MUST be allowed and treated literally.

**dwDNSKEYSignatureValidityPeriod:**  The number of seconds that signatures covering DNSKEY record sets generated for this signing key descriptor's keys are valid, as defined by [[RFC4034]](http://go.microsoft.com/fwlink/?LinkId=107052) section 3.1.5. The value SHOULD be limited to the range 0x00005460 (6 hours) to 0x0x00093A80 (7 days), inclusive, but it can be any value. The default value SHOULD be 0x0003F480 (3 days).

**dwDSSignatureValidityPeriod:**  The number of seconds that signatures covering DS record sets generated for this signing key descriptor's keys are valid, as defined by [RFC4034] section 3.1.5. The value SHOULD be limited to the range 0x00005460 (6 hours) to 0x00093A80 (7 days), inclusive, but it can be any value. The default value SHOULD be 0x0003F480 (3 days).

**dwStandardSignatureValidityPeriod:**  The number of seconds that signatures covering record sets not of type DNSKEY or DS generated for this signing key descriptor's keys are valid, as defined by [RFC4034] section 3.1.5. The value SHOULD be limited to the range 0x00005460 (6 hours) to 0x0x00278D00 (30 days), inclusive, but it can be any value. The default value SHOULD be 0x000D2F00 (10 days).

**dwRolloverType:**  When sent, this value MUST be set to one of the allowed values specified in [ZONE\_SKD\_ROLLOVER\_TYPE (section 2.2.5.1.5)](#Section_ed7c21aa1175456c8d2f48e117b71b05) as follows: this value MUST be DNS\_ROLLOVER\_TYPE\_PREPUBLISH if **fIsKSK** is 0x00000000 and MUST be DNS\_ROLLOVER\_TYPE\_DOUBLE\_SIGNATURE if **fIsKSK** is 0x00000001. On receipt, this value MUST be ignored.

**dwRolloverPeriod:**  The number of seconds between scheduled key rollovers, or 0xFFFFFFFF to disable automatic key rollovers. This value SHOULD be limited to the range 0x00093A80 (1 week) to 0x25980600 (20 years), inclusive, in addition to 0xFFFFFFFF, when **fIsKSK** is 0x00000001, and the range 0x00093A80 (1 week) to 0x09660180 (5 years), inclusive, in addition to 0xFFFFFFFF, when **fIsKSK** is 0x00000000. The default SHOULD be 0x02022900 (13 months) when **fIsKSK** is 0x00000001, and 0x0x00278D00 (1 month) when **fIsKSK** is 0x00000000.

**dwNextRolloverAction:**  This value describes the next key rollover action that the DNS server will take for this signing key descriptor. This value MUST be set to one of the allowed values specified in [ZONE\_SKD\_ROLLOVER\_ACTION (section 2.2.5.1.6)](#Section_2671ecfc951c4d909b452bd1d87fa8f7).

**dwReserved:**  This value MUST be set to 0x00000000 when sent by the client and ignored on receipt by the server.

##### DNS\_RPC\_SKD\_LIST

The DNS\_RPC\_SKD\_LIST structure contains the information about a list of signing key descriptors that are present for a particular zone on the DNS server.

1. typedef struct \_DnssrvRpcZoneSigningKeyList {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. [range(0,1000)] DWORD dwCount;
5. [size\_is(dwCount)] PDNS\_RPC\_SKD SkdArray[];
6. } DNS\_RPC\_SKD\_LIST,
7. \*PDNS\_RPC\_SKD\_LIST;

**dwRpcStructureVersion:**  The structure version number; this MUST be set to 0x00000001.

**dwReserved0:**  MUST be set to zero when sent and MUST be ignored on receipt.

**dwCount:**  The number of signing key descriptors present in the array of signing key descriptors pointed to by **SkdArray**.

**SkdArray:**  An array of structures of type [DNS\_RPC\_SKD (section 2.2.6.2.1)](#Section_f7b0ad424cae40fd87c882af83824639). Each element of the array represents one signing key descriptor.

##### DNS\_RPC\_SKD\_STATE

The DNS\_RPC\_SKD\_STATE structure contains information about the current state of a signing key descriptor.

1. typedef struct \_DnsRpcSigningKeyDescriptorState {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. GUID Guid;
5. FILETIME ftLastRolloverTime;
6. FILETIME ftNextRolloverTime;
7. DWORD dwState;
8. DWORD dwCurrentRolloverStatus;
9. [string] wchar\_t\* pwszActiveKey;
10. [string] wchar\_t\* pwszStandbyKey;
11. [string] wchar\_t\* pwszNextKey;
12. DWORD dwReserved;
13. } DNS\_RPC\_SKD\_STATE,
14. \*PDNS\_RPC\_SKD\_STATE;

**dwRpcStructureVersion:**  The structure version number; this MUST be set to 0x00000001.

**dwReserved0:**  MUST be set to zero when sent and MUST be ignored on receipt.

**Guid:**  A unique identifier for this signing key descriptor.

**ftLastRolloverTime:**  The time at which the last successful rollover event was performed for this signing key descriptor. This value MUST be 0 if no rollover has been performed on this signing key descriptor.

**ftNextRolloverTime:**  The time at which the next rollover for this signing key descriptor is scheduled. This MAY be 0 if no rollover event is scheduled. When the time comes for a key rollover to start, the signing key descriptor is added to the Rollover Queue, and its **dwCurrentRolloverStatus** is changed to DNS\_SKD\_STATUS\_QUEUED. If another signing key descriptor in the zone is in the process of rolling, **ftNextRolloverTime** MAY represent a time in the past.

**dwState:**  The current state of this signing key descriptor. This MUST be set to one of the following values.[<47>](#Appendix_A_47)

| Value | Meaning |
| --- | --- |
| DNS\_SKD\_STATE\_ACTIVE  0x00000000 | The signing key descriptor is active and in use for [**online signing**](#gt_d4d668bc-02db-4c88-a2e8-255f067104b4) of the zone. |
| DNS\_SKD\_STATE\_RETIRED  0x00000001 | The signing key descriptor is no longer in use for online signing. |

**dwCurrentRolloverStatus:**  The current rollover status of this signing key descriptor. This MUST be set to one of the following values, representing the various stages of key rollover as described in [[RFC4641]](http://go.microsoft.com/fwlink/?LinkId=225979) and [[RFC5011]](http://go.microsoft.com/fwlink/?LinkId=225980):

| Value | Meaning |
| --- | --- |
| DNS\_SKD\_STATUS\_NOT\_ROLLING  0x00000000 | The signing key descriptor is not currently in the process of rolling over keys. |
| DNS\_SKD\_STATUS\_QUEUED  0x00000001 | This signing key descriptor is waiting for another rollover to complete before its rollover can begin. After the signing key descriptor reaches the head of the Rollover Queue, the signing key descriptor will move into the DNS\_SKD\_STATUS\_ROLL\_STARTED state. |
| DNS\_SKD\_STATUS\_ROLL\_STARTED  0x00000002 | This signing key descriptor has begun the process of key rollover. Signing key descriptors representing [**ZSKs**](#gt_14f37d22-0ca6-4a19-b423-9b40463092b6) will move from this state to the DNS\_SKD\_STATUS\_ZSK\_WAITING\_FOR\_DNSKEY\_TTL state, and signing key descriptors representing KSKs will move from this state to the DNS\_SKD\_STATUS\_KSK\_WAITING\_FOR\_DS\_UPDATE state. |
| DNS\_SKD\_STATUS\_ZSK\_WAITING\_FOR\_DNSKEY\_TTL  0x00000003 | This ZSK signing key descriptor is waiting for the previous key to expire in all caching resolvers (it is waiting for the DNSKEY TTL to expire). The signing key descriptor will next move into the DNS\_SKD\_STATUS\_ZSK\_WAITING\_FOR\_MAXZONE\_TTL state. |
| DNS\_SKD\_STATUS\_ZSK\_WAITING\_FOR\_MAXZONE\_TTL  0x00000004 | This ZSK signing key descriptor is waiting for the signatures using the previous key to expire in all caching resolvers (it is waiting for the largest record TTL to expire). This is the final state for ZSK rollovers. The signing key descriptor will move into the DNS\_SKD\_STATUS\_NOT\_ROLLING state when this portion of key rollover is complete. |
| DNS\_SKD\_STATUS\_KSK\_WAITING\_FOR\_DS\_UPDATE  0x00000005 | This KSK signing key descriptor is waiting for a DS record corresponding to the new key to appear in the parent zone. If DS records are found in the parent zone, the server MUST set the zone's "ParentHasSecureDelegation" property to 0x00000001 and continue to wait until the parent's DS record set includes the new key, at which point the signing key descriptor will move into the DNS\_SKD\_STATUS\_KSK\_WAITING\_FOR\_DS\_TTL state. If no DS records are found in the parent zone, the server MUST set the zone's "ParentHasSecureDelegation" property to 0x00000000 and transition the signing key descriptor into the DNS\_SKD\_STATUS\_KSK\_WAITING\_FOR\_DNSKEY\_TTL state. If there is an error or if the presence of a DS record set in the parent zone cannot be determined, the server MUST continue to attempt to query for this record set for up to 15 minutes if the zone's "ParentHasSecureDelegation" property is 0x00000000 or until the "PokeZoneKeyRollover" command is received if it is 0x00000001. |
| DNS\_SKD\_STATUS\_KSK\_WAITING\_FOR\_DS\_TTL  0x00000006 | This KSK signing key descriptor is waiting for the DS record set in the parent zone to expire in all caching resolvers (it is waiting for the parent DS TTL to expire). If the zone's "RFC5011KeyRollovers" property is TRUE, the signing key descriptor will next move into the DNS\_SKD\_STATUS\_WAITING\_FOR\_5011\_REMOVE\_HOLD\_DOWN state. Otherwise, this is a final state for KSK rollovers, and signing key descriptors will move into the DNS\_SKD\_STATUS\_NOT\_ROLLING state when this portion of key rollover is complete. |
| DNS\_SKD\_STATUS\_KSK\_WAITING\_FOR\_DNSKEY\_TTL  0x00000007 | This KSK signing key descriptor is waiting for the previous key to expire in all caching resolvers (it is waiting for the DNSKEY TTL to expire). This is a final state for KSK rollovers, and signing key descriptors will move into the DNS\_SKD\_STATUS\_NOT\_ROLLING state when this portion of key rollover is complete. |
| DNS\_SKD\_STATUS\_KSK\_WAITING\_FOR\_5011\_REMOVE\_HOLD\_DOWN  0x00000008 | This KSK signing key descriptor is waiting for the RFC5011 remove hold-down time before the revoked previous key can be removed. This is a final state for KSK rollovers, and signing key descriptors will move into the DNS\_SKD\_STATUS\_NOT\_ROLLING state when this portion of key rollover is complete. |
| DNS\_SKD\_STATUS\_ROLL\_ERROR  0x00000009 | This signing key descriptor experienced an unrecoverable error during the key rollover. |

**pwszActiveKey:**  Signing key pointer string for the signing key descriptor's currently active key. This is the key that is currently being used to sign zone records.

**pwszStandbyKey:**  Signing key pointer string for the signing key descriptor's standby key. The key represented by this string has several different roles depending on the associated signing key descriptor's "fIsKSK" flag and its "dwRolloverStatus":

* If the signing key descriptor's "fIsKSK" flag is TRUE, pwszStandbyKey represents the "double signature" key as described in [RFC4641] section 4.2.2, also depicted as the "standby" key in [RFC5011] section 6.
* If the signing key descriptor's "fIsKSK" flag is FALSE, **pwszStandbyKey** will generally be NULL unless the SKD is in the process of key rollover:
  + If the signing key descriptor's "dwRolloverStatus" is DNS\_SKD\_STATUS\_ZSK\_WAITING\_FOR\_DNSKEY\_TTL, **pwszStandbyKey** represents the "pre-publish" key as described in [RFC4641] section 4.2.1.1.
  + If the signing key descriptor's "dwRolloverStatus" is DNS\_SKD\_STATUS\_ZSK\_WAITING\_FOR\_MAXZONE\_TTL, **pwszStandbyKey** represents the previously active key during the "new RRSIGs" phase of Pre-Publish Key Rollover, as described in [RFC4641] section 4.2.1.1.

**pwszNextKey:**  Signing key pointer string for the signing key descriptor's next key. The key represented by this string has several different roles depending on the associated signing key descriptor's "fIsKSK" flag:

* If the signing key descriptor's "fIsKSK" flag is TRUE, **pwszNextKey** represents the next key that will be consumed during key rollover. It is not published in the zone and is not used to sign any other records. If the zone's "RFC5011KeyRollovers" property is TRUE, this key becomes the next "standby" key according to [RFC5011]. Otherwise, this key is used as the "double signature" key according to [RFC4641] as the signing key descriptor's key rollover process begins.
* If the signing key descriptor's "fIsKSK" flag is FALSE, **pwszNextKey** represents the "pre-publish" key as described in [RFC4641] section 4.2.1.1. When the SKD is in the process of key rollover, **pwszNextKey** may be populated with a newly generated post-rollover "pre-publish" key.

**dwReserved:**  MUST be set to zero when sent and MUST be ignored on receipt.

##### DNS\_RPC\_TRUST\_POINT

The DNS\_RPC\_TRUST\_POINT structure contains information about a trust point or a node in the "TrustAnchors" zone.

1. typedef struct \_DnssrvRpcTrustPoint {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. [string] char\* pszTrustPointName;
5. TRUSTPOINT\_STATE eTrustPointState;
6. \_\_int64 i64LastActiveRefreshTime;
7. \_\_int64 i64NextActiveRefreshTime;
8. \_\_int64 i64LastSuccessfulActiveRefreshTime;
9. DWORD dwLastActiveRefreshResult;
10. DWORD dwReserved;
11. } DNS\_RPC\_TRUST\_POINT,
12. \*PDNS\_RPC\_TRUST\_POINT;

**dwRpcStructureVersion:**  The structure version number; it MUST be set to 0x00000001.

**dwReserved0:**  MUST be set to zero when sent and MUST be ignored on receipt.

**pszTrustPointName:**  The FQDN of the trust point or node in the "TrustAnchors" zone represented by this structure. This MUST be a non-empty, non-null string.

**eTrustPointState:**  An enum containing the current trust point state. This MUST be set to one of the following values.

| Value | Meaning |
| --- | --- |
| TRUSTPOINT\_STATE\_INITIALIZED  0x00000000 | This structure represents a node in the "TrustAnchors" zone that does not contain any trust anchors. This node is not a trust point. |
| TRUSTPOINT\_STATE\_DSPENDING  0x00000001 | This trust point contains only DS trust anchors (trust anchors in the TRUSTANCHOR\_STATE\_DSPENDING or TRUSTANCHOR\_STATE\_DSINVALID state), rendering it unusable for DNSSEC proofs. |
| TRUSTPOINT\_STATE\_ACTIVE  0x00000002 | This trust point contains at least one trust anchor in the TRUSTANCHOR\_STATE\_VALID or TRUSTANCHOR\_STATE\_MISSING state. |
| TRUSTPOINT\_STATE\_DELETE\_PENDING  0x00000003 | This trust point contains only trust anchors in the TRUSTANCHOR\_STATE\_REVOKED state. |

**i64LastActiveRefreshTime:** The time of the last [**active refresh**](#gt_79ac1b1f-1063-4f6f-8d2f-ec034c123ec6). This is set to zero to indicate that no active refresh has occurred. This is a 64-bit value representing the number of 100-nanosecond intervals since January 1, 1601 [**Coordinated Universal Time (UTC)**](#gt_f2369991-a884-4843-a8fa-1505b6d5ece7).

**i64NextActiveRefreshTime:**  The scheduled time of the next active refresh, or zero to indicate that no active refresh is scheduled. This is a 64-bit value representing the number of 100-nanosecond intervals since January 1, 1601 (UTC).

**i64LastSuccessfulActiveRefreshTime:**  The time of the last successful active refresh, or zero to indicate that no active refresh has occurred. This is a 64-bit value representing the number of 100-nanosecond intervals since January 1, 1601 (UTC). A successful active refresh is defined as an active refresh resulting in retrieval of one or more DNSKEY records for the trust point and, if this trust point has trust anchors in the TRUSTANCHOR\_STATE\_VALID state, signifies that one or more of the retrieved DNSKEY records was validated by DNSSEC.

**dwLastActiveRefreshResult:**  The result of the last active refresh, either ERROR\_SUCCESS or a nonzero value to indicate that an error has occurred.

**dwReserved:**  MUST be set to zero when sent and MUST be ignored on receipt.

##### DNS\_RPC\_TRUST\_POINT\_LIST

The DNS\_RPC\_TRUST\_POINT\_LIST structure contains zero or more [DNS\_RPC\_TRUST\_POINT](#Section_4bcc003085254d94bc79c057e3f650d1) structures.

1. typedef struct \_DnssrvRpcTrustPointList {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. [range(0,500000)] DWORD dwTrustPointCount;
5. [size\_is(dwTrustPointCount)] PDNS\_RPC\_TRUST\_POINT TrustPointArray[];
6. } DNS\_RPC\_TRUST\_POINT\_LIST,
7. \*PDNS\_RPC\_TRUST\_POINT\_LIST;

**dwRpcStructureVersion:**  The structure version number; this MUST be set to 0x00000001.

**dwReserved0:**  MUST be set to zero when sent and MUST be ignored on receipt.

**dwTrustPointCount:**  The size of the **TrustPointArray** array.

**TrustPointArray:**  An array of pointers to DNS\_RPC\_TRUST\_POINT structures.

##### DNS\_RPC\_TRUST\_ANCHOR

The DNS\_RPC\_TRUST\_ANCHOR structure contains information about a trust anchor.

1. typedef struct \_DnssrvRpcTrustAnchor {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. WORD wTrustAnchorType;
5. WORD wKeyTag;
6. WORD wRRLength;
7. TRUSTANCHOR\_STATE eTrustAnchorState;
8. \_\_int64 i64EnteredStateTime;
9. \_\_int64 i64NextStateTime;
10. DWORD dwReserved;
11. [size\_is(wRRLength)] BYTE RRData[];
12. } DNS\_RPC\_TRUST\_ANCHOR,
13. \*PDNS\_RPC\_TRUST\_ANCHOR;

**dwRpcStructureVersion:**  The structure version number; this MUST be set to 0x00000001.

**dwReserved0:**  MUST be set to zero when sent and MUST be ignored on receipt.

**wTrustAnchorType:**  The DNS record type corresponding to the trust anchor. This MUST be set to one of the following values.

| Value | Meaning |
| --- | --- |
| DNS\_TYPE\_DS  0x002B | A DS record type [[RFC4034]](http://go.microsoft.com/fwlink/?LinkId=107052). |
| DNS\_TYPE\_DNSKEY  0x0030 | A DNSKEY record type [RFC4034]. |

**wKeyTag:**  The DNSSEC key tag for this trust anchor. The key tag for a DS record trust anchor MUST match the value of the record’s "Key Tag" field (see [RFC4034]). The key tag for a DNSKEY record trust anchor MUST match the value calculated for the DNSKEY record (see [RFC4034] Appendix B), with the exception that the REVOKE bit of the DNSKEY flags field MUST be set to zero before the calculation.

**wRRLength:**  The length of the **RRData** array.

**eTrustAnchorState:**  The current state of the trust anchor. This MUST be one of the following values.

| Value | Meaning |
| --- | --- |
| TRUSTANCHOR\_STATE\_DSPENDING  0x00000001 | This **trust anchor** can be replaced with a matching DNSKEY trust anchor when the associated trust point has had a successful active refresh. If this state is set, **wTrustAnchorType** MUST be DNS\_TYPE\_DS. |
| TRUSTANCHOR\_STATE\_DSINVALID  0x00000002 | The associated **trust point** has had a successful active refresh, but no DNSKEY record was found that matches this trust anchor. If this state is set, **wTrustAnchorType** MUST be DNS\_TYPE\_DS. |
| TRUSTANCHOR\_STATE\_ADDPEND  0x00000003 | This **trust anchor** will become valid after the expiration of the RFC 5011 add hold-down time (see [[RFC5011]](http://go.microsoft.com/fwlink/?LinkId=225980)). This corresponds to the "AddPend" state in RFC 5011. |
| TRUSTANCHOR\_STATE\_VALID  0x00000004 | This **trust anchor** is trusted for DNSSEC proofs because it was either explicitly added by the administrator or became valid after the expiration of the RFC 5011 add hold-down time (see [RFC5011]). This corresponds to the "Valid" state in RFC 5011. |
| TRUSTANCHOR\_STATE\_MISSING  0x00000005 | This trust anchor was in the TRUSTANCHOR\_STATE\_VALID state but was missing in the last successful active refresh. It is still trusted for DNSSEC proofs. This corresponds to the "Valid" state in [RFC5011]. |
| TRUSTANCHOR\_STATE\_REVOKED  0x00000006 | This **trust anchor** has been marked as revoked by the administrator for the **trust point**'s zone. It can never again be trusted for DNSSEC proofs. This corresponds to the "Revoked" state in [RFC5011]. |

**i64EnteredStateTime:**  The time at which this trust anchor entered its current state. This is a 64-bit value representing the number of 100-nanosecond intervals since January 1, 1601 (UTC).

**i64NextStateTime:**  The time at which this trust anchor is scheduled to exit the current state. This is a 64-bit value representing the number of 100-nanosecond intervals since January 1, 1601 (UTC). The meaning is dependent on the value of **eTrustAnchorState**.

| Value of eTrustAnchorState | Meaning |
| --- | --- |
| TRUSTANCHOR\_STATE\_DSPENDING  0x00000001 | Reserved. The value of **i64NextStateTime** MUST be set to zero when sent and MUST be ignored on receipt. |
| TRUSTANCHOR\_STATE\_DSINVALID  0x00000002 | Reserved. The value of **i64NextStateTime** MUST be set to zero when sent and MUST be ignored on receipt. |
| TRUSTANCHOR\_STATE\_ADDPEND  0x00000003 | This **trust anchor** is scheduled to enter the TRUSTANCHOR\_STATE\_VALID state on or after the value of **i64NextStateTime**. This MUST be equivalent to the value of **i64EnteredStateTime** added to the value of the add hold-down time (see [RFC5011]). |
| TRUSTANCHOR\_STATE\_VALID  0x00000004 | Reserved. The value of **i64NextStateTime** MUST be set to zero when sent and MUST be ignored on receipt. |
| TRUSTANCHOR\_STATE\_MISSING  0x00000005 | Reserved. The value of **i64NextStateTime** MUST be set to zero when sent and MUST be ignored on receipt. |
| TRUSTANCHOR\_STATE\_REVOKED  0x00000006 | This **trust anchor** will become eligible for deletion on or after the value of i64NextStateTime. This MUST be equivalent to the value of **i64EnteredStateTime** added to the value of the remove hold-down time (see [RFC5011]). |

**dwReserved:**  MUST be set to zero when sent and MUST be ignored on receipt.

**RRData:**  Binary data in the same format as [DNS\_RPC\_RECORD\_DNSKEY (section 2.2.2.2.4.15)](#Section_a9d25f0622b8468c944a5ec60a801a45) if **wTrustAnchorType** is DNS\_TYPE\_DNSKEY, or binary data in the same format as [DNS\_RPC\_RECORD\_DS (section 2.2.2.2.4.12)](#Section_ea58fdc5daae41569a00c76a9062b060) if **wTrustAnchorType** is DNS\_TYPE\_DS.

##### DNS\_RPC\_TRUST\_ANCHOR\_LIST

The DNS\_RPC\_TRUST\_ANCHOR\_LIST structure contains zero or more [DNS\_RPC\_TRUST\_ANCHOR](#Section_3ac97d1e7f7b4cd3aa24ccbde00ef0be) structures.

1. typedef struct \_DnssrvRpcTrustAnchorList {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. [range(0,500000)] DWORD dwTrustAnchorCount;
5. [size\_is(dwTrustAnchorCount)] PDNS\_RPC\_TRUST\_ANCHOR TrustAnchorArray[];
6. } DNS\_RPC\_TRUST\_ANCHOR\_LIST,
7. \*PDNS\_RPC\_TRUST\_ANCHOR\_LIST;

**dwRpcStructureVersion:**  The structure version number; this MUST be set to 0x00000001.

**dwReserved0:**  MUST be set to zero when sent and MUST be ignored on receipt.

**dwTrustAnchorCount:**  The size of the **TrustAnchorArray** array.

**TrustAnchorArray:**  An array of pointers to DNS\_RPC\_TRUST\_ANCHOR structures.

##### DNS\_RPC\_SIGNING\_VALIDATION\_ERROR

The DNS\_RPC\_SIGNING\_VALIDATION\_ERROR structure describes an error that occurred during the use of an SKD.

1. typedef struct \_DnssrvRpcSigningValidationError {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. GUID guidSKD;
5. [string] wchar\_t\* pwszSigningKeyPointerString;
6. DWORD dwExtendedError;
7. DWORD dwReserved;
8. } DNS\_RPC\_SIGNING\_VALIDATION\_ERROR,
9. \*PDNS\_RPC\_SIGNING\_VALIDATION\_ERROR;

**dwRpcStructureVersion:**  The structure version number; this MUST be set to 0x00000001.

**dwReserved0:**  MUST be set to zero when sent and MUST be ignored on receipt.

**guidSKD:**  The unique identifier for the signing key descriptor that caused the validation error.

**pwszSigningKeyPointerString:**  The signing key pointer string of the signing key that caused the validation error.

**dwExtendedError:**  MUST be set to zero when sent.

**dwReserved:**  MUST be set to zero when sent and MUST be ignored on receipt.

##### DNS\_RPC\_ZONE\_DNSSEC\_SETTINGS

The DNS\_RPC\_ZONE\_DNSSEC\_SETTINGS structure[<48>](#Appendix_A_48) represents the DNSSEC properties of a zone.

1. typedef struct DnssrvRpcZoneDnssecSettings  {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. DWORD fIsSigned;
5. DWORD fSignWithNSEC3;
6. DWORD fNSEC3OptOut;
7. DWORD dwMaintainTrustAnchor;
8. DWORD fParentHasSecureDelegation;
9. DWORD dwDSRecordAlgorithms;
10. DWORD fRFC5011KeyRollovers;
11. BYTE bNSEC3HashAlgorithm;
12. BYTE bNSEC3RandomSaltLength;
13. WORD wNSEC3IterationCount;
14. LPWSTR pwszNSEC3UserSalt;
15. DWORD dwDNSKEYRecordSetTtl;
16. DWORD dwDSRecordSetTtl;
17. DWORD dwSignatureInceptionOffset;
18. DWORD dwSecureDelegationPollingPeriod;
19. DWORD dwPropagationTime;
20. DWORD cbNSEC3CurrentSaltLength;
21. PBYTE pbNSEC3CurrentSalt;
22. GUID CurrentRollingSKDGuid;
23. DWORD pdwBufferLength;
24. PBYTE ppBuffer;
25. DWORD dwCount;
26. PDNS\_RPC\_ZONE\_SKD pZoneSkdArray;
27. } DNS\_RPC\_ZONE\_DNSSEC\_SETTINGS,
28. \*PDNS\_RPC\_ZONE\_DNSSEC\_SETTINGS;

**dwRpcStructureVersion:**  The structure version number; this MUST be set to 0x00000001.

**dwReserved0:**  MUST be set to zero when sent and MUST be ignored on receipt.

**fIsSigned:**  States whether or not the zone is signed.

**fSignWithNSEC3:**  States whether the zone has NSEC3 Authenticated Denial of Existence support.

**fNSEC3OptOut:**  States whether the zone has unsecure delegations.

**dwMaintainTrustAnchor:**  States whether Trust Anchors are maintained for this zone.

**fParentHasSecureDelegation:**  Delegation Status (Secure\UnSecure) for this zone from the parent.

**dwDSRecordAlgorithms:**  Algorithms used for generating a hash of the DNSKEY record.

**fRFC5011KeyRollovers:**  5011 rollover status (Enabled\Disabled) for this zone.

**bNSEC3HashAlgorithm:**  Algorithm used for generating NSEC3 hash (see [[RFC5155]](http://go.microsoft.com/fwlink/?LinkId=225981) section 5).

**bNSEC3RandomSaltLength:**  Length of Salt used in generating NSEC3 records for this zone (see [RFC5155] section 5).

**wNSEC3IterationCount:**  Iteration count for generating NSEC3 records for this zone (see [RFC5155] section 5).

**pwszNSEC3UserSalt:**  User defined salt used for generating NSEC3 records for this zone (see [RFC5155] section 5).

**dwDNSKEYRecordSetTtl:**  Time-to-live (TTL) for the DNSKEY resource record.

**dwDSRecordSetTtl:**  TTL for the DS Resource Record.

**dwSignatureInceptionOffset:**  Time in seconds for Inception of Signatures for RRSIGs as defined in [[RFC4034]](http://go.microsoft.com/fwlink/?LinkId=107052) section 3.1.5.

**dwSecureDelegationPollingPeriod:**  The interval, in seconds, to refresh the set of delegation signer (DS) records in a secure delegation.

**dwPropagationTime:**  The time, in seconds, that it takes for zone data changes to propagate to other copies of the zone.

**cbNSEC3CurrentSaltLength:**  Length of the Current User salt for building an NSEC3 chain of zone records.

**pbNSEC3CurrentSalt:**  Pointer to the pwszNSEC3UserSalt for building an NSEC3 chain of zone records.

**CurrentRollingSKDGuid:**  Unique identifier of a rolling SKD of a zone, if any.

**pdwBufferLength:**  A pointer to an integer that on success contains the length of the buffer pointed to by **ppBuffer**.

**ppBuffer:**  A pointer to a pointer that points to a buffer containing the enumerated records. The buffer is a series of structures beginning with a [DNS\_RPC\_NODE structure (section 2.2.2.2.3)](#Section_cb5539fa67fd40e09ea5468ecc56bd66). The records for the node will be represented by a series of [DNS\_RPC\_RECORD structures (section 2.2.2.2.5)](#Section_ac7939811c6043b8be59cdbb5c4ecb8a). The number of DNS\_RPC\_RECORD structures following a **DNS\_RPC\_NODE** structure is given by the wRecordCount member of **DNS\_RPC\_NODE**.

**dwCount:**  The number of signing key descriptors present in the array of signing key descriptors pointed to by **SkdArray**.

**pZoneSkdArray:**  A list of SKDs for a zone. This is the array of the **DNS\_RPC\_ZONE\_SKD** structure.

##### DNS\_RPC\_ZONE\_SKD

The DNS\_RPC\_ZONE\_SKD structure[<49>](#Appendix_A_49) groups all the properties of a signing key descriptor of a zone.

1. typedef struct DnssrvRpcZoneSKDSettings {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. PDNS\_RPC\_SKD pSkd;
5. PDNS\_RPC\_SKD\_STATE pSkdState;
6. PDNS\_RPC\_SKD\_STATE\_EX pSkdStateEx;
7. } DNS\_RPC\_ZONE\_SKD,
8. \*PDNS\_RPC\_ZONE\_SKD;

**dwRpcStructureVersion:**  The structure version number; this MUST be set to 0x00000001.

**dwReserved0:**  MUST be set to zero when sent and MUST be ignored on receipt.

**pSkd:**  The static properties of a zone SKD. This is a [DNS\_RPC\_SKD structure (section 2.2.6.2.1)](#Section_f7b0ad424cae40fd87c882af83824639).

**pSkdState:**  The dynamic properties of a zone SKD. This is a [DNS\_RPC\_SKD\_STATE structure (section 2.2.6.2.3)](#Section_b211f98844044c14b293bafd114b0eb6).

**pSkdStateEx:**  The extended dynamic properties of a zone SKD. This is a [DNS\_RPC\_SKD\_STATE\_EX structure (section 2.2.6.2.11)](#Section_4578b2654ff9429492d505dbaa845037).

##### DNS\_RPC\_SKD\_STATE\_EX

The DNS\_RPC\_SKD\_STATE\_EX structure [<50>](#Appendix_A_50) represents the collection of extended dynamic configuration information of a signing key descriptor state.

1. typedef struct \_DnsRpcSigningKeyDescriptorStateEx {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. GUID Guid;
5. DWORD dwCurrentRollState;
6. DWORD fManualTrigger;
7. DWORD dwPreRollEventFired;
8. FILETIME ftNextKeyGenerationTime;
9. DWORD dwRevokedOrSwappedDnskeysLength;
10. PBYTE pRevokedOrSwappedDnskeysBuffer;
11. DWORD dwFinalDnskeysLength;
12. PBYTE pFinalDnskeys;
13. KeySignScope eActiveKeyScope;
14. KeySignScope eStandbyKeyScope;
15. KeySignScope eNextKeyScope;
16. } DNS\_RPC\_SKD\_STATE\_EX,
17. \*PDNS\_RPC\_SKD\_STATE\_EX;

**dwRpcStructureVersion:**  The structure version number; this MUST be set to 0x00000001.

**dwReserved0:**  This MUST be set to zero when sent and MUST be ignored on receipt.

**Guid:**  A unique identifier for this signing key descriptor.

**dwCurrentRollState:**  The current rollover status of this signing key descriptor. Note that these are DNS Server Management Protocol implementations of the protocol specified rollover states of SKDs in DNS\_RPC\_SKD\_STATE.

| Value | Mapping in DNS\_RPC\_SKD\_STATE |
| --- | --- |
| DNS\_SKD\_ROLL\_STATE\_NOT\_STARTED  0x00000000 | DNS\_SKD\_STATUS\_NOT\_ROLLING |
| DNS\_SKD\_ROLL\_STATE\_ZSK\_SWAP\_ACTIVE\_WITH\_ROLLOVER  0x00000001 | DNS\_SKD\_STATUS\_ZSK\_WAITING\_FOR\_DNSKEY\_TTL |
| DNS\_SKD\_ROLL\_STATE\_ZSK\_FINISH  0x00000002 | DNS\_SKD\_STATUS\_ZSK\_WAITING\_FOR\_MAXZONE\_TTL |
| DNS\_SKD\_ROLL\_STATE\_KSK\_WAITING\_FOR\_DS  0x00000003 | DNS\_SKD\_STATUS\_KSK\_WAITING\_FOR\_DS\_UPDATE |
| DNS\_SKD\_ROLL\_STATE\_KSK\_REVOKE  0x00000004 | DNS\_SKD\_STATUS\_KSK\_WAITING\_FOR\_DS\_TTL  The key is revoked once the rollover is completed. |
| DNS\_SKD\_ROLL\_STATE\_KSK\_FINISH  0x00000005 | DNS\_SKD\_STATUS\_KSK\_WAITING\_FOR\_DS\_TTL  The key is not revoked and is used with the rolled over key-set. |
| DNS\_SKD\_ROLL\_STATE\_MAX  0x00000005 | DNS\_SKD\_STATUS\_KSK\_WAITING\_FOR\_DS\_TTL |
| DNS\_SKD\_STATUS\_ROLL\_ERROR  0x00000009 | This signing key descriptor experienced an unrecoverable error during the key rollover. |

**fManualTrigger:**  TRUE if the rollover was triggered manually.

**dwPreRollEventFired:**  Specifies which prerollover event has been fired.

**ftNextKeyGenerationTime:**  The time at which the next key was added to the zone.

**dwRevokedOrSwappedDnskeysLength:**  The length of the revoked or swapped DNSKEY RRSet.

**pRevokedOrSwappedDnskeysBuffer:**  Presigned DNSKEY RRSet for ZSK swap. This is a pointer to a pointer that points to a buffer containing the enumerated records. The buffer is a series of structures beginning with a [DNS\_RPC\_NODE structure (section 2.2.2.2.3)](#Section_cb5539fa67fd40e09ea5468ecc56bd66). The records for the node will be represented by a series of [DNS\_RPC\_RECORD structures (section 2.2.2.2.5)](#Section_ac7939811c6043b8be59cdbb5c4ecb8a). The number of **DNS\_RPC\_RECORD** structures following a **DNS\_RPC\_NODE** structure is given by the wRecordCount member of **DNS\_RPC\_NODE**.

**dwFinalDnskeysLength:**  Length of presigned DNSKEY RRSet.

**pFinalDnskeys:**  Presigned DNSKEY RRSet Post Rollover. This is a pointer to a pointer that points to a buffer containing the enumerated records. The buffer is a series of structures beginning with a **DNS\_RPC\_NODE** structure. The records for the node will be represented by a series of **DNS\_RPC\_RECORD** structures. The number of **DNS\_RPC\_RECORD** structures following a **DNS\_RPC\_NODE** structure is given by the wRecordCount member of **DNS\_RPC\_NODE**.

**eActiveKeyScope:**  Signing key scope for the SKD's active key. The signing key scope is defined in [KeySignScope (section 2.2.6.1.2)](#Section_b67bcf7387b5449a91c9b470ea42b038).

**eStandbyKeyScope:**  Signing key scope for the SKD's standby key. The signing key scope is defined in KeySignScope.

**eNextKeyScope:**  Signing key scope for the SKD's next key. The signing key scope is defined in KeySignScope.

### Application Directory Partition Messages

#### Enumerations and Constants

##### DNS\_RPC\_DP\_FLAGS

The DNS\_RPC\_DP\_FLAGS enumeration is used by the DNS server to indicate the state of an application directory partition.[<51>](#Appendix_A_51) Any combination of the values below MAY be specified, with the exception that, of the following values, more than one MUST NOT be specified: DNS\_DP\_LEGACY, DNS\_DP\_DOMAIN\_DEFAULT, and DNS\_DP\_FOREST\_DEFAULT.

If a root hint zone is found in any application directory partition that is not marked with either DNS\_DP\_LEGACY or DNS\_DP\_DOMAIN\_DEFAULT, then the DNS server MUST ignore it.

| Constant/value | Description |
| --- | --- |
| DNS\_DP\_AUTOCREATED  0x00000001 | The application directory partition was automatically created by the DNS server. This flag is set whenever either the DNS\_DP\_DOMAIN\_DEFAULT or DNS\_DP\_FOREST\_DEFAULT flags are set. |
| DNS\_DP\_LEGACY  0x00000002 | This application directory partition represents the default naming context in the directory server. This flag is set when the application directory partition's DN matches "CN=MicrosoftDNS, CN=System" appended with the value of the **defaultNamingContext** attribute of the root DN. |
| DNS\_DP\_DOMAIN\_DEFAULT  0x00000004 | This application directory partition is replicated across all DNS servers in the [**Active Directory domain**](#gt_fcaec097-23d5-4b8f-b3e7-5739cc9c1d78). This flag is set when the application directory partition's DN matches the value of the "DomainDirectoryPartitionBaseName" DNS server string property (surrounded by "CN=" and ",") and appended with the value of the **defaultNamingContext** attribute of the root DN. |
| DNS\_DP\_FOREST\_DEFAULT  0x00000008 | This application directory partition is replicated across all DNS servers in the [**Active Directory forest**](#gt_9bf0a16f-e546-41f1-9e45-50655e20beb5). This flag is set when the application directory partition's DN matches the value of the "ForestDirectoryPartitionBaseName" DNS server string property (surrounded by "CN=" and ",") appended with the value of the **rootDomainNamingContext** attribute of the root DN. |
| DNS\_DP\_ENLISTED  0x00000010 | This flag indicates that the DNS server is enlisted in this application directory partition. It is set when the value of the local directory server's dsServiceName attribute (the DN for the local directory server) is present in either the **msDS-NC-Replica-Locations** or **msDS-NC-RO-Replica-Locations** [<52>](#Appendix_A_52) attributes (sections 2.380-2.381) of the application directory partition [**crossRef object**](#gt_353fac65-0774-4ba8-8081-eb4c963f94e7) (see section 6.1.1.2.1.1.5). |
| DNS\_DP\_DELETED  0x00000020 | This application directory partition is in the process of being deleted by the directory server. This flag is set when, during a poll of the application directory partitions, an application directory partition that was present during a previous poll is no longer present. If this application directory partition is not present in the directory server the next time the DNS server polls for application directory partition information, the DNS server MUST remove all zones stored in this application directory partition from the in-memory DNS Zone Table (section [3.1.1](#Section_e72286df3e4c45359a0ce9cc944248c2)) and MUST remove this application directory partition from the in-memory Application Directory Partition Table (section 3.1.1). |

#### Structures

##### DNS\_RPC\_DP\_INFO

The DNS\_RPC\_DP\_INFO structure represents the current state of an application directory partition on the directory server.[<53>](#Appendix_A_53)

1. typedef struct \_DnssrvRpcDirectoryPartition {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. [string] char\* pszDpFqdn;
5. [string] wchar\_t\* pszDpDn;
6. [string] wchar\_t\* pszCrDn;
7. DWORD dwFlags;
8. DWORD dwZoneCount;
9. DWORD dwState;
10. DWORD dwReserved[3];
11. [string] wchar\_t\* pwszReserved[3];
12. [range(0,10000)] DWORD dwReplicaCount;
13. [size\_is(dwReplicaCount)] PDNS\_RPC\_DP\_REPLICA ReplicaArray[];
14. } DNS\_RPC\_DP\_INFO,
15. \*PDNS\_RPC\_DP\_INFO;

**dwRpcStructureVersion:**  The structure version number; this value MUST be set to 0x00000000.

**dwReserved0:**  MUST be set to zero when sent and MUST be ignored on receipt.

**pszDpFqdn:**  A pointer to a null-terminated UTF-8 string that specifies the FQDN of the application directory partition. This value is read from the **dnsRoot** attribute of the partition crossRef object (see **pszCrDn**) converted to UTF-8 for this application directory partition.

**pszDpDn:**  A pointer to a null-terminated Unicode string that specifies the distinguished name for the application directory partition [**naming context root**](#gt_d6dac363-88bc-4250-914d-b62364e36ad8) object. This is the value of the **nCName** attribute of the application directory partition crossRef object (see **pszCrDn**).

**pszCrDn:**  A pointer to a null-terminated Unicode string that specifies the distinguished name for the application directory partition crossRef object (located beneath "CN=Partitions, CN=Configuration, <Forest DN>").

**dwFlags:**  The application directory partition properties; this MUST be set to a combination of allowed values for DNS\_RPC\_DP\_FLAGS (section [2.2.7.1.1](#Section_27e378aad4d743de8b343e5b957a7130)).

**dwZoneCount:**  The number of zones from this application directory partition that are loaded in the DNS server's memory. This value is incremented or decremented in the Application Directory Partition Table whenever a DNS Zone Table entry corresponding to a zone in this application directory partition is initialized or deleted, respectively.

**dwState:**  The current state of this application directory partition. This MUST be set to one of the following values:

| Value | Meaning | Source |
| --- | --- | --- |
| DNS\_DP\_OKAY  0x00000000 | The application directory partition is running and ready for all operations. | The Application Directory Partition naming context root object's **instanceType** attribute has neither DS\_INSTANCETYPE\_NC\_COMING (0x00000010), nor the DS\_INSTANCETYPE\_NC\_GOING ( 0x00000020) bit set. |
| DNS\_DP\_STATE\_REPL\_INCOMING  0x00000001 | The application directory partition is replicating onto the directory server but has not completed an initial synchronization so will be ignored for the time being. | The Application Directory Partition naming context root object's **instanceType** attribute has the ( DS\_INSTANCETYPE\_NC\_COMING ( 0x00000010) bit set. |
| DNS\_DP\_STATE\_REPL\_OUTGOING  0x00000002 | The application directory partition is being deleted from the directory server and so will be ignored. | The Application Directory Partition naming context root object's **instanceType** attribute has the S\_INSTANCETYPE\_NC\_GOING ( 0x00000020) bit set. |
| DNS\_DP\_STATE\_UNKNOWN  0x00000003 | The application directory partition state is unavailable for unknown reasons. | The Application Directory Partition naming context root object's **instanceType** attribute is unavailable due to an error condition. |

**dwReserved:**  MUST be set to zero when sent and MUST be ignored on receipt.

**pwszReserved:**  MUST be set to zero when sent and MUST be ignored on receipt.

**dwReplicaCount:**  The number of replication locations for the application directory partition. This value MUST be between 0 and 10000. This value is calculated from the values of the **msDS-NC-Replica-Locations** and **msDS-NC-RO-Replica-Locations**[<54>](#Appendix_A_54)attributes of the application directory partition crossRef object (see **pszCrDn**), as the sum of the number of DNs listed in each attribute.

**ReplicaArray:**  Array of DNS\_RPC\_DP\_REPLICA (section [2.2.7.2.2](#Section_9528535cd6a444a29c6f964e8adefa56)), that contains information about replication locations for this application directory partition. This structure is populated from the values of the **msDS-NC-Replica-Locations** (section 2.380) and **msDS-NC-RO-Replica-Locations** (section 2.381) attributes of the application directory partition crossRef object (see **pszCrDn**). Failure to read any of those attributes will be treated as if no replica exists for that attribute.

##### DNS\_RPC\_DP\_REPLICA

The DNS\_RPC\_DP\_REPLICA structure contains information about an application directory partition replica by giving a distinguished name which can be used to uniquely identify the replica.[<55>](#Appendix_A_55)

1. typedef struct \_DnssrvRpcDirectoryPartitionReplica {
2. [string] wchar\_t\* pszReplicaDn;
3. } DNS\_RPC\_DP\_REPLICA,
4. \*PDNS\_RPC\_DP\_REPLICA;

**pszReplicaDn:**  A pointer to a null-terminated Unicode string that specifies the distinguished name that identifies a specific directory server.

##### DNS\_RPC\_DP\_ENUM

The DNS\_RPC\_DP\_ENUM structure contains abbreviated information about an application directory partition.[<56>](#Appendix_A_56)

1. typedef struct \_DnssrvRpcDirectoryPartitionEnum {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. [string] char\* pszDpFqdn;
5. DWORD dwFlags;
6. DWORD dwZoneCount;
7. } DNS\_RPC\_DP\_ENUM,
8. \*PDNS\_RPC\_DP\_ENUM;

**dwRpcStructureVersion:**  As specified in section [2.2.7.2.1](#Section_bd2a817d6a6940d3befc0c198a9c6e80).

**dwReserved0:**  As specified in section 2.2.7.2.1.

**pszDpFqdn:**  As specified in section 2.2.7.2.1.

**dwFlags:**  As specified in section 2.2.7.2.1.

**dwZoneCount:**  As specified in section 2.2.7.2.1.

##### DNS\_RPC\_DP\_LIST

The DNS\_RPC\_DP\_LIST structure contains a list of application directory partition information structures.[<57>](#Appendix_A_57)

1. typedef struct \_DnssrvRpcDirectoryPartitionList {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. [range(0,5000)] DWORD dwDpCount;
5. [size\_is(dwDpCount)] PDNS\_RPC\_DP\_ENUM DpArray[];
6. } DNS\_RPC\_DP\_LIST,
7. \*PDNS\_RPC\_DP\_LIST;

**dwRpcStructureVersion:**  As specified in section [2.2.7.2.1](#Section_bd2a817d6a6940d3befc0c198a9c6e80).

**dwReserved0:**  As specified in section 2.2.7.2.1.

**dwDpCount:**  The number of DNS\_RPC\_DP\_ENUM (section [2.2.7.2.3](#Section_324a939828c6463f93f68505904dc738)) structures present in the array pointed to by DpArray.

**DpArray:**  An array of DNS\_RPC\_DP\_ENUM structures (section 2.2.7.2.3), containing information about the application directory partitions available to the DNS server.

##### DNS\_RPC\_ENLIST\_DP

The DNS\_RPC\_ENLIST\_DP structure contains the information required to create, delete or enumerate application directory partitions.[<58>](#Appendix_A_58)

1. typedef struct \_DnssrvRpcEnlistDirPart {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. [string] char\* pszDpFqdn;
5. DWORD dwOperation;
6. } DNS\_RPC\_ENLIST\_DP,
7. \*PDNS\_RPC\_ENLIST\_DP;

**dwRpcStructureVersion:**  The DNS management structure version number; this value MUST be set to 0x00000001.

**dwReserved0:**  As specified in section [2.2.7.2.1](#Section_bd2a817d6a6940d3befc0c198a9c6e80).

**pszDpFqdn:**  As specified in section 2.2.7.2.1.

**dwOperation:**  The application directory partition operation to be performed by the DNS server; this MUST be set to one of the following values:

| Value | Meaning |
| --- | --- |
| DNS\_DP\_OP\_CREATE  0x00000001 | Create and enlist (DNS\_DP\_OP\_ENLIST) a new application directory partition. |
| DNS\_DP\_OP\_DELETE  0x00000002 | Delete an existing application directory partition. If the application directory partition has been marked DNS\_DP\_AUTOCREATED, DNS\_DP\_LEGACY, DNS\_DP\_DOMAIN\_DEFAULT, DNS\_DP\_FOREST\_DEFAULT, or DNS\_DP\_DELETED, as specified in section [2.2.7.1.1](#Section_27e378aad4d743de8b343e5b957a7130), or if the DNS server cannot connect and bind to the [**FSMO role owner**](#gt_de81e9fd-25f5-4e90-aadb-1d35c5e8a06b), then the server MUST return an error. |
| DNS\_DP\_OP\_ENLIST  0x00000003 | Enlist this DNS server in an existing application directory partition. If the application directory partition has been marked DNS\_DP\_ENLISTED or DNS\_DP\_DELETED, as specified in section 2.2.7.1.1, then the DNS server MUST return an error. |
| DNS\_DP\_OP\_UNENLIST  0x00000004 | Un-enlist this DNS server from an existing application directory partition. If the application directory partition has been marked DNS\_DP\_DELETED, as specified in section 2.2.7.1.1, then the DNS server MUST return an error. |
| DNS\_DP\_OP\_CREATE\_DOMAIN  0x00000005 | Create a domain partition on the directory server if one does not already exist. |
| DNS\_DP\_OP\_CREATE\_FOREST  0x00000006 | Create a forest partition on the directory server if it does not already exist. |

##### DNS\_RPC\_ZONE\_CHANGE\_DP

The DNS\_RPC\_ZONE\_CHANGE\_DP structure contains information required to move a zone to a different application directory partition on the DNS server.[<59>](#Appendix_A_59)

1. typedef struct \_DnssrvRpcZoneChangePartition {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. [string] char\* pszDestPartition;
5. } DNS\_RPC\_ZONE\_CHANGE\_DP,
6. \*PDNS\_RPC\_ZONE\_CHANGE\_DP;

**dwRpcStructureVersion:**  As specified in section [2.2.7.2.5](#Section_7f445256e1694f1ea244d4223fbdf604).

**dwReserved0:**  As specified in section [2.2.7.2.1](#Section_bd2a817d6a6940d3befc0c198a9c6e80).

**pszDestPartition:**  A pointer to a null-terminated UTF-8 string that specifies the distinguished name for a new application directory partition to which a zone is to be moved.

### AutoConfig Messages

#### Enumerations and Constants

##### DNS\_RPC\_AUTOCONFIG

The DNS\_RPC\_AUTOCONFIG enumeration specifies a set of autoconfiguration operations to be immediately performed by the DNS server. Any combination of the values below can be specified, with the exception of the following values, of which at most one value may be specified: DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT, DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_PREPEND, and DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_APPEND. An implementation SHOULD[<60>](#Appendix_A_60) support all values in this table.

If the DNS server will act as the first DNS server for a new domain in a new forest (2) , the following values SHOULD[<61>](#Appendix_A_61) be specified: DNS\_RPC\_AUTOCONFIG\_INTERNAL\_ROOTHINTS, DNS\_RPC\_AUTOCONFIG\_INTERNAL\_FORWARDERS, and DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT.

If the DNS server will act as a DNS server in an existing domain on a writeable domain controller, the following values SHOULD be specified: DNS\_RPC\_AUTOCONFIG\_INTERNAL\_ROOTHINTS, DNS\_RPC\_AUTOCONFIG\_INTERNAL\_FORWARDERS, and DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_APPEND.

In all other cases, including a DNS server for a new child domain or a DNS server operating on a [**read only domain controller (RODC)**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870), the following values SHOULD be specified: DNS\_RPC\_AUTOCONFIG\_INTERNAL\_ROOTHINTS, DNS\_RPC\_AUTOCONFIG\_INTERNAL\_FORWARDERS, and DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_PREPEND.

The DNS server performs autoconfiguration in the following order: root hints, forwarders, self-pointing, and zone creation.

The DNS server SHOULD[<62>](#Appendix_A_62) ignore any bit value not specified in the table below, with one exception: A value of 0x00000000 MUST be treated identically to 0xFFFFFFFF (DNS\_RPC\_AUTOCONFIG\_ALL).

| Constant/value | Description |
| --- | --- |
| DNS\_RPC\_AUTOCONFIG\_INTERNAL\_ROOTHINTS  0x00000001 | The server automatically configures root hints. To construct root hints, the server sends a DNS query of type NS for the DNS root name to each of the DNS servers and for each of the local machine's network adapters. The server builds its root hints by selecting the set of NS records that appear in each of the aforementioned NS query responses. If the DNS server cannot find a non-empty set of root hints, it performs no action. |
| DNS\_RPC\_AUTOCONFIG\_INTERNAL\_FORWARDERS  0x00000002 | The server automatically configures forwarders. To construct forwarders, the DNS server locates a peer DNS server by sending a DNS query of type NS for the domain name specified in the **pszNewDomainName** field of DNS\_RPC\_AUTOCONFIGURE (section [2.2.8.2.1](#Section_414cf6fba8884c5591a46f77dff66cbe)). For each peer server, the DNS server performs a ServerInfo query (section [3.1.4.7](#Section_a90a44f0f64e44b09e35a7fc49f6adea)). The DNS server uses the set of forwarders in the result of this query from the first peer available. If no peer servers with forwarders can be found, the DNS server collects all of the DNS servers for each of the local machine's network adapters and uses the resulting list of IP addresses as the new list of forwarders. |
| DNS\_RPC\_AUTOCONFIG\_INTERNAL\_ZONES  0x00000004 | If the AdminConfigured DNS server property (section [3.1.1.1.1](#Section_8903e50a91834a7d964053f6f5a91481)) has been set to a nonzero value, the server takes no action. Otherwise, the server checks to see whether it is the only DC in the forest. If the server is not a DC or is not the only DC in the forest, the server MUST perform no action. To determine whether the server is the only DC in the forest, it performs an LDAP query on the local directory server using the LDAP filter "(objectCategory=ntdsDsa)" with the credentials of the user who initiated the autoconfigure operation or the DNS Server Credentials (section [3.1.1](#Section_e72286df3e4c45359a0ce9cc944248c2)) if user credentials are not available. If the LDAP result count is one, the server can assume that it is the only DC in the forest. If the local directory server does not respond or does not generate a result, then further processing of DNS\_RPC\_AUTOCONFIG\_INTERNAL\_ZONES MUST halt, with ERROR\_SUCCESS returned.  If the AdminConfigured DNS server property (section 3.1.1.1.1) is zero and the DNS server is the only DC in the forest, the DNS server SHOULD look up the locally configured name of the domain of which the server is a member, and construct two zone names: one equal to the domain name and one equal to the domain name prepended by the string "\_msdcs." If neither of these zones currently exists on the DNS server, the DNS server SHOULD create both of these zones. |
| DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT  0x00000010 | The server automatically replaces the server list with the appropriate loop-back address. If this flag is specified, then the server MUST ignore the DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_PREPEND and DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_APPEND flags. |
| DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_PREPEND  0x00000020 | The server automatically inserts the appropriate loop-back address at the start of the server list. If this flag is specified, then the server MUST ignore the DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_APPEND flag. |
| DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_APPEND  0x00000040 | The server automatically inserts the appropriate loop-back address at the end of the server list. |
| DNS\_RPC\_AUTOCONFIG\_INTERNAL\_RETURN\_ERRORS  0x00008000 | If this flag is set then the server will return the errors that it encounters while performing auto-configuration; else ERROR\_SUCCESS will always be returned. |
| DNS\_RPC\_AUTOCONFIG\_ALL  0xFFFFFFFF | The server performs all autoconfiguration operations. |

#### Structures

##### DNS\_RPC\_AUTOCONFIGURE

The DNS\_RPC\_AUTOCONFIGURE structure contains the information required to auto-configure the DNS server.

1. typedef struct \_DnsRpcAutoConfigureLonghorn {
2. DWORD dwRpcStructureVersion;
3. DWORD dwReserved0;
4. DWORD dwAutoConfigFlags;
5. DWORD dwReserved1;
6. [string] char\* pszNewDomainName;
7. } DNS\_RPC\_AUTOCONFIGURE,
8. \*PDNS\_RPC\_AUTOCONFIGURE;

**dwRpcStructureVersion:**  The structure version number; this value MUST be set to 0x00000000.

**dwReserved0:**  MUST be set to zero when sent and MUST be ignored on receipt.

**dwAutoConfigFlags:**  The autoconfiguration operation being requested by the client as specified in DNS\_RPC\_AUTOCONFIG (section [2.2.8.1.1](#Section_d02b0aa23a704f66a63709bd55f6ec6d)).

**dwReserved1:**  MUST be set to zero when sent and MUST be ignored on receipt.

**pszNewDomainName:**  A pointer to a null-terminated UTF-8 string which contains the name of the directory server domain that this DNS server is about to join.

### Logging Messages

#### Enumerations and Constants

##### DNS\_LOG\_LEVELS

The DNS\_LOG\_LEVELS bit field is a 32-bit integer that specifies the various filters and options that can be configured for the DNS server to log packet exchange information to the server log file. There are four layers of filtering:

* Content filter: Filters on the function (that is, the DNS opcode) of the content of a packet.
* Type filter: Filters on whether the packet is a question or an answer.
* Direction filter: Filters on the network direction of the packet (received or sent).
* Transport filter: Filters on the transport mechanism (TCP or UDP).

Since filters are applied independently, and a packet is logged only if allowed by all filters, setting all bits for any given filter to zero indicates that no packets are to be logged.

Bits other than those listed in the following table can be set to any arbitrary value when sent, and MUST be ignored on receipt.

| Constant/value | Description |
| --- | --- |
| DNS\_LOG\_LEVEL\_QUERY  0x00000001 | The server allows query packet exchanges through the content filter. |
| DNS\_LOG\_LEVEL\_NOTIFY  0x00000010 | The server allows packet exchanges related to zone exchange through the content filter. |
| DNS\_LOG\_LEVEL\_UPDATE  0x00000020 | The server allows packet exchanges related to zone updates through the content filter. |
| DNS\_LOG\_LEVEL\_QUESTIONS  0x00000100 | The server allows packets containing questions through the type filter. |
| DNS\_LOG\_LEVEL\_ANSWERS  0x00000200 | The server allows packets containing answers through the type filter. |
| DNS\_LOG\_LEVEL\_SEND  0x00001000 | The server allows packets it sends out through the direction filter. |
| DNS\_LOG\_LEVEL\_RECV  0x00002000 | The server allows packets it receives through the direction filter. |
| DNS\_LOG\_LEVEL\_UDP  0x00004000 | The server allows UDP packet exchange through the transport filter. |
| DNS\_LOG\_LEVEL\_TCP  0x00008000 | The server allows TCP packet exchange through the transport filter. |
| DNS\_LOG\_LEVEL\_ALL\_PACKETS  0x0000FFFF | The server logs operations that fulfill the following filter set: DNS\_LOG\_LEVEL\_SEND or DNS\_LOG\_LEVEL\_RECV, or DNS\_LOG\_LEVEL\_TCP or DNS\_LOG\_LEVEL\_UDP, or DNS\_LOG\_LEVEL\_QUERY or DNS\_LOG\_LEVEL\_NOTIFY or DNS\_LOG\_LEVEL\_UPDATE, or DNS\_LOG\_LEVEL\_QUESTIONS or DNS\_LOG\_LEVEL\_ANSWERS. |
| DNS\_LOG\_LEVEL\_DS\_WRITE  0x00010000 | Independent of the values of the other filters, logs Active Directory write operations. |
| DNS\_LOG\_LEVEL\_DS\_UPDATE  0x00020000 | Independent of the values of the other filters, logs Active Directory polling operations and operations during DNS updates (secure and unsecure) on Active Directory integrated zones. |
| DNS\_LOG\_LEVEL\_FULL\_PACKETS  0x01000000 | If allowed by the filters, the server logs the entire packet to the log file. |
| DNS\_LOG\_LEVEL\_UNMATCHED\_RESPONSE  0x02000000 | If allowed by the filters, the server logs response packets that do not match any outstanding query.[<63>](#Appendix_A_63) |
| DNS\_LOG\_LEVEL\_WRITE\_THROUGH  0x80000000 | If allowed by the filters, the server saves packet logging information to persistent storage. |

##### DNS\_EVENTLOG\_TYPES

The DNS server can enable several levels of event-logging. This MUST be set to one of the values specified below:

| Constant/value | Description |
| --- | --- |
| EVENT\_LOG\_SUCCESS  0x00000000 | The server will log events for all successful operations. |
| EVENT\_LOG\_ERROR\_TYPE  0x00000001 | The server will log events for all operations that result in an error. |
| EVENT\_LOG\_WARNING\_TYPE  0x00000002 | The server will log events for all operations that result in a warning. |
| EVENT\_LOG\_INFORMATION\_TYPE  0x00000004 | The server will log events for all operations for informative purposes. |

### Server Statistics Messages

#### Enumerations and Constants

##### DNSSRV\_STATID\_TYPES

The DNSSRV\_STATID\_TYPES is a 32-bit integer that enumerates the possible types of DNS server statistics. When requesting statistics, these values may be combined to request multiple statistics buffers in the same operation. When statistics are returned, each DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)) contains a value in the **StatId** field with a single bit set to indicate the type of statistics that are contained in the associated buffer.

| Constant/value | Description |
| --- | --- |
| DNSSRV\_STATID\_TIME  0x00000001 | If the **StatId** field is set in the request, a DNSSRV\_TIME\_STATS (section [2.2.10.2.4](#Section_238b54f6bfdf4bb891ccc5ddbde6e7ac)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_QUERY  0x00000002 | If the **StatId** field is set in the request, a DNSSRV\_QUERY\_STATS (section [2.2.10.2.5](#Section_3fe0d4da23f74371854bbb480fb21586)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_QUERY2  0x00000004 | If the **StatId** field is set in the request, a DNSSRV\_QUERY2\_STATS (section [2.2.10.2.6](#Section_538b073821f247e5b2120b4b858fdaca)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_RECURSE  0x00000008 | If the **StatId** field is set in the request, a DNSSRV\_RECURSE\_STATS (section [2.2.10.2.7](#Section_402dd0cf46f646fda58a088fddc04a73)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_MASTER  0x00000010 | If the **StatId** field is set in the request, a DNSSRV\_MASTER\_STATS (section [2.2.10.2.9](#Section_80779ec12b52499eaecc7018d0cf58a1)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_SECONDARY  0x00000020 | If the **StatId** field is set in the request, a DNSSRV\_SECONDARY\_STATS (section [2.2.10.2.10](#Section_e047d72501084f7f857f8665c1021694)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_WINS  0x00000040 | If the **StatId** field is set in the request, a DNSSRV\_WINS\_STATS (section [2.2.10.2.11](#Section_49da9ba8b2df42aa93cb6ad7f8eb287f)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_WIRE\_UPDATE  0x00000100 | If the **StatId** field is set in the request, a DNSSRV\_UPDATE\_STATS (section [2.2.10.2.12](#Section_3c28e68edae6444b93a5416607d9002a)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_SKWANSEC  0x00000200 | If the **StatId** field is set in the request, a DNSSRV\_SKWANSEC\_STATS (section [2.2.10.2.13](#Section_8a9bf38fcda6485083bc6fa59936c988)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_DS  0x00000400 | If the **StatId** field is set in the request, a DNSSRV\_DS\_STATS (section [2.2.10.2.14](#Section_02cbf8802d26454499d773294b664a78)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_NONWIRE\_UPDATE  0x00000800 | If the **StatId** field is set in the request, a DNSSRV\_UPDATE\_STATS (section 2.2.10.2.12) structure will be included in the output buffer. |
| DNSSRV\_STATID\_MEMORY  0x00010000 | If the **StatId** field is set in the request, a DNSSRV\_MEMORY\_STATS (section [2.2.10.2.16](#Section_303ccf5702b4411da6e5d741e00aebd1)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_TIMEOUT  0x00020000 | If the **StatId** field is set in the request, a DNSSRV\_TIMEOUT\_STATS (section [2.2.10.2.17](#Section_ada3c79feb75473d980961243f108609)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_DBASE  0x00040000 | If the **StatId** field is set in the request, a DNSSRV\_DBASE\_STATS (section [2.2.10.2.18](#Section_3c4ae7e2344542018aaf992933ed02c3)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_RECORD  0x00080000 | If the **StatId** field is set in the request, a DNSSRV\_RECORD\_STATS (section [2.2.10.2.19](#Section_c1e4a7a7cec2441e9e9243eddd7e7e33)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_PACKET  0x00100000 | If the **StatId** field is set in the request, a DNSSRV\_PACKET\_STATS (section [2.2.10.2.20](#Section_b0be7f78ae4c41df9748535bc121a1c6)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_NBSTAT  0x00200000 | If the **StatId** field is set in the request, a DNSSRV\_NBSTAT\_STATS (section [2.2.10.2.21](#Section_eec0b96271844ea7b5653500306a8a3d)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_ERRORS  0x00400000 | If the **StatId** field is set in the request, a DNSSRV\_ERROR\_STATS (section [2.2.10.2.23](#Section_ea5599f0cd27401bb7a3cb96cd501c90)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_CACHE  0x00800000 | If the **StatId** is set in the request, a DNSSRV\_CACHE\_STATS (section [2.2.10.2.24](#Section_9502a725118042ed91d362d3d43e2365)) structure will be included in the output buffer. |
| DNSSRV\_STATID\_DNSSEC  0x01000000 | If the **StatId** is set in the request, a DNSSRV\_CACHE\_DNSSEC (section [2.2.10.2.8](#Section_c56e41c88d99475db497fbc59593880a)) structure will be included in the output buffer.[<64>](#Appendix_A_64) |
| DNSSRV\_STATID\_PRIVATE  0x10000000 | If the **StatId** is set in the request, a DNSSRV\_PRIVATE\_STATS (section [2.2.10.2.22](#Section_2c72272dc8cf451a94a942475acdba45)) structure will be included in the output buffer. |

#### Structures

##### DNSSRV\_STAT\_HEADER

The DNSSRV\_STAT\_HEADER precedes each DNSSRV\_STAT (section [2.2.10.2.2](#Section_c4dd5c55f4344b968bb59d69e28ec7c2)) structure which provides DNS server runtime statistics. This structure MUST be formatted as follows:

1. typedef struct \_DnsStatHeader {
2. DWORD StatId;
3. WORD wLength;
4. BOOLEAN fClear;
5. UCHAR fReserved;
6. } DNSSRV\_STAT\_HEADER,
7. \*PDNSSRV\_STAT\_HEADER;

**StatId:**  The type of statistics contained in the DNSSRV\_STAT structure. This value MUST be set to one of the allowed values specified in section [2.2.10.1.1](#Section_6e5f45dfbf644c53867b2a1157472523).

**wLength:**  The length, in bytes, of the **Buffer** member in the DNSSRV\_STAT structure.

**fClear:**  A Boolean value that indicates whether the server is to clear the statistics buffer for the server attribute indicated at by StatId.

**fReserved:**  MUST be set to zero when sent and MUST be ignored on receipt.

##### DNSSRV\_STATS

The DNSSRV\_STATS structure carries server statistics information. This structure MUST be interpreted as one of the more specific statistics structures specified in sections [2.2.10.2.4](#Section_238b54f6bfdf4bb891ccc5ddbde6e7ac) through [2.2.10.2.24](#Section_9502a725118042ed91d362d3d43e2365), depending upon the StatId value in the Header member. This structure MUST be formatted as follows:

1. typedef struct \_DnsStat {
2. DNSSRV\_STAT\_HEADER Header;
3. BYTE Buffer[1];
4. } DNSSRV\_STAT,
5. \*PDNSSRV\_STAT,
6. \*PDNSSRV\_STATS;

**Header:**  A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**Buffer:**  A variable length array of bytes that contains information specific to the type of DNS server statistics, as specified by the StatId value in the Header.

##### DNS\_SYSTEMTIME

The DNS\_SYSTEMTIME structure stores time values for DNS statistics. It is always populated by the server, which MUST supply valid values. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| wYear | | | | | | | | | | | | | | | | wMonth | | | | | | | | | | | | | | | |
| wDayOfWeek | | | | | | | | | | | | | | | | wDay | | | | | | | | | | | | | | | |
| wHour | | | | | | | | | | | | | | | | wMinute | | | | | | | | | | | | | | | |
| wSecond | | | | | | | | | | | | | | | | wMillisecond | | | | | | | | | | | | | | | |

**wYear (2 bytes):** The year, as a 16-bit, unsigned integer. Valid values are from 1601 to 30827.

**wMonth (2 bytes):** The month from 1 (January) to 12 (December), as a 16-bit, unsigned integer.

**wDayOfWeek (2 bytes):** The day of the week from 0 (Sunday) to 6 (Saturday), as a 16-bit, unsigned integer.

**wDay (2 bytes):** The day of the month from 1 to 31, as a 16-bit, unsigned integer.

**wHour (2 bytes):** The hour from 0 to 23, as a 16-bit, unsigned integer.

**wMinute (2 bytes):** The minute from 0 to 59, as a 16-bit, unsigned integer.

**wSecond (2 bytes):** The second from 0 to 59, as a 16-bit, unsigned integer.

**wMillisecond (2 bytes):** The millisecond from 0 to 999, as a 16-bit, unsigned integer.

##### DNSSRV\_TIME\_STATS

The DNSSRV\_TIME\_STATS structure has the DNS server's time-related statistics. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ServerStartTimeSeconds | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LastClearTimeSeconds | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecondsSinceServerStart | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecondsSinceLastClear | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ServerStartTime (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LastClearTime (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**ServerStartTimeSeconds (4 bytes):** The number of seconds that has elapsed since the server machine was last restarted, that is, the operating system uptime in seconds, as a 32-bit unsigned integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**LastClearTimeSeconds (4 bytes):** The number of seconds that elapsed between the time the server machine was restarted and the last time the server statistics were cleared, that is, the operating system uptime in seconds at the time of the last statistics reset, as a 32-bit unsigned integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**SecondsSinceServerStart (4 bytes):** The number of seconds since the server started, that is, the uptime of the DNS server software in seconds, as a 32-bit unsigned integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**SecondsSinceLastClear (4 bytes):** The number of seconds since the last time that the server statistics were cleared, as a 32-bit unsigned integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ServerStartTime (16 bytes):** A DNS\_SYSTEMTIME (section [2.2.10.2.3](#Section_fc487ec46e26482ca9944f019afe0e4c)) structure that contains the time the server started.

**LastClearTime (16 bytes):** A DNS\_SYSTEMTIME (section 2.2.10.2.3) structure that contains the time the server statistics was last cleared.

##### DNSSRV\_QUERY\_STATS

DNSSRV\_QUERY\_STATS defines a structure that carries the DNS server's statistics values related to query processing over different transports. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpQueries | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpResponses | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpQueriesSent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpResponsesReceived | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpClientConnections | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpQueries | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpResponses | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpQueriesSent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpResponsesReceived | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**UdpQueries (4 bytes):** The cumulative number of queries received over UDP, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**UdpResponses (4 bytes):** The cumulative number of query responses sent over UDP, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**UdpQueriesSent (4 bytes):** The cumulative number of queries sent over UDP by this server to other remote servers, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**UdpResponsesReceived (4 bytes):** The cumulative number of query responses received over UDP by the server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TcpClientConnections (4 bytes):** The cumulative number of TCP connections accepted by this server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TcpQueries (4 bytes):** The cumulative number of queries received over TCP, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TcpResponses (4 bytes):** The cumulative number of query responses sent over TCP, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TcpQueriesSent (4 bytes):** The cumulative number of queries sent over TCP by this server to other remote servers, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TcpResponsesReceived (4 bytes):** The cumulative number of query responses over TCP received by the server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

##### DNSSRV\_QUERY2\_STATS

The DNSSRV\_QUERY2\_STATS structure contains DNS server statistics related to query processing by type. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TotalQueries | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Standard | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Notify | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Update | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TKeyNego (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TypeA | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TypeNs | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TypeSoa | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TypeMx | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TypePtr | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TypeSrv | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TypeAll | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TypeIxfr | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TypeAxfr | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TypeOther | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**TotalQueries (4 bytes):** The total number of queries received by the server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**Standard (4 bytes):** The number of standard DNS queries received by the server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**Notify (4 bytes):** The number of zone notification requests received by the server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**Update (4 bytes):** The number of dynamic update requests received by the server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TKeyNego (4 bytes):** The number of TKEY [[RFC2930]](http://go.microsoft.com/fwlink/?LinkId=90397) negotiation requests received by the server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field. This field SHOULD[<65>](#Appendix_A_65) be present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**TypeA (4 bytes):** The number of queries received for record type DNS\_TYPE\_A, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TypeNs (4 bytes):** The number of queries received for record type DNS\_TYPE\_NS, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TypeSoa (4 bytes):** The number of queries received for record type DNS\_TYPE\_SOA, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TypeMx (4 bytes):** The number of queries received for record type DNS\_TYPE\_MX, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TypePtr (4 bytes):** The number of queries received for record type DNS\_TYPE\_PTR, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TypeSrv (4 bytes):** The number of queries received for record type DNS\_TYPE\_SRV, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TypeAll (4 bytes):** The number of queries received for record type DNS\_TYPE\_ALL, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TypeIxfr (4 bytes):** The number of queries received for record type DNS\_TYPE\_IXFR, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TypeAxfr (4 bytes):** The number of queries received for record type DNS\_TYPE\_AXFR, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TypeOther (4 bytes):** The number of queries received for any other record type not mentioned above, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

##### DNSSRV\_RECURSE\_STATS

The DNSSRV\_RECURSE\_STATS structure has the DNS server's statistics related to recursive resource record lookups. This structure SHOULD[<66>](#Appendix_A_66) be formatted as follows.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ReferralPasses | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| QueriesRecursed | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OriginalQuestionRecursed | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AdditionalRecursed | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TotalQuestionsRecursed | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Retries | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LookupPasses | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Forwards | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sends | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Responses | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ResponseUnmatched | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ResponseMismatched (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ResponseFromForwarder | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ResponseAuthoritative | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ResponseNotAuth | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ResponseAnswer | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ResponseNameError | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ResponseRcode | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ResponseEmpty | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ResponseDelegation | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ResponseNonZoneData | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ResponseUnsecure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ResponseBadPacket | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SendResponseDirect | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ContinueCurrentRecursion | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ContinueCurrentLookup | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ContinueNextLookup | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RootNsQuery | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RootNsResponse | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CacheUpdateAlloc | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CacheUpdateResponse | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CacheUpdateFree | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CacheUpdateRetry | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SuspendedQuery | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ResumeSuspendedQuery | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PacketTimeout | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FinalTimeoutQueued | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FinalTimeoutExpired | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Failures | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecursionFailure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ServerFailure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PartialFailure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CacheUpdateFailure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecursePassFailure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FailureReachAuthority | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FailureReachPreviousResponse | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FailureRetryCount | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpTry | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpConnectFailure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpConnect | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpQuery | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpResponse | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpDisconnect | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DiscardedDuplicateQueries (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DuplicateCoalesedQueries (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| GnzLocalQuery (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| GnzRemoteQuery (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| GnzRemoteResponse (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| GnzRemoteResponseCacheSuccess (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| GnzRemoteResponseCacheFailure (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CacheLockingDiscards (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**ReferralPasses (4 bytes):** The number of times the server returned a referral value, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**QueriesRecursed (4 bytes):** The number of queries received that required recursive lookups, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**OriginalQuestionRecursed (4 bytes):** The number of new recursive queries initiated, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**AdditionalRecursed (4 bytes):** The number of recursions performed to return additional data or CNAME, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TotalQuestionsRecursed (4 bytes):** The number of total recursions including original and additional, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**Retries (4 bytes):** The number of retries performed for recursive queries sent by the server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**LookupPasses (4 bytes):** The number of recursive lookups performed, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**Forwards (4 bytes):** The number of recursive queries sent to forwarding servers, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**Sends (4 bytes):** The total number of recursive queries sent by the server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**Responses (4 bytes):** The number of query responses received by the server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ResponseUnmatched (4 bytes):** The number of responses received for which an outstanding query with a matching transaction-id could not be located, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ResponseMismatched (4 bytes):** The number of responses received for which an outstanding query with a matching transaction-id was located but response was invalid for the query, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field. This field SHOULD be present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**ResponseFromForwarder (4 bytes):** The number of responses received from forwarders, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ResponseAuthoritative (4 bytes):** The number of responses received from the server authoritative for the zone, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ResponseNotAuth (4 bytes):** The number of responses received from a server not authoritative for the zone, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ResponseAnswer (4 bytes):** The number of responses received from other servers for recursive queries, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ResponseNameError (4 bytes):** The number of name errors received by the server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ResponseRcode (4 bytes):** The number of errors other than name errors received by the server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ResponseEmpty (4 bytes):** The number of empty responses received from other servers, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ResponseDelegation (4 bytes):** The number of delegation responses received by the server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ResponseNonZoneData (4 bytes):** The number of error responses when a name is not found in the zone, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ResponseUnsecure (4 bytes):** The number of unsecure responses received when the server is configured to receive secure responses, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ResponseBadPacket (4 bytes):** The number of bad response packets received, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**SendResponseDirect (4 bytes):** The number of responses that the DNS server received from remote servers and sent directly to clients, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ContinueCurrentRecursion (4 bytes):** The number of additional remote queries generated by the DNS server during normal query processing, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ContinueCurrentLookup (4 bytes):** The number of times the server received a response from a remote DNS server while processing a client query and restarted recursion, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ContinueNextLookup (4 bytes):** The number of times the server started a lookup with the next query, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**RootNsQuery (4 bytes):** The number of times the server sent a query for a root name server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**RootNsResponse (4 bytes):** The number of times the server processed a response from one of its root servers, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**CacheUpdateAlloc (4 bytes):** The number of times the server allocated a query to be sent to update a cache entry, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**CacheUpdateResponse (4 bytes):** The number of times the server received responses for a query sent to update a cache entry, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**CacheUpdateFree (4 bytes):** The number of times the server released a query request or response packet sent to update a cache entry, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**CacheUpdateRetry (4 bytes):** The number of times the server reattempted a query to update cache entry information, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**SuspendedQuery (4 bytes):** The number of times the server suspended sending a query needed to update cache entry information, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ResumeSuspendedQuery (4 bytes):** The number of times the server resumed a suspended query that was needed to update cache entry information, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**PacketTimeout (4 bytes):** The number of timed-out recursive queries, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**FinalTimeoutQueued (4 bytes):** The number of recursive queries enlisted to wait for final time-out before they expire, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**FinalTimeoutExpired (4 bytes):** The number of recursive queries expired without the server receiving any response, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**Failures (4 bytes):** Not used. Senders MUST set this value to zero, and receivers MUST ignore it.

**RecursionFailure (4 bytes):** The number of times the server received failures for recursion queries to remote servers, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**ServerFailure (4 bytes):** The number of times the server sent failures to the client, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**PartialFailure (4 bytes):** The number of times the server received failures for recursion queries to remote servers, when it had already received an answer but was looking up additional records, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**CacheUpdateFailure (4 bytes):** The number of times the server received failure for self-generated cache update recursion queries to remote servers, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**RecursePassFailure (4 bytes):** The number of times the server failed to perform recursive lookups on queries, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**FailureReachAuthority (4 bytes):** The number of times the server failed to perform recursive lookups on queries, because it failed to reach an authoritative server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**FailureReachPreviousResponse (4 bytes):** The number of times the server received failure while performing recursive lookup on queries, because the query recursed back to the domain from which a name server had already responded, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**FailureRetryCount (4 bytes):** Not used. Senders MUST set this value to zero, and receivers MUST ignore it.

**TcpTry (4 bytes):** The number of times the server started a recursive query over TCP, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TcpConnectFailure (4 bytes):** Not used. Senders MUST set this value to zero, and receivers MUST ignore it.

**TcpConnect (4 bytes):** The number of times the server successfully established a TCP connection to send a recursive query, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TcpQuery (4 bytes):** The number of times the server sent a recursive query over TCP, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TcpResponse (4 bytes):** The number of times the server received a recursive query response over TCP, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**TcpDisconnect (4 bytes):** The number of times the server disconnected a connection that was established to send a recursive query over TCP to a remote server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field.

**DiscardedDuplicateQueries (4 bytes):** The number of times the server discarded a query that was received from the same client with the same transaction ID when there was already a query with the same query name, type ID, and transaction ID outstanding, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field. This field MUST be present only if ResponseMismatched is present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**DuplicateCoalesedQueries (4 bytes):** The number of times the server coalesced a query that was received from a client while another query with the same query name and type ID was outstanding at the server for processing, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field. This field MUST be present if and only if ResponseMismatched is present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**GnzLocalQuery (4 bytes):** The number of times a [**GNZ**](#gt_4b2ec78c-50a1-4093-8005-d59ecb829f49) lookup query was answered locally, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field. This field SHOULD be present but MUST be absent if ResponseMismatched is absent. A client can tell whether the field is present based on the size of the buffer holding this structure.

**GnzRemoteQuery (4 bytes):** The number of times a GNZ lookup query was sent to a remote server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field. This field MUST be present if and only if GnzLocalQuery is present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**GnzRemoteResponse (4 bytes):** The number of times a GNZ lookup query response was received from a remote server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field. This field MUST be present if and only if GnzLocalQuery is present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**GnzRemoteResponseCacheSuccess (4 bytes):** The number of times a GNZ cache update query response was successfully received from a remote server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field. This field MUST be present if and only if GnzLocalQuery is present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**GnzRemoteResponseCacheFailure (4 bytes):** The number of times the server received failure for GNZ cache update query requests sent to a remote server, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field. This field MUST be present if and only if GnzLocalQuery is present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**CacheLockingDiscards (4 bytes):** The number of times the server discarded a cache update due to cache record locking, as an unsigned 32-bit integer. If the value is greater than 0xFFFFFFFF, then the value modulo 0x100000000 is stored in the field. This field SHOULD[<67>](#Appendix_A_67) be present. A client can tell whether the field is present based on the size of the buffer holding this structure.

##### DNSSRV\_DNSSEC\_STATS

The DNSSRV\_DNSSEC\_STATS structure has the DNS server statistics related a DNSSEC signature or DS digest hash succeeding or failing.[<68>](#Appendix_A_68)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SuccessfulValidations | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FailedValidations | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecursionFailures | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**SuccessfulValidations (4 bytes):** The number of times a validation attempt on a DNSSEC signature or DS digest hash succeeded.

**FailedValidations (4 bytes):** The number of times a validation attempt on a DNSSEC signature or DS digest hash failed.

**RecursionFailures (4 bytes):** The number of times a validating recursive name resolution query attempt failed while fetching DNSSEC data.

##### DNSSRV\_MASTER\_STATS

The DNSSRV\_MASTER\_STATS structure has the DNS server statistics related to overall DNS protocol processing. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NotifySent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Request | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NameError | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FormError | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AxfrLimit | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Refused | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RefuseSecurity | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RefuseShutdown | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RefuseLoading (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RefuseZoneLocked | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RefuseServerFailure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RefuseNotAuth (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RefuseReadOnly (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Failure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AxfrRequest | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AxfrSuccess | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StubAxfrRequest (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrRequest | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrNoVersion | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrUpdateSuccess | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrTcpRequest | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrTcpSuccess | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrAxfr | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrUdpRequest | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrUdpSuccess | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrUdpForceTcp | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrUdpForceAxfr | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**NotifySent (4 bytes):** The number of update notifications sent to secondaries by the server.

**Request (4 bytes):** The number of zone transfer requests received by the server.

**NameError (4 bytes):** The number of name error responses returned by the server.

**FormError (4 bytes):** The number of invalid format error responses returned by the server.

**AxfrLimit (4 bytes):** The number of [**full zone transfer**](#gt_2d944edd-a550-4b8a-98d8-af495aaa2f8f) requests rejected due to time restrictions between successive full zone transfers.

**Refused (4 bytes):** The total number of times the server rejected requests for dynamic updates or zone transfers.

**RefuseSecurity (4 bytes):** The number of times the server rejected zone transfer requests due to secondary security restrictions.

**RefuseShutdown (4 bytes):** The number of times the server rejected zone transfer requests because zone transfer was disabled or because the requesting IP address was not permitted to transfer the zone.

**RefuseLoading (4 bytes):** The number of times the server rejected zone transfer requests, due to a zone not being fully loaded. This field SHOULD be present, but MUST be absent if StubAxfrRequest is absent. [<69>](#Appendix_A_69)A client can tell whether the field is present based on the size of the buffer holding this structure.

**RefuseZoneLocked (4 bytes):** The number of times the server rejected zone transfer requests, due to the zone already being locked for some operation.

**RefuseServerFailure (4 bytes):** The number of times the server rejected zone transfer requests, due to processing failures at the server.

**RefuseNotAuth (4 bytes):** The number of times the server rejected zone transfer requests, because the zone is not authoritative on the server. This field MUST be present if and only if RefuseLoading is present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**RefuseReadOnly (4 bytes):** The number of times the server rejected zone transfer requests, due to the zone being hosted on an RODC. This field MUST be present if and only if RefuseLoading is present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**Failure (4 bytes):** The number of times the server hit a zone transfer failure.

**AxfrRequest (4 bytes):** The number of full zone transfer requests received by the server.

**AxfrSuccess (4 bytes):** The number of full zone transfers successfully completed by the server.

**StubAxfrRequest (4 bytes):** The number of full zone transfer requests received by the server for stub zones. This field SHOULD[<70>](#Appendix_A_70) be present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**IxfrRequest (4 bytes):** The number of [**incremental zone transfer**](#gt_831053cd-38aa-4fcc-81bf-d0cbb6cb573b) requests received by the server.

**IxfrNoVersion (4 bytes):** The number of servers that received an incremental zone transfer request, but there was not a suitable version number available for incremental zone transfer.

**IxfrUpdateSuccess (4 bytes):** The number of success responses for incremental zone transfer sent by the server.

**IxfrTcpRequest (4 bytes):** The number of incremental zone transfer requests received by the server over TCP.

**IxfrTcpSuccess (4 bytes):** The number of success responses for incremental zone transfers sent by the server over TCP.

**IxfrAxfr (4 bytes):** The number of incremental zone transfer requests received by the server, which required a full zone transfer.

**IxfrUdpRequest (4 bytes):** The number of incremental zone transfer requests received by the server over UDP.

**IxfrUdpSuccess (4 bytes):** The number of success responses for incremental zone transfers sent by the server over UDP.

**IxfrUdpForceTcp (4 bytes):** The number of incremental zone transfer requests received by the server over UDP, for which the server responded using TCP.

**IxfrUdpForceAxfr (4 bytes):** The number of incremental zone transfer requests received by the server over UDP, for which the server responded with a full zone transfer.

##### DNSSRV\_SECONDARY\_STATS

The DNSSRV\_SECONDARY\_STATS structure has the DNS server statistics related to secondary zone processing.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NotifyReceived | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NotifyInvalid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NotifyPrimary | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NotifyNonPrimary (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NotifyNoVersion | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NotifyNewVersion | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NotifyCurrentVersion | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NotifyOldVersion | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NotifyMasterUnknown | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SoaRequest | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SoaResponse | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SoaResponseInvalid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SoaResponseNameError | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AxfrRequest | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AxfrResponse | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AxfrSuccess | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AxfrRefused | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AxfrInvalid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StubAxfrRequest (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StubAxfrResponse (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StubAxfrSuccess (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StubAxfrRefused (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StubAxfrInvalid (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrUdpRequest | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrUdpResponse | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrUdpSuccess | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrUdpUseTcp | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrUdpUseAxfr | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrUdpWrongServer | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrUdpNoUpdate | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrUdpNewPrimary | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrUdpFormerr | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrUdpRefused | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrUdpInvalid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrTcpRequest | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrTcpResponse | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrTcpSuccess | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrTcpAxfr | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrTcpFormerr | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrTcpRefused | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IxfrTcpInvalid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**NotifyReceived (4 bytes):** The number of zone notifications received by the server.

**NotifyInvalid (4 bytes):** The number of invalid zone notifications received by the server.

**NotifyPrimary (4 bytes):** The number of zone notifications for primary zones received by the server.

**NotifyNonPrimary (4 bytes):** The number of zone notifications for nonprimary zones received by the server. This field SHOULD[<71>](#Appendix_A_71) be present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**NotifyNoVersion (4 bytes):** The number of zone notifications received by the server, for which the server has no SOA.

**NotifyNewVersion (4 bytes):** The number of zone notifications received by the server, where the received SOA has a newer version number than that of the SOA already present on the server.

**NotifyCurrentVersion (4 bytes):** The number of zone notifications received by the server where the received SOA has same version number as that of the SOA already present on the server.

**NotifyOldVersion (4 bytes):** The number of zone notifications received by the server, where the received SOA has an older version number than the SOA already present on the server.

**NotifyMasterUnknown (4 bytes):** The number of zone notifications received by the server, where notifications are received from a server that is not present in the list of masters for the zone.

**SoaRequest (4 bytes):** The number of SOA query requests sent by the server to zone masters, to initiate zone transfer.

**SoaResponse (4 bytes):** The number of SOA responses received by the server from the zone master.

**SoaResponseInvalid (4 bytes):** The number of invalid SOA responses received by the server from the zone master.

**SoaResponseNameError (4 bytes):** Not used, the receiver MUST ignore this value.

**AxfrRequest (4 bytes):** The number of full zone transfer requests sent by the server.

**AxfrResponse (4 bytes):** The number of full zone transfer responses received by the server.

**AxfrSuccess (4 bytes):** The number of full zone transfer success responses received by the server.

**AxfrRefused (4 bytes):** The number of full zone transfer rejection responses received by the server.

**AxfrInvalid (4 bytes):** The number of full zone transfer invalid responses received by the server.

**StubAxfrRequest (4 bytes):** The number of full zone transfer requests sent by the server for stub zones. This field MUST be present if and only if NotifyNonPrimary is present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**StubAxfrResponse (4 bytes):** The number of full zone transfer responses received by the server for stub zones. This field MUST be present if and only if NotifyNonPrimary is present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**StubAxfrSuccess (4 bytes):** The number of full zone transfer success responses received by the server for stub zones. This field MUST be present if and only if NotifyNonPrimary is present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**StubAxfrRefused (4 bytes):** The number of full zone transfer rejection responses received by the server. This field MUST be present if and only if NotifyNonPrimary is present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**StubAxfrInvalid (4 bytes):** The number of full zone transfer invalid responses received by the server. This field MUST be present if and only if NotifyNonPrimary is present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**IxfrUdpRequest (4 bytes):** The number of incremental zone transfer requests sent by the server over UDP.

**IxfrUdpResponse (4 bytes):** The number of incremental zone transfer success responses received by the server over UDP.

**IxfrUdpSuccess (4 bytes):** The number of incremental zone transfer success responses received by the server over UDP.

**IxfrUdpUseTcp (4 bytes):** The number of incremental zone transfer responses received by the server over UDP, indicating that TCP is needed.

**IxfrUdpUseAxfr (4 bytes):** The number of incremental zone transfer responses received by the server over UDP, indicating that full zone transfer is needed.

**IxfrUdpWrongServer (4 bytes):** The number of incremental zone transfer responses received by the server over UDP, where the remote sender is not among the masters for this zone.

**IxfrUdpNoUpdate (4 bytes):** The number of incremental zone transfer responses received by the server over UDP, where no updates were found and hence no zone transfer is needed.

**IxfrUdpNewPrimary (4 bytes):** The number of incremental zone transfer responses received by the server over UDP, where the SOA indicates a new primary server name.

**IxfrUdpFormerr (4 bytes):** The number of incremental zone transfer responses received by the server over UDP, where either the master does not support incremental zone transfer or the master indicated that the zone transfer request was malformed.

**IxfrUdpRefused (4 bytes):** The number of incremental zone transfer rejection responses received by the server over UDP.

**IxfrUdpInvalid (4 bytes):** The number of incremental zone transfer invalid responses received by the server over UDP.

**IxfrTcpRequest (4 bytes):** The number of incremental zone transfer requests sent by the server over TCP.

**IxfrTcpResponse (4 bytes):** The number of incremental zone transfer success responses received by the server over TCP.

**IxfrTcpSuccess (4 bytes):** The number of incremental zone transfer success responses received by the server over TCP.

**IxfrTcpAxfr (4 bytes):** The number of incremental zone transfer responses received by the server over TCP, indicating that full zone transfer is needed.

**IxfrTcpFormerr (4 bytes):** The number of incremental zone transfer responses received by the server over TCP, where either the primary DNS server does not support incremental zone transfer or the primary DNS server indicated that the zone transfer request was malformed.

**IxfrTcpRefused (4 bytes):** The number of incremental zone transfer rejection responses received by the server over TCP.

**IxfrTcpInvalid (4 bytes):** The number of incremental zone transfer invalid responses received by the server over TCP.

##### DNSSRV\_WINS\_STATS

The DNSSRV\_WINS\_STATS structure has DNS server statistics related to WINS lookups. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| WinsLookups | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| WinsResponses | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| WinsReverseLookups | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| WinsReverseResponses | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**WinsLookups (4 bytes):** The number of WINS lookup requests received by the server.

**WinsResponses (4 bytes):** The number of WINS responses sent by the server.

**WinsReverseLookups (4 bytes):** The number of reverse WINS lookup requests received by the server.

**WinsReverseResponses (4 bytes):** The number of reverse WINS lookup responses sent by the server.

##### DNSSRV\_UPDATE\_STATS

The DNSSRV\_UPDATE\_STATS structure has DNS server statistics related to dynamic updates processing. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Received | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Empty | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NoOps | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Completed | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rejected | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FormErr | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NxDomain | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NotImpl | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Refused | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| YxDomain | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| YxRrset | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NxRrset | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NotAuth | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NotZone | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RefusedNonSecure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RefusedAccessDenied | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecureSuccess | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecureContinue | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecureFailure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecureDsWriteFailure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsSuccess | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsWriteFailure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| unused\_was\_Collisions | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| unused\_was\_CollisionsRead | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| unused\_was\_CollisionsWrite | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| unused\_was\_CollisionsDsWrite | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Queued | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Retry | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Timeout | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| InQueue | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Forwards | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpForwards | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ForwardResponses | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ForwardTimeouts | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ForwardInQueue | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UpdateType (156 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**Received (4 bytes):** The number of dynamic update requests received by the server.

**Empty (4 bytes):** The number of empty dynamic update requests received by the server.

**NoOps (4 bytes):** The number of no-op dynamic update requests (such as a dynamic update request with no update records) received by the server.

**Completed (4 bytes):** The number of completed dynamic update requests received by the server.

**Rejected (4 bytes):** The number of dynamic update requests rejected by the server.

**FormErr (4 bytes):** The number of dynamic update requests rejected by the server, due to malformed packets.

**NxDomain (4 bytes):** The number of dynamic update requests rejected by the server, due to name error.

**NotImpl (4 bytes):** The number of dynamic update requests rejected by the server, due to unimplemented functionality.

**Refused (4 bytes):** The number of dynamic update requests rejected by the server, due to malformed packets.

**YxDomain (4 bytes):** The number of dynamic update requests rejected by the server, due to policy restrictions.

**YxRrset (4 bytes):** The number of dynamic update requests rejected by the server, due to an unknown domain name.

**NxRrset (4 bytes):** The number of dynamic update requests rejected by the server, due to an unknown resource record name.

**NotAuth (4 bytes):** The number of dynamic update requests rejected by the server, due to the server not being authoritative for the zone.

**NotZone (4 bytes):** The number of dynamic update requests rejected by the server, due to the zone name not being recognized as one for which it is authoritative.

**RefusedNonSecure (4 bytes):** The number of dynamic update requests rejected by the server, due to a non-secure update request received for a zone where secure updates are required.

**RefusedAccessDenied (4 bytes):** The number of dynamic update requests rejected by the server, due to a failure to update records in the directory server.

**SecureSuccess (4 bytes):** The number of [**secure dynamic update**](#gt_20cbcdff-fbb7-4c77-9ccc-4787afd75eb7) requests received by the server that were successfully applied.

**SecureContinue (4 bytes):** Not used. Senders MUST set this value to zero and the receiver MUST ignore it

**SecureFailure (4 bytes):** The number of secure dynamic update requests received by the server that could not be successfully applied.

**SecureDsWriteFailure (4 bytes):** The number of secure dynamic update requests received by the server that the server failed to update in the directory server.

**DsSuccess (4 bytes):** The number of unsecure dynamic update requests received by the server, that were successfully updated in the directory server.

**DsWriteFailure (4 bytes):** The number of unsecure dynamic update requests received by the server that the server failed to update in the directory server.

**unused\_was\_Collisions (4 bytes):** MUST be set to zero when sent and MUST be ignored on receipt.

**unused\_was\_CollisionsRead (4 bytes):** MUST be set to zero when sent and MUST be ignored on receipt.

**unused\_was\_CollisionsWrite (4 bytes):** MUST be set to zero when sent and MUST be ignored on receipt.

**unused\_was\_CollisionsDsWrite (4 bytes):** MUST be set to zero when sent and MUST be ignored on receipt.

**Queued (4 bytes):** The number of updates packets received that needed to be sent to other remote servers.

**Retry (4 bytes):** MUST be set to zero when sent and MUST be ignored on receipt.

**Timeout (4 bytes):** The number of update packets received, that timed-out while waiting to update the remote server.

**InQueue (4 bytes):** The number of update packets received which are waiting in the update queue for updates to complete on the remote server.

**Forwards (4 bytes):** The number of update packets received that were forwarded to other servers.

**TcpForwards (4 bytes):** The number of update packets received over TCP that were forwarded to other servers.

**ForwardResponses (4 bytes):** The number of response packets received for the update requests that were forwarded to other servers.

**ForwardTimeouts (4 bytes):** The number of update packets which timed out waiting for a response from other servers.

**ForwardInQueue (4 bytes):** The number of update packets forwarded to other servers and which are waiting for a response.

**UpdateType (156 bytes):** An array of counters that keep track of the number of update requests received for different DNS record types. This array has a total of 39 entries from DNS\_TYPE\_ZERO to DNS\_TYPE\_DNAME.

##### DNSSRV\_SKWANSEC\_STATS

The DNSSRV\_SKWANSEC\_STATS structure has DNS server statistics related to [**security context**](#gt_88d49f20-6c95-4b64-a52c-c3eca2fe5709) processing. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecContextCreate | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecContextFree | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecContextQueue | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecContextQueueInNego | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecContextQueueNegoComplete | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecContextQueueLength | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecContextDequeue | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecContextTimeout | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecPackAlloc | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecPackFree | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecTkeyInvalid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecTkeyBadTime | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecTsigFormerr | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecTsigEcho | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecTsigBadKey | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecTsigVerifySuccess | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecTsigVerifyFailed | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**SecContextCreate (4 bytes):** The number of security contexts created by the server since the server was started.

**SecContextFree (4 bytes):** The number of security contexts released by the server since the server was started.

**SecContextQueue (4 bytes):** The total number of security contexts in the queue for negotiation on the server since the server was started.

**SecContextQueueInNego (4 bytes):** The number of security contexts entered in negotiation since the server was started.

**SecContextQueueNegoComplete (4 bytes):** The number of security contexts that have completed negotiation since the server was started.

**SecContextQueueLength (4 bytes):** The number of security contexts currently queued.

**SecContextDequeue (4 bytes):** The total number of security contexts removed from the queue for negotiation since the server was started.

**SecContextTimeout (4 bytes):** The total number of security contexts in the negotiation list that timed out since the server was started.

**SecPackAlloc (4 bytes):** The number of buffers allocated by the server for use with GSS-API signature validation.

**SecPackFree (4 bytes):** The number of buffers for use with GSS-API signature validation released by the server.

**SecTkeyInvalid (4 bytes):** The number of secure DNS update messages from which TKEY was successfully retrieved.

**SecTkeyBadTime (4 bytes):** The number of secure DNS update messages that had TKEY with a skewed time stamp.

**SecTsigFormerr (4 bytes):** The number of TSIG records from which signature extraction failed.

**SecTsigEcho (4 bytes):** The number of echo TSIG records received by the server, indicating that the remote server is not security aware. [[RFC2845]](http://go.microsoft.com/fwlink/?LinkId=90388)

**SecTsigBadKey (4 bytes):** The number of TSIG records received for which the cached security context could not be found.

**SecTsigVerifySuccess (4 bytes):** The number of TSIG records received for which the signature was successfully verified.

**SecTsigVerifyFailed (4 bytes):** The number of TSIG records received for which signature verification failed.

##### DNSSRV\_DS\_STATS

The DNSSRV\_DS\_STATS structure has DNS server statistics related to directory server processing. The UpdateLists member through DsWriteType member refer to statistical values, when the server is propagating changes from the in-memory database to the directory server.

This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsTotalNodesRead | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsTotalRecordsRead | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsNodesLoaded | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsRecordsLoaded | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsTombstonesRead | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsUpdateSearches | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsUpdateNodesRead | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsUpdateRecordsRead | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UpdateLists | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UpdateNodes | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UpdateSuppressed | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UpdateWrites | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UpdateTombstones | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UpdateRecordChange | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UpdateAgingRefresh | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UpdateAgingOn | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UpdateAgingOff | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UpdatePacket | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UpdatePacketPrecon | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UpdateAdmin | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UpdateAutoConfig | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UpdateScavenge | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsNodesAdded | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsNodesModified | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsNodesTombstoned | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsNodesDeleted | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsRecordsAdded | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsRecordsReplaced | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsWriteSuppressed | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsSerialWrites | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LdapTimedWrites | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LdapWriteTimeTotal | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LdapWriteAverage | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LdapWriteMax | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LdapWriteBucket0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LdapWriteBucket1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LdapWriteBucket2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LdapWriteBucket3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LdapWriteBucket4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LdapWriteBucket5 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LdapSearchTime | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FailedDeleteDsEntries | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FailedReadRecords | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FailedLdapModify | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FailedLdapAdd | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PollingPassesWithDsErrors (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LdapReconnects (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DsWriteType (160 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**DsTotalNodesRead (4 bytes):** The total number of DNS nodes read from the directory server.

**DsTotalRecordsRead (4 bytes):** The total number of resource records read from the directory server.

**DsNodesLoaded (4 bytes):** The number of valid DNS nodes found in the directory server and loaded in memory by the server.

**DsRecordsLoaded (4 bytes):** The number of resource records loaded in memory by the server.

**DsTombstonesRead (4 bytes):** The number of nodes read from the directory server and found in a tombstoned state.

**DsUpdateSearches (4 bytes):** The number of zone update searches performed on the directory server.

**DsUpdateNodesRead (4 bytes):** The number of DNS nodes that were read from the directory server and contained updated information.

**DsUpdateRecordsRead (4 bytes):** The number of resource records that were read from the directory server and contained updated information.

**UpdateLists (4 bytes):** The number of in-memory nodes with an updated list of record.

**UpdateNodes (4 bytes):** The number of in-memory nodes that required an update in the directory server.

**UpdateSuppressed (4 bytes):** The number of in-memory nodes that did not require any write to the directory server.

**UpdateWrites (4 bytes):** The number of in-memory nodes that required writing to the directory server.

**UpdateTombstones (4 bytes):** The number of in-memory nodes that required tombstoning.

**UpdateRecordChange (4 bytes):** The number of in-memory nodes that required record changes.

**UpdateAgingRefresh (4 bytes):** The number of in-memory nodes that required an aging information refresh.

**UpdateAgingOn (4 bytes):** The number of in-memory nodes that required aging to be enabled.

**UpdateAgingOff (4 bytes):** The number of in-memory nodes that required aging to be disabled.

**UpdatePacket (4 bytes):** The number of in-memory nodes modified as a result of update packets being received.

**UpdatePacketPrecon (4 bytes):** The number of in-memory nodes modified as a result of update packets being received with prerequisites (as discussed in [[RFC2136]](http://go.microsoft.com/fwlink/?LinkId=107017) section 2.4).

**UpdateAdmin (4 bytes):** The number of in-memory nodes modified as a result of administrator initiated changes.

**UpdateAutoConfig (4 bytes):** The number of in-memory nodes modified as a result of an auto-configure operation.

**UpdateScavenge (4 bytes):** The number of in-memory nodes modified as a result of a scavenging cycle.

**DsNodesAdded (4 bytes):** The number of new nodes added to the directory server.

**DsNodesModified (4 bytes):** The number of nodes modified in the directory server.

**DsNodesTombstoned (4 bytes):** The number of nodes tombstoned in the directory server.

**DsNodesDeleted (4 bytes):** The number of nodes deleted from the directory server.

**DsRecordsAdded (4 bytes):** The number of records added to the directory server.

**DsRecordsReplaced (4 bytes):** The number of records modified or replaced in the directory server.

**DsWriteSuppressed (4 bytes):** The number of records added to the directory server.

**DsSerialWrites (4 bytes):** The number of records that had matching data and hence were not written to the directory server.

**LdapTimedWrites (4 bytes):** The number of times the server performed a timed LDAP write operation.

**LdapWriteTimeTotal (4 bytes):** The cumulative time, in milliseconds, consumed by server-performed timed LDAP write operations.

**LdapWriteAverage (4 bytes):** The average time, in milliseconds, for all server performed timed LDAP write operations since the server was last restarted.

**LdapWriteMax (4 bytes):** The longest duration taken, in milliseconds, for any single server-performed timed LDAP write-operation.

**LdapWriteBucket0 (4 bytes):** The number of LDAP write-operations that took less than 10 milliseconds.

**LdapWriteBucket1 (4 bytes):** The number of LDAP write-operations that took between 10 and 100 milliseconds.

**LdapWriteBucket2 (4 bytes):** The number of LDAP write-operations that took between 100 milliseconds and 1 second.

**LdapWriteBucket3 (4 bytes):** The number of LDAP write-operations that took between 1 and 10 seconds.

**LdapWriteBucket4 (4 bytes):** The number of LDAP write-operations that took between 10 and 100 seconds.

**LdapWriteBucket5 (4 bytes):** The number of LDAP write-operations that took more than 100 seconds.

**LdapSearchTime (4 bytes):** The cumulative time, in milliseconds, consumed by server-performed LDAP searches.

**FailedDeleteDsEntries (4 bytes):** The number of times the server failed to delete entries from the directory server.

**FailedReadRecords (4 bytes):** The number of times the server failed to read records from the directory server.

**FailedLdapModify (4 bytes):** The number of times the server failed to modify records in the directory server.

**FailedLdapAdd (4 bytes):** The number of times the server failed to add entries to the directory server.

**PollingPassesWithDsErrors (4 bytes):** The number of times the server hit failure while polling zones in the directory server. This field SHOULD[<72>](#Appendix_A_72) be present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**LdapReconnects (4 bytes):** The number of times the server attempted to reconnect to the directory server. This field MUST be present if and only if PollingPassesWithDsErrors is present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**DsWriteType (160 bytes):** An array of 32-bit unsigned integers that keeps track of update requests for different DNS record types as specified DNS\_RECORD\_TYPE (section [2.2.2.1.1](#Section_39b03b89226440638198d62f62a6441a)). There are a total of 40 entries each corresponding to the number of received update requests for different record types in the order specified in DNS\_RECORD\_TYPE (section 2.2.2.1.1), starting from DNS\_TYPE\_ZERO to DNS\_TYPE\_DNAME.

##### DNSSRV\_MEMTAG\_STATS

The DNSSRV\_MEMTAG\_STATS structure has DNS server statistics related to memory allocations for a given purpose. This structure is used by DNSSRV\_MEMORY\_STATS (section [2.2.10.2.16](#Section_303ccf5702b4411da6e5d741e00aebd1)) to collect the list of statistics of memory allocated for various purposes. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Alloc | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Free | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Memory | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Alloc (4 bytes):** The cumulative number of times memory allocations have been performed for a given purpose.

**Free (4 bytes):** The cumulative number of times memory has been released for a given purpose.

**Memory (4 bytes):** The total size of memory, in bytes, currently in use for a given purpose.

##### DNSSRV\_MEMORY\_STATS

The DNSSRV\_MEMORY\_STATS structure has DNS server statistics related to memory usage for different operations on the server. It provides statistical information about memory usage since the server started or server statistics were last cleared. The structure supports allocations of two types: blocks of common (but implementation-specific) sizes, and blocks of arbitrary sizes. This allows servers to use a separate internal mechanism to optimize allocations of common sizes if they so choose. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Memory | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Alloc | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Free | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StdUsed | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StdReturn | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StdInUse | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StdMemory | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StdToHeapAlloc | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StdToHeapFree | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StdToHeapInUse | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StdToHeapMemory | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StdBlockAlloc | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StdBlockUsed | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StdBlockReturn | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StdBlockInUse | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StdBlockFreeList | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StdBlockFreeListMemory | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StdBlockMemory | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| MemTags (624 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**Memory (4 bytes):** The total memory currently allocated by the servers, in bytes.

**Alloc (4 bytes):** The cumulative number of times memory was allocated by the server.

**Free (4 bytes):** The cumulative number of times memory was released by the server.

**StdUsed (4 bytes):** The cumulative number of times a common-size block of memory was allocated by the server.

**StdReturn (4 bytes):** The cumulative number of times a common-size block of memory was released by the server.

**StdInUse (4 bytes):** The total number of common-size blocks of allocated memory currently used by the server.

**StdMemory (4 bytes):** The total size, in bytes, of common-size blocks that are currently being used by the server.

**StdToHeapAlloc (4 bytes):** The cumulative number of arbitrary-size blocks of memory allocated from system memory.

**StdToHeapFree (4 bytes):** The cumulative number of arbitrary-size blocks of memory released to system memory.

**StdToHeapInUse (4 bytes):** The number of arbitrary-size blocks of memory currently in use.

**StdToHeapMemory (4 bytes):** The total size of memory, in bytes, currently used by non-standard sized blocks.

**StdBlockAlloc (4 bytes):** The cumulative number of common-size blocks allocated by the server.

**StdBlockUsed (4 bytes):** The cumulative number of common-size blocks allocated from an internal free list.

**StdBlockReturn (4 bytes):** The cumulative number of common-size blocks returned from an internal free list.

**StdBlockInUse (4 bytes):** The number of common-size blocks currently being used.

**StdBlockFreeList (4 bytes):** The number of common-size blocks currently on internal free lists.

**StdBlockFreeListMemory (4 bytes):** The total size of memory, in bytes, of common size blocks currently on internal free lists.

**StdBlockMemory (4 bytes):** The total size of memory, in bytes, of all currently allocated blocks.

**MemTags (624 bytes):** An array of 52 DNSSRV\_MEMTAG\_STATS (section [2.2.10.2.15](#Section_0fbecaa99f8e4e9a8e94e0dd94d87710)) specifying memory statistics for various server operations. The table below gives the context applicable to each element of this array, where the Value column indicates the element number.

| Value | Meaning |
| --- | --- |
| MEMTAG\_NONE  0x00000001 | Not related to a particular operation. |
| MEMTAG\_PACKET\_UDP  0x00000002 | UDP Packets. |
| MEMTAG\_PACKET\_TCP  0x00000003 | TCP Packets. |
| MEMTAG\_NAME  0x00000004 | Name-related operations. |
| MEMTAG\_ZONE  0x00000005 | Zone operations. |
| MEMTAG\_UPDATE  0x00000006 | Name updates. |
| MEMTAG\_UPDATE\_LIST  0x00000007 | Record update list. |
| MEMTAG\_TIMEOUT  0x00000008 | Timeout |
| MEMTAG\_NODEHASH  0x00000009 | Node hash. |
| MEMTAG\_DS\_DN  0x0000000A | Directory server distinguished name. |
| MEMTAG\_DS\_MOD  0x0000000B | Directory server module. |
| MEMTAG\_DS\_RECORD  0x0000000C | Directory server records. |
| MEMTAG\_DS\_OTHER  0x0000000D | Other directory server related operations. |
| MEMTAG\_THREAD  0x0000000E | Thread management. |
| MEMTAG\_NBSTAT  0x0000000F | NBSTAT packets operations. |
| MEMTAG\_DNSLIB  0x00000010 | DNS library management. |
| MEMTAG\_TABLE  0x00000011 | Record table operations. |
| MEMTAG\_SOCKET  0x00000012 | Socket operations. |
| MEMTAG\_CONNECTION  0x00000013 | Connection establishment / destruction. |
| MEMTAG\_REGISTRY  0x00000014 | Registry operations. |
| MEMTAG\_RPC  0x00000015 | RPC operations. |
| MEMTAG\_STUFF  0x00000016 | Miscellaneous operations. |
| MEMTAG\_FILEBUF  0x00000017 | File buffer operations. |
| MEMTAG\_REMOTE  0x00000018 | Remote IP address operations. |
| MEMTAG\_EVTCTRL  0x00000019 | Event control operations. |
| MEMTAG\_SAFE  0x0000001A | Miscellaneous queuing operations. |
| MEMTAG\_RECORD\_UNKNOWN  0x0000001B | Record operations. |
| MEMTAG\_RECORD\_FILE  0x0000001C | File-based operations. |
| MEMTAG\_RECORD\_DS  0x0000001D | Directory server-based RR operations. |
| MEMTAG\_RECORD\_AXFR  0x0000001E | Complete zone transfer operations. |
| MEMTAG\_RECORD\_IXFR  0x0000001F | Single Record transfer operations. |
| MEMTAG\_RECORD\_DYNUP  0x00000020 | RR operations for dynamic update. |
| MEMTAG\_RECORD\_ADMIN  0x00000021 | RR operations for administration. |
| MEMTAG\_RECORD\_AUTO  0x00000022 | RR operations for autoconfig. |
| MEMTAG\_RECORD\_CACHE  0x00000023 | RR operations for cache. |
| MEMTAG\_RECORD\_NOEXIST  0x00000024 | RR operations for non-existent records. |
| MEMTAG\_RECORD\_WINS  0x00000025 | RR operations for WINS. |
| MEMTAG\_RECORD\_WINSPTR  0x00000026 | RR operations for WINS-PTR. |
| MEMTAG\_RECORD\_COPY  0x00000027 | RR copy operations. |
| MEMTAG\_NODE\_UNKNOWN  0x00000028 | Node operations for database. |
| MEMTAG\_NODE\_FILE  0x00000029 | Node operations for file. |
| MEMTAG\_NODE\_DS  0x0000002A | Node operations for directory server. |
| MEMTAG\_NODE\_AXFR  0x0000002B | Node operations for complete zone transfer. |
| MEMTAG\_NODE\_IXFR  0x0000002C | Node operations for single record transfer. |
| MEMTAG\_NODE\_DYNUP  0x0000002D | Node operations for dynamic update. |
| MEMTAG\_NODE\_ADMIN  0x0000002E | Node operations for administration. |
| MEMTAG\_NODE\_AUTO  0x0000002F | Node operations for autoconfig. |
| MEMTAG\_NODE\_CACHE  0x00000030 | Node operations for cache. |
| MEMTAG\_NODE\_NOEXIST  0x00000031 | Node operations for non-existent records. |
| MEMTAG\_NODE\_WINS  0x00000032 | Node operations for WINS. |
| MEMTAG\_NODE\_WINSPTR  0x00000033 | Node operations for WINS-PTR. |
| MEMTAG\_NODE\_COPY  0x00000034 | Node operations for copy. |

##### DNSSRV\_TIMEOUT\_STATS

The DNSSRV\_TIMEOUT\_STATS structure has DNS server statistics related to timeout operations on the server. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SetTotal | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SetDirect | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SetFromDereference | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SetFromChildDelete | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AlreadyInSystem | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Checks | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecentAccess | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ActiveRecord | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CanNotDelete | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Deleted | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ArrayBlocksCreated | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ArrayBlocksDeleted | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DelayedFreesQueued | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DelayedFreesQueuedWithFunction | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DelayedFreesExecuted | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DelayedFreesExecutedWithFunction | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**SetTotal (4 bytes):** The total number of times the server marked a node as being eligible for deletion when it is no longer in use by the cache.

**SetDirect (4 bytes):** The number of times the server marked a node as being eligible for deletion when it is no longer in use by the cache, by directly referencing the node.

**SetFromDereference (4 bytes):** The number of times the server marked a node as being eligible for deletion when it is no longer in use by the cache because the last reference was deleted.

**SetFromChildDelete (4 bytes):** The number of times the server marked a node as being eligible for deletion when it is no longer in use by the cache because the node's last child was deleted.

**AlreadyInSystem (4 bytes):** The number of times the server marked a node as being eligible for deletion when it is no longer in use by the cache when the node was already so marked.

**Checks (4 bytes):** The number of times the server performed any node timeout marking operation.

**RecentAccess (4 bytes):** The number of times the server encountered a cache node that it could not delete because the node had recently been accessed.

**ActiveRecord (4 bytes):** The number of times while performing checks the server encountered a cache node that had records present while checking nodes for deletion.

**CanNotDelete (4 bytes):** The number of times the server encountered a cache node that was marked for deletion that could not be deleted because it had been recently accessed or because it had active records or child nodes.

**Deleted (4 bytes):** The number of times the server successfully deleted a cache node that was marked as eligible for deletion.

**ArrayBlocksCreated (4 bytes):** The number of times the server created a block to hold more references to cache nodes eligible for deletion.

**ArrayBlocksDeleted (4 bytes):** The number of times the server deleted a block to hold references to cache nodes eligible for deletion.

**DelayedFreesQueued (4 bytes):** The number of times the server entered a block of memory into an internal list of memory blocks that may be freed at some time in the future.

**DelayedFreesQueuedWithFunction (4 bytes):** The number of times the server entered a block of memory into an internal list of memory blocks that may be freed at some time in the future where the block is freed using a function other than the standard memory free function.

**DelayedFreesExecuted (4 bytes):** The number of times the server released a block of memory that had previously been entered into an internal list of memory blocks that may be freed at some time in the future.

**DelayedFreesExecutedWithFunction (4 bytes):** The number of times the server released a block of memory that had previously been entered into an internal list of memory blocks that may be freed at some time in the future, where a function other than the standard memory free function was used for release.

##### DNSSRV\_DBASE\_STATS

The DNSSRV\_DBASE\_STATS structure has DNS server statistics related to the database tree. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NodeMemory | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NodeInUse | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NodeUsed | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NodeReturn | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**NodeMemory (4 bytes):** The total size, in bytes, of server memory currently used for nodes.

**NodeInUse (4 bytes):** The number of nodes currently allocated for use in the record database.

**NodeUsed (4 bytes):** The cumulative number of nodes allocated for use in the record database.

**NodeReturn (4 bytes):** The cumulative number of nodes freed from the record database.

##### DNSSRV\_RECORD\_STATS

The DNSSRV\_RECORD\_STATS structure has DNS server statistics related to record usage. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| InUse | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Used | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Return | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Memory | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CacheTotal | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CacheCurrent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CacheTimeouts | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SlowFreeQueued | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SlowFreeFinished | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**InUse (4 bytes):** The number of resource records currently allocated by the server.

**Used (4 bytes):** The cumulative number of resource records allocated by the server.

**Return (4 bytes):** The cumulative number of resource records freed by the server.

**Memory (4 bytes):** The amount of memory, in bytes, currently allocated for resource records by the server.

**CacheTotal (4 bytes):** The cumulative number resource records cached by the server.

**CacheCurrent (4 bytes):** The number of resource records currently cached by the server.

**CacheTimeouts (4 bytes):** The cumulative number of resource records that have been freed from the DNS server's cache.

**SlowFreeQueued (4 bytes):** Some cached record types, such as NS and SOA, are not immediately freed to the pool of allocated records, instead they are placed in a timeout queue and returned after this timeout expires. This is the cumulative count of such slow-free records that have been entered into the timeout queue.

**SlowFreeFinished (4 bytes):** The number of slow frees (see **SlowFreeQueued** above) that have been completed.

##### DNSSRV\_PACKET\_STATS

The DNSSRV\_PACKET\_STATS structure has DNS server statistics related to packets usage[<73>](#Appendix_A_73). This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpAlloc | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpFree | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpNetAllocs | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpMemory | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpUsed | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpReturn | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpResponseReturn | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpQueryReturn | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpInUse | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpInFreeList | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpAlloc | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpRealloc | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpFree | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpNetAllocs | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpMemory | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecursePacketUsed | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecursePacketReturn | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PacketsForNsListUsed (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PacketsForNsListReturned (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PacketsForNsListInUse (optional) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**UdpAlloc (4 bytes):** The cumulative number of UDP packets allocated by the server from system memory.

**UdpFree (4 bytes):** The cumulative number of UDP packets returned by the server to system memory.

**UdpNetAllocs (4 bytes):** The number of currently allocated UDP packets.

**UdpMemory (4 bytes):** The number of bytes of memory used by allocated or taken from the free list for use in query processing.

**UdpUsed (4 bytes):** The cumulative number of UDP packets from the pool of packets used by the server.

**UdpReturn (4 bytes):** The cumulative number of UDP packets freed or returned to the free list by the server.

**UdpResponseReturn (4 bytes):** The cumulative number of UDP packets freed or returned to the free list by the server that were UDP response packets.

**UdpQueryReturn (4 bytes):** The cumulative number of UDP query packets freed or returned to the free list by the server that were UDP query packets.

**UdpInUse (4 bytes):** The number of UDP packets currently in use to process queries.

**UdpInFreeList (4 bytes):** The number of UDP packets currently on the server's free list.

**TcpAlloc (4 bytes):** The cumulative number of TCP buffers allocated by the server from system memory.

**TcpRealloc (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**TcpFree (4 bytes):** The cumulative number of TCP buffers returned by the server to system memory.

**TcpNetAllocs (4 bytes):** The number of allocated TCP buffers currently allocated by the server.

**TcpMemory (4 bytes):** The total system memory, in bytes, used by TCP buffers currently allocated by the server.

**RecursePacketUsed (4 bytes):** The cumulative number of packets used by the server for recursion queries.

**RecursePacketReturn (4 bytes):** The cumulative number of packets that were used for recursive queries and then returned by the server to the pool of packets.

**PacketsForNsListUsed (4 bytes):** The total number of TCP buffers used by the server for name server list query messages. This field SHOULD[<74>](#Appendix_A_74) be present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**PacketsForNsListReturned (4 bytes):** The total number of TCP buffers that were used for name server lists in query messages, returned by the server to the pool of packets. This field MUST be present if and only if PacketsForNsListUsed is present. A client can tell whether the field is present based on the size of the buffer holding this structure.

**PacketsForNsListInUse (4 bytes):** The number of TCP buffers that are currently being used by the server for name lists in query messages. This field MUST be present if and only if PacketsForNsListUsed is present. A client can tell whether the field is present based on the size of the buffer holding this structure.

##### DNSSRV\_NBSTAT\_STATS

The DNSSRV\_NBSTAT\_STATS structure has DNS server statistics related to NBSTAT buffers usage. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NbstatAlloc | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NbstatFree | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NbstatNetAllocs | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NbstatMemory | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NbstatUsed | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NbstatReturn | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NbstatInUse | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NbstatInFreeList | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**NbstatAlloc (4 bytes):** The cumulative number of NetBIOS packet buffers allocated by the server from system memory.

**NbstatFree (4 bytes):** The cumulative number of NetBIOS packet buffers returned by the server to system memory.

**NbstatNetAllocs (4 bytes):** The number of NetBIOS packet buffers currently allocated by the server.

**NbstatMemory (4 bytes):** The total memory used by the NetBIOS packet buffers currently allocated by the server.

**NbstatUsed (4 bytes):** The cumulative number of NetBIOS buffers currently in use by the server either servicing queries or in a free list.

**NbstatReturn (4 bytes):** The cumulative number of NetBIOS buffers freed or returned by the server to a free list.

**NbstatInUse (4 bytes):** The number of NetBIOS buffers currently being used by the server to service queries or being held in a free list.

**NbstatInFreeList (4 bytes):** The number of NetBIOS buffers currently in a free list.

##### DNSSRV\_PRIVATE\_STATS

The DNSSRV\_PRIVATE\_STATS structure has DNS server statistics related to internal server processing. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordFile | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordFileFree | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordDs | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordDsFree | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordAdmin | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordAdminFree | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordDynUp | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordDynUpFree | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordAxfr | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordAxfrFree | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordIxfr | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordIxfrFree | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordCopy | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordCopyFree | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordCache | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RecordCacheFree | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpSocketPnpDelete | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpRecvFailure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpErrorMessageSize | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpConnResets | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpConnResetRetryOverflow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpGQCSFailure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpGQCSFailureWithContext | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpGQCSConnReset | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpIndicateRecvFailures | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UdpRestartRecvOnSockets | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpConnectAttempt | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpConnectFailure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpConnect | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpQuery | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TcpDisconnect | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecTsigVerifyOldSig | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecTsigVerifyOldFailed | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SecBigTimeSkewBypass | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ZoneLoadInit | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ZoneLoadComplete | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ZoneDbaseDelete | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ZoneDbaseDelayedDelete | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**RecordFile (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**RecordFileFree (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**RecordDs (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**RecordDsFree (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**RecordAdmin (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**RecordAdminFree (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**RecordDynUp (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**RecordDynUpFree (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**RecordAxfr (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**RecordAxfrFree (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**RecordIxfr (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**RecordIxfrFree (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**RecordCopy (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**RecordCopyFree (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**RecordCache (4 bytes):** MUST be set to zero when sent and MUST be ignored on receipt.

**RecordCacheFree (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**UdpSocketPnpDelete (4 bytes):** The number of UDP sockets that have been closed and had their locally allocated state freed by the server because a UDP error occurred or because the socket was closed in response to an IP address change on the local machine.

**UdpRecvFailure (4 bytes):** The number of times the server failed to receive UDP packet.

**UdpErrorMessageSize (4 bytes):** The number of times the server received an error from UDP socket due to the large size of the receive packet.

**UdpConnResets (4 bytes):** The number of times the server received a connection reset error from UDP.

**UdpConnResetRetryOverflow (4 bytes):** The number of times the server received a connection reset error from UDP and could not clear the error by resubmitting a receive operation.

**UdpGQCSFailure (4 bytes):** The number of times the server received an error from UDP.

**UdpGQCSFailureWithContext (4 bytes):** The number of times the server received an error from UDP where no internal state for the UDP operation was available.

**UdpGQCSConnReset (4 bytes):** The number of times the server received an error from UDP indicating that a remote address was unreachable.

**UdpIndicateRecvFailures (4 bytes):** The number of times the server received a critical error while attempting to perform a UDP receive operation.

**UdpRestartRecvOnSockets (4 bytes):** The number of times the server attempted to restart receive operations on its UDP sockets due to UDP errors.

**TcpConnectAttempt (4 bytes):** MUST be set to zero when sent and MUST be ignored on receipt.

**TcpConnectFailure (4 bytes):** MUST be set to zero when sent and MUST be ignored on receipt.

**TcpConnect (4 bytes):** The number of times the server was able to successfully establish a TCP connection to a remote the server.

**TcpQuery (4 bytes):** The number of times the server sent a recursive query over a TCP connection.

**TcpDisconnect (4 bytes):** The number of times the server disconnected a TCP connection.

**SecTsigVerifyOldSig (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**SecTsigVerifyOldFailed (4 bytes):** Unused. Senders MUST set this value to zero and receivers MUST ignore it.

**SecBigTimeSkewBypass (4 bytes):** The number of times the server received a TKEY that had a time-skew within the allowable range of 1 day.

**ZoneLoadInit (4 bytes):** The number of times the server prepared to load or reload a zone from persistent storage or from a zone transfer.

**ZoneLoadComplete (4 bytes):** MUST be set to zero when sent and MUST be ignored on receipt.

**ZoneDbaseDelete (4 bytes):** MUST be set to zero when sent and MUST be ignored on receipt.

**ZoneDbaseDelayedDelete (4 bytes):** MUST be set to zero when sent and MUST be ignored on receipt.

##### DNSSRV\_ERROR\_STATS

The DNSSRV\_ERROR\_STATS structure has DNS server statistics related to the different types of errors returned by the server. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NoError | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FormError | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ServFail | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NxDomain | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NotImpl | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Refused | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| YxDomain | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| YxRRSet | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NxRRSet | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NotAuth | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NotZone | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Max | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| BadSig | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| BadKey | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| BadTime | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UnknownError | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**NoError (4 bytes):** The number of occurrences where the server returned success (0x00000000) and query was successfully responded to.

**FormError (4 bytes):** The number of occurrences where the server returned error code 0x00000001 due to a malformed query.

**ServFail (4 bytes):** The number of occurrences where the server returned error code 0x00000002 due to a failure in query processing at server.

**NxDomain (4 bytes):** The number of occurrences where the server returned a name error code 0x00000003.

**NotImpl (4 bytes):** The number of occurrences where the server returned error code 0x00000004 due to unimplemented functionality.

**Refused (4 bytes):** The number of occurrences where the server returned error code 0x00000005 due to policy restrictions.

**YxDomain (4 bytes):** The number of occurrences where the server returned error code 0x00000006 due to a domain not being found.

**YxRRSet (4 bytes):** The number of occurrences where the server returned error code 0x00000007 due to the unexpected existence of a resource record.

**NxRRSet (4 bytes):** The number of occurrences where the server returned error code 0x00000008, because the requested resource record did not exist.

**NotAuth (4 bytes):** The number of occurrences where the server returned error code 0x00000009 due to the server not being authoritative for the zone.

**NotZone (4 bytes):** The number of occurrences where the server returned error 0x0000000A (10) due to the requested zone not being found.

**Max (4 bytes):** The number of occurrences where the server returned an error code 0x0000000F (15) which is larger than 4 bits and the server needed to introduce the OPT field in the response packet.

**BadSig (4 bytes):** The number of occurrences where the server returned error 0x00000010 (16) due to a bad signature being present in the query.

**BadKey (4 bytes):** The number of occurrences where the server returned error 0x00000011 (17) due to a bad key being present in the query.

**BadTime (4 bytes):** The number of occurrences where the server returned error 0x00000012 (18) due to a bad time stamp being present in the query.

**UnknownError (4 bytes):** The number of occurrences where the server returned an error code that was caused by any other reason than those listed above.

##### DNSSRV\_CACHE\_STATS

The DNSSRV\_CACHE\_STATS structure has DNS server statistics related to the server cache. This structure MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CacheExceededLimitChecks | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SuccessfulFreePasses | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FailedFreePasses | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PassesWithNoFrees | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PassesRequiringAggressiveFree | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (8 bytes):** A structure of type DNSSRV\_STAT\_HEADER (section [2.2.10.2.1](#Section_271b57b1759c4c5c8238912cd1b3be2a)).

**CacheExceededLimitChecks (4 bytes):** Not used. Senders MUST set this value to zero and receivers MUST ignore it.

**SuccessfulFreePasses (4 bytes):** The number of times since the server last started that the server cache was found to exceed the cache size limit, which is 90 percent of the MaxCacheSize (section [3.1.1.1.1](#Section_8903e50a91834a7d964053f6f5a91481)), and that an attempt to free nodes resulted in the cache size limit being met. After reaching 0xFFFFFFFF, the value increments to 0x00000000.

**FailedFreePasses (4 bytes):** The number of times since the server last started that the server cache was found to exceed the cache size limit, which is 90 percent of the MaxCacheSize (section 3.1.1.1.1), and that an attempt to free nodes was unsuccessful in meeting the cache size limit. After reaching 0xFFFFFFFF, the value increments to 0x00000000.

**PassesWithNoFrees (4 bytes):** The number of times since the server last started that the server cache was found to exceed the cache size limit, which is 90 percent of the MaxCacheSize (section 3.1.1.1.1), but when the server scanned the cache looking for nodes containing no records or only [**expired DNS records**](#gt_c0105e97-de24-448b-8514-78fd557e9164) to free, it found no nodes that could be freed. After reaching 0xFFFFFFFF, the value increments to 0x00000000.

**PassesRequiringAggressiveFree (4 bytes):** The number of times since the server last started that the server cache was found to exceed the cache size limit, which is 90 percent of the MaxCacheSize (section 3.1.1.1.1), and that the server scanned the cache aggressively attempting to free even nodes that contain unexpired records. An aggressive scan frees, in order, nodes containing records that are to expire within the next hour, records that are to expire within the next day, and all records if needed, and halts the freeing process immediately once the cache size limit is reached. After reaching 0xFFFFFFFF, the value increments to 0x00000000.

### Key Structures

#### Enumerations and Constants

##### Cryptographic Algorithm Name

In the context of this protocol, a Cryptographic Algorithm Name is a null-terminated Unicode string representing a digital signature algorithm. The following values are acceptable.

| Name | Description |
| --- | --- |
| "RSA" | The RSA signature algorithm specified in [[FIPS186]](http://go.microsoft.com/fwlink/?LinkId=89869) section 5. Key pairs for use with this algorithm are represented in the RSA Key Pair format specified in section [2.2.11.2.1](#Section_244cca32e77a4d8a951d6fd918d55a98). |
| "ECDSA\_P256" | The ECDSA signature algorithm specified in [FIPS186] section 6, computed over the curve P-256 specified in [FIPS186] Appendix D.1.2.3. Key pairs for use with this algorithm are represented in the ECDSA Key Pair format specified in section [2.2.11.2.2](#Section_2520414ed4f1483784696eb771c64992). |
| "ECDSA\_P384" | The ECDSA signature algorithm specified in [FIPS186] section 6, computed over the curve P-384 specified in [FIPS186] Appendix D.1.2.4. Key pairs for use with this algorithm are represented in the ECDSA Key Pair format specified in section [2.2.11.2.3](#Section_ed7dcb2f37794814b548ae37bb82653a). |

#### Structures

##### RSA Key Pair

The RSA Key Pair structure is used to store a key pair (a public key and corresponding private key) for use with the RSA digital signature algorithm.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Reserved1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ModulusBitLength | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LengthOfPublicExponent | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LengthOfModulus | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LengthOfPrime1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LengthOfPrime2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PublicExponent (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Modulus (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Prime1 (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Prime2 (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Reserved1 (4 bytes):** MUST be 0x32415352.

**ModulusBitLength (4 bytes):** This MUST be a 32-bit unsigned integer in little-endian format. It MUST be the length of the RSA modulus, in bits, equal to 8 times the quantity referred to as **k** in [[RFC3447]](http://go.microsoft.com/fwlink/?LinkId=90422) section 2.

**LengthOfPublicExponent (4 bytes):** This MUST be a 32-bit unsigned integer in little-endian format. It MUST be the length of the **PublicExponent** field, in bytes.

**LengthOfModulus (4 bytes):** This MUST be a 32-bit unsigned integer in little-endian format. It MUST be the length of the **Modulus** field, in bytes.

**LengthOfPrime1 (4 bytes):** This MUST be a 32-bit unsigned integer in little-endian format. It MUST be the length of the **Prime1** field, in bytes.

**LengthOfPrime2 (4 bytes):** This MUST be a 32-bit unsigned integer in little-endian format. It MUST be the length of the **Prime2** field, in bytes.

**PublicExponent (variable):** This MUST be the public exponent of the key pair, referred to as **e** in [RFC3447] section 2. It MUST be encoded in big-endian format.

**Modulus (variable):** This MUST be the RSA modulus, referred to as **n** in [RFC3447] section 2. It MUST be equal to **Prime1** \* **Prime2**. It MUST be encoded in big-endian format.

**Prime1 (variable):** This MUST be the first prime factor of the RSA modulus, referred to as **p** in [RFC3447] section 2. It MUST be encoded in big-endian format.

**Prime2 (variable):** This MUST be the second prime factor of the RSA modulus, referred to as **q** in [RFC3447] section 2. It MUST be encoded in big-endian format.

##### ECDSA\_P256 Key Pair

The ECDSA\_P256 Key Pair structure is used to store an ECDSA\_P256 key pair (a public key and corresponding private key) for use with the ECDSA digital signature algorithm.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Reserved1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Reserved2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| X (32 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Y (32 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| d (32 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Reserved1 (4 bytes):** MUST be 0x324B4345.

**Reserved2 (4 bytes):** MUST be 0x00000020.

**X (32 bytes):** This MUST be the x-coordinate of the ECDSA public key. It MUST be encoded in big-endian format.

**Y (32 bytes):** This MUST be the y-coordinate of the ECDSA public key. It MUST be encoded in big-endian format.

**d (32 bytes):** This MUST be the ECDSA private key. It MUST be encoded in big-endian format.

##### ECDSA\_P384 Key Pair

The ECDSA\_P256 Key Pair structure is used to store an ECDSA\_P384 key pair (a public key and corresponding private key) for use with the ECDSA digital signature algorithm.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Reserved1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Reserved2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| X (48 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Y (48 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| d (48 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Reserved1 (4 bytes):** MUST be 0x324B4345.

**Reserved2 (4 bytes):** MUST be 0x00000030.

**X (48 bytes):** This MUST be the x-coordinate of the ECDSA public key. It MUST be encoded in big-endian format.

**Y (48 bytes):** This MUST be the y-coordinate of the ECDSA public key. It MUST be encoded in big-endian format.

**d (48 bytes):** This MUST be the ECDSA private key. It MUST be encoded in big-endian format.

##### Protection Key Identifier

The Protection Key Identifier structure is used to store metadata about the key used to cryptographically wrap the DNSSEC key as part of the Exported Key Pair structure specified in section [2.2.11.2.6](#Section_820903b3170440b6b977ac9154a90ffd).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Reserved1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Reserved2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Reserved3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| L0KeyID | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| L1KeyID | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| L2KeyID | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RootKeyID (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Reserved4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DomainNameLength | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ForestNameLength | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DNSDomainName (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DNSForestName (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Reserved1 (4 bytes):** MUST be 0x00000001.

**Reserved2 (4 bytes):** MUST be 0x4B53444B.

**Reserved3 (4 bytes):** MUST be 0x00000000.

**L0KeyID (4 bytes):** An L0 index, as defined in [[MS-GKDI]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-GKDI%5d.pdf) section 3.1.4.1.

**L1KeyID (4 bytes):** An L1 index, as defined in [MS-GKDI] section 3.1.4.1.

**L2KeyID (4 bytes):** An L2 index, as defined in [MS-GKDI] section 3.1.4.1.

**RootKeyID (16 bytes):** A root key identifier, as defined in [MS-GKDI] section 3.1.4.1.

**Reserved4 (4 bytes):** MUST be 0x00000000.

**DomainNameLength (4 bytes):** A 32-bit unsigned integer, encoded in little-endian format. It MUST be the length, in bytes, of the **DNSDomainName** field.

**ForestNameLength (4 bytes):** A 32-bit unsigned integer, encoded in little-endian format. It MUST be the length, in bytes, of the **DNSForestName** field.

**DNSDomainName (variable):** A null-terminated Unicode string containing the DNS-style name of the Active Directory domain in which this identifier was created.

**DNSForestName (variable):** A null-terminated Unicode string containing the DNS-style name of the Active Directory forest in which this identifier was created.

##### Protection Key Attributes

The Protection Key Attributes structure is used to store some metadata about how a key pair is cryptographically wrapped as part of the Exported Key Pair structure (section [2.2.11.2.6](#Section_820903b3170440b6b977ac9154a90ffd)). It is a structure in ASN.1 format, encoded using DER encoding as specified in [[X690]](http://go.microsoft.com/fwlink/?LinkId=90593). The ASN.1 definition for this structure is as follows.

1. microsoft OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 311 }
2. msKeyProtection OBJECT IDENTIFIER := { microsoft 74 }
3. protectionInfo OBJECT IDENTIFIER ::= { msKeyProtection 1 }
4. sidProtected OBJECT IDENTIFIER ::= { protectionInfo 1 }
5. sidName UTF8 STRING ::= "SID"
6. ProtectionKeyAttribute ::= SEQUENCE {
7. protectionInfo OBJECT IDENTIFIER,
8. SEQUENCE SIZE (1) {
9. sidProtected OBJECT IDENTIFIER,
10. SEQUENCE SIZE (1) {
11. SEQUENCE SIZE (1) {
12. SEQUENCE SIZE (1) {
13. sidName UTF8 STRING,
14. sidString UTF8 STRING
15. }
16. }
17. }
18. }
19. }

##### Exported Key Pair

The Exported Key Pair structure is used to wrap a ZSK for secure storage in the Active Directory database.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Reserved1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Reserved2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LengthOfAlgorithmName | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LengthOfProtectedKeyBlob | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LengthOfKeyName | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AlgorithmName (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ProtectedKeyBlob (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| KeyName (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Reserved1 (4 bytes):** MUST be 0x00000014.

**Reserved2 (4 bytes):** MUST be 0x4B545250.

**LengthOfAlgorithmName (4 bytes):** A 32-bit unsigned integer, encoded using little-endian format. This MUST be equal to the length of the **AlgorithmName** field, in bytes.

**LengthOfProtectedKeyBlob (4 bytes):** A 32-bit unsigned integer, encoded using little-endian format. This MUST be equal to the length of the **ProtectedKeyBlob** field, in bytes.

**LengthOfKeyName (4 bytes):** A 32-bit unsigned integer, encoded using little-endian format. This MUST be equal to the length of the **KeyName** field, in bytes.

**AlgorithmName (variable):** The Cryptographic Algorithm Name, as specified in section [2.2.11.1.1](#Section_a430d9bdec994fa1a2f9d982018d7f44), of the digital signature algorithm that the key encapsulated in the **ProtectedKeyBlob** field is intended for use with.

**ProtectedKeyBlob (variable):** A BLOB containing the encrypted key pair, constructed as specified in section [3.1](#Section_bdac51424baf4b62bcced49eafc9c3e6).

**KeyName (variable):** A null-terminated Unicode string containing implementation-dependent data.

### Zone Statistics Messages

#### Enumerations and Constants

| Constant/Value | Description |
| --- | --- |
| MAX\_RECORD\_TYPES  0x0000001D | Specifies the maximum record types supported. |
| MAX\_ZONE\_TRANSFER\_TYPES  0x00000002 | Specifies the maximum zone transfer types supported (currently AXFR and IXFR). |
| DNS\_RPC\_ZONE\_STATS\_GET  0x00000000 | Enumerates zone statistics. |
| DNS\_RPC\_ZONE\_STATS\_CLEAR  0x00000001 | Enumerates zone statistics and resets the zone statistics to zero. |

##### DNS\_ZONE\_STATS\_TYPE

Note: Some of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview in the Product Behavior appendix.

This is the enumerator for all zone statistics types.[<75>](#Appendix_A_75)

| Enumerator Value | Description |
| --- | --- |
| ZONE\_STATS\_TYPE\_RECORD\_A = 0 | A record type |
| ZONE\_STATS\_TYPE\_RECORD\_AAAA | AAAA record type |
| ZONE\_STATS\_TYPE\_RECORD\_PTR | PTR record type |
| ZONE\_STATS\_TYPE\_RECORD\_CNAME | CNAME record type |
| ZONE\_STATS\_TYPE\_RECORD\_MX | MX record type |
| ZONE\_STATS\_TYPE\_RECORD\_AFSDB | AFDSB record type |
| ZONE\_STATS\_TYPE\_RECORD\_ATMA | ATMA record type |
| ZONE\_STATS\_TYPE\_RECORD\_DHCID | DHCID record type |
| ZONE\_STATS\_TYPE\_RECORD\_DNAME | DNAME record type |
| ZONE\_STATS\_TYPE\_RECORD\_HINFO | HINFO record type |
| ZONE\_STATS\_TYPE\_RECORD\_ISDN | ISDN record type |
| ZONE\_STATS\_TYPE\_RECORD\_MG | MG record type |
| ZONE\_STATS\_TYPE\_RECORD\_MB | MB record type |
| ZONE\_STATS\_TYPE\_RECORD\_MINFO | MINFO record type |
| ZONE\_STATS\_TYPE\_RECORD\_NAPTR | NAPTR record type |
| ZONE\_STATS\_TYPE\_RECORD\_NXT | NXT record type |
| ZONE\_STATS\_TYPE\_RECORD\_KEY | KEY record type |
| ZONE\_STATS\_TYPE\_RECORD\_MR | MR record type |
| ZONE\_STATS\_TYPE\_RECORD\_RP | RP record type |
| ZONE\_STATS\_TYPE\_RECORD\_RT | RT record type |
| ZONE\_STATS\_TYPE\_RECORD\_SRV | SRV record type |
| ZONE\_STATS\_TYPE\_RECORD\_SIG | SIG record type |
| ZONE\_STATS\_TYPE\_RECORD\_TEXT | TXT record type |
| ZONE\_STATS\_TYPE\_RECORD\_WKS | WKS record type |
| ZONE\_STATS\_TYPE\_RECORD\_X25 | X25 record type |
| ZONE\_STATS\_TYPE\_RECORD\_DNSKEY | DNSKEY record type |
| ZONE\_STATS\_TYPE\_RECORD\_DS | DS record type |
| ZONE\_STATS\_TYPE\_RECORD\_NS | NS record type |
| ZONE\_STATS\_TYPE\_RECORD\_SOA | SOA record type |
| ZONE\_STATS\_TYPE\_RECORD\_TLSA | TLSA record type |
| ZONE\_STATS\_TYPE\_RECORD\_ALL | All record types |
| ZONE\_STATS\_TYPE\_RECORD\_OTHERS | Resource records not specified in this list |
| ZONE\_STATS\_TYPE\_TRANSFER\_AXFR | Axft transfer type |
| ZONE\_STATS\_TYPE\_TRANSFER\_IXFR | Ixfr transfer type |
| ZONE\_STATS\_TYPE\_UPDATE | Zone Update |
| MAX\_ZONE\_STATS\_TYPES | Specifies the maximum zone statistics types supported |

#### Structures

##### DNSSRV\_ZONE\_TIME\_STATS

The DNSSRV\_ZONE\_TIME\_STATS structure[<76>](#Appendix_A_76) contains zone time statistics information.

1. typedef struct \_DnsZoneTimeStats {
2. DNS\_SYSTEMTIME StatsCollectionStartTime;
3. } DNSSRV\_ZONE\_TIME\_STATS,
4. \*PDNSSRV\_ZONE\_TIME\_STATS;

**StatsCollectionStartTime:**  The time when zone statistics collection started.

##### DNSSRV\_ZONE\_QUERY\_STATS

The DNSSRV\_ZONE\_QUERY\_STATS structure[<77>](#Appendix_A_77) contains per-zone per-record-type statistics.

1. typedef struct \_DnsZoneQueryStats  {
2. DNS\_ZONE\_STATS\_TYPE RecordType;
3. ULONG64 QueriesResponded;
4. ULONG64 QueriesReceived;
5. ULONG64 QueriesFailure;
6. ULONG64 QueriesNameError;
7. } DNSSRV\_ZONE\_QUERY\_STATS,
8. \*PDNSSRV\_ZONE\_QUERY\_STATS;

**RecordType:**  The type of record for which the query was received. The value SHOULD be of type DNS\_ZONE\_STATS\_TYPE.

**QueriesResponded:**  The total number of queries to which the server responded for a specific zone.

**QueriesReceived:**  The total number of queries received by the server for a specific zone.

**QueriesFailure:**  The total number of queries for which the server responded with server failure for a specific zone.

**QueriesNameError:**  The total number of queries for which the server responded with a name error for a specific zone.

##### DNSSRV\_ZONE\_TRANSFER\_STATS

The DNSSRV\_ZONE\_TRANSFER\_STATS structure[<78>](#Appendix_A_78) contains zone transfer statistics per zone.

1. typedef struct \_DnsZoneTransferStats  {
2. DNS\_ZONE\_STATS\_TYPE TransferType;
3. ULONG64 RequestReceived;
4. ULONG64 RequestSent;
5. ULONG64 ResponseReceived;
6. ULONG64 SuccessReceived;
7. ULONG64 SuccessSent;
8. } DNSSRV\_ZONE\_TRANSFER\_STATS,
9. \*PDNSSRV\_ZONE\_TRANSFER\_STATS;

**TransferType:**  The type of zone transfer request for which the query was received. The value is of type DNS\_ZONE\_STATS\_TYPE.

**RequestReceived:**  The total number of zone transfer requests received by the server for a specific zone.

**RequestSent:**  The total number of zone transfer requests sent by the server for a specific zone.

**ResponseReceived:**  The total number of zone transfer responses received by the server for a specific zone.

**SuccessReceived:**  The total number of zone transfer requests received successfully by the receiver for a specific zone.

**SuccessSent:**  The total number of zone transfer responses sent by the server for a specific zone.

##### DNSSRV\_ZONE\_UPDATE\_STATS

The DNSSRV\_ZONE\_UPDATE\_STATS structure[<79>](#Appendix_A_79) contains statistics about the dynamic updates per zone.

1. typedef struct \_DnsZoneUpdateStats  {
2. DNS\_ZONE\_STATS\_TYPE Type;
3. ULONG64 DynamicUpdateReceived;
4. ULONG64 DynamicUpdateRejected;
5. } DNSSRV\_ZONE\_UPDATE\_STATS,
6. \*PDNSSRV\_ZONE\_UPDATE\_STATS;

**Type:**  The type of zone update request for which statistics are required. The value is of type [DNS\_ZONE\_STATS\_TYPE (section 2.2.12.1.1)](#Section_8659f901293c4e8f862a6b7861b01118).

**DynamicUpdateReceived:**  The total number of dynamic updates accepted on a specified zone.

**DynamicUpdateRejected:**  The total number of dynamic updates rejected on a specified zone.

##### DNS\_RPC\_ZONE\_STATS\_V1

The DNS\_RPC\_ZONE\_STATS\_V1 structure[<80>](#Appendix_A_80) contains all the statistics about a zone.

1. typedef struct \_DnsRpcZoneStats  {
2. DWORD dwRpcStructureVersion;
3. DNSSRV\_ZONE\_TIME\_STATS ZoneTimeStats;
4. DNSSRV\_ZONE\_QUERY\_STATS ZoneQueryStats[MAX\_RECORD\_TYPES];
5. DNSSRV\_ZONE\_TRANSFER\_STATS ZoneTransferStats[MAX\_ZONE\_TRANSFER\_TYPES];
6. DNSSRV\_ZONE\_UPDATE\_STATS ZoneUpdateStats;
7. } DNS\_RPC\_ZONE\_STATS\_V1,
8. \*PDNS\_RPC\_ZONE\_STATS\_V1;

**dwRpcStructureVersion:**  The DNS management structure version number. This value MUST be set to 0x00000001.

**ZoneTimeStats:**  Information about the zone time statistics in DNSSRV\_ZONE\_TIME\_STATS.

**ZoneQueryStats:**  An array of DNSSRV\_ZONE\_QUERY\_STATS.

**ZoneTransferStats:**  An array of DNSSRV\_ZONE\_TRANSFER\_STATS.

**ZoneUpdateStats:**  An array of DNSSRV\_ZONE\_UPDATE\_STATS.

### Zone Scope or Cache Scope Messages

#### Enumerations and Constants

#### Structures

##### DNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST

The [DNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST](#Section_d0ac5580a8464e5aa526c5e17c00e15d) structure[<81>](#Appendix_A_81) contains a list of zone scopes or cache scopes to be enumerated.

1. typedef struct \_DnsRpcEnumZoneScopeList {
2. DWORD dwRpcStructureVersion;
3. DWORD dwZoneScopeCount;
4. LPWSTR ZoneScopeArray[1];
5. } DNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST,
6. \*PDNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST;

**dwRpcStructureVersion:**  The DNS management structure version number. This value MUST be set to 0x00000001.

**dwZoneScopeCount:**  The number of zone scopes or cache scopes.

**ZoneScopeArray:**  An array containing the names of zone scopes or cache scopes.

##### DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO

###### DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1

The DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1 structure[<82>](#Appendix_A_82) contains the name of the zone scope or cache scope.

1. typedef struct \_DnsRpcScopeCreate {
2. DWORD dwFlags;
3. LPWSTR pwszScopeName;
4. } DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1,
5. \*PDNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1;

**dwFlags:**  Specifies the behavior that the DNS server SHOULD follow when creating the scope. This field is used only when the operation is CreateZoneScope. For any other value than the following, a new empty zone scope is created:

| Value | Meaning |
| --- | --- |
| DNS\_ZONE\_LOAD\_OVERWRITE\_MEMORY  0x00000010 | If this value is specified, the DNS server MUST attempt to find and load the zone scope database from persistent storage instead of creating a new empty zone scope. If a pre-existing zone scope database is not found, or if there is a failure in loading the existing database file, the DNS server MUST fail the operation and return an error. If a cache scope is being created, this operation fails on the DNS server and an ERROR\_INVALID\_PARAMETER error is returned. |

**pwszScopeName:**  The name of the zone scope or cache scope.

##### DNS\_RPC\_ZONE\_SCOPE\_INFO

###### DNS\_RPC\_ZONE\_SCOPE\_INFO\_V1

The DNS\_RPC\_ZONE\_SCOPE\_INFO\_V1 structure[<83>](#Appendix_A_83) contains the details of the zone scope or cache scope.

1. typedef struct \_DnsRpcZoneScopeInfo {
2. DWORD dwRpcStructureVersion;
3. LPWSTR pwszScopeName;
4. LPWSTR pwszDataFile;
5. } DNS\_RPC\_ZONE\_SCOPE\_INFO\_V1,
6. \*PDNS\_RPC\_ZONE\_SCOPE\_INFO\_V1;

**dwRpcStructureVersion:**  The DNS management structure version number. This value MUST be set to 0x00000001.

**pwszScopeName:**  The name of the zone scope or cache scope.

**pwszDataFile:**  The name of the zone scope or cache scope data file.

### Server Scope Messages

#### Structures

##### DNS\_RPC\_ENUM\_SCOPE\_LIST

The DNS\_RPC\_ENUM\_SCOPE\_LIST structure[<84>](#Appendix_A_84) contains the list of server scopes configured on the DNS server.

1. typedef struct \_DnsRpcEnumScopeList {
2. DWORD dwRpcStructureVersion;
3. DWORD dwScopeCount;
4. LPWSTR ScopeArray[1];
5. } DNS\_RPC\_ENUM\_SCOPE\_LIST,
6. \*PDNS\_RPC\_ENUM\_SCOPE\_LIST;

**dwRpcStructureVersion:**  The DNS management structure version number. This value MUST be set to 0x00000000.

**dwScopeCount:**  The number of server scopes.

**ScopeArray:**  An array containing the names of server scopes.

### Policies

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

DNS Policy constants and structures SHOULD[<85>](#Appendix_A_85) be used during DNS policy update.

#### Enumerations and Constants

##### Constants

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The following DNS Policy constants are used during a DNS Policy update, as specified in the UpdatePolicy operation (section [3.1.4.1](#Section_9500a7e8165d4b13be860ddc43100eef)). For detail on how they affect DNS policy update, see UpdatePolicy in section 3.1.4.1.

| Constant/value | Description |
| --- | --- |
| DNS\_RPC\_FLAG\_POLICY\_CRITERIA\_FQDN  0x00000001 | Specifies that the criteria (section [2.2.15.2.4](#Section_be16f14ddf7440fe892c0718ebd32e84)) for matching a DNS Policy is based on the query name in the question section of a DNS query in a [**DNS Operation**](#gt_8536bec5-df4d-4463-82bc-4434a7ea493f) ([[RFC1034]](http://go.microsoft.com/fwlink/?LinkId=90263) section 3.7). |
| DNS\_RPC\_FLAG\_POLICY\_CRITERIA\_CLIENT\_SUBNET  0x00000002 | Specifies that the criteria (section 2.2.15.2.4) for matching a DNS Policy is based on the client subnet record, which is derived from the IP address of a resolver in a DNS Operation ([RFC1034]) section 2.4). |
| DNS\_RPC\_FLAG\_POLICY\_CRITERIA\_SERVER\_IP  0x00000004 | Specifies that the criteria (section 2.2.15.2.4) for matching a DNS Policy is based on the IP address on which the DNS server receives the DNS query in a DNS Operation. |
| DNS\_RPC\_FLAG\_POLICY\_CRITERIA\_QUERY\_TYPE  0x00000008 | Specifies that the criteria (section 2.2.15.2.4) for matching a DNS Policy is based on the QTYPE of a DNS query in a DNS Operation ([[RFC1035]](http://go.microsoft.com/fwlink/?LinkId=90264) section 3.2.3). |
| DNS\_RPC\_FLAG\_POLICY\_CRITERIA\_TIME\_OF\_DAY  0x000000010 | Specifies that the criteria (section 2.2.15.2.4) for matching a DNS Policy is based on the Time Of Day in start-time : end-time format where time is expressed in hh:mm, when the DNS server receives a DNS query during a DNS Operation. |
| DNS\_RPC\_FLAG\_POLICY\_CRITERIA\_TRANSPORT\_PROTOCOL  0x000000020 | Specifies that the criteria (section 2.2.15.2.4) for matching a DNS Policy is based on the Transport Layer Protocol (TCP or UDP) used to send a DNS query to the DNS server during a DNS Operation. |
| DNS\_RPC\_FLAG\_POLICY\_CRITERIA\_NETWORK\_PROTOCOL  0x00000040 | Specifies that the criteria (section 2.2.15.2.4) for matching a DNS Policy is based the Internet Protocol that is used (IPv4 or IPv6) to send a DNS Query to the DNS server during a DNS Operation. |
| DNS\_RPC\_FLAG\_POLICY\_CONDITION  0x00010000 | Specifies that the criteria (section 2.2.15.2.4) for matching a DNS Policy is based on the [DNS\_RPC\_POLICY\_CONDITION (section 2.2.15.1.1.2)](#Section_6b98c962d2084475ae181a068b4b925c) that connects the various criteria in a DNS operation. |
| DNS\_RPC\_FLAG\_POLICY\_PROCESSING\_ORDER  0x00020000 | Specifies the processing order of a DNS policy. A processing order of a DNS Policy determines whether this policy is to be applied to the DNS operation, in case there are other DNS policies ([DNS\_RPC\_POLICY (section 2.2.15.2.5)](#Section_89be092dec014ab384e45a56622f9de8)) at the same level that also match the DNS operation. |
| DNS\_RPC\_FLAG\_POLICY\_CONTENT  0x00040000 | Specifies the zone scope, cache scope, or server scope from which a DNS operation is to be performed in case the DNS Policy is a match. For more details about the Policy content, see [DNS\_RPC\_POLICY\_CONTENT (section 2.2.15.2.2)](#Section_dd2e4ce56eea4dc4b9f7058eb9703381). |

###### DNS\_RPC\_CRITERIA\_COMPARATOR

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The DNS\_RPC\_CRITERIA\_COMPARATOR enumeration specifies the logical condition which connects the DNS Policy Criteria evaluation during DNS Operations.

| Enumerator Value | Description |
| --- | --- |
| Equals = 1 | Specifies that the values in a criteria (section [2.2.15.2.5](#Section_89be092dec014ab384e45a56622f9de8)) of a DNS Policy are connected by a logical OR condition. |
| NotEquals | Specifies that the values in a criteria (section 2.2.15.2.5) of a DNS Policy are connected by logical AND condition. |

###### DNS\_RPC\_POLICY\_CONDITION

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The DNS\_RPC\_POLICY\_CONDITION enumeration specifies the logical condition that connects the DNS Policy Criteria evaluation during DNS operations.

| Enumerator Value | Description |
| --- | --- |
| DNS\_AND = 0 | While evaluating a DNS Policy (section [2.2.15.2.5](#Section_89be092dec014ab384e45a56622f9de8)) during a DNS Operation, all criteria (section [2.2.15.2.4](#Section_be16f14ddf7440fe892c0718ebd32e84) configured for that particular DNS Policy MUST match. |
| DNS\_OR | While evaluating a DNS Policy during a DNS Operation, at least one configured criterion MUST match. |

###### DNS\_RPC\_POLICY\_LEVEL

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The DNS\_RPC\_POLICY\_LEVEL enumeration specifies that the DNS Policy is applied for a zone, cache zone, or at server level.

| Enumerator Value | Description |
| --- | --- |
| DnsPolicyServerLevel = 0 | The DNS Policy is applicable at the server level for all DNS operations. |
| DnsPolicyZoneLevel | The DNS Policy is applicable only for a specified zone. It is applicable for all DNS operations allowed for any zone.  **Note**  For all DNS operations, Recursive Query is not possible for a zone because the zone never recurses for records it owns. |
| DnsPolicyLevelMax | Shows the maximum level types supported. |

###### DNS\_RPC\_POLICY\_ACTION\_TYPE

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The DNS\_RPC\_POLICY\_ACTION\_TYPE enumeration specifies the action to be applied when a DNS Policy is matched.

| Enumerator Value | Description |
| --- | --- |
| DnsPolicyDeny=0 | Denies the specific DNS operation. |
| DnsPolicyAllow | Allows a specific DNS operation. |
| DNSPolicyIgnore | Ignores a specific DNS operation by dropping the related query. |
| DnsPolicyActionMax | Shows the maximum action types supported. |

###### DNS\_RPC\_POLICY\_TYPE

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The DNS\_RPC\_POLICY\_TYPE enumeration specifies the DNS operation for which the DNS policy is applicable.

| Enumerator Value | Description |
| --- | --- |
| DnsPolicyQueryProcessing=0 | The DNS policy is applicable for DNS queries. |
| DnsPolicyRecursion | The DNS policy is applicable for recursive queries. |

###### DNS\_RPC\_CRITERIA\_ENUM

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The DNS\_RPC\_CRITERIA\_ENUM enumeration specifies the various criteria that a DNS server needs to match during a DNS operation to have a successful DNS policy match. For more information, see section [3.1.8.2](#Section_38bc9b8b84ec47b68964b900b426918e).

| Enumerator Value | Description |
| --- | --- |
| DnsPolicyCriteriaFqdn=0 | This specifies that the criteria for match of a DNS policy is based on the query name in the question section [[RFC1034]](http://go.microsoft.com/fwlink/?LinkId=90263) section 3.7 of a DNS query, in a DNS operation. |
| DnsPolicyCriteriaSubnet | This specifies that the criteria for match of a DNS policy is based on the client subnet record, derived from the IP address of a resolver [RFC1034] section 2.4 in a DNS Operation. |
| DnsPolicyCriteriaInterface | This specifies that the criteria for match of a DNS policy is based on the IP address on which the DNS server receives the DNS query in a DNS operation. |
| DnsPolicyCriteriaQtype | This specifies that the criteria for match of a DNS policy is based on the QTYPE [[RFC1035]](http://go.microsoft.com/fwlink/?LinkId=90264) section 3.2.3 of a DNS query in a DNS operation. |
| DnsPolicyCriteriaTime | This specifies that the criteria for match of a DNS policy is based on the time of day, in minutes, when the DNS server receives a DNS query during a DNS operation. |
| DnsPolicyCriteriaTransportProtocol | This specifies that the criteria for match of a DNS policy is based on the transport layer protocol (TCP or UDP) used to send a DNS query to the DNS server during a DNS operation. |
| DnsPolicyCriteriaNetworkProtocol | This specifies that the criteria for match of a DNS policy is based on the Internet protocol used (IPv4 or IPv6) to send a DNS query to the DNS server during a DNS operation. |
| DnsPolicyCriteriaMax | This shows the maximum number of criteria type supported by DNS policy. |

#### Structures

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

##### DNS\_RPC\_CLIENT\_SUBNET\_RECORD

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The DNS\_RPC\_CLIENT\_SUBNET\_RECORD structure contains the IPv4 and IPv6 subnets that are grouped together.

1. typedef struct \_ClientSubnetRecord {
2. LPWSTR pwszClientSubnetName;
3. PDNS\_ADDR\_ARRAY pIPAddr;
4. PDNS\_ADDR\_ARRAY pIPv6Addr;
5. } DNS\_RPC\_CLIENT\_SUBNET\_RECORD,
6. \*PDNS\_RPC\_CLIENT\_SUBNET\_RECORD;

**pwszClientSubnetName:**   (variable) A NULL-terminated Unicode string containing the name of the client subnet record.

**pIPAddr:**  A pointer to a [DNS\_ADDR\_ARRAY (section 2.2.3.2.3)](#Section_56ba5fabf304486699a44f1c1f9247a3) structure that contains a list of IP subnets contained in this client subnet record along with the SubnetLength as defined in [DNS ADD USER (section 2.2.3.2.2.2)](#Section_6e041c763b55480a84fbfeebcb0cc9db).

**pIPv6Addr:**  A pointer to a DNS\_ADDR\_ARRAY structure that contains a list of IPv6 subnets contained in this client subnet record along with the SubnetLength as defined in DNS ADD USER.

##### DNS\_RPC\_POLICY\_CONTENT

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The DNS\_RPC\_POLICY\_CONTENT structure contains the zone scope, cache scope, or server scope details that are used to service the DNS operation if a DNS policy’s [DNS\_RPC\_POLICY\_ACTION\_TYPE (section 2.2.15.1.1.4)](#Section_11503add9e7b455b8d491c9653e04e80) is DnsPolicyAllow.

1. typedef struct \_DnssrvRpcPolicyActionContent {
2. LPWSTR pwszScopeName;
3. DWORD dwWeight;
4. } DNS\_RPC\_POLICY\_CONTENT,
5. \*PDNS\_RPC\_POLICY\_CONTENT;

**pwszScopeName:**  A NULL-terminated Unicode string containing the name of the zone scope, cache scope or server scope.

**dwWeight:**  A 32-bit unsigned integer that specifies the weight associated with the scope name. The weight of a scope determines the number of responses that are sent from that scope. For example, if a DNS\_RPC\_POLICY has pContentList with two DNS\_RPC\_POLICY\_CONTENT items having scope name and weight as {Scope1,2} and {Scope2,3}, then when the DNS policy is a match, Scope1 is used to respond to the DNS operation for the first two times the DNS policy is a match. Scope2 is used to respond to the DNS operation for the next three times the DNS policy is a match. The sequence is repeated for further matches of the DNS policy. If a **dwWeight** of a DNS\_RPC\_POLICY\_CONTENT is not given. its default weight is 1. So if two or more DNS\_RPC\_POLICY\_CONTENT structures are given during DNS\_RPC\_POLICY creation without a value for **dwWeight**, all of them will get weight of 1 and the DNS operation will be performed from each scope in a round-robin fashion. Allowed values for weight are any positive number from 1 and higher to 0xffffffff. If 0 is sent as a weight, the DNS server returns the error DNS\_ERROR\_POLICY\_INVALID\_WEIGHT.

##### DNS\_RPC\_POLICY\_CONTENT\_LIST

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The DNS\_RPC\_POLICY\_CONTENT\_LIST structure contains a list of [DNS\_RPC\_POLICY\_CONTENT](#Section_dd2e4ce56eea4dc4b9f7058eb9703381) structures configured for a DNS policy.

1. typedef struct \_DnssrvRpcPolicyAction {
2. DWORD dwContentCount;
3. PDNS\_RPC\_POLICY\_CONTENT pContent[1];
4. } DNS\_RPC\_POLICY\_CONTENT\_LIST,
5. \*PDNS\_RPC\_POLICY\_CONTENT\_LIST;

**dwContentCount:**  An unsigned integer specifying the number of DNS\_RPC\_POLICY\_CONTENT elements present.

**pContent:**  An array of pointers to DNS\_RPC\_POLICY\_CONTENT structure.

##### DNS\_RPC\_CRITERIA

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The DNS\_RPC\_CRITERIA structure contains the DNS policy criteria that is associated with a DNS policy.

1. typedef struct {
2. DNS\_RPC\_CRITERIA\_ENUM type;
3. LPWSTR pCriteria;
4. } DNS\_RPC\_CRITERIA,
5. \*PDNS\_RPC\_CRITERIA;

**type:**  This specifies the type of criteria associated with the DNS policy. The value is of type [DNS\_RPC\_CRITERIA\_ENUM (section 2.2.15.1.1.6)](#Section_4b707d19860c461eb7c57e6322db26e9).

**pCriteria:**  A NULL-terminated Unicode string containing the DNS policy criteria details.

##### DNS\_RPC\_POLICY

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The DNS\_RPC\_POLICY structure contains all details associated with a DNS policy.

1. typedef struct \_DnssrvRpcPolicy {
2. LPWSTR pwszPolicyName;
3. DNS\_RPC\_POLICY\_LEVEL level;
4. DNS\_RPC\_POLICY\_TYPE appliesOn;
5. DNS\_RPC\_POLICY\_ACTION\_TYPE action;
6. DNS\_RPC\_POLICY\_CONDITION condition;
7. BOOL isEnabled;
8. DWORD dwProcessingOrder;
9. LPSTR pszZoneName;
10. PDNS\_RPC\_POLICY\_CONTENT\_LIST pContentList;
11. DWORDLONG flags;
12. DWORD dwCriteriaCount;
13. PDNS\_RPC\_CRITERIA pCriteriaList[1];
14. } DNS\_RPC\_POLICY,
15. \*PDNS\_RPC\_POLICY;

**pwszPolicyName:**  A NULL-terminated Unicode string containing the name of the DNS policy. The name is unique across a level as specified in [DNS\_RPC\_POLICY\_LEVEL (section 2.2.15.1.1.3)](#Section_1519cc9db58848fbb3afe16b319b805e).

**level:**  This specifies whether the policy is configured for a zone (including a cache zone) or is at server level. The value is of type DNS\_RPC\_POLICY\_LEVEL.

**appliesOn:**  This specifies the DNS operation for which the DNS policy is applicable. The value is of type [DNS\_RPC\_POLICY\_TYPE (section 2.2.15.1.1.5)](#Section_e2e0048d03a845dcbc27b7a4ad14d737).

**action:**  This specifies the action to be applied on a DNS operation when there is a DNS policy match. The value is of type [DNS\_RPC\_POLICY\_ACTION\_TYPE (section 2.2.15.1.1.4)](#Section_11503add9e7b455b8d491c9653e04e80).

**condition:**  This specifies the logical operation across the DNS policy criteria of a DNS policy, which determines whether the DNS policy match has succeeded or failed. The value is of type [DNS\_RPC\_POLICY\_CONDITION (section 2.2.15.1.1.2)](#Section_6b98c962d2084475ae181a068b4b925c).

**isEnabled:**  A BOOL variable that specifies whether a DNS policy is enabled. TRUE indicates that the DNS policy MUST be applied to the DNS operation; FALSE indicates that the DNS policy is disabled and MUST NOT be applied to the DNS operation.

**dwProcessingOrder:**  An unsigned integer that specifies the order in which this DNS policy is processed, along with 0 or more other DNS policies for a given level 2.2.15.1.1.3 and DNS\_RPC\_POLICY\_TYPE (section 2.2.15.1.1.5) during a DNS operation.

**pszZoneName:**  A NULL-terminated string containing the name of the zone for which this DNS policy is configured.

**pContentList:**  An object of type [DNS\_RPC\_POLICY\_CONTENT\_LIST (section 2.2.15.2.3)](#Section_5e1af43060b242a6958e5e7c661ab99d) that has a list of zone scope, cache scope, or server scope with weight as defined in [DNS\_RPC\_POLICY\_CONTENT (section 2.2.15.2.2)](#Section_dd2e4ce56eea4dc4b9f7058eb9703381). If the DNS policy matches the criteria in **pCriteriaList** and its action is DnsPolicyAllow, then the zone scopes, cache scopes, or server scopes contained in pContentList are used in the DNS operation as per their **dwWeight**.

**flags:**  This is used during update of a DNS policy. The various bits of flags show which members of the DNS Policy are to be updated. For possible values of the bits of flags. see section [2.2.15.1.1](#Section_a37b8ff71a784a159ce4cbe38d41cc19). For details on how this is used during a policy update, see the operation UpdatePolicy in section [3.1.4.1](#Section_9500a7e8165d4b13be860ddc43100eef).

**dwCriteriaCount:**  An unsigned integer containing the number of DNS policy criteria that are configured for this DNS policy.

**pCriteriaList:**  An array of [DNS\_RPC\_CRITERIA (section 2.2.15.2.4)](#Section_be16f14ddf7440fe892c0718ebd32e84) that are compared with each other using condition DNS\_RPC\_POLICY\_CONDITION (section 2.2.15.1.1.2) to match a DNS policy.

##### DNS\_RPC\_POLICY\_NAME

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The DNS\_RPC\_POLICY\_NAME structure contains the details of the DNS policy when the DNS policies are enumerated at a specified level (section [2.2.15.1.1.3](#Section_1519cc9db58848fbb3afe16b319b805e)).

1. typedef struct \_DnsRpcPolicyType {
2. LPWSTR pwszPolicyName;
3. DNS\_RPC\_POLICY\_TYPE appliesOn;
4. BOOL fEnabled;
5. DWORD processingOrder;
6. } DNS\_RPC\_POLICY\_NAME,
7. \*PDNS\_RPC\_POLICY\_NAME;

**pwszPolicyName:**  A NULL-terminated Unicode string containing the name of the DNS policy. The name is unique across a level as specified in DNS\_RPC\_POLICY\_LEVEL (section 2.2.15.1.1.3).

**appliesOn:**  This specifies the DNS operation to which the DNS policy applies. The value is of type [DNS\_RPC\_POLICY\_TYPE (section 2.2.15.1.1.5)](#Section_e2e0048d03a845dcbc27b7a4ad14d737).

**fEnabled:**  A BOOL variable that specifies whether a DNS policy is enabled.

**processingOrder:**  An unsigned integer that specifies the order in which this DNS policy is processed, along with 0 or more other DNS policies for a given level (section 2.2.15.1.1.3) and DNS\_RPC\_POLICY\_TYPE (section 2.2.15.1.1.5) during a DNS operation.

##### DNS\_RPC\_ENUMERATE\_POLICY\_LIST

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The DNS\_RPC\_ENUMERATE\_POLICY\_LIST structure contains all the DNS policies at a specified level (section [2.2.15.1.1.3](#Section_1519cc9db58848fbb3afe16b319b805e)).

1. typedef struct \_DnsRpcEnumPolicyList {
2. DWORD dwPolicyCount;
3. PDNS\_RPC\_POLICY\_NAME pPolicyArray[1];
4. } DNS\_RPC\_ENUMERATE\_POLICY\_LIST,
5. \*PDNS\_RPC\_ENUMERATE\_POLICY\_LIST;

**dwPolicyCount:**  An unsigned integer that specifies the total number of DNS\_RPC\_POLICY\_NAME elements.

**pPolicyArray:**  An array of pointers of [DNS\_RPC\_POLICY\_NAME (section 2.2.15.2.6)](#Section_c97d6de9ddf44579bdece242bccb349d) structures.

## Directory Service Schema Elements

The DNS Server Management Protocol accesses the directory service schema classes and attributes listed in the following table. Those listed as unused are read and stored, but not processed by the protocol. For the syntactic specifications of the following Class or Class/Attribute pairs, refer to: [[MS-ADSC]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ADSC%5d.pdf), [[MS-ADA1]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ADA1%5d.pdf), [[MS-ADA2]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ADA2%5d.pdf), and [[MS-ADA3]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ADA3%5d.pdf). The specifications of the dnsProperty and dnsRecord attributes are described in this section.[<86>](#Appendix_A_86)

| Class | Attribute |
| --- | --- |
| container | displayName  ntSecurityDescriptor |
| crossRef | dnsRoot  Enabled  msDS-NC-Replica-Locations  msDS-NC-RO-Replica-Locations  nCName  ntSecurityDescriptor  objectClass  systemFlags  msDS-Behavior-Version  usnChanged (unused) |
| crossRefContainer | fSMORoleOwner  msDS-Behavior-Version |
| dnsZone[<87>](#Appendix_A_87) | dnsProperty  ntSecurityDescriptor  objectGUID  whenChanged  msDNS-IsSigned  msDNS-NSEC3OptOut  msDNS-SigningKeys  msDNS-SignWithNSEC3  msDNS-NSEC3UserSalt  msDNS-DNSKEYRecords  msDNS-DSRecordSetTTL  msDNS-NSEC3Iterations  msDNS-PropagationTime  msDNS-NSEC3CurrentSalt  msDNS-RFC5011KeyRollovers  msDNS-NSEC3HashAlgorithm  msDNS-DSRecordAlgorithms  msDNS-DNSKEYRecordSetTTL  msDNS-MaintainTrustAnchor  msDNS-NSEC3RandomSaltLength  msDNS-SigningKeyDescriptors  msDNS-SignatureInceptionOffset  msDNS-ParentHasSecureDelegation  msDNS-SecureDelegationPollingPeriod |
| dnsNode | dnsRecord  dnsTombstoned  whenChanged  usnChanged (unused) |
| domainDns | instanceType |
| group | groupType |
| nTDSDSA | hasMasterNCs  msDS-Behavior-Version  msDS-HasMasterNCs |
| rootDse | configurationNamingContext  defaultNamingContext  dnsHostName  dsServiceName  namingContexts  rootDomainNamingContext  schemaNamingContext  serverName  supportedCapabilities |
| msDNS-ServerSettings | msDNS-KeymasterZones |

### Object Classes

#### msDNS-ServerSettings

An object of this object class MUST be created (if it does not already exist) by any DNS server that becomes the [**key master**](#gt_0e6ec17a-5cf0-43f5-8454-e4c229c632a3) for a directory service-integrated zone.[<88>](#Appendix_A_88) The object MUST exist in the directory service as a sibling object of (sharing the same parent object as) the object given by the dsServiceName attribute in the rootDse object on the key master server.

### Attributes

#### dnsProperty

The dnsProperty attribute is used to store zone properties. This attribute MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| DataLength | | | | | | | | NameLength | | | | | | | | Flag | | | | | | | | Version | | | | | | | |
| Id | | | | | | | | Data (variable) | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Name | | | | | | | |

**DataLength (1 byte):** An unsigned binary integer containing the length, in bytes, of the Data field.

**NameLength (1 byte):** Not Used. The value MUST be ignored and assumed to be 0x00000001.

**Flag (1 byte):** This field is reserved for future use. The value MUST be 0x00000000.

**Version (1 byte):** The version number associated with the property attribute. The value MUST be 0x00000001.

**Id (1 byte):** The property attribute's type. See [Property Id (section 2.3.2.1.1)](#Section_3af638710cc44179916c5caade55a8f3).

**Data (variable):** The data associated with an Id. See Property Id (section 2.3.2.1.1).

**Name (1 byte):** Not used. The value MUST be of length 1 byte, and MUST be ignored.

##### Property Id

The Id specifies the type of data in a dnsProperty's Data field.[<89>](#Appendix_A_89)

| Constant/value | Description |
| --- | --- |
| DSPROPERTY\_ZONE\_TYPE  0x00000001 | The zone type. See [dwZoneType (section 2.2.5.2.4.1)](#Section_e86515440fbb40388232375ff2d8a55e). |
| DSPROPERTY\_ZONE\_ALLOW\_UPDATE  0x00000002 | Whether dynamic updates are allowed. See fAllowUpdate (section 2.2.5.2.4.1). |
| DSPROPERTY\_ZONE\_SECURE\_TIME  0x00000008 | The time at which the zone became secure. See Time Zone Secured ([3.1.1](#Section_e72286df3e4c45359a0ce9cc944248c2)). |
| DSPROPERTY\_ZONE\_NOREFRESH\_INTERVAL  0x00000010 | The zone no refresh interval. See dwNoRefreshInterval (section 2.2.5.2.4.1). |
| DSPROPERTY\_ZONE\_REFRESH\_INTERVAL  0x00000020 | The zone refresh interval. See dwRefreshInterval (section 2.2.5.2.4.1). |
| DSPROPERTY\_ZONE\_AGING\_STATE  0x00000040 | Whether aging is enabled. See fAging (section 2.2.5.2.4.1). |
| DSPROPERTY\_ZONE\_SCAVENGING\_SERVERS  0x00000011 | A list of DNS servers that will perform scavenging. The list is formatted as an [IP4 ARRAY (section 2.2.3.2.1)](#Section_588ae29671bf402f999686ecee39dc29). See aipScavengeServers (section 2.2.5.2.4.1).[<90>](#Appendix_A_90) |
| DSPROPERTY\_ZONE\_AGING\_ENABLED\_TIME  0x00000012 | The time interval before the next scavenging cycle. See dwAvailForScavengeTime (section 2.2.5.2.4.1). |
| DSPROPERTY\_ZONE\_DELETED\_FROM\_HOSTNAME  0x00000080 | The name of the server that deleted the zone. The value is a null-terminated Unicode string. The server SHOULD[<91>](#Appendix_A_91) ignore this value. |
| DSPROPERTY\_ZONE\_MASTER\_SERVERS  0x00000081 | A list of DNS servers that will perform zone transfers. The list is formatted as an IP4 ARRAY (section 2.2.3.2.1). See aipMasters (section 2.2.5.2.4.1).[<92>](#Appendix_A_92) |
| DSPROPERTY\_ZONE\_AUTO\_NS\_SERVERS  0x00000082 | A list of servers which MAY autocreate a delegation. The list is formatted as an IP4 ARRAY (section 2.2.3.2.1).[<93>](#Appendix_A_93) |
| DSPROPERTY\_ZONE\_DCPROMO\_CONVERT  0x00000083 | The flag value representing the state of conversion of the zone. See [DcPromo Flag (section 2.3.2.1.2)](#Section_4ec7bdf71807417996afce1c1cd448b7). |
| DSPROPERTY\_ZONE\_SCAVENGING\_SERVERS\_DA  0x00000090 | A list of DNS servers that will perform scavenging. The list is formatted as a [DNS\_ADDR\_ARRAY (section 2.2.3.2.3)](#Section_56ba5fabf304486699a44f1c1f9247a3). The DNS server MUST read and write the aipScavengeServers (section 2.2.5.2.4.1) setting using property Id DSPROPERTY\_ZONE\_SCAVENGING\_SERVERS and SHOULD also read and write the aipScavengeServers (section 2.2.5.2.4.1) setting using property Id DSPROPERTY\_ZONE\_SCAVENGING\_SERVERS\_DA. During read, if the property values are not identical, the DNS server SHOULD use the property value specified by this property Id. |
| DSPROPERTY\_ZONE\_MASTER\_SERVERS\_DA  0x00000091 | A list of DNS servers that will perform zone transfers. The list is formatted as a DNS\_ADDR\_ARRAY (section 2.2.3.2.3). The DNS server MUST read and write this list using property Id DSPROPERTY\_ZONE\_MASTER\_SERVERS and SHOULD also read and write this list using property Id DSPROPERTY\_ZONE\_MASTER\_SERVERS\_DA. During read, if the property values are not identical, the DNS server SHOULD use the property value specified by this property Id. |
| DSPROPERTY\_ZONE\_AUTO\_NS\_SERVERS\_DA  0x00000092 | A list of servers which MAY autocreate a delegation. The list is formatted as a DNS\_ADDR\_ARRAY (section 2.2.3.2.3) The DNS server MUST read and write this list using property Id DSPROPERTY\_ZONE\_AUTO\_NS\_SERVERS and SHOULD also read and write this list using property Id DSPROPERTY\_ZONE\_AUTO\_NS\_SERVERS\_DA. During read, if the property values are not identical, the DNS server SHOULD use the value specified by property Id. |
| DSPROPERTY\_ZONE\_NODE\_DBFLAGS  0x00000100 | See [DNS\_RPC\_NODE\_FLAGS (section 2.2.2.1.2)](#Section_f448341f512d414aaaa3e303d592fcd2). |

##### DcPromo Flag

The DcPromo flag represents the DcPromo target application directory partition for the zone. If, during zone creation ("ZoneCreate" operation of the R\_Dnssrvoperation (section [3.1.4.1](#Section_9500A7E8165D4B13BE860DDC43100EEF)) method call), a zone is placed into the directory partition that represents the default naming context because the correct directory partition was not available at the time, the zone's DcPromo flag is set appropriately to reflect this. While polling the directory server, and if the time elapsed since the last directory server polling operation is more than 15 minutes, the server SHOULD[<94>](#Appendix_A_94) check whether it is in RODC mode (a server is in RODC mode if ForceRODCMode [section [3.1.1.1.1](#Section_8903E50A91834A7D964053F6F5A91481)] is TRUE or fReadOnlyDC [section [2.2.4.2.2.3](#Section_12233DD4DD644B1C95FD6A566E529AC9)] is TRUE). If the time elapsed is less than 15 minutes, or if the server is in RODC mode, the server MUST NOT perform the following operations. If the server is not in RODC mode and if the DNS server discovers a zone with a nonzero DcPromo flag, the zone and the Zone Access Control List (section [3.1.1](#Section_E72286DF3E4C45359A0CE9CC944248C2)) MUST be moved from their current location to the application directory partition specified in the following table if that partition is now available.[<95>](#Appendix_A_95)

| Constant/value | Description |
| --- | --- |
| DCPROMO\_CONVERT\_NONE  0x00000000 | No change to existing zone storage. |
| DCPROMO\_CONVERT\_DOMAIN  0x00000001 | Zone is to be moved to the DNS domain partition. This is the partition in the Application Directory Partition Table (section 3.1.1) that has the DNS\_DP\_DOMAIN\_DEFAULT bit set in dwDpFlags (section [2.2.5.2.7.2](#Section_f0a445761d3f43ccbece07ae958f5b36)). See DNS\_ZONE\_CREATE\_FOR\_DCPROMO (section [2.2.5.2.7.1](#Section_780eba2615ea43d3a2b377ed9ab00690)).If DownlevelDCsInDomain is nonzero, the zone is to be stored in the directory partition that represents the default naming context. See DNS\_DP\_LEGACY (section [2.2.7.1.1](#Section_27e378aad4d743de8b343e5b957a7130)). |
| DCPROMO\_CONVERT\_FOREST  0x00000002 | Zone is to be moved to the DNS forest partition. This is the partition in the Application Directory Partition Table (section 3.1.1) that has the DNS\_DP\_FOREST\_DEFAULT bit set in dwDpFlags (section 2.2.5.2.7.2). See DNS\_ZONE\_CREATE\_FOR\_DCPROMO\_FOREST (section 2.2.5.2.7.1). |

#### dnsRecord

The dnsRecord attribute is used to store DNS resource record definitions. This attribute MUST be formatted as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| DataLength | | | | | | | | | | | | | | | | Type | | | | | | | | | | | | | | | |
| Version | | | | | | | | Rank | | | | | | | | Flags | | | | | | | | | | | | | | | |
| Serial | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TtlSeconds | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Reserved | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TimeStamp | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Data (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**DataLength (2 bytes):** An unsigned binary integer containing the length, in bytes, of the Data field.

**Type (2 bytes):** The resource record's type. See [DNS\_RECORD\_TYPE (section 2.2.2.1.1)](#Section_39b03b89226440638198d62f62a6441a).

**Version (1 byte):** The version number associated with the resource record attribute. The value MUST be 0x05.

**Rank (1 byte):** The least-significant byte of one of the RANK\* flag values. See [dwFlags (section 2.2.2.2.5)](#Section_ac7939811c6043b8be59cdbb5c4ecb8a).

**Flags (2 bytes):** Not used. The value MUST be 0x0000.

**Serial (4 bytes):** The serial number of the SOA record of the zone containing this resource record. See [DNS\_RPC\_RECORD\_SOA (section 2.2.2.2.4.3)](#Section_dcd3ec16d6bf4bb491286172f9e5f066).

**TtlSeconds (4 bytes):** See dwTtlSeconds (section 2.2.2.2.5). This field uses big-endian byte order.

**Reserved (4 bytes):** This field is reserved for future use. The value MUST be 0x00000000.

**TimeStamp (4 bytes):** See dwTimeStamp (section 2.2.2.2.5).

**Data (variable):** The resource record's data. See [DNS\_RPC\_RECORD\_DATA (section 2.2.2.2.4)](#Section_38b873927f614e3092639f0fb832d084).

#### msDNS-IsSigned

This attribute value MUST correspond to the value of the IsSigned zone property (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)).

#### msDNS-NSEC3OptOut

This attribute value MUST correspond to the value of the NSEC3OptOut zone property (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)).

#### msDNS-SigningKeys

This attribute value MUST contain a collection of exported signing key pairs. Each attribute value MUST be formatted as follows.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| GUID (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ExportedKey (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**GUID (16 bytes):** A GUID value that corresponds to an active, standby, or next key from the [DNS\_RPC\_SKD\_STATE (section 2.2.6.2.3)](#Section_b211f98844044c14b293bafd114b0eb6) structure for one of the signing key descriptors in the zone's signing key descriptor list.

**ExportedKey (variable):** An exported signing key in [Exported Key Pair](#Section_820903b3170440b6b977ac9154a90ffd) format. When this attribute value is written, the DNS server MUST follow the procedure in section [3.1.7.1](#Section_33a9931f7e064a44b29214541ad39c84) to export each key. When this attribute value is read, the DNS server MUST follow the procedure in section [3.1.7.2](#Section_9fb68ee30b244878a2804c03ea572c78) to import each key.

#### msDNS-SignWithNSEC3

This attribute value MUST correspond to the value of the SignWithNSEC3 zone property (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)).

#### msDNS-NSEC3UserSalt

This attribute value MUST correspond to the value of the NSEC3UserSalt zone property (section [3.1.1.2.3](#Section_51da10a5d508497dae49525a332d055b)).

#### msDNS-DNSKEYRecords

This attribute value MUST contain the DNSKEY records and all RRSIG records covering type DNSKEY for the root of the zone as specified by [[RFC4035]](http://go.microsoft.com/fwlink/?LinkID=107053).

#### msDNS-DSRecordSetTTL

This attribute value MUST correspond to the value of the DSRecordSetTTL zone property (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)).

#### msDNS-NSEC3Iterations

This attribute value MUST correspond to the value of the NSEC3Iterations zone property (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)).

#### msDNS-PropagationTime

This attribute value MUST correspond to the value of the PropagationTime zone property (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)).

#### msDNS-NSEC3CurrentSalt

This attribute value MUST correspond to the value of the NSEC3CurrentSalt zone property (section [3.1.1.2.3](#Section_51da10a5d508497dae49525a332d055b)).

#### msDNS-RFC5011KeyRollovers

This attribute value MUST correspond to the value of the RFC5011KeyRollovers zone property (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)).

#### msDNS-NSEC3HashAlgorithm

This attribute value MUST correspond to the value of the NSEC3HashAlgorithm zone property (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)).

#### msDNS-DSRecordAlgorithms

This attribute value MUST correspond to the value of the DSRecordAlgorithms zone property (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)).

#### msDNS-DNSKEYRecordSetTTL

This attribute value MUST correspond to the value of the DNSKEYRecordSetTTL zone property (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)).

#### msDNS-MaintainTrustAnchor

This attribute value MUST correspond to the value of the MaintainTrustAnchor zone property (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)).

#### msDNS-NSEC3RandomSaltLength

This attribute value MUST correspond to the value of the NSEC3RandomSaltLength zone property (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)).

#### msDNS-SigningKeyDescriptors

This attribute is used to store the zone's signing key descriptor list. Each value of this attribute represents a single signing key descriptor and MUST be formatted as follows.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Version | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| fIsKsk | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Guid (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| pwszKeyStorageProvider (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| bSigningAlgorithm | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwKeyLength | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwInitialRolloverOffset | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwDNSKEYSignatureValidityPeriod | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwDSSignatureValidityPeriod | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwStandardSignatureValidityPeriod | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwRolloverType | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwRolloverPeriod | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwNextRolloverAction | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ftLastRolloverTime | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ftNextRolloverTime | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwState | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwCurrentRolloverStatus | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwCurrentRollState | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| fManualTrigger | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dwPreRollEventFired | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ftNextKeyGenerationTime | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RevokedOrSwappedRecordCount | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FinalRecordCount | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| pwszActiveKey (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ActiveKeyScope | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| pwszStandbyKey (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StandbyKeyScope | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| pwszNextKey (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NextKeyScope | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RevokedOrSwappedDnskeys (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FinalDnskeys (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Version (4 bytes):** This value MUST be 0x00000001.

**fIsKsk (4 bytes):** The value of this field MUST correspond to the value from the [DNS\_RPC\_SKD (section 2.2.6.2.1)](#Section_f7b0ad424cae40fd87c882af83824639) structure for this signing key descriptor.

**Guid (16 bytes):** The value of this field MUST correspond to the value from the DNS\_RPC\_SKD (section 2.2.6.2.1) structure for this signing key descriptor.

**pwszKeyStorageProvider (variable):** The value of this field MUST correspond to the value from the DNS\_RPC\_SKD (section 2.2.6.2.1) structure for this signing key descriptor.

**bSigningAlgorithm (4 bytes):** The value of this field MUST correspond to the value from the DNS\_RPC\_SKD (section 2.2.6.2.1) structure for this signing key descriptor.

**dwKeyLength (4 bytes):** The value of this field MUST correspond to the value from the DNS\_RPC\_SKD (section 2.2.6.2.1) structure for this signing key descriptor.

**dwInitialRolloverOffset (4 bytes):** The value of this field MUST correspond to the value from the DNS\_RPC\_SKD (section 2.2.6.2.1) structure for this signing key descriptor.

**dwDNSKEYSignatureValidityPeriod (4 bytes):** The value of this field MUST correspond to the value from the DNS\_RPC\_SKD (section 2.2.6.2.1) structure for this signing key descriptor.

**dwDSSignatureValidityPeriod (4 bytes):** The value of this field MUST correspond to the value from the DNS\_RPC\_SKD (section 2.2.6.2.1) structure for this signing key descriptor.

**dwStandardSignatureValidityPeriod (4 bytes):** The value of this field MUST correspond to the value from the DNS\_RPC\_SKD (section 2.2.6.2.1) structure for this signing key descriptor.

**dwRolloverType (4 bytes):** The value of this field MUST correspond to the value from the DNS\_RPC\_SKD (section 2.2.6.2.1) structure for this signing key descriptor.

**dwRolloverPeriod (4 bytes):** The value of this field MUST correspond to the value from the DNS\_RPC\_SKD (section 2.2.6.2.1) structure for this signing key descriptor.

**dwNextRolloverAction (4 bytes):** The value of this field MUST correspond to the value from the DNS\_RPC\_SKD (section 2.2.6.2.1) structure for this signing key descriptor.

**ftLastRolloverTime (8 bytes):** This value MUST correspond to the value of **ftLastRolloverTime** from the [DNS\_RPC\_SKD\_STATE (section 2.2.6.2.3)](#Section_b211f98844044c14b293bafd114b0eb6) structure for this signing descriptor.

**ftNextRolloverTime (8 bytes):** This value MUST correspond to the value of **ftNextRolloverTime** from the DNS\_RPC\_SKD\_STATE (section 2.2.6.2.3) structure for this signing descriptor.

**dwState (4 bytes):** This value MUST correspond to the value of **dwState** from the DNS\_RPC\_SKD\_STATE (section 2.2.6.2.3) structure for this signing descriptor.

**dwCurrentRolloverStatus (4 bytes):** This value MUST correspond to the value of **dwCurrentRolloverStatus** from the DNS\_RPC\_SKD\_STATE (section 2.2.6.2.3) structure for this signing descriptor.

**dwCurrentRollState (4 bytes):** This value corresponds to the next step in a signing key descriptor's rollover process and MUST be set to one of the following values.

| Value | Meaning |
| --- | --- |
| DNS\_SKD\_ROLL\_STATE\_NOT\_STARTED  0x00000000 | The signing key descriptor is not currently in the process of rolling over keys. |
| DNS\_SKD\_ROLL\_STATE\_ZSK\_SWAP  0x00000001 | The next step for a signing key descriptor whose "fIsKSK" field is 0x00000000 is to move into the "new RRSIGs" phase of the pre-publish key rollover, as described in [[RFC4641]](http://go.microsoft.com/fwlink/?LinkId=225979) section 4.2.1.1. |
| DNS\_SKD\_ROLL\_STATE\_ZSK\_FINISH  0x00000002 | The next step for a signing key descriptor whose "fIsKSK" field is 0x00000000 is to move into the "DNSKEY removal" phase of the pre-publish key rollover, as described in [RFC4641] section 4.2.1.1. |
| DNS\_SKD\_ROLL\_STATE\_KSK\_DS\_WAIT  0x00000003 | The next step for a signing key descriptor whose "fIsKSK" field is 0x00000001 is to wait for the "DS change" step of the "Key Signing Key Rollovers" process, as described in [RFC4641] section 4.2.2. |
| DNS\_SKD\_ROLL\_STATE\_KSK\_REVOKE  0x00000004 | The next step for a signing key descriptor whose "fIsKSK" field is 0x00000001 is to revoke a key according to [[RFC5011]](http://go.microsoft.com/fwlink/?LinkId=225980) section 6.3 or 6.5. |
| DNS\_SKD\_ROLL\_STATE\_KSK\_FINISH  0x00000005 | The next step for a signing key descriptor whose "fIsKSK" field is 0x00000001 is to move into the "DNSKEY removal" phase of the "Key Signing Key Rollovers" process, as described in [RFC4641] section 4.2.2. |

**fManualTrigger (4 bytes):** This value MUST be set to 0x00000001 in response to a successful "ZonePerformKeyRollover" operation on a signing key descriptor. When the SKD completes its rollover, this value MUST be set to 0x00000000.

**dwPreRollEventFired (4 bytes):** This value MUST be set to 0x00000001 when 90 percent of the "dwRolloverPeriod" for a signing key descriptor whose "fIsKSK" flag is 0x00000001 has elapsed. It MUST be set to 0x00000002 when 95 percent of this rollover period has elapsed, and it MUST be set to 0x00000003 when there is less than 1 day remaining before such a signing key descriptor begins its key rollover process. Otherwise, this value MUST be 0x00000000.

**ftNextKeyGenerationTime (8 bytes):** This value represents the time at which the most recent value of the "pwszNextKey" field of a signing key descriptor whose "fIsKSK" flag is 0x00000000 was generated.

**RevokedOrSwappedRecordCount (4 bytes):** This value MUST indicate the number of values present in the list of records in the **RevokedOrSwappedDnskeys** field.

**FinalRecordCount (4 bytes):** This value MUST indicate the number of values present in the list of records in the **FinalRecordCount** field.

**pwszActiveKey (variable):** This value MUST correspond to the value of **pwszActiveKey** from the DNS\_RPC\_SKD\_STATE (section 2.2.6.2.3) structure for this signing descriptor.

**ActiveKeyScope (4 bytes):** This value corresponds to the signing scope of **pwszActiveKey** and MUST be set to one of the following values.

| Value | Meaning |
| --- | --- |
| DNS\_SIGN\_SCOPE\_DEFAULT  0x00000000 | The key is used for its default purpose: If the signing key descriptor's "fIsKSK" field is set to 0x00000001, the key is used to sign only DNSKEY records in the zone. If the signing key descriptor's "fIsKSK" field is set to 0x00000000, the key is used to sign all records in the zone. |
| DNS\_SIGN\_SCOPE\_DNSKEY\_ONLY  0x00000001 | The key is used to sign only DNSKEY records in the zone. |
| DNS\_SIGN\_SCOPE\_ALL\_RECORDS  0x00000002 | The key is used to sign all records in the zone. |
| DNS\_SIGN\_SCOPE\_ADD\_ONLY  0x00000003 | The key is published as a DNSKEY in the zone, but it is not used to sign any records. |
| DNS\_SIGN\_SCOPE\_DO\_NOT\_PUBLISH  0x00000004 | The key is not published to the zone and is not used to sign any records. |
| DNS\_SIGN\_SCOPE\_REVOKED  0x00000005 | The key is published as a DNSKEY in the zone with its "Revoked" bit ([RFC5011] section 2.1) set. It is used to sign DNSKEY records. |

**pwszStandbyKey (variable):** This value MUST correspond to the value of **pwszStandbyKey** from the DNS\_RPC\_SKD\_STATE (section 2.2.6.2.3) structure for this signing descriptor.

**StandbyKeyScope (4 bytes):** This value corresponds to the signing scope of **pwszActiveKey** and MUST be set to one of the values previously described for "ActiveKeyScope".

**pwszNextKey (variable):** This value MUST correspond to the value of **pwszNextKey** from the DNS\_RPC\_SKD\_STATE (section 2.2.6.2.3) structure for this signing descriptor.

**NextKeyScope (4 bytes):** This value corresponds to the signing scope of **pwszNextKey** and MUST be set to one of the values previously described for "ActiveKeyScope".

**RevokedOrSwappedDnskeys (variable):** This field MUST contain a variable number of DNS records in the same format as the dnsRecord attribute (section [2.3.2.2](#Section_6912b33854724f59b9120edb536b6ed8)). The number of records in this list is specified by **RevokedOrSwappedRecordCount**. If **RevokedOrSwappedRecordCount** is zero, the length of this field MUST be 0 bytes. The DNS records in this field correspond to a precomputed list of DNSKEY and associated RRSIG records that are published to the zone as the SKD transitions into DNS\_SKD\_STATUS\_ZSK\_WAITING\_FOR\_MAXZONE\_TTL status if the signing key descriptor's "fIsKSK" field is set to 0x00000000, and as the SKD transitions into DKS\_SKD\_STATUS\_KSK\_WAITING\_FOR\_5011\_REMOVE\_HOLD\_DOWN if the signing key descriptor's "fIsKSK" field is set to 0x00000001.

**FinalDnskeys (variable):** This field MUST contain a number of DNS records in the same format as the dnsRecord attribute (section 2.3.2.2). The number of records in this list is specified by **FinalRecordCount**. If **FinalRecordCount** is zero, the length of this field MUST be 0 bytes. The DNS records in this field correspond to a precomputed list of DNSKEY and associated RRSIG records that are published to the zone as the signing key descriptor's key rollover process concludes.

#### msDNS-SignatureInceptionOffset

This attribute value MUST correspond to the value of the SignatureInceptionOffset zone property (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)).

#### msDNS-ParentHasSecureDelegation

This attribute value MUST correspond to the value of the ParentHasSecureDelegation zone property (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)).

#### msDNS-SecureDelegationPollingPeriod

This attribute value MUST correspond to the value of the SecureDelegationPollingPeriod zone property (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)).

#### msDNS-KeymasterZones

This attribute MUST contain a list of distinguished names for all of the directory service-integrated zones for which the DNS server is the key master.

# Protocol Details

No additional timers or other state is required on the client side of this protocol. Calls made by the higher-layer protocol or application are passed directly to the transport, and the results returned by the transport are passed directly back to the higher-layer protocol or application.

The following sections specify details of the DNS DnsServer Remote Protocol, including abstract data models, interface method syntax, and message processing rules.

## DnsServer Server Details

The DNS Server Management Protocol is stateless; that is, each message in the protocol is independent. Furthermore, the running state of the zone on the server does not affect this protocol. The type of zone (primary, secondary, stub, and so on) can determine which method calls can be executed successfully using that zone. Restrictions on zone type are specified in the descriptions of the method calls.

Certain actions taken by the server require an underlying protocol. For example, the **EnlistDirectoryPartition** operation of the R\_Dnssrvoperation (section [3.1.4.1](#Section_9500a7e8165d4b13be860ddc43100eef)) method call can cause the server to communicate with the Active Directory server with a separate protocol. Implementations encountering error events or error code returns in the execution of these underlying protocols can, in certain cases, generate an error return for the DNS protocol. Where this is the case, the description of the action undertaken will specify that an error code can be returned.

### Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

**Global Server State:** The global state of the server set to one of the following values:

* Loading: the DNS server is loading configuration and zone data.
* Running: the DNS server has loaded all data and is serving queries.
* Stopping: the DNS server is shutting down.

**DNS Server Configuration:** Configuration information for the server, in persistent storage, in the form of (name, value) pairs. The list of metadata information can be found in section [3.1.1.1](#Section_c4833797156c4c48a380d40dd1760eb9).

**DNS Server AD Connection:** An ADCONNECTION\_HANDLE as defined in [[MS-DTYP]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-DTYP%5d.pdf) section 2.2.2. This element is used every time the DNS server needs to communicate to the directory server.

**DNS Server Configuration Access Control List:** An access control list that specifies what client identities have read and write permissions on the DNS Server Configuration. If the DNS server is directory server integrated, the [**access control list**](#gt_9f92aa05-dd0a-45f2-88d6-89f1fb654395) is stored in the local directory server.[<96>](#Appendix_A_96) Otherwise, this access control list is not stored in persistent storage and is dynamically created at server start time.[<97>](#Appendix_A_97)

**DNS Zone Table:** Configuration information for DNS zones, in persistent and in-memory storage. The Zone Table can be stored persistently either in a file or in the local directory server, but not both simultaneously. The Zone Table also resides in-memory, behaving as a cache containing the current working copy of both zones loaded from persistent storage, as well as zones retrieved from remote DNS servers. A query to a zone MUST be responded to using only the data in the corresponding in-memory zone. A modification to any elements of a zone, such as a DNS update of records [[RFC2136]](http://go.microsoft.com/fwlink/?LinkId=107017), MUST be reflected immediately in the corresponding in-memory zone and MUST be immediately transactionally committed to DS-integrated storage afterwards (see "WriteDirtyZones" in section [3.1.4.1](#Section_9500a7e8165d4b13be860ddc43100eef)). Each update to the in-memory zone MUST be atomic. If an update to the in-memory zone does not succeed, the in-memory zone MUST be restored to its previous state before the update. Queries to a zone during an in-memory zone modification process are responded to using the post-update zone state. For zones stored in the local directory server, this table may include zones that are in the process of being deleted (see "DeleteZoneFromDs" in section 3.1.4.1).

The in-memory DNS Zone Table is used for queries and modifications for all zone operations (see section [3.1.4](#Section_bdffbbf3e31b49ba8b8d8abde125a9d8)). The in-memory Zone Table is populated during server initialization per-zone from either the local persistent storage or DS-integrated Zone Table. When modifications are made to a zone, such as after a DNS update or zone transfer, the changes are reflected first in the in-memory Zone Table, which is then copied per zone, for all zone types except DNS\_ZONE\_TYPE\_CACHE (section [2.2.5.1.1](#Section_27e138a7110c44a4afcbb95f35f00306)), to either the local persistent storage or immediately to the DS-integrated Zone Table. In-memory data retrieved from remote DNS servers are not copied to local persistent or DS-integrated storage, except for secondary zones with an fDsIntegrated value of FALSE (section [2.2.5.2.6](#Section_fc8b181af8b84953992e8102008d23cd)), which MUST eventually be copied to local persistent storage. For DS-integrated zones, the server polls the directory server using the LDAP protocol every DsPollingInterval (section 3.1.1.1) to copy DS-integrated zones to the respective in-memory zones. If an error occurs during polling, the DNS server MUST NOT mark the zone as shutdown (see section [2.2.5.2.2](#Section_015f97afba5048bbaf444a542f3ff44a)) and MUST attempt to poll the zone again after DsPollingInterval (section 3.1.1.1) seconds have elapsed. Zones of type DNS\_ZONE\_TYPE\_CACHE (section 2.2.5.1.1) are never written to persistent storage. All contents of a zone of type DNS\_ZONE\_TYPE\_CACHE MUST be discarded when the DNS server process is terminated or when the "ClearCache" operation (section 3.1.4.1) is executed.

The local persistent storage DNS Zone Table is copied to the in-memory DNS Zone Table on server initialization and is copied from the in-memory Zone Table after a modification to the in-memory Zone Table is complete.

The directory server-integrated DNS Zone Table is copied to the in-memory DNS Zone Table on server initialization and is copied from the in-memory Zone Table immediately after a modification to the in-memory Zone Table is complete. When changes occur in the DS-integrated Zone Table, the changes are not reflected in the in-memory Zone Table until the DNS server polls the directory server to update the in-memory Zone Table with the modified DS-integrated Zone Table. If changes happened simultaneously to the in-memory Zone Table and the DS-integrated Zone Table, then the post-modified DS-integrated Zone Table is copied to and overwrites the in-memory Zone Table.

For each zone, the DNS Zone Table consists of the following:

**Zone Name:** The name of the zone.

**Zone Status:** Operational state information pertaining to the zone, such as the information in DNS\_RPC\_ZONE\_FLAGS (section 2.2.5.2.2).

**Metadata:** Configuration information for the zone, in the form of (name, value) pairs. The list of metadata information can be found in section [3.1.1.2](#Section_8df021b347ad4829a1c25588165c27e7).

**Zone GUID:** A [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) associated with the zone. The default value of this property MUST be NULL. If this zone is stored in the directory server, then this value is initialized from the **objectGUID** attribute of the associated "dnsZone" object in the DS-integrated DNS Zone Table, which is generated as specified in [[MS-ADTS]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ADTS%5d.pdf), section 3.1.1.1.2, when the zone is first added to the directory server. When the server polls the directory server and discovers that a zone has been deleted from the DS-integrated DNS Zone Table, it uses the **objectGUID** attribute of that "dnsZone" object to identify the corresponding zone in the in-memory copy of the DNS Zone Table.

**DNS Nodes and Records:** The collection of DNS records for each DNS zone. Each distinct DNS owner name (see [[RFC1035]](http://go.microsoft.com/fwlink/?LinkId=90264)) present in the zone is represented by a node. Each node in the zone has a collection of DNS records that pertain to the DNS owner name of the node. Each DNS record also has metadata which is specified in section 3.1.1.2. The collection of DNS nodes and records for each zone MUST contain a node representing the name of the zone itself, which MUST contain an SOA record that stores the fields present in the DNS\_RPC\_RECORD\_SOA structure (section [2.2.2.2.4.3](#Section_DCD3EC16D6BF4BB491286172F9E5F066)). The zone serial number is stored in the dwSerialNo field of this SOA record. DNS records may be accessed or updated by the local directory server through directory server replication and by remote DNS servers through the DNS protocol [RFC1035] and DNS update [RFC2136].

**DNS Node Tombstone State:** Each node in a zone MAY have a Boolean value indicating if this DNS node is a tombstone.[<98>](#Appendix_A_98)

**Zone Access Control List:** An access control list that specifies what client identities have permissions on this DNS Zone. If the zone is stored in the directory server, the access control list is stored in the **ntSecurityDescriptor** attribute of the "dnsZone" object (section [2.3](#Section_74db40e109174ecb863d9bce5165ebf3)) and can be modified using standard LDAP modify operations (see [MS-ADTS] section 3.1.1.5.3). If the zone is not stored in the directory server, the zone does not have an access control list associated with it and instead the **DNS Server Configuration Access Control List** is used as the access control list for the zone.[<99>](#Appendix_A_99)

**Last Transferred Zone Serial Number:** The zone serial number that was last sent in a complete [RFC1035] or incremental [[RFC1995]](http://go.microsoft.com/fwlink/?LinkId=106956) zone transfer to a remote DNS server.

**Time of Last SOA Check:** For a secondary or stub zone, the time at which the primary zone was last contacted (whether successfully or unsuccessfully) to compare zone serial numbers. The value is expressed as the number of seconds since the system booted, in unsigned 32-bit integer format. The default value of this property MUST be zero.

**Time Zone Secured:** The time at which the zone's AllowUpdate property (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)) was last changed from any value to ZONE\_UPDATE\_SECURE (section [2.2.6.1.1](#Section_d4b84209f00c478f80d78dd0f1633d9e)). Changes of the zone's AllowUpdate property to any other value MUST NOT cause a change to Time Zone Secured., The value is expressed as the number of seconds since 12:00 A.M. January 1, 1601 Coordinated Universal Time (UTC) in unsigned 64-bit integer format. The default value of this property MUST be zero. If this zone is stored in the local directory server, then this value is initialized from and written to the "whenChanged" attribute of the "dnsZone".

**Dirty Flag:** A Boolean variable present only in the in-memory copy of a zone. Set to true only if the zone has been modified in memory and there is a copy of the zone in persistent storage to which the in-memory modifications have not been committed.

**Signing Key Descriptor List:** A list of zero or more signing key descriptors associated with the zone, used to inform the online signing process. Each entry in this list consists of the fields in the [DNS\_RPC\_SKD](#Section_f7b0ad424cae40fd87c882af83824639) (see section 2.2.6.2.1) and [DNS\_RPC\_SKD\_STATE](#Section_b211f98844044c14b293bafd114b0eb6) (see section 2.2.6.2.3) structures.[<100>](#Appendix_A_100)

**Rollover Queue:** An ordered list of zero or more signing key descriptors in the zone ready for key rollover. A signing key descriptor whose **dwRolloverPeriod** is not 0xFFFFFFFF is automatically added to this queue when **dwRolloverPeriod** seconds have elapsed since the signing key descriptor's last successful key rollover, or since the zone was initially online-signed. A signing key descriptor may be added to this queue prior to this time by invoking the "PerformZoneKeyRollover" operation of the R\_DnssrvOperation (Opnum 0) method (section 3.1.4.1). The DNS server SHOULD[<101>](#Appendix_A_101) perform key rollover on each item in this queue, one at a time, according to the process specified in [[RFC4641]](http://go.microsoft.com/fwlink/?LinkId=225979) and [[RFC5011]](http://go.microsoft.com/fwlink/?LinkId=225980).

**Application Directory Partition Table:** The DNS server SHOULD[<102>](#Appendix_A_102) support the concept of application directory partitions. Each entry in the Application Directory Partition Table, stored in memory, consists of the fields in DNS\_RPC\_DP\_INFO (section [2.2.7.2.1](#Section_bd2a817d6a6940d3befc0c198a9c6e80)). This table is populated during DNS server initialization through queries to the local directory server using the LDAP protocol. To populate this table, the DNS server MUST use LDAP queries to enumerate all objects under "CN=Partitions, CN=Configuration, <Forest DN>" of object class "crossRef" and for each object's read attribute values as specified by the definitions of the fields of DNS\_RPC\_DP\_INFO (section 2.2.7.2.1). Certain fields do not correspond directly to data stored in local directory server (see section 2.2.7.2.1).The Application Directory Partition Table is kept up-to-date as partitions are created or deleted on the local server, by writing changes to the local directory server and immediately polling to refresh the Application Directory Partition Table. The DNS server polls the directory server at an interval specified by DsPollingInterval (see section 3.1.1.1) to reflect changes made by remote directory servers (see section 3.1.4.1). If the default DNS Domain Partition or the default DNS forest partition is not present when polling, the server MUST attempt to create and enlist in these partitions as part of the polling process.

**Application Directory Partition Access Control List:** In addition to the fields in DNS\_RPC\_DP\_INFO 2.2.7.2.1) each entry in the Application Directory Partition Table MUST also contain an access control list stored persistently in the directory server in the **ntSecurityDescriptor** attribute of the "crossRef" object associated with the Application Directory Partition.[<103>](#Appendix_A_103)

**Remote Server Table:** An in-memory state table of EDNS [[RFC2671]](http://go.microsoft.com/fwlink/?LinkId=107022) support statuses of remote DNS servers that the local server has previously contacted. The status of a remote server is cached for the interval specified by EDnsCacheTimeout (section [3.1.1.1.1](#Section_8903E50A91834A7D964053F6F5A91481)). The state of a remote server can be set to one of the following values:

Unknown: the remote server's EDNS **[RFC2671]** support is indeterminate; initial state.

Not supported: the remote server does not support EDNS **[RFC2671]**.

Ok: the remote server supports EDNS **[RFC2671]**.

Maybe not supported: the remote server has not responded, and an EDNS **[RFC2671]** support state cannot yet be determined.

**Statistics:** An in-memory structure whose elements correspond directly with the objects specified in sections [2.2.10.2.4](#Section_238b54f6bfdf4bb891ccc5ddbde6e7ac) through [2.2.10.2.24](#Section_9502a725118042ed91d362d3d43e2365), omitting the "Header" field of each. These values are made available to clients of the DNS Server Management Protocol by the DNS Server when processing R\_DnssrvComplexOperation2 (section [3.1.4.8](#Section_d28e3ba85742417dad6d2e0139ab2ad9)) method calls with operation type "Statistics".

**DNS Server Credentials:** The credentials that the DNS server process will be invoked as. These credentials MUST be used for all file, registry, and directory service LDAP operations where user credentials are not available.[<104>](#Appendix_A_104)

**DownlevelDCsInDomain:** The count of downlevel domain controllers in the domain in an unsigned 32-bit integer format. The default value MUST be zero.[<105>](#Appendix_A_105)

**Domain Naming Master Identity:** Host name of the Domain Naming Master [**FSMO role**](#gt_73841222-e9d8-4dc1-83a1-206c75f4f90f) represented as a string (wchar\*). Whenever the DNS server makes any changes to crossRef objects, it MUST establish an LDAP connection to the Host whose name is stored here, and modify its version of the object accordingly.

**Local security groups:** A list of group identities with accompanying membership information. When permissions are set for an object, a local security group identity can be used to set permissions for all members of that group.

#### DNS Server Configuration Information

The list of names that are used in (name, value) pairs in DNS Server Configuration information is given below.

##### DNS Server Integer Properties

Note: Some of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview in the Product Behavior appendix.

The following properties are 32-bit integers. The term "Boolean" means that a value of 0x00000000 indicates that the stated property is false, and any nonzero value indicates that the stated property is true. All properties are writable unless stated otherwise. The type ID for these properties is DNSSRV\_TYPEID\_NAME\_AND\_PARAM, listed in section [2.2.1.1.1](#Section_c49b8142a36441c8914a7675a573b5e4). Property values on reset or load SHOULD be verified to be within the property's allowable range, except when the value is zero and the zero value is allowed. If the value is outside the range, or if the value is zero and the zero value is not allowed, the server SHOULD[<106>](#Appendix_A_106) return an error.

**AddressAnswerLimit:** The maximum number of records that the DNS server will include in a DNS response message. If this value is set to 0x00000000, the DNS server MUST NOT enforce any artificial limit on number of records in a response, and if a response becomes larger than the DNS UDP packet size, the truncation bit MUST be set (see [[RFC1035]](http://go.microsoft.com/fwlink/?LinkId=90264)). The value SHOULD be limited to the range from 0x00000005 to 0x0000001C, inclusive, or the value 0x00000000, but it MAY be any value. The default value MUST be 0x00000000, and the value of zero MUST be allowed.

**AdminConfigured:** A Boolean value indicating whether the server has been configured by an administrator. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000000, and the value of zero MUST be allowed and treated literally.[<107>](#Appendix_A_107)

**AllowCNAMEAtNS:** A Boolean value indicating whether the server will permit the target domain names of NS records to resolve to CNAME records. If true, this pattern of DNS records will be allowed; otherwise, the DNS server will return errors when encountering this pattern of DNS records while resolving queries. The value SHOULD[<108>](#Appendix_A_108) be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000001, and the value of zero MUST be allowed and treated literally.

**AllowUpdate:** A Boolean value indicating whether the server will permit any DNS update operations. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000001, and the value of zero MUST be allowed and treated literally.

**AutoCacheUpdate:** A Boolean value indicating whether the server writes updated delegation information to persistent storage when it determines that newer information is available. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000000, and the value of zero MUST be allowed and treated literally.

**AutoConfigFileZones:** The type of zones for which SOA and NS records will be automatically configured with the DNS server's local host name as the primary DNS server for the zone when the zone is loaded from file. This property MUST be set to any combination of the following values. If the property value is zero, no automatic configuration will be performed for any zone. The value's range MUST be unlimited. The default value SHOULD be 0x00000001, and the value of zero MUST be allowed and treated literally.[<109>](#Appendix_A_109)

| Value | Meaning |
| --- | --- |
| 0x00000001  ZONE\_AUTO\_CONFIG\_UPDATE | Perform automatic configuration of zones that have a value of "AllowUpdate" not equal to zero. |
| 0x00000002  ZONE\_AUTO\_CONFIG\_STATIC | Perform automatic configuration of zones that have a value of "AllowUpdate" equal to zero. |

**BindSecondaries:** A Boolean value indicating whether the server will permit send DNS zone transfer response messages with more than one record in each response if the zone transfer request did not have the characters "MS" appended to it. If true, the DNS server will include only one record in each response if the zone transfer request did not have the characters "MS" appended to it. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000000, and the value of zero MUST be allowed and treated literally.[<110>](#Appendix_A_110)

**BootMethod:** The DNS\_BOOT\_METHODS (section [2.2.4.1.1](#Section_dc737abd3e844814a62a9398c770f28f)) value corresponding to the DNS server's boot method. The value SHOULD be limited to the range from 0x00000000 to 0x00000003, inclusive, but it MAY be any value. The default value MUST be 0x00000000, and the value of zero MUST be allowed and treated literally.

**DebugLevel:** The DNS server MUST ignore any value that is set for this property.

**DefaultAgingState:** A Boolean value that will be used as the default Aging (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)) property value on new zones. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000000, and the value of zero MUST be allowed and treated literally.[<111>](#Appendix_A_111)

**DefaultNoRefreshInterval:** A value, in hours, that will be used as the default NoRefreshInterval (section 3.1.1.2.1) property value on new zones. The value SHOULD be limited to the range from 0x00000000 to 0x00002238 (1 year), inclusive, but it MAY be any value. The default value MUST be 0x000000A8 (7 days), and the value of zero MUST be allowed and treated literally.[<112>](#Appendix_A_112)

**DefaultRefreshInterval:** A value in hours that will be used as the default RefreshInterval (section 3.1.1.2.1) property value on new zones. The value SHOULD be limited to the range from 0x00000000 to 0x00002238 (1 year), inclusive, but it MAY be any value. The default value MUST be 0x000000A8 (7 days), and the value of zero MUST be allowed and treated literally.[<113>](#Appendix_A_113)

**DeleteOutsideGlue:** A Boolean value indicating whether the DNS server will delete DNS glue records found outside a delegated subzone when reading records from persistent storage. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000000, and the value of zero MUST be allowed and treated literally.

**DisjointNets:** This is a Boolean value property. The DNS server MUST ignore any value that is set for this property.

**DsLazyUpdateInterval:** A value, in seconds, indicating how frequently the DNS server will submit updates to the directory server without specifying the LDAP\_SERVER\_LAZY\_COMMIT\_OID control ([[MS-ADTS]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ADTS%5d.pdf) section 3.1.1.3.4.1.7) while processing DNS dynamic update requests. This control instructs the directory server that it may sacrifice durability guarantees on updates to improve performance and is meant to improve DNS server update performance. This control MUST only be sent by the DNS server to the directory server attached to an LDAP update initiated by the DNS server in response to a DNS dynamic update request. If the value is nonzero, LDAP updates performed while processing DNS dynamic update requests MUST NOT specify the LDAP\_SERVER\_LAZY\_COMMIT\_OID control, if a period of fewer than DsLazyUpdateInterval seconds has passed since the last LDAP update specifying this control. If a period of time greater than DsLazyUpdateInterval seconds passes in which the DNS server does not perform an LDAP update specifying this control, the DNS server MUST specify this control on the next update. The value SHOULD be limited to the range from 0x00000000 to 0x0000003c. The default value MUST be 0x00000003, and the value zero MUST be treated as indicating that the DNS server MUST NOT specify the LDAP\_SERVER\_LAZY\_COMMIT\_OID control while processing any DNS dynamic update requests.[<114>](#Appendix_A_114)

**DsPollingInterval:** The interval, in seconds, at which the DNS server will check the directory service for new or changed DNS zones and records. The value SHOULD be limited to the range from 0x0000001E to 0x00000E10, inclusive, but it MAY be any value. The default value SHOULD be 0x000000B4 (3 minutes), and the value of zero SHOULD be treated as a flag value for the default, but it MAY be allowed and treated literally. Any time a DNS server acting as the primary server for the zone successfully transfers a copy of the zone to a remote DNS server, the DNS server acting as primary MUST copy the zone serial number from the zone transfer response to the zone's Last Transferred Zone Serial Number (section [3.1.1](#Section_e72286df3e4c45359a0ce9cc944248c2)). This value MUST be stored in local non-persistent storage and MUST NOT be replicated to any other DNS server. During polling, if the serial number on a DNS record read from the directory server is higher than the current zone serial number, the current zone serial number MUST be set to the value found in the DNS record. If the DNS server is configured to allow zone transfer for the zone and the current zone serial number is equal to the Last Transferred Zone Serial Number, and if changes to any DNS records for the zone are found during polling where the serial number found in the DNS record is less than or equal to the current zone serial number, the DNS server MUST increment the zone serial number using serial number arithmetic [[RFC1982]](http://go.microsoft.com/fwlink/?LinkId=184551). If the DNS server is not configured to allow zone transfers for the zone the server MUST NOT increment the zone serial number if DNS records are found during polling where the serial number found in the DNS record is less than or equal to the current zone serial number.[<115>](#Appendix_A_115)

**DsTombstoneInterval:** The age at which tombstone objects in the directory service will be deleted. The value SHOULD be limited to the range from 0x0003F480 (3 days) to 0x0049D400 (8 weeks), inclusive, but it MAY be any value. The default value SHOULD be 0x00127500 (14 days), and the value of zero SHOULD be treated as a flag value for the default, but it MAY be allowed and treated literally. Every day at 2:00 AM local time the DNS server MUST conduct a search of all zones stored in the directory server for nodes which have the dnsTombstoned attribute set to TRUE and an [EntombedTime (section 2.2.2.2.4.23)](#Section_def7736add094b4ab8d66a702a7ecde0) value greater than **DsTombstoneInterval** seconds in the past. Any such nodes MUST be permanently deleted from the directory server [<116>](#Appendix_A_116)

**EnableRegistryBoot:** A value which, if present in local persistent configuration at boot time, indicates that the DNS server MUST rewrite the value of the **BootMethod** property (as described in DNS\_BOOT\_METHODS 2.2.4.1.1), and then delete the value of **EnableRegistryBoot** from local persistent configuration. The value of this property MUST be processed before the value of the **BootMethod** property. The DNS server MUST NOT allow this property to be set using the DNS Server Management Protocol. If the value of this property is locally set to 0x00000000, the DNS server MUST change the value of the **BootMethod** property to BOOT\_METHOD\_FILE (see section 2.2.4.1.1). If the value of this property is locally set to DNS\_FRESH\_INSTALL\_BOOT\_REGISTRY\_FLAG (0xFFFFFFFF), the DNS server MUST change the value of the **BootMethod** property to BOOT\_METHOD\_UNINITIALIZED (see section 2.2.4.1.1). If this property is locally set to any other value, the DNS server MUST change the value of the **BootMethod** property to BOOT\_METHOD\_REGISTRY (see section 2.2.4.1.1). The value's range MUST be unlimited. The default value MUST be DNS\_FRESH\_INSTALL\_BOOT\_REGISTRY\_FLAG, and the value zero MUST be allowed and treated literally.

**EventLogLevel:** All events whose type (as specified in DNS\_EVENTLOG\_TYPES (section [2.2.9.1.2](#Section_9422EB05EBF54B86AC1BE79EBF2E3B37))), is less than or equal to **Eventloglevel**, will be written to the event log. The value SHOULD be limited to the range from 0x00000000 to 0x00000007 inclusive, but it MAY be any value. The default value MUST be 0x00000004. Note that a value of **EventLogLevel** in the range from 0x00000004 to 0x00000007, inclusive, will result in all types of event being written to the event log.

**ForceSoaSerial:** User-specified value to use for the SOA **serial number** field [RFC1035] in any new SOA record, or 0x00000000 not to force a user-specified value and to instead use the value 0x00000001 as the default SOA **serial number** value. The value's range MUST be unlimited. The default value MUST be 0x00000000.

**ForceSoaExpire:** User-specified value to use for the SOA expire field [RFC1035] in any new SOA record, or 0x00000000 not to force a user-specified value and to instead use 0x00015180 as the default SOA expire field value. The value's range MUST be unlimited. The default value MUST be 0x00000000.

**ForceSoaRetry:** User-specified value to use for the SOA retry field [RFC1035] in any new SOA record, or 0x00000000 not to force a user-specified value and to instead use the value 0x00000258 as the default SOA retry field value. The value's range MUST be unlimited. The default value MUST be 0x00000000.

**ForceSoaRefresh:** User-specified value to use for the SOA refresh field [RFC1035] in any new SOA record, or 0x00000000 not to force a user-specified value and to instead use the value 0x00000384 as the default SOA refresh field value. The value's range MUST be unlimited. The default value MUST be 0x00000000.

**ForceSoaMinimumTtl:** User-specified value to use for the SOA minimum **TTL** field [RFC1035] in any new SOA record, or 0x00000000 not to force a user-specified value and to instead use the value 0x00000E10 as the default SOA minimum **TTL** field value. The value's range MUST be unlimited. The default value MUST be 0x00000000.

**ForwardDelegations:** A Boolean value indicating how the DNS server will handle forwarding and delegations. If set to true, the DNS server MUST use forwarders instead of a cached delegation when both are available. Otherwise, the DNS server MUST use a cached delegation instead of forwarders when both are available. The value SHOULD be limited to the range from 0x00000000 to 0x00000001 inclusive, but it MAY be any value. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.

**ForwardingTimeout:** The number of seconds that the DNS server will wait for a response when sending a query to a forwarder before assuming that no response will ever be received. The value SHOULD be limited to the range from 0x00000001 to 0x0000000F, inclusive, but it MAY be any value. The default value SHOULD be 0x00000003, and the value zero SHOULD be treated as a flag value for the default, but it MAY be allowed and treated literally.[<117>](#Appendix_A_117)

**IsSlave:** A Boolean value indicating whether the DNS server will use normal recursion to resolve queries if all forwarders are unavailable. If true, the DNS server MUST NOT use normal recursion if all forwarders are unavailable. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.

**LocalNetPriority:** A Boolean value indicating how the DNS server will order IP address records. If true, the DNS server MUST order answer records such that all of those containing IP addresses within the same subnet, when LocalNetPriorityNewMask is applied, as that of the IP address of the client that submitted the query, and are placed first. Also, the server SHOULD randomly order that initial set of answer records with same-subnet IP addresses. If false, the DNS server MUST not reorder answer records in the order that they were retrieved from the database. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value SHOULD be 0x00000001, and the value zero MUST be allowed and treated literally.[<118>](#Appendix_A_118)

**LogFileMaxSize:** The maximum size, in bytes, of the DNS server log file. When the file reaches this size, the DNS server MUST delete the log file and create a new log file. The value's range MUST be unlimited. The default value SHOULD be 0x1DCD6500 (500 MB), and the value zero MUST be allowed and treated literally.[<119>](#Appendix_A_119)

**LogLevel:** The type of information that the DNS server will write to the DNS server log file in DNS\_LOG\_LEVELS (section [2.2.9.1.1](#Section_fc6275bab4d34e81941703d004369075)) format. The value's range MUST be unlimited. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.[<120>](#Appendix_A_120)

**LooseWildcarding:** A Boolean value indicating the type of algorithm that the DNS server will use to locate a wildcard node when using a DNS wildcard record [[RFC1034]](http://go.microsoft.com/fwlink/?LinkId=90263) to answer a query. If true, the DNS server will use the first node it encounters with a record of the same type as the query type. Otherwise, the DNS server will use the first node it encounters that has records of any type. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.

**MaxCacheTtl:** The maximum time duration, in seconds, for which the DNS server can cache a resource record obtained from a remote server as a successful query response. The value SHOULD be limited to the range from 0x00000000 to 0x00278D00 (30 days), inclusive, but it MAY be any value. The default value MUST be 0x00015180 (1 day), and the value zero MUST be allowed and treated literally.

**MaxNegativeCacheTtl:** The maximum time duration, in seconds, for which the DNS server can cache a name error or an empty authoritative response, obtained from a remote server as an unsuccessful query response in its cache (see [[RFC2308]](http://go.microsoft.com/fwlink/?LinkId=187326)). The value SHOULD be limited to the range from 0x00000000 to 0x00278D00 (30 days), inclusive, but it MAY be any value. The default value MUST be 0x00000384 (15 minutes), and the value zero MUST be allowed and treated literally.[<121>](#Appendix_A_121)

**MaxTrustAnchorActiveRefreshInterval:** The maximum time duration, in seconds, for which the DNS server will wait between active refreshes. If an active refresh fails, the retry time MUST be no more than one-tenth of this value. See the calculation of the "queryInterval" and "retryTime" values in [[RFC5011]](http://go.microsoft.com/fwlink/?LinkId=225980). The value MUST be limited to the range 0x00000E10 (1 hour) to 0x0013C680 (15 days), inclusive. The default value MUST be 0x0013C680 (15 days).[<122>](#Appendix_A_122)

**NameCheckFlag:** The DNS\_NAME\_CHECK\_FLAGS (section [2.2.4.1.2](#Section_914badedbfe04e249150197b7ea2ba5d)) value corresponding to the level of name checking performed by the DNS server. The value SHOULD be limited to the range from 0x00000000 to 0x00000003, inclusive, but it MAY be any value. The default value SHOULD be 0x00000002 (DNS\_ALLOW\_MULTIBYTE\_NAMES), and the value zero MUST be allowed and treated literally.[<123>](#Appendix_A_123)

**NoRecursion:** A Boolean value indicating whether the DNS server will perform any recursion. If true, the DNS server MUST NOT recurse and will only answer queries for authoritative data.

**NoUpdateDelegations:** A Boolean value indicating whether the DNS server will accept DNS updates to delegation records of type NS. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value SHOULD be 0x00000000, and the value zero MUST be allowed and treated literally.[<124>](#Appendix_A_124)

**PublishAutonet:** A Boolean value indicating whether the DNS server will publish local IPv4 addresses in the 169.254.x.x subnet as IPv4 addresses for the local machine's domain name. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.[<125>](#Appendix_A_125)

**QuietRecvFaultInterval:** A property used to debug reception of UDP traffic for a recursive query. This property is the minimum time interval, in seconds, starting when the server begins waiting for the query to arrive on the network, after which the server MAY log a debug message indicating that the server is to stop running. If the value is zero or is less than the value of QuietRecvLogInterval, then the value of QuietRecvLogInterval MUST be used. If the value is greater than or equal to the value of QuietRecvLogInterval, then the literal value of QuietRecvFaultInterval MUST be used. The value's range MUST be unlimited. The default value MUST be 0x00000000. The server MAY ignore this property.[<126>](#Appendix_A_126)

**QuietRecvLogInterval:** A property used to debug reception of UDP traffic for a recursive query. This property is the minimum time interval, in seconds, starting when the server begins waiting for the query to arrive on the network, or when the server logs an eponymous debug message for the query, after which the server MUST log a debug message indicating that the server is still waiting to receive network traffic. If the value is zero, logging associated with the two QuietRecv properties MUST be disabled, and the QuietRecvFaultInterval property MUST be ignored. If the value is non-zero, logging associated with the two QuietRecv properties MUST be enabled, and the QuietRecvFaultInterval property MUST NOT be ignored. The value's range MUST be unlimited. The default value MUST be 0x00000000. The server MAY ignore this property.[<127>](#Appendix_A_127)

**RecursionRetry:** The time interval, in seconds, for which the DNS server waits before it retries a recursive query to a remote DNS server for which it did not receive a response. The value SHOULD be limited to the range from 0x00000001 to 0x0000000F, inclusive, but it MAY be any value. The default value MUST be 0x00000003, and the value zero SHOULD be treated as a flag value for the default, but it MAY be allowed and treated literally.

**RecursionTimeout:** The time interval, in seconds, for which the DNS server waits for a recursive query response from a remote DNS server. The value SHOULD be limited to the range from 0x00000001 to 0x0000000F, inclusive, but it MAY be any value. The default value SHOULD be 0x00000008, and the value zero SHOULD be treated as a flag value for the default, but it MAY be allowed and treated literally.[<128>](#Appendix_A_128)

**ReloadException:** A Boolean value indicating whether the DNS server will perform an internal restart if an unexpected fatal error is encountered. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value SHOULD be 0x00000000, and the value zero MUST be allowed and treated literally.[<129>](#Appendix_A_129)

**RoundRobin:** A Boolean value indicating whether the DNS server will dynamically reorder records in responses to attempt to provide load balancing. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000001, and the value zero MUST be allowed and treated literally.

**RpcProtocol:** The DNS\_RPC\_PROTOCOLS (section [2.2.1.1.2](#Section_cbae04989a604455977845476f7331f5)) value corresponding to the RPC protocols to which the DNS server will respond. If this value is set to 0x00000000, the DNS server MUST NOT respond to RPC requests for any protocol. The value's range MUST be unlimited, for example, from 0x00000000 to 0xFFFFFFFF. The default value SHOULD be 0x00000005.[<130>](#Appendix_A_130)

**SecureResponses:** A Boolean value indicating whether the DNS server is configured to cache only those records that are in the same subtree as the name in the original query. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value SHOULD be 0x00000001, and the value zero MUST be allowed and treated literally.[<131>](#Appendix_A_131)

**SendPort:** The port number to use as the source port when sending UDP queries to a remote DNS server. If set to zero, the DNS server MUST allow the stack to select a random port. The value's range MUST be unlimited. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.

**ScavengingInterval:** The time interval, in hours, between which the DNS server will schedule DNS stale record scavenging. The value SHOULD be limited to the range from 0x00000000 to 0x00002238, inclusive. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated as a flag to disable scavenging. If the value is non-zero and a "StartScavenging" operation is initiated, the value is ignored and scavenging begins immediately.[<132>](#Appendix_A_132)

**SocketPoolSize:** The number of [**UDP**](#gt_a70f5e84-6960-42f0-a160-ba0281eb548d) sockets per address family that the DNS server will use for sending remote queries. The value MUST be limited to the range from 0x00000000 to 0x00002710, inclusive. The default value MUST be 0x000009C4, and the value zero MUST be allowed and treated literally.[<133>](#Appendix_A_133)

**StrictFileParsing:** A Boolean value indicating whether the DNS server will treat errors encountered while reading zones from a file as fatal. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value SHOULD be 0x00000000, and the value zero MUST be allowed and treated literally.

**SyncDsZoneSerial:** The conditions under which the DNS server immediately commits uncommitted zone serial numbers to persistent storage. The value SHOULD be limited to the range from 0x00000000 to 0x00000004, inclusive, but it MAY be any value. The default value SHOULD be 0x00000002, and the value zero MUST be allowed and treated literally.[<134>](#Appendix_A_134)

| Value | Meaning |
| --- | --- |
| 0x00000000  ZONE\_SERIAL\_SYNC\_OFF | Never force immediate commit of serial number to persistent storage. |
| 0x00000001  ZONE\_SERIAL\_SYNC\_SHUTDOWN | Force immediate commit of uncommitted serial numbers to persistent storage when the DNS server is shut down. |
| 0x00000002  ZONE\_SERIAL\_SYNC\_XFER | Force immediate commit of uncommitted serial numbers to persistent storage when the DNS server is shut down or when an uncommitted serial number is advertised during zone transfer. |
| 0x00000003  ZONE\_SERIAL\_SYNC\_VIEW | Force immediate commit of uncommitted serial numbers to persistent storage when the DNS server is shut down or when an uncommitted serial number is advertised during zone transfer or when a zone has been loaded or when a zone has been read from Active Directory.[<135>](#Appendix_A_135) |
| 0x00000004  ZONE\_SERIAL\_SYNC\_READ | Force immediate commit of uncommitted serial numbers to persistent storage when the DNS server is shut down or when an uncommitted serial number is advertised during zone transfer or when a zone has been loaded or when a zone has been read from Active Directory. |

**UpdateOptions:** The possible zone update settings on the DNS server. Each bit that follows can be used to enable a specific update processing rule to modify the default DNS server update processing behavior. The value's range MUST be unlimited. The default value MUST be 0x0000030F (DNS\_DEFAULT\_UPDATE\_OPTIONS), and the value zero MUST be allowed and treated literally.[<136>](#Appendix_A_136)

The following values are used to disable dynamic updates for non-secure zones.

| Value | Meaning |
| --- | --- |
| 0x00000001  UPDATE\_NO\_SOA | Disable for SOA records. |
| 0x00000002  UPDATE\_NO\_ROOT\_NS | Disable for root name servers. |
| 0x00000004  UPDATE\_NO\_DELEGATION\_NS | Disable for name servers of delegated zones. |
| 0x00000008  UPDATE\_NO\_SERVER\_HOST | Disable for address records in the DNS server's own host record. |

The following values are used to disable dynamic updates for secure zones.

| Value | Meaning |
| --- | --- |
| 0x00000100  UPDATE\_SECURE\_NO\_SOA | Disable for SOA records. |
| 0x00000200  UPDATE\_SECURE\_NO\_ROOT\_NS | Disable for root name-servers. |
| 0x00000400  UPDATE\_SECURE\_NO\_DELEGATION\_NS | Disable for name-servers of delegated zones. |
| 0x00000800  UPDATE\_SECURE\_NO\_SERVER\_HOST | Disable for address records in the DNS server's own host-record. |
| 0x01000000  UPDATE\_NO\_DS\_PEERS | Disable for directory server peers for the DNS server. |

Other possible values (regardless of zone type) are as follows.

| Value | Meaning |
| --- | --- |
| 0x00000000  UPDATE\_ANY | Server allows dynamic updates for all record types. |
| 0x0000030F  DNS\_DEFAULT\_UPDATE\_OPTIONS | Disable all dynamic updates, except for SOA and NS updates for secure zones. |
| 0x01000000  UPDATE\_NO\_DS\_PEERS | Disable relay of server's address record update to remote DNS servers for non-secure zones. |

**UseSystemEventLog:** A Boolean value indicating whether the DNS server will write event logs to a repository that is global for the entire system or to a repository that is specific to the DNS server. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.

**Version:** A read-only 32-bit integer containing the DNS server version in DNSSRV\_VERSION (section [2.2.4.2.1](#Section_abf93ed679384564b21486762a1c4dea)) format. This property is read-only.

**XfrConnectTimeout:** The value, in seconds, that the DNS server will wait, for any DNS TCP connection to a remote DNS server to be established, before assuming that the remote DNS server will not respond. The value SHOULD be limited to the range from 0x00000005 to 0x00000078, inclusive, but it MAY be any value. The default value MUST be 0x0000001E, and the value zero MUST be treated as a flag value for the default.[<137>](#Appendix_A_137)

**WriteAuthorityNs:** A Boolean value indicating whether the DNS server will include NS records for the root of a zone in DNS responses that are answered using authoritative zone data. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be unlimited. The default value MUST be 0x00000000, and the value zero MUST be allowed.[<138>](#Appendix_A_138)

**AdditionalRecursionTimeout:** The time interval, in seconds, for which the DNS server waits while recursing to obtain resource records for use in the additional section of DNS responses from a remote DNS server. The value SHOULD be limited to the range from 0x00000000 to 0x0000000F, inclusive, but it MAY be any value. The default value SHOULD be 0x00000004, and the value zero SHOULD be treated as a flag value for the default, but it MAY be allowed and treated literally.[<139>](#Appendix_A_139)

**AppendMsZoneTransferTag:** A Boolean value indicating whether the DNS server will indicate to the remote DNS servers that it supports multiple DNS records in each zone transfer response message by appending the characters "MS" at the end of zone transfer requests. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value SHOULD be 0x00000000, and the value zero MUST be allowed and treated literally.[<140>](#Appendix_A_140)

**AutoCreateDelegations:** The possible settings for automatic delegation creation for new zones on the DNS server. The value SHOULD be limited to the range from 0x00000000 to 0x00000002, inclusive, but it MAY be any value. The default value SHOULD be 0x00000002 (DNS\_ACD\_ONLY\_IF\_NO\_DELEGATION\_IN\_PARENT), and the value zero MUST be allowed and treated literally.[<141>](#Appendix_A_141)

| Value | Meaning |
| --- | --- |
| 0x00000000  DNS\_ACD\_DONT\_CREATE | The server does not create delegations automatically. |
| 0x00000001  DNS\_ACD\_ALWAYS\_CREATE | The server always creates delegations automatically. |
| 0x00000002  DNS\_ACD\_ONLY\_IF\_NO\_  DELEGATION\_IN\_PARENT | The server creates a new delegation in the parent zone only if there is no existing delegation present for the zone. |

**BreakOnAscFailure:** A Boolean value indicating whether the DNS server will execute a debug break if an error is encountered during security negotiation for secure updates. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.[<142>](#Appendix_A_142)

**CacheEmptyAuthResponses:** A Boolean value indicating if the DNS server will store empty authoritative responses [RFC2308] in the cache. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000001, and the value zero MUST be allowed and treated literally.[<143>](#Appendix_A_143)

**DirectoryPartitionAutoEnlistInterval:** The interval, in seconds, at which the DNS server will attempt to enlist itself in the DNS domain partition and DNS forest partition if it is not already enlisted. The value SHOULD be limited to the range from 0x00000E10 (1 hour) to 0x00ED4E00 (180 days), inclusive, but it MAY be any value. The default value MUST be 0x00015180 (1 day), and the value zero SHOULD be treated as a flag value for the default, but it MAY be allowed and treated literally.[<144>](#Appendix_A_144)

**DisableAutoReverseZones:** A Boolean value indicating whether the DNS server will disable the automatic server boot-time creation of three authoritative reverse lookup zones (0.in-addr.arpa, 127.in-addr.arpa, and 255.in-addr.arpa). The value SHOULD be limited to the range from 0x00000000 to 0x00000001, inclusive, but it MAY be any value. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.

**EDnsCacheTimeout:** The interval, in seconds, for which the DNS server will cache the remote DNS server support of EDNS [[RFC2671]](http://go.microsoft.com/fwlink/?LinkId=107022). The value SHOULD be limited to the range from 0x0000000A to 0x00015180 (1 day), inclusive, but it MAY be any value. The default value SHOULD be 0x00000384 (15 minutes), and the value zero SHOULD be treated as a flag value for the default, but it MAY be allowed and treated literally.[<145>](#Appendix_A_145)

**EnableDirectoryPartitions:** A Boolean value indicating whether the DNS server will support application directory partitions. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000001, and the value zero MUST be allowed and treated literally.[<146>](#Appendix_A_146)

**EnableDnsSec:** A Boolean value indicating whether the DNS server will perform additional query processing for secure DNS records, as specified in [[RFC4033]](http://go.microsoft.com/fwlink/?LinkId=107051), [[RFC4034]](http://go.microsoft.com/fwlink/?LinkId=107052), and [[RFC4035]](http://go.microsoft.com/fwlink/?LinkID=107053). The value SHOULD be limited to a range of 0x00000000 to 0x00000001, inclusive, but it MAY be any value. The default value MUST be 0x00000001 and the value zero MUST be allowed and treated literally.[<147>](#Appendix_A_147)

**EnableEDnsProbes:** A Boolean value indicating whether the DNS server will include EDNS [RFC2671] records in remote queries (with the possible exception of queries sent to a remote Global Names Zone (GNZ); see "GlobalNamesEnableEDnsProbes" later in this section). The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value SHOULD be 0x00000001, and the value zero MUST be allowed and treated literally.[<148>](#Appendix_A_148)

**EnableEDnsReception:** A Boolean value indicating whether the DNS server will accept queries that contain an EDNS [RFC2671] record. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000001, and the value zero MUST be allowed and treated literally.[<149>](#Appendix_A_149)

**EnableIPv6:** A Boolean value indicating whether the DNS server will listen on local IPv6 addresses. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value SHOULD be 0x00000001, and the value zero MUST be allowed and treated literally.[<150>](#Appendix_A_150)

**EnableForwarderReordering:** A Boolean value indicating whether the DNS server will perform forwarder list reordering of the DynamicForwarder list (section [3.1.1.1.2](#Section_f73f36ca3f0640caa392f7837d62642f)) at run time. The value MUST be limited to 0x00000000 and 0x00000001. The default value MUST be 0x00000001, and the value zero MUST be allowed and treated literally.[<151>](#Appendix_A_151)

**EnableIQueryResponseGeneration:** A Boolean value indicating whether the DNS server will fabricate IQUERY responses. If set to true, the DNS server MUST fabricate IQUERY responses when it receives queries of type IQUERY. Otherwise, the DNS server will return an error when such queries are received. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.[<152>](#Appendix_A_152)

**EnableOnlineSigning:** A Boolean value indicating whether the DNS server will sign directory server-integrated zones when these zones are loaded or when records in a zone are added, removed, or modified. The value also indicates whether signing new zones will be permitted. The value MUST be limited to 0x00000000 and 0x00000001. The default value MUST be 0x00000001, and the value zero MUST be allowed and treated literally.[<153>](#Appendix_A_153)

**EnableSendErrorSuppression:** A Boolean value indicating whether the DNS server will attempt to suppress large volumes of DNS error responses sent to remote IP addresses that may be attempting to attack the DNS server. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000001, and the value zero MUST be allowed and treated literally.[<154>](#Appendix_A_154)

**EnableUpdateForwarding:** A Boolean value indicating whether the DNS server will forward updates received for secondary zones to the primary DNS server for the zone. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.[<155>](#Appendix_A_155)

**EnablePolicies:** A Boolean value indicating whether the DNS server uses DNS Policy during a DNS Operation. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000001, and the value zero MUST be allowed and treated literally.

**EnableWinsR:** A Boolean value indicating whether the DNS server will perform NetBIOS name resolution in order to map IP addresses to machine names while processing queries in zones where WINS-R information has been configured. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000001, and the value zero MUST be allowed and treated literally.[<156>](#Appendix_A_156)

**ForceDsaBehaviorVersion:** The minimum value to use as the behavior version of the local directory server, or 0xFFFFFFFF. Values for this property MUST be limited to those specified in "msDS-Behavior-Version: DC Functional Level", [MS-ADTS] (section 6.1.4.4), in addition to 0xFFFFFFFF, which MUST be the default value. The DNS Server reads the **msDS-BehaviorVersion** attribute of the local directory server's "nTDSDSA" object and compares it with this property. If the value read from the directory server is greater than the specified ForceDsaBehaviorVersion, or if ForceDsaBehaviorVersion is 0xFFFFFFFF, this property is set to the value read from the directory server. This property SHOULD be returned by the DNS Server in the **dwDsDsaVersion** field of the DNS\_RPC\_SERVER\_INFO structure (section [2.2.4.2.2](#Section_ac444baf4bf94f36912e3041d4c46361)) when processing the "ServerInfo" operation of the R\_DnssrvQuery method (section [3.1.4.2](#Section_b0419a70ac0b40baab941510992bc574)).

**ForceDomainBehaviorVersion:** The minimum value to use as the behavior version of the domain, or 0xFFFFFFFF. Values for this property MUST be limited to those specified in "msDS-Behavior-Version: Domain NC Functional Level", [MS-ADTS] (section 6.1.4.4), in addition to 0xFFFFFFFF, which MUST be the default value. The DNS Server reads the **msDS-BehaviorVersion** attribute of the domain's crossRef object and compares it with this property. If the value read from the directory server is greater than the specified ForceDomainBehaviorVersion, or if ForceDomainBehaviorVersion is 0xFFFFFFFF, this property is set to the value read from the directory server. This property SHOULD be returned by the DNS Server in the **dwDsDomainVersion** field of the DNS\_RPC\_SERVER\_INFO structure (section 2.2.4.2.2) when processing the "ServerInfo" operation of the R\_DnssrvQuery method (section 3.1.4.2)

**ForceForestBehaviorVersion:** The minimum value to use as the behavior version of the forest (1), or 0xFFFFFFFF. Values for this property MUST be limited to those specified in "msDS-Behavior-Version: Forest Functional Level", [MS-ADTS] section 6.1.4.4, in addition to 0xFFFFFFFF, which MUST be the default value. The DNS Server reads the **msDS-BehaviorVersion** attribute of the forest's "crossRefContainer" object and compares it with this property. If the value read from the directory server is greater than the specified ForceForestBehaviorVersion, or if ForceForestBehaviorVersion is 0xFFFFFFFF, this property is set to the value read from the directory server. This property SHOULD be returned by the DNS Server in the **dwDsForestVersion** field of the DNS\_RPC\_SERVER\_INFO structure (section 2.2.4.2.2) when processing the 2.2.4.2.2 operation of the R\_DnssrvQuery method (section 2.2.4.2.2

**HeapDebug:** A Boolean value indicating whether the DNS server will execute a debug break when internal memory corruption is detected. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.[<157>](#Appendix_A_157)

**LameDelegationTtl:** The number of seconds that MUST elapse before the DNS server requeries DNS servers of the parent zone when a [**lame delegation**](#gt_18f6daaf-1345-455e-8a27-c478c048643b) is encountered. The value SHOULD[<158>](#Appendix_A_158) be limited to the range from 0x00000000 to 0x00278D00 (30 days), inclusive, but it MAY be any value. The default value SHOULD be 0x00000000, and the value zero MUST be allowed and treated literally.

**LocalNetPriorityNetMask:** A value that specifies the network mask the DNS server uses to sort IPv4 addresses. A value of 0xFFFFFFFF indicates that the DNS server MUST use traditional IPv4 network mask for the address. Any other value is a network mask, in host byte order that the DNS server MUST use to retrieve network masks from IP addresses for sorting purposes. The value's range MUST be unlimited. The default value MUST be 0x000000FF, and the value zero MUST be allowed and treated literally.[<159>](#Appendix_A_159)

**MaxCacheSize:** The maximum size of memory, in kilobytes, that the DNS server can use to store DNS data in the cache. The value SHOULD[<160>](#Appendix_A_160) be limited to the range from 0x000001F4 to 0xFFFFFFFF, inclusive, or 0x00000000, but it MAY be any value. The default value SHOULD be 0x00000000, which MUST be allowed and treated as a flag value for no limit on maximum size of memory. If the value is nonzero, the DNS server SHOULD treat this as a soft limit, allowing it to be exceeded for limited durations, and also attempt to limit cache memory to 90 percent of this value.

**MaximumSignatureScanPeriod:** The maximum time, in seconds, before which the server MUST scan all signed zones for a signature refresh. The value MUST be limited to the range 0x00000E10 (1 hour) to 0x00278D00 (30 days), inclusive. The default value MUST be 0x00015180 (1 day), and the value zero MUST be allowed and treated literally.[<161>](#Appendix_A_161)

**MaxResourceRecordsInNonSecureUpdate:** The maximum number of resource records that the DNS server accepts in a single DNS update request. The value SHOULD be limited to the range from 0x0000000A to 0x00000078, inclusive, but it MAY be any value. The default value SHOULD be 0x0000001E, and the value zero SHOULD be treated as a flag value for the default, but it MAY be allowed and treated literally.[<162>](#Appendix_A_162)

**OperationsLogLevel:** The operations (in addition to those specified by OperationsLogLevel2) that are logged to the DNS server log file using any combination of the values that follow. The value's range MUST be unlimited. The default value SHOULD be 0x00000000, and the value zero MUST be allowed and treated literally.[<163>](#Appendix_A_163)

| Value | Meaning |
| --- | --- |
| 0x00000001  DNSLOG\_WRITE\_THROUGH | The server saves operational logging information to persistent storage. |
| 0x00000010  DNSLOG\_EVENT | The server logs event logging information to the log file. |
| 0x00000020  DNSLOG\_INIT | The server logs operational logging information to the log file for server start and stop activities. |
| 0x00002000  DNSLOG\_DSPOLL | The server logs operational logging information to the log file for activities related to loading a zone from the directory server. |
| 0x00004000  DNSLOG\_DSWRITE | The server logs operational logging information to the log file for activities related to writing zone data to the directory server. |
| 0x00020000  DNSLOG\_TOMBSTN | The server logs operational logging information to the log file for activities related to updating tombstoned nodes. |
| 0x00100000  DNSLOG\_LOOKUP | The server logs operational logging information to the log file for local resource lookup activities. |
| 0x00200000  DNSLOG\_RECURSE | The server logs operational logging information to the log file for activities performed during recursive query lookup. |
| 0x00400000  DNSLOG\_REMOTE | The server logs operational logging information to the log file for activities related to interaction with remote name servers. |

**OperationsLogLevel2:** The operations (in addition to those specified by OperationsLogLevel) that are logged to the DNS server log file using any combination of the values that follow. The value's range MUST be unlimited. The default value SHOULD be 0x00000000, and the value zero MUST be allowed and treated literally.[<164>](#Appendix_A_164)

| Value | Meaning |
| --- | --- |
| 0x01000000  DNSLOG\_PLUGIN | The server logs operational logging information to the log file for activities related to interaction with plug-in DLLs. |

**MaximumUdpPacketSize:** The maximum UDP packet size, in bytes, that the DNS server can accept. The value MUST be limited to 0x00000200 to 0x00004000.[<165>](#Appendix_A_165) The server MUST return an error if an attempt is made to change the value of this property through this protocol. This property may only be changed by modifying the value in persistent storage.[<166>](#Appendix_A_166)

**RecurseToInternetRootMask:** The DNS server MUST ignore any value set for this property.

**SelfTest:** A mask value indicating whether data consistency checking is performed once, each time the service starts. If the check fails, the server posts an event log warning. If the least significant bit (regardless of other bits) of this value is one, the DNS server verifies for each active and update-allowing primary zone, that the IP address records are present in the zone for the zone's SOA record's master server. If the least significant bit (regardless of other bits) of this value is zero, no data consistency checking will be performed. The value's range MUST be from 0x00000000 to 0xFFFFFFFF, inclusive. The default value MUST be 0xFFFFFFFF.

**SilentlyIgnoreCNameUpdateConflicts:** A Boolean value indicating whether the DNS server will ignore CNAME conflicts during DNS update processing. The value SHOULD be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.[<167>](#Appendix_A_167)

**ScopeOptionValue:** An integer value that determines a name in a name value pair that the DNS server looks for in the OPT record of an incoming query. This is also the name of a name value pair that a resolver DNS server writes to the OPT RR of a DNS query for which it recurses. The value SHOULD be limited to the range from 0x00000008 to 0x0000FFFF excluding the range values, but it MAY be any value. If it is any value other than the range, the DNS server sets it to 0x0000FF98. If the value is not set or set to 0, the DNS server disables this behavior.

**TcpReceivePacketSize:** The maximum TCP packet size, in bytes, that the DNS server can accept. The value MUST be limited to the range from 0x00004000 to 0x00010000, inclusive. Values outside of this range MUST cause the server to return an error. The default value MUST be 0x00010000.[<168>](#Appendix_A_168)

**XfrThrottleMultiplier:** The multiple used to determine how long the DNS server refuses zone transfer requests after a successful zone transfer has been completed. The total time for which a zone will refuse another zone transfer request at the end of a successful zone transfer is computed as this value multiplied by the number of seconds required for the zone transfer that just completed. The server SHOULD refuse zone transfer requests for no more than ten minutes. The value SHOULD be limited to the range from 0x00000000 to 0x00000064, inclusive, but it MAY be any value. The default value MUST be 0x0000000A, and the value zero MUST be allowed and treated literally.[<169>](#Appendix_A_169)

**UdpRecvThreadCount:** The number of receive threads handling incoming UDP traffic that the server MUST run simultaneously. The value MUST be limited to the range 0x00000000 to 0x00000800, inclusive. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated as the count of processors in the machine.[<170>](#Appendix_A_170)

The DNS server SHOULD also support the following properties.[<171>](#Appendix_A_171)

**AllowMsdcsLookupRetry:** A Boolean value indicating whether the DNS server will attempt to retry failed lookup operations in the immediate parent of the zone where the lookup was originally performed. This lookup retry MUST only be applied if the name of the zone where the lookup was originally performed began with the string "\_msdcs" and the immediate parent of the zone where the lookup was originally performed is present on the DNS server. The value's range MUST be limited to 0x00000000 and 0x00000001. The default value SHOULD be 0x00000001, and the value zero MUST be allowed and treated literally.[<172>](#Appendix_A_172)

**AllowReadOnlyZoneTransfer:** A Boolean value indicating whether the DNS server will allow zone transfers for zones that are stored in the directory server when the directory server does not support write operations. The value MUST be limited to 0x00000000 and 0x00000001. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.

**DsBackgroundLoadPaused:** A Boolean value indicating whether the DNS server is enabled to pause background loading of information from directory server if a node is found with same node-name same as pointed to by DsBackgroundPauseName. The value MUST be limited to 0x00000000 and 0x00000001. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.[<173>](#Appendix_A_173)

**DsMinimumBackgroundLoadThreads:** The minimum number of background threads that the DNS server will use to load zone data from the directory service. The value MUST be limited to the range from 0x00000000 to 0x00000005, inclusive. If the value is 0x00000000, then the DNS server MUST NOT start background threads to load zone data from the directory service. The default value MUST be 0x00000001, and the value zero MUST be treated as allowed.

**DsRemoteReplicationDelay:** The minimum interval, in seconds, that the DNS server waits between the time it determines that a single object has changed on a remote directory server and the time it attempts to replicate the single object change. The value MUST be limited to the range from 0x00000005 to 0x00000E10, inclusive. The default value MUST be 0x0000001E, and the value zero MUST be treated as a flag value for the default.

**EnableDuplicateQuerySuppression:** A Boolean value indicating whether the DNS server will not send remote queries when there is already a remote query with the same name and query type outstanding. The value MUST be limited to 0x00000000 and 0x00000001. The default value MUST be 0x00000001, and the value zero MUST be allowed and treated literally.

**EnableGlobalNamesSupport:** A Boolean value indicating whether the DNS server will use any GNZ data while responding to DNS queries and updates. The value MUST be limited to 0x00000000 and 0x00000001. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.

**EnableVersionQuery:** This property controls what version information the DNS server will respond with when a DNS query with class set to CHAOS and type set to TXT is received. The value's range MUST be limited to the values in the following table. The default value SHOULD be 0x00000000.[<174>](#Appendix_A_174)

| Value | Meaning |
| --- | --- |
| 0x00000000  DNS\_VERSION\_QUERY\_OFF | No version information will be returned. |
| 0x00000001  DNS\_VERSION\_QUERY\_FULL | The server responds with major operating system version, minor operating system version, and operating system revision. |
| 0x00000002  DNS\_VERSION\_QUERY\_MINIMAL | The server responds with major operating system version and minor operating system version. |

**EnableRsoForRodc:** A Boolean value indicating whether the DNS server will attempt to replicate single updated DNS objects from remote directory servers ahead of normally scheduled replication when operating on a directory server that does not support write operations. The value MUST be limited to 0x00000000 and 0x00000001, but it MAY be any value. The default value SHOULD be 0x00000001, and the value zero MUST be allowed and treated literally.

**ForceRODCMode:** A Boolean value indicating whether the DNS server will always operate as if the directory server does not support write operations. If TRUE, the DNS server MUST operate as if the directory server does not support write operations; otherwise, the DNS server MUST query the directory server to determine whether it supports write operations. The value MUST be limited to 0x00000000 and 0x00000001. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.[<175>](#Appendix_A_175)

**GlobalNamesAlwaysQuerySrv:** A Boolean value that indicates, when FALSE, that the DNS server will attempt to use GNZ service records (SRV records named "\_globalnames.\_msdcs.<forestroot>") from the server's cache when updating the list of remote DNS servers hosting a GNZ, or when TRUE, that the server MUST always attempt a remote DNS query for such records. The value MUST be ignored if the server hosts a GNZ. The value MUST be limited to 0x00000000 and 0x00000001. The default value MUST be 0x00000000, and the value zero MUST be allowed.

**GlobalNamesBlockUpdates:** A Boolean value indicating whether the DNS server will block updates in authoritative zones if they are for FQDNs that would collide with labels found in the GNZ. If the value of this property is 0x00000000, then a check for this collision MUST NOT be performed.

To test whether a name collides with a name present in the GNZ, the DNS server MUST extract the relative portion of the name that is being updated by removing the rightmost labels which comprise the zone name, and then perform a case-insensitive search in the locally hosted GNZ for a name matching the remaining labels. If a match for these labels is found in the locally hosted GNZ and the value of this property is 0x00000001 then the update MUST be blocked.

The value MUST be limited to 0x00000000 and 0x00000001. The default value MUST be 0x00000001, and the value zero MUST be allowed.

**GlobalNamesEnableEDnsProbes:** A Boolean value indicating whether the DNS server will honor the "EnableEDnsProbes" Boolean value for a remote GNZ. A value of TRUE indicates that the server MUST attempt to use EDNS for queries sent to a remote GNZ if the Boolean value of "EnableEDnsProbes" is also TRUE, and otherwise MUST NOT attempt to use EDNS for such queries. A value of FALSE indicates that the server MUST NOT attempt to use EDNS for queries sent to a remote GNZ, regardless of the value of "EnableEDnsProbes". The value MUST be limited to 0x00000000 and 0x00000001. The default value MUST be 0x00000001, and the value zero MUST be allowed.

**GlobalNamesPreferAAAA:** A Boolean value indicating whether the DNS server will prefer type AAAA address records to type A records when sending queries to a remote DNS server that is hosting a GNZ. If the value is 0x00000000 then queries to a remote DNS server hosting a GNZ MUST be sent using IPv4 if any IPv4 addresses for the remote DNS server name can be found. If no IPv4 addresses are found for the remote DNS server name, then IPv6 addresses MUST be used. If the value of this property is 0x00000001, then IPv6 addresses for the remote DNS server MUST be used, and IPv4 addresses MUST NOT be used unless no IPv6 addresses can be found. The value MUST be limited to 0x00000000 and 0x00000001. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.

**GlobalNamesQueryOrder:** A Boolean value indicating whether the DNS server will prefer GNZ or authoritative zone data when determining what data to use to answer queries. If TRUE, the DNS server MUST prefer authoritative zone data; otherwise, the DNS server MUST prefer GNZ data. The value MUST be limited to 0x00000000 and 0x00000001. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.

**GlobalNamesSendTimeout:** The number of seconds the DNS server will wait when sending a query to a remote GNZ before assuming that no answer will ever be received. The value MUST be limited to the range from 0x00000001 to 0x0000000F, inclusive. The default value MUST be 0x00000003, and the value zero MUST be treated as a flag value for the default.

**GlobalNamesServerQueryInterval:** The maximum interval, in seconds, between queries to refresh the set of remote DNS servers hosting the GNZ. The value MUST be limited to the range from 0x0000003C (60 seconds) to 0x00278D00 (30 days), inclusive. The default value MUST be 0x00005460 (6 hours), and the value zero MUST be treated as a flag value for the default.

**RemoteIPv4RankBoost:** A value to add to all IPv4 addresses for remote DNS servers when selecting between IPv4 and IPv6 remote DNS server addresses. The value MUST be limited to the range from 0x00000000 to 0x0000000A, inclusive. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.

**RemoteIPv6RankBoost:** A value to add to all IPv6 addresses for remote DNS servers when selecting between IPv4 and IPv6 remote DNS server addresses. The value MUST be limited to the range from 0x00000000 to 0x0000000A, inclusive. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated literally.

**MaximumRodcRsoAttemptsPerCycle:** The maximum number of queued single object replication operations that are attempted during each five minute interval of DNS server operation. The value MUST be limited to the range from 0x00000000 to 0x000F4240, inclusive. The default value MUST be 0x00000064, and the value 0x00000000 MUST be allowed and treated as no limitation on the number of queued single object replication operations.

**MaximumRodcRsoQueueLength:** The maximum number of single object replication operations that may be queued at any given time by the DNS server. The value MUST be limited to the range from 0x00000000 to 0x000F4240, inclusive. If the value is 0x00000000 the DNS server MUST NOT enforce an upper bound on the number of single object replication operations queued at any given time. The default value MUST be 0x0000012C, and the value zero MUST be allowed.

**EnableGlobalQueryBlockList:** A Boolean value indicating whether the DNS server blocks queries in locally hosted primary zones that match entries in the **GlobalQueryBlockList** property (see section [3.1.1.1.4](#Section_35e541ef7a594a44ba187cd00aba6a0d)). If the value of this property is 0x00000001, when answering a query using a locally hosted primary zone the DNS server MUST check to see if the relative portion of the query name matches any value in the GlobalQueryBlockList property. If a match is found the DNS server MUST return a name error response instead of a positive answer. The DNS server MUST NOT apply this algorithm to the name of the zone. The block list MUST only be applied to records within each zone. The DNS server MUST NOT perform this check if the value of the EnableGlobalQueryBlockList property is 0x00000000. The value MUST be limited to 0x00000000 and 0x00000001. The default value MUST be 0x00000001, and the value zero MUST be allowed and treated literally.[<176>](#Appendix_A_176)

The DNS server SHOULD[<177>](#Appendix_A_177) also support the following properties.

**OpenACLOnProxyUpdates:** A Boolean value indicating whether the DNS server allows sharing of DNS records with the DnsUpdateProxy group when processing updates in secure zones that are stored in the directory service. During secure dynamic update [[RFC3645]](http://go.microsoft.com/fwlink/?LinkId=90440) negotiation, the DNS server SHOULD check whether DNS records exist in the zone under the name specified in the update request, [[RFC2136]](http://go.microsoft.com/fwlink/?LinkId=107017). If so, the server SHOULD check the client credentials against the access control lists associated with the existing records in the directory service (DS) (see [MS-ADTS] section 5.1.3), before allowing the requested records to be created or modified. If there are no records for the update request name, DNS server SHOULD create records requested by the client, and associate those records with the client's credentials. If OpenACLOnProxyUpdates is set to TRUE, when a member of the DnsUpdateProxy group updates a DNS resource record for which that member has write access, the record access control lists SHOULD be adjusted to grant write privileges to all clients with credentials. The value of OpenACLOnProxyUpdates MUST be limited to 0x00000000 and 0x00000001. The default value MUST be 0x00000001, and the value zero MUST be allowed and treated literally.

**CacheLockingPercent:** The percentage of the original time-to-live value for which all cache entries from non-authoritative responses MUST be locked and MUST NOT be overwritten by data found in subsequent non-authoritative responses. Locked cache entries MUST still be considered for removal from the cache if the soft limit of the maximum cache size is reached (see the MaxCacheSize property, described previously in this section). The value MUST be limited to the range from 0x00000000 to 0x00000064, inclusive. The default value MUST be 0x00000064, and the value zero MUST be allowed and treated literally.

**ZoneWritebackInterval:** The interval at which the data for a file backed zone is periodically synced to its data file in persistent storage, in case the in-memory copy of the zone is not yet committed to the data file. [<178>](#Appendix_A_178) The values can range from 1 minute to 1 week (7\*24\*60). When ZoneWritebackInterval is set to a value of 0, the automatic flushing of zone data to the data file is disabled. This setting applies to all zone scopes present on the zone as well.

**EnablePolicies:** A Boolean value that indicates whether the DNS Policies configured on the DNS server are to be applied on DNS Operations. If the value of the property is 0x00000000, then all policies at the server level and zone level are considered disabled and are not applied. Otherwise, the policies are considered enabled.

**EnableServerPolicies:** A Boolean value that indicates whether the DNS server-level Policies configured on the DNS server are to be applied on DNS Operations. If the value of the property is 0x00000000, then all policies at the server level only are considered disabled and are not applied. Otherwise, the policies are considered enabled. If the **EnablePolicies** property value is 0x00000000, then server-level policies are disabled regardless of the **EnableServerPolicies** setting. If the **EnablePolicies** property value is anything other than 0x00000000, then the **EnableServerPolicies** settings apply.

##### DNS Server Address Array Properties

The following properties are IP address arrays (specified by type IDs DNSSRV\_TYPEID\_ADDRARRAY or DNSSRV\_TYPEID\_IPARRAY, and formatted as [DNS\_ADDR\_ARRAY (section 2.2.3.2.3)](#Section_56ba5fabf304486699a44f1c1f9247a3) or as [IP4\_ARRAY (section 2.2.3.2.1)](#Section_588ae29671bf402f999686ecee39dc29), respectively). The DNS server SHOULD support both types.[<179>](#Appendix_A_179)

**Forwarders:** A list of IP addresses indicating to which remote DNS servers this DNS server will forward unresolved queries. If the list is empty then no forwarding will be performed.

**DynamicForwarders:** A list of IP addresses indicating to which remote DNS servers this DNS server will forward unresolved queries where the list may be reordered by the server, sorted by lower prior response time. If the list is empty, no forwarding will be performed if the Forwarders property (section 3.1.1.1.2) is also empty. If the EnableForwarderReordering property (section [3.1.1.1.1](#Section_8903e50a91834a7d964053f6f5a91481)) is 0x00000000, the Forwarders property will be used; otherwise, the DynamicForwarders property will be used.[<180>](#Appendix_A_180)

**ListenAddresses:** A list of local IP addresses on which the DNS server listens for DNS request messages.

The DNS Server SHOULD[<181>](#Appendix_A_181) also support the following properties:

**BreakOnReceiveFrom:** The DNS server will execute a debug break, for debugging purposes, when a DNS query message is received from any IP address in this list. If NULL then no debug breaks will be executed when query messages are received.

**BreakOnUpdateFrom:** The DNS server will execute a debug break, for debugging purposes, when a DNS update message is received from any IP address in this list. If NULL then no debug breaks will be executed when update messages are received.

**LogIPFilterList:** A list of IP addresses that indicates traffic to or from the IP addresses that are logged when logging is enabled. If NULL, traffic to and from all IP addresses is logged when logging is enabled.

##### DNS Server String Properties

The DNS server SHOULD[<182>](#Appendix_A_182) support the following string properties:

**DomainDirectoryPartitionBaseName:** The first name component to use as the name of the DNS domain partition in UTF-8 format. If empty, the DNS server uses "DomainDnsZones". On input, the type ID for this property is DNSSRV\_TYPEID\_LPWSTR, listed in section [2.2.1.1.1](#Section_c49b8142a36441c8914a7675a573b5e4). On output, the type ID for this property is DNSSRV\_TYPEID\_LPSTR, listed in section 2.2.1.1.1.

**ForestDirectoryPartitionBaseName:** The first name component to use as the name of the DNS forest partition in UTF-8 format. If empty, the DNS server uses "ForestDnsZones". On input, the type ID for this property is DNSSRV\_TYPEID\_LPWSTR, listed in section 2.2.1.1.1. On output, the type ID for this property is DNSSRV\_TYPEID\_LPSTR, listed in section 2.2.1.1.1.

**LogFilePath:** An absolute or relative pathname of the log file to which the DNS server SHOULD[<183>](#Appendix_A_183) output logging information. This protocol only treats the pathname as a string, it does not constrain the syntax in any way. This property is encoded as a null-terminated Unicode string, and the type ID for this property is DNSSRV\_TYPEID\_LPWSTR, listed in section 2.2.1.1.1.

**ServerLevelPluginDll:** An absolute pathname of a dynamic link library that the DNS server may use to resolve unknown names, or an empty string to remove or disable the previously selected DLL. This protocol only treats the pathname as a string, it does not constrain the syntax in any way. This property is encoded as a null-terminated Unicode string, and the type ID for this property is DNSSRV\_TYPEID\_LPWSTR, listed in section 2.2.1.1.1.

The DNS Server SHOULD[<184>](#Appendix_A_184) also support the following properties:

**DsBackgroundPauseName:** A single-label name in UTF-8 format which, when matched to the current node name being read during zone background loading from the directory service, causes the DNS server to set the DsBackgroundLoadPaused (section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a)) property to TRUE and stop loading data in the background until the DsBackgroundLoadPaused property is reset to FALSE. The type ID for this property is DNSSRV\_TYPEID\_LPSTR, listed in section 2.2.1.1.1. This property MUST NOT be possible to set using this protocol.

**DoNotRoundRobinTypes:** An array of record types for which the DNS server will disable round robin. The value MUST be an ASCII string containing integers separated by spaces, in either hexadecimal format (prefixed with the ASCII characters '0x' or '0x'), octal format (prefixed with an ASCII '0' and no subsequent 'x' or 'x'), or decimal format (otherwise). Each integer MUST correspond to a DNS record type number, and SHOULD be a value in the range from 0x00000000 to 0x000000FF, though the element values MAY be any value in the range 0x00000000 to 0xFFFFFFFF. This value MUST NOT be changeable via the DNSP protocol.[<185>](#Appendix_A_185)

**RootTrustAnchorsURL:** A URL in UTF-8 format from which the DNS root trust anchors will be downloaded when the "RetrieveRootTrustAnchors" operation is invoked. The default value MUST be https://data.iana.org/root-anchors/root-anchors.xml.[<186>](#Appendix_A_186)

##### DNS Server String List Properties

The following properties are string lists in UTF-8 format. The type ID for this property is DNSSRV\_TYPEID\_UTF8\_STRING\_LIST, listed in section [2.2.1.1.1](#Section_c49b8142a36441c8914a7675a573b5e4).

The DNS Server SHOULD[<187>](#Appendix_A_187) support the following properties:

**GlobalQueryBlockList:** A list of single-label strings for which queries will be blocked if the query name matches any name in this list within any primary zone on the DNS server. The DNS server MUST NOT block queries if the value of the **EnableGlobalQueryBlockList** property (see section [3.1.1.1.1](#Section_8903e50a91834a7d964053f6f5a91481)) is 0x00000000. For a description of the DNS server's behavior when blocking queries, see the description of the **EnableGlobalQueryBlockList** property (see section 3.1.1.1.1).

When the DNS server process starts, if for both this property and for the **EnableGlobalQueryBlockList** property, no value is found in persistent storage, then the DNS server MUST construct and store as the value of this property a generic list of query names to be blocked, and MUST set the value of the **EnableGlobalQueryBlockList** property to 0x00000001 in persistent storage. If the **EnableGlobalQueryBlockList** property is already set to 0x00000001, then an undefined **GlobalQueryBlockList** property is treated as an empty list.

Construction of the generic list of query names to be blocked MUST be performed as follows: the DNS server MUST enumerate all locally hosted primary and secondary zones. If no locally hosted primary or secondary zone contains a DNS record for the name "isatap" that is not of type TXT then "isatap" MUST be added to the list. If no locally hosted primary or secondary zone contains a DNS record for the name "wpad" that is not of type TXT then "wpad" MUST be added to the list.

**SocketPoolExcludedPortRanges:** A list of numeric port number ranges (for example, {"4000-5000", "34000-34000"}) for which listen sockets will not be opened by the DNS server. Ranges MUST have the smaller number (if unequal) first, and are inclusive. Even single port exclusions MUST be specified as a range. Inputs less than 1 or greater than 65,535 are interpreted as 1 and 65,535 respectively.

#### DNS Zone Configuration Information

The list of names that are used in (name, value) pairs in DNS Zone metadata is given below.

##### DNS Zone Integer Properties

Note: Some of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview in the Product Behavior appendix.

The following properties are 32-bit integers. The term Boolean, as used below, means a 32-bit integer where a value of 0x00000000 indicates that the stated property is false, and any nonzero value indicates that the stated property is true.

**AllowUpdate:** The [DNS\_ZONE\_UPDATE (section 2.2.6.1.1)](#Section_d4b84209f00c478f80d78dd0f1633d9e) value for the zone. The value for this property is limited to those listed in the table in section 2.2.6.1.1. If this property's value is changed from any value to ZONE\_UPDATE\_SECURE, the DNS server MUST set the zone's **Time Zone Secured** (section [3.1.1](#Section_e72286df3e4c45359a0ce9cc944248c2)) property to the current time expressed as the number of seconds since 12:00 A.M. January 1, 1601 Coordinated Universal Time (UTC).

**DsIntegrated:** A Boolean indicating whether the zone is stored in the directory server. This property is read-only.

**DsRecordAlgorithms:** The value of the cryptographic hash algorithm used to generate DS records written to a file named "dsset-<ZoneName>"[<188>](#Appendix_A_188) when the zone is first signed and whenever the DNSKEY record set for the zone is changed. The value MUST be limited to the values in the following table. The default value MUST be 0x00000003.[<189>](#Appendix_A_189)

| Value | Meaning |
| --- | --- |
| 0x00000000  DNS\_ZONE\_GENERATE\_DS\_NONE | Do not generate DS records. |
| 0x00000001  DNS\_ZONE\_GENERATE\_DS\_SHA1 | Use SHA-1 to generate DS records. |
| 0x00000002  DNS\_ZONE\_GENERATE\_DS\_SHA256 | Use SHA-256 to generate DS records. |
| 0x00000004  DNS\_ZONE\_GENERATE\_DS\_SHA384 | Use SHA-384 to generate DS records. |

**DSRecordSetTTL:** The TTL value, in seconds, to assign to any new DS record created for this zone and written to the "dsset-<ZoneName>" file during zone signing or key rollover. The value MUST be limited to the range 0x00000000 to 0x00093A80 (1 week), inclusive. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated as the zone default TTL.[<190>](#Appendix_A_190)

**DNSKEYRecordSetTTL:** The TTL value, in seconds, that is assigned to any new DNSKEY record created for this zone during zone signing or key rollover. The value MUST be limited to the range 0x00000000 to 0x00093A80 (1 week), inclusive. The default value MUST be 0x00000000, and the value zero MUST be allowed and treated as the zone default TTL.[<191>](#Appendix_A_191)

**IsKeymaster:** A Boolean indicating whether the DNS server is the key master for this zone. This property can be modified only by using the "TransferKeymasterRole" operation of the R\_DnssrvOperation (Opnum 0) (section [3.1.4.1)](#Section_9500a7e8165d4b13be860ddc43100eef) method call. The default value MUST be 0x00000000.[<192>](#Appendix_A_192)

**IsSigned:** A Boolean indicating whether the zone is signed via Online Signing. This property can be modified only by using the "ZoneSign" or "ZoneUnsign" operation of the R\_DnssrvOperation (Opnum 0) (section 3.1.4.1) method call. The default value MUST be 0x00000000.[<193>](#Appendix_A_193)

**LogUpdates:** A Boolean indicating whether updates on this zone are logged to permanent storage.

**MaintainTrustAnchor:** This property controls how the DNS server maintains the list of forest-wide Trust Anchors as key rollover takes place for signing key descriptors whose fIsKSK flag is set. As the rollover progresses, new keys are generated and added to the forest-wide TrustAnchors zone, and old keys are removed. The value's range MUST be limited to the values in the following table. The default for this value SHOULD[<194>](#Appendix_A_194) be 0x00000000.

| Value | Meaning |
| --- | --- |
| 0x00000000  DNS\_ZONE\_MAINTAIN\_TA\_NONE | Trust Anchors are not updated as key rollover proceeds. |
| 0x00000001  DNS\_ZONE\_MAINTAIN\_TA\_DNSKEY | Keys are stored in the forest-wide TrustAnchors zone as DNSKEY records as the key rollover proceeds. |

**NoRefreshInterval:** The No Refresh interval value, in hours, for the zone. The value 0x00000000 MUST be treated as a flag value for the value of "DefaultNoRefreshInterval" (section [3.1.1.1.1](#Section_8903e50a91834a7d964053f6f5a91481)).

**NSEC3HashAlgorithm:** The algorithm ID used for hashing node owner names in zones signed with NSEC3 as described in [[RFC5155]](http://go.microsoft.com/fwlink/?LinkId=225981) section 3.1.1. The value's range MUST be limited to the values in the following table. The default for this value SHOULD[<195>](#Appendix_A_195) be 0x00000001.

| Value | Meaning |
| --- | --- |
| 0x00000001  DNS\_NSEC3\_HASH\_ALG\_ID\_SHA1 | Use SHA-1 to hash owner names. |

**NSEC3Iterations:** The number of additional iterations that the hashing function is used when generating hashed owner names for zones signed with NSEC3, as described in [RFC5155] section 3.1.3 and section 5. The value's range MUST be 0x00000000 to 0x000009C4, inclusive. The default value SHOULD[<196>](#Appendix_A_196) be 0x00000032.

**NSEC3OptOut:**  A Boolean indicating whether NSEC3 records in a zone signed with NSEC3 have their Opt-Out flag set, as described in [RFC5155] section 3.1.2.1. The default value SHOULD[<197>](#Appendix_A_197) be 0x00000000.

**NSEC3RandomSaltLength:** When zones are signed with NSEC3, salt may be applied to the hashing function when hashed owner names are generated, as described in [RFC5155] section 3.1.5 and section 5. The "NSEC3RandomSaltLength" is the length, in octets, of randomly generated salt. The value 0x00000000 MUST be treated as a flag indicating that the DNS server MUST NOT generate salt randomly but MUST use the "NSEC3UserSalt" zone property. For any other value, the DNS server MUST generate a random salt of the specified length to be used when generating hashed owner names. The value's range MUST be 0x00000000 to 0x000000FF, inclusive. The default value SHOULD[<198>](#Appendix_A_198) be 0x00000008.

**NotifyLevel:** The DNS\_ZONE\_NOTIFY\_LEVEL (section [2.2.5.1.3](#Section_343f4212ad8a47908aa77c5bc15f7bd2)) value for the zone. The value for this property is limited to those listed in the table in section 2.2.5.1.3.

**ParentHasSecureDelegation:** A Boolean indicating whether this zone has a [**secure delegation**](#gt_26f7fedd-71a6-47c1-977d-4ef92e768246) from a parent zone. The default value SHOULD[<199>](#Appendix_A_199) be 0x00000000.

**PropagationTime:** The expected time, in seconds, that it takes for zone data changes to propagate to other copies of the zone, whether these copies are hosted as secondary zones or, if the zone is directory server-integrated, are other primary copies on the directory server. For zones that are directory server-integrated, the default value SHOULD be 0x0002A300 (2 days). Otherwise, the default SHOULD be 0x00000000.[<200>](#Appendix_A_200)

**RefreshInterval:** The refresh interval value, in hours, for the zone. The value 0x00000000 MUST be treated as a flag value for the value of "DefaultRefreshInterval" (section 3.1.1.1.1).

**RFC5011KeyRollovers:** A Boolean indicating whether the zone follows [[RFC5011]](http://go.microsoft.com/fwlink/?LinkId=225980) section 2 as key rollover takes place for signing key descriptors whose fIsKSK flag is set. The default value SHOULD be 0x00000000.[<201>](#Appendix_A_201)

**SecureDelegationPollingPeriod:** The interval, in seconds, between queries to refresh the set of delegation signer (DS) records in a secure delegation. The value MUST be limited to the range 0x00000E10 (1 hour) to 0x0x00093A80 (1 week), inclusive. The default value SHOULD[<202>](#Appendix_A_202) be 0x0000A8C0 (12 hours).

**SecureSecondaries:** The [DNS\_ZONE\_SECONDARY\_SECURITY (section 2.2.5.1.2)](#Section_751e1cf8c97f41c5ae499a674398d0f3) value for the zone. The value for this property is limited to those listed in the table in section 2.2.5.1.2.

**SignatureInceptionOffset:** The interval, in seconds, that the DNS server subtracts from the current time when generating the signature inception field in new RRSIG records ([[RFC4034]](http://go.microsoft.com/fwlink/?LinkId=107052)). The value's range MUST be 0x00000000 to 0x00093A80, inclusive. The default value SHOULD[<203>](#Appendix_A_203) be 0x00000E10.

**SignWithNSEC3:** A Boolean indicating whether an online-signed zone is signed using NSEC3 ([RFC5155]) for denial of existence. A zone not using NSEC3 will use NSEC ([RFC4034]). The default value SHOULD[<204>](#Appendix_A_204) be 0x00000001.

**Type:** The DNS\_ZONE\_TYPE (section [2.2.5.1.1](#Section_27e138a7110c44a4afcbb95f35f00306)) value for the zone. This property is read-only.

The DNS server SHOULD support the following properties:

**Aging:** A Boolean indicating whether aging SHOULD[<205>](#Appendix_A_205) be enabled for the zone.

**ForwarderSlave:** A Boolean indicating whether normal recursion SHOULD[<206>](#Appendix_A_206) be used to resolve queries if the master servers for the forwarder zone are unreachable.

**ForwarderTimeout:** The number of seconds the DNS server SHOULD[<207>](#Appendix_A_207) wait for response for a forwarded query.

**Unicode:** The server SHOULD[<208>](#Appendix_A_208) ignore any value set for this Boolean property.

**PluginEnabled:** A Boolean indicating whether the zone is configured to use a plugin. If a zone is configured to use a plugin, then incoming queries are forwarded to the plugin for calculation of the appropriate zone scope for query resolution.[<209>](#Appendix_A_209)

**EnablePolicies:** A Boolean value that indicates whether the DNS Policies on the zone configured on the DNS server are to be applied on DNS Operations. If the value of the property is 0x00000000, then all policies at the zone level are considered disabled and are not applied. Otherwise, the policies are considered enabled. If **EnablePolicies** (section 3.1.1.1.1) is 0x00000000, then zone-level policies are disabled regardless of the **EnablePolicies** setting (section 3.1.1.2.1). If the **EnablePolicies** property value is anything other than 0x00000000, then the **EnablePolicies** settings apply.

##### DNS Zone Address Array Properties

The following properties are IP address arrays (specified by type IDs DNSSRV\_TYPEID\_ADDRARRAY or DNSSRV\_TYPEID\_IPARRAY and formatted as DNS\_ADDR\_ARRAY (section [2.2.3.2.3](#Section_56ba5fabf304486699a44f1c1f9247a3)) or IP4\_ARRAY (section [2.2.3.2.1](#Section_588ae29671bf402f999686ecee39dc29)), respectively). The DNS server SHOULD support both types.

**AllowNSRecordsAutoCreation:** A list of IP addresses used to restrict automatic NS record creation for the zone. If the list is empty then NS record creation is not restricted. This setting is ignored if the zone is not stored in the directory server. The DNS server MUST NOT create an NS record for the FQDN of the local machine if one the machine's IP addresses is not present in this list.

**ScavengeServers:** A list of IP addresses of DNS servers authorized to perform scavenging of records in the zone.

The DNS Server SHOULD[<210>](#Appendix_A_210) also support the following properties:

**MasterServers:** A list of IP addresses of primary DNS servers for the zone. This value is required to be non-empty for any zone of a type that requires primary DNS servers: secondary, stub, or forwarder.

**LocalMasterServers:** A list of IP addresses of the zone's primary DNS servers used locally by this DNS server only. If not configured, the MasterServers value is used; otherwise, this list is used in place of the MasterServers value. This value is ignored if the zone type is not stub.

**NotifyServers:** A list of IP addresses of remote DNS servers to be notified for any changes to the zone. If empty, then no remote DNS servers will be notified when changes are made to this zone.

**SecondaryServers:** A list of IP addresses of authorized secondary DNS servers for the zone.

##### DNS Zone String Properties

The following properties are strings.

**DatabaseFile:** The name (with no path) of the zone file or NULL if the zone is not stored in a file.

**ApplicationDirectoryPartition:** The FQDN of the application directory partition that the zone is stored in if "DsIntegrated" is TRUE, or NULL if the zone is not stored in a directory server.

The DNS server SHOULD[<211>](#Appendix_A_211) also support the following properties:

**BreakOnNameUpdate:** The DNS server will execute a debug break when the specified node name within the zone is the target of a DNS update. If this property is NULL or empty the DNS server will not execute debug breaks during DNS update processing.

**Keymaster:** The FQDN of the key master server for the zone[<212>](#Appendix_A_212). The default value MUST be NULL.

**NSEC3UserSalt:** Salt that is to be used when hashed owner names are generated according to [[RFC5155]](http://go.microsoft.com/fwlink/?LinkId=225981) section 5 in zones signed with NSEC3. This property MUST be ignored unless the NSEC3RandomSaltLength property is set to 0x00000000.[<213>](#Appendix_A_213)

**NSEC3CurrentSalt:** The current salt being used by a zone signed with NSEC3 to generate hashed owner names as described in [RFC5155] section 5. This property is read-only.[<214>](#Appendix_A_214)

##### DNS Record Configuration Information

The list of names that are used in (name, value) pairs in DNS Zone metadata is given below. All properties below are 32-bit integers.

**Aging Time Stamp:** A time stamp value that specifies at what time this record was last updated. This property is initialized and written to the **whenChanged** attribute of its "dnsNode" object (section [2.3](#Section_74db40e109174ecb863d9bce5165ebf3)).

##### DNS Zone Scope or Cache Scope Configuration Information

Zone scopes and cache scopes are unique versions of the zone and cache zone respectively. Multiple zone scopes or cache scopes can be configured inside the same zone or cache zone. They MAY contain different resource record sets from each other. [<215>](#Appendix_A_215)

#### DNS Server Server Scope Configuration Information

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The list of names that are used in (name, value) pairs in DNS Server Server scope configuration information is given below.

##### DNS Server Server Scope Integer Properties

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The following properties are 32-bit integers. The term Boolean, as used below, means a 32-bit integer where a value of 0x00000000 indicates that the stated property is FALSE, and any nonzero value indicates that the stated property is TRUE.

These properties are part of a server scope and are applicable when a DNS operation matches a DNS recursion policy and selects a specific server scope

**NoRecursion:** A Boolean value indicating whether the DNS server will perform any recursion. If TRUE, the DNS server MUST NOT recurse and will only answer queries for authoritative data.

##### DNS Server Server Scope Address Array Properties

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The following properties are IP address arrays (specified by type IDs DNSSRV\_TYPEID\_ADDRARRAY or DNSSRV\_TYPEID\_IPARRAY and formatted as DNS\_ADDR\_ARRAY (section [2.2.3.2.3](#Section_56ba5fabf304486699a44f1c1f9247a3)) or IP4\_ARRAY (section [2.2.3.2.1](#Section_588ae29671bf402f999686ecee39dc29)), respectively). The DNS server SHOULD support both types.[<216>](#Appendix_A_216)

These properties are part of a server scope and are applicable when a DNS operation matches a DNS recursion policy and selects a specific server scope.

**Forwarders:** A list of IP addresses indicating to which remote DNS servers this DNS server will forward unresolved queries. If the list is empty then no forwarding will be performed.

### Timers

No timers are required beyond those used internally by RPC to implement resiliency to network outages, as specified in [[MS-RPCE]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-RPCE%5d.pdf) section 3.2.3.2.1.

### Initialization

At initialization time, the server MUST load the DNS Server Configuration (section [3.1.1](#Section_e72286df3e4c45359a0ce9cc944248c2)) from persistent local storage. The server MUST then initialize its zones:

If the server is configured to use a directory server:

* The server MUST invoke the task "Initialize an ADConnection", as defined in [[MS-ADTS]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ADTS%5d.pdf) section 7.6.1.1, with the following parameters:
  + **TaskInputTargetName:** NULL.
  + **TaskInputPortNumber:** 389.
* The server MUST store the new **TaskReturnADConnection** returned from the task as **DNS Server AD Connection**.
* If the AD connection is successfully initialized, the server MUST invoke the task "Setting an LDAP Option on an ADConnection", as defined in [MS-ADTS] section 7.6.1.2 on the Active Directory connection **DNS Server AD Connection**. Parameters for this task are as follows:
  + **TaskInputOptionName:** LDAP\_OPT\_AREC\_EXCLUSIVE.
  + **TaskInputOptionValue:** TRUE.
  + **TaskInputOptionName:** LDAP\_OPT\_PROTOCOL\_VERSION.
  + **TaskInputOptionValue:** 3.
  + **TaskInputOptionName:** LDAP\_OPT\_TIMELIMIT.
  + **TaskInputOptionValue:**  180.
  + **TaskInputOptionName:** LDAP\_OPT\_REFERRALS.
  + **TaskInputOptionValue:** FALSE.
* After the Active Directory connection is initialized and the option is set, the server MUST invoke the "Establishing an ADConnection" task, as specified in [MS-ADTS] section 7.6.1.3, with the **TaskInputADConnection** parameter set to **DNS Server AD Connection**.
* For the final step to complete the connection through LDAP to the local directory server, the server MUST invoke the "Performing an LDAP Bind on an ADConnection" task, as specified in [MS-ADTS] section 7.6.1.4, with the **TaskInputADConnection** parameter set to **DNS Server AD Connection**.
* If any of the previous steps returns an error, the server MUST retry the connection with LDAP up to eight times, unless the **Global Server State** changes to "Stopping", in which case it MUST discontinue initialization. If each of the eight attempts to connect with LDAP fails, the server MUST continue initialization.
  + If the connection with LDAP was successfully established:
    - The server MUST check that the "DnsAdmins" group already exists in the **Local security groups** (see section 3.1.1). If it does not exist, and if the server is not a read-only server, then the server MUST create the "DnsAdmins" group in the **Local security groups**. The groupType attribute value for the "DnsAdmins" group MUST be 0x80000004.
    - If the server is not a read-only server, it MUST:
      * Attempt to add the "MicrosoftDNS" container object by invoking the "Performing an LDAP Operation on an ADConnection" task, as specified in [MS-ADTS] section 7.6.1.6, with the following parameters:
        + **TaskInputADConnection**: **DNS Server AD Connection**.
        + **TaskInputRequestMessage**: protocolOp is set to **addRequest** ([[RFC4511]](http://go.microsoft.com/fwlink/?LinkId=157505) section 4.7).
        + The parameters of the **addRequest** are set as follows:

**entry**: "CN=MicrosoftDNS,CN=System,<Forest DN>"

**attributes**:

**type**: "objectClass"; **vals**: "container"

**type**: "cn"; **vals**: "MicrosoftDNS"

* + - * If the operation was successful, or if the operation failed because the object already existed and the "DnsAdmins" group was newly created in the last step, then the server MUST:
        + Attempt to grant all rights and ownership, with container inheritance, for the "MicrosoftDNS" (distinguished name: "CN=MicrosoftDNS,CN=System,<Forest DN>)" object to the "DnsAdmins" group by following the procedure specified in section [3.1.6.4](#Section_fb192c0d664b4dddb490af241b664f8c).
        + Attempt to grant all rights, with container inheritance, for the "MicrosoftDNS" (distinguished name: "CN=MicrosoftDNS,CN=System,<Forest DN>") object to the "Enterprise Domain Controllers" group by following the procedure specified in section 3.1.6.4.
        + Attempt to remove all rights for the "MicrosoftDNS" (distinguished name: "CN=MicrosoftDNS,CN=System,<Forest DN>") object from the "Authenticated Users" and "Built-In Administrators" groups by following the procedure specified in section 3.1.6.4.
      * If the attempted addition of the "MicrosoftDNS" container object was successful, or if it failed because the object already existed, the server MUST:
        + Check that the **displayName** attribute of the object has been set, by invoking the "Performing an LDAP Operation on an ADConnection" task, as specified in [MS-ADTS] section 7.6.1.6, with the following parameters:

**TaskInputADConnection**: **DNS Server AD Connection**.

**TaskInputRequestMessage**: protocolOp is set to searchRequest ([RFC4511] section 4.5).

The parameters of the **searchRequest** are set as follows:

**baseObject**: "CN=MicrosoftDNS,CN=System,<Forest DN>"

**scope**: base (0)

**derefAliases**: neverDerefAliases (0)

**sizeLimit**: 0

**timeLimit**: 360

**typesOnly**: FALSE

**filter**: "(objectCategory=\*)"

**attributes**: **displayName**

* + - * + If the search request was successful and the "MicrosoftDNS" container has no values for the **displayName** attribute, then modify the **displayName** attribute by invoking the "Performing an LDAP Operation on an ADConnection" task, as specified in [MS-ADTS] section 7.6.1.6, with the following parameters:

**TaskInputADConnection**: **DNS Server AD Connection**.

**TaskInputRequestMessage**: protocolOp is set to modifyRequest ([RFC4511] section 4.6).

The parameters of the **modifyRequest** are set as follows:

**object**: "CN =MicrosoftDNS,CN=System,<Forest DN>"

**changes**:

**operation**: replace

**type**: **displayDNS**

**vals**: "DNS Servers"

* + - * The server MUST attempt to enumerate the application directory by invoking the "Performing an LDAP Operation on an ADConnection" task, as specified in [MS-ADTS] section 7.6.1.6, with the following parameters:
        + **TaskInputADConnection:** **DNS Server AD Connection**.
        + **TaskInputRequestMessage:** **protocolOp** is set to **searchRequest** ([RFC4511] section 4.5).
        + The parameters of the **searchRequest** are set as follows:

**baseObject:** "CN=Partitions,CN=Configuration,<Forest DN>"

**scope:** singleLevel (1)

**derefAliases:** neverDerefAliases (0)

**sizeLimit:** 0

**timeLimit:** 360

**typesOnly:** FALSE

**filter:** "(objectCategory=crossRef)"

**attributes:** "CN, ntSecurityDescriptor, instanceType, ms-DS-SDReferenceDomain, systemFlags, msDS-NC-Replica-Locations, ms-DS-NC-RO-Replica-Locations, nCName, dnsRoot, objectGUID, whenCreated, whenChanged, usnCreated, usnChanged, Enabled, objectClass"

* + - * For each object found in the search, the server MUST use the configuration, replication, and security metadata values contained in the object to construct a structure of type DNS\_RPC\_DP\_INFO (see section [2.2.7.2.1](#Section_bd2a817d6a6940d3befc0c198a9c6e80)), computing the value of each field as specified in section 2.2.7.2.1, and the server MUST insert the structure as an entry in the Application Directory Partition Table. The server MUST create the in-memory Application Directory Partition Access Control List by copying the "ntSecurityDescriptor" attribute of the "crossRef" object. The server MUST also retrieve and store, in memory, the identity of the Domain Naming Master FSMO role owner. If the default DNS Domain Partition or default DNS Forest Partition is not present during polling, the server MUST attempt to create and enlist in these partitions. If any LDAP operation fails, the server MUST continue initialization.

In all cases:

* The server MUST retrieve the list of zones to load from the source specified by the "BootMethod" setting's value (section[2.2.4.1.1](#Section_dc737abd3e844814a62a9398c770f28f)) and attempt to load zones from the configuration source specified by the "BootMethod" setting (section [3.1.1.1.1](#Section_8903e50a91834a7d964053f6f5a91481)).
  + If the method is BOOT\_METHOD\_UNINITIALIZED (section 2.2.4.1.1):
    - If a zone loaded from the local directory server results in a zone with no nodes, the server MUST then attempt to load the same zone from file-based persistent storage.
  + If the method is BOOT\_METHOD\_DIRECTORY (section 2.2.4.1.1):
    - If a zone loaded from the local directory server results in a zone with no nodes, the server MUST then attempt to load the same zone from file-based persistent storage.
    - If the LDAP connection to the directory server is unavailable, the server MUST attempt to load those zones specified in the persistent copy of the DNS Zone Table that are stored in local persistent storage.
    - If the LDAP connection to the directory server is available, the server MUST attempt to load the zones specified in the persistent copy of the DNS Zone Table, but only those zones stored in the Application Directory Partitions in which the server is enlisted. This MUST include at minimum the "defaultNamingContext" of the directory server's rootDSE, the default DNS Domain Partition and the default DNS Forest Partition. If the zone is stored in local persistent storage, the server MUST attempt to load the zone. If the zone is directory server-integrated, the server MUST attempt to load the LDAP "dnsZone" and "dnsNode" objects (section [2.3](#Section_74db40e109174ecb863d9bce5165ebf3)) that represent the zone from the directory server. The DNS server MUST ignore any DNS node in the directory server which has the dnsTombstoned attribute set to TRUE. If an attempt to load a zone fails for any reason, the server MUST clear the contents of the in-memory zone (if any) and mark the zone state as shutdown (see section [2.2.5.2.2](#Section_015F97AFBA5048BBAF444A542F3FF44A)), but continue initialization.
    - If there are no root hints in the local directory server, but root hints were loadable from a file-based persistent storage and are non-empty, the server MUST write the root hints back to the local directory server through the WriteDirtyZones operation [3.1.4.1](#Section_9500a7e8165d4b13be860ddc43100eef) by using the DNS\_ZONE\_LOAD\_OVERWRITE\_DS flag [2.2.5.2.7.1](#Section_780eba2615ea43d3a2b377ed9ab00690).
* The DNS Server Management Protocol server MUST register the RPC interface and begin listening on the RPC transports, as specified in section [2.1](#Section_09591e5ada87438cb70e2ec62dd82314), and limited by the flags specified for the "RpcProtocol" property (section 3.1.1.1.1).
* The server SHOULD invoke the **NetlogonControl2Ex** method with function code NETLOGON\_CONTROL\_FORCE\_DNS\_REG on the Netlogon protocol implementation on the local Domain Controller.[<217>](#Appendix_A_217) (See [[MS-NRPC]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-NRPC%5d.pdf) section 3.5.4.9.1.)

### Message Processing Events and Sequencing Rules

The server MUST indicate to the RPC runtime that it is to perform a strict [**Network Data Representation (NDR)**](#gt_9ebf9540-2c31-43bc-bc56-4a932faabf2d) data consistency check at target level 5.0, as specified in [[MS-RPCE]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-RPCE%5d.pdf) section 3.

Wherever this protocol requires an LDAP operation, if the operation is implemented as an asynchronous LDAP call, the asynchronous result MUST be retrieved prior to returning from the DNS Server Management Protocol operation. The timeout for individual LDAP operations, other than the delete operation, MUST be 180 seconds, and the timeout for LDAP delete operations MUST be 1,440 seconds, unless otherwise stated. LDAP add and modify operations MUST be requested with an asynchronous LDAP method, and the server MUST retry an add or modify operation up to three times if an error prevents submission of the operation, but it MUST NOT retry if the asynchronous result of the operation is unsuccessful. All other operations MUST NOT be retried unless otherwise stated.

Wherever this protocol requires an addition, modification, or deletion of the information in the abstract data model (section [3.1.1](#Section_e72286df3e4c45359a0ce9cc944248c2)), the prescribed operation MUST be performed only on the local in-memory portions of the abstract data model, unless otherwise specified.

Wherever this protocol requires a modification to a DNS Zone Table stored in-memory, the server MUST set the Dirty Flag to TRUE when the modification occurs. Wherever this protocol requires a DNS Zone Table stored in-memory to be written to persistent storage, the server MUST set the Dirty Flag to FALSE upon successful completion of the write.

[**Opnums**](#gt_e127848e-c66d-427d-b3aa-9f904fa4ada7) 0 through 4 are deprecated. Clients SHOULD[<218>](#Appendix_A_218) use opnums 5 through 9 instead and servers SHOULD support all methods in the table.

This interface includes the following methods in RPC opnum order:

Methods in RPC Opnum Order

| Method | Description |
| --- | --- |
| [R\_DnssrvOperation](#Section_9500a7e8165d4b13be860ddc43100eef) | Invokes a specified set of server functions. This method is obsoleted by R\_DnssrvOperation2.  Opnum: 0 |
| [R\_DnssrvQuery](#Section_b0419a70ac0b40baab941510992bc574) | Issues type specific information queries to server. This method is obsoleted by R\_DnssrvQuery2.  Opnum: 1 |
| [R\_DnssrvComplexOperation](#Section_864a6971f66447b9b012826fd2b0a409) | Invokes a specified set of server functions, which return complex structures. This method is obsoleted by R\_DnssrvComplexOperation2.  Opnum: 2 |
| [R\_DnssrvEnumRecords](#Section_d0251c9b9e3e4eecbcc5eb6b995b6108) | Enumerates DNS records on the server. This method is obsoleted by R\_DnssrvEnumRecords2.  Opnum: 3 |
| [R\_DnssrvUpdateRecord](#Section_37eea10100b8495899ebde8cda4b8417) | Adds/deletes/modifies DNS records. This method is obsoleted by R\_DnssrvUpdateRecord2.  Opnum: 4 |
| [R\_DnssrvOperation2](#Section_8c0522b197fb4fa7b4e22c55c0afb0e7) | Invokes a specified set of server functions.  Opnum: 5 |
| [R\_DnssrvQuery2](#Section_a90a44f0f64e44b09e35a7fc49f6adea) | Issues type specific information queries to server.  Opnum: 6 |
| [R\_DnssrvComplexOperation2](#Section_d28e3ba85742417dad6d2e0139ab2ad9) | Invokes a specified set of server functions, which return complex structures.  Opnum: 7 |
| [R\_DnssrvEnumRecords2](#Section_0d236e5899444cdfae98f92460202e29) | Enumerates DNS records on the server.  Opnum: 8 |
| [R\_DnssrvUpdateRecord2](#Section_8f50ae96d87f4fdb85265a86cea25837) | Adds/deletes/modifies DNS records.  Opnum: 9 |
| [R\_DnssrvUpdateRecord3](#Section_12279f8cddaf47b8890591d7635cdfea) | Adds, deletes, or modifies DNS records to the zone or zone scope, or cache zone or cache scope (if specified).  Opnum: 10 |
| [R\_DnssrvEnumRecords3](#Section_d7d4a3ac79954d419fcf1826cce95e2c) | Enumerates DNS records on the server in a particular zone or zone scope, or cache zone or cache scope (if specified).  Opnum: 11 |
| [R\_DnssrvOperation3](#Section_54044c364e9e44fb80dfffb026939b8b) | Invokes a specified set of server functions.  Opnum: 12 |

#### R\_DnssrvOperation (Opnum 0)

Note: Some of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview in the Product Behavior appendix.

The R\_DnssrvOperation method is used to invoke a set of server functions specified by pszOperation.

1. LONG R\_DnssrvOperation(
2. [in] handle\_t hBindingHandle,
3. [in, unique, string] LPCWSTR pwszServerName,
4. [in, unique, string] LPCSTR pszZone,
5. [in] DWORD dwContext,
6. [in, unique, string] LPCSTR pszOperation,
7. [in] DWORD dwTypeId,
8. [in, switch\_is(dwTypeId)] DNSSRV\_RPC\_UNION pData
9. );

**hBindingHandle:** An RPC binding handle to the server. Details concerning binding handles are specified in [[C706]](http://go.microsoft.com/fwlink/?LinkId=89824) section 2.3.

**pwszServerName:** The client SHOULD pass a pointer to the FQDN of the target server as a null-terminated UTF-16LE character string. The server MUST ignore this value.

**pszZone:** A pointer to a null-terminated character string that contains the name of the zone to be queried. For operations specific to a particular zone, this string MUST contain the name of the zone in UTF-8 format or a [**multizone operation string**](#gt_c283d511-037e-4df1-a55e-3a26b379d8bf) (given in the table that follows) that indicates that the operation is performed on multiple zones, but only if dwContext is zero. If dwContext is not zero, then the value of pszZone MUST be ignored. For all other operations this value MUST be set to NULL. When pszZone is NULL, the valid operations are in the first table under the pszOperation section that follows, or are a property name listed in section [3.1.1.1.2](#Section_f73f36ca3f0640caa392f7837d62642f), [3.1.1.1.3](#Section_c9d38538882744e6aa5e022a016ed723), or [3.1.1.1.4](#Section_35e541ef7a594a44ba187cd00aba6a0d). If this value is not NULL, then this value will be used by certain operations as specified in the second table for pszOperation that follows.

The following table shows what values may be specified to request that the operation be performed on multiple zones, using ZONE\_REQUEST\_FILTERS values (section [2.2.5.1.4](#Section_f4cf1f3e7d134010a9155223dcabc15d)).

| Value | Meaning |
| --- | --- |
| "..AllZones" | ZONE\_REQUEST\_PRIMARY |  ZONE\_REQUEST\_SECONDARY |  ZONE\_REQUEST\_AUTO |  ZONE\_REQUEST\_FORWARD |  ZONE\_REQUEST\_REVERSE |  ZONE\_REQUEST\_FORWARDER |  ZONE\_REQUEST\_STUB |  ZONE\_REQUEST\_DS |  ZONE\_REQUEST\_NON\_DS |  ZONE\_REQUEST\_DOMAIN\_DP |  ZONE\_REQUEST\_FOREST\_DP |  ZONE\_REQUEST\_CUSTOM\_DP |  ZONE\_REQUEST\_LEGACY\_DP |
| "..AllZonesAndCache" | ZONE\_REQUEST\_PRIMARY |  ZONE\_REQUEST\_SECONDARY |  ZONE\_REQUEST\_CACHE |  ZONE\_REQUEST\_AUTO |  ZONE\_REQUEST\_FORWARD |  ZONE\_REQUEST\_REVERSE |  ZONE\_REQUEST\_FORWARDER |  ZONE\_REQUEST\_STUB |  ZONE\_REQUEST\_DS |  ZONE\_REQUEST\_NON\_DS |  ZONE\_REQUEST\_DOMAIN\_DP |  ZONE\_REQUEST\_FOREST\_DP |  ZONE\_REQUEST\_CUSTOM\_DP |  ZONE\_REQUEST\_LEGACY\_DP |
| "..AllPrimaryZones" | ZONE\_REQUEST\_PRIMARY |
| "..AllSecondaryZones" | ZONE\_REQUEST\_SECONDARY |
| "..AllForwardZones" | ZONE\_REQUEST\_FORWARD |
| "..AllReverseZones" | ZONE\_REQUEST\_REVERSE |
| "..AllDsZones" | ZONE\_REQUEST\_DS |
| "..AllNonDsZones" | ZONE\_REQUEST\_NON\_DS |
| "..AllPrimaryReverseZones" | ZONE\_REQUEST\_REVERSE | ZONE\_REQUEST\_PRIMARY |
| "..AllPrimaryForwardZones" | ZONE\_REQUEST\_FORWARD | ZONE\_REQUEST\_PRIMARY |
| "..AllSecondaryReverseZones" | ZONE\_REQUEST\_REVERSE | ZONE\_REQUEST\_SECONDARY |
| "..AllSecondaryForwardZones" | ZONE\_REQUEST\_FORWARD | ZONE\_REQUEST\_SECONDARY |

**dwContext:** A value used to specify [**multizone operations**](#gt_9370bb2e-b104-4d3d-b606-d111b021a943) in ZONE\_REQUEST\_FILTERS (section 2.2.5.1.4) format or zero if the operation is not meant to apply to multiple zones. If pszZone is not NULL and matches the name of a zone hosted by the DNS server then the value of dwContext MUST be ignored.

**pszOperation:** A pointer to a null-terminated ASCII character string that contains the name of operation to be performed on the server. These are two sets of allowed values for pszOperation:

If pszZone is set to NULL, pszOperation MUST be either a property name listed in section 3.1.1.1.2, 3.1.1.1.3 or 3.1.1.1.4 , or SHOULD[<219>](#Appendix_A_219) be one of the following.

| Value | Meaning |
| --- | --- |
| ResetDwordProperty | Update the value of a (name, value) pair in DNS Server Configuration. On input, dwTypeId MUST be set to DNSSRV\_TYPEID\_NAME\_AND\_PARAM, and pData MUST point to a structure of type DNS\_RPC\_NAME\_AND\_PARAM (section [2.2.1.2.5](#Section_408e91b91e534631a0515e097394f8d8)) that specifies the name of a property listed in section [3.1.1.1.1](#Section_8903e50a91834a7d964053f6f5a91481) and a new value for that property. |
| Restart | The server SHOULD restart the DNS server process. dwTypeId and pData MUST be ignored by the server.[<220>](#Appendix_A_220) |
| ClearDebugLog | Clear the debug log. dwTypeId and pData MUST be ignored by the server. |
| ClearCache | Delete all cached records from the cache zone or cache scope memory. dwTypeId and pData MUST be ignored by the server. |
| WriteDirtyZones | Write all zones that are stored in local persistent storage to local persistent storage if the zone's **Dirty Flag** (section [3.1.1](#Section_e72286df3e4c45359a0ce9cc944248c2)) is set to TRUE. dwTypeId and pData MUST be ignored by the server. |
| ZoneCreate | Create a zone. On input, dwTypeId SHOULD[<221>](#Appendix_A_221) be set to DNSSRV\_TYPEID\_ZONE\_CREATE. pData MUST point to a structure of one of the types specified in DNS DNS\_RPC\_ZONE\_CREATE\_INFO (section [2.2.5.2.7](#Section_f79e7455e26643d3ab2bf8e75aacfefa)) that contains all parameters of a new zone to be created by the DNS server, and pData MUST conform to the description corresponding to the value of dwTypeId (section [2.2.1.1.1](#Section_c49b8142a36441c8914a7675a573b5e4)) If pData points to a DNS\_ZONE\_TYPE\_CACHE or DNS\_ZONE\_TYPE\_SECONDARY\_CACHE record, the server MUST return a nonzero error. If pData points to a DNS\_ZONE\_TYPE\_STUB, DNS\_ZONE\_TYPE\_SECONDARY, or DNS\_ZONE\_TYPE\_FORWARDER record, the server MAY return a nonzero error, but SHOULD return success.[<222>](#Appendix_A_222) |
| ClearStatistics | Clears server statistics data on the DNS server. dwTypeId and pData MUST be ignored by the server. |
| EnlistDirectoryPartition | On input dwTypeId MUST be set to DNSSRV\_TYPEID\_ENLIST\_DP, and the pData MUST point to a DNS\_RPC\_ENLIST\_DP (section [2.2.7.2.5](#Section_7f445256e1694f1ea244d4223fbdf604)) structure. This operation allows application directory partitions to be added to or deleted from the Application Directory Partition Table, and also allows the DNS server to be directed to add or remove itself from the replication scope of an existing application directory partition. |
| StartScavenging | Initiate a resource record scavenging cycle on the DNS server. dwTypeId, and pData MUST be ignored by the server. |
| AbortScavenging | Terminate a resource record scavenging cycle on the DNS server. dwTypeId and pData MUST be ignored by the server. |
| AutoConfigure | On input, dwTypeId SHOULD be set to DNSSRV\_TYPEID\_AUTOCONFIGURE, in which case pData MUST point to a structure of type DNS\_RPC\_AUTOCONFIGURE (section [2.2.8.2.1](#Section_414cf6fba8884c5591a46f77dff66cbe))[<223>](#Appendix_A_223); dwTypeId MAY instead be set to DNSSRV\_TYPEID\_DWORD in which case pData MUST point to a DWORD in DNS\_RPC\_AUTOCONFIG (section [2.2.8.1.1](#Section_d02b0aa23a704f66a63709bd55f6ec6d)) format. |
| ExportSettings | Export DNS settings on the DNS server to a file on the DNS server. dwTypeId SHOULD be set to DNSSRV\_TYPEID\_LPWSTR, and pData MUST be ignored by the server. |
| PrepareForDemotion | Prepares for demotion by removing references to this DNS server from all zones stored in the directory server. dwTypeId and pData MUST be ignored by the server. |
| PrepareForUninstall | This operation does nothing on the DNS server. dwTypeId and pData MUST be ignored by the server. |
| DeleteNode | On input dwTypeId MUST be set to DNSSRV\_TYPEID\_NAME\_AND\_PARAM, and pData MUST point to a structure of type DNS\_RPC\_NAME\_AND\_PARAM (section 2.2.1.2.5) that contains the FQDN of the node pointed to by pszNodeName in the DNS server's cache to be deleted and a Boolean flag in dwParam to indicate if the node subtree is to be deleted. |
| DeleteRecordSet | On input dwTypeId MUST be set to DNSSRV\_TYPEID\_NAME\_AND\_PARAM, and pData MUST point to a structure of type DNS\_RPC\_NAME\_AND\_PARAM (section 2.2.1.2.5). That structure contains the FQDN of the node to be deleted, which is cached on the DNS server, and the type of record set in the dwParam member, which indicates whether the entire set of this type is to be deleted. The type MUST be a DNS\_RECORD\_TYPE value (section [2.2.2.1.1](#Section_39b03b89226440638198d62f62a6441a)) or 0x00FF, which specifies all types. |
| WriteBackFile | Write all information for root hints back to persistent storage. dwTypeId and pData MUST be ignored by the server. |
| ListenAddresses | On input, dwTypeId MUST be set to DNSSRV\_TYPEID\_IPARRAY or DNSSRV\_TYPEID\_ADDRARRAY and pData MUST point to a structure of type IP4\_ARRAY (section [2.2.3.2.1](#Section_588ae29671bf402f999686ecee39dc29)) or DNS\_ADDR\_ARRAY (section [2.2.3.2.3](#Section_56ba5fabf304486699a44f1c1f9247a3)) respectively, which contains a list of new IP addresses on which the DNS server can listen. The server SHOULD accept DNSSRV\_TYPEID\_ADDRARRAY and DNS\_ADDR\_ARRAY, and MAY accept DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY.[<224>](#Appendix_A_224) |
| Forwarders | On input dwTypeId SHOULD be set to DNSSRV\_TYPEID\_FORWARDERS[<225>](#Appendix_A_225), and pData MUST point to a structure of one of the types specified in DNS\_RPC\_FORWARDERS (section [2.2.5.2.10](#Section_83f4bfffc5fb4029aad305b3d7f4ef40)), which contains information about new IP addresses to which the DNS server can forward queries. |
| LogFilePath | On input dwTypeId MUST be set to DNSSRV\_TYPEID\_LPWSTR, and pData MUST point to a Unicode string that contains an absolute or relative pathname or filename for the debug log file on the DNS server. |
| LogIPFilterList | On input dwTypeId MUST be set to DNSSRV\_TYPEID\_IPARRAY or DNSSRV\_TYPEID\_ADDRARRAY, and pData MUST point to a structure of type IP4\_ARRAY (section 2.2.3.2.1) or DNS\_ADDR\_ARRAY (section 2.2.3.2.3) respectively, which contains a list of new IP addresses used for debug log filter. The DNS server will write to the debug log only for traffic to/from these IP addresses. The server SHOULD accept DNSSRV\_TYPEID\_ADDRARRAY and DNS\_ADDR\_ARRAY, and MAY accept DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY.[<226>](#Appendix_A_226) |
| ForestDirectoryPartitionBaseName | The DNS server MUST return an error. |
| DomainDirectoryPartitionBaseName | The DNS server MUST return an error. |
| GlobalQueryBlockList | Update the list of single-label names for which queries are blocked. Query names that match this list, in any primary zone, will be blocked. On input dwTypeId MUST be set to DNSSRV\_TYPEID\_UTF8\_STRING\_LIST, and pData MUST point to a structure of type DNS\_RPC\_UTF8\_STRING\_LIST (section [2.2.1.2.3](#Section_8c593fe61a074140992c71f97f929ba3)). |
| BreakOnReceiveFrom | On input dwTypeId MUST be set to DNSSRV\_TYPEID\_IPARRAY or DNSSRV\_TYPEID\_ADDRARRAY and pData MUST point to a structure of type IP4\_ARRAY (section 2.2.3.2.1) or DNS\_ADDR\_ARRAY (section 2.2.3.2.3) respectively, that contains a list of new IP addresses for which the DNS server will execute a breakpoint if a packet is received from these IP addresses. The server SHOULD accept DNSSRV\_TYPEID\_ADDRARRAY and DNS\_ADDR\_ARRAY, and MAY accept DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY.[<227>](#Appendix_A_227) |
| BreakOnUpdateFrom | On input dwTypeId MUST be set to DNSSRV\_TYPEID\_IPARRAY or DNSSRV\_TYPEID\_ADDRARRAY, and pData MUST point to a structure of type IP4\_ARRAY (section 2.2.3.2.1) or DNS\_ADDR\_ARRAY (section 2.2.3.2.3) respectively, that contains a list of new IP addresses for which the DNS server will execute a breakpoint if an update is received from these IP addresses. The server SHOULD accept DNSSRV\_TYPEID\_ADDRARRAY and DNS\_ADDR\_ARRAY, and MAY accept DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY.[<228>](#Appendix_A_228) |
| ServerLevelPluginDll | On input **dwTypeId** MUST be set to DNSSRV\_TYPEID\_LPWSTR, and **pData** MUST point to a Unicode string that contains an absolute pathname for server side plug-in binary on the DNS server or an empty Unicode string. |
| ActiveRefreshAllTrustPoints | Schedules an immediate RFC 5011 **active refresh** for all trust points, regardless of the time of the last active refresh. The *dwTypeId* and *pData* parameters MUST be set to zero/NULL by the client and MUST be ignored by the server.[<229>](#Appendix_A_229) |
| CreateServerScope | Creates a server scope on the DNS server. The *dwTypeId* parameter MUST be set to DNSSRV\_TYPEID\_LPWSTR. *pData* MUST point to a Unicode string that contains the name of the server scope to be created.[<230>](#Appendix_A_230) |
| DeleteServerScope | Deletes a server scope on the DNS server. The *dwTypeId* parameter MUST be set to DNSSRV\_TYPEID\_LPWSTR. *pData* MUST point to a Unicode string that contains the name of the server scope to be deleted.[<231>](#Appendix_A_231) |
| CreateClientSubnetRecord | Creates a client subnet record on a DNS server. The *dwTypeId* parameter MUST be set to DNSSRV\_TYPEID\_CLIENT\_SUBNET\_RECORD, and *pData* MUST point to a structure of type DNS\_RPC\_CLIENT\_SUBNET\_RECORD. |
| DeleteClientSubnetRecord | Deletes a client subnet record on a DNS server. The *dwTypeId* parameter MUST be set to DNSSRV\_TYPEID\_LPWSTR, and *pData* MUST point to a NULL-terminated Unicode string containing the name of the client subnet record to be deleted. |
| DeleteSubnetsInRecord | Updates a client subnet record on a DNS server by deleting the IP/IPv6 Subnets from the Client Subnet Record. The *dwTypeId* parameter MUST be set to DNSSRV\_TYPEID\_CLIENT\_SUBNET\_RECORD, and *pData* MUST point to a structure of type DNS\_RPC\_CLIENT\_SUBNET\_RECORD. |
| AddSubnetsInRecord | Updates a client subnet record on a DNS server by adding the IP/IPv6 Subnets to the Client Subnet Record. The *dwTypeId* parameter MUST be set to DNSSRV\_TYPEID\_CLIENT\_SUBNET\_RECORD, and *pData* MUST point to a structure of type DNS\_RPC\_CLIENT\_SUBNET\_RECORD. |
| ResetClientSubnetRecord | Resets a client subnet record on a DNS server by deleting the existing IP/IPv6 Subnets and adding the IP/IPv6 Subnets specific to the client subnet record. The *dwTypeId* parameter MUST be set to DNSSRV\_TYPEID\_CLIENT\_SUBNET\_RECORD, and *pData* MUST point to a structure of type DNS\_RPC\_CLIENT\_SUBNET\_RECORD. |
| CreatePolicy | Creates a DNS Policy at the server level on a DNS server. The *dwTypeId* parameter MUST be set to DNSSRV\_TYPEID\_POLICY, and *pData* MUST point to a structure of type DNS\_RPC\_POLICY. |
| DeletePolicy | Deletes a DNS Policy at the server level on a DNS server. The *dwTypeId* parameter MUST be set to DNSSRV\_TYPEID\_LPWSTR, and *pData* MUST point to NULL-terminated Unicode string containing the name of the DNS Policy. |
| UpdatePolicy | Updates a DNS Policy at the server level on a DNS Server. The *dwTypeId* parameter MUST be set to DNSSRV\_TYPEID\_POLICY, and *pData* MUST point to a structure of type DNS\_RPC\_POLICY. |

If pszZone is not NULL, and pszOperation does not match a property name listed in sections [3.1.1.2.2](#Section_d532370821694c62b1e08569a103a8be) or [3.1.1.2.3](#Section_51da10a5d508497dae49525a332d055b), then pszOperation SHOULD[<232>](#Appendix_A_232) be one of the following:

| Value | Meaning |
| --- | --- |
| ResetDwordProperty | Update the value of a DNS Zone integer property. On input dwTypeId MUST be set to DNSSRV\_TYPEID\_NAME\_AND\_PARAM and pData MUST point to a structure of type DNS\_RPC\_NAME\_AND\_PARAM (section 2.2.1.2.5), which contains the name of a property listed in section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a) for the zone pointed to by pszZone and a new value for that property.[<233>](#Appendix_A_233) |
| ZoneTypeReset | Change the zone's type, for example to convert a secondary zone into a primary zone. On input dwTypeId SHOULD be set to DNSSRV\_TYPEID\_ZONE\_CREATE, and pData SHOULD point to a structure of one of the types specified in DNS\_RPC\_ZONE\_CREATE\_INFO (section 2.2.5.2.7), which contains the new configuration information for the zone. dwTypeId MAY be set to DNSSRV\_TYPEID\_ZONE\_CREATE\_W2K or DNSSRV\_TYPEID\_ZONE\_CREATE\_DOTNET.[<234>](#Appendix_A_234) The server MUST return a nonzero error if the conversion is not implemented. |
| PauseZone | Pause activities for the zone pointed to by pszZone on the DNS server, and do not use this zone to answer queries or take updates until it is resumed. dwTypeId, and pData MUST be ignored by the server. |
| ResumeZone | Resume activities for the zone pointed to by pszZone on the DNS server; the zone thus becomes available to answer queries and take updates. dwTypeId and pData MUST be ignored by the server. |
| DeleteZone | Delete the zone pointed to by pszZone on the DNS server. dwTypeId and pData MUST be ignored by the server. |
| ReloadZone | Reloads data for the zone pointed to by pszZone on the DNS server from persistent storage. dwTypeId, and pData MUST be ignored by the server. |
| RefreshZone | Force a refresh of the secondary zone pointed to by pszZone on the DNS server, from primary zone server. For this operation pszZone MUST point to a secondary zone only. dwTypeId and pData MUST be ignored by the server. |
| ExpireZone | Force expiration of the secondary zone pointed to by pszZone on the DNS server, by invalidating the zone data locally and contacting primary to refresh. For this operation pszZone MUST point to a secondary zone only. dwTypeId, and pData MUST be ignored by the server. |
| IncrementVersion | Same as "WriteBackFile". |
| WriteBackFile | If the zone has uncommitted changes, write back all information for the zone pointed to by pszZone to persistent storage, and notify any secondary DNS servers. dwTypeId and pData MUST be ignored by the server. |
| DeleteZoneFromDs | Delete the zone pointed to by pszZone from the directory server. dwTypeId, and pData MUST be ignored by the server. |
| UpdateZoneFromDs | Refresh data for the zone pointed to by pszZone from the directory server. dwTypeId, and pData MUST be ignored by the server. |
| ZoneExport | Export zone data to a given file on the DNS server. On input dwTypeId MUST be set to DNSSRV\_TYPEID\_ZONE\_EXPORT, and pData MUST point to a structure of type DNS\_RPC\_ZONE\_EXPORT\_INFO (section [2.2.5.2.8](#Section_563518e385464d3c88c8f9b001beaa6e)) that contains a file name pointed to by pszZoneExportFile. |
| ZoneChangeDirectoryPartition | Move a zone to a given application directory partition. On input dwTypeId MUST be set to DNSSRV\_TYPEID\_ZONE\_CHANGE\_DP, and pData MUST point to structure of type DNS\_RPC\_ZONE\_CHANGE\_DP (section [2.2.7.2.6](#Section_6dc9428b7a6f4112a3dc7d250d2b06b4)), which contains the new application directory partition name pointed to by pszDestPartition. |
| DeleteNode | Delete a node. On input dwTypeId MUST be set to DNSSRV\_TYPEID\_NAME\_AND\_PARAM, and pData MUST point to a structure of type DNS\_RPC\_NAME\_AND\_PARAM (section 2.2.1.2.5), which contains the FQDN of the node pointed to by pszNodeName present in the zone pointed to by pszZone on the DNS server to be deleted and a Boolean flag in dwParam to indicate if the node's subtree is to be deleted. |
| DeleteRecordSet | Delete all the DNS records of a particular type at a particular node from the DNS server's cache. On input dwTypeId MUST be set to DNSSRV\_TYPEID\_NAME\_AND\_PARAM, and pData MUST point to a structure of type DNS\_RPC\_NAME\_AND\_PARAM (section 2.2.1.2.5). That structure contains the FQDN of the node to be deleted and the DNS record type in the dwParam member. The type MUST be a DNS\_RECORD\_TYPE value (section 2.2.2.1.1) or 0x00FF, which specifies all types. |
| ForceAgingOnNode | On input dwTypeId MUST be set to DNSSRV\_TYPEID\_NAME\_AND\_PARAM, and pData MUST point to a structure of type DNS\_RPC\_NAME\_AND\_PARAM (section 2.2.1.2.5), which contains a node name in pszNodeName, and a Boolean flag in dwParam to indicate whether aging is performed on all nodes in the subtree. All DNS records at the specified node in the zone named by pszZone will have their aging time stamp set to the current time. If subtree aging is specified by dwParam than all DNS records at all nodes that are children of this node will also have their aging time stamps set to the current time. |
| DatabaseFile | On input dwTypeId SHOULD be set to DNSSRV\_TYPEID\_ZONE\_DATABASE[<235>](#Appendix_A_235), and pData MUST point to a structure of one of the types specified in DNS\_RPC\_ZONE\_DATABASE (section [2.2.5.2.6](#Section_fc8b181af8b84953992e8102008d23cd)), which specifies whether the zone is directory server integrated by setting fDsIntegrated to TRUE, and if it is not then pszFileName MUST point to a Unicode string containing the absolute pathname of a file on the DNS server to which the zone database is stored. |
| MasterServers | On input dwTypeId MUST be set to DNSSRV\_TYPEID\_IPARRAY or DNSSRV\_TYPEID\_ADDRARRAY, and pData MUST point to a structure of type IP4\_ARRAY (section 2.2.3.2.1) or DNS\_ADDR\_ARRAY (section 2.2.3.2.3) respectively, which contains a list of IP addresses of new primary DNS servers for the zone pointed to by pszZone. This operation is valid only for secondary zones present on the server. The server SHOULD accept DNSSRV\_TYPEID\_ADDRARRAY and DNS\_ADDR\_ARRAY, and SHOULD accept DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY. If the input data of either type is accepted and the DNS server is directory-server integrated, the value of *pData* SHOULD be written to the directory server.[<236>](#Appendix_A_236) |
| LocalMasterServers | On input dwTypeId MUST be set to DNSSRV\_TYPEID\_IPARRAY or DNSSRV\_TYPEID\_ADDRARRAY, and pData MUST point to a structure of type IP4\_ARRAY (section 2.2.3.2.1) or DNS\_ADDR\_ARRAY (section 2.2.3.2.3) respectively, which contains a list of IP addresses of new local primary DNS servers for the zone pointed to by pszZone. This operation is valid only for stub zones present on the server, and if configured, this value overrides any primary DNS server configured in the directory server. The server SHOULD accept DNSSRV\_TYPEID\_ADDRARRAY and DNS\_ADDR\_ARRAY, and SHOULD accept DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY.[<237>](#Appendix_A_237) |
| SecondaryServers | On input dwTypeId SHOULD[<238>](#Appendix_A_238) be set to DNSSRV\_TYPEID\_ZONE\_SECONDARIES, and pData MUST point to a structure of one of the types specified in DNS\_RPC\_ZONE\_SECONDARIES (section [2.2.5.2.5](#Section_2e5897350d8943c4a463212857482882)), which contains information about secondary DNS servers for the zone pointed to by pszZone. |
| ScavengeServers | On input dwTypeId MUST be set to DNSSRV\_TYPEID\_IPARRAY or DNSSRV\_TYPEID\_ADDRARRAY, and pData MUST point to a structure of type IP4\_ARRAY (section 2.2.3.2.1) or DNS\_ADDR\_ARRAY (section 2.2.3.2.3) respectively, which contains a list of IP addresses of new servers that can run scavenging on the zone pointed to by pszZone. This operation is valid only for directory server integrated zones. The server SHOULD accept DNSSRV\_TYPEID\_ADDRARRAY, and DNS\_ADDR\_ARRAY, and SHOULD accept DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY. If the input data of either type is accepted and the DNS server is directory server-integrated, the value of *pData* SHOULD be written to the directory server.[<239>](#Appendix_A_239) |
| AllowNSRecordsAutoCreation | On input dwTypeId MUST be set to DNSSRV\_TYPEID\_IPARRAY or DNSSRV\_TYPEID\_ADDRARRAY and pData MUST point to a structure of type IP4\_ARRAY (section 2.2.3.2.1) or DNS\_ADDR\_ARRAY (section 2.2.3.2.3) respectively, which contains a list of IP addresses of new servers that can auto-create NS records for the zone pointed to by pszZone. This operation is valid only for directory server integrated zones. The server SHOULD accept DNSSRV\_TYPEID\_ADDRARRAY and DNS\_ADDR\_ARRAY, and SHOULD accept DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY. If the input data of either type is accepted and the DNS server is directory server-integrated, the value of *pData* SHOULD be written to the directory server.[<240>](#Appendix_A_240) |
| BreakOnNameUpdate | On input dwTypeId MUST be set to DNSSRV\_TYPEID\_LPWSTR, and pData MUST point to a Unicode string that contains the FQDN of the node for which if an update is received the DNS server will execute a breakpoint. |
| SignZone | Sign a zone using DNSSEC, thus making the zone online-signed. The dwTypeId and pData parameters MUST be set to zero/NULL by the client and MUST be ignored by the server. |
| UnsignZone | Unsign a zone signed via online signing and remove all DNSSEC data from the zone. The dwTypeId and pData parameters MUST be set to zero/NULL by the client and MUST be ignored by the server. |
| ResignZone | Refreshes all DNSSEC data in an online-signed zone. The dwTypeId and pData parameters MUST be set to zero/NULL by the client and MUST be ignored by the server. |
| PerformZoneKeyRollover | Queues a signing key descriptor for key rollover. On input, dwTypeId MUST be set to DNSSRV\_TYPEID\_LPWSTR, and pData MUST point to a Unicode string representation of the GUID of the signing key descriptor to be queued for rollover. |
| PokeZoneKeyRollover | Instructs the DNS server to stop waiting for DS records [[RFC4034]](http://go.microsoft.com/fwlink/?LinkId=107052) in the parent zone to be updated and to proceed with key rollover as specified by [[RFC4641]](http://go.microsoft.com/fwlink/?LinkId=225979). On input, dwTypeId MUST be set to DNSSRV\_TYPEID\_LPWSTR, and pData MUST point to a Unicode string representation of the GUID of the signing key descriptor to be queued for rollover. |
| RetrieveRootTrustAnchors | Retrieves the root trust anchors from the XML file specified by the RootTrustAnchorsURL server property (section 3.1.1.1.3) and adds any valid DS records to the root trust anchors. The dwTypeId and pData parameters MUST be set to zero/NULL by the client and MUST be ignored by the server. The pZone parameter MUST be set to "TrustAnchors". |
| TransferKeymasterRole | Transfers the key master role to the current server. The dwTypeId parameter MUST be set to DNSSRV\_TYPEID\_DWORD, and pData MUST point to one of the values defined in the following paragraphs. |
| CreateZoneScope | Creates a zone scope in the specified zone or a cache scope in the specified cache zone. The dwTypeId parameter MUST be set to DNSSRV\_TYPEID\_ZONE\_SCOPE\_CREATE. pData MUST point to a structure of the type [DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1 (section 2.2.13.2.2.1)](#Section_cbe779f029b94a6199fba1d9115d590f) that contains all the parameters needed to create the zone scope or cache scope. pszZone MUST be the name of the zone in which the zone scope is to be created or be specified as "..cache" for a cache scope.[<241>](#Appendix_A_241) |
| DeleteZoneScope | Deletes a zone scope from the specified zone or a cache scope from a specified cache zone. The dwTypeId MUST be set to DNSSRV\_TYPEID\_LPWSTR. pData MUST point to the name of the zone scope or cache scope that is to be deleted. pszZone MUST be the name of the zone from which the zone scope is to be deleted or set to "..cache" for a cache scope.[<242>](#Appendix_A_242) |
| CreatePolicy | Creates a DNS Policy for the specified zone or a cache zone on a DNS server. The dwTypeId parameter MUST be set to DNSSRV\_TYPEID\_POLICY, and pData MUST point to a structure of type DNS\_RPC\_POLICY. |
| DeletePolicy | Deletes a DNS Policy for the specified zone or a cache zone on a DNS server. The dwTypeId parameter MUST be set to DNSSRV\_TYPEID\_LPWSTR, and pData MUST point to NULL-terminated Unicode string containing the name of the DNS Policy. |
| UpdatePolicy | Updates a DNS Policy for the specified zone or a cache zone on a DNS server. The dwTypeId parameter MUST be set to DNSSRV\_TYPEID\_POLICY, and pData MUST point to a structure of type DNS\_RPC\_POLICY. |

**dwTypeId:** A DNS\_RPC\_TYPEID (section 2.2.1.1.1) value that indicates the type of input data pointed to by pData.

**pData:** Input data of type DNSSRV\_RPC\_UNION (section [2.2.1.2.6](#Section_b61a872746b14981a6b3a1d4b92b67c4)), which contains a data structure as specified by dwTypeId.

**Return Values:** The method MUST return ERROR\_SUCCESS (0x00000000) on success or a nonzero Win32 error code value if an error occurred. All error values MUST be treated the same.

When processing this call, the server MUST do the following:

* If the Global Server State (section [3.1](#Section_bdac51424baf4b62bcced49eafc9c3e6)) is not "Running", return a failure.
* Check that the input parameters conform to the syntax requirements above, and if not, return a failure.
* If pszZone is not NULL, search the DNS Zone Table (section 3.1) record for the zone with a name matching the value of pszZone. If a matching zone cannot be found, search the list of multizone operation strings for a name matching the value of pszZone. If a matching name cannot be found, return a failure.
* Validate, as specified in section [3.1.6.1](#Section_7ba0801d74f1499e81a300231ef31952), that the client has permissions to perform the attempted operation. If pszZone is NULL then the DNS server MUST perform the Phase 2 authorization test using the DNS Server Configuration Access Control List. If pszZone is not NULL then the DNS server MUST perform the Phase 2 authorization test using the Zone Access Control List for the zone specified by pszZone. Write privilege MUST be tested for all operations with the following exceptions:
  + If pszOperation is ZoneCreate, and if the zone will be created in the directory service, then Read privilege MUST be tested for.
  + If pszOperation is DeleteZone, and if the zone is stored in the directory service, then Read privilege MUST be tested for.
  + If pszOperation is EnlistDirectoryPartition or ExportSettings, then Read privilege MUST be tested for.
* If the client does not have permission to perform the operation, return a failure.
* If dwContext is not zero or pszZone matches a multizone operation string, then find all zone records in the DNS Zone Table matching the specified multizone filter value.
* If pszZone is NULL and dwContext is zero, execute the operation indicated by the value of pszOperation, as follows:
  + If pszOperation is **ResetDwordProperty**, the server MUST verify that the property name matches a writable property name listed in section 3.1.1.1.1 for which the server supports the "ResetDwordProperty" operation and if not return an error. It SHOULD further verify that the value specified is either within the property's specified allowable range (including zero if it is specified that zero is allowed) and if not return an error. If the value is zero and zero is listed as a flag value for the default in section 3.1.1.1.1, the server SHOULD update the value of the property to be the default for the property and return success. The server MAY fail to verify these restrictions.[<243>](#Appendix_A_243) Otherwise, update the value of the property to be the new value specified and return success.[<244>](#Appendix_A_244) All properties are writable unless "this property is read-only" is specified in the property description in section 3.1.1.1.1.
  + If *pszOperation* matches a property name in section 3.1.1.1.2, 3.1.1.1.3, or 3.1.1.1.4 for which the server supports this value reset operation, the server MUST update the value of the property to be the new value specified in pData and return success. If *pszOperation* matches a property name that the server does not support, the server MUST simply return failure.[<245>](#Appendix_A_245)
  + If pszOperation is Restart, the server MUST restart the DNS server, and return success.
  + During the restart operation, the DNS server MUST try to reload each zone scope (if present) in a zone, one by one from the database. If the DNS server fails to load any of the scopes of the zone, it MAY log an error event and pursue the next scope and subsequently next zone.[<246>](#Appendix_A_246) No error MUST be returned to the user in the event of failure.
  + If pszOperation is ClearDebugLog, the server MUST copy the DNS log file specified by the DNS server's "LogFilePath" (section 3.1.1.1.3) property to the implementation-specific backup directory, if the directory already exists, and overwrite an existing backup directory log file if needed. If the directory does not exist, the copy action MUST NOT be performed. Then, the server MUST delete the current contents of the DNS log file, and return success. The server MUST return success even if file operations on the DNS log file fail.[<247>](#Appendix_A_247)
  + If pszOperation is ClearCache, the server MUST delete all records cached by the DNS server in the cache zone from memory. If a cache scope is specified, delete all records only from that cache scope. If the server is configured to use directory server, the server MUST search for the cache zone (with the LDAP search operation), create (LDAP add) the zone if it doesn't exist, load (LDAP search) any default cache records into the local copy of the cache, and return success. If any of these LDAP operations fails, the server MUST return failure.
  + If pszOperation is WriteDirtyZones, the server MUST, for each primary zone or cache zone on the server:
    - Do nothing, if the zone's **Dirty Flag** (section 3.1.1) is set to FALSE and the zone is not configured with any zone scopes or the zone is not stored in a file.
    - If the zone's **Dirty Flag** is set to TRUE, write the uncommitted information for the zone to the zone's file, send DNS notify ([[RFC1996]](http://go.microsoft.com/fwlink/?LinkId=106957)) messages to all other servers hosting the zones, if they exist, and continue processing zones. If the zone specified is the cache zone, the server SHOULD write the root hints to their permanent storage. If the root hints are stored on the directory server and DownlevelDCsInDomain is nonzero, the server MUST check whether the root hints are empty. If the root hints are empty, the root hints MUST NOT be written to their permanent storage. Otherwise, if the root hints are stored on the directory server the server MUST use LDAP add, delete, and search operations to replace the root hints on the directory server. If there is a failure in writing the root hints records to the directory server, then the server MUST retry the write operation twice.
    - If the zone is configured with scopes, then for each scope the operation attempts to write the scope data to their respective scope database files, if the scope’s **Dirty Flag** (section 3.1.1) is set to TRUE. If any errors occur during this operation, then the operation SHOULD be continued with the next scope in the list and the appropriate error events SHOULD be logged.
    - When all zones have been processed, the server SHOULD return success, regardless of the success or failure of any processing operation.[<248>](#Appendix_A_248)
  + If pszOperation is ZoneCreate, the server MUST attempt to create a new zone entry in the DNS Zone Table using the parameters specified in pData, and return success or failure based on the result.
    - If the zone already exists, the server MUST return a failure.
    - If the zone to be created will use the directory server for persistent storage, the server MUST identify the correct application directory partition for the zone.
      * If dwFlags has the DNS\_ZONE\_CREATE\_FOR\_DCPROMO bit set, this partition MUST be the DNS domain application directory partition.
      * If dwFlags has the DNS\_ZONE\_CREATE\_FOR\_DCPROMO\_FOREST bit set, this partition MUST be the DNS forest application directory partition.
      * Otherwise, if the pszDpFqdn field is populated, this partition MUST be set to the value of that field.
      * Or else, this partition MUST be set to the directory partition that represents the default naming context. (See the description of the DNS\_DP\_LEGACY value in section 3.1.1.2.1).[<249>](#Appendix_A_249)
    - The server MUST perform an LDAP search to verify the existence of this application directory partition, and return a failure if it does not exist, with the following exceptions:
      * If dwFlags is set to DNS\_ZONE\_CREATE\_FOR\_DCPROMO and the DNS domain application directory partition does not exist or is not available, the server MUST replace the chosen partition with the directory partition that represents the default naming context.
      * If dwFlags is set to DNS\_ZONE\_CREATE\_FOR\_DCPROMO\_FOREST and the DNS forest application directory partition does not exist or is not available, the server MUST replace the chosen partition with the directory partition that represents the default naming context.
    - Once the existence of the chosen application directory partition has been verified, the server MUST then perform an LDAP search on that application directory partition to determine whether the zone already exists, and if so, return a failure.
    - If the zone does not exist in the chosen application directory partition, the server MUST create a "dnsZone" object (section [2.3](#Section_74db40e109174ecb863d9bce5165ebf3)) for the zone and its default records, represented as "dnsNode" objects (section 2.3), in the chosen application directory partition using LDAP add operations and return success.
      * If dwFlags is set to DNS\_ZONE\_CREATE\_FOR\_DCPROMO, but the zone is being created in the directory partition representing the default naming context, the "DcPromo Flag" in the "dnsZone" object MUST be set to DCPROMO\_CONVERT\_DOMAIN. (See DcPromo Flag (section [2.3.2.1.2](#Section_4ec7bdf71807417996afce1c1cd448b7)))
      * If dwFlags is set to DNS\_ZONE\_CREATE\_FOR\_DCPROMO\_FOREST, but the zone is being created in the directory partition representing the default naming context, the "DcPromo Flag" in the "dnsZone" object MUST be set to DCPROMO\_CONVERT\_FOREST. (See DcPromo Flag (section 2.3.2.1.2))
    - If there is a failure in writing the records to the directory server, then the server MUST retry the write operation twice.
    - If any of these LDAP operations cannot be completed, even after retries where specified, then the server MUST return failure.
  + If pszOperation is ClearStatistics, the server MUST clear internal server statistics, and return success.
  + If pszOperation is EnlistDirectoryPartition, the server SHOULD[<250>](#Appendix_A_250) perform an application directory partition operation as specified by the contents of the input DNS\_RPC\_ENLIST\_DP (section 2.2.7.2.5) structure. The procedures for these operations are described below:
    - If pszOperation is EnlistDirectoryPartition, and the DNS\_DP\_OP\_CREATE\_FOREST or DNS\_DP\_OP\_CREATE\_DOMAIN operations are specified by the contents of the input DNS\_RPC\_ENLIST\_DP structure, the server SHOULD:
      * Check its local state to determine whether the partition specified by dwOperation is already present, and if so, the server MUST check its local state to determine whether it is not enlisted in the partition, and if so, connect to the directory server that is the FSMO role owner of the domain naming master FSMO role and perform an LDAP modify operation to add or remove the local server's name from the enlistment list (distinguished name "msDS-NC-Replica-Locations" RODCs use "msDS-NC-RO-Replica-Locations").[<251>](#Appendix_A_251). If, based on the local state, the partition already exists and this server is enlisted or any of the above LDAP operations cannot be completed, then the server MUST return a failure.
      * Or, if based on the server's local state, the partition does not exist in the Application Directory Partition Table, create (but not enlist itself in) the partition object using LDAP add commands and add the partition object to the Application Directory Partition Table, returning a failure if either of these operations fails to complete successfully.
      * Poll the directory server for the partitions and enlistment status using LDAP search operations (to update the local state) and return success. If any LDAP operation cannot be completed, then the server MUST return a failure.
    - If pszOperation is EnlistDirectoryPartition, and the DNS\_DP\_OP\_ENLIST or DNS\_DP\_OP\_UNENLIST operations are specified by the contents of the input DNS\_RPC\_ENLIST\_DP structure, the server SHOULD:
      * Check whether the application directory partition specified is either the domain global partition or the forest global partition and whether the operation specified is not DNS\_DP\_OP\_ENLIST, and if the preceding conditions are true, the server MUST return a failure.
      * Check whether, instead, the operation specified is DNS\_DP\_OP\_ENLIST and the partition specified is the domain or forest global partition, and if so, the server MUST connect to the directory server that is the FSMO role owner of the Domain naming master FSMO role and perform an LDAP modify operation to add or remove the local server's name from the enlistment list (distinguished name "msDS-NC-Replica-Locations" (RODCs use "msDS-NC-RO-Replica-Locations"[<252>](#Appendix_A_252))) and return success.
      * Check whether the application directory partition specified is neither the domain global partition nor the forest global partition, and if so, the server MUST:
        + Poll the directory server for the partitions and enlistment status using LDAP search operations (to update the local Application Directory Partition Table), and then:
        + Check the local Application Directory Partition Table for the requested partition, and if the partition does not exist, return a failure.
        + Otherwise, the server MUST check whether the server is already enlisted and the operation is DNS\_DP\_OP\_ENLIST or the server is already unenlisted and the operation is DNS\_DO\_OP\_UNENLIST, and if so, return a failure.
        + Otherwise, the server MUST connect to the directory server that is the FSMO role owner of the Domain naming master FSMO role, and perform an LDAP modify operation to add or remove (for DNS\_DP\_OP\_ENLIST and DNS\_DP\_OP\_UNENLIST, respectively) the local server's name from the enlistment list (distinguished name "msDS-NC-Replica-Locations" (RODCs use "msDS-NC-RO-Replica-Locations")), and return success.
        + If any of the above LDAP operations cannot be completed, then the server MUST return a failure.

If the zone was successfully loaded then the DNS server MUST set the zone's Shutdown flag to zero (section [2.2.5.2.2](#Section_015f97afba5048bbaf444a542f3ff44a)).

* + - If pszOperation is EnlistDirectoryPartition, and the DNS\_DP\_OP\_CREATE operation is specified by the contents of the input DNS\_RPC\_ENLIST\_DP structure, the server SHOULD:
      * Check whether the application directory partition specified is either the domain global partition or the forest global partition, and if so, perform the procedure described above for DNS\_DP\_OP\_CREATE\_DOMAIN or DNS\_DP\_OP\_CREATE\_FOREST, respectively.
      * Otherwise, poll the directory server for the partitions and enlistment status using LDAP search operations (to update the local Application Directory Partition Table), and then check the local Application Directory Partition Table for the requested partition. If the partition already exists, the server MUST return a failure.
      * Otherwise, the server MUST connect to the directory server and create the partition (an LDAP "domainDNS" object) using the LDAP add operation, poll the directory server for the partitions and enlistment status, update the local Application Directory Partition Table, attempt to create the "MicrosoftDNS" object using LDAP add operations, and return success.
      * If any of the above LDAP operations other than the creation of the "MicrosoftDNS" object cannot be completed, then the server MUST return a failure.
    - If pszOperation is EnlistDirectoryPartition, and the DNS\_DP\_OP\_DELETE operation is specified by the contents of the input DNS\_RPC\_ENLIST\_DP structure, the server SHOULD:
      * Poll the directory server for the partitions and enlistment status using LDAP search operations (to update the local Application Directory Partition Table), and then check the local Application Directory Partition Table for the requested partition. If the partition does not exist, the server MUST return a failure.
      * Otherwise, the server MUST connect to the directory server that is the FSMO role owner of the Domain naming master FSMO role and perform an LDAP delete operation on the distinguished name of the crossRef object of the specified application directory partition, and if successful, again poll the directory server to update the local Application Directory Partition Table and return success.
      * If any of the above LDAP operations fails, then the server MUST return a failure. Any LDAP delete operation MUST have no client-side time limit. The server MUST NOT retry any failed LDAP operation.
  + If pszOperation is StartScavenging, the server MUST initiate a resource record scavenging cycle on the DNS server, and return success.
  + If pszOperation is AbortScavenging, the server MUST terminate a resource record scavenging cycle on the DNS server if one is currently in progress, and return success.
  + If pszOperation is AutoConfigure, the server SHOULD perform DNS server autoconfiguration as specified by the contents of the input DNS\_RPC\_AUTOCONFIGURE (section 2.2.8.2.1) structure, and return success or failure based on the results of this operation.[<253>](#Appendix_A_253) To perform DNS server autoconfiguration, the server SHOULD:
    - Configure forwarders, if specified by the input flags and if the server does not currently have any forwarders configured. The list of forwarders is built by querying other servers that host the domain specified in the input arguments and by attempting to copy their [**forwarder**](#gt_001ff1c1-e24f-4766-a5b1-a5802871054f) list using the "ServerInfo" feature of the [R\_DnssrvQuery (section 3.1.4.2)](#Section_b0419a70ac0b40baab941510992bc574) operation. If forwarders cannot be copied from another server, the list of forwarders is copied from the local machine's DNS client's list of DNS servers.
    - Configure root hints, if specified by the input flags. The list of root hints is built by querying the each DNS server on each local network adapter for the root DNS name.
    - Perform self-pointing, if either of the following is true:
      * The DNS server is directory services-integrated and is the first DNS server in the directory services forest, and the DNS\_RPC\_AUTOCONFIG\_INTERNAL\_ZONES flag is set.
      * Any of the DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT, DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_PREPEND, or DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_APPEND flags are set.
    - To perform self-pointing, for each enabled network adapter and for each enabled IP stack (IPv4 or IPv6) on that adapter, the server SHOULD do one of the following:
      * If the DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT flag is set, replace the adapter's IP stack's DNS servers list with the loopback address.
      * If the DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_PREPEND flag is set and the loopback address is not already present, insert the loopback address at the start of the adapter's IP stack's DNS server list.
      * Otherwise, if the loopback address is not already present, insert the loopback address at the end of the adapter's IP stack's DNS server list.
      * Otherwise, make no change to the adapter's IP stack's DNS server list.
    - Create the forest root domain and its "\_msdcs" subdomain, if specified by the input flags, and the directory service domain name of this DNS server matches the directory services forest root domain name, and the domains do not already exist. These two domains are created using LDAP add operations, followed by additional LDAP add operations to install the default records for those domains. If there is a failure in writing the records to the directory server, then the server MUST retry the write operation twice.

If any operation (including LDAP operations) fails, continue processing but record the fact that a failure occurred. At the end of processing, if the DNS\_RPC\_AUTOCONFIG\_INTERNAL\_RETURN\_ERRORS input flag is set, return an error; otherwise, return success.

* + If pszOperation is ExportSettings, the server SHOULD[<254>](#Appendix_A_254) export DNS settings to a file on the DNS server, and return success.
  + If pszOperation is PrepareForDemotion, the server SHOULD[<255>](#Appendix_A_255) prepare the DNS server for demotion by removing references to this DNS server from all zones stored in the directory server, and return success.
  + If pszOperation is PrepareForUninstall, the server SHOULD[<256>](#Appendix_A_256) do nothing, and return success.
  + If pszOperation is DeleteNode, the server MUST check whether the specified node is empty or does not currently exist and return ERROR\_SUCCESS if so. Otherwise it MUST delete all DNS records at the node pointed to by pszNodeName from the DNS server's cache. It MUST also delete all DNS records in the node's subtree if specified by the Boolean flag pointed to by dwParam field in pData, and return success. If the dwParam field in pData is set to FALSE and the node contains subtrees, both the node and its subtrees MUST NOT be deleted and a success status is returned. If the zone is directory server-integrated, the DNS server MUST set the node's DNS Node Tombstone State (section 3.1.1) to TRUE by setting the value of the dnsTombstoned attribute to ,TRUE, and writing a DNS\_RPC\_RECORD\_TS (section [2.2.2.2.4.23](#Section_def7736add094b4ab8d66a702a7ecde0)) in the **dnsRecord** attribute.
  + If pszOperation is DeleteRecordSet, the server MUST check whether the specified node is empty or does not currently exist and return ERROR\_SUCCESS if so. Otherwise it MUST delete all DNS records of the type specified by the dwParam field in pData from the node pointed to by pszNodeName in the DNS server's cache and return success. If this operation deletes the last record from the node and the zone is directory server-integrated, the DNS server MUST set the node's DNS Node Tombstone State (section 3.1.1) to TRUE by setting the value of the dnsTombstoned attribute to TRUE and writing a DNS\_RPC\_RECORD\_TS (section 2.2.2.2.4.23) in the **dnsRecord** attribute.
  + If pszOperation is WriteBackFile, the server SHOULD write the root hints to their permanent storage. If the root hints are stored on the directory server and DownlevelDCsInDomain is nonzero, the server MUST check whether the root hints are empty. If the root hints are empty, the root hints MUST NOT be written to their permanent storage. Otherwise, if the root hints are stored on the directory server, the server MUST use LDAP add, delete, and search operations to replace the root hints on the directory server and return success, regardless of the success or failure of these operations. If there is a failure in writing the root hints records to the directory server, then the server MUST retry the write operation twice, and still return success, even if the retries fail.[<257>](#Appendix_A_257)
  + If pszOperation is LogFilePath, the server MUST store the value passed in pData to be returned, unchanged, in future server information queries. Further, if pData is a NULL pointer or it points to an empty string, the server MUST replace pData's present value with the path to the default implementation specific log file. Finally, the server MUST attempt to create and/or open for write the file specified by the string. If the string is a filename or relative path, the server MUST attempt to create the file relative to the default implementation specific log file path.[<258>](#Appendix_A_258) If the file is opened successfully, then the server MUST commence logging to file and return success. Otherwise, it MUST disable logging to file and return a failure.
  + If pszOperation is ListenAddresses, the server MUST search the incoming array for loopback, multicast, or broadcast addresses, and if any are found, return a failure. Otherwise, the server MUST remove any addresses from the input that are not IPv4 addresses and create a backup copy of the current listen addresses. Then the server MUST attempt to listen on the network interfaces specified by the new listen addresses from the incoming array, and if this attempt fails, the server MUST restore the previous listen addresses and return a failure. Otherwise, the server MUST attempt to update the SOA records for its authoritative zones with the new listen addresses and MUST return success even if the attempt fails. If a zone is directory services-integrated, the server MUST use the LDAP search, add, and delete operations to update the SOA records and return success even if there were unsuccessful LDAP calls. If there is a failure in modifying the records on the directory server, then the server MUST retry the write operation twice, and still return success even if the retries fail.
  + If pszOperation is ServerLevelPluginDll, the server MUST store the value passed in pData and return SUCCESS, indicating only that the value was successfully received. The server MUST NOT validate the value passed, nor attempt to load the DLL, until the server is restarted. When the server restarts, if the value stored for ServerLevelPluginDll is not an empty string, the server MUST attempt to load the DLL specified. If the DLL fails to load for any reason, the server MUST fail to start. If the DLL has been loaded, then whenever the server is required to invoke the DLL query function, the server MUST invoke the query function of the DLL with a query name and type and add any resulting records to the server's cache. Whenever the server processes a query, if the DLL has been loaded, the server MUST invoke the query function of the DLL in the following conditions:
    - If a query cannot be answered with the information already present in the server's zone database and cache, then prior to recursing (if applicable), invoke the DLL query function and try again to answer the query from local data.
    - If a response SHOULD have records in its additional section but no such records are in the server's cache or zone database, invoke the DLL query function and attempt again to find records for the additional section.
  + If pszOperation is ActiveRefreshAllTrustPoints, the server MUST schedule an RFC 5011 active refresh for all configured trust points (if any) and return success.
  + If pszOperation is DeleteServerScope, the server MUST:
    - If the server scope specified in pData does not exist, return DNS\_ERROR\_SCOPE\_DOES\_NOT\_EXIST.
    - If the server scope is being used by a DNS Policy (section [2.2.15.2.2](#Section_dd2e4ce56eea4dc4b9f7058eb9703381)), return DNS\_ERROR\_SERVERSCOPE\_IS\_REFERENCED.
    - The DNS server MUST attempt to delete the server scope in the DNS server, and return success or failure based on the result.
  + If pszOperation is CreateClientSubnetRecord, the server MUST:
    - If the Client Subnet Record already exists, return DNS\_ERROR\_CLIENT\_SUBNET\_DOES\_EXIST.
    - The DNS server MUST attempt to create a new Client Subnet Record entry in the DNS server using the parameters specified in pData, and return success or failure based on the result.
  + If pszOperation is DeleteClientSubnetRecord, the server MUST:
    - If the Client Subnet Record specified in pData does not exist, return DNS\_ERROR\_CLIENT\_SUBNET\_DOES\_NOT\_EXIST.
    - If the Client Subnet Record is being used by a DNS Policy in its Client Subnet Record criteria, then the DNS server MUST return DNS\_ERROR\_CLIENT\_SUBNET\_IS\_ACCESSED.
    - The DNS server MUST attempt to delete the Client Subnet Record entry in the DNS server, and return success or failure based on the result.
  + If pszOperation is DeleteSubnetsInRecord, the server MUST:
    - If the Client Subnet Record specified in pData does not exist, return DNS\_ERROR\_CLIENT\_SUBNET\_DOES\_NOT\_EXIST.
    - If the IP/IPv6 Subnets specified in pData do not exist in the Client Subnet Record on the DNS server, return DNS\_ERROR\_SUBNET\_DOES\_NOT\_EXIST.
    - If deletion of the IP/IPv6 subnets results in the Client Subnet Record not having an IP or IPv6 subnet, return DNS\_ERROR\_ADDRESS\_REQUIRED.
    - The DNS server MUST attempt to delete the IP/IPv6 Subnets in the Client Subnet Record on the DNS server, and return success or failure based on the result.
  + If pszOperation is AddSubnetsInRecord, the server MUST:
    - If the Client Subnet Record specified in pData does not exist, return DNS\_ERROR\_CLIENT\_SUBNET\_DOES\_NOT\_EXIST.
    - If the IP/IPv6 Subnets specified in pData exists in the Client Subnet Record on the DNS server, return DNS\_ERROR\_SUBNET\_DOES\_EXIST.
    - The DNS server MUST attempt to add the IP/IPv6 Subnets in the Client Subnet Record on the DNS server, and return success or failure based on the result.
  + If pszOperation is ResetClientSubnetRecord, the server MUST:
    - If the Client Subnet Record specified in pData does not exist, return DNS\_ERROR\_CLIENT\_SUBNET\_DOES\_NOT\_EXIST.
    - If no IP or IPv6 subnets are specified, return DNS\_ERROR\_ADDRESS\_REQUIRED.
    - The DNS server MUST delete the existing IP/IPv6 Subnets in the Client Subnet Record and add the IP/IPv6 Subnets specified in pData in the Client Subnet Record on the DNS server, and return success or failure based on the result.
  + If pszOperation is CreatePolicy, the server MUST:
    - The DNS server validates whether the DNS Policy parameters specified in pData are valid. If the parameters are invalid the server returns DNS\_ERROR\_POLICY\_INVALID\_SETTINGS. See DNS Policy Validation (section [3.1.8.3](#Section_43a6fc0b785a43bb91d3b5a4f366fdf5)) for details.
    - If the DNS Policy pdata parameter dwProcessingOrder is greater than the highest Processing Order in the given level and appliesOn, return DNS\_ERROR\_POLICY\_INVALID\_SETTINGS.
    - If the DNS Policy pdata parameter pwszPolicyName already exists, return DNS\_ERROR\_POLICY\_ALREADY\_EXISTS. The policy name check is done for the policies configured on the server level.
    - If the value weight in pContentList is 0 (as explained in DNS\_RPC\_POLICY\_CONTENT (section 2.2.15.2.2)) then the DNS server returns DNS\_ERROR\_POLICY\_INVALID\_WEIGHT. Allowed values for weight are any positive number from 1 to 0xffffffff.
    - If DNS Policy pdata parameter dwProcessingOrder is 0 then reset the processing order to the last processing order for the given level and appliesOn.
    - Create the new DNS Policy in the DNS server, and return success or failure based on the result. This DNS Policy is applicable to the DNS Operations at the server level.
    - If DNS Policy pdata parameter dwProcessingOrder is same as an existing DNS Policy in the given level and appliesOn, update this new policy to have this new processing order and increment all DNS Policies whose processing order is equal to or greater than this processing order by 1.
  + If pszOperation is DeletePolicy, the server MUST:
    - If the DNS Policy name specified in pData does not exist in the DNS server, return DNS\_ERROR\_POLICY\_DOES\_NOT\_EXIST.
    - Delete the DNS Policy in the DNS server, and return success or failure based on the result.
    - Reset the processing order of all policies whose processing order is greater than the processing order of the deleted policy by 1 for the given level and appliesOn.
  + If pszOperation is UpdatePolicy, the server MUST:
    - If the DNS Policy name specified in the pwszPolicyName of pData does not exist in the server level policies of the DNS server, return DNS\_ERROR\_POLICY\_DOES\_NOT\_EXIST.
    - If the flags member of DNS\_RPC\_POLICY has DNS\_RPC\_FLAG\_POLICY\_PROCESSING\_ORDER set, the processing order of the DNS policy is changed to the new processing order given in input pData. The processing order of other DNS Policies at the server level for the given appliesOn is adjusted accordingly.
    - If the flags member of DNS\_RPC\_POLICY has DNS\_RPC\_FLAG\_POLICY\_CONDITION set then the Condition of the DNS Policy is changed to the condition specified in the input pData.
    - If the flags member of DNS\_RPC\_POLICY has DNS\_RPC\_FLAG\_POLICY\_CONTENT set then the content of the DNS Policy is changed to the content specified in pData.
    - If any criteria flags specified in Criteria Constants are set, criteria values are removed from the DNS Policy and new criteria values specified in pData are set.
    - Delete the DNS Policy on the DNS server, and return success or failure based on the result.

If pszZone is not NULL and is not a valid multizone operation string, then the server MUST return a failure if it does not contain a zone with the name matching the string pointed to by pszZone. If pszZone is not NULL or if the value of dwContext specifies a multizone operation, the server MUST execute the operation indicated by the value of pszOperation individually for each zone specified by the values of dwContext and pszZone. If a zone operation is performed with a filter in dwContext or a multizone operation string in pszZone, and no zones match the specified filter or satisfy the multi-zone operation string, the server MUST return ERROR\_SUCCESS (0x00000000). If the operation is executed for more than one zone, then for each matching zone, the specified operation MUST be executed with pszZone replaced with the name of the matching zone. If any of these multiple operations return an error, the server MUST return an error; otherwise, the server MUST return success. For any operation, if the specified zone is marked as "AutoCreated", the DNS server MUST return an error.

* + If pszOperation is ResetDwordProperty, the server MUST verify that the property name matches a property name listed in section 3.1.1.2.1 for which the server supports the "ResetDwordProperty" operation, and if not return an error. If the property is specified as "read-only" in section 3.1.1.2.1, the server MUST return an error. If the zone specified is a cache zone, the server MUST return an error. It MUST further verify that the value specified is within the property's allowable range (if specified) and if not return an error. When the property specified is Boolean and the value to be set is greater than 0x00000001, the server MUST replace the value with 0x00000001. If the property name is "AllowUpdate", the server MUST return an error when the zone specified is not Active Directory-integrated and the requested value is ZONE\_UPDATE\_SECURE, or when the zone specified is not a primary zone. If the property name is "AllowUpdate" and the value is not ZONE\_UPDATE\_OFF (section [2.2.6.1.1](#Section_d4b84209f00c478f80d78dd0f1633d9e)), then the server SHOULD invoke the **NetlogonControl2Ex** method with function code **NETLOGON\_CONTROL\_FORCE\_DNS\_REG** on the "Netlogon" protocol implementation on the [**local domain controller (DC)**](#gt_55fcb1d4-6bd8-4bfc-9c58-86a9fb71120f). (See [[MS-NRPC]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-NRPC%5d.pdf) section 3.5.4.9.1.)[<259>](#Appendix_A_259) If the property name is "Aging", the property value is TRUE, and the zone's Aging state is FALSE, then the server MUST reset the zone's Aging time by updating the dwAvailForScavengeTime (section [2.2.5.2.4.1](#Section_e86515440fbb40388232375ff2d8a55e)) value to the current time value, incremented by dwRefreshInterval (section 2.2.5.2.4.1).[<260>](#Appendix_A_260) If the value is zero and zero is listed as a flag value for the default in section 3.1.1.2.1, the server MUST update the value of the property to be the default for that property, and return success. Otherwise, the server MUST update the value of the property for the zone to be the new value specified, and return success.[<261>](#Appendix_A_261)
  + If pszOperation matches a property name listed in section 3.1.1.2.2 or section 3.1.1.2.3 for which the server supports this property reset operation, the server MUST update the value of the property for the zone to be the new value specified, and return success.[<262>](#Appendix_A_262) Otherwise, the server MUST return a nonzero error code.
  + If pszOperation is ZoneTypeReset, the server MUST:
    - Check whether the requested zone type, directory server integration, and (if applicable) application directory partition match the zone's present state, and if so, return success.
    - Check whether the zone is directory server integrated and currently in the process of loading, and if so, return a failure.
    - Check whether the zone has scopes and whether the request is to convert the zone to either a non-primary zone or an AD integrated primary zone, and if so, return a failure.
    - Verify, if the requested zone type is primary, that:
      * There is a complete copy of the zone on the server (that is, the zone is not a forwarder or stub zone).
      * If the fDSIntegrated flag is TRUE:
        + If the zone is a primary zone, that it is not empty.
        + If the zone is currently directory-server-integrated, it is already stored in the requested by pszDpFqdn, and is not a secondary or cache zone.
        + If the zone is currently not directory-server-integrated, it is either a cache zone or a primary zone.
      * If the fDSIntegrated flag is FALSE, that:
        + A copy of the zone is present in local persistent storage.
        + The zone is not shutdown, or empty.
      * If any of the verifications fails, return a failure.
    - Check whether the requested zone type is secondary, and if so, reset the fDSIntegrated flag of the present zone to false.

Otherwise, the server MUST, in accordance with the operation specified:

* + - If the zone is directory server integrated, use LDAP search operations to find the zone's "dnsZone" and "dnsNode" objects (section 2.3) and copy the appropriate zone properties and data to a file. Set the zone's "Zone GUID" property to NULL.
    - If the zone is not directory server integrated, copy the zone's properties and data to the directory server using LDAP add operations (adding appropriate "dnsZone" and "dnsNode" objects to the directory server). If there is a failure in writing the zone records to the directory server, then the server MUST retry the write operation twice.
    - Reset the type information to the requested type.
    - Delete the original zone (using LDAP delete operations to remove the zone's "dnsZone" and "dnsNode" objects if necessary), and return success, or if any of the LDAP operations has failed, even after retries were specified, then return a failure. If deleting the zone from the directory server, the server MUST first attempt up to 4 times to rename the zone being deleted to a temporary name. Regardless of whether the rename is successful, the server then MUST attempt to delete the zone using LDAP delete operations, and retry up to 300 times if LDAP\_ADMIN\_LIMIT\_EXCEEDED is returned, never retrying if LDAP\_INSUFFICIENT\_RIGHTS is returned, and retrying up to 30 times for any other LDAP error.
  + If pszOperation is PauseZone, the server MUST set the zone's Paused flag to TRUE and return success. The same operation MUST be performed for all the existing zone scopes of the zone.
  + If pszOperation is ResumeZone, the server MUST set the zone's Paused flag to FALSE and return success. The same operation MUST be performed for all the existing zone scopes of the zone.
  + If pszOperation is DeleteZone, the server MUST delete the zone pointed to by pszZone from the server's local memory only and ensure that the zone will not be loaded at the next reboot, and return success. This operation does not modify the zone as it appears in the directory server, if it exists there.

The DNS server MUST also delete the associated scopes of that zone. The database file of the scopes MUST not be deleted.

* + If pszOperation is ReloadZone, the server MUST check whether the zone pointed to by pszZone is directory server-integrated and is already in the process of loading, and if so, return a failure. Otherwise, if the zone's **Dirty Flag** (section 3.1.1) is set to TRUE, then the server MUST do the following:
    - If the zone is a cache zone, and the zone is directory server-integrated and there are root hints in the zone, the server SHOULD write root hints to their permanent storage and overwrite existing directory server root hints through the use of the DNS\_ZONE\_LOAD\_OVERWRITE\_DS flag (section [2.2.5.2.7.1](#Section_780eba2615ea43d3a2b377ed9ab00690)). If the root hints are stored on the directory server and DownlevelDCsInDomain is nonzero, the server MUST check whether the root hints are empty. If the root hints are empty, the root hints MUST NOT be written to their permanent storage. Otherwise, if the root hints are stored on the directory server, the server MUST search for and delete the root hints on the directory server using LDAP search and delete commands and write the new root hints to the cache zone on the directory server using LDAP add and modify commands. If there is a failure in writing the root hints records to the directory server, then the server MUST retry the write operation twice.[<263>](#Appendix_A_263)
    - Otherwise, if the zone is not a read-only zone, write a copy of the zone to a file and send a DNS notification to peer or secondary DNS servers, if any.

If this zone has scopes configured, then all the data of the scopes MUST be written one by one to the corresponding scope files, if the scope’s **Dirty Flag** (section 3.1.1) is set to TRUE. If writing to any of the scopes encounters any issue, an error event SHOULD be logged and the error code MUST be returned.

Then the server MUST do the following:

* + - If the zone is a secondary zone, check that it has been stored to a file, and if not, return a failure.
    - If the zone is directory server-integrated, use the LDAP search operation to load the zone's "dnsZone" and "dnsNode" objects (section 2.3) from the directory server into memory and return success.
    - Otherwise, load the zone from the file, and return success. If the zone has scopes, then the DNS Server MUST try to load the scopes one by one. If any of the scope fails to load from the file, an event SHOULD be logged and the error MUST be returned.
    - If any of the above LDAP operations fails, even after retries, where specified, then return a failure.
  + If pszOperation is RefreshZone, and the zone specified is a secondary zone, is not currently transferring from the [**primary server**](#gt_bb76b8f0-0929-47c8-a06a-d3f9a8761d93), and at least 15 seconds has elapsed since the **Time of Last SOA check** (section 3.1.1) of the primary zone, then the server MUST force a refresh of the secondary zone pointed to by pszZone, from the primary DNS server, and return success. Otherwise, the server MUST return an error.
  + If pszOperation is ExpireZone the server MUST force expiration of the secondary zone pointed to by pszZone, by invalidating the zone data locally and contacting the primary DNS server to refresh, and return success.
  + If pszOperation is IncrementVersion,, the server MUST return a failure if the zone is not a primary or cache zone, and it MUST return success if the zone's **Dirty Flag** (section 3.1.1) is set to FALSE or the zone is not stored in a file. Otherwise, the server MUST write the uncommitted information to the file, send DNS notify [RFC1996] messages to all other servers hosting the zones, if they exist, and return success. If the zone specified is the cache zone, the server SHOULD write the root hints to their permanent storage. If the root hints are stored on the directory server and DownlevelDCsInDomain is nonzero, the server MUST check whether the root hints are empty. If the root hints are empty, the root hints MUST NOT be written to their permanent storage. Otherwise, if the root hints are stored on the directory server, the server MUST use LDAP add, delete, and search operations to replace the root hints on the directory server, and return success, regardless of the success or failure of these operations. If there is a failure in writing the root hints records to the directory server, then the server MUST retry the write operation twice, and still return success even if the retries fail.[<264>](#Appendix_A_264)
  + If pszOperation is WriteBackFile, the server MUST return a failure if the zone is not a primary or cache zone, and it MUST return success if the zone's **Dirty Flag** (section 3.1.1) is set to FALSE and it does not have any scopes configured or the zone is not stored in a file. Otherwise, the server MUST write the uncommitted information to the file, send DNS notify ([RFC1996]) messages to all other servers hosting the zones, if they exist, and return success, regardless of the success or failure of these operations. If the zone has scopes, the data of the scopes MUST be written to their corresponding scope files if the scope's **Dirty Flag** (section 3.1.1) is set to TRUE. If the server fails to write the data for any of the scopes it SHOULD log an error event and return the error code. If the operation results in updates only in the scope files and not the zone file, then DNS notify ([RFC1996]) messages SHOULD NOT be sent. If the zone specified is the cache zone, the server SHOULD write the root hints to their permanent storage. If the root hints are stored on the directory server and DownlevelDCsInDomain is nonzero, the server MUST check whether the root hints are empty. If the root hints are empty, the root hints MUST NOT be written to their permanent storage. Otherwise, if the root hints are stored on the directory server, the server MUST use LDAP add, delete, and search operations to replace the root hints on the directory server, and return success, regardless of the success or failure of these operations. If there is a failure in writing the root hints records to the directory server, then the server MUST retry the write operation twice, and still return success even if the retries fail.[<265>](#Appendix_A_265)
  + If pszOperation is DeleteZoneFromDs, the server MUST leave the zone, represented by a "dnsZone" object (section 2.3), intact and return a failure if the specified zone is not directory service-integrated. Otherwise, the server MUST locate the zone and its records, represented by "dnsNode" objects (section 2.3) using LDAP search operations. The server MUST rename the dnzZone object by prepending "..Deleted-" (or "..Deleted.<random number>-" if "..Deleted-" already exists) to the zone's name, then attempt to delete the zone and its records using LDAP delete operations, and retry up to 300 times if LDAP\_ADMIN\_LIMIT\_EXCEEDED is returned, never retrying if LDAP\_INSUFFICIENT\_RIGHTS is returned, and retrying up to 30 times for any other LDAP error. If the deletion from the directory server was successful, then the server MUST delete the local memory copy of the zone, and return success. If any of these LDAP operations cannot be completed, even after retries where specified, then the server MUST return failure.
  + If pszOperation is UpdateZoneFromDs, the server MUST:
    - Verify that the zone is not currently loading if it is a directory server integrated zone; otherwise, return a failure.
    - Refresh data for the zone from the directory server, and return success or failure depending on the result of this operation.
  + If pszOperation is ZoneExport, the server SHOULD:
    - Verify that the zone is not currently loading if it is a directory server integrated zone; otherwise, return a failure.
    - Export zone data for the zone to a file on the DNS server specified by pszZoneExportFile in pData, and return success or failure depending on the result of this operation, but MAY[<266>](#Appendix_A_266) simply return a failure.
  + If pszOperation is ZoneChangeDirectoryPartition, the server MUST:
    - Verify that the specified zone is not currently loading; otherwise, return a failure.
    - Verify that the application directory partition specified by pszDstPartition in pData is already known to the server; otherwise, return a failure.
    - Verify that the specified zone is not already in the destination application directory partition; otherwise, return success.[<267>](#Appendix_A_267)
    - Create a backup copy of the zone properties (the "dnsZone" object) in local storage using LDAP search operations, and then create a temporary "dnsZone" object in the new application directory partition with the zone properties from the backup copy, using LDAP add operations. If a failure occurs, the server MUST delete the temporary zone using the LDAP search and delete operations, and return a failure.
    - Copy the records ("dnsNode" objects) of the old zone to the temporary zone by enumerating the old zone's records using an LDAP search operation and by writing the new records to the temporary zone using LDAP add operations. If there is a failure in writing the records to the directory server, then the server MUST retry the write operation twice. If the search fails or the new records cannot be written, then the server MUST attempt to delete the temporary zone using the LDAP search and delete operations, and retry up to 300 times if LDAP\_ADMIN\_LIMIT\_EXCEEDED is returned, never retrying if LDAP\_INSUFFICIENT\_RIGHTS is returned, and retrying up to 30 times for any other LDAP error, and return a failure.
    - Rename the temporary zone to the final zone name using the LDAP rename operation, and delete the original zone's "dnsZone" and "dnsNode" objects using the LDAP search and delete operations. If the LDAP rename operation fails, the server MUST attempt to delete the temporary zone, and retry up to 300 times if LDAP\_ADMIN\_LIMIT\_EXCEEDED is returned, never retrying if LDAP\_INSUFFICIENT\_RIGHTS is returned, and retrying up to 30 times for any other LDAP error and return a failure. Otherwise, the server MUST return a success.
  + If pszOperation is DeleteNode, then:
    - If the node does not exist, the server MUST return success.
    - Otherwise, if the node specified is not in a primary zone, a cache zone, a cache scope, or a zone scope of a primary file backed zone, or the node is the root node for a zone, the server MUST return failure.
    - Otherwise, if the zone containing the specified node is not directory server-integrated, the server MUST delete the node pointed to by pszNodeName from the zone, MUST delete all DNS records in the node's subtree if the Boolean flag pointed to by the **dwParam** field in pData is set to TRUE, and return success.
    - Otherwise,
      * If the Boolean flag pointed to by the **dwParam** field in pData is set to TRUE, the server MUST poll the directory server for zone changes, using LDAP search operations.
      * If the Boolean flag pointed to by the **dwParam** field in pData is set to FALSE and the node contains subtrees, both the node and its subtrees MUST NOT be deleted and a success status MUST be returned.
      * If the node to be deleted is not a cache node, then the server MUST locate the node's "dnsNode" object (section 2.3) and its children using LDAP search operations, and then perform LDAP modify operations to set each node's dnsTombstoned attribute to TRUE and each node's dnsRecord (section [2.3.2.2](#Section_6912b33854724f59b9120edb536b6ed8)) attribute to contain a DNS\_RPC\_RECORD\_TS record (section 2.2.2.2.4.23) with an EntombedTime value equal to the current time expressed as the number of 100-nanosecond intervals since 12:00 A.M. January 1, 1601 Coordinated Universal Time (UTC).
      * If any of these LDAP operations fails, the server MUST attempt to roll back the previous operations using LDAP modify operations and return failure. If, during an attempt to roll back the deletions, any LDAP operation fails, the server MUST retry up to 2 times, and return failure.
  + If pszOperation is DeleteRecordSet, and the node does not exist or the node exists but does not contain any records, represented as "dnsNode" objects (section 2.3) of the type specified by the dwParam field in pData the server MUST return success. If the zone is directory server-integrated, the server MUST verify with an LDAP search that the node and/or records don't exist before returning success. Otherwise, the server MUST delete the record set of the type specified by **dwParam** field in pData (using LDAP modify operations when the zone is directory server-integrated), and return success. If deleting the record set would delete all records for the node and the zone is stored in the directory server, the DNS server MUST set the node's dnsTombstoned attribute to TRUE and each node's dnsRecord (section 2.3.2.2) attribute to contain a DNS\_RPC\_RECORD\_TS record (section 2.2.2.2.4.23) with an EntombedTime value equal to the current time expressed as the number of 100-nanosecond intervals since 12:00 A.M. January 1, 1601 Coordinated Universal Time (UTC). If any of these LDAP operations fails, the server MUST return failure.
  + If pszOperation is ForceAgingOnNode, and the zone's "Aging" (section 3.1.1.2.1) property is TRUE and the node pointed to by pszNodeNameexists, the server MUST enable aging on the node name pointed to by pszNodeName in the zone and MUST enable aging on the node's subtree if specified by the dwParam value in pData, and return success. Otherwise, the server MUST return a failure.
  + If pszOperation is AllowNSRecordsAutoCreation, the server MUST verify that the zone referenced is a primary zone and that it is a directory service-integrated zone and that it is not in the process of loading. If the verification fails, the server MUST return a failure. If the verification succeeds, the server MUST replace the list of IP addresses for which NS records will be automatically created with the list specified by pData, in the properties for the zone specified by pszZone, and use the LDAP modify operation to write all of the zone's properties to the copy of the zone on the directory server. Then, if any of the server's IP addresses are present in the new list of IP addresses and an NS record for the server is not present in the root of the zone, the server MUST add an NS record for the server to the zone, using the LDAP add operation. If there is a failure in writing the record to the directory server, then the server MUST retry the write operation twice. If none of the server's IP addresses are present in the new list of IP addresses and an NS record for the server is present in the root of the zone, the server MUST delete the NS record for the server from the zone, using the LDAP delete operation. Finally, if any of these LDAP operations could not be completed, even after retries where specified, then the server MUST return a failure; otherwise, the server MUST return success.
  + If pszOperation is DatabaseFile, the server MUST:
    - Verify that the zone pointed to by pszZone exists; that if the fDsIntegrated field of the DNS\_RPC\_ZONE\_DATABASE structure is set to TRUE, the zone is directory services-integrated, and is not in the process of loading; and that if fDsIntegrated is set to FALSE, the zone is not directory services-integrated. If any of these verifications fail, the server MUST return a failure.
    - Check whether pszFilename is not NULL and fDsIntegrated is TRUE, and if so, return a failure.
    - Check whether pszFilename is NULL and fDsIntegrated is TRUE, and if so, return success.
    - Check whether pszFilename is NULL and fDsIntegrated is FALSE, and if so, create the default database file for the zone and configure the zone to use that file, and return success.
    - Check whether pszFilename is not NULL and fDsIntegrated is FALSE, and if so, create the database file specified by pszFilename for the zone and configure the zone to use that file, and return success, or return a failure if the file name could not be created as specified.
  + If pszOperation is SignZone, the server MUST:
    - Verify that the zone pointed to by pszZone exists, that the zone's IsSigned property is FALSE, that the zone is a Primary zone, and that the zone's Keymaster property is set to TRUE. If any of these verifications fails, the server MUST return a failure.
    - Check whether the EnableOnlineSigning server property is TRUE. If it is FALSE and the zone is directory services-integrated, the server MUST return a failure.
    - Add appropriate DNSSEC records to the zone according to the entries in the zone's signing key descriptor list and [[RFC4035]](http://go.microsoft.com/fwlink/?LinkID=107053), and return failure if any operation fails.
    - If the zone has scopes, the server MUST initiate signing on the zone scopes. If any of the scope signing fails, the zone MUST be marked as unsigned, an appropriate event is logged, and an error code is returned.
    - Set the zone's IsSigned flag to TRUE, and return success.
  + If pszOperation is UnsignZone, the server MUST:
    - Verify that the zone pointed to by pszZone exists, that the zone's IsSigned property is TRUE, that the zone is a Primary zone, and that the zone's Keymaster property is set to TRUE. If any of these verifications fails, the server MUST return a failure.
    - Check whether the EnableOnlineSigning server property is TRUE. If it is FALSE and the zone is directory services-integrated, the server MUST return a failure.
    - Remove all DNSSEC records of type DNSKEY, RRSIG, NSEC, and NSEC3 from the zone, and return failure if any operation fails.
    - If the zone has scopes, the server MUST unsign all the scopes one by one. If any of the scopes fails to be unsigned the value of the zone IsSigned property MUST be kept unchanged, an appropriate event is logged, and an error code is returned.
    - Set the zone's IsSigned flag to FALSE, and return success.
  + If pszOperation is ResignZone, the server MUST:
    - Verify that the zone pointed to by pszZone exists, that the zone's IsSigned property is TRUE, that the zone is a Primary zone, and that the zone's Keymaster property is set to TRUE. If any of these verifications fails, the server MUST return a failure.
    - Check whether the EnableOnlineSigning server property is TRUE. If it is FALSE and the zone is directory services-integrated, the server MUST return a failure.
    - Regenerate all DNSSEC records in the zone as done for the "SignZone" operation, and return failure if any operation fails.
    - If the zone has scopes, the server MUST start the re-sign operation on them. If any of the scopes fail to re-sign, the value of the zone IsSigned property MUST be kept unchanged, an appropriate event SHOULD be logged, and an error code MUST be returned.
    - Return success.
  + If pszOperation is PerformZoneKeyRollover, the server MUST:
    - Verify that the zone pointed to by pszZone exists, that the zone's IsSigned property is TRUE, that the zone is a Primary zone, and that the zone's Keymaster property is set to TRUE. If any of these verifications fails, the server MUST return a failure.
    - Find the signing key descriptor indicated by pData in the zone's signing key descriptor list. If the signing key descriptor is not in this list, the server MUST return a failure.
    - Put the specified signing key descriptor into the zone's **rollover queue**, and return success.
  + If pszOperation is PokeZoneKeyRollover, the server MUST:
    - Verify that the zone pointed to by pszZone exists, that the zone's IsSigned property is TRUE, that the zone is a Primary zone, and that that the zone’s Keymaster property is set to TRUE. If any of these verifications fails, the server MUST return a failure.
    - Find the signing key descriptor indicated by pData in the zone's signing key descriptor list. If the signing key descriptor is not in this list, the server MUST return a failure.
    - If the dwCurrentRolloverStatus member of the DNS\_RPC\_SKD\_STATE structure for this signing key descriptor is not DNS\_SKD\_STATUS\_KSK\_WAITING\_FOR\_DS\_UPDATE, the server MUST return a failure.
    - Otherwise, the DNS server MUST advance the dwCurrentRolloverStatus member of the DNS\_RPC\_SKD\_STATE structure for this signing key descriptor to DNS\_SKD\_STATUS\_KSK\_WAITING\_FOR\_DS\_TTL and proceed with key rollover for this signing key descriptor as specified in [RFC4641], and return success.
  + If pszOperation is RetrieveRootTrustAnchors, the server MUST:
    - Verify that:
      * The zone pointed to by pszZone is the Trust Anchors zone.
      * The server is not a read-only server.
      * The "EnableDnsSec" server property (section 3.1.1.1.1) is TRUE.
      * The "RootTrustAnchorsURL" property (section 3.1.1.1.3) is not NULL, that the scheme is "https", and that the host and url-path are nonempty (see [[RFC1738]](http://go.microsoft.com/fwlink/?LinkId=90287)).
    - If any of these verifications fails, return a failure. Otherwise, the server MUST:
      * Create the Trust Anchors zone if it does not exist. If the creation fails, return an error.
      * Open an HTTPS connection to the host and port defined by the "RootTrustAnchorsURL" property. If the connection fails or times out, return an error.
      * Retrieve the XML document specified by the url-path or return an error.
      * Parse the XML document strictly according to the schema defined in [draft-jabley-dnssec-trust-anchor-03]. If the XML document deviates from the schema, return an error.
      * For each DS trust anchor specified by the XML document, verify that the algorithm and digest type are supported by the server, and that the length of the digest is valid. If the DS trust anchor is unsupported, continue to the next DS trust anchor. If none of the trust anchors are supported, return an error. If the trust anchor is supported and the digest length is invalid, return an error. Otherwise, add the trust anchor to a list of pending trust anchors.
      * Add each trust anchor in the pending list of trust anchors to the root node of the Trust Anchors zone. If the add attempt fails, return an error.
      * Schedule an immediate RFC 5011 active refresh for all trust points, and return success.
  + If pszOperation is TransferKeymasterRole, the server MUST:
    - Verify that dwTypeId is DNSSRV\_TYPEID\_DWORD and that pData points to one of the following values. If any of these verifications fails, the server MUST return a failure.

| Value | Meaning |
| --- | --- |
| DNS\_ZONE\_TRANSFER\_KEYMASTER\_ROLE  0x00000001 | Assign the key master role to the current server only if the zone is currently signed and the current server has access to the private key material corresponding to the signing key descriptors for the zone. |
| DNS\_ZONE\_SEIZE\_KEYMASTER\_ROLE  0x00000002 | Force assignment of the key master role to the current server, allowing assignment on unsigned zones or zones with no signing key descriptors. If the zone has signing key descriptors, this operation MUST return a failure if private key material for all signing key descriptors is not accessible by the current server. |
| DNS\_ZONE\_POLL\_KEYMASTER\_ROLE  0x00000003 | Requests that the server refresh the key master zone flags by reading from the directory service. |
| DNS\_ZONE\_SEIZE\_KEYMASTER\_ROLE\_WITHOUT\_KEY\_CHECKS  0x00000004 | Force assignment of the key master role to the current server, without checking to see whether private key material is accessible by the current server. |

* + - Verify that the zone pointed to by pszZone exists, that the zone is a Primary zone that is directory services-integrated, and that the zone is not read-only. If any of these verifications fails, the server MUST return a failure.
    - If the value of pData is DNS\_ZONE\_TRANSFER\_KEYMASTERROLE or DNS\_ZONE\_SEIZE\_KEYMASTER\_ROLE or DNS\_ZONE\_SEIZE\_KEYMASTER\_ROLE\_WITHOUT\_KEY\_CHECKS, the server MUST:
      * Verify that the "IsSigned" property of the zone (section 3.1.1.2.1) is TRUE or that the value of pData is DNS\_ZONE\_SEIZE\_KEYMASTER\_ROLE. If not, return a failure.
      * For an AD-backed zone, refresh the list of key master servers from the directory service or, if this operation fails, return a failure.
      * Return success if the "IsKeymaster" property of the zone (section 3.1.1.2.1) is TRUE and the value of pData is DNS\_ZONE\_TRANSFER\_KEYMASTER\_ROLE.
      * For an AD-backed zone, check whether the value of pData is DNS\_ZONE\_TRANSFER\_KEYMASTER\_ROLE or DNS\_ZONE\_SEIZE\_KEYMASTER\_ROLE and the zone has one or more signing key descriptors and, if so, verify that the private key material is available for each of the signing key descriptors.
      * For a file-backed zone, check whether the value of pData is DNS\_ZONE\_SEIZE\_KEYMASTER\_ROLE and the zone has one or more signing key descriptors and, if so, verify that the private key material is available for each of the signing key descriptors.
      * For an AD-backed zone, query the directory service for the value of the current key master. If this operation fails, and the value of pData is DNS\_ZONE\_TRANSFER\_KEYMASTER\_ROLE, return a failure.
      * For an AD-backed zone, check whether the value of pData is DNS\_ZONE\_TRANSFER\_KEYMASTER\_ROLE and, if so, verify that the query in the preceding step returned a value for the current key master, and that the current key master is marked as a key master by invoking the [R\_DnssrvQuery2](#Section_a90a44f0f64e44b09e35a7fc49f6adea) operation (section 3.1.4.7) on the current key master. The pszZone value used MUST match the value of pszZone passed to this operation, and pszOperation MUST be set to "IsKeymaster". If the current key master returns an error or FALSE, return a failure.
      * For an AD-backed zone, refresh the zone properties from the directory service. If this operation fails, the server MUST ignore the failure.
      * For an AD-backed zone, perform an LDAP modify operation to add the DN of the zone to the "msDNS-KeymasterZones" attribute of the server settings object ("CN=DNS Settings,CN=<server\_name>,CN=Servers,CN=<site\_name>, CN=Sites,CN=Configuration,DC=<domain name>") or, if this operation fails, return a failure.
      * For an AD-backed zone, perform an LDAP delete operation to delete the DN of the zone from the "msDNS-KeymasterZones" attribute of the previous key master server settings object ("CN=DNS Settings,CN=<previous\_keymaster\_server\_name>,CN=Servers,CN=<site\_name>, CN=Sites,CN=Configuration,DC=<domain name>") or, if this operation fails, return a failure.
      * For an AD-backed zone, check whether the value of pData is DNS\_ZONE\_TRANSFER\_KEYMASTER\_ROLE and, if so, perform the TransferKeymasterRole operation on the previous key master, with all parameters matching those passed to the current operation except that pData MUST point to DNS\_ZONE\_POLL\_KEYMASTER\_ROLE. If this operation fails, the server MUST ignore the failure.
      * Return success.
    - If the value of pData is DNS\_ZONE\_POLL\_KEYMASTER\_ROLE, the server MUST:
      * Open an LDAP connection to the Domain Naming Master FSMO role holder or to the local directory service if an LDAP connection to the Domain Naming Master FSMO role holder cannot be opened.
      * Perform an LDAP search operation to retrieve the value of the "msDNS-KeymasterZones" attribute of the DNS server settings object ("CN=DNS Settings,CN=<server\_name>,CN=Servers,CN=<site\_name>, CN=Sites,CN=Configuration,DC=<domain name>") and, if the operation fails, return a failure.
      * The DNS server MUST iterate each zone in the DNS Zone Table (section [3.1.1.2](#Section_8df021b347ad4829a1c25588165c27e7)) and for each zone:
        + If the zone is not directory service-integrated, ignore it.
        + Otherwise, if the zone is present in the "msDNS-KeymasterZones" attribute and the zone's IsKeymaster property (see section 3.1.1.2.1) is not TRUE or if the zone is not present in the "msDNS-KeymasterZones" attribute and the zone's IsKeymaster property is TRUE:

Set the zone's IsKeymaster property (section 3.1.1.2.1) to TRUE if the zone is present in the "msDNS-KeymasterZones" attribute or to FALSE if the zone is not present in the "msDNS-KeymasterZones" attribute.

Retrieve the FQDN of the zone's current key master: if the zone's IsKeymaster property is TRUE, set the zone's Keymaster property to the FQDN of the local host; otherwise, perform an LDAP search using the search filter "(&(msDNS-KeymasterZones=<zone name>)(objectCategory=msDNS-ServerSettings))" and set the zone's Keymaster property to the dnsHostName attribute value found on the parent object of the object returned by this search.

* + If pszOperation is CreateZonescope, the server MUST:
    - Verify that the zone pointed to by pszZone exists, that the zone is a primary file backed zone, that it is not an autocreated zone, that it is a non-reverse lookup zone, and that a scope does not exist with the given scope name in the specified zone. If any of these verifications fails, the server MUST return a failure. For cache scopes, if the scope does exist in the cache, the server MUST return a failure.
    - Create the zone scope or cache scope with the given scope name and return success if the creation is successful, otherwise return a failure.
  + If pszOperation is DeleteZonescope, the server MUST:
    - Verify that the zone pointed to by pszZone exists, that the zone is a primary file backed zone, that it is not an autocreated zone, that it is a non-reverse lookup zone, and that a scope does exist with the given scope name in the specified zone. If any of these verifications fails, the server MUST return a failure. For a cache scope, delete the scope if it exists; otherwise the server MUST return a failure.
    - If the zone scope or cache scope specified in pData does not exist, return DNS\_ERROR\_SCOPE\_DOES\_NOT\_EXIST.
    - If the zone scope or cache scope is being used by a DNS Policy (section 2.2.15.2.2), then the DNS server MUST return DNS\_ERROR\_ZONESCOPE\_IS\_REFERENCED.
    - The DNS server MUST attempt to delete the zone scope or cache scope in the DNS server, and return success or failure based on the result.
  + If pszOperation is CreatePolicy, the server MUST:
    - The DNS server checks whether the zone specified by pZone exists and, if not, returns DNS\_ERROR\_ZONE\_DOES\_NOT\_EXIST.
    - The DNS server validates whether the DNS Policy parameters specified in pData are valid. If the parameters are invalid, return DNS\_ERROR\_POLICY\_INVALID\_SETTINGS. For details, see DNS Policy Validation (section 3.1.8.3).
    - If the DNS Policy pData parameter dwProcessingOrder is greater than the highest Processing Order in the given level and appliesOn for the zone, return DNS\_ERROR\_POLICY\_INVALID\_SETTINGS.
    - If the DNS Policy name as specified in the pData parameter pwszPolicyName already exists, return DNS\_ERROR\_POLICY\_ALREADY\_EXISTS. The policy name check is done for the policies configured on the zone.
    - If the value weight in pContentList is 0 (as explained in DNS\_RPC\_POLICY\_CONTENT (section 2.2.15.2.2)) then the DNS server returns DNS\_ERROR\_POLICY\_INVALID\_WEIGHT. Allowed values for weight are any positive number from 1 to 0xffffffff.
    - If DNS Policy pData parameter dwProcessingOrder is 0 then reset the processing order to the last processing order for the specified level and appliesOn in the zone.
    - Create the new DNS Policy on the DNS server, and return success or failure based on the result. This DNS Policy is applicable to the DNS Operations at the zone level for that zone.
    - If the DNS Policy pData parameter dwProcessingOrder is the same as an existing DNS Policy in the specified level and appliesOn of the zone, update this new policy to use the new processing order. All DNS Policies whose processing order is equal to or greater than this processing order are incremented by 1.
  + If pszOperation is DeletePolicy, the server MUST:
    - If the zone specified by pZone does not exist, return DNS\_ERROR\_ZONE\_DOES\_NOT\_EXIST.
    - If the DNS Policy name specified in pData does not exist in the zone, return DNS\_ERROR\_POLICY\_DOES\_NOT\_EXIST.
    - Delete the DNS Policy in the zone of the DNS server, and return success or failure based on the result.
    - Increment the processing order of all policies whose processing order is greater than the processing order of the deleted policy by 1 for the given level and appliesOn in the zone.
  + If pszOperation is UpdatePolicy, the server MUST:
    - If the zone given by pZone does not exist, return DNS\_ERROR\_ZONE\_DOES\_NOT\_EXIST.
    - If the DNS Policy name specified in the member pwszPolicyName of pData does not exist in the specified zone policies of the DNS server, return DNS\_ERROR\_POLICY\_DOES\_NOT\_EXIST.
    - If the flags member of DNS\_RPC\_POLICY has DNS\_RPC\_FLAG\_POLICY\_PROCESSING\_ORDER set, update the processing order of the DNS policy to the new processing order specified in the input pData. Adjust the processing order of other DNS Policies at that zone for the given appliesOn accordingly.
    - If the flags member of DNS\_RPC\_POLICY has DNS\_RPC\_FLAG\_POLICY\_CONDITION set, then update the Condition of the DNS Policy to the condition specified in the input pData.
    - If the flags member of DNS\_RPC\_POLICY has DNS\_RPC\_FLAG\_POLICY\_CONTENT set, then update the content of the DNS Policy to the content specified in pData.
    - If any criteria flags as specified in Criteria Constants are set, remove the criteria values from the DNS Policy and set new criteria values as specified in pData.
    - Delete the DNS Policy on the DNS server, and return success or failure based on the result.

#### R\_DnssrvQuery (Opnum 1)

The R\_DnssrvQuery method queries the DNS server for information. The type of information queried for is specified by the client using the pszZone and pszOperation parameters. For the purpose of selecting an output structure type the server MUST consider the value of dwClientVersion (section [2.2.1.2.1](#Section_a237781bb048495d844b10ffb38df2a8)) to be 0x00000000 when responding to this method.

1. LONG R\_DnssrvQuery(
2. [in] handle\_t hBindingHandle,
3. [in, unique, string] LPCWSTR pwszServerName,
4. [in, unique, string] LPCSTR pszZone,
5. [in, unique, string] LPCSTR pszOperation,
6. [out] PDWORD pdwTypeId,
7. [out, switch\_is(\*pdwTypeId)] DNSSRV\_RPC\_UNION\* ppData
8. );

**hBindingHandle:** An RPC binding handle to the server. Details concerning binding handles are specified in [[C706]](http://go.microsoft.com/fwlink/?LinkId=89824) section 2.3.

**pwszServerName:** The client can pass a pointer to the FQDN of the target server as a null-terminated UTF-16LE character string. The server MUST ignore this value.

**pszZone:**  A pointer to a null-terminated character string that contains name of the zone to be queried. For operations specific to a particular zone, this field MUST contain the name of the zone in UTF-8 format. For all other operations, this field MUST be NULL.

**pszOperation:**  A pointer to a null-terminated character string that contains the name of the operation to be performed on the server. These are two sets of allowed values for pszOperation:

If pszZone is set to NULL, pszOperation MUST be either a property name listed in section [3.1.1.1](#Section_c4833797156c4c48a380d40dd1760eb9), or the following.

| Value | Meaning |
| --- | --- |
| "ServerInfo" | On output pdwTypeId SHOULD be set according to the value of the dwClientVersion field (section 2.2.1.2.1). If dwClientVersion is 0x00000000, then pdwTypeId SHOULD be set to DNSSRV\_TYPEID\_SERVER\_INFO\_W2K. If dwClientVersion is 0x00060000, then pdwTypeId SHOULD be set to DNSSRV\_TYPEID\_SERVER\_INFO\_DOTNET. If dwClientVersion is 0x00070000, then pdwTypeId SHOULD be set to DNSSRV\_TYPEID\_SERVER\_INFO[<268>](#Appendix_A_268) ppData MUST point to a structure of one of the types specified in DNS\_RPC\_SERVER\_INFO (section [2.2.4.2.2](#Section_ac444baf4bf94f36912e3041d4c46361)), which SHOULD contain the configuration information for the DNS server, but MAY have some fields set to zero even when the related configuration value is nonzero.[<269>](#Appendix_A_269) |

If pszZone is not NULL, pszOperation MUST be either a property name listed in section [3.1.1.2](#Section_8df021b347ad4829a1c25588165c27e7), or one of the following.

| Value | Meaning |
| --- | --- |
| "Zone" | On output the value pointed to by pdwTypeId SHOULD[<270>](#Appendix_A_270) be set to DNSSRV\_TYPEID\_ZONE and ppData MUST point to a structure of one of the types specified in DNS\_RPC\_ZONE (section [2.2.5.2.1](#Section_f22773cabfbf46a58042fbda1f3c4ad2)), which contains abbreviated information about the zone pointed to by pszZone. |
| "ZoneInfo" | On output the value pointed to by pdwTypeId SHOULD[<271>](#Appendix_A_271) be set to DNSSRV\_TYPEID\_ZONE\_INFOand ppData MUST point to a structure of one of the types specified in DNS\_RPC\_ZONE\_INFO (section [2.2.5.2.4](#Section_5e6b44a913c44c3aa7a2b5576016c3cf)), which contains full information about the zone pointed to by pszZone. |

**pdwTypeId:** A pointer to an integer that on success contains a value of type DNS\_RPC\_TYPEID (section [2.2.1.1.1](#Section_c49b8142a36441c8914a7675a573b5e4)) that indicates the type of data pointed to by ppData.

**ppData:** A DNSSRV\_RPC\_UNION(section [2.2.1.2.6](#Section_b61a872746b14981a6b3a1d4b92b67c4)) that contains a data-structure as indicated by dwTypeId.

**Return Values:** A Win32 error code indicating whether the operation completed successfully (0x00000000) or failed (any other value).

When processing this call, the server MUST do the following:

* If the Global Server State (section [3.1](#Section_bdac51424baf4b62bcced49eafc9c3e6)) is not "Running", return a failure.
* Check that the input parameters conform to the syntax requirements above, and if not return a failure.
* If pszZone is not NULL, search the DNS Zone Table (section 3.1) for the zone with name matching the value of pszZone. If a matching zone cannot be found return a failure.
* Validate, as specified in section [3.1.6.1](#Section_7ba0801d74f1499e81a300231ef31952), that the client has permissions to perform the attempted operation. If pszZone is NULL then the DNS server MUST perform the Phase 2 authorization test using the DNS Server Configuration Access Control List. If pszZone is not NULL then the DNS server MUST perform the Phase 2 authorization test using the Zone Access Control List for the zone specified by pszZone. Read privilege MUST be tested for all operations. If the client does not have permission to perform the operation, the server MUST return a failure.
* If pszZone is NULL, execute the operation indicated by the value of pszOperation specified as follows:
  + If pszOperation is ServerInfo, the server MUST return in ppData configuration information for the DNS server, and return success.
  + If pszOperation matches a property name listed in section [3.1.1.1.1](#Section_8903e50a91834a7d964053f6f5a91481), the server SHOULD[<272>](#Appendix_A_272) return DNSSRV\_TYPEID\_DWORD in pdwTypeId and return in ppData the value associated with that property, and return success. The server MAY return a nonzero error code.
  + If pszOperation matches a property name listed in section [3.1.1.1.2](#Section_f73f36ca3f0640caa392f7837d62642f), the server SHOULD[<273>](#Appendix_A_273) return DNSSRV\_TYPEID\_ADDRARRAY in pdwTypeId, return in ppData the value associated with that property as a DNS\_ADDR\_ARRAY (section [2.2.3.2.1](#Section_588ae29671bf402f999686ecee39dc29)), and return success; it MAY instead return DNSSRV\_TYPEID\_ADDRARRAY in the pdwTypeId, return in ppData the value associated with that property as an IP4\_ARRAY (section 2.2.3.2.1), and return success; or it MAY instead return a nonzero error code.[<274>](#Appendix_A_274)
  + If pszOperation matches a property name listed in section [3.1.1.1.3](#Section_c9d38538882744e6aa5e022a016ed723) that the server supports, the server MUST return DNSSRV\_TYPEID\_LPSTR for UTF-8 string properties or DNSSRV\_TYPEID\_LPWSTR for Unicode string properties in pdwTypeId, and return in ppData a pointer to the UTF-8 or Unicode string associated with that property, and return success.[<275>](#Appendix_A_275) If the property name is not supported, the server MUST return a nonzero error code.
  + If pszOperation matches a property name listed in section [3.1.1.1.4](#Section_35e541ef7a594a44ba187cd00aba6a0d) that the server supports, the server MUST return DNSSRV\_TYPEID\_UTF8\_STRING\_LIST, and return in ppData the DNS\_RPC\_UTF8\_STRING\_LIST (section [2.2.1.2.3](#Section_8c593fe61a074140992c71f97f929ba3)) associated with that property, and return success.
* If pszZone is not NULL, execute the operation indicated by the value of pszOperation, specified as follows:
  + If pszOperation is Zone, the server instead returns information about the zone in DNS\_RPC\_ZONE (section 2.2.5.2.1) format in ppData, and return success.
  + If pszOperation is ZoneInfo, the server instead returns information about the zone in DNS\_RPC\_ZONE\_INFO (section 2.2.5.2.4) format in ppData, and return success.
  + If pszOperation matches a property name listed in section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a), the server MUST return DNSSRV\_TYPEID\_DWORD in pdwTypeId, return in ppData the value associated with that property, and return success.
  + If pszOperation matches a property name listed in section [3.1.1.2.2](#Section_d532370821694c62b1e08569a103a8be) that the server supports, the server SHOULD[<276>](#Appendix_A_276) return DNSSRV\_TYPEID\_ADDRARRAY in pdwTypeId, return in ppData the value associated with that property as a DNS\_ADDR\_ARRAY (section [2.2.3.2.3](#Section_56ba5fabf304486699a44f1c1f9247a3)), and return success; or it MAY instead return DNSSRV\_TYPEID\_IPARRAY in pdwTypeId, return in ppData the value associated with that property as an IP4\_ARRAY (section [2.2.3.1.1](#Section_042395980c9b469bb1339f0142c2b1c5)), and return success. If the property name is not supported, the server MUST return a nonzero error code.

#### R\_DnssrvComplexOperation (Opnum 2)

Note: Some of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview in the Product Behavior appendix.

The R\_DnssrvComplexOperation method is used to invoke a set of server functions specified by the caller. These functions generally return more complex structures than simple 32-bit integer values, unlike the operations accessible through R\_DnssrvOperation. For the purpose of selecting an output structure type the server MUST consider the value of dwClientVersion (section [2.2.1.2.1](#Section_a237781bb048495d844b10ffb38df2a8)) to be 0x00000000 when responding to this method.

1. LONG R\_DnssrvComplexOperation(
2. [in] handle\_t hBindingHandle,
3. [in, unique, string] LPCWSTR pwszServerName,
4. [in, unique, string] LPCSTR pszZone,
5. [in, unique, string] LPCSTR pszOperation,
6. [in] DWORD dwTypeIn,
7. [in, switch\_is(dwTypeIn)] DNSSRV\_RPC\_UNION pDataIn,
8. [out] PDWORD pdwTypeOut,
9. [out, switch\_is(\*pdwTypeOut)] DNSSRV\_RPC\_UNION\* ppDataOut
10. );

**hBindingHandle:** An RPC binding handle to the server. Details concerning binding handles are specified in [[C706]](http://go.microsoft.com/fwlink/?LinkId=89824) section 2.3.

**pwszServerName:** The client SHOULD pass a pointer to the FQDN of the target server as a null-terminated UTF-16LE character string. The server MUST ignore this value.

**pszZone:** The name of the zone that is being operated on. This MUST be set to NULL unless pszOperation is set to QueryDwordProperty, in which case this value MUST be set either to NULL (to indicate that DNS server Configuration information is being requested) or to the name of the zone to be queried in UTF-8 format (to indicate that a DNS Zone integer property is being requested). This value will be used by certain operations as specified in the table below.

**pszOperation:** The operation to perform. The value of pszOperation SHOULD[<277>](#Appendix_A_277) be one of the following:

| Value | Meaning |
| --- | --- |
| EnumZones | Enumerate zones present on the DNS server qualifying for a specified simple zone filter value. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_DWORD and pDataIn MUST point to any combination of [ZONE\_REQUEST\_FILTERS (section 2.2.5.1.4)](#Section_f4cf1f3e7d134010a9155223dcabc15d) values. Unless an error is returned, on output the value pointed to by pdwTypeOut MUST be set to DNSSRV\_TYPEID\_ZONE\_LIST and ppDataOut MUST point to a structure of one of the types specified in [DNS\_RPC\_ZONE\_LIST (section 2.2.5.2.3)](#Section_e43b2e88e3d54e909c0708d2f2dc57ed). |
| EnumZones2 | Enumerate zones present on the DNS server qualifying for a specified complex zone filter value. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_ENUM\_ZONES\_FILTER and pDataIn MUST point to a structure of type [DNS\_RPC\_ENUM\_ZONES\_FILTER (section 2.2.5.2.9)](#Section_b2c763771c5042f483c6b514a1a7e65e). Unless an error is returned, on output the value pointed to by pdwTypeOut MUST be set to DNSSRV\_TYPEID\_ZONE\_LIST and MUST ppDataOut point to a structure of one of the types specified in DNS\_RPC\_ZONE\_LIST. |
| EnumDirectoryPartitions | Enumerate the Application Directory Partition Table known to the DNS server. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_DWORD and pDataIn MUST be set to zero if all application directory partitions are enumerated or to 0x000000001 if the DNS domain partition and DNS forest partition are excluded from results. Unless an error is returned, on output the value pointed to by pdwTypeOut MUST be set to DNSSRV\_TYPEID\_DP\_LIST and ppDataOut MUST point to a structure of type [DNS\_RPC\_DP\_LIST (section 2.2.7.2.4)](#Section_56b1d38f78964632b7dc0913ff3ef9b1). |
| DirectoryPartitionInfo | Retrieve detailed information about a specified application directory partition. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_LPSTR and pDataIn MUST point to a null-terminated UTF-8 string specifying the distinguished name of an application directory partition. Unless an error is returned, on output the value pointed to by pdwTypeOut MUST be DNSSRV\_TYPEID\_DP\_INFO and ppDataOut MUST point to a structure of type [DNS\_RPC\_DP\_INFO (section 2.2.7.2.1)](#Section_bd2a817d6a6940d3befc0c198a9c6e80). |
| Statistics | Retrieve statistics. On input dwTypeIn MUST be set to DNSSRV\_TYPEID\_DWORD and pDataIn MUST point to any combination of the [DNSSRV\_STATID\_TYPES (section 2.2.10.1.1)](#Section_6e5f45dfbf644c53867b2a1157472523) values. Unless an error is returned, on output the value pointed to by pdwTypeOut MUST be set to DNSSRV\_TYPEID\_BUFFER and ppDataOut MUST point to a [DNS\_RPC\_BUFFER structure (section 2.2.1.2.2)](#Section_cd4d047c3e894bc2b1651dc60ba538d5) that contains a list of variable sized [DNSSRV\_STAT structures (section 2.2.10.2.2)](#Section_c4dd5c55f4344b968bb59d69e28ec7c2). |
| QueryDwordProperty | Retrieve the value of a 32-bit integer property. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID \_LPSTR and pDataIn MUST point to a null-terminated UTF-8 string specifying a zone property name listed in section [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a) (if pszZone is non-NULL) or server property name listed in section [3.1.1.1.1](#Section_8903e50a91834a7d964053f6f5a91481) (if pszZone is NULL). Unless an error is returned, on output the value pointed to by pdwTypeOut MUST be set to DNSSRV\_TYPEID\_DWORD and ppDataOut MUST point to a DWORD value. |
| IpValidate | Validate a list of IP addresses. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_IP\_VALIDATE and pDataIn MUST point to a [DNS\_RPC\_IP\_VALIDATE structure (section 2.2.3.2.4)](#Section_2a367e0b5a8245d6aa77fbf407ed8d61) containing a list of IP addresses to be validated and the context information for validation as specified in section 2.2.3.2.4. Unless an error is returned, on output the value pointed to by pdwTypeOut MUST be set to DNSSRV\_TYPEID\_ADDRARRAY and ppDataOut MUST point to a structure of type [DNS\_ADDR\_ARRAY (section 2.2.3.2.3)](#Section_56ba5fabf304486699a44f1c1f9247a3) that contains IP validation results (section [2.2.3.2.1](#Section_588ae29671bf402f999686ecee39dc29)). |
| ModifyZoneSigningKeyDescriptor | Creates, deletes, or modifies a signing key descriptor (SKD) for the specified zone. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_SKD and pDataIn MUST point to a structure of type [DNS\_RPC\_SKD (section 2.2.6.2.1)](#Section_f7b0ad424cae40fd87c882af83824639). If GUID inside DNS\_RPC\_SKD is set to zero, the server MUST create a new signing key descriptor. If GUID inside DNS\_RPC\_SKD is set to a nonzero value and if all other fields in the structure are NULL, the server MUST delete the signing key descriptor from the zone. Otherwise, the server MUST modify the signing key descriptor for the specified zone. Unless an error is returned, on output the value pointed to by pdwTypeOut MUST be set to DNSSRV\_TYPEID\_SKD and ppDataOut MUST point to a structure of type DNS\_RPC\_SKD (section 2.2.6.2.1). |
| EnumZoneSigningKeyDescriptors | Retrieves the signing key descriptor found in the zone's signing key descriptor list for the specified zone. Input parameters (dwTypeIn and pDataIn) are ignored. Unless an error is returned, on output the value pointed to by pdwTypeOut MUST be set to DNSSRV\_TYPEID\_SKD\_LIST and ppDataOut MUST point to a structure of type [DNS\_RPC\_SKD\_LIST (section 2.2.6.2.2)](#Section_6a715b5cf8c24b26923bca23cca2bd57). |
| GetZoneSigningKeyDescriptorState | Retrieves the SKD state (section [2.2.6.2.3](#Section_b211f98844044c14b293bafd114b0eb6)) for the specified zone and the signing key descriptor GUID. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_LPWSTR and pDataIn MUST point to a string containing the GUID of the signing key descriptor. Unless an error is returned, on output the value pointed to by pdwTypeOut MUST be set to DNSSRV\_TYPEID\_SKD\_STATE and ppDataOut MUST point to a structure of type DNS\_RPC\_SKD\_STATE (section 2.2.6.2.3). |
| SetZoneSigningKeyDescriptorState | Modifies the SKD state (section 2.2.6.2.3) for the specified zone and the signing key descriptor GUID. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_SKD\_STATE and pDataIn MUST point to a structure of type DNS\_RPC\_SKD\_STATE (section 2.2.6.2.3). Note that only one key pointer string inside DNS\_RPC\_SKD\_STATE will be set per a specific operation as described below. Unless an error is returned, on output the value pointed to by pdwTypeOut MUST be set to DNSSRV\_TYPEID\_SKD\_STATE and ppDataOut MUST point to a structure of type DNS\_RPC\_SKD\_STATE (section 2.2.6.2.3) containing the modified SKD state. |
| ValidateZoneSigningParameters | Validates the zone signing parameters and returns a structure describing the invalid signing parameters. Input parameters (dwTypeIn and pDataIn) are ignored. Unless success is returned, on output the value pointed to by pdwTypeOut MUST be set to DNSSRV\_TYPEID\_SIGNING\_VALIDATION\_ERROR and ppDataOut MUST point to a structure of type [DNS\_RPC\_SIGNING\_VALIDATION\_ERROR (section 2.2.6.2.8)](#Section_b9b7d8ba458b4c589ae5c9616a52aa4a) containing invalid elements of the zone configuration. |
| EnumerateKeyStorageProviders | Enumerates key storage providers installed on the DNS server. On input, dwTypeIn and pDataIn are ignored. Unless an error is returned, on output the value pointed to by pdwTypeOut MUST be set to DNSSRV\_TYPEID\_UNICODE\_STRING\_LIST and ppDataOut MUST point to a structure of type [DNS\_RPC\_UNICODE\_STRING\_LIST (section 2.2.1.2.4)](#Section_ad7d4230cccf41589287328eb753e716) that contains a list of storage providers installed on the DNS server. |
| EnumerateTrustPoints | Retrieve a list of trust points, containing either all trust points or only those at or below a given FQDN. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_LPSTR and pDataIn MUST point either to a null pointer or to a null-terminated UTF-8 string specifying an FQDN. If pDataIn points to a null pointer, the server MUST return all of the trust points. If pDataIn is an FQDN and there is a trust point or parent of a trust point at the FQDN, the server MUST return the trust point at the FQDN (or an empty trust-point structure for the FQDN if the FQDN is not a trust point) followed by empty trust-point structures for each immediate child of the FQDN, if any. An empty trust-point structure is a structure in which eTrustPointState is TRUST\_POINT\_STATE\_INITIALIZED and all elements other than pszTrustPointName and dwRpcStructureVersion are zero. If pDataIn is an FQDN and there is neither a trust point nor the parent of a trust point at the FQDN, the server MUST return a nonzero error. Unless an error is returned, on output the value pointed to by pdwTypeOut MUST be set to DNSSRV\_TYPEID\_TRUST\_POINT\_LIST and ppDataOut MUST point to a structure of type [DNS\_RPC\_TRUST\_POINT\_LIST (section 2.2.6.2.5)](#Section_4a950c7f5f734b0eb0d2c467dde70976). |
| EnumerateTrustAnchors | Retrieve a list of the trust anchors at a given FQDN. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_LPSTR and pDataIn MUST point to a null-terminated UTF-8 string specifying an FQDN. If the FQDN specified is not a trust point, the server MUST return a nonzero error. Unless an error is returned, on output the value pointed to by pdwTypeOut MUST be set to DNSSRV\_TYPEID\_TRUST\_ANCHOR\_LIST and ppDataOut MUST point to a structure of type [DNS\_RPC\_TRUST\_ANCHOR\_LIST (section 2.2.6.2.7)](#Section_b70ad9a4fb654fea80f3eef09cbc54b9). |
| ExportZoneSigningSettings | Exports all the Dnssec settings of a file-backed primary zone from a server. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_DWORD and pDataIn SHOULD be 1 to get KSK details in the exported **DNS\_RPC\_ZONE\_DNSSEC\_SETTINGS** structure; otherwise, pDataIn SHOULD be zero. Unless an error is returned, on output pdwTypeOut is set to DNSSRV\_TYPEID\_ZONE\_SIGNING\_SETTINGS and ppDataOut points to a structure of type **PDNS\_RPC\_ZONE\_DNSSEC\_SETTINGS**. |
| ImportZoneSigningSettings | Imports the Dnssec settings to a primary file-backed zone on a server and takes appropriate action based on the signing metadata imported.  On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_ZONE\_SIGNING\_SETTINGS and pDataIn SHOULD be a structure of type PDNS\_RPC\_ZONE\_DNSSEC\_SETTINGS.  If this operation is invoked on a server that hosts a primary unsigned copy of a file-backed zone and the fIsSigned Property of PDNS\_RPC\_ZONE\_DNSSEC\_SETTINGS is 1, then the server becomes a [**nonkey master primary server**](#gt_0ab40b6b-2ca7-4782-8484-0361cff40833) for that zone. Unless an error is returned, on output pdwTypeOut is set to DNSSRV\_TYPEID\_DWORD and ppDataOut points to a structure of type ImportOpResult. |
| EnumZoneScopes | Enumerates all the zone scopes in a zone or cache scopes in a cache zone. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_NULL and pDataIn SHOULD be NULL. The pszZone MUST be the zone name for which zone scopes are to be enumerated or it MUST be "..cache". Unless an error is returned, on output pdwTypeOut is set to DNSSRV\_TYPEID\_ZONE\_SCOPE\_ENUM and ppDataOut points to a structure of type PDNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST. |
| ZoneStatistics | Gets the zone statistics from the server. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_DWORD and pDataIn SHOULD be either DNS\_RPC\_ZONE\_STATS\_GET, which gets the current zone statistics, or DNS\_RPC\_ZONE\_STATS\_CLEAR, which clears the zone statistics after getting them. The pZone MUST point to the zone information for which statistics are required. Unless an error is returned, on output pdwTypeOut SHOULD be set to DNSSRV\_TYPEID\_ZONE\_STATS and ppDataOut SHOULD point to a structure of type DNS\_RPC\_ZONE\_STATS. |
| EnumServerScopes | Enumerates all the server scopes in a DNS server. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_NULL and pDataIn SHOULD be NULL. Unless an error is returned, on output, pdwTypeOut SHOULD be set to DNSSRV\_TYPEID\_SCOPE\_ENUM and ppDataOut points to a structure of type PDNS\_RPC\_ENUM\_SCOPE\_LIST.[<278>](#Appendix_A_278) |
| EnumerateClientSubnetRecord | Enumerates the names all the Client Subnet Records on the DNS server. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_NULL and pDataIn SHOULD be NULL. Unless an error is returned, on output pdwTypeOut SHOULD be set to DNSSRV\_TYPEID\_UNICODE\_STRING\_LIST and ppDataOut points to a structure of type PDNS\_RPC\_UNICODE\_STRING\_LIST. |
| GetClientSubnetRecord | Gets the details of the Client Subnet Record on the DNS server. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_LPWSTR and pDataIn SHOULD be name of the Client Subnet Record. Unless an error is returned, on output pdwTypeOut SHOULD be set to DNSSRV\_TYPEID\_CLIENT\_SUBNET\_RECORD and ppDataOut points to a structure of type PDNS\_RPC\_CLIENT\_SUBNET\_RECORD. |
| EnumeratePolicy | Enumerates the policies configured on the server level or zone level for a specified zone on a DNS server. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_NULL and pDataIn SHOULD be NULL. Unless an error is returned, on output pdwTypeOut SHOULD be set to DNSSRV\_TYPEID\_POLICY\_ENUM and ppDataOut points to a structure of type PDNS\_RPC\_ENUMERATE\_POLICY\_LIST. |
| GetPolicy | Gets the details of a DNS Policy configured on the server level or on the zone level for a specified zone on the DNS server. On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_LPWSTR and pDataIn SHOULD be name of the DNS Policy. Unless an error is returned, on output pdwTypeOut SHOULD be set to DNSSRV\_TYPEID\_POLICY and ppDataOut points to a structure of type PDNS\_RPC\_POLICY. |

**dwTypeIn:** A [DNS\_RPC\_TYPEID (section 2.2.1.1.1)](#Section_c49b8142a36441c8914a7675a573b5e4) value indicating the type of input data pointed to by pDataIn.

**pDataIn:** Input data of type [DNSSRV\_RPC\_UNION (section 2.2.1.2.6)](#Section_b61a872746b14981a6b3a1d4b92b67c4), which contains a data structure of the type indicated by dwTypeIn.

**pdwTypeOut:** A pointer to a DWORD that on success returns a DNS\_RPC\_TYPEID (section 2.2.1.1.1) value indicating the type of output data pointed to by ppDataOut.

**ppDataOut:** A pointer to output data of type DNSSRV\_RPC\_UNION, which on success contains a data structure of the type indicated by pdwTypeOut.

**Return Values:** The method MUST return ERROR\_SUCCESS (0x00000000) on success or a nonzero Win32 error code value if an error occurred. All error values MUST be treated the same.

When processing this call, the server MUST do the following:

* If the **Global Server State** (section [3.1.1](#Section_e72286df3e4c45359a0ce9cc944248c2)) is not "Running", return a failure.
* Check that the input parameters conform to the syntax requirements above, and if not, return a failure.
* If pszZone is not NULL, verify that pszOperation is set to QueryDwordProperty, ModifyZoneSigningKeyDescriptor, EnumZoneSigningKeyDescriptors, GetZoneSigningKeyDescriptorState, SetZoneSigningKeyDescriptorState, ValidateZoneSigningParameters, EnumeratePolicy, or GetPolicy. If it is not, return a failure.
* If pszOperation is set to QueryDwordProperty, verify that dwTypeIn is set to DNSSRV\_TYPEID\_LPSTR. If it is not, return a failure.
* If pszOperation is set to ModifyZoneSigningKeyDescriptor, verify that dwTypeIn is set to DNSSRV\_TYPEID\_SKD. If it is not, return a failure.
* If pszOperation is set to GetZoneSigningKeyDescriptorState, verify that dwTypeIn is set to DNSSRV\_TYPEID\_LPWSTR. If it is not, return a failure.
* If pszOperation is set to SetZoneSigningKeyDescriptorState, verify that dwTypeIn is set to DNSSRV\_TYPEID\_SKD\_STATE. If it is not, return a failure.
* If pszZone is not NULL, search the DNS Zone Table (section 3.1.1) for the zone with a name matching the value of pszZone. If a matching zone cannot be found, return a failure.
* Validate, as specified in section [3.1.6.1](#Section_7ba0801d74f1499e81a300231ef31952), that the client has permissions to perform the attempted operation. If pszZone is NULL then the DNS server MUST perform the Phase 2 authorization test using the DNS server Configuration Access Control List. If pszZone is not NULL then the DNS server MUST perform the Phase 2 authorization test using the Zone Access Control List for the zone specified by pszZone. Write privilege MUST be tested for the ModifyZoneSigningKeyDescriptor and SetZoneSigningKeyDescriptorState operations. Read privilege MUST be tested for all other operations. If the client does not have permission to perform the operation, the server MUST return a failure.
* If pszZone is not NULL, and pszOperation is QueryDwordProperty, and pDataIn matches a property name listed in section 3.1.6.1, and the server supports that property, the server MUST set pdwTypeOut to DNSSRV\_TYPEID\_DWORD, set ppDataOut to the DWORD value of the property, and return success. If the property name is not supported, the server MUST return a nonzero error code.
* If pszZone is not NULL, and pszOperation is ModifyZoneSigningKeyDescriptor:
  + If the **GUID** field of the **DNS\_RPC\_SKD** structure pointed to by pDataIn is set to zero, the server MUST create a new signing key descriptor for the specified zone and add it to the zone's signing key descriptor list. If this operation succeeds, the server MUST set pdwTypeOut to DNSSRV\_TYPEID\_SKD and MUST set ppDataOut to point to a structure of type DNS\_RPC\_SKD representing the newly created signing key descriptor, and return success. Otherwise, the server MUST return a nonzero error code.
  + If the **GUID** field of the **DNS\_RPC\_SKD** structure pointed to by pDataIn is nonzero, and all other fields are set to zero, the server MUST locate the specified SKD in the zone's signing key descriptor list. If the SKD is found, the server MUST delete the specified SKD from the zone's signing key descriptor list. If this operation succeeds, the server MUST set pdwTypeOut to DNSSRV\_TYPEID\_SKD and MUST set ppDataOut to point to a structure of type DNS\_RPC\_SKD representing the deleted signing key descriptor, and return success. Otherwise, the server MUST return a nonzero error code.
  + If the **GUID** field of the **DNS\_RPC\_SKD** structure pointed to by pDataIn is nonzero, and one or more of the other fields are nonzero, the server MUST locate the specified SKD in the zone's signing key descriptor list. If the SKD is found, the server MUST modify this SKD as follows:
    - If any of the dwDNSKEYSignatureValidityPeriod, "dwDSSignatureValidityPeriod", "dwStandardSignatureValidityPeriod", or "dwNextRolloverAction" fields of the DNS\_RPC\_SKD pointed to by pDataIn are nonzero, modify the appropriate field in the SKD found in the zone's signing key descriptor list.
    - If the **dwRolloverPeriod** field of the DNS\_RPC\_SKD structure pointed to by pDataIn is nonzero, modify the appropriate field of the SKD found in the zone's signing key descriptor list. If the previous value of this field in the SKD was 0xFFFFFFFF, and the new value is some other nonzero value, the server MUST also modify the signing key descriptor's associated **ftNextRolloverTime** to the current time plus the new **dwRolloverPeriod**. If the previous value of this field in the SKD was not 0xFFFFFFFF, and the new value is 0xFFFFFFFF, the server MUST also set the signing key descriptor's associated **ftNextRolloverTime** to zero.
    - If any other fields of the DNS\_RPC\_SKD pointed to by pDataIn are nonzero, ignore these fields.

If this operation succeeds, the server MUST set pdwTypeOut to DNSSRV\_TYPEID\_SKD and MUST set ppDataOut to point to a structure of type DNS\_RPC\_SKD representing the modified signing key descriptor, and return success. Otherwise, the server MUST return a nonzero error code.

* If pszZone is not NULL, and pszOperation is SetZoneSigningKeyDescriptorState, the server MUST located the SKD specified by the **GUID** field of the DNS\_RPC\_SKD\_STATE pointed to by pDataIn in the zone's signing key descriptor list. If the SKD is found, the server MUST modify exactly one of the signing key descriptor's **pwszActiveKey**, **pwszStandbyKey**, or **pwszNextKey** fields as follows:
  + If the **pwszActiveKey** field of the DNS\_RPC\_SKD\_STATE structure pointed to by pDataIn is nonzero, modify the signing key descriptor's **pwszActiveKey** field.
  + If the **pwszActiveKey** field of the DNS\_RPC\_SKD\_STATE structure pointed to by pDataIn is NULL, and the **pwszStandbyKey** field of this structure is nonzero, modify the signing key descriptor's **pwszStandbyKey**.
  + If both the **pwszActiveKey** and **pwszStandbyKey** fields of the DNS\_RPC\_SKD\_STATE structure pointed to by pDataIn are NULL, and the **pwszNextKey** field of this structure is nonzero, modify the signing key descriptor's **pwszNextKey**.

If this operation succeeds, the server MUST set pdwTypeOut to DNSSRV\_TYPEID\_SKD\_STATE and MUST set ppDataOut to point to a structure of type DNS\_RPC\_SKD\_STATE representing the modified signing key descriptor, and return success. Otherwise, the server MUST return a nonzero error code.

* If pszZone is not NULL, and pszOperation is EnumZoneSigningKeyDescriptors, GetZoneSigningKeyDescriptorState, or ValidateZoneSigningParameters, execute the operation indicated by the value of pszOperation as previously specified against the specified zone.
* If pszZone is NULL, execute the operation indicated by the value of pszOperation as specified above.
* If pszZone is not NULL, and pszOperation is ExportZoneSigningSettings:
  + On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_DWORD.
  + To get KSK details in exported DNS\_RPC\_ZONE\_DNSSEC\_SETTINGS, pDataIn is 1; otherwise, zero.
  + Unless an error is returned, on output pdwTypeOut is set to DNSSRV\_TYPEID\_ZONE\_SIGNING\_SETTINGS and ppDataOut points to a structure of type PDNS\_RPC\_ZONE\_DNSSEC\_SETTINGS.
* If pszZone is not NULL, and pszOperation is ImportZoneSigningSettings:
  + On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_ZONE\_SIGNING\_SETTINGS and pDataIn SHOULD be a structure of type PDNS\_RPC\_ZONE\_DNSSEC\_SETTINGS.
  + Unless an error is returned, on output pdwTypeOut is set to DNSSRV\_TYPEID\_DWORD and ppDataOut points to a structure of type ImportOpResult.
  + If this operation is invoked on a server hosting a file-backed unsigned zone, and if the fIsSigned property of DNS\_RPC\_ZONE\_DNSSEC\_SETTINGS is 1, then the server becomes a nonkey master primary server of that signed zone.
  + If this operation is invoked on a server hosting a file-backed signed zone, and if the fIsSigned property of DNS\_RPC\_ZONE\_DNSSEC\_SETTINGS is 1, and if there is a difference in the imported and existing settings that requires re-signing, then the zone is marked for staggered signing with the new settings.
  + If this operation is invoked on a server hosting a file-backed signed zone, and if the fIsSigned property of DNS\_RPC\_ZONE\_DNSSEC\_SETTINGS is 0, then the zone is unsigned on the target server.
* If pszZone is not NULL, and pszOperation is EnumZoneScopes:
  + On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_NULL.
  + pDataIn SHOULD be NULL.
  + The pszZone MUST be the zone name for which zone scopes are to be enumerated, or it MUST be "..cache" to enumerate cache scopes.
  + Unless an error is returned, on output pdwTypeOut is set to DNSSRV\_TYPEID\_ZONE\_SCOPE\_ENUM and ppDataOut points to a structure of type PDNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST.
* If pszZone is not NULL, and pszOperation is ZoneStatistics:
  + On input, dwTypeIn MUST be set to DNSSRV\_TYPEID\_DWORD.
  + pDataIn SHOULD be either DNS\_RPC\_ZONE\_STATS\_GET, which gets the current Zone statistics or DNS\_RPC\_ZONE\_STATS\_GETCLEAR if one wants to clear the Zone Statistics after getting them.
  + The pZone MUST point to the zone information for which statistics are required.
  + Unless an error is returned, on output pdwTypeOut SHOULD be set to DNSSRV\_TYPEID\_ZONE\_STATS and ppDataOut SHOULD point to a structure of type DNS\_RPC\_ZONE\_STATS.
* If the pszOperation is EnumerateClientSubnetRecord:
  + The pszZone is NULL. This operation is at the server level.
  + The DNS server MUST return all the Client Subnet Record names, and return success or failure depending on the result. The output pdwTypeOut SHOULD be set to DNSSRV\_TYPEID\_UNICODE\_STRING\_LIST and ppDataOut SHOULD point to a structure of type DNS\_RPC\_UNICODE\_STRING\_LIST.
* If the pszOperation is GetClientSubnetRecord:
  + The pszZone is NULL. This operation is at the server level.
  + pDataIn SHOULD be a NULL-terminated Unicode string, which is the name of the Client Subnet Record whose details will be retrieved.
  + If the Client Subnet Record name given in input pData does not exist, the DNS server SHOULD return DNS\_ERROR\_CLIENT\_SUBNET\_DOES\_NOT\_EXIST.
  + The DNS server MUST return all the Client Subnet Record details and return success or failure depending on the result. The output pdwTypeOut SHOULD be set to DNSSRV\_TYPEID\_CLIENT\_SUBNET\_RECORD and ppDataOut SHOULD point to a structure of type DNS\_RPC\_CLIENT\_SUBNET\_RECORD.
* If pszZone is NULL and the pszOperation is EnumeratePolicy:
  + The DNS server MUST return all the DNS Policies at the server level and return success or failure depending on the result. The output pdwTypeOut SHOULD be set to DNSSRV\_TYPEID\_POLICY\_ENUM and ppDataOut SHOULD point to a structure of type PDNS\_RPC\_ENUMERATE\_POLICY\_LIST.
* If pszZone is not NULL and the pszOperation is EnumeratePolicy:
  + Retrieve the zone associated with pszZone. If the zone is not found return the error DNS\_ERROR\_ZONE\_DOES\_NOT\_EXIST.
  + The DNS server MUST return all the DNS Policies configured for the pszZonel and return success or failure depending on the result. The output pdwTypeOut SHOULD be set to DNSSRV\_TYPEID\_POLICY\_ENUM and ppDataOut SHOULD point to a structure of type PDNS\_RPC\_ENUMERATE\_POLICY\_LIST.
* If pszZone is NULL and the pszOperation is GetPolicy:
  + pDataIn SHOULD be a NULL terminated Unicode string, which is the name of the DNS Policy whose details will be retrieved.
  + If the DNS Policy given by the NULL terminated Unicode string pDataIn does not exist at the Server level, then the DNS server must return the error DNS\_ERROR\_POLICY\_DOES\_NOT\_EXIST.
  + The DNS server MUST return the details of the corresponding DNS Policy setting at the server level and return success or failure depending on the result. The output pdwTypeOut SHOULD be set to DNSSRV\_TYPEID\_POLICY and ppDataOut SHOULD point to a structure of type PDNS\_RPC\_POLICY.
* If pszZone is not NULL and the pszOperation is GetPolicy:
  + Retrieve the zone associated with pszZone. If the zone is not found return the error DNS\_ERROR\_DOES\_NOT\_EXIST.
  + pDataIn SHOULD be a NULL terminated Unicode string, which is the name of the DNS Policy on the zone whose details will be retrieved.
  + If the DNS Policy as specified in pDataIn is not found in the zone, return the error DNS\_ERROR\_POLICY\_DOES\_NOT\_EXIST.
  + The DNS server MUST return the details of the corresponding DNS Policy on the zone and return success or failure depending on the result. The output pdwTypeOut SHOULD be set to DNSSRV\_TYPEID\_POLICY and ppDataOut SHOULD point to a structure of type PDNS\_RPC\_POLICY.

#### R\_DnssrvEnumRecords (Opnum 3)

The R\_DnssrvEnumRecords method enumerates DNS records on the server.

1. LONG R\_DnssrvEnumRecords(
2. [in] handle\_t hBindingHandle,
3. [in, unique, string] LPCWSTR pwszServerName,
4. [in, unique, string] LPCSTR pszZone,
5. [in, unique, string] LPCSTR pszNodeName,
6. [in, unique, string] LPCSTR pszStartChild,
7. [in] WORD wRecordType,
8. [in] DWORD fSelectFlag,
9. [in, unique, string] LPCSTR pszFilterStart,
10. [in, unique, string] LPCSTR pszFilterStop,
11. [out] PDWORD pdwBufferLength,
12. [out, size\_is(, \*pdwBufferLength)]
13. PBYTE\* ppBuffer
14. );

**hBindingHandle:** An RPC binding handle to the server. Details concerning binding handles are specified in [[C706]](http://go.microsoft.com/fwlink/?LinkId=89824) section 2.3.

**pwszServerName:** The client SHOULD pass a pointer to the FQDN of the target server as a null-terminated UTF-16LE character string. The server MUST ignore this value.

**pszZone:**  A pointer to a null-terminated character string that contains the name of the zone to be queried. For operations specific to a particular zone, this field MUST contain the name of the zone in UTF-8 format. For all other operations, this field MUST be NULL.

**pszNodeName:** A pointer to a null-terminated character string that contains the node name at which to modify a record. A string that is not dot-terminated indicates a name relative to the zone root. A value of "@" indicates the zone root itself. A dot-terminated string indicates the name is an FQDN.

**pszStartChild:** A pointer to a null-terminated character string that contains the name of the child node at which to start enumeration. A NULL value indicates to start a new record enumeration. The client application can pass the last retrieved child node of pszNodeName to continue a previous enumeration.

**wRecordType:** An integer value that indicates the type of record to enumerate. Any value can be used, as specified in [DNS\_RECORD\_TYPE (section 2.2.2.1.1)](#Section_39b03b89226440638198d62f62a6441a). The query-only value DNS\_TYPE\_ALL indicates all types of records.

**fSelectFlag:** An integer value that specifies what records are included in the response. Any combination of the values below MUST be supported. Values not listed below MUST be ignored.

| Value | Meaning |
| --- | --- |
| DNS\_RPC\_VIEW\_AUTHORITY\_DATA  0x00000001 | Include records from authoritative zones. |
| DNS\_RPC\_VIEW\_CACHE\_DATA  0x00000002 | Include records from the DNS server's cache. |
| DNS\_RPC\_VIEW\_GLUE\_DATA  0x00000004 | Include glue records. |
| DNS\_RPC\_VIEW\_ROOT\_HINT\_DATA  0x00000008 | Include root hint records. |
| DNS\_RPC\_VIEW\_ADDITIONAL\_DATA  0x00000010 | Include additional records. |
| DNS\_RPC\_VIEW\_NO\_CHILDREN  0x00010000 | Do not include any records from child nodes. |
| DNS\_RPC\_VIEW\_ONLY\_CHILDREN  0x00020000 | Include only children nodes of the specified node in the results. For example: if a zone, "example.com", has child nodes, "a.example.com" and "b.example.com", calling R\_DnssrcEnumRecords(…,"example.com", "example.com", NULL, DNS\_TYPE\_ALL, DNS\_RPC\_VIEW\_ONLY\_CHILDREN, …, …, …, …) will return DNS\_RPC\_NODES for "a" and "b". |

**pszFilterStart:** Reserved for future use only. This MUST be set to NULL by clients and ignored by servers.

**pszFilterStop:** Reserved for future use only. This MUST be set to NULL by clients and ignored by servers.

**pdwBufferLength:** A pointer to an integer that on success contains the length of the buffer pointed to by ppBuffer.

**ppBuffer:** A pointer to a pointer that on success points to a buffer containing the enumerated records. The buffer is a series of structures beginning with a DNS\_RPC\_NODE structure (section [2.2.2.2.3](#Section_cb5539fa67fd40e09ea5468ecc56bd66)). The records for the node will be represented by a series of DNS\_RPC\_RECORD (section [2.2.2.2.5](#Section_ac7939811c6043b8be59cdbb5c4ecb8a)) structures. The number of DNS\_RPC\_RECORD structures following a DNS\_RPC\_NODE structure is given by the wRecordCount member of DNS\_RPC\_NODE.

**Return Values:** The method MUST return ERROR\_SUCCESS (0x00000000) on success or a non-zero Win32 error code if an error occurred. All error values MUST be treated the same, except that if the return code is ERROR\_MORE\_DATA (0x000000EA) then the enumeration contains more results than can fit into a single RPC buffer. In this case the client application can call this method again passing the last retrieved child as the pszStartChild argument to retrieve the next set of results.

When processing this call, the server MUST do the following:

* If the Global Server State (section [3.1](#Section_bdac51424baf4b62bcced49eafc9c3e6)) is not "Running", return a failure.
* Check that the input parameters conform to the syntax requirements above, and if not return a failure.
* If pszZone is not NULL, search the DNS Zone Table for a zone with a name matching the value of pszZone. If a matching zone cannot be found, return a failure. If pszZone is NULL, assume for the operations below that pszZone specifies the cache zone.
* Validate, as specified in section [3.1.6.1](#Section_7ba0801d74f1499e81a300231ef31952), that the client has permissions to perform the attempted operation. The DNS server MUST perform the Phase 2 authorization test using the Zone Access Control List for the zone specified by pszZone. Read privilege MUST be tested for this operation. If the client does not have permission to perform the operation, the server MUST return a failure.
* Locate the node indicated by pszNodeName in the zone indicated by pszZoneName. If no such node is found, then return DNS\_ERROR\_NAME\_DOES\_NOT\_EXIST, and set the output buffer length to zero.
* If pStartChild is non-NULL it indicates that this call is in continuation of an earlier call to R\_DnssrvEnumRecords that returned ERROR\_MORE\_DATA (0x000000EA), hence the server MUST attempt to locate this node and return failure if it cannot be found. The server MUST then continue the enumeration from there.
* Return output records that meet the criteria specified by the value of fSelectFlag, in parameters pointed to by pdwBufferLength and ppBuffer, and return success. If these criteria are met--the zone is stored in a directory server; the DsMinimumBackgroundLoadThreads server property (section [3.1.1.1.1](#Section_8903e50a91834a7d964053f6f5a91481)) is not 0x00000000; the zone is currently loading in the background; and the node indicated by pszNodeName has not yet been loaded into memory--the DNS server MUST behave as if the requested data does not exist in the zone.
* The server MUST return matching records for any **wType** value that is explicitly defined in the DNS\_RECORD\_TYPE structure. The server MUST also respond to type values exceeding 0x0031 that have matching records.

#### R\_DnssrvUpdateRecord (Opnum 4)

Note: Some of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview in the Product Behavior appendix.

The R\_DnssrvUpdateRecord method is used to add a new DNS record or modify/delete an existing DNS record at the server. This operation SHOULD[<279>](#Appendix_A_279) be supported.

1. LONG R\_DnssrvUpdateRecord(
2. [in] handle\_t hBindingHandle,
3. [in, unique, string] LPCWSTR pwszServerName,
4. [in, unique, string] LPCSTR pszZone,
5. [in, string] LPCSTR pszNodeName,
6. [in, unique] PDNS\_RPC\_RECORD pAddRecord,
7. [in, unique] PDNS\_RPC\_RECORD pDeleteRecord
8. );

**hBindingHandle:** An RPC binding handle to the server. Details concerning binding handles are specified in [[C706]](http://go.microsoft.com/fwlink/?LinkId=89824) section 2.3.

**pwszServerName:** The client SHOULD pass a pointer to the FQDN of the target server as a null-terminated UTF-16LE character string. The server MUST ignore this value.

**pszZone:** A pointer to a null-terminated character string that contains the name of the zone to be queried. For operations specific to a particular zone, this field MUST contain the name of the zone in UTF-8 format. For all other operations, this field MUST be NULL.

**pszNodeName:** A pointer to a null-terminated character string that contains the node name at which to modify a record. A string that is not dot-terminated indicates a name relative to the zone root. A value of "@" indicates the zone root itself. A dot-terminated string indicates the name is an FQDN.

**pAddRecord:** A pointer to a structure of type DNS\_RPC\_RECORD (section [2.2.2.2.5](#Section_ac7939811c6043b8be59cdbb5c4ecb8a)) that contains information based on the operation being performed as specified below.

**pDeleteRecord:** A pointer to a structure of type DNS\_RPC\_RECORD (section 2.2.2.2.5) that contains information based on the operation being performed as specified below.

To add a record:

* + pAddRecord: The DNS RR data of the new record.
  + pDeleteRecord: MUST be set to NULL.

To delete a record:

* + pAddRecord: MUST be set to NULL.
  + pDeleteRecord: Individual DNS RR data of the record to be deleted.

To replace a record:

* + pAddRecord: New record data.
  + pDeleteRecord: Old record data.

To add an empty node:

* + pAddRecord: MUST be set to NULL.
  + pDeleteRecord: MUST be set to NULL.

**Return Values:** The method MUST return ERROR\_SUCCESS (0x00000000) on success or a non-zero Win32 error code if an error occurred. All error values MUST be treated the same.

When processing this call, the server MUST do the following:

* If the Global Server State (section [3.1](#Section_bdac51424baf4b62bcced49eafc9c3e6)) is not "Running", return a failure.
* Check that the input parameters conform to the syntax requirements above, and if not return a failure.
* The server SHOULD support **pAddRecord** and/or **pDeleteRecord** for the explicitly defined types in section [2.2.2.1.1](#Section_39b03b89226440638198d62f62a6441a).[<280>](#Appendix_A_280) If any of the passed record types are not supported by the server, return a failure.
* If the **pAddRecord** is for an explicitly defined resource record type DNS\_TYPE\_CNAME (section 2.2.2.1.1), then delete any existing DNS\_TYPE\_CNAME record for the node specified in **pszNodeName**, before adding the record.
* If pszZone is not NULL, search the DNS Zone Table for a zone with a name matching the value of pszZone. If a matching zone cannot be found return a failure.
* Validate, as specified in section [3.1.6.1](#Section_7ba0801d74f1499e81a300231ef31952), that the client has permissions to perform the attempted operation. The DNS server MUST perform the Phase 2 authorization test using the Zone Access Control List for the zone specified by pszZone. Read privilege MUST be tested for this operation. If the client does not have permission to perform the operation, the server MUST return a failure.
* Locate the node indicated by **pszNodeName** in the zone indicated by pszZoneName. If no such node is found then return ERROR\_SUCCESS.
* If both **pAddRecord** and pDeleteRecord are NULL, then the server MUST add an empty node to the database if the node does not already exist. If the node already exists, the server MUST return ERROR\_SUCCESS.
* If pszZoneName is NULL or points to "..Cache" then the operation SHOULD be performed on the DNS server's cache and MAY be performed on the DNS server's set of root hint records.[<281>](#Appendix_A_281) If pszZoneName points to "..RootHints" then the operation MUST be performed on the DNS server's set of root hint records.
* If pszZoneName points to a primary zone, attempt to perform addition/deletion/update of the record. If the operation is successful, increment the zone serial number using serial number arithmetic [[RFC1982]](http://go.microsoft.com/fwlink/?LinkId=184551). If the last record at the node is being deleted and the zone is stored in the directory server, the DNS server MUST set the node's dnsTombstoned attribute to TRUE and the node's dnsRecord (section [2.3.2.2](#Section_6912b33854724f59b9120edb536b6ed8)) attribute to contain a DNS\_RPC\_RECORD\_TS record (section [2.2.2.2.4.23](#Section_def7736add094b4ab8d66a702a7ecde0)) with an EntombedTime value equal to the current time expressed as the number seconds since 12:00 A.M. January 1, 1601 Coordinated Universal Time (UTC). If the zone is directory server-integrated and the update causes new or modified records to be committed to the directory, the new zone serial number MUST also be written to the **Serial** field of the **dnsRecord** attribute, as specified in2.3.2.2. If this operation deletes the last record from the node and the zone is directory server-integrated, the DNS server MUST set the node's DNS Node Tombstone State (section [3.1.1](#Section_e72286df3e4c45359a0ce9cc944248c2)) to TRUE by setting the value of the **dnsTombstoned** attribute to TRUE and writing a DNS\_RPC\_RECORD\_TS (section 2.2.2.2.4.23) in the **dnsRecord** attribute.
* If both **pAddRecord** and **pDeleteRecord** are not NULL and a resource record is being replaced, if the **dwFlags** field is not set to DNS\_RPC\_FLAG\_RECORD\_CREATE\_PTR, the PTR record for the A/AAAA record being replaced is deleted. If the **dwFlags** field is set to DNS\_RPC\_FLAG\_SUPPRESS\_RECORD\_UPDATE\_PTR, the PTR record of the A/AAAA record being replaced is not deleted.
* Return success or a failure to indicate the result of the attempted operation.

#### R\_DnssrvOperation2 (Opnum 5)

The R\_DnssrvOperation2 method is used to invoke a set of server functions specified by the caller. The DNS server SHOULD implement R\_DnssrvOperation2.

All parameters are as specified by the R\_DnssrvOperation method (section [3.1.4.1](#Section_9500a7e8165d4b13be860ddc43100eef)) with the following exceptions:

1. LONG R\_DnssrvOperation2(
2. [in] handle\_t hBindingHandle,
3. [in] DWORD dwClientVersion,
4. [in] DWORD dwSettingFlags,
5. [in, unique, string] LPCWSTR pwszServerName,
6. [in, unique, string] LPCSTR pszZone,
7. [in] DWORD dwContext,
8. [in, unique, string] LPCSTR pszOperation,
9. [in] DWORD dwTypeId,
10. [in, switch\_is(dwTypeId)] DNSSRV\_RPC\_UNION pData
11. );

**dwClientVersion:** The client version in DNS\_RPC\_CURRENT\_CLIENT\_VER (section [2.2.1.2.1](#Section_a237781bb048495d844b10ffb38df2a8)) format.

**dwSettingFlags:** Reserved for future use. MUST be set to zero by clients and MUST be ignored by servers.

**Return Values:** The method MUST return ERROR\_SUCCESS (0x00000000) on success or a nonzero Win32 error code value if an error occurred. All error values MUST be treated the same.

When processing this call, the server MUST perform the same actions as for the R\_DnssrvOperation method (section 3.1.4.1) except in the event the dwClientVersion is greater than the server version, in which case the server MUST return the highest version number known to the server.

#### R\_DnssrvQuery2 (Opnum 6)

The R\_DnssrvQuery2 method queries the DNS server for information. The type of information queried for is specified by the client using the pszZone and pszOperation parameters. The DNS server SHOULD implement R\_ DnssrvQuery2 [<282>](#Appendix_A_282).

All parameters are as specified by the R\_DnssrvQuery method (section [3.1.4.2](#Section_b0419a70ac0b40baab941510992bc574)) with the following exceptions:

1. LONG R\_DnssrvQuery2(
2. [in] handle\_t hBindingHandle,
3. [in] DWORD dwClientVersion,
4. [in] DWORD dwSettingFlags,
5. [in, unique, string] LPCWSTR pwszServerName,
6. [in, unique, string] LPCSTR pszZone,
7. [in, unique, string] LPCSTR pszOperation,
8. [out] PDWORD pdwTypeId,
9. [out, switch\_is(\*pdwTypeId)] DNSSRV\_RPC\_UNION\* ppData
10. );

**dwClientVersion:** The client version in DNS\_RPC\_CURRENT\_CLIENT\_VER (section [2.2.1.2.1](#Section_a237781bb048495d844b10ffb38df2a8)) format.

**dwSettingFlags:** Reserved for future use only. This field MUST be set to zero by clients and ignored by servers.

**Return Values:** Return values behaviors and interpretations are same as they are for R\_DnssrvQuery method (section 3.1.4.2).

When processing this call, the server MUST perform the same actions as for the R\_DnssrvQuery method (section 3.1.4.2), except that for output structure types with multiple versions, the server MUST return the structure type selected by dwClientVersion except in the event the dwClientVersion is greater than the server version, in which case the server MUST return the highest version number known to itself.

#### R\_DnssrvComplexOperation2 (Opnum 7)

The R\_DnssrvComplexOperation2 method is used to invoke a set of server functions specified by the caller. These functions generally return more complex structures than simple 32-bit integer values, unlike the operations accessible through R\_DnssrvOperation. The DNS server SHOULD implement R\_DnssrvComplexOperation2.

All parameters are as specified by the R\_DnssrvComplexOperation method (section [3.1.4.3](#Section_864a6971f66447b9b012826fd2b0a409)) with the following exceptions:

1. LONG R\_DnssrvComplexOperation2(
2. [in] handle\_t hBindingHandle,
3. [in] DWORD dwClientVersion,
4. [in] DWORD dwSettingFlags,
5. [in, unique, string] LPCWSTR pwszServerName,
6. [in, unique, string] LPCSTR pszZone,
7. [in, unique, string] LPCSTR pszOperation,
8. [in] DWORD dwTypeIn,
9. [in, switch\_is(dwTypeIn)] DNSSRV\_RPC\_UNION pDataIn,
10. [out] PDWORD pdwTypeOut,
11. [out, switch\_is(\*pdwTypeOut)] DNSSRV\_RPC\_UNION\* ppDataOut
12. );

**dwClientVersion:** The client version in DNS\_RPC\_CURRENT\_CLIENT\_VER (section [2.2.1.2.1](#Section_a237781bb048495d844b10ffb38df2a8)) format.

**dwSettingFlags:** Reserved for future use only. This field MUST be set to zero by clients and ignored by servers.

**Return Values:** Return values and interpretations are the same as for R\_DnssrvComplexOperation (section 3.1.4.3).

When processing this call, the server MUST perform the same actions as for the R\_DnssrvComplexOperation method (section 3.1.4.3) except that for output structure types with multiple versions, the server MUST return the structure type selected by dwClientVersion except in the event the dwClientVersion is greater than the server version, in which case the server MUST return the highest version number known to itself.

#### R\_DnssrvEnumRecords2 (Opnum 8)

The R\_DnssrvEnumRecords2 method enumerates DNS records on the server. The DNS server SHOULD implement R\_DnssrvEnumRecords2 [<283>](#Appendix_A_283).

All parameters are as specified by the [R\_DnssrvEnumRecords method (section 3.1.4.4)](#Section_d0251c9b9e3e4eecbcc5eb6b995b6108) with the following exceptions:

1. LONG R\_DnssrvEnumRecords2(
2. [in] handle\_t hBindingHandle,
3. [in] DWORD dwClientVersion,
4. [in] DWORD dwSettingFlags,
5. [in, unique, string] LPCWSTR pwszServerName,
6. [in, unique, string] LPCSTR pszZone,
7. [in, unique, string] LPCSTR pszNodeName,
8. [in, unique, string] LPCSTR pszStartChild,
9. [in] WORD wRecordType,
10. [in] DWORD fSelectFlag,
11. [in, unique, string] LPCSTR pszFilterStart,
12. [in, unique, string] LPCSTR pszFilterStop,
13. [out] PDWORD pdwBufferLength,
14. [out, size\_is(, \*pdwBufferLength)]
15. PBYTE\* ppBuffer
16. );

**dwClientVersion:** The client version in DNS\_RPC\_CURRENT\_CLIENT\_VER (section [2.2.1.2.1](#Section_a237781bb048495d844b10ffb38df2a8)) format.

**dwSettingFlags:** Reserved for future use only. This field MUST be set to zero by clients and ignored by servers.

**Return Values:** Return values behaviors and interpretations are same as they are for R\_DnssrvEnumRecords method.

When processing this call, the server MUST perform the same actions as for the R\_DnssrvEnumRecords method.

#### R\_DnssrvUpdateRecord2 (Opnum 9)

The R\_DnssrvUpdateRecord2 method is used to add a new DNS record or modify/delete an existing DNS record at the server. The DNS server SHOULD implement R\_ DnssrvEnumRecords2.[<284>](#Appendix_A_284)

All parameters are as specified by the [R\_DnssrvUpdateRecord method (section 3.1.4.5)](#Section_37eea10100b8495899ebde8cda4b8417) with the following exceptions:

1. LONG R\_DnssrvUpdateRecord2(
2. [in] handle\_t hBindingHandle,
3. [in] DWORD dwClientVersion,
4. [in] DWORD dwSettingFlags,
5. [in, unique, string] LPCWSTR pwszServerName,
6. [in, unique, string] LPCSTR pszZone,
7. [in, string] LPCSTR pszNodeName,
8. [in, unique] PDNS\_RPC\_RECORD pAddRecord,
9. [in, unique] PDNS\_RPC\_RECORD pDeleteRecord
10. );

**dwClientVersion:** The client version in DNS\_RPC\_CURRENT\_CLIENT\_VER (section [2.2.1.2.1](#Section_a237781bb048495d844b10ffb38df2a8)) format.

**dwSettingFlags:** Reserved for future use only. This field MUST be set to zero by clients and ignored by servers.

**Return Values:** The method MUST return ERROR\_SUCCESS (0x00000000) on success or a nonzero Win32 error code if an error occurred. All error values MUST be treated the same. All record types SHOULD be supported, but if an operation is attempted on an unsupported record type, the method MUST return a nonzero Win32 error code.

When processing this call, the server MUST perform the same actions as for the R\_DnssrvUpdateRecord method.

#### R\_DnssrvUpdateRecord3 (Opnum 10)

The R\_DnssrvUpdateRecord3 method is used to add a new DNS record or modify or delete an existing DNS record in a zone or in a zone scope, or in a cache zone or cache scope, if specified. The DNS server SHOULD[<285>](#Appendix_A_285) implement R\_ DnssrvUpdateRecord3.

All parameters are as specified by the methods [R\_DnssrvUpdateRecord (section 3.1.4.5)](#Section_37eea10100b8495899ebde8cda4b8417) and [R\_DnssrvUpdateRecord2 (section 3.1.4.10)](#Section_8f50ae96d87f4fdb85265a86cea25837) with the following exceptions:

1. LONG R\_DnssrvUpdateRecord3(
2. [in] handle\_t hBindingHandle,
3. [in] DWORD dwClientVersion,
4. [in] DWORD dwSettingFlags,
5. [in, unique, string] LPCWSTR pwszServerName,
6. [in, unique, string] LPCSTR pszZone,
7. [in, unique, string] LPCWSTR pwszZonescope,
8. [in, string] LPCSTR pszNodeName,
9. [in, unique] PDNS\_RPC\_RECORD pAddRecord,
10. [in, unique] PDNS\_RPC\_RECORD pDeleteRecord
11. );

**pwszZonescope:** A pointer to a null-terminated character string that contains the name of the zone scope or cache scope inside the zone to be queried. For operations specific to a particular zone scope or cache scope, this field MUST contain the name of the zone scope or cache scope. If the value is NULL, the API gives the same behavior as R\_DnssrvUpdateRecord2.

When processing this call, the server MUST perform the same actions as for the R\_DnssrvUpdateRecord2 method.

#### R\_DnssrvEnumRecords3 (Opnum 11)

The R\_DnssrvEnumRecords3 method enumerates DNS records on a zone or a zone scope, or cache zone or a cache scope, if specified. The DNS server SHOULD[<286>](#Appendix_A_286) implement R\_DnssrvEnumRecords3.

All parameters are as specified by the [R\_DnssrvEnumRecords method (section 3.1.4.4)](#Section_d0251c9b9e3e4eecbcc5eb6b995b6108) and implement the [R\_DnssrvEnumRecords2 method (section 3.1.4.9)](#Section_0d236e5899444cdfae98f92460202e29) with the following exceptions:

1. LONG R\_DnssrvEnumRecords3(
2. [in] handle\_t hBindingHandle,
3. [in] DWORD dwClientVersion,
4. [in] DWORD dwSettingFlags,
5. [in, unique, string] LPCWSTR pwszServerName,
6. [in, unique, string] LPCSTR pszZone,
7. [in, unique, string] LPCWSTR pwszZoneScope,
8. [in, unique, string] LPCSTR pszNodeName,
9. [in, unique, string] LPCSTR pszStartChild,
10. [in] WORD wRecordType,
11. [in] DWORD fSelectFlag,
12. [in, unique, string] LPCSTR pszFilterStart,
13. [in, unique, string] LPCSTR pszFilterStop,
14. [out] PDWORD pdwBufferLength,
15. [out, size\_is(, \*pdwBufferLength)]
16. PBYTE\* ppBuffer
17. );

**pwszZoneScope:** A pointer to a null-terminated character string that contains the name of the zone scope inside the zone or cache scope inside the cache zone that is to be queried. For operations specific to a particular zone scope or cache scope, this field MUST contain the name of the zone scope or cache scope. If the value is NULL, the API gives the same behavior as the R\_DnssrvEnumRecords2 method.

When processing this call, the server MUST perform the same actions as for the R\_DnssrvEnumRecords2 method.

#### R\_DnssrvOperation3 (Opnum 12)

Note: Some of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview in the Product Behavior appendix.

The R\_DnssrvOperation3 method is used to invoke a set of server functions specified by the caller on the zone scope or cache scope if specified. The DNS server SHOULD[<287>](#Appendix_A_287) implement R\_DnssrvOperation3.

All parameters are as specified by the methods [R\_DnssrvOperation (section 3.1.4.1)](#Section_9500a7e8165d4b13be860ddc43100eef) and [R\_DnssrvOperation2 (section 3.1.4.6)](#Section_8c0522b197fb4fa7b4e22c55c0afb0e7) with the following exceptions.

1. DNS\_STATUS R\_DnssrvOperation3(
2. [in] handle\_t hBindingHandle,
3. [in] DWORD dwClientVersion,
4. [in] DWORD dwSettingFlags,
5. [in, unique, string] LPCWSTR pwszServerName,
6. [in, unique, string] LPCSTR pszZone,
7. [in, unique, string] LPCWSTR pwszZoneScopeName,
8. [in] DWORD dwContext,
9. [in, unique, string] LPCSTR pszOperation,
10. [in] DWORD dwTypeId,
11. [in, switch\_is(dwTypeId)] DNSSRV\_RPC\_UNION pData
12. );

**pwszZoneScopeName:** A pointer to a null-terminated character string that contains the name of the zone scope in the zone or cache scope in a cache zone, or a server scope configured on the DNS server in which the operation is to be performed. For operations specific to a particular zone scope, this field MUST contain the name of the zone scope. If the value is NULL then the API gives the same behavior as R\_DnssrvOperation2. If the value is not NULL then pszZone MUST point to a null-terminated character string that contains the name of the zone in UTF-8 format. In this case the type of the zone pointed to by pszZone MUST be a primary zone. It MUST also be a non-autocreated zone, a non-reverse lookup zone, and a non-AD integrated zone. For operations specific to server scopes, this field MUST contain the name of the server scope and the **pszZone** field MUST be NULL. For operations specific to cache scopes, this field MUST contain the name of the cache scope, and the **pszZone** field MUST be "..cache."

If pszZone is not NULL and pwszZoneScopeName is not NULL, pszOperation MUST be set to one of the following values:

| Value | Meaning |
| --- | --- |
| "DeleteNode" | Deletes a node from the given zone scope of a specified zone or a cache scope in a specified cache zone. On input, dwTypeId MUST be set to DNSSRV\_TYPEID\_NAME\_AND\_PARAM (section [2.2.2.1.1](#Section_39b03b89226440638198d62f62a6441a)), and pData MUST point to a structure of type [DNS\_RPC\_NAME\_AND\_PARAM (section 2.2.1.2.5)](#Section_408e91b91e534631a0515e097394f8d8). That structure contains the name of the node to be deleted as pointed by pszNodeName, and a Boolean flag in dwParam that indicates if the node's subtree is to be deleted. |
| "DeleteRecordSet" | Deletes all the DNS records of a particular type at a particular node that is present in the given zone scope of a specified zone or a cache scope in a specified cache zone. On input, dwTypeId MUST be set to DNSSRV\_TYPEID\_NAME\_AND\_PARAM (section 2.2.2.1.1). pData MUST point to a structure of type DNS\_RPC\_NAME\_AND\_PARAM (section 2.2.1.2.5). That structure contains the name of the node to be deleted and the DNS record type in the dwParam member. The type MUST be of value of either DNS\_RECORD\_TYPE (section 2.2.2.1.1) or 0x00FF, which specifies all types. |

If pszZone is NULL and pwszZoneScopeName is not NULL, pszOperation MUST be set to one of the following values.

| Value | Meaning |
| --- | --- |
| "Forwarders" | On input, dwTypeId SHOULD[<288>](#Appendix_A_288) be set to DNSSRV\_TYPEID\_FORWARDERS, and pData MUST point to a structure of one of the types specified in [DNS\_RPC\_FORWARDERS (section 2.2.5.2.10)](#Section_83f4bfffc5fb4029aad305b3d7f4ef40), which contains information about new IP addresses to which the DNS server SHOULD forward queries. These IP addresses are part of the server scope as specified in the pwszZoneScopeName. |
| "ResetDwordProperty" | Update the value of a (name, value) pair in the DNS Server Configuration. On input, dwTypeId MUST be set to DNSSRV\_TYPEID\_NAME\_AND\_PARAM, and pData MUST point to a structure of type DNS\_RPC\_NAME\_AND\_PARAM (section 2.2.1.2.5) that specifies the name of a property listed in section [3.1.1.3.1](#Section_7394837917b0401180804feab27d1f1f) and a new value for that property. |

When processing this call, the server MUST perform the same actions as for the R\_DnssrvOperation2 method. Operations specific to this method are as described in the preceding table. These operations are processed as specified in R\_DnssrvOperation, in the given zone scope or cache scope specified in pwszZoneScopeName of a zone or cache zone specified in pszZone or in the server scope specified in pwszZoneScopeName with pszZone being NULL.

#### R\_DnssrvQuery3 (Opnum 13)

Note: Some of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview in the Product Behavior appendix.

The R\_DnssrvQuery3 method queries the DNS server for information. The type of information queried for is specified by the client using the pszZone, pwszZoneScopeName, and pszOperation parameters. The DNS server SHOULD[<289>](#Appendix_A_289) implement R\_DnssrvQuery3.

All the parameters are as specified by the [R\_DnssrvQuery2](#Section_a90a44f0f64e44b09e35a7fc49f6adea) method with the following exceptions:

1. LONG R\_DnssrvQuery3(
2. [in] handle\_t hBindingHandle,
3. [in] DWORD dwClientVersion,
4. [in] DWORD dwSettingFlags,
5. [in, unique, string] LPCWSTR pwszServerName,
6. [in, unique, string] LPCSTR pszZone,
7. [in, unique, string] LPCWSTR pwszZoneScopeName,
8. [in, unique, string] LPCSTR pszOperation,
9. [out] PDWORD pdwTypeId,
10. [out, switch\_is(\*pdwTypeId)] DNSSRV\_RPC\_UNION\* ppData
11. );

**pwszZoneScopeName:** A pointer to a null-terminated character string that contains the name of the zone scope inside the zone or cache scope inside the cache zone to be queried or a server scope configured on the DNS server. For operations specific to a particular zone scope or cache scope, this field MUST contain the name of the zone scope or cache scope. If the value is NULL, then the API is as specified in R\_DnssrvQuery2 (section 3.1.4.7).

If pszZone is not NULL and pwszZoneScopeName is not NULL, pszOperation MUST be set to one of the following values:

| Value | Meaning |
| --- | --- |
| ScopeInfo | On output the value pointed to by pdwTypeId SHOULD be set to DNSSRV\_TYPEID\_ZONE\_SCOPE\_INFO and ppData MUST point to a structure of one of the types specified in [DNS\_RPC\_ZONE\_SCOPE\_INFO\_V1 (section 2.2.13.2.3.1)](#Section_7dc5c61adb9b4704a287a9713f24b0c6), which contains full information about the zone pointed to by pszZone or cache if "..cache" is specified in pszZone. |

* If pszZone is not NULL and pwszZoneScopeName is not NULL, and pszOperation value is ScopeInfo:
  + On input, pdwTypeId MUST be set to DNSSRV\_TYPEID\_ZONE\_SCOPE\_INFO.
  + pwszZoneScopeName MUST be the pointer to the name of the zone scope or cache scope that is to be queried.
  + pszZone MUST be the name of the zone in which the zone scope information is queried, or, for cache scope, it MUST be "..cache".
  + ppData MUST be in the format of DNS\_RPC\_ZONE\_SCOPE\_INFO\_V1.

If pszZone is NULL and pwszZoneScopeName is not NULL, pszOperation MUST be either a property name listed in section [3.1.1.3](#Section_e01cf84de8954104a8da29d29bf6b4f0) or set to one of the following values:

| Value | Meaning |
| --- | --- |
| "Forwarders" or "DynamicForwarders" | On output, the value pointed to by pdwTypeId SHOULD be set to DNSSRV\_TYPEID\_ADDRARRAY and ppData MUST point to a structure as specified in [DNS\_ADDR\_ARRAY (section 2.2.3.2.3)](#Section_56ba5fabf304486699a44f1c1f9247a3), which contains list of IP address.[<290>](#Appendix_A_290) |

* If pszZone is NULL and pwszZoneScopeName is not NULL, and pszOperation value is Forwarders or DynamicForwarders:
  + On input, pdwTypeId MUST be set to DNSSRV\_TYPEID\_ADDRARRAY.
  + pwszZoneScopeName MUST be the pointer to the name of the server scope that is to be queried.
  + pszZone MUST be NULL.
  + ppData MUST be in the format of **DNS\_ADDR\_ARRAY**.

### Timer Events

No protocol timer events are required on the server beyond the timers required in the underlying RPC protocol.

### Other Local Events

#### Three-phase authorization test

When a three-phase authorization test is performed, the following phases MUST be performed in order:

**Phase 1:** If the DNS server is directory server integrated then the client's credentials MUST be tested for Read privilege against the DNS Server Configuration Access Control List (see section [3.1.1](#Section_e72286df3e4c45359a0ce9cc944248c2)). This tests whether or not the client can be granted access to any of the functionality of the DNS Server Management Protocol. If this test is passed, then the server MUST proceed to Phase 2. If the DNS server is not directory server integrated, and if the client is a member of either the Administrators group or the System Operators group, access MUST be granted and further authorization testing MUST NOT be performed. Otherwise access MUST be denied and the server MUST return an error.

**Phase 2:** If the authorization test in Phase 1 is passed and the DNS server is directory server integrated, then the DNS server MUST perform an explicit ACL check for either Read or Write privilege. The ACL used for this test MUST be one of the three listed in the following table, and, for either Read or Write privilege, as specified in the description of the request being processed.

| Access Control List | Description |
| --- | --- |
| DNS Server Configuration Access Control List (see section 3.1.1) | This ACL is tested for Read privilege in Phase 1 to gate basic access to the protocol. It is also used to control access for any operation that is not performed against a specific zone or directory partition. |
| Application Directory Partition Access Control List (see section 3.1.1) | This ACL is used to control access for any operation that is performed against the directory partition. Operations that are performed against zones do not use this ACL. |
| Zone Access Control List (see section 3.1.1) | This ACL is used to control access for any operation that is performed against a zone that is stored in the directory server. If a zone is stored in the directory server inside a partition, any operation specific to the zone will use the Zone ACL. |

**Phase 3:** If the authorization test in Phase 2 is passed and the DNS server is directory server integrated, then the DNS server MUST impersonate the client for any actions performed against a directory server (for impersonation details, see [[MS-RPCE]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-RPCE%5d.pdf) section 2.2.1.1.9), unless the target of the modification is a dnsNode object whose Aging Time Stamp attribute (section [3.1.1.2.4](#Section_b01b73cf11a34d249561b8361c458bcd)) is older than the Time Zone Secured attribute of the zone (section 3.1.1). If the operation against the directory server fails, the DNS server MUST return an error.

#### Directory server security descriptors reading and caching

If the server is directory server integrated, directory server [**security descriptors**](#gt_e5213722-75a9-44e7-b026-8e4833f0d350) MUST be read from the directory server using LDAP every DsPollingInterval (section [3.1.1](#Section_e72286df3e4c45359a0ce9cc944248c2)) after DNS server boot. After each read, the server MUST cache the security descriptors.

Additionally, a Zone Access Control List (section 3.1.1) security descriptor MUST be read from the directory server when the corresponding zone is loaded during server boot time. This security descriptor MUST also be read when the corresponding zone is created through the ZoneCreate operation (section [3.1.4.1](#Section_9500a7e8165d4b13be860ddc43100eef)) and when the corresponding zone's directory partition encounters the EnlistDirectoryPartition operation (section 3.1.4.1).

Additionally, an Application Directory Partition Access Control List (section 3.1.1) security descriptor MUST be read from the directory server when the corresponding application directory partition is loaded during server boot time. This security descriptor MUST also be read when the corresponding application directory partition encounters the EnlistDirectoryPartition or ZoneChangeDirectoryPartition operation (section 3.1.4.1).

#### dnsRecord in the Directory Server

If the server is directory server integrated, then whenever dnsRecord attribute values (section [2.3.2.2](#Section_6912b33854724f59b9120edb536b6ed8)) are written to the directory server by using LDAP, each string MUST be converted from type DNS\_RPC\_NAME (section [2.2.2.2.1](#Section_3fd41adcc69e407b979e721251403132)) to type DNS\_COUNT\_NAME (section [2.2.2.2.3](#Section_cb5539fa67fd40e09ea5468ecc56bd66)). Similarly, when reading dnsRecords, the DNS server MUST convert each string of type DNS\_COUNT\_NAME to type DNS\_RPC\_NAME.

#### Modifying Directory Server Security Descriptors

Whenever the security descriptor for a directory server object needs to be modified, the server MUST perform the following procedure:

1. Perform an LDAP operation on an ADConnection as specified in [[MS-ADTS]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ADTS%5d.pdf) section 7.6.1.6, with the following parameters:
   * **TaskInputADConnection**: DNS Server AD Connection
   * **TaskInputRequestMessage**: protocolOp is set to **searchRequest** [[RFC4511]](http://go.microsoft.com/fwlink/?LinkId=157505) section 4.5).
   * **searchRequest** parameters are set as follows:
   * **baseObject**: The specified distinguished name of the object to be modified.
   * **scope**: base (0)
   * **derefAliases**: neverDerefAliases (0)
   * **sizeLimit**: 0
   * **timeLimit**: 360
   * **typesOnly**: FALSE
   * **filter**: "(objectCategory=\*)"
   * **attributes**: "ntSecurityDescriptor"
2. If the search request is successful, modify the security descriptor returned to grant or deny the specified rights to the specified local security group.
3. If the security descriptor is successfully modified, perform an LDAP operation on an ADConnection as specified in [MS-ADTS] section 7.6.1.6, with the following parameters:
   * TaskInputADConnection: **DNS Server AD Connection**
   * **TaskInputRequestMessage**: protocolOp is set to **modifyRequest** ([RFC4511] section 4.6)
   * Set the **modifyRequest** parameters as follows:
   * **object**: The specified distinguished name of the object to be modified.
   * **changes**:
   * **operation**: replace
   * **type**: "ntSecurityDescriptor"
   * **vals**: modified security descriptor

### Key Processing Rules

#### Constructing an Exported Key

The steps for constructing an exported key are as follows:

1. Obtain the Zone Signing Key. Encode it in a data structure appropriate for the signature algorithm, as specified in section [2.2.11.1.1](#Section_a430d9bdec994fa1a2f9d982018d7f44).
2. If the zone is stored in the default DNS domain application directory partition or the default application directory partition, let ProtectionSid denote the DOMAIN\_DOMAIN\_CONTROLLERS SID specified in [[MS-DTYP]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-DTYP%5d.pdf) section 2.4.2.4; otherwise, let ProtectionSid denote the ENTERPRISE\_DOMAIN\_CONTROLLERS SID specified in [MS-DTYP] section 2.4.2.4.
3. Construct a security descriptor in self-relative format, in the format specified in [MS-DTYP] section 2.4.6, using the following field values:
   1. **Sbz1** is set to zero.
   2. All **Control** bits except for SR are cleared.
   3. The **OwnerSid** field is set to ProtectionSid.
   4. The **GroupSid** field is set to the LOCAL\_SYSTEM SID specified in [MS-DTYP] section 2.4.2.4.
   5. The **Sacl** field is absent.
   6. The **Dacl** field contains two access control entries, as follows:
      1. The first entry contains an ACCESS\_ALLOWED\_ACE structure as specified in [MS-DTYP] section 2.4.4.2, with the **Sid** field set to ProtectionSid and the Mask value set to 0x3.
      2. The second entry contains an ACCESS\_ALLOWED\_ACE structure as specified in [MS-DTYP] section 2.4.4.2, with the **Sid** field set to the EVERYONE SID specified in [MS-DTYP] section 2.4.2.4 and the Mask value set to 0x2.
4. Obtain a group seed key for the security descriptor constructed in step 3, with NULL root key ID, using the procedure specified in [[MS-GKDI]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-GKDI%5d.pdf) section 3.2.4.
5. Construct a Protection Key Attributes structure (section [2.2.11.2.5](#Section_093dba1315c84848b27838afc5c0f5ed)) with the sidString element set to the string representation (specified in [MS-DTYP] section 2.4.2.1) of ProtectionSid (step 2).
6. Construct a Protection Key Identifier structure (section [2.2.11.2.4](#Section_98a575daca484afdba79f77a8bed4e4e)) using the key identifiers obtained in step 2.
7. Derive an AES-256 key from the group seed key retrieved in step 4 as follows:
   1. Derive a 64-byte secret using the key derivation procedure specified in [SP800-108] section 5.1 with HMAC [FIPS198-1] using SHA-512 [FIPS180-3] as the underlying PRF, using the Unicode string L"KDS service" as the label, and using the Unicode string L"KDS private key" as the context.
   2. Compute the SHA-256 hash [FIPS180-3] of the secret computed in step 7a.
8. Generate a random 256-bit AES key for use as the content encryption key, and a 12-byte random nonce. Encrypt the structure created in step 1 using the AES algorithm [[FIPS197]](http://go.microsoft.com/fwlink/?LinkId=89870) in GCM mode [[SP800-38D]](http://go.microsoft.com/fwlink/?LinkId=186038) using this key and nonce, and using an Integrity Check Value (ICV) length of 16 bytes. Append the 16-byte ICV to the end of the cipher text.
9. Encrypt the content encryption key generated in step 8 with the key derived in step 7, using AES [FIPS197] in CBC mode [SP800-38D] with PKCS#7 padding ([[RFC3852]](http://go.microsoft.com/fwlink/?LinkId=90445) section 6.3) with a random Initialization Vector (IV).
10. Construct a protected key blob using the CMS Enveloped-Data format specified in [RFC3852] section 6, as follows:
    1. Set the **version** field to 2.
    2. Omit the **originatorInfo** and **unprotectedAttrs** fields.
    3. In the **recipientInfos** structure, create a single **KEKRecipientInfo** member as follows:
       1. Set the **keyIdentifier** field of the KEK identifier to the result of step 6.
       2. Set the **other** field of the KEK identifier to the result of step 5.
       3. Omit the **date** field of the KEK identifier.
       4. Set the **keyEncryptionAlgorithm** field to AES256-CBC as specified in [[RFC3565]](http://go.microsoft.com/fwlink/?LinkId=229738) section 4.1 and the **encryptedKey** field to the result of step 9.
    4. In the **EncryptedContentInfo** structure:
       1. Set the **contentType** field to Data, as specified in [RFC3852] section 4.
       2. Set the **contentEncryptionAlgorithm** field to AES256-GCM, as specified in [[RFC5084]](http://go.microsoft.com/fwlink/?LinkId=229742) section 3.2, using the nonce and ICV length from step 8.
       3. Set the **encryptedContent** field to the result of step 8.
11. Construct an Exported Key Pair structure (section [2.2.11.2.6](#Section_820903b3170440b6b977ac9154a90ffd)) with the **ProtectedKeyBlob** field set to the result of step 10.

#### Importing an Exported Key

The steps for importing an exported key are as follows:

1. Validate that the input is in the format specified in section [2.2.11.2.6](#Section_820903b3170440b6b977ac9154a90ffd) by checking that the contents of the **Reserved1** and **Reserved2** fields match the expected values and that the **AlgorithmName** field has one of the values specified in section [2.2.11.1.1](#Section_a430d9bdec994fa1a2f9d982018d7f44). If not, fail and return an error.
2. Extract the **ProtectedKeyBlob** field, and verify that it is a syntactically correct DER-encoded ASN.1 structure of the Enveloped-data content type specified in [[RFC3852]](http://go.microsoft.com/fwlink/?LinkId=90445) section 6. If not, fail and return an error.
3. Extract the **keyIdentifier** field of the sole **KEKRecipientInfo** member of the **recipientInfos** structure in the protected key blob, and validate that it is in the format specified in section 2.2.11.2.6 by checking that the contents of the **Reserved1**, **Reserved2**, **Reserved3**, and **Reserved4** fields match their expected values. If not, fail and return an error.
4. Extract the **other** field of the KEK identifier in the aforementioned **KEKRecipientInfo** member, and validate that it is a syntactically correct DER-encoded ASN.1 structure conforming to the format specified in section [2.2.11.2.5](#Section_093dba1315c84848b27838afc5c0f5ed). If not, fail and return an error.
5. Using the sidString value in the Protection Key Attributes structure obtained in step 4, construct a security descriptor as specified in section [3.1.7.1](#Section_33a9931f7e064a44b29214541ad39c84) step 3.
6. Using the information in the **Protection Key Identifier** structure obtained in step 3 and the security descriptor constructed in step 5, obtain a group seed key by using the procedure specified in [[MS-GKDI]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-GKDI%5d.pdf) section 3.2.4. If unsuccessful, fail and return an error.
7. From the seed key obtained in step 6, derive the key encryption key as specified in section 3.1.7.1 step 7.
8. Use the key encryption key derived in step 7 to decrypt the contents of the **encryptedKey** field of the **KEKRecipientInfo** member obtained in step 3 by reversing the process in section 3.1.7.1 step 9. The result will be the content encryption key.
9. Extract the **encryptedContent** field of the protected key blob structure, and separate the ICV (contained in the last 16 bytes) from the cipher text (the rest of the field). Decrypt the cipher text using AES-GCM with the content encryption key obtained in step 8, and verify that the ICV computed during decryption matches the value in the blob. If not, fail and return an error.
10. Parse the result of step 9 based on the value of the **AlgorithmName** field, as specified in section 2.2.11.1.1.

### DNS Policy

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

#### Client Subnet Record

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

A Client Subnet Record is described by a NULL-terminated Unicode string containing a list of IPv4 or IPv6 subnets and the subnet length, as described in [DNS\_RPC\_CLIENT\_SUBNET\_RECORD (section 2.2.15.2.1)](#Section_c8b7e015035f424d90bef1c5f0b60eab). For example:

{"southasia", {201.37.23.0/24, 201.58.16.00/20}}

This example creates a Client Subnet Record for the region "southasia" containing the subnets 201.37.23.0/24 and 201.58.16.00/20.

#### DNS Policy Criteria

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

A [**DNS Policy Criteria**](#gt_71aebfeb-8787-432e-a8c8-5aa8eacd3e0a) contains properties that are matched for DNS operations. Appropriate action is applied to a DNS operation based on the result, expressed as a NULL-terminated Unicode string as describe in [DNS\_RPC\_CRITERIA (section 2.2.15.2.4)](#Section_be16f14ddf7440fe892c0718ebd32e84).

The Unicode string identifiers EQ and NE stand for Equals and Not Equals respectively. A **pCriteria** Unicode string can contain EQ or NE identifiers with values, or both can be present in a single criterion. For example, pCriteria = "EQ,a,b,c" indicates that the DNS policy matches the criteria type for a value a, b, or c. Similarly, pCriteria = "NE,a,b,c," indicates that a DNS policy matches the criteria type for a value not equal to a, b, and c.

The following table describes the DNS Policy Criteria:

| Policy Criteria | Definition |
| --- | --- |
| Fully Qualified Domain Name | Specifies that the criteria for match of a DNS Policy in a DNS operation, as described in DNS\_RPC\_CRITERIA (section 2.2.15.2.4), is based on the query name in the question ([[RFC1034]](http://go.microsoft.com/fwlink/?LinkId=90263) section 3.7) of a DNS query. For example, a [DNS\_RPC\_POLICY (section 2.2.15.2.5)](#Section_89be092dec014ab384e45a56622f9de8) with type=DnsPolicyCriteriaFqdn and pCriteria = "EQ,a.contoso.com" will match a Query with QName= "a.contoso.com". Criteria also support wild cards. For example, a criteria "EQ,\*.contoso.com" means the DNS policy will match for a query with QName anything in contoso.com, including the QName contoso.com. If the criteria is invalid, the DNS server returns DNS\_ERROR\_POLICY\_INVALID\_CRITERIA\_FQDN. |
| Client Subnet Record | Contains the IPv4 and IPv6 subnets, which are matched against the address of the source device from which the DNS operation message is initiated. For example, if an administrator creates a client subnet record "southasia" as explained in [Client Subnet Record (section 3.1.8.1)](#Section_7f8aadf248d14a3c8a47e00e88a915e1) and a DNS Operation originates from a source having subnet 201.37.23.0/24, then this is a match for the DNS Policy. If the criteria is invalid, the DNS server returns DNS\_ERROR\_POLICY\_INVALID\_CRITERIA\_CLIENT\_SUBNET. |
| Server Interface | Contains the IPv4 or IPv6 interface address on the DNS server. A DNS Operation message can be matched on the basis of the interface on which the message is received. This criteria is identified as described in [DNS\_RPC\_CRITERIA\_ENUM (section 2.2.15.1.1.6)](#Section_4b707d19860c461eb7c57e6322db26e9). For example, if the DNS Server has interfaces with addresses 10.172.1.1 and 192.168.1.1 and there is a DNS Policy with criteria type=DnsPolicyCriteriaInterface and pCriteria= "EQ,10.172.1.1" then a DNS query of a DNS operation that is received on the interface with address "192.168.1.1" will not be a match for the DNS policy. If the criteria is invalid, the DNS server returns DNS\_ERROR\_POLICY\_INVALID\_CRITERIA\_INTERFACE. |
| Question Type | Contains the QType of an incoming message in a DNS operation. For example, if the criteria is "EQ,AAAA,CNAME" then the DNS policy is a match if the incoming query of the DNS Operation has a QTYPE, as defined in [[RFC1035]](http://go.microsoft.com/fwlink/?LinkId=90264) section 3.2.3, of AAAA or CNAME. If the criteria is invalid, the DNS server returns DNS\_ERROR\_POLICY\_INVALID\_CRITERIA\_QUERY\_TYPE. |
| Network Protocol | Specifies that the criteria for match of a DNS Policy is based on the Internet Protocol used (IPv4 or IPv6) to send a DNS Query to the DNS Server during a DNS Operation. For example, if there is a criteria with type=DnsPolicyCriteriaNetworkProtocol and pCriteria="EQ,IPv4" and the DNS Server receives a query for a DNS operation on its IP v4 address then the DNS policy corresponding to this criteria is a match. Possible values that can be used in this criteria are "IPv4" and "IPv6". If the criteria is invalid, the DNS server returns DNS\_ERROR\_POLICY\_INVALID\_CRITERIA\_NETWORK\_PROTOCOL. |
| Transport Protocol | Specifies that the criteria for match of a DNS Policy is based on the Transport Layer Protocol (TCP or UDP) used to send a DNS Query to the DNS Server during a DNS Operation. For example, if there is a criteria with type=DnsPolicyCriteriaTransportProtocol and pCriteria="EQ,TCP" and the DNS Server receives a query for a DNS operation using transport protocol TCP then the DNS policy corresponding to this criteria is a match. Possible values that can be used in this criteria are "TCP" and "UDP". If the criteria is invalid, the DNS server returns DNS\_ERROR\_POLICY\_INVALID\_CRITERIA\_TRANSPORT\_PROTOCOL. |
| Time of Day | Specifies that the criteria for match of a DNS Policy is based on the time of day in minutes when the DNS Server receives a DNS Query during a DNS Operation.For example, if there is a criteria with type=DnsPolicyCriteriaTimeOfDay and pCriteria="EQ,16:00-18:00" and DNS policy action is "DNSPolicyIgnore" and the DNS Server receives a query for a DNS operation at a time between 16:00 and 18:00 local time of the DNS Server, then the DNS policy corresponding to this criteria is a match and since the action is DNSPolicyIgnore, the query will be dropped. For example, this can give the DNS server a short load time. Possible values that can be used in this criteria include any time span within the 24 hours of a day. If the criteria is invalid, the DNS server returns DNS\_ERROR\_POLICY\_INVALID\_CRITERIA\_TIME\_OF\_DAY. |

#### DNS Policy Validation

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The DNS Policy configured at the server level has certain restrictions. The following table describes the valid settings:

| DNS\_RPC\_POLICY\_LEVEL | DNS\_RPC\_POLICY\_TYPE allowed | DNS\_RPC\_POLICY\_ACTION\_TYPE allowed | DNS Policy Content |
| --- | --- | --- | --- |
| DnsPolicyServerLevel | DnsPolicyQueryProcessing | DnsPolicyDeny  DnsPolicyIgnore | There MUST be no DNS Policy content specified for DNS Policy at the server level. |
| DnsPolicyServerLevel | DnsPolicyRecursion | DnsPolicyDeny  DnsPolicyIgnore | There MUST be no DNS Policy content specified. |
| DnsPolicyServerLevel | DnsPolicyRecursion | DnsPolicyAllow | The DNS Policy content field MUST be populated with server scopes. |
| DnsPolicyZoneLevel | DnsPolicyQueryProcessing | DnsPolicyDeny  DnsPolicyIgnore | There MUST be no DNS Policy content specified. |
| DnsPolicyZoneLevel | DnsPolicyQueryProcessing | DnsPolicyAllow | The DNS Policy content field MUST be populated with zone scopes configured for the zone. |
| DnsPolicyZoneLevel |  | DnsPolicyDeny  DnsPolicyIgnore | There MUST be no DNS Policy content specified. |
| DnsPolicyZoneLevel |  | DnsPolicyAllow | The DNS Policy content field MUST be populated with zone scopes configured for the zone from which Zone Transfer will take place. |
| DnsPolicyZoneLevel |  | DnsPolicyDeny  DnsPolicyIgnore | There MUST be no DNS Policy content specified. |
| DnsPolicyZoneLevel |  | DnsPolicyAllow | The DNS Policy content field MUST be populated with zone scopes configured for the zone on which update has to happen. |

# Protocol Examples

## Querying a DNS server DWORD property

The following example specifies how to query the value of a DWORD DNS server property. In this example the value of the "LogLevel" property will be read.

The client calls R\_DnssrvQuery2 and provides the following parameters:

* DNS\_RPC\_CURRENT\_CLIENT\_VER as the client version.
* Zero as the settings flag.
* A Unicode string containing the FQDN of the DNS server whose LogLevel property is to be read as the server name.
* NULL as the zone name.
* "LogLevel" as the operation.
* A pointer to a DWORD where the DNS RPC type of the output data will be stored.
* A pointer to a DNSSRV\_RPC\_UNION (section [2.2.1.2.6](#Section_b61a872746b14981a6b3a1d4b92b67c4)) structure where the results of the DNS RPC operation will be stored.

The DNS server will return ERROR\_SUCCESS and additionally:

* The data type output value will be set to DNSSRV\_TYPEID\_DWORD.
* The DWORD member of the DNSSRV\_RPC\_UNION output structure will be set to the DNS server version in DNSSRV\_VERSION (section [2.2.4.2.1](#Section_abf93ed679384564b21486762a1c4dea)) format.

## Modifying a DNS server DWORD property

The following example specifies how to set the value of a DWORD DNS server property. In this example the value of the "LogLevel" property will be set.

The client formats a DNSSRV\_RPC\_UNION (section [2.2.1.2.6](#Section_b61a872746b14981a6b3a1d4b92b67c4)) structure to represent the request by setting the "Dword" member of the union one of the ZONE\_REQUEST\_FILTER values. Use

* The **NameAndParam** member of the DNSSRV\_RPC\_UNION is set to point to a DNS\_RPC\_NAME\_AND\_PARAM (section [2.2.1.2.5](#Section_408e91b91e534631a0515e097394f8d8)) structure (stored on the stack or elsewhere).
* The node name member of this DNS\_RPC\_NAME\_AND\_PARAM structure is set to "LogLevel".
* The **dwParam** member of this DNS\_RPC\_NAME\_AND\_PARAM structure is set to the desired combination of logging level bit flags, formatted as a DWORD. For example, to request logging of all incoming queries with full packet detail one would specify 0x0100E101 "(DNS\_LOG\_LEVEL\_QUERY|DNS\_LOG\_LEVEL\_QUESTIONS|DNS\_LOG\_LEVEL\_RECV|DNS\_LOG\_LEVEL\_UDP|DNS\_LOG\_LEVEL\_TCP|DNS\_LOG\_LEVEL\_FULL\_PACKETS)".

The client calls R\_DnssrvOperation2 and provides the following parameters:

* DNS\_RPC\_CURRENT\_CLIENT\_VER as the client version.
* Zero as the settings flag.
* A Unicode string containing the FQDN of the DNS server whose LogLevel property is to be read as the server name.
* NULL as the zone name.
* Zero as the context.
* "ResetDwordProperty" as the operation.
* DNSSRV\_TYPEID\_NAME\_AND\_PARAM as the type ID.
* A pointer to the DNSSRV\_RPC\_UNION structure created above as the RPC data.

The DNS server will return ERROR\_SUCCESS if the operation was successful or a Windows 32 error code if the operation failed.

## Creating a New Zone

The following example specifies how to create a new primary zone named "example.com". This zone will be stored in a file (and not in the directory).

The client formats a DNSSRV\_RPC\_UNION structure to represent the request:

* The ZoneCreate member of the DNSSRV\_RPC\_UNION is set to point to a DNS\_RPC\_ZONE\_CREATE\_INFO (section [2.2.5.2.7](#Section_f79e7455e26643d3ab2bf8e75aacfefa)) structure (stored on the stack or elsewhere). The entire structure should be zeroed out prior to use.
* The **pszZoneName** of this DNS\_RPC\_ZONE\_CREATE\_INFO structure is set to "example.com".
* The **dwZoneType** member of this DNS\_RPC\_ZONE\_CREATE\_INFO structure is set to DNS\_ZONE\_TYPE\_PRIMARY.

The client calls R\_DnssrvOperation2 and provides the following parameters:

* DNS\_RPC\_CURRENT\_CLIENT\_VER as the client version.
* Zero as the settings flag.
* A Unicode string containing the FQDN of the DNS server on which the zone is to be created.
* NULL as the zone name.
* Zero as the context.
* "ZoneCreate" as the operation.
* DNSSRV\_TYPEID\_ZONE\_CREATE as the type ID.
* A pointer to the DNSSRV\_RPC\_UNION structure created above as the RPC data.

The DNS server will return ERROR\_SUCCESS if the operation was successful or a Windows 32 error code if the operation failed.

## Enumerating Zones

The following example specifies how to enumerate all zones on the DNS server.

The client formats a DNSSRV\_RPC\_UNION structure to represent the request by setting the Dword member of the union to any ZONE\_REQUEST\_FILTER value. Use ZONE\_REQUEST\_ALL\_ZONES to enumerate all DNS server zones (with the exception of autocreated zones and the cache zone).

The client calls R\_DnssrvComplexOperation2 and provides the following parameters:

* DNS\_RPC\_CURRENT\_CLIENT\_VER as the client version.
* Zero as the settings flag.
* A Unicode string containing the FQDN of the DNS server on which the zone is to be enumerated.
* NULL as the zone name.
* Zero as the context.
* "EnumZones" as the operation.
* DNSSRV\_TYPEID\_DWORD as in the input type ID.
* A pointer to the DNSSRV\_RPC\_UNION structure created above as the input RPC data.
* A pointer to a DWORD where the DNS RPC type of the output data will be stored.
* A pointer to a DNSSRV\_RPC\_UNION structure where the results of the RPC operation will be stored.

The DNS server will return ERROR\_SUCCESS if the operation was successful or a Windows 32 error code if the operation failed. If the operation was successful then the output type ID will be set to DNSSRV\_TYPEID\_ZONE\_LIST and the ZoneList member of the output DNSSRV\_RPC\_UNION structure will be set to the zone enumeration results. The client can iterate the elements of ZoneList.ZoneArray in the union to examine the zones returned by the enumeration.

Once the client is finished with the zone enumeration result it MUST:

* Call MIDL\_user\_free on the pszZoneName and pszDpFqdn member of each element of the ZoneList.ZoneArray in the DNSSRV\_RPC\_UNION structure.
* Call MIDL\_user\_free on each pointer in the ZoneList.ZoneArray.
* Call MIDL\_user\_free on the ZoneList.ZoneArray pointer itself.

## Creating and Deleting a DNS Record

The following example specifies how to create a DNS record representing the IPv4 address "1.2.3.4" for the host named "host1" in the existing primary zone named "example.com". The new record will have a TTL of one hour.

The client formats a [DNS\_RPC\_RECORD structure (section 2.2.2.2.5)](#Section_ac7939811c6043b8be59cdbb5c4ecb8a), stored on the stack or elsewhere using a buffer at least large enough to hold the DNS\_RPC\_RECORD structure plus the [DNS\_RPC\_RECORD\_DATA](#Section_38b873927f614e3092639f0fb832d084) in the Buffer member, to represent the new record data as follows:

* **wDataLength** is set to the size of the data that will be stored in the Buffer member. In this case, because the record data will be a [DNS\_RPC\_RECORD\_A (section 2.2.2.2.4.1)](#Section_117c2ff9909445b283c25e44518e0bac) structure, the value of **wDataLength** is set to 4.
* **wType** is set to the desired record type (section [2.2.2.1.1](#Section_39b03b89226440638198d62f62a6441a)), in this case DNS\_TYPE\_A.
* **dwFlags**, **dwSerial**, **dwTimeStamp**, and **dwReserved** are set to zero.
* **dwTtlSeconds** is set to the desired TTL value in seconds, in this case 3600 for one hour.
* The client formats the Buffer member as a DNS\_RPC\_RECORD\_A structure. The byte values 0x01, 0x02, 0x03, and 0x04 are set in the four bytes of memory starting at the offset of Buffer.

The client calls [R\_DnssrvUpdateRecord2](#Section_8f50ae96d87f4fdb85265a86cea25837) and provides the following parameters:

* [DNS\_RPC\_CURRENT\_CLIENT\_VER](#Section_a237781bb048495d844b10ffb38df2a8) as the client version.
* Zero as the settings flag.
* A Unicode string containing the FQDN of the DNS server on which the operation is to be performed.
* "example.com" as the zone name.
* "host1" as the node name.
* A pointer to the DNS\_RPC\_RECORD created above as the *pAddRecord* parameter.
* A NULL pointer as the *pDeleteRecord* pointer.

The DNS server will return ERROR\_SUCCESS if the record was successfully created or a Windows error code on failure.

To delete this DNS record, format a DNS\_RPC\_RECORD structure exactly as described above, and call R\_DnssrvUpdateRecord2 in exactly the same way but pass NULL as the *pAddRecord* parameter and the DNS\_RPC\_RECORD pointer as the *pDeleteRecord*.

## Creating a Zone Scope

The following example specifies how to create a new zone scope named "example\_americas" in example.com created in section [4.3](#Section_8c30ab9a4ca64a3fb1930d2a32ce4229). This operation is allowed only on a file-backed zone.

The client calls [R\_DnssrvOperation2 (section 3.1.4.6)](#Section_8c0522b197fb4fa7b4e22c55c0afb0e7) and provides the following parameters:

* [DNS\_RPC\_CURRENT\_CLIENT\_VER (section 2.2.1.2.1)](#Section_a237781bb048495d844b10ffb38df2a8) as the client version.
* Zero as the settings flag.
* A Unicode string containing the FQDN of the DNS server on which the zone is to be created.
* "example.com" as the zone name.
* Zero as the context.
* CreateZonescope as the operation.
* DNSSRV\_TYPEID\_ZONE\_SCOPE\_CREATE as the type ID.
* Create a [DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1 (section 2.2.13.2.2.1)](#Section_cbe779f029b94a6199fba1d9115d590f) structure with dwFlags as zero and pwszScopeName as "example\_americas". Pass this structure as RPC data.

The DNS server returns ERROR\_SUCCESS if the operation was successful or a Windows error code if the operation fails.

## Deleting a Zone Scope

The following example specifies how to delete an existing zone scope named "example\_americas" in example.com created in section [4.6](#Section_64b8e0369b6f4ef7a7fd593340538e60). This operation is allowed only on a file-backed zone.

The client calls [R\_DnssrvOperation2 (section 3.1.4.6)](#Section_8c0522b197fb4fa7b4e22c55c0afb0e7) and provides the following parameters:

* [DNS\_RPC\_CURRENT\_CLIENT\_VER (section 2.2.1.2.1)](#Section_a237781bb048495d844b10ffb38df2a8) as the client version.
* Zero as the settings flag.
* A Unicode string containing the FQDN of the DNS server on which the zone is to be created.
* "example.com" as the zone name.
* Zero as the context.
* DeleteZonescope as the operation.
* DNSSRV\_TYPEID\_LPWSTR as the type ID.
* Unicode string "example\_americas" as RPC Data.

The DNS server returns ERROR\_SUCCESS if the operation was successful or a Windows error code if the operation failed.

## Enumerating Zone Scopes

The following example specifies how to enumerate all zone scopes on a zone example.com on the DNS server.

The client calls [R\_DnssrvComplexOperation2 (section 3.1.4.8)](#Section_d28e3ba85742417dad6d2e0139ab2ad9) and provides the following parameters:

* [DNS\_RPC\_CURRENT\_CLIENT\_VER (section 2.2.1.2.1)](#Section_a237781bb048495d844b10ffb38df2a8) as the client version.
* Zero as the settings flag.
* A Unicode string containing the FQDN of the DNS server on which the zone scopes are to be enumerated.
* "example.com" as the zone name.
* Zero as the context.
* EnumZonescopes as the operation.
* DNSSRV\_TYPEID\_NULL as the input type ID.
* NULL as the input RPC data.
* A pointer to a DWORD where the DNS RPC type of the output data will be stored.
* A pointer to a **DNSSRV\_RPC\_UNION** structure where the results of the RPC operation will be stored.

The DNS server returns ERROR\_SUCCESS if the operation is successful or a Windows error code if the operation fails. If the operation is successful, the output type ID will be set to DNSSRV\_TYPEID\_ZONE\_SCOPE\_ENUM and the ZonescopeList member of the output **DNSSRV\_RPC\_UNION** structure will be set to the zone scope enumeration results. The client can iterate the elements of ZonescopeList.ZoneArray in the union to examine the zones returned by the enumeration.

After the client is finished with the zone scope enumeration result, it MUST call MIDL\_user\_free on each pointer in the ZonescopeList.ZonescopeArray.

## Creating and Deleting a DNS Record in a Zone Scope

The following example specifies how to create a DNS record representing the IPv4 address "1.2.3.4" for the host named "host1" in the existing zone scope "example\_americas" on the primary zone named "example.com". The new record will have a TTL of one hour.

The client formats a [DNS\_RPC\_RECORD structure (section 2.2.2.2.5)](#Section_ac7939811c6043b8be59cdbb5c4ecb8a), stored on the stack or elsewhere using a buffer at least large enough to hold the **DNS\_RPC\_RECORD** structure plus the [DNS\_RPC\_RECORD\_DATA (section 2.2.2.2.4)](#Section_38b873927f614e3092639f0fb832d084) in the buffer member, to represent the new record data as follows:

* **wDataLength** is set to the size of the data that will be stored in the buffer member. In this case, because the record data will be a [DNS\_RPC\_RECORD\_A structure (section 2.2.2.2.4.1)](#Section_117c2ff9909445b283c25e44518e0bac), the value of **wDataLength** is set to 4.
* **wType** is set to the desired record type (section [2.2.2.1.1](#Section_39b03b89226440638198d62f62a6441a)), in this case DNS\_TYPE\_A.
* **dwFlags**, **dwSerial**, **dwTimeStamp**, and **dwReserved** are set to zero.
* **dwTtlSeconds** is set to the desired TTL value in seconds, in this case 3600 for one hour.
* The client formats the buffer member as a **DNS\_RPC\_RECORD\_A** structure. The byte values 0x01, 0x02, 0x03, and 0x04 are set in the four bytes of memory starting at the offset of the buffer.

The client calls [R\_DnssrvUpdateRecord3](#Section_12279f8cddaf47b8890591d7635cdfea) and provides the following parameters:

* [DNS\_RPC\_CURRENT\_CLIENT\_VER (section 2.2.1.2.1)](#Section_a237781bb048495d844b10ffb38df2a8) as the client version.
* Zero as the settings flag.
* A Unicode string containing the FQDN of the DNS server on which the operation is to be performed.
* "example.com" as the zone name.
* "host1" as the node name.
* A pointer to the **DNS\_RPC\_RECORD** created above as the *pAddRecord* parameter.
* A NULL pointer as the *pDeleteRecord* pointer.
* "example\_americas" as the zone scope name. If this is provided as NULL, the record is added to the default zone scope maintaining the legacy behavior.

The DNS server returns ERROR\_SUCCESS if the record is successfully created or a Windows error code on failure.

To delete this DNS record, format a **DNS\_RPC\_RECORD** structure exactly as described above, and call R\_DnssrvUpdateRecord3 (section 3.1.4.11) in exactly the same way, but pass NULL as the *pAddRecord* parameter and the **DNS\_RPC\_RECORD** pointer as the *pDeleteRecord*.

## Creating a Policy

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The following example specifies how to create a new [**server level policy**](#gt_e4c4b49e-bca4-4854-9e27-67ef0035f06e) named "DenyAllQueryForContosso.com" to deny any query for QName under contoso.com that asks explicitly for type=RRSIG.

The client calls [R\_DnssrvOperation (section 3.1.4.1)](#Section_9500a7e8165d4b13be860ddc43100eef) and provides the following parameters:

* A Unicode string containing the FQDN of the DNS server on which the policy is to be created.
* NULL as the value of *pszZone*.
* Zero as the context.
* CreatePolicy as the operation.
* DNSSRV\_TYPEID\_POLICY as the type ID.

Create a **DNS\_RPC\_POLICY** structure with *pwszPolicyName* as "DenyAllQueryForContosso.com", *level* as DnsPolicyServerLevel, *appliesOn* as DnsPolicyQueryProcessing, *action* as DnsPolicyDeny, *condition* as DNS\_AND, *isEnabled* as 1, *dwProcessingOrder* as 0, *pszZoneName* as NULL, *pContentList* as NULL, *flags* as 0, *dwCriteriaCount* as 2. The *pCriteriaList* list should have 2 DNS\_RPC\_CRITERIA members having the values {type=DnsPolicyCriteriaFqdn; pCriteria="EQ,\*.contoso.com"} and {type=DnsPolicyCriteriaQttype; pCriteria="EQ,RRSIG"}. Pass this RPC data structure as *pData*.

The DNS server returns ERROR\_SUCCESS if the operation was successful or a Windows error code if the operation fails.

## Updating a Policy

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The following example specifies how to update the server level policy named "DenyAllQueryForContosso.com" created in [Creating a Policy (section 4.10)](#Section_0a6660e099e941feba462146226b95db).

The client calls [R\_DnssrvOperation (section 3.1.4.1)](#Section_9500a7e8165d4b13be860ddc43100eef) and provides the following parameters:

* A Unicode string containing the FQDN of the DNS server on which the policy is to be updated.
* NULL as the value of *pszZone*.
* Zero as the context.
* UpdatePolicy as the operation.
* DNSSRV\_TYPEID\_POLICY as the type ID.

Create a **DNS\_RPC\_POLICY** structure with *pwszPolicyName* as "DenyAllQueryForContosso.com", *level* as DnsPolicyServerLevel, *appliesOn* as DnsPolicyQueryProcessing, *action* as DnsPolicyDeny. Other properties can be set if they are being updated. Set the **flags** field for each property of **DNS\_RPC\_POLICY** to be updated, as defined in [Constants (section 2.2.15.1.1)](#Section_a37b8ff71a784a159ce4cbe38d41cc19). Pass this RPC data structure as *pData*.

The DNS server returns ERROR\_SUCCESS if the operation was successful or a Windows error code if the operation fails.

## Deleting a Policy

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The following example specifies how to delete the server level policy named "DenyAllQueryForContosso.com" previously created.

The client calls [R\_DnssrvOperation (section 3.1.4.1)](#Section_9500a7e8165d4b13be860ddc43100eef) and provides the following parameters:

* A Unicode string containing the FQDN of the DNS server on which the policy is to be deleted.
* NULL as the value of *pszZone*.
* Zero as the context.
* DeletePolicy as the operation.
* DNSSRV\_TYPEID\_LPWSTR as the type ID.
* A null-terminated Unicode string containing the name of the policy to be deleted ("DenyAllQueryForContosso.com") as *pData*.

The DNS server returns ERROR\_SUCCESS if the operation was successful or a Windows error code if the operation fails.

## Enumerating Policies

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The following example specifies how to enumerate all the server level policies on the DNS Server.

The client calls [R\_DnssrvComplexOperation (section 3.1.4.3)](#Section_864a6971f66447b9b012826fd2b0a409) and provides the following parameters:

* A Unicode string containing the FQDN of the DNS server on which the policies are to be enumerated.
* NULL as the value of *pszZone*.
* EnumeratePolicy as the operation.
* DNSSRV\_TYPEID\_NULL as the type ID.
* NULL as the value of *pDataIn*.

The DNS server returns ERROR\_SUCCESS if the operation was successful or a Windows error code if the operation fails. If the operation is successful, *pdwTypeOut* SHOULD be of type DNSSRV\_TYPEID\_POLICY\_ENUM, and *ppDataOut* SHOULD point toPDNS\_RPC\_ENUMERATE\_POLICY\_LIST.

## Creating a Client Subnet Record

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The following example specifies how to create a new client subnet record named "Europe" that contains the addresses *20.10.0.0/16* and *2001:db8:abcd:0022::0/64*.

The client calls [R\_DnssrvOperation (section 3.1.4.1)](#Section_9500a7e8165d4b13be860ddc43100eef) and provides the following parameters:

* A Unicode string containing the FQDN of the DNS server on which the client subnet record is to be created.
* NULL as the value of *pszZone*.
* Zero as the context.
* CreateClientSubnetRecord as the operation.
* DNSSRV\_TYPEID\_CLIENT\_SUBNET\_RECORD as the type ID.

Create a [DNS\_RPC\_CLIENT\_SUBNET\_RECORD (section 2.2.15.2.1)](#Section_c8b7e015035f424d90bef1c5f0b60eab) structure with *pwszClientSubnetName* as "Europe", a Unicode string containing the name of the client subnet record to be created. Set *pIPAddr* and *pIPv6Addr* to the addresses *20.10.0.0* and *2001:db8:abcd:0022::0*, respectively. Set *SubnetLength* to 16 and 64, respectively, to specify the subnet length of the IP addresses sent.

Pass this RPC data structure as *pData*.

The DNS server returns ERROR\_SUCCESS if the operation is successful or a Windows error code if the operation fails.

## Deleting a Client Subnet Record

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The following example specifies how to delete the client subnet record "Europe" created in [Creating a Client Subnet Record (section 4.14)](#Section_7232d384985a4562b858441d97ced9ec).

The client calls [R\_DnssrvOperation (section 3.1.4.1)](#Section_9500a7e8165d4b13be860ddc43100eef) and provides the following parameters:

* A Unicode string containing the FQDN of the DNS server on which the client subnet record is to be deleted.
* NULL as the value of *pszZone*.
* Zero as the context.
* DeleteClientSubnetRecord as the operation.
* DNSSRV\_TYPEID\_LPWSTR as the type ID.
* A null-terminated Unicode string containing the name of the client subnet record to be deleted ("Europe") as *pData*.

The DNS server returns ERROR\_SUCCESS if the operation is successful or a Windows error code if the operation fails.

## Enumerating Client Subnet Records

Note: All of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

The following example specifies how to enumerate all the client subnet records on the DNS Server.

The client calls [R\_DnssrvComplexOperation (section 3.1.4.3)](#Section_864a6971f66447b9b012826fd2b0a409) and provides the following parameters:

* A Unicode string containing the FQDN of the DNS server on which the client subnet records are to be enumerated.
* NULL as the value of *pszZone*.
* EnumerateClientSubnetRecord as the operation.
* DNSSRV\_TYPEID\_NULL as the type ID.
* NULL as the value of *pDataIn*.

The DNS server returns ERROR\_SUCCESS if the operation is successful or a Windows error code if the operation fails.If the operation is successful, *pdwTypeOut* SHOULD be of type DNSSRV\_TYPEID\_UNICODE\_STRING\_LIST, and *ppDataOut* SHOULD point to a structure of type PDNS\_RPC\_UNICODE\_STRING\_LIST.

# Security

## Security Considerations for Implementers

This protocol allows any user to establish a connection to the RPC server. The protocol uses the underlying RPC protocol to retrieve the identity of the caller that made the method call as specified in [[MS-RPCE]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-RPCE%5d.pdf), section 3.3.3.4.3. Clients should create an authenticated RPC connection. Servers should use this identity to perform method-specific access checks.

### Security Considerations Specific to the DNS Server Management Protocol

DNS data and DNS server operations exposed by the DNS Server Management Protocol should be protected by access checks based on the identity of the RPC client. DNS server settings, DNS zones, DNS records, and the Application Directory Partition Table can each be protected by a different access control list to allow for delegation of administrative control over the DNS server.

It is important that implementations of the DNS Server Management Protocol do not allow anonymous RPC connections and should protect DNS access to all data and operations with access control checks based on client identity.

It is also important for clients and servers not to use RPC over named pipes as it is vulnerable to man-in-the-middle attacks. TCP/IP RPC should be used instead.

The DNS Server Management Protocol does not require clients to request RPC\_C\_AUTHN\_LEVEL\_PKT\_PRIVACY or servers to enforce it. If privacy of DNS management traffic is important implementers should consider using IPSec or another technology to provide encryption of data at a lower layer.

## Index of Security Parameters

| Security Parameter | Section |
| --- | --- |
| RPC\_C\_AUTHN\_GSS\_NEGOTIATE | Section [2.1.1](#Section_cafd4f91def54329ac8566eab1b67eec) |
| RPC\_C\_AUTHN\_GSS\_KERBEROS | Section 2.1.1 |
| RPC\_C\_AUTHN\_WINNT | Section 2.1.1 |
| RPC\_C\_IMP\_LEVEL\_IMPERSONATE | Section [2.1.2](#Section_6ba440f3eae24d8e85a1e62b6030bc8f) |

# Appendix A: Full IDL

Note: Some of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview in the Product Behavior appendix.

For ease of implementation the full IDL is provided below, where "ms-rpce.idl" refers to the IDL found in [[MS-RPCE]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-RPCE%5d.pdf) Appendix A. The syntax uses the IDL syntax extensions defined in [MS-RPCE] section 2.2.4. For example, as noted in [MS-RPCE] section 2.2.4.9, a pointer\_default declaration is not required and pointer\_default(unique) is assumed.

1. import "ms-dtyp.idl";
2. typedef struct \_DnsStatHeader
3. {
4. DWORD StatId;
5. WORD wLength;
6. BOOLEAN fClear;
7. UCHAR fReserved;
8. }DNSSRV\_STAT\_HEADER, \*PDNSSRV\_STAT\_HEADER;
9. typedef struct \_DnsStat
10. {
11. DNSSRV\_STAT\_HEADER Header;
12. BYTE Buffer[1];
13. }DNSSRV\_STAT, \*PDNSSRV\_STAT, \*PDNSSRV\_STATS;
14. typedef struct \_IP4\_ARRAY
15. {
16. DWORD AddrCount;
17. [size\_is( AddrCount )] DWORD AddrArray[];
18. }
19. IP4\_ARRAY, \*PIP4\_ARRAY;
20. typedef struct \_DnsAddr
21. {
22. CHAR MaxSa[32];
23. DWORD DnsAddrUserDword[8];
24. }
25. DNS\_ADDR, \*PDNS\_ADDR;
26. typedef struct \_DnsAddrArray
27. {
28. DWORD MaxCount;
29. DWORD AddrCount;
30. DWORD Tag;
31. WORD Family;
32. WORD WordReserved;
33. DWORD Flags;
34. DWORD MatchFlag;
35. DWORD Reserved1;
36. DWORD Reserved2;
37. [size\_is( AddrCount )] DNS\_ADDR AddrArray[];
38. }
39. DNS\_ADDR\_ARRAY, \*PDNS\_ADDR\_ARRAY;
40. //
41. // RPC buffer type for returned data
42. //
43. typedef struct \_DnssrvRpcBuffer
44. {
45. DWORD dwLength;
46. [size\_is(dwLength)] BYTE Buffer[];
47. }
48. DNS\_RPC\_BUFFER, \*PDNS\_RPC\_BUFFER;
49. //
50. // Server data types
51. //
52. typedef struct \_DnsRpcServerInfoW2K
53. {
54. // version
55. // basic configuration flags
56. DWORD dwVersion;
57. UCHAR fBootMethod;
58. BOOLEAN fAdminConfigured;
59. BOOLEAN fAllowUpdate;
60. BOOLEAN fDsAvailable;
61. //
62. // pointer section
63. //
64. [string] char \* pszServerName;
65. // DS container
66. [string] wchar\_t \* pszDsContainer;
67. // IP interfaces
68. PIP4\_ARRAY aipServerAddrs;
69. PIP4\_ARRAY aipListenAddrs;
70. // forwarders
71. PIP4\_ARRAY aipForwarders;
72. // future extensions
73. PDWORD pExtension1;
74. PDWORD pExtension2;
75. PDWORD pExtension3;
76. PDWORD pExtension4;
77. PDWORD pExtension5;
78. //
79. // DWORD section
80. //
81. // logging
82. DWORD dwLogLevel;
83. DWORD dwDebugLevel;
84. // configuration DWORDs
85. DWORD dwForwardTimeout;
86. DWORD dwRpcProtocol;
87. DWORD dwNameCheckFlag;
88. DWORD cAddressAnswerLimit;
89. DWORD dwRecursionRetry;
90. DWORD dwRecursionTimeout;
91. DWORD dwMaxCacheTtl;
92. DWORD dwDsPollingInterval;
93. // aging / scavenging
94. DWORD dwScavengingInterval;
95. DWORD dwDefaultRefreshInterval;
96. DWORD dwDefaultNoRefreshInterval;
97. DWORD dwReserveArray[10];
98. //
99. // BYTE section
100. //
101. // configuration flags
102. BOOLEAN fAutoReverseZones;
103. BOOLEAN fAutoCacheUpdate;
104. // recursion control
105. BOOLEAN fRecurseAfterForwarding;
106. BOOLEAN fForwardDelegations;
107. BOOLEAN fNoRecursion;
108. BOOLEAN fSecureResponses;
109. // lookup control
110. BOOLEAN fRoundRobin;
111. BOOLEAN fLocalNetPriority;
112. // BIND compatibility and mimicking
113. BOOLEAN fBindSecondaries;
114. BOOLEAN fWriteAuthorityNs;
115. // Bells and whistles
116. BOOLEAN fStrictFileParsing;
117. BOOLEAN fLooseWildcarding;
118. // aging / scavenging
119. BOOLEAN fDefaultAgingState;
120. BOOLEAN fReserveArray[15];
121. }
122. DNS\_RPC\_SERVER\_INFO\_W2K, \*PDNS\_RPC\_SERVER\_INFO\_W2K;
123. typedef struct \_DnsRpcServerInfoDotNet
124. {
125. DWORD dwRpcStructureVersion;
126. DWORD dwReserved0;
127. // basic configuration flags
128. DWORD dwVersion;
129. UCHAR fBootMethod;
130. BOOLEAN fAdminConfigured;
131. BOOLEAN fAllowUpdate;
132. BOOLEAN fDsAvailable;
133. //
134. // pointer section
135. //
136. [string] char \* pszServerName;
137. // DS container
138. [string] wchar\_t \* pszDsContainer;
139. // IP interfaces
140. PIP4\_ARRAY aipServerAddrs;
141. PIP4\_ARRAY aipListenAddrs;
142. // forwarders
143. PIP4\_ARRAY aipForwarders;
144. // logging
145. PIP4\_ARRAY aipLogFilter;
146. [string] wchar\_t \* pwszLogFilePath;
147. // Server domain/forest
148. [string] char \* pszDomainName; // UTF-8 FQDN
149. [string] char \* pszForestName; // UTF-8 FQDN
150. // Built-in directory partitions
151. [string] char \* pszDomainDirectoryPartition; // UTF-8 FQDN
152. [string] char \* pszForestDirectoryPartition; // UTF-8 FQDN
153. // future extensions
154. [string] char \* pExtensions[ 6 ];
155. //
156. // DWORD section
157. //
158. // logging
159. DWORD dwLogLevel;
160. DWORD dwDebugLevel;
161. // configuration DWORDs
162. DWORD dwForwardTimeout;
163. DWORD dwRpcProtocol;
164. DWORD dwNameCheckFlag;
165. DWORD cAddressAnswerLimit;
166. DWORD dwRecursionRetry;
167. DWORD dwRecursionTimeout;
168. DWORD dwMaxCacheTtl;
169. DWORD dwDsPollingInterval;
170. DWORD dwLocalNetPriorityNetMask;
171. // aging and scavenging
172. DWORD dwScavengingInterval;
173. DWORD dwDefaultRefreshInterval;
174. DWORD dwDefaultNoRefreshInterval;
175. DWORD dwLastScavengeTime;
176. // more logging
177. DWORD dwEventLogLevel;
178. DWORD dwLogFileMaxSize;
179. // Active Directory information
180. DWORD dwDsForestVersion;
181. DWORD dwDsDomainVersion;
182. DWORD dwDsDsaVersion;
183. DWORD dwReserveArray[ 4 ];
184. //
185. // BYTE section
186. //
187. // configuration flags
188. BOOLEAN fAutoReverseZones;
189. BOOLEAN fAutoCacheUpdate;
190. // recursion control
191. BOOLEAN fRecurseAfterForwarding;
192. BOOLEAN fForwardDelegations;
193. BOOLEAN fNoRecursion;
194. BOOLEAN fSecureResponses;
195. // lookup control
196. BOOLEAN fRoundRobin;
197. BOOLEAN fLocalNetPriority;
198. // BIND compatibility and mimicking
199. BOOLEAN fBindSecondaries;
200. BOOLEAN fWriteAuthorityNs;
201. // Bells and whistles
202. BOOLEAN fStrictFileParsing;
203. BOOLEAN fLooseWildcarding;
204. // aging \ scavenging
205. BOOLEAN fDefaultAgingState;
206. BOOLEAN fReserveArray[ 15 ];
207. }
208. DNS\_RPC\_SERVER\_INFO\_DOTNET, \*PDNS\_RPC\_SERVER\_INFO\_DOTNET;
209. typedef struct \_DnsRpcServerInfoLonghorn
210. {
211. DWORD dwRpcStructureVersion;
212. DWORD dwReserved0;
213. // basic configuration flags
214. DWORD dwVersion;
215. UCHAR fBootMethod;
216. BOOLEAN fAdminConfigured;
217. BOOLEAN fAllowUpdate;
218. BOOLEAN fDsAvailable;
219. //
220. // pointer section
221. //
222. [string] char \* pszServerName;
223. // DS container
224. [string] wchar\_t \* pszDsContainer;
225. // IP interfaces
226. PDNS\_ADDR\_ARRAY aipServerAddrs;
227. PDNS\_ADDR\_ARRAY aipListenAddrs;
228. // forwarders
229. PDNS\_ADDR\_ARRAY aipForwarders;
230. // logging
231. PDNS\_ADDR\_ARRAY aipLogFilter;
232. [string] wchar\_t \* pwszLogFilePath;
233. // Server domain/forest
234. [string] char \* pszDomainName; // UTF-8 FQDN
235. [string] char \* pszForestName; // UTF-8 FQDN
236. // Built-in directory partitions
237. [string] char \* pszDomainDirectoryPartition; // UTF-8 FQDN
238. [string] char \* pszForestDirectoryPartition; // UTF-8 FQDN
239. // future extensions
240. [string] char \* pExtensions[ 6 ];
241. //
242. // DWORD section
243. //
244. // logging
245. DWORD dwLogLevel;
246. DWORD dwDebugLevel;
247. // configuration DWORDs
248. DWORD dwForwardTimeout;
249. DWORD dwRpcProtocol;
250. DWORD dwNameCheckFlag;
251. DWORD cAddressAnswerLimit;
252. DWORD dwRecursionRetry;
253. DWORD dwRecursionTimeout;
254. DWORD dwMaxCacheTtl;
255. DWORD dwDsPollingInterval;
256. DWORD dwLocalNetPriorityNetMask;
257. // aging and scavenging
258. DWORD dwScavengingInterval;
259. DWORD dwDefaultRefreshInterval;
260. DWORD dwDefaultNoRefreshInterval;
261. DWORD dwLastScavengeTime;
262. // more logging
263. DWORD dwEventLogLevel;
264. DWORD dwLogFileMaxSize;
265. // Active Directory information
266. DWORD dwDsForestVersion;
267. DWORD dwDsDomainVersion;
268. DWORD dwDsDsaVersion;
269. BOOLEAN fReadOnlyDC;
270. DWORD dwReserveArray[ 3 ];
271. //
272. // BYTE section
273. //
274. // configuration flags
275. BOOLEAN fAutoReverseZones;
276. BOOLEAN fAutoCacheUpdate;
277. // recursion control
278. BOOLEAN fRecurseAfterForwarding;
279. BOOLEAN fForwardDelegations;
280. BOOLEAN fNoRecursion;
281. BOOLEAN fSecureResponses;
282. // lookup control
283. BOOLEAN fRoundRobin;
284. BOOLEAN fLocalNetPriority;
285. // BIND compatibility and mimicking
286. BOOLEAN fBindSecondaries;
287. BOOLEAN fWriteAuthorityNs;
288. // Bells and whistles
289. BOOLEAN fStrictFileParsing;
290. BOOLEAN fLooseWildcarding;
291. // aging \ scavenging
292. BOOLEAN fDefaultAgingState;
293. BOOLEAN fReserveArray[ 15 ];
294. }
295. DNS\_RPC\_SERVER\_INFO\_LONGHORN, \*PDNS\_RPC\_SERVER\_INFO\_LONGHORN, DNS\_RPC\_SERVER\_INFO, \*PDNS\_RPC\_SERVER\_INFO;
296. typedef struct \_DnssrvRpcForwardersW2K
297. {
298. DWORD fRecurseAfterForwarding;
299. DWORD dwForwardTimeout;
300. PIP4\_ARRAY aipForwarders;
301. }
302. DNS\_RPC\_FORWARDERS\_W2K, \*PDNS\_RPC\_FORWARDERS\_W2K;
303. typedef struct \_DnssrvRpcForwardersDotNet
304. {
305. DWORD dwRpcStructureVersion;
306. DWORD dwReserved0;
307. DWORD fRecurseAfterForwarding;
308. DWORD dwForwardTimeout;
309. PIP4\_ARRAY aipForwarders;
310. }
311. DNS\_RPC\_FORWARDERS\_DOTNET, \*PDNS\_RPC\_FORWARDERS\_DOTNET;
312. typedef struct \_DnssrvRpcForwardersLonghorn
313. {
314. DWORD dwRpcStructureVersion;
315. DWORD dwReserved0;
316. DWORD fRecurseAfterForwarding;
317. DWORD dwForwardTimeout;
318. PDNS\_ADDR\_ARRAY aipForwarders;
319. }
320. DNS\_RPC\_FORWARDERS\_LONGHORN, \*PDNS\_RPC\_FORWARDERS\_LONGHORN, DNS\_RPC\_FORWARDERS, \*PDNS\_RPC\_FORWARDERS;
321. //
322. // Basic zone data
323. //
324. //typedef struct \_DnssrvRpcZoneFlags
325. //{
326. // DWORD Paused : 1;
327. // DWORD Shutdown : 1;
328. // DWORD Reverse : 1;
329. // DWORD AutoCreated : 1;
330. // DWORD DsIntegrated : 1;
331. // DWORD Aging : 1;
332. // DWORD Update : 2;
333. // DWORD ReadOnly : 1;
334. // DWORD UnUsed : 23;
335. //}
336. //DNS\_RPC\_ZONE\_FLAGS, \*PDNS\_RPC\_ZONE\_FLAGS;
337. typedef DWORD DNS\_RPC\_ZONE\_FLAGS;
338. typedef struct \_DnssrvRpcZoneW2K
339. {
340. [string] wchar\_t \* pszZoneName;
341. DNS\_RPC\_ZONE\_FLAGS Flags;
342. UCHAR ZoneType;
343. UCHAR Version;
344. }
345. DNS\_RPC\_ZONE\_W2K, \*PDNS\_RPC\_ZONE\_W2K;
346. typedef struct \_DnssrvRpcZoneDotNet
347. {
348. DWORD dwRpcStructureVersion;
349. DWORD dwReserved0;
350. [string] wchar\_t \* pszZoneName;
351. DNS\_RPC\_ZONE\_FLAGS Flags;
352. UCHAR ZoneType;
353. UCHAR Version;
354. DWORD dwDpFlags;
355. [string] char \* pszDpFqdn;
356. }
357. DNS\_RPC\_ZONE\_DOTNET, \*PDNS\_RPC\_ZONE\_DOTNET, DNS\_RPC\_ZONE, \*PDNS\_RPC\_ZONE;
358. //
359. // Zone enumeration
360. //
361. typedef struct \_DnssrvRpcZoneListW2K
362. {
363. [range(0,500000)] DWORD dwZoneCount;
364. [size\_is(dwZoneCount)] PDNS\_RPC\_ZONE\_W2K ZoneArray[];
365. }
366. DNS\_RPC\_ZONE\_LIST\_W2K, \*PDNS\_RPC\_ZONE\_LIST\_W2K;
367. typedef struct \_DnssrvRpcZoneListDotNet
368. {
369. DWORD dwRpcStructureVersion;
370. DWORD dwReserved0;
371. [range(0,500000)] DWORD dwZoneCount;
372. [size\_is(dwZoneCount)] PDNS\_RPC\_ZONE\_DOTNET ZoneArray[];
373. }
374. DNS\_RPC\_ZONE\_LIST\_DOTNET, \*PDNS\_RPC\_ZONE\_LIST\_DOTNET, DNS\_RPC\_ZONE\_LIST, \*PDNS\_RPC\_ZONE\_LIST;
375. //
376. // DNSSEC trust point enumeration
377. //
378. typedef enum
379. {
380. TRUSTPOINT\_STATE\_INITIALIZED,
381. TRUSTPOINT\_STATE\_DSPENDING,
382. TRUSTPOINT\_STATE\_ACTIVE,
383. TRUSTPOINT\_STATE\_DELETE\_PENDING,
384. TRUSTPOINT\_STATE\_DELETED
385. }
386. TRUSTPOINT\_STATE, \*PTRUSTPOINT\_STATE;
387. typedef enum
388. {
389. TRUSTANCHOR\_STATE\_INITIALIZED,
390. TRUSTANCHOR\_STATE\_DSPENDING,
391. TRUSTANCHOR\_STATE\_DSINVALID,
392. TRUSTANCHOR\_STATE\_ADDPEND,
393. TRUSTANCHOR\_STATE\_VALID,
394. TRUSTANCHOR\_STATE\_MISSING,
395. TRUSTANCHOR\_STATE\_REVOKED,
396. TRUSTANCHOR\_STATE\_DELETED
397. }
398. TRUSTANCHOR\_STATE, \*PTRUSTANCHOR\_STATE;
399. typedef struct \_DnssrvRpcTrustPoint
400. {
401. DWORD dwRpcStructureVersion;
402. DWORD dwReserved0;
403. [string] char \* pszTrustPointName;
404. TRUSTPOINT\_STATE eTrustPointState;
405. \_\_int64 i64LastActiveRefreshTime;
406. \_\_int64 i64NextActiveRefreshTime;
407. \_\_int64 i64LastSuccessfulActiveRefreshTime;
408. DWORD dwLastActiveRefreshResult;
409. DWORD dwReserved;
410. }
411. DNS\_RPC\_TRUST\_POINT, \*PDNS\_RPC\_TRUST\_POINT;
412. typedef struct \_DnssrvRpcTrustPointList
413. {
414. DWORD dwRpcStructureVersion;
415. DWORD dwReserved0;
416. [range(0,500000)] DWORD dwTrustPointCount;
417. [size\_is(dwTrustPointCount)] PDNS\_RPC\_TRUST\_POINT TrustPointArray[];
418. }
419. DNS\_RPC\_TRUST\_POINT\_LIST, \*PDNS\_RPC\_TRUST\_POINT\_LIST;
420. //
421. // Signing Key Descriptor (SKD) definitions for online signing
422. //
423. // Each SKD has a set of static configuration represented by a DNS\_RPC\_SKD
424. // structure that defines how the SKD is used to generate keys and sign
425. // records in the zone. Each SKD is uniquely identified by its GUID field,
426. // which is dynamically generated by the DNS server when the SKD is created.
427. // Information on the dynamic state of the SKD, including identifiers for
428. // the current keys associated with the SKD, is represented using the
429. // DNS\_RPC\_SKD\_STATE structure.
430. //
431. // Guid: A unique identifier for this SKD.
432. //
433. // pwszKeyStorageProvider: The KSP to use to generate keys.
434. //
435. // fStoreKeysInDirectory: If TRUE, keys will be stored on the zone object
436. // in Active Directory. If FALSE, keys will be wrapped in self-signed
437. // certificates in the local machine store.
438. //
439. // fIsKSK: TRUE if this SKD represents a Key Signing Key, FALSE for a Zone
440. // Signing Key.
441. //
442. // bSigningAlgorithm: DNSSEC signature generation algorithm.
443. //
444. // dwKeyLength: Length, in bits, of keys. Ignored if the algorithm specified
445. // by bSigningAlgorithm does not support variable-length keys.
446. //
447. // dwInitialRolloverOffset: Amount of time, in seconds, to delay the first
448. // scheduled key rollover. This allows for key rollovers to be staggered.
449. //
450. // dwDNSKEYSignatureValidityPeriod: Amount of time, in seconds, that signatures
451. // covering DNSKEY record sets should be valid.
452. //
453. // dwDSSignatureValidityPeriod: Amount of time, in seconds, that signatures
454. // covering DS record sets should be valid.
455. //
456. // dwStandardSignatureValidityPeriod: Amount of time, in seconds, that signatures
457. // covering all other record sets should be valid.
458. //
459. // dwRolloverType: Key rollover method (see [RFC4641]).
460. //
461. // dwRolloverPeriod: Amount of time, in seconds, between scheduled key rollovers
462. // or 0xFFFFFFFF to disable automatic key rollover.
463. //
464. // dwNextRolloverAction: The action to take for this SKD on the next key
465. // manual or scheduled key rollover event.
466. //
467. typedef struct \_DnssrvRpcSigningKeyDescriptor
468. {
469. DWORD dwRpcStructureVersion;
470. DWORD dwReserved0;
471. GUID Guid;
472. [string] wchar\_t\* pwszKeyStorageProvider;
473. BOOL fStoreKeysInDirectory;
474. BOOL fIsKSK;
475. BYTE bSigningAlgorithm;
476. DWORD dwKeyLength;
477. DWORD dwInitialRolloverOffset;
478. DWORD dwDNSKEYSignatureValidityPeriod;
479. DWORD dwDSSignatureValidityPeriod;
480. DWORD dwStandardSignatureValidityPeriod;
481. DWORD dwRolloverType;
482. DWORD dwRolloverPeriod;
483. DWORD dwNextRolloverAction;
484. DWORD dwReserved;
485. }
486. DNS\_RPC\_SKD, \*PDNS\_RPC\_SKD;
487. //
488. // For dwActiveKeyScope, dwStandByKeyScope, dwNextKeyScope
489. // KeySignScope defines the scope of the key in a signed zone.
490. //
491. typedef enum \_KeySignScope
492. {
493. //
494. // SIGN\_SCOPE\_DEFAULT specifies that the scope will be determined by the
495. // key flags. That is, KSK is used to sign DNSKEY set only and ZSK is
496. // used to sign all record sets.
497. //
499. SIGN\_SCOPE\_DEFAULT,
501. //
502. // A key with SIGN\_SCOPE\_DNSKEY\_ONLY scope will only be used to sign DNSKEY
503. // set. This gives the user a way to override the ZSK flag when signing.
504. //
506. SIGN\_SCOPE\_DNSKEY\_ONLY,
508. //
509. // A key with SIGN\_SCOPE\_ALL\_RECORDS scope will be used to sign all record
510. // sets. This gives the user a way to override the KSK flag when signing.
511. //
513. SIGN\_SCOPE\_ALL\_RECORDS,
515. //
516. // A key with SIGN\_SCOPE\_ADD\_ONLY scope will be added to zone file, but
517. // not used for signing. It is for user to pre-publish a key.
518. //
520. SIGN\_SCOPE\_ADD\_ONLY,
521. //
522. // A key with SIGN\_SCOPE\_DO\_NOT\_PUBLISH will not be added to the zone file,
523. // and will not be used for signing. It's used to remove a key.
524. //
525. SIGN\_SCOPE\_DO\_NOT\_PUBLISH,
526. //
527. // A key with SIGN\_SCOPE\_REVOKED will be published to the zone with its
528. // "revoked" bit set to TRUE, and will be used to sign the DNSKEY set only.
529. //
530. SIGN\_SCOPE\_REVOKED
531. } KeySignScope;
532. //
533. // Signing Key Descriptor (SKD) dynamic state extended
534. //
535. //
536. // Guid: Unique identifier for the SKD
537. //
538. // dwCurrentRollState: Internal Status for Rollover.
539. //
540. // fManualTrigger: TRUE if Rollover was triggered manually.
541. //
542. // dwPreRollEventFired: Specifies which Pre Rollover Event has been fired
543. //
544. // ftNextKeyGenerationTime: Time at which Next Key was added to the zone.
545. //
546. // dwRevokedOrSwappedDnskeysLength: Length of the Revoked or Swaped DNSKEY RRSet
547. //
548. // pRevokedOrSwappedDnskeysBuffer: Pre-Signed DNSKEY RRSet for ZSK swap
549. //
550. // dwFinalDnskeysLength: Length of Pre-Signed DNSKEY RRSet
551. //
552. // pFinalDnskeys: Pre-Signed DNSKEY RRSet Post Rollover
553. //
554. // eActiveKeyScope: Signing key Scope for the SKD's active key.
555. //
556. // eStandbyKeyScope: Signing key Scope for the SKD's standby key.
557. //
558. // eNextKeyScope: Signing key Scope for the SKD's next key.
559. //
560. typedef struct \_DnsRpcSigningKeyDescriptorStateEx
561. {
562. DWORD dwRpcStructureVersion;
563. DWORD dwReserved0;
564. GUID Guid;
565. DWORD dwCurrentRollState;
566. DWORD fManualTrigger;
567. DWORD dwPreRollEventFired;
568. FILETIME ftNextKeyGenerationTime;
569. DWORD dwRevokedOrSwappedDnskeysLength;
570. PBYTE pRevokedOrSwappedDnskeysBuffer;
571. DWORD dwFinalDnskeysLength;
572. PBYTE pFinalDnskeys;
573. KeySignScope eActiveKeyScope;
574. KeySignScope eStandByKeyScope;
575. KeySignScope eNextKeyScope;
576. }
577. DNS\_RPC\_SKD\_STATE\_EX, \*PDNS\_RPC\_SKD\_STATE\_EX;
578. //
579. // Signing Key Descriptor (SKD) dynamic state
580. //
581. // The static configuration for each SKD is represented by a DNS\_RPC\_SKD
582. // structure. In addition to these static configuration parameters, each SKD
583. // also has dynamic configuration associated with it, including pointers to
584. // the current keys for the SKD and other information. The collection of
585. // dynamic configuration information for each SKD is represented by a
586. // DNS\_RPC\_SKD\_STATE structure.
587. //
588. // A signing key pointer string contains a unique identifier for a signing
589. // key. For keys stored in the local machine certificate store, this
590. // identifier is the certificate serial number. For keys stored in Active
591. // Directory, this identifier is a GUID. The matching GUID for a key may be
592. // found in one of the values of the key attribute on the zone object along
593. // with a binary exported representation of the key. Note that the GUID for
594. // a key is not directly related to the GUID for the SKD.
595. //
596. // Guid: Unique identifier for the SKD
597. //
598. // ftLastRolloverTime: The time at which the last rollover event was performed.
599. //
600. // ftNextRolloverTime: The time at which the next rollover action must take place.
601. //
602. // dwState: The current state of this SKD.
603. //
604. // dwCurrentRolloverStatus: Current rollover status of this SKD.
605. //
606. // pwszActiveKey: Signing key pointer string for the SKD's active key.
607. //
608. // pwszStandbyKey: Signing key pointer string for the SKD's standby key.
609. //
610. // pwszNextKey: Signing key pointer string for the SKD's next key. This key
611. // will be used during the next key rollover event.
612. //
613. typedef struct \_DnsRpcSigningKeyDescriptorState
614. {
615. DWORD dwRpcStructureVersion;
616. DWORD dwReserved0;
617. GUID Guid;
618. FILETIME ftLastRolloverTime;
619. FILETIME ftNextRolloverTime;
620. DWORD dwState;
621. DWORD dwCurrentRolloverStatus;
622. [string] wchar\_t \* pwszActiveKey;
623. [string] wchar\_t \* pwszStandbyKey;
624. [string] wchar\_t \* pwszNextKey;
625. DWORD dwReserved;
626. }
627. DNS\_RPC\_SKD\_STATE, \*PDNS\_RPC\_SKD\_STATE;
628. //
629. // Signing Key Descriptor (SKD) Properties for a zone.
630. //
631. // pSKd Static properties of a Zone SKD. This is a DNS\_RP\_SKD structure
632. //
633. // psKdState Dynamic properties of a Zone SKD. This is a DNS\_RP\_SKD\_STATE structure
634. //
635. // psKdStateEx Extended Dynamic properties of a Zone SKD. This is a DNS\_RP\_SKD\_STATE\_EX // structure
636. typedef struct \_DnssrvRpcZoneSKDSettings
637. {
638. DWORD dwRpcStructureVersion;
639. DWORD dwReserved0;
640. PDNS\_RPC\_SKD pSkd;
641. PDNS\_RPC\_SKD\_STATE pSkdState;
642. PDNS\_RPC\_SKD\_STATE\_EX pSkdStateEx;
644. } DNS\_RPC\_ZONE\_SKD, \*PDNS\_RPC\_ZONE\_SKD;
645. //
646. // DNSSEC Settings of a Zone
648. typedef struct \_DnssrvRpcZoneDnssecSettings
649. {
650. DWORD dwRpcStructureVersion;
651. DWORD dwReserved0;
652. DWORD fIsSigned;
653. DWORD fSignWithNSEC3;
654. DWORD fNSEC3OptOut;
655. DWORD dwMaintainTrustAnchor;
656. DWORD fParentHasSecureDelegation;
657. DWORD dwDSRecordAlgorithms;
658. DWORD fRFC5011KeyRollovers;
659. BYTE bNSEC3HashAlgorithm;
660. BYTE bNSEC3RandomSaltLength;
661. WORD wNSEC3IterationCount;
662. LPWSTR pwszNSEC3UserSalt;
663. DWORD dwDNSKEYRecordSetTtl;
664. DWORD dwDSRecordSetTtl;
665. DWORD dwSignatureInceptionOffset;
666. DWORD dwSecureDelegationPollingPeriod;
667. DWORD dwPropagationTime;
668. DWORD cbNSEC3CurrentSaltLength;
669. PBYTE pbNSEC3CurrentSalt;
670. GUID CurrentRollingSKDGuid;
671. DWORD dwBufferLength;
672. PBYTE pBuffer;
673. DWORD dwCount;
674. PDNS\_RPC\_ZONE\_SKD pZoneSkdArray[1] ;
675. } DNS\_RPC\_ZONE\_DNSSEC\_SETTINGS, \*PDNS\_RPC\_ZONE\_DNSSEC\_SETTINGS;
676. typedef struct \_DnssrvRpcTrustAnchor
677. {
678. DWORD dwRpcStructureVersion;
679. DWORD dwReserved0;
680. WORD wTrustAnchorType;
681. WORD wKeyTag;
682. WORD wRRLength;
683. TRUSTANCHOR\_STATE eTrustAnchorState;
684. \_\_int64 i64EnteredStateTime;
685. \_\_int64 i64NextStateTime;
686. DWORD dwReserved;
687. [size\_is(wRRLength)]
688. BYTE RRData[];
689. }
690. DNS\_RPC\_TRUST\_ANCHOR, \*PDNS\_RPC\_TRUST\_ANCHOR;
691. typedef struct \_DnssrvRpcTrustAnchorList
692. {
693. DWORD dwRpcStructureVersion;
694. DWORD dwReserved0;
695. [range(0,500000)] DWORD dwTrustAnchorCount;
696. [size\_is(dwTrustAnchorCount)] PDNS\_RPC\_TRUST\_ANCHOR TrustAnchorArray[];
697. }
698. DNS\_RPC\_TRUST\_ANCHOR\_LIST, \*PDNS\_RPC\_TRUST\_ANCHOR\_LIST;
699. //
700. // Directory partition enumeration and info
701. //
702. typedef struct \_DnssrvRpcDirectoryPartitionEnum
703. {
704. DWORD dwRpcStructureVersion;
705. DWORD dwReserved0;
706. [string] char \* pszDpFqdn;
707. DWORD dwFlags;
708. DWORD dwZoneCount;
709. }
710. DNS\_RPC\_DP\_ENUM, \*PDNS\_RPC\_DP\_ENUM;
711. typedef struct \_DnssrvRpcDirectoryPartitionList
712. {
713. DWORD dwRpcStructureVersion;
714. DWORD dwReserved0;
715. [range(0,5000)] DWORD dwDpCount;
716. [size\_is(dwDpCount)] PDNS\_RPC\_DP\_ENUM DpArray[];
717. }
718. DNS\_RPC\_DP\_LIST, \*PDNS\_RPC\_DP\_LIST;
719. typedef struct \_DnssrvRpcDirectoryPartitionReplica
720. {
721. [string] wchar\_t \* pszReplicaDn;
722. }
723. DNS\_RPC\_DP\_REPLICA, \*PDNS\_RPC\_DP\_REPLICA;
724. typedef struct \_DnssrvRpcDirectoryPartition
725. {
726. DWORD dwRpcStructureVersion;
727. DWORD dwReserved0;
728. [string] char \* pszDpFqdn;
729. [string] wchar\_t \* pszDpDn;
730. [string] wchar\_t \* pszCrDn;
731. DWORD dwFlags;
732. DWORD dwZoneCount;
733. DWORD dwState;
734. DWORD dwReserved[ 3 ];
735. [string] wchar\_t \* pwszReserved[ 3 ];
736. [range(0,10000)] DWORD dwReplicaCount;
737. [size\_is(dwReplicaCount)] PDNS\_RPC\_DP\_REPLICA ReplicaArray[];
738. }
739. DNS\_RPC\_DP\_INFO, \*PDNS\_RPC\_DP\_INFO;
740. //
741. // Enlist (or create) directory partition
742. //
743. typedef struct \_DnssrvRpcEnlistDirPart
744. {
745. DWORD dwRpcStructureVersion;
746. DWORD dwReserved0;
747. [string] char \* pszDpFqdn; // UTF8
748. DWORD dwOperation;
749. }
750. DNS\_RPC\_ENLIST\_DP, \*PDNS\_RPC\_ENLIST\_DP;
751. //
752. // Zone export
753. //
754. typedef struct \_DnssrvRpcZoneExport
755. {
756. DWORD dwRpcStructureVersion;
757. DWORD dwReserved0;
758. [string] char \* pszZoneExportFile;
759. }
760. DNS\_RPC\_ZONE\_EXPORT\_INFO, \*PDNS\_RPC\_ZONE\_EXPORT\_INFO;
761. //
762. // Zone property data
763. //
764. typedef struct \_DnssrvRpcZoneSecondariesW2K
765. {
766. DWORD fSecureSecondaries;
767. DWORD fNotifyLevel;
768. PIP4\_ARRAY aipSecondaries;
769. PIP4\_ARRAY aipNotify;
770. }
771. DNS\_RPC\_ZONE\_SECONDARIES\_W2K, \*PDNS\_RPC\_ZONE\_SECONDARIES\_W2K;
772. typedef struct \_DnssrvRpcZoneSecondariesDotNet
773. {
774. DWORD dwRpcStructureVersion;
775. DWORD dwReserved0;
776. DWORD fSecureSecondaries;
777. DWORD fNotifyLevel;
778. PIP4\_ARRAY aipSecondaries;
779. PIP4\_ARRAY aipNotify;
780. }
781. DNS\_RPC\_ZONE\_SECONDARIES\_DOTNET, \*PDNS\_RPC\_ZONE\_SECONDARIES\_DOTNET;
782. typedef struct \_DnssrvRpcZoneSecondariesLonghorn
783. {
784. DWORD dwRpcStructureVersion;
785. DWORD dwReserved0;
786. DWORD fSecureSecondaries;
787. DWORD fNotifyLevel;
788. PDNS\_ADDR\_ARRAY aipSecondaries;
789. PDNS\_ADDR\_ARRAY aipNotify;
790. }
791. DNS\_RPC\_ZONE\_SECONDARIES\_LONGHORN, \*PDNS\_RPC\_ZONE\_SECONDARIES\_LONGHORN, DNS\_RPC\_ZONE\_SECONDARIES, \*PDNS\_RPC\_ZONE\_SECONDARIES;
792. typedef struct \_DnssrvRpcZoneDatabaseW2K
793. {
794. DWORD fDsIntegrated;
795. [string] char \* pszFileName;
796. }
797. DNS\_RPC\_ZONE\_DATABASE\_W2K, \*PDNS\_RPC\_ZONE\_DATABASE\_W2K;
798. typedef struct \_DnssrvRpcZoneDatabaseDotNet
799. {
800. DWORD dwRpcStructureVersion;
801. DWORD dwReserved0;
802. DWORD fDsIntegrated;
803. [string] char \* pszFileName;
804. }
805. DNS\_RPC\_ZONE\_DATABASE\_DOTNET, \*PDNS\_RPC\_ZONE\_DATABASE\_DOTNET, DNS\_RPC\_ZONE\_DATABASE, \*PDNS\_RPC\_ZONE\_DATABASE;
806. typedef struct \_DnssrvRpcZoneChangePartition
807. {
808. DWORD dwRpcStructureVersion;
809. DWORD dwReserved0;
810. [string] char \* pszDestPartition;
811. }
812. DNS\_RPC\_ZONE\_CHANGE\_DP, \*PDNS\_RPC\_ZONE\_CHANGE\_DP;
813. typedef struct \_DnsRpcZoneInfoW2K
814. {
815. [string] char \* pszZoneName;
816. DWORD dwZoneType;
817. DWORD fReverse;
818. DWORD fAllowUpdate;
819. DWORD fPaused;
820. DWORD fShutdown;
821. DWORD fAutoCreated;
822. // Database info
823. DWORD fUseDatabase;
824. [string] char \* pszDataFile;
825. // Masters
826. PIP4\_ARRAY aipMasters;
827. // Secondaries
828. DWORD fSecureSecondaries;
829. DWORD fNotifyLevel;
830. PIP4\_ARRAY aipSecondaries;
831. PIP4\_ARRAY aipNotify;
832. // WINS or NetBIOS lookup
833. DWORD fUseWins;
834. DWORD fUseNbstat;
835. // Aging
836. DWORD fAging;
837. DWORD dwNoRefreshInterval;
838. DWORD dwRefreshInterval;
839. DWORD dwAvailForScavengeTime;
840. PIP4\_ARRAY aipScavengeServers;
841. // save some space, just in case
842. // avoid versioning issues if possible
843. DWORD pvReserved1;
844. DWORD pvReserved2;
845. DWORD pvReserved3;
846. DWORD pvReserved4;
847. }
848. DNS\_RPC\_ZONE\_INFO\_W2K, \*PDNS\_RPC\_ZONE\_INFO\_W2K;
849. typedef struct \_DnsRpcZoneInfoDotNet
850. {
851. DWORD dwRpcStructureVersion;
852. DWORD dwReserved0;
853. [string] char \* pszZoneName;
854. DWORD dwZoneType;
855. DWORD fReverse;
856. DWORD fAllowUpdate;
857. DWORD fPaused;
858. DWORD fShutdown;
859. DWORD fAutoCreated;
860. // Database info
861. DWORD fUseDatabase;
862. [string] char \* pszDataFile;
863. // Masters
864. PIP4\_ARRAY aipMasters;
865. // Secondaries
866. DWORD fSecureSecondaries;
867. DWORD fNotifyLevel;
868. PIP4\_ARRAY aipSecondaries;
869. PIP4\_ARRAY aipNotify;
870. // WINS or NetBIOS lookup
871. DWORD fUseWins;
872. DWORD fUseNbstat;
873. // Aging
874. DWORD fAging;
875. DWORD dwNoRefreshInterval;
876. DWORD dwRefreshInterval;
877. DWORD dwAvailForScavengeTime;
878. PIP4\_ARRAY aipScavengeServers;
879. // Forwarder zones
880. DWORD dwForwarderTimeout;
881. DWORD fForwarderSlave;
882. // Stub zones
883. PIP4\_ARRAY aipLocalMasters;
884. // Directory partition
885. DWORD dwDpFlags;
886. [string] char \* pszDpFqdn;
887. [string] wchar\_t \* pwszZoneDn;
888. // Xfr time information
889. DWORD dwLastSuccessfulSoaCheck;
890. DWORD dwLastSuccessfulXfr;
891. // save some space, just in case
892. DWORD dwReserved1;
893. DWORD dwReserved2;
894. DWORD dwReserved3;
895. DWORD dwReserved4;
896. DWORD dwReserved5;
897. [string] char \* pReserved1;
898. [string] char \* pReserved2;
899. [string] char \* pReserved3;
900. [string] char \* pReserved4;
901. }
902. DNS\_RPC\_ZONE\_INFO\_DOTNET, \*PDNS\_RPC\_ZONE\_INFO\_DOTNET;
903. typedef struct \_DnsRpcZoneInfoLonghorn
904. {
905. DWORD dwRpcStructureVersion;
906. DWORD dwReserved0;
907. [string] char \* pszZoneName;
908. DWORD dwZoneType;
909. DWORD fReverse;
910. DWORD fAllowUpdate;
911. DWORD fPaused;
912. DWORD fShutdown;
913. DWORD fAutoCreated;
914. // Database info
915. DWORD fUseDatabase;
916. [string] char \* pszDataFile;
917. // Masters
918. PDNS\_ADDR\_ARRAY aipMasters;
919. // Secondaries
920. DWORD fSecureSecondaries;
921. DWORD fNotifyLevel;
922. PDNS\_ADDR\_ARRAY aipSecondaries;
923. PDNS\_ADDR\_ARRAY aipNotify;
924. // WINS or NetBIOS lookup
925. DWORD fUseWins;
926. DWORD fUseNbstat;
927. // Aging
928. DWORD fAging;
929. DWORD dwNoRefreshInterval;
930. DWORD dwRefreshInterval;
931. DWORD dwAvailForScavengeTime;
932. PDNS\_ADDR\_ARRAY aipScavengeServers;
933. // Forwarder zones
934. DWORD dwForwarderTimeout;
935. DWORD fForwarderSlave;
936. // Stub zones
937. PDNS\_ADDR\_ARRAY aipLocalMasters;
938. // Directory partition
939. DWORD dwDpFlags;
940. [string] char \* pszDpFqdn;
941. [string] wchar\_t \* pwszZoneDn;
942. // Xfr time information
943. DWORD dwLastSuccessfulSoaCheck;
944. DWORD dwLastSuccessfulXfr;
945. DWORD fQueuedForBackgroundLoad;
946. DWORD fBackgroundLoadInProgress;
947. BOOL fReadOnlyZone;
948. // Additional zone transfer information
949. DWORD dwLastXfrAttempt;
950. DWORD dwLastXfrResult;
951. }
952. DNS\_RPC\_ZONE\_INFO\_LONGHORN, \*PDNS\_RPC\_ZONE\_INFO\_LONGHORN, DNS\_RPC\_ZONE\_INFO, \*PDNS\_RPC\_ZONE\_INFO;
953. //
954. // Zone create data
955. //
956. typedef struct \_DnsRpcZoneCreateInfo
957. {
958. [string] char \* pszZoneName;
959. DWORD dwZoneType;
960. DWORD fAllowUpdate;
961. DWORD fAging;
962. DWORD dwFlags;
963. // Database info
964. [string] char \* pszDataFile;
965. DWORD fDsIntegrated;
966. DWORD fLoadExisting;
967. // Admin name (if auto-create SOA)
968. [string] char \* pszAdmin;
969. // Masters (if secondary)
970. PIP4\_ARRAY aipMasters;
971. // Secondaries
972. PIP4\_ARRAY aipSecondaries;
973. DWORD fSecureSecondaries;
974. DWORD fNotifyLevel;
975. // Reserve some space to avoid versioning issues
976. [string] char \* pvReserved1;
977. [string] char \* pvReserved2;
978. [string] char \* pvReserved3;
979. [string] char \* pvReserved4;
980. [string] char \* pvReserved5;
981. [string] char \* pvReserved6;
982. [string] char \* pvReserved7;
983. [string] char \* pvReserved8;
984. DWORD dwReserved1;
985. DWORD dwReserved2;
986. DWORD dwReserved3;
987. DWORD dwReserved4;
988. DWORD dwReserved5;
989. DWORD dwReserved6;
990. DWORD dwReserved7;
991. DWORD dwReserved8;
992. }
993. DNS\_RPC\_ZONE\_CREATE\_INFO\_W2K, \*PDNS\_RPC\_ZONE\_CREATE\_INFO\_W2K;
994. typedef struct \_DnsRpcZoneCreateInfoDotNet
995. {
996. DWORD dwRpcStructureVersion;
997. DWORD dwReserved0;
998. [string] char \* pszZoneName;
999. DWORD dwZoneType;
1000. DWORD fAllowUpdate;
1001. DWORD fAging;
1002. DWORD dwFlags;
1003. // Database info
1004. [string] char \* pszDataFile;
1005. DWORD fDsIntegrated;
1006. DWORD fLoadExisting;
1007. // Admin name (if auto-create SOA)
1008. [string] char \* pszAdmin;
1009. // Masters (if secondary)
1010. PIP4\_ARRAY aipMasters;
1011. // Secondaries
1012. PIP4\_ARRAY aipSecondaries;
1013. DWORD fSecureSecondaries;
1014. DWORD fNotifyLevel;
1015. // Forwarder zones
1016. DWORD dwTimeout;
1017. DWORD fRecurseAfterForwarding;
1018. // Directory partition
1019. DWORD dwDpFlags; // specify built-in DP or
1020. [string] char \* pszDpFqdn; // UTF8 FQDN of partition
1021. DWORD dwReserved[ 32 ];
1022. }
1023. DNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET, \*PDNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET;
1024. typedef struct \_DnsRpcZoneCreateInfoLonghorn
1025. {
1026. DWORD dwRpcStructureVersion;
1027. DWORD dwReserved0;
1028. [string] char \* pszZoneName;
1029. DWORD dwZoneType;
1030. DWORD fAllowUpdate;
1031. DWORD fAging;
1032. DWORD dwFlags;
1033. // Database info
1034. [string] char \* pszDataFile;
1035. DWORD fDsIntegrated;
1036. DWORD fLoadExisting;
1037. // Admin name (if auto-create SOA)
1038. [string] char \* pszAdmin;
1039. // Masters (if secondary)
1040. PDNS\_ADDR\_ARRAY aipMasters;
1041. // Secondaries
1042. PDNS\_ADDR\_ARRAY aipSecondaries;
1043. DWORD fSecureSecondaries;
1044. DWORD fNotifyLevel;
1045. // Forwarder zones
1046. DWORD dwTimeout;
1047. DWORD fRecurseAfterForwarding;
1048. // Directory partition
1049. DWORD dwDpFlags; // specify built-in DP or
1050. [string] char \* pszDpFqdn; // UTF8 FQDN of partition
1051. DWORD dwReserved[ 32 ];
1052. }
1053. DNS\_RPC\_ZONE\_CREATE\_INFO\_LONGHORN, \*PDNS\_RPC\_ZONE\_CREATE\_INFO\_LONGHORN, DNS\_RPC\_ZONE\_CREATE\_INFO, \*PDNS\_RPC\_ZONE\_CREATE\_INFO;
1054. //
1055. // SKD collection used to enumerate the SKDs for a zone
1056. //
1057. typedef struct \_DnssrvRpcZoneSigningKeyList
1058. {
1059. DWORD dwRpcStructureVersion;
1060. DWORD dwReserved0;
1061. [range(0,1000)] DWORD dwCount;
1062. [size\_is(dwCount)] PDNS\_RPC\_SKD SkdArray[];
1063. }
1064. DNS\_RPC\_SKD\_LIST, \*PDNS\_RPC\_SKD\_LIST;
1065. //
1066. // Online signing validation output structure: this structure is an output
1067. // of the validation operation. If the zone signing parameters are found to
1068. // contain an error or a problem, this structure specifies the GUID of the SKD
1069. // (if any) and the specific key (if any) and the error code.
1070. //
1071. typedef struct \_DnssrvRpcSigningValidationError
1072. {
1073. DWORD dwRpcStructureVersion;
1074. DWORD dwReserved0;
1075. GUID guidSKD;
1076. [string] wchar\_t \* pwszSigningKeyPointerString;
1077. DWORD dwExtendedError;
1078. DWORD dwReserved;
1079. }
1080. DNS\_RPC\_SIGNING\_VALIDATION\_ERROR, \*PDNS\_RPC\_SIGNING\_VALIDATION\_ERROR;
1081. typedef struct \_DnsRpcAutoConfigureLonghorn
1082. {
1083. DWORD dwRpcStructureVersion;
1084. DWORD dwReserved0;
1085. DWORD dwAutoConfigFlags;
1086. DWORD dwReserved1;
1087. [string] char \* pszNewDomainName;
1088. }
1089. DNS\_RPC\_AUTOCONFIGURE, \*PDNS\_RPC\_AUTOCONFIGURE;
1090. //
1091. // EnumZones2 filter specification
1092. //
1093. typedef struct \_DnsRpcEnumZonesFilter
1094. {
1095. DWORD dwRpcStructureVersion;
1096. DWORD dwReserved0;
1097. DWORD dwFilter;
1098. [string] char \* pszPartitionFqdn;
1099. [string] char \* pszQueryString;
1100. [string] char \* pszReserved[ 6 ];
1101. }
1102. DNS\_RPC\_ENUM\_ZONES\_FILTER, \*PDNS\_RPC\_ENUM\_ZONES\_FILTER;
1103. //
1104. // RPC record structure
1105. //
1106. typedef struct \_DnssrvRpcRecord
1107. {
1108. WORD wDataLength;
1109. WORD wType;
1110. DWORD dwFlags;
1111. DWORD dwSerial;
1112. DWORD dwTtlSeconds;
1113. DWORD dwTimeStamp;
1114. DWORD dwReserved;
1115. [size\_is(wDataLength)] BYTE Buffer[];
1116. }
1117. DNS\_RPC\_RECORD, \*PDNS\_RPC\_RECORD,
1118. DNS\_FLAT\_RECORD, \*PDNS\_FLAT\_RECORD;
1119. //
1120. // These RPC structures have no version because they are simple
1121. // are they are explicitly defined by their names.
1122. //
1123. typedef struct \_DnssrvRpcNameAndParam
1124. {
1125. DWORD dwParam;
1126. [string] char \* pszNodeName;
1127. }
1128. DNS\_RPC\_NAME\_AND\_PARAM, \*PDNS\_RPC\_NAME\_AND\_PARAM;
1129. typedef struct \_DnsRpcIPValidateLonghorn
1130. {
1131. DWORD dwRpcStructureVersion;
1132. DWORD dwReserved0;
1133. DWORD dwContext;
1134. DWORD dwReserved1;
1135. [string] char \* pszContextName;
1136. PDNS\_ADDR\_ARRAY aipValidateAddrs;
1137. }
1138. DNS\_RPC\_IP\_VALIDATE, \*PDNS\_RPC\_IP\_VALIDATE;
1139. //
1140. // String array
1141. //
1142. typedef struct \_DnsRpcUtf8StringList
1143. {
1144. [range(0,10000)] DWORD dwCount;
1145. [size\_is(dwCount),string] char \* pszStrings[];
1146. }
1147. DNS\_RPC\_UTF8\_STRING\_LIST, \*PDNS\_RPC\_UTF8\_STRING\_LIST;
1148. typedef struct \_DnsRpcUnicodeStringList
1149. {
1150. [range(0,10000)] DWORD dwCount;
1151. [size\_is(dwCount),string] wchar\_t \* pwszStrings[];
1152. }
1153. DNS\_RPC\_UNICODE\_STRING\_LIST, \*PDNS\_RPC\_UNICODE\_STRING\_LIST;
1154. typedef enum
1155. {
1156. Equals=1,
1157. NotEquals
1158. }
1159. DNS\_RPC\_CRITERIA\_COMPARATOR;
1160. typedef enum
1161. {
1162. DNS\_AND,
1163. DNS\_OR
1164. }
1165. DNS\_RPC\_POLICY\_CONDITION;
1166. typedef enum
1167. {
1168. DnsPolicyServerLevel,
1169. DnsPolicyZoneLevel,
1170. DnsPolicyLevelMax
1171. }DNS\_RPC\_POLICY\_LEVEL;
1172. typedef enum
1173. {
1174. DnsPolicyDeny,
1175. DnsPolicyAllow,
1176. DnsPolicyIgnore,
1177. DnsPolicyActionMax
1178. }DNS\_RPC\_POLICY\_ACTION\_TYPE;
1179. typedef enum
1180. {
1181. DnsPolicyQueryProcessing,
1182. DnsPolicyZoneTransfer,
1183. DnsPolicyDynamicUpdate,
1184. DnsPolicyRecursion,
1185. DnsPolicyMax
1186. } DNS\_RPC\_POLICY\_TYPE;
1187. typedef enum {
1188. DnsPolicyCriteriaSubnet,
1189. DnsPolicyCriteriaTransportProtocol,
1190. DnsPolicyCriteriaNetworkProtocol,
1191. DnsPolicyCriteriaInterface,
1192. DnsPolicyCriteriaFqdn,
1193. DnsPolicyCriteriaQtype,
1194. DnsPolicyCriteriaTime,
1195. DnsPolicyCriteriaMax
1196. }DNS\_RPC\_CRITERIA\_ENUM;
1197. typedef struct \_ClientSubnetRecord
1198. {
1199. LPWSTR pwszClientSubnetName;
1200. PDNS\_ADDR\_ARRAY pIPAddr;
1201. PDNS\_ADDR\_ARRAY pIPv6Addr;
1202. }DNS\_RPC\_CLIENT\_SUBNET\_RECORD,\*PDNS\_RPC\_CLIENT\_SUBNET\_RECORD;
1203. typedef struct \_DnssrvRpcPolicyActionContent
1204. {
1205. LPWSTR pwszScopeName;
1206. DWORD dwWeight;
1207. }DNS\_RPC\_POLICY\_CONTENT, \* PDNS\_RPC\_POLICY\_CONTENT;
1208. typedef struct \_DnssrvRpcPolicyAction
1209. {
1210. [range (0,50000)] DWORD dwContentCount;
1211. [size\_is (dwContentCount)] PDNS\_RPC\_POLICY\_CONTENT pContent[];
1212. }DNS\_RPC\_POLICY\_CONTENT\_LIST, \* PDNS\_RPC\_POLICY\_CONTENT\_LIST;
1213. typedef struct \_CriteriaList
1214. {
1215. DNS\_RPC\_CRITERIA\_ENUM type;
1216. LPWSTR pCriteria;
1217. }DNS\_RPC\_CRITERIA,\*PDNS\_RPC\_CRITERIA;
1218. typedef struct \_DnssrvRpcPolicy
1219. {
1220. LPWSTR pwszPolicyName;
1221. DNS\_RPC\_POLICY\_LEVEL level;
1222. DNS\_RPC\_POLICY\_TYPE appliesOn;
1223. DNS\_RPC\_POLICY\_ACTION\_TYPE action;
1224. DNS\_RPC\_POLICY\_CONDITION condition;
1225. BOOL isEnabled;
1226. DWORD dwProcessingOrder;
1227. LPSTR pszZoneName;
1228. PDNS\_RPC\_POLICY\_CONTENT\_LIST pContentList;
1229. DWORDLONG flags;
1230. [range (0,50000)] DWORD dwCriteriaCount;
1231. [size\_is (dwCriteriaCount)] PDNS\_RPC\_CRITERIA pCriteriaList[];
1232. }DNS\_RPC\_POLICY, \*PDNS\_RPC\_POLICY;
1233. typedef struct \_DnsRpcPolicyType {
1234. LPWSTR pwszPolicyName;
1235. DNS\_RPC\_POLICY\_TYPE appliesOn;
1236. BOOL fEnabled;
1237. DWORD processingOrder;
1238. }DNS\_RPC\_POLICY\_NAME, \* PDNS\_RPC\_POLICY\_NAME;
1239. typedef struct \_DnsRpcEnumPolicyList
1240. {
1241. [range(0,50000)] DWORD dwPolicyCount;
1242. [size\_is(dwPolicyCount)] PDNS\_RPC\_POLICY\_NAME pPolicyArray[];
1243. } DNS\_RPC\_ENUMERATE\_POLICY\_LIST, \* PDNS\_RPC\_ENUMERATE\_POLICY\_LIST;
1244. //
1245. // Union of RPC types
1246. //
1247. typedef enum \_DnssrvRpcTypeId
1248. {
1249. DNSSRV\_TYPEID\_NULL = 0,
1250. DNSSRV\_TYPEID\_DWORD,
1251. DNSSRV\_TYPEID\_LPSTR,
1252. DNSSRV\_TYPEID\_LPWSTR,
1253. DNSSRV\_TYPEID\_IPARRAY,
1254. DNSSRV\_TYPEID\_BUFFER, // 5
1255. DNSSRV\_TYPEID\_SERVER\_INFO\_W2K,
1256. DNSSRV\_TYPEID\_STATS,
1257. DNSSRV\_TYPEID\_FORWARDERS\_W2K,
1258. DNSSRV\_TYPEID\_ZONE\_W2K,
1259. DNSSRV\_TYPEID\_ZONE\_INFO\_W2K, // 10
1260. DNSSRV\_TYPEID\_ZONE\_SECONDARIES\_W2K,
1261. DNSSRV\_TYPEID\_ZONE\_DATABASE\_W2K,
1262. DNSSRV\_TYPEID\_ZONE\_TYPE\_RESET\_W2K,
1263. DNSSRV\_TYPEID\_ZONE\_CREATE\_W2K,
1264. DNSSRV\_TYPEID\_NAME\_AND\_PARAM, // 15
1265. DNSSRV\_TYPEID\_ZONE\_LIST\_W2K,
1266. DNSSRV\_TYPEID\_ZONE\_RENAME,
1267. DNSSRV\_TYPEID\_ZONE\_EXPORT,
1268. DNSSRV\_TYPEID\_SERVER\_INFO\_DOTNET,
1269. DNSSRV\_TYPEID\_FORWARDERS\_DOTNET, // 20
1270. DNSSRV\_TYPEID\_ZONE,
1271. DNSSRV\_TYPEID\_ZONE\_INFO\_DOTNET,
1272. DNSSRV\_TYPEID\_ZONE\_SECONDARIES\_DOTNET,
1273. DNSSRV\_TYPEID\_ZONE\_DATABASE,
1274. DNSSRV\_TYPEID\_ZONE\_TYPE\_RESET\_DOTNET, // 25
1275. DNSSRV\_TYPEID\_ZONE\_CREATE\_DOTNET,
1276. DNSSRV\_TYPEID\_ZONE\_LIST,
1277. DNSSRV\_TYPEID\_DP\_ENUM,
1278. DNSSRV\_TYPEID\_DP\_INFO,
1279. DNSSRV\_TYPEID\_DP\_LIST, // 30
1280. DNSSRV\_TYPEID\_ENLIST\_DP,
1281. DNSSRV\_TYPEID\_ZONE\_CHANGE\_DP,
1282. DNSSRV\_TYPEID\_ENUM\_ZONES\_FILTER,
1283. DNSSRV\_TYPEID\_ADDRARRAY,
1284. DNSSRV\_TYPEID\_SERVER\_INFO, // 35
1285. DNSSRV\_TYPEID\_ZONE\_INFO,
1286. DNSSRV\_TYPEID\_FORWARDERS,
1287. DNSSRV\_TYPEID\_ZONE\_SECONDARIES,
1288. DNSSRV\_TYPEID\_ZONE\_TYPE\_RESET,
1289. DNSSRV\_TYPEID\_ZONE\_CREATE, // 40
1290. DNSSRV\_TYPEID\_IP\_VALIDATE,
1291. DNSSRV\_TYPEID\_AUTOCONFIGURE,
1292. DNSSRV\_TYPEID\_UTF8\_STRING\_LIST,
1293. DNSSRV\_TYPEID\_UNICODE\_STRING\_LIST,
1294. DNSSRV\_TYPEID\_SKD, // 45
1295. DNSSRV\_TYPEID\_SKD\_LIST,
1296. DNSSRV\_TYPEID\_SKD\_STATE,
1297. DNSSRV\_TYPEID\_SIGNING\_VALIDATION\_ERROR,
1298. DNSSRV\_TYPEID\_TRUST\_POINT\_LIST,
1299. DNSSRV\_TYPEID\_TRUST\_ANCHOR\_LIST, // 50
1300. DNSSRV\_TYPEID\_ZONE\_SIGNING\_SETTINGS,
1301. DNSSRV\_TYPEID\_ZONE\_SCOPE\_ENUM,
1302. DNSSRV\_TYPEID\_ZONE\_STATS,
1303. DNSSRV\_TYPEID\_ZONE\_SCOPE\_CREATE,
1304. DNSSRV\_TYPEID\_ZONE\_SCOPE\_INFO, // 55
1305. DNSSRV\_TYPEID\_SCOPE\_ENUM,
1306. DNSSRV\_TYPEID\_CLIENT\_SUBNET\_RECORD,
1307. DNSSRV\_TYPEID\_POLICY,
1308. DNSSRV\_TYPEID\_POLICY\_NAME,
1309. DNSSRV\_TYPEID\_POLICY\_ENUM // 60
1310. }
1311. DNS\_RPC\_TYPEID, \*PDNS\_RPC\_TYPEID;
1312. #define DNS\_RPC\_ZONE\_STATS\_VER 1
1313. #define DNS\_RPC\_ZONE\_STATS DNS\_RPC\_ZONE\_STATS\_V1
1314. #define PDNS\_RPC\_ZONE\_STATS PDNS\_RPC\_ZONE\_STATS\_V1
1315. #define DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_VER 1
1316. #define DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1
1317. #define PDNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO PDNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1
1318. #define DNS\_RPC\_ZONE\_SCOPE\_INFO\_VER 1
1319. #define DNS\_RPC\_ZONE\_SCOPE\_INFO DNS\_RPC\_ZONE\_SCOPE\_INFO\_V1
1320. #define PDNS\_RPC\_ZONE\_SCOPE\_INFO PDNS\_RPC\_ZONE\_SCOPE\_INFO\_V1
1321. #define DNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST\_VER 1
1322. typedef struct \_DnsRpcEnumZoneScopeList
1323. {
1324. DWORD dwRpcStructureVersion;
1325. DWORD dwZoneScopeCount;
1326. // array of dwZoneScopeCount zones
1327. LPWSTR ZoneScopeArray[1];
1328. } DNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST, \* PDNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST;
1329. //
1330. // DNS server statistics
1331. //
1332. typedef struct \_DnsSystemTime
1333. {
1334. WORD wYear;
1335. WORD wMonth;
1336. WORD wDayOfWeek;
1337. WORD wDay;
1338. WORD wHour;
1339. WORD wMinute;
1340. WORD wSecond;
1341. WORD wMilliseconds;
1342. }
1343. DNS\_SYSTEMTIME;
1344. //
1345. // Zone time statisticsinfo.
1346. //
1347. typedef struct \_DnsZoneTimeStats
1348. {
1349. DNS\_SYSTEMTIME StatsCollectionStartTime;
1350. }
1351. DNSSRV\_ZONE\_TIME\_STATS, \*PDNSSRV\_ZONE\_TIME\_STATS;
1352. #define MAX\_RECORD\_TYPES 31
1353. #define MAX\_ZONE\_TRANSFER\_TYPES 2
1354. //
1355. // Enum for all zone statistics types
1356. //
1357. typedef enum \_DNS\_ZONE\_STATS\_TYPE {
1358. //
1359. // Record types. If new zone stats record type is added/deleted
1360. // then update MAX\_RECORD\_TYPES accordingly.
1361. //
1362. ZONE\_STATS\_TYPE\_RECORD\_A = 0,
1363. ZONE\_STATS\_TYPE\_RECORD\_AAAA,
1364. ZONE\_STATS\_TYPE\_RECORD\_PTR,
1365. ZONE\_STATS\_TYPE\_RECORD\_CNAME,
1366. ZONE\_STATS\_TYPE\_RECORD\_MX,
1367. ZONE\_STATS\_TYPE\_RECORD\_AFSDB,
1368. ZONE\_STATS\_TYPE\_RECORD\_ATMA,
1369. ZONE\_STATS\_TYPE\_RECORD\_DHCID,
1370. ZONE\_STATS\_TYPE\_RECORD\_DNAME,
1371. ZONE\_STATS\_TYPE\_RECORD\_HINFO,
1372. ZONE\_STATS\_TYPE\_RECORD\_ISDN,
1373. ZONE\_STATS\_TYPE\_RECORD\_MG,
1374. ZONE\_STATS\_TYPE\_RECORD\_MB,
1375. ZONE\_STATS\_TYPE\_RECORD\_MINFO,
1376. ZONE\_STATS\_TYPE\_RECORD\_NAPTR,
1377. ZONE\_STATS\_TYPE\_RECORD\_NXT,
1378. ZONE\_STATS\_TYPE\_RECORD\_KEY,
1379. ZONE\_STATS\_TYPE\_RECORD\_MR,
1380. ZONE\_STATS\_TYPE\_RECORD\_RP,
1381. ZONE\_STATS\_TYPE\_RECORD\_RT,
1382. ZONE\_STATS\_TYPE\_RECORD\_SRV,
1383. ZONE\_STATS\_TYPE\_RECORD\_SIG,
1384. ZONE\_STATS\_TYPE\_RECORD\_TEXT,
1385. ZONE\_STATS\_TYPE\_RECORD\_WKS,
1386. ZONE\_STATS\_TYPE\_RECORD\_X25,
1387. ZONE\_STATS\_TYPE\_RECORD\_DNSKEY,
1388. ZONE\_STATS\_TYPE\_RECORD\_DS,
1389. ZONE\_STATS\_TYPE\_RECORD\_NS,
1390. ZONE\_STATS\_TYPE\_RECORD\_SOA,
1391. ZONE\_STATS\_TYPE\_RECORD\_TLSA,
1392. ZONE\_STATS\_TYPE\_RECORD\_ALL,
1393. ZONE\_STATS\_TYPE\_RECORD\_OTHERS,
1394. //
1395. // Zone transfer types. If new zone transfer type is added/deleted
1396. // then update MAX\_ZONE\_TRANSFER\_TYPES accordingly.
1397. //
1398. ZONE\_STATS\_TYPE\_TRANSFER\_AXFR,
1399. ZONE\_STATS\_TYPE\_TRANSFER\_IXFR,
1400. //
1401. // Zone update.
1402. //
1403. ZONE\_STATS\_TYPE\_UPDATE,
1404. MAX\_ZONE\_STATS\_TYPES
1405. } DNS\_ZONE\_STATS\_TYPE, \*PDNS\_DONE\_STATS\_TYPE;
1406. //
1407. // Per zone per record type statistics.
1408. //
1409. typedef struct \_DnsZoneQueryStats {
1410. DNS\_ZONE\_STATS\_TYPE RecordType;
1411. ULONG64 QueriesResponded;
1412. ULONG64 QueriesReceived;
1413. ULONG64 QueriesFailure;
1414. ULONG64 QueriesNameError;
1415. }
1416. DNSSRV\_ZONE\_QUERY\_STATS, \*PDNSSRV\_ZONE\_QUERY\_STATS;
1417. //
1418. // Zone transfer statistics.
1419. //
1420. typedef struct \_DnsZoneTransferStats {
1421. DNS\_ZONE\_STATS\_TYPE TransferType;
1422. ULONG64 RequestReceived;
1423. ULONG64 RequestSent;
1424. ULONG64 ResponseReceived;
1425. ULONG64 SuccessReceived;
1426. ULONG64 SuccessSent;
1427. }
1428. DNSSRV\_ZONE\_TRANSFER\_STATS, \*PDNSSRV\_ZONE\_TRANSFER\_STATS;
1429. //
1430. // Zone update statistics.
1431. //
1432. typedef struct \_DnsZoneUpdateStats {
1433. DNS\_ZONE\_STATS\_TYPE Type;
1434. ULONG64 DynamicUpdateReceived;
1435. ULONG64 DynamicUpdateRejected;
1436. }
1437. DNSSRV\_ZONE\_UPDATE\_STATS, \*PDNSSRV\_ZONE\_UPDATE\_STATS;
1438. typedef struct \_DnsRpcZoneStats {
1439. DWORD dwRpcStructureVersion;
1440. DNSSRV\_ZONE\_TIME\_STATS ZoneTimeStats;
1441. DNSSRV\_ZONE\_QUERY\_STATS ZoneQueryStats[MAX\_RECORD\_TYPES];
1442. DNSSRV\_ZONE\_TRANSFER\_STATS ZoneTransferStats[MAX\_ZONE\_TRANSFER\_TYPES];
1443. DNSSRV\_ZONE\_UPDATE\_STATS ZoneUpdateStats;
1444. }DNS\_RPC\_ZONE\_STATS\_V1, \*PDNS\_RPC\_ZONE\_STATS\_V1;
1445. typedef struct \_DnsRpcScopeCreate
1446. {
1447. DWORD dwFlags ;
1448. LPWSTR pwszScopeName; // Scope name that is to be created
1449. }DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1,\*PDNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1;
1450. typedef struct \_DnsRpcZoneScopeInfo
1451. {
1452. DWORD dwRpcStructureVersion;
1453. LPWSTR pwszScopeName;
1454. LPWSTR pwszDataFile;
1455. } DNS\_RPC\_ZONE\_SCOPE\_INFO\_V1, \*PDNS\_RPC\_ZONE\_SCOPE\_INFO\_V1;
1456. typedef struct \_DnsRpcEnumScopeList
1457. {
1458. DWORD dwRpcStructureVersion;
1459. DWORD dwScopeCount;
1460. LPWSTR ScopeArray[1];
1461. } DNS\_RPC\_ENUM\_SCOPE\_LIST, \*PDNS\_RPC\_ENUM\_SCOPE\_LIST;
1462. typedef [switch\_type(DWORD)] union \_DnssrvSrvRpcUnion
1463. {
1464. [case(DNSSRV\_TYPEID\_NULL)] PBYTE Null;
1465. [case(DNSSRV\_TYPEID\_DWORD)] DWORD Dword;
1466. [case(DNSSRV\_TYPEID\_LPSTR)] [string] char \* String;
1467. [case(DNSSRV\_TYPEID\_LPWSTR)] [string] wchar\_t \* WideString;
1468. [case(DNSSRV\_TYPEID\_IPARRAY)] PIP4\_ARRAY IpArray;
1469. [case(DNSSRV\_TYPEID\_BUFFER)]
1470. PDNS\_RPC\_BUFFER Buffer;
1471. [case(DNSSRV\_TYPEID\_SERVER\_INFO\_W2K)]
1472. PDNS\_RPC\_SERVER\_INFO\_W2K ServerInfoW2K;
1473. [case(DNSSRV\_TYPEID\_STATS)]
1474. PDNSSRV\_STATS Stats;
1475. [case(DNSSRV\_TYPEID\_FORWARDERS\_W2K)]
1476. PDNS\_RPC\_FORWARDERS\_W2K ForwardersW2K;
1477. [case(DNSSRV\_TYPEID\_ZONE\_W2K)]
1478. PDNS\_RPC\_ZONE\_W2K ZoneW2K;
1479. [case(DNSSRV\_TYPEID\_ZONE\_INFO\_W2K)]
1480. PDNS\_RPC\_ZONE\_INFO\_W2K ZoneInfoW2K;
1481. [case(DNSSRV\_TYPEID\_ZONE\_SECONDARIES\_W2K)]
1482. PDNS\_RPC\_ZONE\_SECONDARIES\_W2K SecondariesW2K;
1483. [case(DNSSRV\_TYPEID\_ZONE\_DATABASE\_W2K)]
1484. PDNS\_RPC\_ZONE\_DATABASE\_W2K DatabaseW2K;
1485. [case(DNSSRV\_TYPEID\_ZONE\_CREATE\_W2K)]
1486. PDNS\_RPC\_ZONE\_CREATE\_INFO\_W2K ZoneCreateW2K;
1487. [case(DNSSRV\_TYPEID\_NAME\_AND\_PARAM)]
1488. PDNS\_RPC\_NAME\_AND\_PARAM NameAndParam;
1489. [case(DNSSRV\_TYPEID\_ZONE\_LIST\_W2K)]
1490. PDNS\_RPC\_ZONE\_LIST\_W2K ZoneListW2K;
1491. [case(DNSSRV\_TYPEID\_SERVER\_INFO\_DOTNET)]
1492. PDNS\_RPC\_SERVER\_INFO\_DOTNET ServerInfoDotNet;
1493. [case(DNSSRV\_TYPEID\_FORWARDERS\_DOTNET)]
1494. PDNS\_RPC\_FORWARDERS\_DOTNET ForwardersDotNet;
1495. [case(DNSSRV\_TYPEID\_ZONE)]
1496. PDNS\_RPC\_ZONE Zone;
1497. [case(DNSSRV\_TYPEID\_ZONE\_INFO\_DOTNET)]
1498. PDNS\_RPC\_ZONE\_INFO\_DOTNET ZoneInfoDotNet;
1499. [case(DNSSRV\_TYPEID\_ZONE\_SECONDARIES\_DOTNET)]
1500. PDNS\_RPC\_ZONE\_SECONDARIES\_DOTNET SecondariesDotNet;
1501. [case(DNSSRV\_TYPEID\_ZONE\_DATABASE)]
1502. PDNS\_RPC\_ZONE\_DATABASE Database;
1503. [case(DNSSRV\_TYPEID\_ZONE\_CREATE\_DOTNET)]
1504. PDNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET ZoneCreateDotNet;
1505. [case(DNSSRV\_TYPEID\_ZONE\_LIST)]
1506. PDNS\_RPC\_ZONE\_LIST ZoneList;
1507. [case(DNSSRV\_TYPEID\_ZONE\_EXPORT)]
1508. PDNS\_RPC\_ZONE\_EXPORT\_INFO ZoneExport;
1509. [case(DNSSRV\_TYPEID\_DP\_INFO)]
1510. PDNS\_RPC\_DP\_INFO DirectoryPartition;
1511. [case(DNSSRV\_TYPEID\_DP\_ENUM)]
1512. PDNS\_RPC\_DP\_ENUM DirectoryPartitionEnum;
1513. [case(DNSSRV\_TYPEID\_DP\_LIST)]
1514. PDNS\_RPC\_DP\_LIST DirectoryPartitionList;
1515. [case(DNSSRV\_TYPEID\_ENLIST\_DP)]
1516. PDNS\_RPC\_ENLIST\_DP EnlistDirectoryPartition;
1517. [case(DNSSRV\_TYPEID\_ZONE\_CHANGE\_DP)]
1518. PDNS\_RPC\_ZONE\_CHANGE\_DP ZoneChangeDirectoryPartition;
1519. [case(DNSSRV\_TYPEID\_ENUM\_ZONES\_FILTER)]
1520. PDNS\_RPC\_ENUM\_ZONES\_FILTER EnumZonesFilter;
1521. [case(DNSSRV\_TYPEID\_ADDRARRAY)]
1522. PDNS\_ADDR\_ARRAY AddrArray;
1523. [case(DNSSRV\_TYPEID\_SERVER\_INFO)]
1524. PDNS\_RPC\_SERVER\_INFO ServerInfo;
1525. [case(DNSSRV\_TYPEID\_ZONE\_CREATE)]
1526. PDNS\_RPC\_ZONE\_CREATE\_INFO ZoneCreate;
1527. [case(DNSSRV\_TYPEID\_FORWARDERS)]
1528. PDNS\_RPC\_FORWARDERS Forwarders;
1529. [case(DNSSRV\_TYPEID\_ZONE\_SECONDARIES)]
1530. PDNS\_RPC\_ZONE\_SECONDARIES Secondaries;
1531. [case(DNSSRV\_TYPEID\_IP\_VALIDATE)]
1532. PDNS\_RPC\_IP\_VALIDATE IpValidate;
1533. [case(DNSSRV\_TYPEID\_ZONE\_INFO)]
1534. PDNS\_RPC\_ZONE\_INFO ZoneInfo;
1535. [case(DNSSRV\_TYPEID\_AUTOCONFIGURE)]
1536. PDNS\_RPC\_AUTOCONFIGURE AutoConfigure;
1537. [case(DNSSRV\_TYPEID\_UTF8\_STRING\_LIST)]
1538. PDNS\_RPC\_UTF8\_STRING\_LIST Utf8StringList;
1539. [case(DNSSRV\_TYPEID\_UNICODE\_STRING\_LIST)]
1540. PDNS\_RPC\_UNICODE\_STRING\_LIST UnicodeStringList;
1541. [case(DNSSRV\_TYPEID\_SKD)]
1542. PDNS\_RPC\_SKD Skd;
1543. [case(DNSSRV\_TYPEID\_SKD\_LIST)]
1544. PDNS\_RPC\_SKD\_LIST SkdList;
1545. [case(DNSSRV\_TYPEID\_SKD\_STATE)]
1546. PDNS\_RPC\_SKD\_STATE SkdState;
1547. [case(DNSSRV\_TYPEID\_SIGNING\_VALIDATION\_ERROR)]
1548. PDNS\_RPC\_SIGNING\_VALIDATION\_ERROR SigningValidationError;
1549. [case(DNSSRV\_TYPEID\_TRUST\_POINT\_LIST)]
1550. PDNS\_RPC\_TRUST\_POINT\_LIST TrustPointList;
1551. [case(DNSSRV\_TYPEID\_TRUST\_ANCHOR\_LIST)]
1552. PDNS\_RPC\_TRUST\_ANCHOR\_LIST TrustAnchorList;
1553. [case(DNSSRV\_TYPEID\_ZONE\_SIGNING\_SETTINGS)]
1554. PDNS\_RPC\_ZONE\_DNSSEC\_SETTINGS ZoneDnsSecSettings;
1555. [case(DNSSRV\_TYPEID\_ZONE\_SCOPE\_ENUM)]
1556. PDNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST ZoneScopeList;
1557. [case(DNSSRV\_TYPEID\_ZONE\_STATS)]
1558. PDNS\_RPC\_ZONE\_STATS ZoneStats;
1559. [case(DNSSRV\_TYPEID\_ZONE\_SCOPE\_CREATE)]
1560. PDNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO ScopeCreate;
1561. [case(DNSSRV\_TYPEID\_ZONE\_SCOPE\_INFO)]
1562. PDNS\_RPC\_ZONE\_SCOPE\_INFO ScopeInfo;
1563. [case(DNSSRV\_TYPEID\_SCOPE\_ENUM)]
1564. PDNS\_RPC\_ENUM\_SCOPE\_LIST ScopeList;
1565. [case(DNSSRV\_TYPEID\_CLIENT\_SUBNET\_RECORD)]
1566. PDNS\_RPC\_CLIENT\_SUBNET\_RECORD SubnetList;
1567. [case(DNSSRV\_TYPEID\_POLICY)]
1568. PDNS\_RPC\_POLICY pPolicy;
1569. [case(DNSSRV\_TYPEID\_POLICY\_NAME)]
1570. PDNS\_RPC\_POLICY\_NAME pPolicyName;
1571. [case(DNSSRV\_TYPEID\_POLICY\_ENUM)]
1572. PDNS\_RPC\_ENUMERATE\_POLICY\_LIST pPolicyList;
1573. }
1574. DNSSRV\_RPC\_UNION;
1575. typedef enum \_ImportOperationResult
1576. {
1577. // No change was detected in Signing Settings imported and that of the Zone
1578. IMPORT\_STATUS\_NOOP,
1579. // Zone is marked for Re-Sign
1580. IMPORT\_STATUS\_SIGNING\_READY,
1581. // Zone is marked for Unsign
1582. IMPORT\_STATUS\_UNSIGNING\_READY,
1583. // Change was detected but no re-signing\unsigning required
1584. IMPORT\_STATUS\_CHANGED
1585. } ImportOpResult;
1586. [
1587. uuid(50abc2a4-574d-40b3-9d66-ee4fd5fba076),
1588. version(5.0),
1589. pointer\_default(unique)
1590. ]
1591. interface DnsServer
1592. {
1593. LONG
1594. R\_DnssrvOperation(
1595. [in] handle\_t hBindingHandle,
1596. [in, unique, string] LPCWSTR pwszServerName,
1597. [in, unique, string] LPCSTR pszZone,
1598. [in] DWORD dwContext,
1599. [in, unique, string] LPCSTR pszOperation,
1600. [in] DWORD dwTypeId,
1601. [in, switch\_is(dwTypeId)] DNSSRV\_RPC\_UNION pData
1602. );
1603. LONG
1604. R\_DnssrvQuery(
1605. [in] handle\_t hBindingHandle,
1606. [in, unique, string] LPCWSTR pwszServerName,
1607. [in, unique, string] LPCSTR pszZone,
1608. [in, unique, string] LPCSTR pszOperation,
1609. [out] PDWORD pdwTypeId,
1610. [out, switch\_is(\*pdwTypeId)] DNSSRV\_RPC\_UNION \* ppData
1611. );
1612. LONG
1613. R\_DnssrvComplexOperation(
1614. [in] handle\_t hBindingHandle,
1615. [in, unique, string] LPCWSTR pwszServerName,
1616. [in, unique, string] LPCSTR pszZone,
1617. [in, unique, string] LPCSTR pszOperation,
1618. [in] DWORD dwTypeIn,
1619. [in, switch\_is(dwTypeIn)] DNSSRV\_RPC\_UNION pDataIn,
1620. [out] PDWORD pdwTypeOut,
1621. [out, switch\_is(\*pdwTypeOut)] DNSSRV\_RPC\_UNION \* ppDataOut
1622. );
1623. LONG
1624. R\_DnssrvEnumRecords(
1625. [in] handle\_t hBindingHandle,
1626. [in, unique, string] LPCWSTR pwszServerName,
1627. [in, unique, string] LPCSTR pszZone,
1628. [in, unique, string] LPCSTR pszNodeName,
1629. [in, unique, string] LPCSTR pszStartChild,
1630. [in] WORD wRecordType,
1631. [in] DWORD fSelectFlag,
1632. [in, unique, string] LPCSTR pszFilterStart,
1633. [in, unique, string] LPCSTR pszFilterStop,
1634. [out] PDWORD pdwBufferLength,
1635. [out, size\_is(, \*pdwBufferLength)] PBYTE \* ppBuffer
1636. );
1637. LONG
1638. R\_DnssrvUpdateRecord(
1639. [in] handle\_t hBindingHandle,
1640. [in, unique, string] LPCWSTR pwszServerName,
1641. [in, unique, string] LPCSTR pszZone,
1642. [in, string] LPCSTR pszNodeName,
1643. [in, unique] PDNS\_RPC\_RECORD pAddRecord,
1644. [in, unique] PDNS\_RPC\_RECORD pDeleteRecord
1645. );
1646. LONG
1647. R\_DnssrvOperation2(
1648. [in] handle\_t hBindingHandle,
1649. [in] DWORD dwClientVersion,
1650. [in] DWORD dwSettingFlags,
1651. [in, unique, string] LPCWSTR pwszServerName,
1652. [in, unique, string] LPCSTR pszZone,
1653. [in] DWORD dwContext,
1654. [in, unique, string] LPCSTR pszOperation,
1655. [in] DWORD dwTypeId,
1656. [in, switch\_is(dwTypeId)] DNSSRV\_RPC\_UNION pData
1657. );
1658. LONG
1659. R\_DnssrvQuery2(
1660. [in] handle\_t hBindingHandle,
1661. [in] DWORD dwClientVersion,
1662. [in] DWORD dwSettingFlags,
1663. [in, unique, string] LPCWSTR pwszServerName,
1664. [in, unique, string] LPCSTR pszZone,
1665. [in, unique, string] LPCSTR pszOperation,
1666. [out] PDWORD pdwTypeId,
1667. [out, switch\_is(\*pdwTypeId)] DNSSRV\_RPC\_UNION \* ppData
1668. );
1669. LONG
1670. R\_DnssrvComplexOperation2(
1671. [in] handle\_t hBindingHandle,
1672. [in] DWORD dwClientVersion,
1673. [in] DWORD dwSettingFlags,
1674. [in, unique, string] LPCWSTR pwszServerName,
1675. [in, unique, string] LPCSTR pszZone,
1676. [in, unique, string] LPCSTR pszOperation,
1677. [in] DWORD dwTypeIn,
1678. [in, switch\_is(dwTypeIn)] DNSSRV\_RPC\_UNION pDataIn,
1679. [out] PDWORD pdwTypeOut,
1680. [out, switch\_is(\*pdwTypeOut)] DNSSRV\_RPC\_UNION \* ppDataOut
1681. );
1682. LONG
1683. R\_DnssrvEnumRecords2(
1684. [in] handle\_t hBindingHandle,
1685. [in] DWORD dwClientVersion,
1686. [in] DWORD dwSettingFlags,
1687. [in, unique, string] LPCWSTR pwszServerName,
1688. [in, unique, string] LPCSTR pszZone,
1689. [in, unique, string] LPCSTR pszNodeName,
1690. [in, unique, string] LPCSTR pszStartChild,
1691. [in] WORD wRecordType,
1692. [in] DWORD fSelectFlag,
1693. [in, unique, string] LPCSTR pszFilterStart,
1694. [in, unique, string] LPCSTR pszFilterStop,
1695. [out] PDWORD pdwBufferLength,
1696. [out, size\_is(, \*pdwBufferLength)] PBYTE \* ppBuffer
1697. );
1698. LONG
1699. R\_DnssrvUpdateRecord2(
1700. [in] handle\_t hBindingHandle,
1701. [in] DWORD dwClientVersion,
1702. [in] DWORD dwSettingFlags,
1703. [in, unique, string] LPCWSTR pwszServerName,
1704. [in, unique, string] LPCSTR pszZone,
1705. [in, string] LPCSTR pszNodeName,
1706. [in, unique] PDNS\_RPC\_RECORD pAddRecord,
1707. [in, unique] PDNS\_RPC\_RECORD pDeleteRecord
1708. );
1709. LONG
1710. R\_DnssrvUpdateRecord3(
1711. [in] handle\_t hBindingHandle,
1712. [in] DWORD dwClientVersion,
1713. [in] DWORD dwSettingFlags,
1714. [in, unique, string] LPCWSTR pwszServerName,
1715. [in, unique, string] LPCSTR pszZone,
1716. [in, unique, string] LPCWSTR pwszZoneScope,
1717. [in, string] LPCSTR pszNodeName,
1718. [in, unique] PDNS\_RPC\_RECORD pAddRecord,
1719. [in, unique] PDNS\_RPC\_RECORD pDeleteRecord
1720. );
1722. LONG
1723. R\_DnssrvEnumRecords3(
1724. [in] handle\_t hBindingHandle,
1725. [in] DWORD dwClientVersion,
1726. [in] DWORD dwSettingFlags,
1727. [in, unique, string] LPCWSTR pwszServerName,
1728. [in, unique, string] LPCSTR pszZone,
1729. [in, unique, string] LPCWSTR pwszZoneScope,
1730. [in, unique, string] LPCSTR pszNodeName,
1731. [in, unique, string] LPCSTR pszStartChild,
1732. [in] WORD wRecordType,
1733. [in] DWORD fSelectFlag,
1734. [in, unique, string] LPCSTR pszFilterStart,
1735. [in, unique, string] LPCSTR pszFilterStop,
1736. [out] PDWORD pdwBufferLength,
1737. [out, size\_is(, \*pdwBufferLength)] PBYTE \* ppBuffer
1738. );
1739. LONG
1740. R\_DnssrvOperation3(
1741. [in] handle\_t hBindingHandle,
1742. [in] DWORD dwClientVersion,
1743. [in] DWORD dwSettingFlags,
1744. [in, unique, string] LPCWSTR pwszServerName,
1745. [in, unique, string] LPCSTR pszZone,
1746. [in, unique, string] LPCWSTR pwszZoneScope,
1747. [in] DWORD dwContext,
1748. [in, unique, string] LPCSTR pszOperation,
1749. [in] DWORD dwTypeId,
1750. [in, switch\_is(dwTypeId)] DNSSRV\_RPC\_UNION pData
1751. );
1753. LONG
1754. R\_DnssrvQuery3(
1755. [in] DWORD dwClientVersion,
1756. [in] DWORD dwSettingFlags,
1757. [in, unique, string] LPCWSTR pwszServerName,
1758. [in, unique, string] LPCSTR pszZone,
1759. [in, unique, string] LPCWSTR pszZoneScopeName,
1760. [in, unique, string] LPCSTR pszOperation,
1761. [out] PDWORD pdwTypeId,
1762. [out, switch\_is(\*pdwTypeId)] DNSSRV\_RPC\_UNION \* ppData
1763. );
1764. }

# Appendix B: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs.

Note: Some of the information in this section is subject to change because it applies to an unreleased, preliminary version of the Windows Server operating system, and thus may differ from the final version of the server software when released. All behavior notes that pertain to the unreleased, preliminary version of the Windows Server operating system contain specific references to Windows Server 2016 Technical Preview as an aid to the reader.

* Windows NT operating system
* Windows 2000 operating system
* Windows XP operating system
* Windows Server 2003 operating system
* Windows Vista operating system
* Windows Server 2008 operating system
* Windows 7 operating system
* Windows Server 2008 R2 operating system
* Windows 8 operating system
* Windows Server 2012 operating system
* Windows 8.1 operating system
* Windows Server 2012 R2 operating system
* Windows 10 operating system
* Windows Server 2016 Technical Preview operating system

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that the product does not follow the prescription.

[<1> Section 2.1](#Appendix_A_Target_1): RPC over named pipes is supported on Windows NT, Windows 2000, and Windows Server 2003 only.

[<2> Section 2.1.2](#Appendix_A_Target_2): Windows 2000 and Windows Server 2003 clients always request RPC\_C\_QOS\_CAPABILITIES\_MUTUAL\_AUTH. Windows Server 2008, Windows Server 2008 R2 operating system, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview clients additionally request RPC\_C\_QOS\_CAPABILITIES\_IGNORE\_DELEGATE\_FAILURE during [R\_DnssrvOperation (section 3.1.4.1)](#Section_9500a7e8165d4b13be860ddc43100eef) or [R\_DnssrvOperation2 (section 3.1.4.6)](#Section_8c0522b197fb4fa7b4e22c55c0afb0e7) when *pszOperation* is "EnlistDirectoryPartition".

[<3> Section 2.1.2](#Appendix_A_Target_3): Windows 2000 and Windows Server 2003 clients always request RPC\_C\_IMP\_LEVEL\_DELEGATE. Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview clients request RPC\_C\_IMP\_LEVEL\_DELEGATE during R\_DnssrvOperation or R\_DnssrvOperation2 when *pszOperation* is "EnlistDirectoryPartition".

[<4> Section 2.2.1.1.1](#Appendix_A_Target_4): Windows Server 2008, Windows Server 2008 R2, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10, and Windows Server 2016 Technical Preview support type IDs up to and including DNSSRV\_TYPEID\_UTF8\_STRING\_LIST. Windows Server 2003 supports type IDs up to and including DNSSRV\_TYPEID\_ZONE\_LIST, as enumerated in section [2.2.1.1.1](#Section_c49b8142a36441c8914a7675a573b5e4). Windows 2000 supports type IDs up to and including DNSSRV\_TYPEID\_ZONE\_LIST\_W2K. The DNSSRV\_TYPEID\_ZONE\_SCOPE\_ENUM structure is available only in Windows Server 2012 R2 and Windows Server 2016 Technical Preview.

[<5> Section 2.2.1.1.2](#Appendix_A_Target_5): Windows clients and servers use this value to indicate use of LPC [[MSDN-RPC]](http://go.microsoft.com/fwlink/?LinkId=90075).

[<6> Section 2.2.1.2.6](#Appendix_A_Target_6): Windows Server 2003 supports elements of this union up to and including ZoneCreateDotNet. Windows 2000 supports elements of this union up to and including ZoneListW2K.

[<7> Section 2.2.2.1.1](#Appendix_A_Target_7): Windows 2000 does not support the following types: DNS\_TYPE\_SIG, DNS\_TYPE\_KEY, DNS\_TYPE\_NXT, DNS\_TYPE\_NAPTR, and DNS\_TYPE\_DNAME. Windows Server 2003 does not support DNS\_TYPE\_NAPTR and DNS\_TYPE\_DNAME. The types DNS\_TYPE\_DS, DNS\_TYPE\_RRSIG, DNS\_TYPE\_NSEC, DNS\_TYPE\_DNSKEY, and DNS\_TYPE\_DHCID are supported only on Windows Server 2008 R2. DNS\_TYPE\_NSEC3 and DNS\_TYPE\_NSEC3PARAM are supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview. DNS\_TYPE\_TLSA is supported on Windows Server 2016 Technical Preview only.

[<8> Section 2.2.2.1.2](#Appendix_A_Target_8): Windows 2000 does not support the DNS\_RPC\_FLAG\_OPEN\_ACL record flag. DNS\_RPC\_FLAG\_RECORD\_WIRE\_FORMAT and DNS\_RPC\_FLAG\_SUPPRESS\_RECORD\_UPDATE\_PTR are supported in Windows Server 2016 Technical Preview only.

[<9> Section 2.2.2.2.4.2](#Appendix_A_Target_9): Windows 2000 and Windows Server 2003 do not support DNS\_TYPE\_DNAME.

[<10> Section 2.2.2.2.4.9](#Appendix_A_Target_10): This record type is not supported in Windows 2000.

[<11> Section 2.2.2.2.4.10](#Appendix_A_Target_11): This record type is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<12> Section 2.2.2.2.4.11](#Appendix_A_Target_12): This record type is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<13> Section 2.2.2.2.4.12](#Appendix_A_Target_13): This record type is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<14> Section 2.2.2.2.4.13](#Appendix_A_Target_14): This record type is not supported in Windows 2000.

[<15> Section 2.2.2.2.4.14](#Appendix_A_Target_15): This record type is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<16> Section 2.2.2.2.4.15](#Appendix_A_Target_16): This record type is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<17> Section 2.2.2.2.4.17](#Appendix_A_Target_17): This record type is not supported in Windows 2000.

[<18> Section 2.2.2.2.4.20](#Appendix_A_Target_18): This record type is not supported in Windows 2000.

[<19> Section 2.2.2.2.4.24](#Appendix_A_Target_19): This record type is supported only by Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<20> Section 2.2.2.2.4.25](#Appendix_A_Target_20): This record type is supported only by Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<21> Section 2.2.2.2.4.26](#Appendix_A_Target_21): DNS\_RPC\_RECORD\_TLSA is supported in Windows Server 2016 Technical Preview only.

[<22> Section 2.2.2.2.4.27](#Appendix_A_Target_22): The DNS\_RPC\_RECORD\_UNKNOWN structure is supported in Windows Server 2016 Technical Preview only.

[<23> Section 2.2.2.2.5](#Appendix_A_Target_23): In Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012, if the **dwFlags** field is set to DNS\_RPC\_FLAG\_RECORD\_WIRE\_FORMAT, the error DNS\_ERROR\_RECORD\_FORMAT is returned.

[<24> Section 2.2.2.2.5](#Appendix_A_Target_24): The records DNS\_TYPE\_DS, DNS\_TYPE\_RRSIG, DNS\_TYPE\_NSEC, DNS\_TYPE\_DNSKEY and DNS\_TYPE\_DHCID are not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<25> Section 2.2.3.1.1](#Appendix_A_Target_25): Windows 2000 and Windows Server 2003 do not support IP validation.

[<26> Section 2.2.3.1.2](#Appendix_A_Target_26): Windows 2000 and Windows Server 2003 do not support IP validation.

[<27> Section 2.2.4.1.1](#Appendix_A_Target_27): Windows NT 4.0 operating system populates its database in the following order, until successful: from a file-based persistent storage or from the persistent copy of the DNS Zone Table.

[<28> Section 2.2.4.2.1](#Appendix_A_Target_28): Windows uses the build number as the OS Revision.

[<29> Section 2.2.4.2.2.1](#Appendix_A_Target_29): Except for Windows NT Server 4.0 operating system, which predates Active Directory, Windows Server operating system uses "cn=MicrosoftDNS,cn=System" as the constant container RDN. A complete DS Container string could, for example, be "cn=MicrosoftDNS,cn=System,DC=corp,DC=contoso,DC=com".

[<30> Section 2.2.4.2.2.2](#Appendix_A_Target_30): This version of the structure is for use with Windows Server 2003.

[<31> Section 2.2.4.2.2.3](#Appendix_A_Target_31): This version of the structure is for use with Windows Server 2008 and Windows Server 2008 R2.

[<32> Section 2.2.5.1.1](#Appendix_A_Target_32): Windows 2000 does not support the forwarder or stub zone types. Windows 2000 and Windows Server 2003 do not support the secondary cache zone type.

[<33> Section 2.2.5.1.4](#Appendix_A_Target_33): Windows 2000 does not support any zone request filter values that involve application directory partitions. Windows 2000 does not support stub or forwarder zone request filters.

[<34> Section 2.2.5.1.5](#Appendix_A_Target_34): Only Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview support DNSSEC key rollover. Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview support only DNS\_ROLLOVER\_TYPE\_PREPUBLISH for signing key descriptors where fIsKSK is FALSE and DNS\_ROLLOVER\_TYPE\_DOUBLE\_SIGNATURE for signing key descriptors where fIsKSK is TRUE.

[<35> Section 2.2.5.1.6](#Appendix_A_Target_35): Only Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview support DNSSEC key rollover.

[<36> Section 2.2.5.2.1](#Appendix_A_Target_36): Windows 2000 only supports DNS\_RPC\_ZONE\_W2K.

[<37> Section 2.2.5.2.2](#Appendix_A_Target_37): The Windows DNS server auto-creates the 0.in-addr.arpa, 127.in-addr.arpa, and 255.in-addr.arpa zones as a performance optimization to avoid unnecessary recursions to the root server for queries for standard IP addresses such as 0.0.0.0, 127.0.0.1 (loopback), and 255.255.255.255 (broadcast).

[<38> Section 2.2.5.2.2](#Appendix_A_Target_38): Windows 2000 and Windows Server 2003 do not support the ReadOnly bit.

[<39> Section 2.2.5.2.3](#Appendix_A_Target_39): Windows 2000 only supports DNS\_RPC\_ZONE\_LIST\_W2K.

[<40> Section 2.2.5.2.4.2](#Appendix_A_Target_40): Windows Server incorrectly sets this to 0x00000000.

[<41> Section 2.2.5.2.4.3](#Appendix_A_Target_41): Windows Server incorrectly sets this to 0x00000000.

[<42> Section 2.2.5.2.8](#Appendix_A_Target_42): This structure is not implemented in Windows 2000.

[<43> Section 2.2.5.2.10.1](#Appendix_A_Target_43): Windows 2000 uses 5 minutes (300 seconds).

[<44> Section 2.2.6.1.2](#Appendix_A_Target_44): KeySignScope is available in Windows Server 2012 R2 and Windows Server 2016 Technical Preview only.

[<45> Section 2.2.6.1.3](#Appendix_A_Target_45): ImportOpResult is available in Windows Server 2012 R2 and Windows Server 2016 Technical Preview only.

[<46> Section 2.2.6.2.1](#Appendix_A_Target_46): Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview support RSASHA1, RSASHA1-NSEC3-SHA1, RSASHA256, and RSASHA512.

[<47> Section 2.2.6.2.3](#Appendix_A_Target_47): Windows Server 2012 operating system, Windows Server 2012 R2, and Windows Server 2016 Technical Preview support automatic DNSSEC signing of zones.

[<48> Section 2.2.6.2.9](#Appendix_A_Target_48): The **DNS\_RPC\_ZONE\_DNSSEC\_SETTINGS** structure is available in Windows Server 2012 R2 and Windows Server 2016 Technical Preview only.

[<49> Section 2.2.6.2.10](#Appendix_A_Target_49): The **DNS\_RPC\_ZONE\_SKD** structure is available in Windows Server 2012 R2 and Windows Server 2016 Technical Preview only.

[<50> Section 2.2.6.2.11](#Appendix_A_Target_50): The **DNS\_RPC\_SKD\_STATE\_EX** structure is available in Windows Server 2012 R2 and Windows Server 2016 Technical Preview only.

[<51> Section 2.2.7.1.1](#Appendix_A_Target_51): This enumeration is not supported in Windows NT, Windows 2000, and Windows XP.

[<52> Section 2.2.7.1.1](#Appendix_A_Target_52): Windows Server 2003 does not support read-only DCs and does not process the **msDS-NC-RO-Replica-Locations**.

[<53> Section 2.2.7.2.1](#Appendix_A_Target_53): DNS\_RPC\_DP\_INFO is not supported by Windows NT, Windows 2000, and Windows XP.

[<54> Section 2.2.7.2.1](#Appendix_A_Target_54): Windows 2000 and Windows Server 2003 do not support read-only DCs and do not process the **msDS-NC-RO-Replica-Locations**.

[<55> Section 2.2.7.2.2](#Appendix_A_Target_55): This structure and its associated operations are not supported by Windows NT, Windows 2000, and Windows XP.

[<56> Section 2.2.7.2.3](#Appendix_A_Target_56): This structure is not supported by Windows NT, Windows 2000, and Windows XP.

[<57> Section 2.2.7.2.4](#Appendix_A_Target_57): This structure and its associated operations are not supported by Windows NT, Windows 2000, and Windows XP.

[<58> Section 2.2.7.2.5](#Appendix_A_Target_58): This structure and its associated operations are not supported by Windows NT, Windows 2000, and Windows XP.

[<59> Section 2.2.7.2.6](#Appendix_A_Target_59): This structure and its associated operations are not supported by Windows NT, Windows 2000, and Windows XP.

[<60> Section 2.2.8.1.1](#Appendix_A_Target_60): Windows NT 4.0 and Windows 2000 do not support this structure. Windows Server 2003 does not support the following values: DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_PREPEND, DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_APPEND (use DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT instead), and DNS\_RPC\_AUTOCONFIG\_INTERNAL\_RETURN\_ERRORS.

[<61> Section 2.2.8.1.1](#Appendix_A_Target_61): Windows Server 2003 does not support the DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_PREPEND constant. Use DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT instead.

[<62> Section 2.2.8.1.1](#Appendix_A_Target_62): Windows Server 2003 uses the values in the following table to obtain a constant. Windows Server 2003 interprets each value in the right-hand column as the corresponding constant in the left-hand column, regardless of the version of the client connecting to it. The client uses the corresponding values in the table to indicate each constant, regardless of the version of the server it is connecting to. No Windows implementation checks the version of the other communicating host when determining how to select or interpret these values.

| Constant | Value used by Windows Server 2003 |
| --- | --- |
| DNS\_RPC\_AUTOCONFIG\_INTERNAL\_ROOTHINTS | 0x00000001 |
| DNS\_RPC\_AUTOCONFIG\_INTERNAL\_FORWARDERS | 0x00000002 |
| DNS\_RPC\_AUTOCONFIG\_ZONES | 0x00000008 |
| DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT | 0x00000004 |
| DNS\_RPC\_AUTOCONFIG\_ALL | 0xFFFFFFFF |

[<63> Section 2.2.9.1.1](#Appendix_A_Target_63): DNS\_LOG\_LEVEL\_UNMATCHED\_RESPONSE is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<64> Section 2.2.10.1.1](#Appendix_A_Target_64): DNSSRV\_STATID\_DNSSEC is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<65> Section 2.2.10.2.6](#Appendix_A_Target_65): Windows 2000 DNS servers do not include this field.

[<66> Section 2.2.10.2.7](#Appendix_A_Target_66): Windows 2000 DNS servers do not implement the **ResponseMismatched** field. Windows 2000 and Windows Server 2003 DNS servers do not implement the **GnzLocalQuery** field.

[<67> Section 2.2.10.2.7](#Appendix_A_Target_67): This field is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<68> Section 2.2.10.2.8](#Appendix_A_Target_68): This record type is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<69> Section 2.2.10.2.9](#Appendix_A_Target_69): Windows 2000 and Windows Server 2003 DNS servers do not include this field.

[<70> Section 2.2.10.2.9](#Appendix_A_Target_70): Windows 2000 DNS servers do not include this field.

[<71> Section 2.2.10.2.10](#Appendix_A_Target_71): Windows 2000 DNS servers do not include this field.

[<72> Section 2.2.10.2.14](#Appendix_A_Target_72): Windows 2000 does not include this field.

[<73> Section 2.2.10.2.20](#Appendix_A_Target_73): Windows 2000 does not support **PacketsForNsListUsed**, **PacketsForNsListReturned**, and **PacketsForNsListInUse**.

[<74> Section 2.2.10.2.20](#Appendix_A_Target_74): Windows 2000 DNS servers do not include this field.

[<75> Section 2.2.12.1.1](#Appendix_A_Target_75): The **DNS\_ZONE\_STATS\_TYPE** enumerator is available in Windows Server 2012 R2 and Windows Server 2016 Technical Preview only.

[<76> Section 2.2.12.2.1](#Appendix_A_Target_76): The **DNSSRV\_ZONE\_TIME\_STATS** structure is available in Windows 8.1, Windows Server 2012 R2, Windows 10, and Windows Server 2016 Technical Preview only.

[<77> Section 2.2.12.2.2](#Appendix_A_Target_77): The **DNSSRV\_ZONE\_QUERY\_STATS** structure is available in Windows Server 2012 R2 and Windows Server 2016 Technical Preview only.

[<78> Section 2.2.12.2.3](#Appendix_A_Target_78): The **DNSSRV\_ZONE\_TRANSFER\_STATS** structure is available in Windows Server 2012 R2 and Windows Server 2016 Technical Preview only.

[<79> Section 2.2.12.2.4](#Appendix_A_Target_79): The **DNSSRV\_ZONE\_UPDATE\_STATS** structure is available in Windows 8.1, Windows Server 2012 R2, Windows 10, and Windows Server 2016 Technical Preview only.

[<80> Section 2.2.12.2.5](#Appendix_A_Target_80): The **DNS\_RPC\_ZONE\_STATS\_V1** structure is available in Windows Server 2012 R2 and Windows Server 2016 Technical Preview only.

[<81> Section 2.2.13.2.1](#Appendix_A_Target_81): The **DNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST** structure is available in Windows Server 2012 R2 and Windows Server 2016 Technical Preview only.

[<82> Section 2.2.13.2.2.1](#Appendix_A_Target_82): The **DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1** structure is available in Windows Server 2012 R2 and Windows Server 2016 Technical Preview only.

[<83> Section 2.2.13.2.3.1](#Appendix_A_Target_83): The **DNS\_RPC\_ZONE\_SCOPE\_INFO\_V1** structure is available in Windows Server 2012 R2 and Windows Server 2016 Technical Preview only.

[<84> Section 2.2.14.1.1](#Appendix_A_Target_84): The **DNS\_RPC\_ENUM\_SCOPE\_LIST** structure is supported in Windows Server 2012 R2 with [[MSKB-2919355]](http://go.microsoft.com/fwlink/?LinkId=397642) and Windows Server 2016 Technical Preview and is reserved for future use.

[<85> Section 2.2.15](#Appendix_A_Target_85): DNS Policy constants and structures are implemented in Windows 10 and Windows Server 2016 Technical Preview only.

[<86> Section 2.3](#Appendix_A_Target_86): The dnsProperty and dnsRecord attributes, and their associated properties, are not supported on Windows NT 4.0.

[<87> Section 2.3](#Appendix_A_Target_87): The following attributes of dnsZone are supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview:

* msDNS-IsSigned
* msDNS-NSEC3OptOut
* msDNS-SigningKeys
* msDNS-SignWithNSEC3
* msDNS-NSEC3UserSalt
* msDNS-DNSKEYRecords
* msDNS-DSRecordSetTTL
* msDNS-NSEC3Iterations
* msDNS-PropagationTime
* msDNS-NSEC3CurrentSalt
* msDNS-RFC5011KeyRollovers
* msDNS-NSEC3HashAlgorithm
* msDNS-DSRecordAlgorithms
* msDNS-DNSKEYRecordSetTTL
* msDNS-MaintainTrustAnchor
* msDNS-NSEC3RandomSaltLength
* msDNS-SigningKeyDescriptors
* msDNS-SignatureInceptionOffset
* msDNS-ParentHasSecureDelegation
* msDNS-SecureDelegationPollingPeriod

[<88> Section 2.3.1.1](#Appendix_A_Target_88): msDNS-ServerSettings is supported only by Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<89> Section 2.3.2.1.1](#Appendix_A_Target_89): The following table lists dnsProperty Ids that are supported under different versions of Windows Server.

| Property Name | Windows NT 4.0 | Windows 2000 | Windows Server 2003 | Windows Server 2008 | Windows Server 2008 R2 | Windows Server 2012 | Windows Server 2012 R2 | Windows Server 2016 Technical Preview |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DSPROPERTY\_ZONE\_TYPE |  | X | X | X | X | X | X | X |
| DSPROPERTY\_ZONE\_ALLOW\_UPDATE |  | X | X | X | X | X | X | X |
| DSPROPERTY\_ZONE\_SECURE\_TIME |  | X | X | X | X | X | X | X |
| DSPROPERTY\_ZONE\_NONREFRESH\_INTERVAL |  | X | X | X | X | X | X | X |
| DSPROPERTY\_ZONE\_REFRESH\_INTERVAL |  | X | X | X | X | X | X | X |
| DSPROPERTY\_ZONE\_AGING\_STATE |  | X | X | X | X | X | X | X |
| DSPROPERTY\_ZONE\_SCAVENGING\_SERVERS |  | X | X | X | X | X | X | X |
| DSPROPERTY\_ZONE\_DELETED\_FROM\_HOSTNAME |  | X | X |  |  |  |  | X |
| DSPROPERTY\_ZONE\_AGING\_ENABLED\_TIME |  |  |  | X | X | X | X | X |
| DSPROPERTY\_ZONE\_MASTER\_SERVERS |  |  |  | X | X | X | X | X |
| DSPROPERTY\_ZONE\_AUTO\_NS\_SERVERS |  |  | X | X | X | X | X | X |
| DSPROPERTY\_ZONE\_DCPROMO\_CONVERT |  |  | X | X | X | X | X | X |
| DSPROPERTY\_ZONE\_SCAVENGING\_SERVERS\_DA |  |  |  | X | X | X | X | X |
| DSPROPERTY\_ZONE\_MASTER\_SERVERS\_DA |  |  |  | X | X | X | X | X |
| DSPROPERTY\_ZONE\_AUTO\_NS\_SERVERS\_DA |  |  |  | X | X | X | X | X |
| DSPROPERTY\_ZONE\_NODE\_DBFLAGS |  | X | X | X | X | X | X | X |

[<90> Section 2.3.2.1.1](#Appendix_A_Target_90): The DNS server does not write the DSPROPERTY\_ZONE\_SCAVENGING\_SERVERS [propertyId](#Section_3af638710cc44179916c5caade55a8f3) if ForceForestBehaviorVersion (section [3.1.1.1.1](#Section_8903e50a91834a7d964053f6f5a91481)) indicates a forest (1) behavior version corresponding to Windows NT, Windows 2000, or Windows Server 2003.

[<91> Section 2.3.2.1.1](#Appendix_A_Target_91): Windows 2000 and Windows Server 2003 initialize this value with the hostname of the server when the zone is being deleted and preserve the value at all other times. Windows Server 2008 and Windows Server 2008 R2 ignore this value. Windows NT Server 4.0 does not support this structure. The hostname written is the FQDN of the local machine, as determined by the GetComputerNameExW system call.

[<92> Section 2.3.2.1.1](#Appendix_A_Target_92): The DNS server does not write the DSPROPERTY\_ZONE\_MASTER\_SERVERS propertyId if ForceForestBehaviorVersion (section 3.1.1.1.1) indicates a forest behavior version corresponding to Windows NT, Windows 2000, or Windows Server 2003.

[<93> Section 2.3.2.1.1](#Appendix_A_Target_93): The DNS server does not write the DSPROPERTY\_ZONE\_AUTO\_NS\_SERVERS propertyId if ForceForestBehaviorVersion (section 3.1.1.1.1) indicates a forest behavior version corresponding to Windows NT, Windows 2000, or Windows Server 2003.

[<94> Section 2.3.2.1.2](#Appendix_A_Target_94): The RODC mode check is not supported on Windows NT, Windows 2000, and Windows Server 2003.

[<95> Section 2.3.2.1.2](#Appendix_A_Target_95): The DcPromo flags are not supported on Windows NT and Windows 2000.

[<96> Section 3.1.1](#Appendix_A_Target_96): Windows Server (except Windows NT Server 4.0 which predates Active Directory) uses "cn=MicrosoftDNS,cn=System" as the constant container relative distinguished name. A complete DS Container string could, for example, be "cn=MicrosoftDNS,cn=System,DC=corp,DC=contoso,DC=com". The access control list is stored in the ntSecurityDescriptor attribute of this container and can be modified using standard LDAP modify operations (see [[MS-ADTS]](file:///E:\Target\Windows\Published\Books\MS-DNSP\%5bMS-ADTS%5d.pdf) section 3.1.1.5.3).

[<97> Section 3.1.1](#Appendix_A_Target_97): In Windows, this access control list by default grants Full Control to the Domain Administrators group, Full Control to members of the "DnsAdmins" group, and Full Control to members of the Enterprise Domain Controllers group if the DNS server is Active Directory integrated, and Full control to the Administrators group and the System Operators group otherwise.

[<98> Section 3.1.1](#Appendix_A_Target_98): Windows Server (except Windows NT Server 4.0 which predates Active Directory) uses the **dnsTombstoned** attribute to store DNS Record Tombstone State in the directory server. A value of TRUE indicates that the node is a tombstone. Any other value indicates that the node is not a tombstone. Windows Server does not support DNS Record Tombstone state for zones that are not stored in the directory server.

[<99> Section 3.1.1](#Appendix_A_Target_99): In Windows 2000, Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2, this Access Control List by default grants Full Control to the Domain Administrators Group, Create All Child Objects privilege to Authenticated Users, and Read privilege to Everyone. If the zone is not stored in the DNS Forest Partition in the directory server, Full Control is also granted to the "DnsAdmins" group. In Windows Server 2008 and Windows Server 2008 R2, Full Control is also granted to members of the Enterprise Domain Controllers group, and Container Inheritance is enabled. In all other versions of Windows, Container Inheritance is not enabled.

[<100> Section 3.1.1](#Appendix_A_Target_100): Only Windows Server 2012, Windows Server 2012 R2 and Windows Server 2016 Technical Preview support this element.

[<101> Section 3.1.1](#Appendix_A_Target_101): Only Windows Server 2012, Windows Server 2012 R2 and Windows Server 2016 Technical Preview support this element.

[<102> Section 3.1.1](#Appendix_A_Target_102): The Windows 2000 DNS server does not implement an Application Directory Partition Table and does not support any operations related to application directory partitions.

[<103> Section 3.1.1](#Appendix_A_Target_103): Windows Server except Windows NT Server 4.0 (which predates Active Directory) and Windows 2000 (which predates Application Directory Partitions) use "CN=MicrosoftDNS,CN=PartitionName" as the container relative distinguished name, where PartitionName is ForestDnsZones, DomainDnsZones, or a custom label specified by the administrator. A complete distinguished name for the object where this Access Control List is stored could be, for example, "CN=MicrosoftDNS,CN=DomainDnsZones,DC=corp,DC=contoso,DC=com". The access control list is stored in the **ntSecurityDescriptor** attribute of this container and can be modified using standard LDAP modify operations (see [MS-ADTS] section 3.1.1.5.3).

By default this Access Control List grants Full Control to members of the "DnsAdmins" group, Full Control to members of the Enterprise Domain Controllers group, and if the name of this partition is not ForestDnsZones Full Control to members of the Domain Administrators group.

[<104> Section 3.1.1](#Appendix_A_Target_104): Windows Server uses the LocalSystem account as the default **DNS Server Credentials**.

[<105> Section 3.1.1](#Appendix_A_Target_105): Windows NT 4.0 and Windows 2000 do not support DownlevelDCsInDomain. All the supporting versions of the DNS servers acquire the value using the LDAP filter "(&(objectCategory=ntdsDsa)(!(msDS-Behavior-Version>=x))(|(msDS-HasMasterNCs=y)(hasMasterNCs=y)))", where x is the forest functional level value ("ms-DS-Behavior-Version: Forest Functional Level", [MS-ADTS] section 6.1.4.4) that corresponds to that of Windows Server 2003, and y is the domain partition value ("nTDSDSA Object", [MS-ADTS] section 6.1.1.2.2.1.2.1.1).

[<106> Section 3.1.1.1.1](#Appendix_A_Target_106): Range verification is not supported in Windows NT 4.0, Windows 2000, and Windows Server 2003. In these versions, the range is unlimited, unless otherwise specified for a property. On upgrade, from Windows NT 4.0, Windows 2000, or Windows Server 2003 to Windows Server 2008 or Windows Server 2008 R2, range verification is enforced on values set under the previous version. On upgrade, if the value is zero, but not in the new version's range, and the zero value is disallowed, then the default value is used.

[<107> Section 3.1.1.1.1](#Appendix_A_Target_107): In Windows NT 4.0 this property does not exist.

[<108> Section 3.1.1.1.1](#Appendix_A_Target_108): In Windows NT 4.0 this property does not exist.

[<109> Section 3.1.1.1.1](#Appendix_A_Target_109): In Windows NT 4.0 and Windows 2000 this property does not exist.

[<110> Section 3.1.1.1.1](#Appendix_A_Target_110): In Windows NT 4.0, Windows 2000, and Windows Server 2003, the default value is 0x00000001.

[<111> Section 3.1.1.1.1](#Appendix_A_Target_111): Windows NT 4.0 does not implement this property.

[<112> Section 3.1.1.1.1](#Appendix_A_Target_112): Windows NT 4.0 does not support this property.

[<113> Section 3.1.1.1.1](#Appendix_A_Target_113): Windows NT 4.0 does not support this property.

[<114> Section 3.1.1.1.1](#Appendix_A_Target_114): Windows NT 4.0 and Windows 2000 do not support this property.

[<115> Section 3.1.1.1.1](#Appendix_A_Target_115): In Windows NT 4.0 and Windows 2000, the default value is 0x0000012C (5 minutes).

[<116> Section 3.1.1.1.1](#Appendix_A_Target_116): In Windows NT 4.0, Windows 2000, and Windows Server 2003, the default value is 0x00093A80 (7 days).

[<117> Section 3.1.1.1.1](#Appendix_A_Target_117): In Windows NT 4.0, Windows 2000, and Windows Server 2003, the default value is 0x00000005.

[<118> Section 3.1.1.1.1](#Appendix_A_Target_118): Windows NT 4.0 uses zero as the default value.

[<119> Section 3.1.1.1.1](#Appendix_A_Target_119): In Windows NT 4.0 this parameter is not implemented. In Windows 2000, the default value is 0x04000000 (4 MB).

[<120> Section 3.1.1.1.1](#Appendix_A_Target_120): The following table lists DNS\_LOG\_LEVELS flags that are supported for different versions of Windows Server. Where a flag is unsupported, the flag will be stored but ignored.

| Property Name | Windows NT 4.0 | Windows 2000 | Windows Server 2003 | Windows Server 2008 | Windows Server 2008 R2 | Windows Server 2012 | Windows Server 2012 R2 | Windows Server 2016 Technical Preview |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DNS\_LOG\_LEVEL\_ANSWERS | X | X | X | X | X | X | X | X |
| DNS\_LOG\_LEVEL\_DS\_UPDATE | X | X |  |  |  |  |  |  |
| DNS\_LOG\_LEVEL\_DS\_WRITE | X | X |  |  |  |  |  |  |
| DNS\_LOG\_LEVEL\_FULL\_PACKETS | X | X | X | X | X | X | X | X |
| DNS\_LOG\_LEVEL\_NOTIFY | X | X | X | X | X | X | X | X |
| DNS\_LOG\_LEVEL\_QUERY | X | X | X | X | X | X | X | X |
| DNS\_LOG\_LEVEL\_QUESTIONS | X | X | X | X | X | X | X | X |
| DNS\_LOG\_LEVEL\_RECV | X | X | X | X | X | X | X | X |
| DNS\_LOG\_LEVEL\_SEND | X | X | X | X | X | X | X | X |
| DNS\_LOG\_LEVEL\_TCP | X | X | X | X | X | X | X | X |
| DNS\_LOG\_LEVEL\_UDP | X | X | X | X | X | X | X | X |
| DNS\_LOG\_LEVEL\_UNMATCHED\_RESPONSE |  |  |  |  | X | X | X | X |
| DNS\_LOG\_LEVEL\_UPDATE | X | X | X | X | X | X | X | X |
| DNS\_LOG\_LEVEL\_WRITE\_THROUGH | X | X | X | X | X | X | X | X |

[<121> Section 3.1.1.1.1](#Appendix_A_Target_121): Windows NT 4.0 does not implement this property.

[<122> Section 3.1.1.1.1](#Appendix_A_Target_122): This parameter is implemented only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<123> Section 3.1.1.1.1](#Appendix_A_Target_123): In Windows NT 4.0 the default value is 0x00000003.

[<124> Section 3.1.1.1.1](#Appendix_A_Target_124): Windows NT 4.0 does not implement this property.

[<125> Section 3.1.1.1.1](#Appendix_A_Target_125): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<126> Section 3.1.1.1.1](#Appendix_A_Target_126): In Windows NT 4.0, this property is not implemented.

[<127> Section 3.1.1.1.1](#Appendix_A_Target_127): In Windows NT 4.0, this property is not supported.

[<128> Section 3.1.1.1.1](#Appendix_A_Target_128): In Windows NT 4.0, Windows 2000, and Windows Server 2003, the default value is 0x0000000F.

[<129> Section 3.1.1.1.1](#Appendix_A_Target_129): In Windows NT 4.0 and Windows 2000, this property is not implemented. In Windows Server 2003, the default value is 0x00000001.

[<130> Section 3.1.1.1.1](#Appendix_A_Target_130): In Windows NT 4.0, Windows 2000, Windows Server 2003, and Windows Server 2008, the default value is 0xFFFFFFFF.

[<131> Section 3.1.1.1.1](#Appendix_A_Target_131): In Windows NT 4.0 the default value is 0.

[<132> Section 3.1.1.1.1](#Appendix_A_Target_132): In Windows NT 4.0, this property is not implemented. In Windows 2000 and Windows Server 2003, the value's range MUST be unlimited, and the value zero MUST be treated as a flag value for 0xFFFFFFFF.

[<133> Section 3.1.1.1.1](#Appendix_A_Target_133): Windows NT 4.0 does not implement this property.

[<134> Section 3.1.1.1.1](#Appendix_A_Target_134): In Windows NT 4.0, this property is not implemented. In Windows 2000, the default value is 0x00000001.

[<135> Section 3.1.1.1.1](#Appendix_A_Target_135): In Windows NT 4.0, Windows 2000, Windows Server 2003, and Windows Server 2008, this value is not implemented.

[<136> Section 3.1.1.1.1](#Appendix_A_Target_136): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<137> Section 3.1.1.1.1](#Appendix_A_Target_137): Windows NT 4.0 does not implement this property.

[<138> Section 3.1.1.1.1](#Appendix_A_Target_138): Windows NT Server 4.0 and Windows 2000 do not limit this value.

[<139> Section 3.1.1.1.1](#Appendix_A_Target_139): In Windows NT 4.0 and Windows 2000, this property is not implemented. In Windows Server 2003, the default value is 0x0000000F, the minimum value is 0x00000003, the maximum value is 0x00000078, and values greater than the maximum or less than the minimum are treated as flag values for the maximum and minimum respectively.

[<140> Section 3.1.1.1.1](#Appendix_A_Target_140): In Windows NT 4.0 and Windows 2000, this property is not implemented. In Windows Server 2003, the default value is 0x00000001.

[<141> Section 3.1.1.1.1](#Appendix_A_Target_141): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<142> Section 3.1.1.1.1](#Appendix_A_Target_142): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<143> Section 3.1.1.1.1](#Appendix_A_Target_143): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<144> Section 3.1.1.1.1](#Appendix_A_Target_144): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<145> Section 3.1.1.1.1](#Appendix_A_Target_145): In Windows NT 4.0 and Windows 2000, this property is not implemented. In Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 operating system, and Windows Server 2016 Technical Preview, the default value is 0x00015180 (1 day), and the allowed range is 0x00000E10 (1 hour) to 0x00EFF100 (182 days).

[<146> Section 3.1.1.1.1](#Appendix_A_Target_146): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<147> Section 3.1.1.1.1](#Appendix_A_Target_147): This property is not implemented in Windows NT 4.0 and Windows 2000. Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview process DNSSEC based on [[RFC2535]](http://go.microsoft.com/fwlink/?LinkId=107021) and the value is an enumerated DWORD, with the permitted range between 0x00000000 to 0x00000002, inclusive. The meaning of the allowed values is indicated in the following table.

| Name/Value | Meaning |
| --- | --- |
| DNS\_DNSSEC\_DISABLED  0x00000000 | The server will not include DNSSEC information in responses. |
| DNS\_DNSSEC\_ENABLED\_IF\_EDNS  0x00000001 | The server will include DNSSEC information in a response only if the client request had EDNS [[RFC2671]](http://go.microsoft.com/fwlink/?LinkId=107022) enabled. |
| DNS\_DNSSEC\_ENABLED\_ALWAYS  0x00000002 | The server will include DNSSEC information in a response whenever such information is available. |

[<148> Section 3.1.1.1.1](#Appendix_A_Target_148): In Windows NT 4.0 and Windows 2000, this property is not implemented. In Windows Server 2008 the default value is zero.

[<149> Section 3.1.1.1.1](#Appendix_A_Target_149): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<150> Section 3.1.1.1.1](#Appendix_A_Target_150): In Windows NT 4.0 and Windows 2000, this property is not implemented. Default values are as follows:

* Windows Server 2003: zero (FALSE)
* Windows Server 2008: nonzero value (TRUE)
* Windows Server 2008 R2: nonzero value (TRUE)

[<151> Section 3.1.1.1.1](#Appendix_A_Target_151): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<152> Section 3.1.1.1.1](#Appendix_A_Target_152): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<153> Section 3.1.1.1.1](#Appendix_A_Target_153): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<154> Section 3.1.1.1.1](#Appendix_A_Target_154): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<155> Section 3.1.1.1.1](#Appendix_A_Target_155): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<156> Section 3.1.1.1.1](#Appendix_A_Target_156): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<157> Section 3.1.1.1.1](#Appendix_A_Target_157): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<158> Section 3.1.1.1.1](#Appendix_A_Target_158): In Windows NT 4.0 and Windows 2000, this property is not implemented. In Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview, the default value is 0x00015180 (1 day).

[<159> Section 3.1.1.1.1](#Appendix_A_Target_159): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<160> Section 3.1.1.1.1](#Appendix_A_Target_160): In Windows NT 4.0 and Windows 2000, this property is not implemented. In Windows Server 2003, the default value is 0xFFFFFFFF (DNS\_SERVER\_UNLIMITED\_CACHE\_SIZE).

[<161> Section 3.1.1.1.1](#Appendix_A_Target_161): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<162> Section 3.1.1.1.1](#Appendix_A_Target_162): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<163> Section 3.1.1.1.1](#Appendix_A_Target_163): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<164> Section 3.1.1.1.1](#Appendix_A_Target_164): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<165> Section 3.1.1.1.1](#Appendix_A_Target_165): In Windows, the default value varies with the operating system version. In Windows Server 2003, and Windows Server 2008, the default value is 0x00000500. In Windows Server 2008 R2, the default value is 0x00000FA0.

[<166> Section 3.1.1.1.1](#Appendix_A_Target_166): This property is not supported in Windows NT 4.0 or Windows 2000.

[<167> Section 3.1.1.1.1](#Appendix_A_Target_167): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<168> Section 3.1.1.1.1](#Appendix_A_Target_168): Windows NT 4.0 and Windows 2000 do not support this property.

[<169> Section 3.1.1.1.1](#Appendix_A_Target_169): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<170> Section 3.1.1.1.1](#Appendix_A_Target_170): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<171> Section 3.1.1.1.1](#Appendix_A_Target_171): Windows NT 4.0, Windows 2000, and Windows Server 2003 do not support these properties.

[<172> Section 3.1.1.1.1](#Appendix_A_Target_172): In Windows NT 4.0, Windows 2000, Windows Server 2003, and Windows Server 2008 R2, this property is not implemented.

[<173> Section 3.1.1.1.1](#Appendix_A_Target_173): This property is not supported on Windows NT 4.0, Windows 2000, or Windows Server 2003.

[<174> Section 3.1.1.1.1](#Appendix_A_Target_174): On Windows Server 2008 and Windows Server 2008 R2, the default value is 0x00000001. On Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview, the default value is 0x00000000.

[<175> Section 3.1.1.1.1](#Appendix_A_Target_175): This property is not supported in Windows NT 4.0, Windows 2000, or on Windows Server 2003

[<176> Section 3.1.1.1.1](#Appendix_A_Target_176): The **EnableGlobalQueryBlockList** property is not supported in Windows NT, Windows 2000, or Windows Server 2003.

[<177> Section 3.1.1.1.1](#Appendix_A_Target_177): The **OpenACLOnProxyUpdates** and **CacheLockingPercent** properties are not supported in Windows NT, Windows 2000, Windows Server 2003, or Windows Server 2008.

[<178> Section 3.1.1.1.1](#Appendix_A_Target_178): **ZoneWritebackInterval** is available only in Windows Server 2012 R2 and Windows Server 2016 Technical Preview.

[<179> Section 3.1.1.1.2](#Appendix_A_Target_179): Windows NT Server 4.0, Windows 2000, and Windows Server 2003 use DNSSRV\_TYPEID\_IPARRAY for input and return values. Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview accept DNSSRV\_TYPEID\_IPARRAY and DNSSRV\_TYPEID\_ADDRARRAY as input and output DNSSRV\_TYPEID\_ADDRARRAY unless dwClientVersion is used to request a previous format.

[<180> Section 3.1.1.1.2](#Appendix_A_Target_180): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<181> Section 3.1.1.1.2](#Appendix_A_Target_181): Windows 2000 does not support these properties.

[<182> Section 3.1.1.1.3](#Appendix_A_Target_182): Windows 2000 does not support these properties.

[<183> Section 3.1.1.1.3](#Appendix_A_Target_183): If the path or filename is not absolute, Windows Server stores the log file relative to the "%SystemRoot%\System32" directory.

[<184> Section 3.1.1.1.3](#Appendix_A_Target_184): Windows 2000 and Windows 2003 do not support these properties.

[<185> Section 3.1.1.1.3](#Appendix_A_Target_185): In Windows NT 4.0 and Windows 2000, this property is not implemented.

[<186> Section 3.1.1.1.3](#Appendix_A_Target_186): This parameter is implemented only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<187> Section 3.1.1.1.4](#Appendix_A_Target_187): Windows 2000 and Windows Server 2003 do not support these properties.

[<188> Section 3.1.1.2.1](#Appendix_A_Target_188): On Windows, it is written into the system32\dns directory.

[<189> Section 3.1.1.2.1](#Appendix_A_Target_189): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<190> Section 3.1.1.2.1](#Appendix_A_Target_190): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<191> Section 3.1.1.2.1](#Appendix_A_Target_191): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<192> Section 3.1.1.2.1](#Appendix_A_Target_192): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<193> Section 3.1.1.2.1](#Appendix_A_Target_193): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<194> Section 3.1.1.2.1](#Appendix_A_Target_194): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<195> Section 3.1.1.2.1](#Appendix_A_Target_195): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<196> Section 3.1.1.2.1](#Appendix_A_Target_196): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<197> Section 3.1.1.2.1](#Appendix_A_Target_197): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<198> Section 3.1.1.2.1](#Appendix_A_Target_198): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<199> Section 3.1.1.2.1](#Appendix_A_Target_199): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<200> Section 3.1.1.2.1](#Appendix_A_Target_200): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<201> Section 3.1.1.2.1](#Appendix_A_Target_201): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<202> Section 3.1.1.2.1](#Appendix_A_Target_202): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<203> Section 3.1.1.2.1](#Appendix_A_Target_203): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<204> Section 3.1.1.2.1](#Appendix_A_Target_204): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<205> Section 3.1.1.2.1](#Appendix_A_Target_205): This property is not supported on Windows NT 4.0.

[<206> Section 3.1.1.2.1](#Appendix_A_Target_206): This property is not supported on Windows NT 4.0 and Windows 2000. Furthermore, it is only supported on zones configured for forwarding.

[<207> Section 3.1.1.2.1](#Appendix_A_Target_207): This property is not supported on Windows NT 4.0 and Windows 2000. Furthermore, it is only supported on zones configured for forwarding.

[<208> Section 3.1.1.2.1](#Appendix_A_Target_208): This property is supported only on Windows NT 4.0.

[<209> Section 3.1.1.2.1](#Appendix_A_Target_209): The PluginEnabled property of a zone is available in Windows Server 2012 R2 and Windows Server 2016 Technical Preview only.

[<210> Section 3.1.1.2.2](#Appendix_A_Target_210): Windows 2000 does not support these properties.

[<211> Section 3.1.1.2.3](#Appendix_A_Target_211): Windows 2000 does not support these properties.

[<212> Section 3.1.1.2.3](#Appendix_A_Target_212): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<213> Section 3.1.1.2.3](#Appendix_A_Target_213): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<214> Section 3.1.1.2.3](#Appendix_A_Target_214): This property is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<215> Section 3.1.1.2.5](#Appendix_A_Target_215): DNS zone scope configuration information is available in Windows Server 2012 R2 and Windows Server 2016 Technical Preview only. Zone scopes inherit all the properties and configurations of the zone in which they are created unless overridden explicitly.

[<216> Section 3.1.1.3.2](#Appendix_A_Target_216): Windows NT Server 4.0, Windows 2000, and Windows Server 2003 use DNSSRV\_TYPEID\_IPARRAY for input and return values. Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview accept DNSSRV\_TYPEID\_IPARRAY and DNSSRV\_TYPEID\_ADDRARRAY as input and output DNSSRV\_TYPEID\_ADDRARRAY unless dwClientVersion is used to request a previous format.

[<217> Section 3.1.3](#Appendix_A_Target_217): Windows NT 4.0 does not support invocation of the Netlogon protocol implementation.

[<218> Section 3.1.4](#Appendix_A_Target_218): Windows 2000 supports only opnums 0 through 4.

[<219> Section 3.1.4.1](#Appendix_A_Target_219): The following values are implemented in Windows Server 2016 Technical Preview only.

* CreateClientSubnetRecord
* DeleteClientSubnetRecord
* DeleteSubnetsInRecord
* AddSubnetsInRecord
* ResetClientSubnetRecord
* CreatePolicy
* DeletePolicy
* UpdatePolicy

[<220> Section 3.1.4.1](#Appendix_A_Target_220): In Windows, the DNS server process can fail on the Restart command.

[<221> Section 3.1.4.1](#Appendix_A_Target_221): Windows 2000 uses DNSSRV\_TYPEID\_ZONE\_CREATE\_W2K. Windows Server 2003 uses DNSSRV\_TYPEID\_ZONE\_CREATE\_DOTNET.

[<222> Section 3.1.4.1](#Appendix_A_Target_222): Windows NT Server 4.0 and Windows 2000 return error 9611 (invalid DNS zone type) for ZoneCreate operations with DNS\_ZONE\_TYPE\_STUB or DNS\_ZONE\_TYPE\_CACHE record types. Windows returns the same error for DNS\_ZONE\_TYPE\_CACHE and DNS\_ZONE\_TYPE\_SECONDARY\_CACHE.

[<223> Section 3.1.4.1](#Appendix_A_Target_223): Windows 2000 returns a failure for this value of pszOperation. Windows Server 2003 accepts DWORD input only. The Windows Server 2003 DNS client sends DWORD input.

[<224> Section 3.1.4.1](#Appendix_A_Target_224): Windows XP and Windows Server 2003 accept DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY and do not accept DNSSRV\_TYPEID\_ADDRARRAY and DNS\_ADDR\_ARRAY. Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview accept DNSSRV\_TYPEID\_ADDR\_ARRAY and DNS\_ADDR\_ARRAY and do not accept DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY.

[<225> Section 3.1.4.1](#Appendix_A_Target_225): Windows 2000 uses DNSSRV\_TYPEID\_FORWARDERS\_W2K. Windows Server 2003 uses DNSSRV\_TYPEID\_FORWARDERS\_DOTNET.

[<226> Section 3.1.4.1](#Appendix_A_Target_226): Windows NT 4.0 and Windows 2000 do not support this value. Windows XP and Windows Server 2003 accept DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY and do not accept DNSSRV\_TYPEID\_ADDRARRAY and DNS\_ADDR\_ARRAY. Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview accept DNSSRV\_TYPEID\_ADDR\_ARRAY and DNS\_ADDR\_ARRAY and do not accept DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY.

[<227> Section 3.1.4.1](#Appendix_A_Target_227): See behavior note for the LogIPFilterList value.

[<228> Section 3.1.4.1](#Appendix_A_Target_228): See behavior note for the LogIPFilterList value.

[<229> Section 3.1.4.1](#Appendix_A_Target_229): This operation is supported only on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

[<230> Section 3.1.4.1](#Appendix_A_Target_230): This operation is supported in Windows Server 2012 R2 with [MSKB-2919355] and Windows Server 2016 Technical Preview and is reserved for future use.

[<231> Section 3.1.4.1](#Appendix_A_Target_231): This operation is supported in Windows Server 2012 R2 with [MSKB-2919355] and Windows Server 2016 Technical Preview and is reserved for future use.

[<232> Section 3.1.4.1](#Appendix_A_Target_232): The following values are supported on Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

* SignZone
* UnsignZone
* ResignZone
* PerformZoneKeyRollover
* PokeZoneKeyRollover
* RetrieveRootTrustAnchor
* TransferKeymasterRole

[<233> Section 3.1.4.1](#Appendix_A_Target_233): A Windows implementation allows DNS\_ZONE\_NOTIFY\_LEVEL to be set only to values 0x0 through 0x1. Attempts to set this property to a higher value result in the effective value 0x1.

[<234> Section 3.1.4.1](#Appendix_A_Target_234): Windows 2000 uses DNSSRV\_TYPEID\_ZONE\_CREATE\_W2K, and cannot convert from other types. Windows Server 2003 uses DNSSRV\_TYPEID\_ZONE\_CREATE\_DOTNET, and can convert from DNSSRV\_TYPEID\_ZONE\_CREATE\_W2K.

Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview use DNSSRV\_TYPEID\_ZONE\_CREATE and can convert from DNSSRV\_TYPEID\_ZONE\_CREATE\_W2K and DNSSRV\_TYPEID\_ZONE\_CREATE\_DOTNET.

[<235> Section 3.1.4.1](#Appendix_A_Target_235): Windows 2000 uses DNSSRV\_TYPEID\_ZONE\_DATABASE\_W2K. Windows Server 2003 uses DNSSRV\_TYPEID\_ZONE\_DATABASE.

[<236> Section 3.1.4.1](#Appendix_A_Target_236): If ForceForestBehaviorVersion (section 3.1.1.1.1) indicates a forest behavior version of Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016 Technical Preview the server writes only DNS\_ADDR\_ARRAY values to the directory server. Otherwise, the server writes both IP4\_ARRAY and DNS\_ADDR\_ARRAY values. Windows NT 4.0, Windows 2000, and Windows Server 2003 do not support this forest version check, and write only IP4\_ARRAY values to the directory server.

Windows 2000 and Windows Server 2003 accept DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY and silently disregard DNSSRV\_TYPEID\_ADDRARRAY and DNS\_ADDR\_ARRAY. They also write only the IP4\_ARRAY value to the directory server if the server is DS-integrated; when reading from the directory server, only the IP4\_ARRAY value is read, and any DNS\_ADDR\_ARRAY values are ignored. Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview accept DNSSRV\_TYPEID\_ADDRARRAY and DNS\_ADDR\_ARRAY and do not accept DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY, and write both formats to the directory server if the server is DS-integrated; when reading from the directory server, the DNS\_ADDR\_ARRAY value is read if it exists; otherwise the IP4\_ARRAY value is read.

[<237> Section 3.1.4.1](#Appendix_A_Target_237): Windows 2000 does not support this operation. Windows Server 2003 accepts DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY and does not accept DNSSRV\_TYPEID\_ADDRARRAY and DNS\_ADDR\_ARRAY. Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview accept DNSSRV\_TYPEID\_ADDR\_ARRAY and DNS\_ADDR\_ARRAY and do not accept DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY.

[<238> Section 3.1.4.1](#Appendix_A_Target_238): Windows 2000 uses DNSSRV\_TYPEID\_ZONE\_SECONDARIES\_W2K. Windows Server 2003 uses DNSSRV\_TYPEID\_ZONE\_SECONDARIES\_DOTNET.

[<239> Section 3.1.4.1](#Appendix_A_Target_239): See behavior note for the MasterServer value.

[<240> Section 3.1.4.1](#Appendix_A_Target_240): See behavior note for the MasterServer value.

[<241> Section 3.1.4.1](#Appendix_A_Target_241): CreateZoneScope is available only in Windows Server 2012 R2 and Windows Server 2016 Technical Preview.

[<242> Section 3.1.4.1](#Appendix_A_Target_242): DeleteZoneScope is available only in Windows Server 2012 R2 and Windows Server 2016 Technical Preview.

[<243> Section 3.1.4.1](#Appendix_A_Target_243): In Windows NT 4.0, Windows 2000, and Windows Server 2003, no range limiting or zero/nonzero restrictions are applied.

[<244> Section 3.1.4.1](#Appendix_A_Target_244): The following table lists property names that are supported as an input to the *pszOperation* parameter for different versions of Windows Server.

| Property name | Windows NT 4.0 | Windows 2000 | Windows Server 2003 | Windows Server 2008 | Windows Server 2008 R2 | Windows Server 2012 | Windows Server 2012 R2 | Windows Server 2016 Technical Preview |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| AdditionalRecursionTimeout |  |  | X | X | X | X | X | X |  |
| AddressAnswerLimit | X | X | X | X | X | X | X | X |  |
| AdminConfigured |  | X | X | X | X | X | X | X |  |
| AllowCNAMEAtNS |  | X | X | X | X | X | X | X |  |
| AllowMsdcsLookupRetry |  |  |  | X |  |  |  |  |  |
| AllowReadOnlyZoneTransfer |  |  |  | X | X | X | X | X |  |
| AllowUpdate | X | X | X | X | X | X | X | X |  |
| AppendMsZoneTransferTag |  |  | X | X | X | X | X | X |  |
| AutoCacheUpdate | X | X | X | X | X | X | X | X |  |
| AutoConfigFileZones |  |  | X | X | X | X | X | X |  |
| AutoCreateDelegations |  |  | X | X | X | X | X | X |  |
| BindSecondaries | X | X | X | X | X | X | X | X |  |
| BootMethod | X | X | X | X | X | X | X | X |  |
| BreakOnAscFailure |  |  | X | X | X | X | X | X |  |
| CacheEmptyAuthResponses |  |  | X | X | X | X | X | X |  |
| CacheLockingPercent |  |  |  |  | X | X | X | X |  |
| DebugLevel | X | X | X | X | X | X | X | X |  |
| DefaultAgingState |  | X | X | X | X | X | X | X |  |
| DefaultNoRefreshInterval |  | X | X | X | X | X | X | X |  |
| DefaultRefreshInterval |  | X | X | X | X | X | X | X |  |
| DeleteOutsideGlue | X | X | X | X | X | X | X | X |  |
| DirectoryPartitionAutoEnlistInterval |  |  | X | X | X | X | X | X |  |
| DisjointNets | X | X | X | X | X | X | X | X |  |
| DsBackgroundLoadPaused |  |  |  | X | X | X | X | X |  |
| DsLazyUpdateInterval |  |  | X | X | X | X | X | X |  |
| DsMinimumBackgroundLoadThreads |  |  |  | X | X | X | X | X |  |
| DsPollingInterval | X | X | X | X | X | X | X | X |  |
| DsRemoteReplicationDelay |  |  |  | X | X | X | X | X |  |
| DsTombstoneInterval | X | X | X | X | X | X | X | X |  |
| EDnsCacheTimeout |  |  | X | X | X | X | X | X |  |
| EnableDirectoryPartitions |  |  | X | X | X | X | X | X |  |
| EnableDnsSec |  |  | X | X | X | X | X | X |  |
| EnableDuplicateQuerySuppression |  |  |  | X | X | X | X | X |  |
| EnableEDnsProbes |  |  | X | X | X | X | X | X |  |
| EnableEDnsReception |  |  | X | X | X | X | X | X |  |
| EnableForwarderReordering |  |  |  |  |  | X | X | X |  |
| EnableGlobalNamesSupport |  |  |  | X | X | X | X | X |  |
| EnableIPv6 |  |  | X | X | X | X | X | X |  |
| EnableIQueryResponseGeneration |  |  | X | X | X | X | X | X |  |
| EnableOnlineSigning |  |  |  |  |  | X | X | X |  |
| EnablePolicies |  |  |  |  |  |  |  | X |  |
| EnableRegistryBoot | X | X | X | X | X | X | X | X |  |
| EnableRsoForRodc |  |  |  | X | X | X | X | X |  |
| EnableSendErrorSuppression |  |  | X | X | X | X | X | X |  |
| EnableUpdateForwarding |  |  | X | X | X | X | X | X |  |
| EnableVersionQuery |  |  |  | X | X | X | X | X |  |
| EnableWinsR |  |  | X | X | X | X | X | X |  |
| EventLogLevel | X | X | X | X | X | X | X | X |  |
| ForceDomainBehaviorVersion |  |  | X | X | X | X | X | X |  |
| ForceDsaBehaviorVersion |  |  | X | X | X | X | X | X |  |
| ForceForestBehaviorVersion |  |  | X | X | X | X | X | X |  |
| ForceRODCMode |  |  |  | X | X | X | X | X |  |
| ForceSoaExpire | X | X | X | X | X | X | X | X |  |
| ForceSoaMinimumTtl | X | X | X | X | X | X | X | X |  |
| ForceSoaRefresh | X | X | X | X | X | X | X | X |  |
| ForceSoaRetry | X | X | X | X | X | X | X | X |  |
| ForceSoaSerial | X | X | X | X | X | X | X | X |  |
| ForwardDelegations | X | X | X | X | X | X | X | X |  |
| ForwardingTimeout | X | X | X | X | X | X | X | X |  |
| GlobalNamesAlwaysQuerySrv |  |  |  | X | X | X | X | X |  |
| GlobalNamesBlockUpdates |  |  |  | X | X | X | X | X |  |
| GlobalNamesEnableEDnsProbes |  |  |  | X | X | X | X | X |  |
| GlobalNamesPreferAAAA |  |  |  | X | X | X | X | X |  |
| GlobalNamesQueryOrder |  |  |  | X | X | X | X | X |  |
| GlobalNamesSendTimeout |  |  |  | X | X | X | X | X |  |
| GlobalNamesServerQueryInterval |  |  |  | X | X | X | X | X |  |
| HeapDebug |  |  | X | X | X | X | X | X |  |
| IsSlave | X | X | X | X | X | X | X | X |  |
| LameDelegationTtl |  |  | X | X | X | X | X | X |  |
| LocalNetPriority | X | X | X | X | X | X | X | X |  |
| LocalNetPriorityNetMask |  |  | X | X | X | X | X | X |  |
| LogFileMaxSize |  | X | X | X | X | X | X | X |  |
| LogLevel | X | X | X | X | X | X | X | X |  |
| LooseWildcarding | X | X | X | X | X | X | X | X |  |
| MaxCacheSize |  |  | X | X | X | X | X | X |  |
| MaxCacheTtl | X | X | X | X | X | X | X | X |  |
| MaximumRodcRsoAttemptsPerCycle |  |  |  | X | X | X | X | X |  |
| MaximumRodcRsoQueueLength |  |  |  | X | X | X | X | X |  |
| MaximumSignaturesScanPeriod |  |  |  |  |  | X | X | X |  |
| MaximumUdpPacketSize |  |  | X | X | X | X | X | X |  |
| MaxNegativeCacheTtl |  | X | X | X | X | X | X | X |  |
| MaxResourceRecordsInNonSecureUpdate |  |  | X | X | X | X | X | X |  |
| MaxTrustAnchorActiveRefreshInterval |  |  |  |  |  | X | X | X |  |
| NameCheckFlag | X | X | X | X | X | X | X | X |  |
| NoRecursion | X | X | X | X | X | X | X | X |  |
| NoUpdateDelegations |  | X | X | X | X | X | X | X |  |
| OpenACLOnProxyUpdates |  |  |  |  | X | X | X | X |  |
| OperationsLogLevel |  |  | X | X | X | X | X | X |  |
| OperationsLogLevel2 |  |  | X | X | X | X | X | X |  |
| PublishAutonet |  |  | X | X | X | X | X | X |  |
| QuietRecvFaultInterval |  | X | X | X | X | X | X | X |  |
| QuietRecvLogInterval |  | X | X | X | X | X | X | X |  |
| RecurseToInternetRootMask |  |  | X | X | X | X | X | X |  |
| RecursionRetry | X | X | X | X | X | X | X | X |  |
| RecursionTimeout | X | X | X | X | X | X | X | X |  |
| ReloadException |  |  | X | X | X | X | X | X |  |
| RemoteIPv4RankBoost |  |  |  | X | X | X | X | X |  |
| RemoteIPv6RankBoost |  |  |  | X | X | X | X | X |  |
| RoundRobin | X | X | X | X | X | X | X | X |  |
| RpcProtocol | X | X | X | X | X | X | X | X |  |
| ScavengingInterval |  | X | X | X | X | X | X | X |  |
| ScopeOptionValue |  |  |  |  |  |  |  | X |  |
| SecureResponses | X | X | X | X | X | X | X | X |  |
| SelfTest |  |  | X | X | X | X | X | X |  |
| SendPort | X | X | X | X | X | X | X | X |  |
| SilentlyIgnoreCNameUpdateConflicts |  |  | X | X | X | X | X | X |  |
| SocketPoolSize |  | X | X | X | X | X | X | X |  |
| StrictFileParsing | X | X | X | X | X | X | X | X |  |
| SyncDsZoneSerial |  | X | X | X | X | X | X | X |  |
| TcpReceivePacketSize |  |  | X | X | X | X | X | X |  |
| UdpRecvThreadCount |  |  |  |  |  | X | X | X |  |
| UpdateOptions |  |  | X | X | X | X | X | X |  |
| UseSystemEventLog | X | X | X | X | X | X | X | X |  |
| Version |  |  |  | X | X | X | X | X |  |
| WriteAuthorityNs | X | X | X | X | X | X | X | X |  |
| XfrConnectTimeout |  | X | X | X | X | X | X | X |  |
| XfrThrottleMultiplier |  |  | X | X | X | X | X | X |  |
| ZoneWritebackInterval |  |  |  |  |  |  | X | X |  |

[<245> Section 3.1.4.1](#Appendix_A_Target_245): The following table lists property names that are supported as an input to the *pszOperation* parameter for different versions of Windows.

| Property name | Windows NT 4.0 | Windows | Windows Server 2003 | Windows Server 2008 | Windows Server 2008 R2 | Windows Server 2012 | Windows Server 2012 R2 | Windows Server 2016 Technical Preview |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Forwarders | X | X | X | X | X | X | X | X |
| ListenAddresses | X | X | X | X | X | X | X | X |
| BreakOnReceiveFrom |  |  | X | X | X | X | X | X |
| BreakOnUpdateFrom |  |  | X | X | X | X | X | X |
| DomainDirectoryPartitionBaseName |  |  | X | X | X | X | X | X |
| DynamicForwarders |  |  |  |  |  | X | X | X |
| ForestDirectoryPartitionBaseName |  |  | X | X | X | X | X | X |
| LogFilePath |  |  | X | X | X | X | X | X |
| LogIPFilterList |  |  | X | X | X | X | X | X |
| ServerLevelPluginDll |  |  | X | X | X | X | X | X |
| GlobalQueryBlockList |  |  |  | X | X | X | X | X |
| RootTrustAnchorsURL |  |  |  |  |  | X | X | X |
| SocketPoolExcludedPortRanges |  |  |  |  | X | X | X | X |
| DsBackgroundPauseName |  |  |  |  |  | X | X | X |

[<246> Section 3.1.4.1](#Appendix_A_Target_246): zone scopes are available only in Windows Server 2012 R2 and Windows Server 2016 Technical Preview.

[<247> Section 3.1.4.1](#Appendix_A_Target_247): Windows Server attempts to back up the log file to the "%SYSTEMROOT%\System32\dns\backup\" directory.

[<248> Section 3.1.4.1](#Appendix_A_Target_248): If ForceDomainBehaviorVersion (section 3.1.1.1.1) indicates a domain behavior version of Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016 Technical Preview, root hints MUST be written to the DNS domain partition. Otherwise, root hints MUST be written to the default application directory partition.

[<249> Section 3.1.4.1](#Appendix_A_Target_249): If ForceDomainBehaviorVersion (section 3.1.1.1.1) indicates a domain behavior version of Windows NT or Windows 2000, [**stub**](#gt_4cef864e-5108-43a7-a631-68ffc7967546) and forwarder zones MUST NOT be created in the default application directory partition. If this partition is specified during ZoneCreate, the server MUST return a failure.

[<250> Section 3.1.4.1](#Appendix_A_Target_250): Windows 2000 does not support this operation.

[<251> Section 3.1.4.1](#Appendix_A_Target_251): Windows 2000 and Windows Server 2003 do not support RODCs and do not process the **msDS-NC-RO-Replica-Locations**.

[<252> Section 3.1.4.1](#Appendix_A_Target_252): Windows 2000 and Windows Server 2003 do not support RODCs and do not process the **msDS-NC-RO-Replica-Locations**.

[<253> Section 3.1.4.1](#Appendix_A_Target_253): Windows 2000 does not support this operation. Windows Server 2003 takes a DWORD value for pData input parameter.

[<254> Section 3.1.4.1](#Appendix_A_Target_254): Windows 2000 and Windows Server 2003 do not support this operation.

[<255> Section 3.1.4.1](#Appendix_A_Target_255): Windows 2000 and Windows Server 2003 do not support this operation.

[<256> Section 3.1.4.1](#Appendix_A_Target_256): Windows 2000 and Windows Server 2003 do not support this operation.

[<257> Section 3.1.4.1](#Appendix_A_Target_257): If ForceDomainBehaviorVersion (section 3.1.1.1.1) indicates a domain behavior version of Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016 Technical Preview root hints MUST be written to the DNS domain partition. Otherwise, root hints MUST be written to the default application directory partition.

[<258> Section 3.1.4.1](#Appendix_A_Target_258): Windows stores the log file relative to the "%SystemRoot%\System32" directory, if the path or filename given is not absolute.

[<259> Section 3.1.4.1](#Appendix_A_Target_259): Windows NT 4.0 does not support invocation of the "Netlogon" protocol implementation.

[<260> Section 3.1.4.1](#Appendix_A_Target_260): Aging is not supported on Windows NT Server 4.0.

[<261> Section 3.1.4.1](#Appendix_A_Target_261): The following table lists the property names that are supported as input for the "ResetDwordProperty" operation when pszZone is not NULL, for different versions of Windows.

| Property name | Windows NT 4.0 | Windows | Windows Server 2003 | Windows Server 2008 | Windows Server 2008 R2 | Windows Server 2012 | Windows Server 2012 R2 | Windows Server 2016 Technical Preview |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| AllowUpdate | X | X | X | X | X | X | X | X |
| SecureSecondaries | X | X | X | X | X | X | X | X |
| NotifyLevel |  | X | X | X | X | X | X | X |
| LogUpdates | X | X | X | X | X | X | X | X |
| NoRefreshInterval |  | X | X | X | X | X | X | X |
| RefreshInterval |  | X | X | X | X | X | X | X |
| Aging |  | X | X | X | X | X | X | X |
| ForwarderSlave |  |  | X | X | X | X | X | X |
| ForwarderTimeout |  |  | X | X | X | X | X | X |
| Unicode | X |  |  |  |  |  |  | X |
| DsRecordAlgorithms |  |  |  |  |  | X | X | X |
| DNSKEYRecordSetTTL |  |  |  |  |  | X | X | X |
| DsRecordSetTTL |  |  |  |  |  | X | X | X |
| IsKeymaster |  |  |  |  |  | X | X | X |
| IsSigned |  |  |  |  |  | X | X | X |
| MaintainTrustAnchor |  |  |  |  |  | X | X | X |
| NSEC3HashAlgorithm |  |  |  |  |  | X | X | X |
| NSEC3Iterations |  |  |  |  |  | X | X | X |
| NSEC3OptOut |  |  |  |  |  | X | X | X |
| NSEC3RandomSaltLength |  |  |  |  |  | X | X | X |
| ParentHasSecureDelegation |  |  |  |  |  | X | X | X |
| PropagationTime |  |  |  |  |  | X | X | X |
| RFC5011KeyRollovers |  |  |  |  |  | X | X | X |
| SecureDelegationPollingPeriod |  |  |  |  |  | X | X | X |
| SignatureInceptionOffset |  |  |  |  |  | X | X | X |
| SignWithNSEC3 |  |  |  |  |  | X | X | X |
| PluginEnabled |  |  |  |  |  |  | X | X |

[<262> Section 3.1.4.1](#Appendix_A_Target_262): The following table lists property names that are supported as an input to the pszOperation parameter for different versions of Windows Server.

| Property name | Windows NT 4.0 | Windows 2000 | Windows Server 2003 | Windows Server 2008 | Windows Server 2008 R2 | Windows Server 2012 | Windows Server 2012 R2 | Windows Server 2016 Technical Preview |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Masters | X | X | X | X | X | X | X | X |
| Secondaries | X | X | X | X | X | X | X | X |
| TypeReset | X | X | X | X | X | X | X | X |
| DatabaseFile | X | X | X | X | X | X | X | X |
| AllowAutoNS |  | X | X | X | X | X | X | X |
| ScavengeServers |  | X | X | X | X | X | X | X |
| BreakOnNameUpdate |  |  | X | X | X | X | X | X |
| ChangeDP |  |  | X | X | X | X | X | X |
| LocalMasters |  |  | X | X | X | X | X | X |
| NotifyList |  |  |  |  |  |  |  |  |
| Keymaster |  |  |  |  |  | X | X | X |
| NSEC3UserSalt |  |  |  |  |  | X | X | X |
| NSEC3CurrentSalt |  |  |  |  |  | X | X | X |

[<263> Section 3.1.4.1](#Appendix_A_Target_263): If ForceDomainBehaviorVersion (section 3.1.1.1.1) indicates a domain behavior version of Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016 Technical Preview root hints MUST be written to the DNS domain partition. Otherwise, root hints MUST be written to the default application directory partition.

[<264> Section 3.1.4.1](#Appendix_A_Target_264): If ForceDomainBehaviorVersion (section 3.1.1.1.1) indicates a domain behavior version of Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016 Technical Preview root hints MUST be written to the DNS domain partition. Otherwise, root hints MUST be written to the default application directory partition.

[<265> Section 3.1.4.1](#Appendix_A_Target_265): If ForceDomainBehaviorVersion (section 3.1.1.1.1) indicates a domain behavior version of Windows NT or Windows 2000, the server MUST also verify that either the specified zone is not a stub or forwarder zone, or the destination application directory partition is not the default application directory partition. Otherwise, the server MUST return a failure.

[<266> Section 3.1.4.1](#Appendix_A_Target_266): Windows 2000 does not implement this operation and therefore will return a failure.

[<267> Section 3.1.4.1](#Appendix_A_Target_267): If ForceDomainBehaviorVersion (section 3.1.1.1.1) indicates a domain behavior version of Windows, root hints MUST be written to the DNS domain partition. Otherwise, root hints MUST be written to the default application directory partition.

[<268> Section 3.1.4.2](#Appendix_A_Target_268): The following table lists various DNSSRV\_TYPEID\_SERVER\_INFO values returned by **R\_DnsSrvQuery()**, **R\_DnsSrvQuery2()** methods, for different versions of Windows Server.

| dwClientVersion | Windows 2000 | Windows Server 2003 | Windows Server 2008 | Windows Server 2012 | Windows Server 2012 R2 | Windows Server 2016 Technical Preview |
| --- | --- | --- | --- | --- | --- | --- |
| 0x00000000 | DNSSRV\_TYPEID\_SERVER\_INFO\_W2K | DNSSRV\_TYPEID\_SERVER\_INFO\_W2K | DNSSRV\_TYPEID\_SERVER\_INFO\_W2K | DNSSRV\_TYPEID\_SERVER\_INFO\_W2K | DNSSRV\_TYPEID\_SERVER\_INFO\_W2K | DNSSRV\_TYPEID\_SERVER\_INFO\_W2K |
| 0x00060000 | DNSSRV\_TYPEID\_SERVER\_INFO\_W2K | DNSSRV\_TYPEID\_SERVER\_INFO\_DOTNET | DNSSRV\_TYPEID\_SERVER\_INFO\_DOTNET | DNSSRV\_TYPEID\_SERVER\_INFO\_DOTNET | DNSSRV\_TYPEID\_SERVER\_INFO\_DOTNET | DNSSRV\_TYPEID\_SERVER\_INFO\_DOTNET |
| 0x00070000 | DNSSRV\_TYPEID\_SERVER\_INFO\_W2K | DNSSRV\_TYPEID\_SERVER\_INFO\_DOTNET | DNSSRV\_TYPEID\_SERVER\_INFO | DNSSRV\_TYPEID\_SERVER\_INFO | DNSSRV\_TYPEID\_SERVER\_INFO | DNSSRV\_TYPEID\_SERVER\_INFO |

[<269> Section 3.1.4.2](#Appendix_A_Target_269): Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview set the dwLocalNetPriorityNetMask field of DNS\_RPC\_SERVER\_INFO to zero, regardless of the effective value of dwLocalNetPriorityNetMask.

[<270> Section 3.1.4.2](#Appendix_A_Target_270): Windows 2000 uses DNSSRV\_TYPEID\_ZONE\_W2K. Windows Server 2003 uses DNSSRV\_TYPEID\_ZONE.

[<271> Section 3.1.4.2](#Appendix_A_Target_271): Windows 2000 uses DNSSRV\_TYPEID\_ZONE\_INFO\_W2K. Windows Server 2003 uses DNSSRV\_TYPEID\_ZONE\_INFO\_DOTNET.

[<272> Section 3.1.4.2](#Appendix_A_Target_272): Windows Server 2003 does not support the "Version" property with this operation.

[<273> Section 3.1.4.2](#Appendix_A_Target_273): Windows 2000 and Windows Server 2003 use DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY.

[<274> Section 3.1.4.2](#Appendix_A_Target_274): All Windows Server versions incorrectly set pdwTypeId to DNSSRV\_TYPEID\_DWORD, and truncate ppData to DWORD size when R\_DnssrvQuery is called with pszOperation set to "ListenAddresses" or "Forwarders". Windows Server 2003 does not support the "Forwarders" and "ListenAddresses" properties here

[<275> Section 3.1.4.2](#Appendix_A_Target_275): All Windows Server versions that have the "DsBackgroundPauseName" property incorrectly set pdwTypeId to DNSSRV\_TYPEID\_DWORD, and truncate ppData to DWORD size when R\_DnssrvQuery is called with pszOperation set to "DsBackgroundPauseName".

[<276> Section 3.1.4.2](#Appendix_A_Target_276): Windows 2000 and Windows Server 2003 use DNSSRV\_TYPEID\_IPARRAY and IP4\_ARRAY.

[<277> Section 3.1.4.3](#Appendix_A_Target_277): The following pszOperations values are implemented in Windows Server 2016 Technical Preview only.

* EnumerateClientSubnetRecord
* GetClientSubnetRecord
* EnumeratePolicy
* GetPolicy

The following pszOperations values are implemented only in Windows Server 2012 R2 and Windows Server 2016 Technical Preview.

* ExportZoneSigningSettings
* ImportZoneSigningSettings
* EnumZoneScopes
* ZoneStatistics

The following pszOperations values are implemented only in Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.

* ModifyZoneSigningKeyDescriptor
* EnumZoneSigningKeyDescriptors
* GetZoneSigningKeyDescriptorState
* SetZoneSigningKeyDescriptorState
* ValidateZoneSigningParameters
* EnumerateKeyStorageProviders
* EnumerateTrustPoints
* EnumerateTrustAnchors

[<278> Section 3.1.4.3](#Appendix_A_Target_278): This operation is supported in Windows Server 2012 R2 with [MSKB-2919355] and Windows Server 2016 Technical Preview and is reserved for future use.

[<279> Section 3.1.4.5](#Appendix_A_Target_279): Windows 2000 does not support this operation. No version of Windows Server supports the DNS\_TYPE\_LOC for this operation.

[<280> Section 3.1.4.5](#Appendix_A_Target_280): Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview do not support updates or deletions of the DNS\_TYPE\_ZERO, DNS\_TYPE\_LOC, and DNS\_TYPE\_ALL types.

[<281> Section 3.1.4.5](#Appendix_A_Target_281): Windows 2000 does not allow additions with pszZoneName "..Cache" and treats pszZoneName NULL as "..RootHints". Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview treat pszZoneName NULL and pszZoneName "..Cache" as pszZoneName "..RootHints".

[<282> Section 3.1.4.7](#Appendix_A_Target_282): Windows 2000 does not support this operation.

[<283> Section 3.1.4.9](#Appendix_A_Target_283): Windows 2000 does not support this operation.

[<284> Section 3.1.4.10](#Appendix_A_Target_284): Windows 2000 does not support this operation. No version of Windows Server supports the DNS\_TYPE\_LOC for this operation.

[<285> Section 3.1.4.11](#Appendix_A_Target_285): The RPC method [R\_DnssrvUpdateRecord3](#Section_12279f8cddaf47b8890591d7635cdfea) is available only in Windows Server 2012 R2 and Windows Server 2016 Technical Preview.

[<286> Section 3.1.4.12](#Appendix_A_Target_286): The RPC method [R\_DnssrvEnumRecords3](#Section_d7d4a3ac79954d419fcf1826cce95e2c) is available only in Windows Server 2012 R2 and Windows Server 2016 Technical Preview.

[<287> Section 3.1.4.13](#Appendix_A_Target_287): The RPC method [R\_DnssrvOperation3](#Section_54044c364e9e44fb80dfffb026939b8b) is available only in Windows Server 2012 R2 and Windows Server 2016 Technical Preview.

[<288> Section 3.1.4.13](#Appendix_A_Target_288): This operation is supported in Windows Server 2012 R2 with [MSKB-2919355] and Windows Server 2016 Technical Preview. It is reserved for future use.

[<289> Section 3.1.4.14](#Appendix_A_Target_289): The RPC method R\_DnssrvQuery3 is available only in Windows Server 2012 R2 and Windows Server 2016 Technical Preview.

[<290> Section 3.1.4.14](#Appendix_A_Target_290): This operation is supported in Windows Server 2012 R2 and Windows Server 2016 Technical Preview with [MSKB-2919355] and is reserved for future use.

# Change Tracking

This section identifies changes that were made to this document since the last release. Changes are classified as New, Major, Minor, Editorial, or No change.

The revision class **New** means that a new document is being released.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

* A document revision that incorporates changes to interoperability requirements or functionality.
* The removal of a document from the documentation set.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **Editorial** means that the formatting in the technical content was changed. Editorial changes apply to grammatical, formatting, and style issues.

The revision class **No change** means that no new technical changes were introduced. Minor editorial and formatting changes may have been made, but the technical content of the document is identical to the last released version.

Major and minor changes can be described further using the following change types:

* New content added.
* Content updated.
* Content removed.
* New product behavior note added.
* Product behavior note updated.
* Product behavior note removed.
* New protocol syntax added.
* Protocol syntax updated.
* Protocol syntax removed.
* New content added due to protocol revision.
* Content updated due to protocol revision.
* Content removed due to protocol revision.
* New protocol syntax added due to protocol revision.
* Protocol syntax updated due to protocol revision.
* Protocol syntax removed due to protocol revision.
* Obsolete document removed.

Editorial changes are always classified with the change type **Editorially updated**.

Some important terms used in the change type descriptions are defined as follows:

* **Protocol syntax** refers to data elements (such as packets, structures, enumerations, and methods) as well as interfaces.
* **Protocol revision** refers to changes made to a protocol that affect the bits that are sent over the wire.

The changes made to this document are listed in the following table. For more information, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com).

| Section | Tracking number (if applicable) and description | Major change (Y or N) | Change type |
| --- | --- | --- | --- |
| [1.1](#Section_a95b05daf1fd4db394b4817fdaa1f642) Glossary | Added definition of cache scope. | Y | Content update. |
| [2.2.1.1.1](#Section_c49b8142a36441c8914a7675a573b5e4) DNS\_RPC\_TYPEID | Added cache scope to description of DNSSRV\_TYPEID\_ZONE\_SCOPE\_ENUM, DNSSRV\_TYPEID\_ZONE\_SCOPE\_CREATE, and DNSSRV\_TYPEID\_ZONE\_SCOPE\_INFO. | Y | Content update. |
| [2.2.1.2.6](#Section_b61a872746b14981a6b3a1d4b92b67c4) DNSSRV\_RPC\_UNION | Updated content for Windows 10 and Windows Server 2016 Technical Preview. | Y | Content update. |
| 2.2.1.2.6 DNSSRV\_RPC\_UNION | Added cache scope to descriptions of ZoneScopeList, ScopeCreate, and ScopeInfo. | Y | Content update. |
| [2.2.2.1.1](#Section_39b03b89226440638198d62f62a6441a) DNS\_RECORD\_TYPE | Updated content for Windows 10 and Windows Server 2016 Technical Preview. | Y | Content update. |
| [2.2.2.1.2](#Section_f448341f512d414aaaa3e303d592fcd2) DNS\_RPC\_NODE\_FLAGS | Updated content for Windows 10 and Windows Server 2016 Technical Preview. | Y | Content update. |
| [2.2.2.2.4.26](#Section_3164a62650e749ab8bd900966440fd62) DNS\_RPC\_RECORD\_TLSA | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.2.2.4.27](#Section_48645c7312e84b60baf7c28f80a14ac4) DNS\_RPC\_RECORD\_UNKNOWN | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.2.2.5](#Section_ac7939811c6043b8be59cdbb5c4ecb8a) DNS\_RPC\_RECORD | Updated content for Windows 10 and Windows Server 2016 Technical Preview. | Y | Content update. |
| [2.2.4.2.2.2](#Section_84f3331d499d49fe9f61ab4c5dde6377) DNS\_RPC\_SERVER\_INFO\_DOTNET | 71173 : Specified that dwReserved0 is set to zero and pExtensions is set to NULL. | Y | Content update. |
| [2.2.5.2.4.1](#Section_e86515440fbb40388232375ff2d8a55e) DNS\_RPC\_ZONE\_INFO\_W2K | 71163 : Revised description of fNotifyLevel. | Y | Content update. |
| [2.2.6.2.4](#Section_4bcc003085254d94bc79c057e3f650d1) DNS\_RPC\_TRUST\_POINT | 71172 : Revised eTrustPointState field values to be consistent with other sections. | N | Content update. |
| [2.2.6.2.6](#Section_3ac97d1e7f7b4cd3aa24ccbde00ef0be) DNS\_RPC\_TRUST\_ANCHOR | 71172 : Revised eTrustPointState and eTrustAnchorState field values to be consistent with other sections. | N | Content update. |
| [2.2.12.1.1](#Section_8659f901293c4e8f862a6b7861b01118) DNS\_ZONE\_STATS\_TYPE | Updated content for Windows 10 and Windows Server 2016 Technical Preview. | Y | Content update. |
| [2.2.13](#Section_65cf48dfa5d8406fb60ef3a9789f9a29) Zone Scope or Cache Scope Messages | Added Cache Scope to section name. | Y | Content update. |
| [2.2.13.2.1](#Section_fe6fb7243db047ba9b00852703f430c4) DNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST | Specified that cache scopes are also enumerated. | Y | Content update. |
| [2.2.13.2.2.1](#Section_cbe779f029b94a6199fba1d9115d590f) DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1 | Specified that the structure also contains the name of the cache scope. | Y | Content update. |
| [2.2.13.2.3.1](#Section_7dc5c61adb9b4704a287a9713f24b0c6) DNS\_RPC\_ZONE\_SCOPE\_INFO\_V1 | Added cache scope to structure definition. | Y | Content update. |
| [2.2.15](#Section_accfbf80a9a942d69077453f34fd8685) Policies | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.15.1](#Section_169e564a8ce7445a85557212cd713766) Enumerations and Constants | Added section for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.15.1.1](#Section_a37b8ff71a784a159ce4cbe38d41cc19) Constants | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.15.1.1.1](#Section_4a5790e65cbe4cbea56cc7e4fabdf847) DNS\_RPC\_CRITERIA\_COMPARATOR | Added section with content for Windows10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.15.1.1.2](#Section_6b98c962d2084475ae181a068b4b925c) DNS\_RPC\_POLICY\_CONDITION | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.15.1.1.3](#Section_1519cc9db58848fbb3afe16b319b805e) DNS\_RPC\_POLICY\_LEVEL | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.15.1.1.4](#Section_11503add9e7b455b8d491c9653e04e80) DNS\_RPC\_POLICY\_ACTION\_TYPE | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.15.1.1.5](#Section_e2e0048d03a845dcbc27b7a4ad14d737) DNS\_RPC\_POLICY\_TYPE | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.15.1.1.6](#Section_4b707d19860c461eb7c57e6322db26e9) DNS\_RPC\_CRITERIA\_ENUM | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.15.2](#Section_332949faa7284c9d96cd9ec67a9b6662) Structures | Added section for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.15.2.1](#Section_c8b7e015035f424d90bef1c5f0b60eab) DNS\_RPC\_CLIENT\_SUBNET\_RECORD | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.15.2.2](#Section_dd2e4ce56eea4dc4b9f7058eb9703381) DNS\_RPC\_POLICY\_CONTENT | Added section with content for Windows10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.15.2.3](#Section_5e1af43060b242a6958e5e7c661ab99d) DNS\_RPC\_POLICY\_CONTENT\_LIST | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.15.2.4](#Section_be16f14ddf7440fe892c0718ebd32e84) DNS\_RPC\_CRITERIA | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.15.2.5](#Section_89be092dec014ab384e45a56622f9de8) DNS\_RPC\_POLICY | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.15.2.6](#Section_c97d6de9ddf44579bdece242bccb349d) DNS\_RPC\_POLICY\_NAME | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [2.2.15.2.7](#Section_e1c7065259a844eb844a1cda0b1453b8) DNS\_RPC\_ENUMERATE\_POLICY\_LIST | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [3.1.1.1.1](#Section_8903e50a91834a7d964053f6f5a91481) DNS Server Integer Properties | Updated content for Windows 10 and Windows Server 2016 Technical Preview. | Y | Content update. |
| [3.1.1.2.1](#Section_7bc88855d86a41f1826fa81788adb95a) DNS Zone Integer Properties | Updated content for Windows 10 and Windows Server 2016 Technical Preview. | Y | Content update. |
| [3.1.1.2.5](#Section_322505e531df48358a0708f06a3aea95) DNS Zone Scope or Cache Scope Configuration Information | Added cache scope. | Y | Content update. |
| [3.1.1.3](#Section_e01cf84de8954104a8da29d29bf6b4f0) DNS Server Server Scope Configuration Information | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [3.1.1.3.1](#Section_7394837917b0401180804feab27d1f1f) DNS Server Server Scope Integer Properties | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [3.1.1.3.2](#Section_c3dafa34e5ee4517883c32e0c84a578b) DNS Server Server Scope Address Array Properties | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [3.1.4](#Section_bdffbbf3e31b49ba8b8d8abde125a9d8) Message Processing Events and Sequencing Rules | Added cache zone and cache scope to definition of R\_DnssrvUpdateRecord3 and R\_DnssrvEnumRecords3. | Y | Content update. |
| [3.1.4.1](#Section_9500a7e8165d4b13be860ddc43100eef) R\_DnssrvOperation (Opnum 0) | Updated content for Windows 10 and Windows Server 2016 Technical Preview. | Y | Content update. |
| 3.1.4.1 R\_DnssrvOperation (Opnum 0) | Added behavior for cache scopes. | Y | Content update. |
| [3.1.4.3](#Section_864a6971f66447b9b012826fd2b0a409) R\_DnssrvComplexOperation (Opnum 2) | Updated content for Windows 10 and Windows Server 2016 Technical Preview. | Y | Content update. |
| 3.1.4.3 R\_DnssrvComplexOperation (Opnum 2) | Added behavior for cache scopes. | Y | Content update. |
| [3.1.4.5](#Section_37eea10100b8495899ebde8cda4b8417) R\_DnssrvUpdateRecord (Opnum 4) | Updated content for Windows 10 and Windows Server 2016 Technical Preview. | Y | Content update. |
| [3.1.4.11](#Section_12279f8cddaf47b8890591d7635cdfea) R\_DnssrvUpdateRecord3 (Opnum 10) | Added cache scope to description of pwszZonescope pointer. | Y | Content update. |
| [3.1.4.12](#Section_d7d4a3ac79954d419fcf1826cce95e2c) R\_DnssrvEnumRecords3 (Opnum 11) | Added cache scope to description of pwszZoneScope pointer. | Y | Content update. |
| [3.1.4.13](#Section_54044c364e9e44fb80dfffb026939b8b) R\_DnssrvOperation3 (Opnum 12) | Added cache scope to description and processing steps. | Y | Content update. |
| 3.1.4.13 R\_DnssrvOperation3 (Opnum 12) | Updated content for Windows 10 and Windows Server 2016 Technical Preview. | Y | Content update. |
| [3.1.4.14](#Section_0cb4d9cee08c40e6b4d55603b3fbc880) R\_DnssrvQuery3 (Opnum 13) | Added cache scope to description of pwszZoneScopeName. | Y | Content update. |
| 3.1.4.14 R\_DnssrvQuery3 (Opnum 13) | Updated content for Windows 10 and Windows Server 2016 Technical Preview. | Y | Content update. |
| [3.1.8](#Section_1c69bed4f2714f9aac64c3e04bde99f0) DNS Policy | Added section for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [3.1.8.1](#Section_7f8aadf248d14a3c8a47e00e88a915e1) Client Subnet Record | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [3.1.8.2](#Section_38bc9b8b84ec47b68964b900b426918e) DNS Policy Criteria | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [3.1.8.3](#Section_43a6fc0b785a43bb91d3b5a4f366fdf5) DNS Policy Validation | Added section with content for Windows10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [4.10](#Section_0a6660e099e941feba462146226b95db) Creating a Policy | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [4.11](#Section_45189bb6b17a4a2489a83c13c20b1184) Updating a Policy | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [4.12](#Section_0438e532a71141d8bdd4795e7f4e2695) Deleting a Policy | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [4.13](#Section_47a4747ad33d4d0792c8d75cdf0bb6e1) Enumerating Policies | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [4.14](#Section_7232d384985a4562b858441d97ced9ec) Creating a Client Subnet Record | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [4.15](#Section_c1b4a31cd44344d5b995631994aa4563) Deleting a Client Subnet Record | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [4.16](#Section_d0507a147e4947aa818fb3c501a0b71d) Enumerating Client Subnet Records | Added section with content for Windows 10 and Windows Server 2016 Technical Preview. | Y | New content added. |
| [6](#Section_83136c8ef5ea4ec5bf332134053d33bd) Appendix A: Full IDL | Updated content for Windows 10 and Windows Server 2016 Technical Preview. | Y | Content update. |
| [7](#Section_4a9a3ba310eb430eb1571fed0aaf85a5) Appendix B: Product Behavior | Updated applicability list for Windows 10. | Y | Content update. |
| 7 Appendix B: Product Behavior | Updated product behavior notes for Windows 10 and Windows Server 2016 Technical Preview. | Y | Product behavior note updated. |

# Index

**"**

["ECDSA\_P256"](#section_a430d9bdec994fa1a2f9d982018d7f44) 171

["ECDSA\_P384"](#section_a430d9bdec994fa1a2f9d982018d7f44) 171

["RSA"](#section_a430d9bdec994fa1a2f9d982018d7f44) 171

**\_**

[\_DnsCacheStats packet](#section_9502a725118042ed91d362d3d43e2365) 170

[\_DnsDbaseStats packet](#section_3c4ae7e2344542018aaf992933ed02c3) 160

[\_DnsMemoryStats packet](#section_303ccf5702b4411da6e5d741e00aebd1) 154

[\_DnsNbstatStats packet](#section_eec0b96271844ea7b5653500306a8a3d) 164

[\_DnsPacketStats packet](#section_b0be7f78ae4c41df9748535bc121a1c6) 162

[\_DnsPrivateStats packet](#section_2c72272dc8cf451a94a942475acdba45) 165

[\_DnsRecordStats packet](#section_c1e4a7a7cec2441e9e9243eddd7e7e33) 161

[\_DnsTimeoutStats packet](#section_ada3c79feb75473d980961243f108609) 158

[\_ErrorStats packet](#section_ea5599f0cd27401bb7a3cb96cd501c90) 168

**A**

[Abstract data model](#section_e72286df3e4c45359a0ce9cc944248c2) 203

[server](#section_e72286df3e4c45359a0ce9cc944248c2) 203

[Applicability](#section_d2cb6a5fc29c48b2a1cd8e51e749138f) 25

**B**

[BOOT\_METHOD\_DIRECTORY](#section_dc737abd3e844814a62a9398c770f28f) 68

[BOOT\_METHOD\_FILE](#section_dc737abd3e844814a62a9398c770f28f) 68

[BOOT\_METHOD\_REGISTRY](#section_dc737abd3e844814a62a9398c770f28f) 68

[BOOT\_METHOD\_UNINITIALIZED](#section_dc737abd3e844814a62a9398c770f28f) 68

**C**

[Capability negotiation](#section_a9d5443512b8491d92c98c2c6c3aa667) 25

[Change tracking](#section_93cc65f1eebb4497ac5432bb745ecd71) 369

[Client requirements](#section_00838343c85e4843a3c45f50a6a720fa) 203

[Common data types](#section_1d88a0dea17a46f0b002b0cb7b50c793) 28

[Creating a client subnet record example](#section_7232d384985a4562b858441d97ced9ec) 303

[Creating a new zone example](#section_8c30ab9a4ca64a3fb1930d2a32ce4229) 297

[Creating a policy](#section_0a6660e099e941feba462146226b95db) 301

[Creating a policy example](#section_0a6660e099e941feba462146226b95db) 301

[Creating a zone scope example](#section_64b8e0369b6f4ef7a7fd593340538e60) 299

[Creating and deleting a dns record example](#section_c87b1caf904d4d8aa7d13a6908112cd3) 298

[Creating and deleting a DNS record in a zone scope](#section_2a406d47dd3c4dd4a8129cc15d23cd02) 300

[Creating and deleting a dns record in a zone scope example](#section_2a406d47dd3c4dd4a8129cc15d23cd02) 300

[Creating and deleting DNS record example](#section_c87b1caf904d4d8aa7d13a6908112cd3) 298

[Creating new zone example](#section_8c30ab9a4ca64a3fb1930d2a32ce4229) 297

**D**

[Data model - abstract](#section_e72286df3e4c45359a0ce9cc944248c2) 203

[server](#section_e72286df3e4c45359a0ce9cc944248c2) 203

Data types

[common - overview](#section_1d88a0dea17a46f0b002b0cb7b50c793) 28

[DCPROMO\_CONVERT\_DOMAIN](#section_4ec7bdf71807417996afce1c1cd448b7) 194

[DCPROMO\_CONVERT\_FOREST](#section_4ec7bdf71807417996afce1c1cd448b7) 194

[DCPROMO\_CONVERT\_NONE](#section_4ec7bdf71807417996afce1c1cd448b7) 194

[Deleting a client subnet record example](#section_c1b4a31cd44344d5b995631994aa4563) 304

[Deleting a policy](#section_0438e532a71141d8bdd4795e7f4e2695) 302

[Deleting a policy example](#section_0438e532a71141d8bdd4795e7f4e2695) 302

[Deleting a zone scope example](#section_729d57f33f0249a882d0962d7f2a7935) 299

[Deleting DNS record example](#section_c87b1caf904d4d8aa7d13a6908112cd3) 298

[Directory service schema elements](#section_74db40e109174ecb863d9bce5165ebf3) 190

[DNS\_ADD\_USER packet](#section_6e041c763b55480a84fbfeebcb0cc9db) 66

[DNS\_ADDR packet](#section_aea3ba9bde484f0ea4c84f7c89404b99) 65

[DNS\_ADDR structure](#section_835c236a4d354a1ebc4cf5eb27bfb06d) 65

[DNS\_ADDR\_ARRAY structure](#section_56ba5fabf304486699a44f1c1f9247a3) 67

[DNS\_ALLOW\_ALL\_NAMES](#section_914badedbfe04e249150197b7ea2ba5d) 69

[DNS\_ALLOW\_MULTIBYTE\_NAMES](#section_914badedbfe04e249150197b7ea2ba5d) 69

[DNS\_ALLOW\_NONRFC\_NAMES](#section_914badedbfe04e249150197b7ea2ba5d) 69

[DNS\_ALLOW\_RFC\_NAMES\_ONLY](#section_914badedbfe04e249150197b7ea2ba5d) 69

[DNS\_COUNT\_NAME packet](#section_2af863063bd94c86b763fd33e16e3e5b) 44

[DNS\_DP\_AUTOCREATED](#section_27e378aad4d743de8b343e5b957a7130) 113

[DNS\_DP\_DELETED](#section_27e378aad4d743de8b343e5b957a7130) 113

[DNS\_DP\_DOMAIN\_DEFAULT](#section_27e378aad4d743de8b343e5b957a7130) 113

[DNS\_DP\_ENLISTED](#section_27e378aad4d743de8b343e5b957a7130) 113

[DNS\_DP\_FOREST\_DEFAULT](#section_27e378aad4d743de8b343e5b957a7130) 113

[DNS\_DP\_LEGACY](#section_27e378aad4d743de8b343e5b957a7130) 113

[DNS\_FLAT\_RECORD](#section_ac7939811c6043b8be59cdbb5c4ecb8a) 59

[DNS\_IPVAL\_DNS\_DELEGATIONS](#section_042395980c9b469bb1339f0142c2b1c5) 63

[DNS\_IPVAL\_DNS\_FORWARDERS](#section_042395980c9b469bb1339f0142c2b1c5) 63

[DNS\_IPVAL\_DNS\_ROOTHINTS](#section_042395980c9b469bb1339f0142c2b1c5) 63

[DNS\_IPVAL\_DNS\_SERVERS](#section_042395980c9b469bb1339f0142c2b1c5) 63

[DNS\_IPVAL\_DNS\_ZONE\_MASTERS](#section_042395980c9b469bb1339f0142c2b1c5) 63

[DNS\_IPVAL\_INVALID\_ADDR](#section_f9f3901a862f4bdba7c4963dae44c13e) 64

[DNS\_IPVAL\_NO\_RESPONSE](#section_f9f3901a862f4bdba7c4963dae44c13e) 64

[DNS\_IPVAL\_NO\_TCP](#section_f9f3901a862f4bdba7c4963dae44c13e) 64

[DNS\_IPVAL\_NOT\_AUTH\_FOR\_ZONE](#section_f9f3901a862f4bdba7c4963dae44c13e) 64

[DNS\_IPVAL\_UNKNOWN\_ERROR](#section_f9f3901a862f4bdba7c4963dae44c13e) 64

[DNS\_IPVAL\_UNREACHABLE](#section_f9f3901a862f4bdba7c4963dae44c13e) 64

[DNS\_LOG\_LEVEL\_ALL\_PACKETS](#section_fc6275bab4d34e81941703d004369075) 120

[DNS\_LOG\_LEVEL\_ANSWERS](#section_fc6275bab4d34e81941703d004369075) 120

[DNS\_LOG\_LEVEL\_DS\_UPDATE](#section_fc6275bab4d34e81941703d004369075) 120

[DNS\_LOG\_LEVEL\_DS\_WRITE](#section_fc6275bab4d34e81941703d004369075) 120

[DNS\_LOG\_LEVEL\_FULL\_PACKETS](#section_fc6275bab4d34e81941703d004369075) 120

[DNS\_LOG\_LEVEL\_NOTIFY](#section_fc6275bab4d34e81941703d004369075) 120

[DNS\_LOG\_LEVEL\_QUERY](#section_fc6275bab4d34e81941703d004369075) 120

[DNS\_LOG\_LEVEL\_QUESTIONS](#section_fc6275bab4d34e81941703d004369075) 120

[DNS\_LOG\_LEVEL\_RECV](#section_fc6275bab4d34e81941703d004369075) 120

[DNS\_LOG\_LEVEL\_SEND](#section_fc6275bab4d34e81941703d004369075) 120

[DNS\_LOG\_LEVEL\_TCP](#section_fc6275bab4d34e81941703d004369075) 120

[DNS\_LOG\_LEVEL\_UDP](#section_fc6275bab4d34e81941703d004369075) 120

[DNS\_LOG\_LEVEL\_UNMATCHED\_RESPONSE](#section_fc6275bab4d34e81941703d004369075) 120

[DNS\_LOG\_LEVEL\_UPDATE](#section_fc6275bab4d34e81941703d004369075) 120

[DNS\_LOG\_LEVEL\_WRITE\_THROUGH](#section_fc6275bab4d34e81941703d004369075) 120

[DNS\_ROLLOVER\_ACTION\_DEFAULT](#section_2671ecfc951c4d909b452bd1d87fa8f7) 79

[DNS\_ROLLOVER\_ACTION\_NORMAL](#section_2671ecfc951c4d909b452bd1d87fa8f7) 79

[DNS\_ROLLOVER\_ACTION\_RETIRE](#section_2671ecfc951c4d909b452bd1d87fa8f7) 79

[DNS\_ROLLOVER\_ACTION\_REVOKE\_STANDBY](#section_2671ecfc951c4d909b452bd1d87fa8f7) 79

[DNS\_ROLLOVER\_TYPE\_DOUBLE\_SIGNATURE](#section_ed7c21aa1175456c8d2f48e117b71b05) 79

[DNS\_ROLLOVER\_TYPE\_PREPUBLISH](#section_ed7c21aa1175456c8d2f48e117b71b05) 79

[DNS\_RPC\_AUTOCONFIG\_ALL](#section_d02b0aa23a704f66a63709bd55f6ec6d) 118

[DNS\_RPC\_AUTOCONFIG\_INTERNAL\_FORWARDERS](#section_d02b0aa23a704f66a63709bd55f6ec6d) 118

[DNS\_RPC\_AUTOCONFIG\_INTERNAL\_RETURN\_ERRORS](#section_d02b0aa23a704f66a63709bd55f6ec6d) 118

[DNS\_RPC\_AUTOCONFIG\_INTERNAL\_ROOTHINTS](#section_d02b0aa23a704f66a63709bd55f6ec6d) 118

[DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT](#section_d02b0aa23a704f66a63709bd55f6ec6d) 118

[DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_APPEND](#section_d02b0aa23a704f66a63709bd55f6ec6d) 118

[DNS\_RPC\_AUTOCONFIG\_INTERNAL\_SELFPOINT\_PREPEND](#section_d02b0aa23a704f66a63709bd55f6ec6d) 118

[DNS\_RPC\_AUTOCONFIG\_INTERNAL\_ZONES](#section_d02b0aa23a704f66a63709bd55f6ec6d) 118

[DNS\_RPC\_AUTOCONFIGURE structure](#section_414cf6fba8884c5591a46f77dff66cbe) 120

[DNS\_RPC\_BUFFER structure](#section_cd4d047c3e894bc2b1651dc60ba538d5) 34

[DNS\_RPC\_CLIENT\_SUBNET\_RECORD structure](#section_c8b7e015035f424d90bef1c5f0b60eab) 186

[DNS\_RPC\_CRITERIA structure](#section_be16f14ddf7440fe892c0718ebd32e84) 188

[DNS\_RPC\_CURRENT\_CLIENT\_VER packet](#section_a237781bb048495d844b10ffb38df2a8) 34

[DNS\_RPC\_DP\_ENUM structure](#section_324a939828c6463f93f68505904dc738) 116

[DNS\_RPC\_DP\_INFO structure](#section_bd2a817d6a6940d3befc0c198a9c6e80) 114

[DNS\_RPC\_DP\_LIST structure](#section_56b1d38f78964632b7dc0913ff3ef9b1) 116

[DNS\_RPC\_DP\_REPLICA structure](#section_9528535cd6a444a29c6f964e8adefa56) 115

[DNS\_RPC\_ENLIST\_DP structure](#section_7f445256e1694f1ea244d4223fbdf604) 116

[DNS\_RPC\_ENUM\_SCOPE\_LIST structure](#section_eb2f8d9cf68e44389fddd7e9ec1a52bd) 182

[DNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST structure](#section_fe6fb7243db047ba9b00852703f430c4) 180

[DNS\_RPC\_ENUM\_ZONES\_FILTER structure](#section_b2c763771c5042f483c6b514a1a7e65e) 97

[DNS\_RPC\_ENUMERATE\_POLICY\_LIST structure](#section_e1c7065259a844eb844a1cda0b1453b8) 190

[DNS\_RPC\_FLAG\_AGING\_ON](#section_f448341f512d414aaaa3e303d592fcd2) 43

[DNS\_RPC\_FLAG\_AUTH\_ZONE\_ROOT](#section_f448341f512d414aaaa3e303d592fcd2) 43

[DNS\_RPC\_FLAG\_CACHE\_DATA](#section_f448341f512d414aaaa3e303d592fcd2) 43

[DNS\_RPC\_FLAG\_NODE\_COMPLETE](#section_f448341f512d414aaaa3e303d592fcd2) 43

[DNS\_RPC\_FLAG\_NODE\_STICKY](#section_f448341f512d414aaaa3e303d592fcd2) 43

[DNS\_RPC\_FLAG\_OPEN\_ACL](#section_f448341f512d414aaaa3e303d592fcd2) 43

[DNS\_RPC\_FLAG\_POLICY\_CONDITION](#section_a37b8ff71a784a159ce4cbe38d41cc19) 182

[DNS\_RPC\_FLAG\_POLICY\_CONTENT](#section_a37b8ff71a784a159ce4cbe38d41cc19) 182

[DNS\_RPC\_FLAG\_POLICY\_CRITERIA\_CLIENT\_SUBNET](#section_a37b8ff71a784a159ce4cbe38d41cc19) 182

[DNS\_RPC\_FLAG\_POLICY\_CRITERIA\_FQDN](#section_a37b8ff71a784a159ce4cbe38d41cc19) 182

[DNS\_RPC\_FLAG\_POLICY\_CRITERIA\_NETWORK\_PROTOCOL](#section_a37b8ff71a784a159ce4cbe38d41cc19) 182

[DNS\_RPC\_FLAG\_POLICY\_CRITERIA\_QUERY\_TYPE](#section_a37b8ff71a784a159ce4cbe38d41cc19) 182

[DNS\_RPC\_FLAG\_POLICY\_CRITERIA\_SERVER\_IP](#section_a37b8ff71a784a159ce4cbe38d41cc19) 182

[DNS\_RPC\_FLAG\_POLICY\_CRITERIA\_TIME\_OF\_DAY](#section_a37b8ff71a784a159ce4cbe38d41cc19) 182

[DNS\_RPC\_FLAG\_POLICY\_CRITERIA\_TRANSPORT\_PROTOCOL](#section_a37b8ff71a784a159ce4cbe38d41cc19) 182

[DNS\_RPC\_FLAG\_POLICY\_PROCESSING\_ORDER](#section_a37b8ff71a784a159ce4cbe38d41cc19) 182

[DNS\_RPC\_FLAG\_RECORD\_CREATE\_PTR](#section_f448341f512d414aaaa3e303d592fcd2) 43

[DNS\_RPC\_FLAG\_RECORD\_DEFAULT\_TTL](#section_f448341f512d414aaaa3e303d592fcd2) 43

[DNS\_RPC\_FLAG\_RECORD\_TTL\_CHANGE](#section_f448341f512d414aaaa3e303d592fcd2) 43

[DNS\_RPC\_FLAG\_SUPPRESS\_NOTIFY](#section_f448341f512d414aaaa3e303d592fcd2) 43

[DNS\_RPC\_FLAG\_ZONE\_DELEGATION](#section_f448341f512d414aaaa3e303d592fcd2) 43

[DNS\_RPC\_FLAG\_ZONE\_ROOT](#section_f448341f512d414aaaa3e303d592fcd2) 43

[DNS\_RPC\_FORWARDERS](#section_2b015323fedd4bf8bcc40df5da06450f) 99

[DNS\_RPC\_FORWARDERS structure](#section_83f4bfffc5fb4029aad305b3d7f4ef40) 98

[DNS\_RPC\_FORWARDERS\_DOTNET structure](#section_4356fa2462664bb2ac5e519b6afe9237) 98

[DNS\_RPC\_FORWARDERS\_LONGHORN structure](#section_2b015323fedd4bf8bcc40df5da06450f) 99

[DNS\_RPC\_FORWARDERS\_W2K structure](#section_7c71bbd3a46d4f8ebca79bc9e153454f) 98

[DNS\_RPC\_IP\_VALIDATE structure](#section_2a367e0b5a8245d6aa77fbf407ed8d61) 67

[DNS\_RPC\_NAME packet](#section_3fd41adcc69e407b979e721251403132) 44

[DNS\_RPC\_NAME\_AND\_PARAM structure](#section_408e91b91e534631a0515e097394f8d8) 35

[DNS\_RPC\_NODE packet](#section_cb5539fa67fd40e09ea5468ecc56bd66) 45

[DNS\_RPC\_POLICY structure](#section_89be092dec014ab384e45a56622f9de8) 188

[DNS\_RPC\_POLICY\_CONTENT structure](#section_dd2e4ce56eea4dc4b9f7058eb9703381) 187

[DNS\_RPC\_POLICY\_CONTENT\_LIST structure](#section_5e1af43060b242a6958e5e7c661ab99d) 187

[DNS\_RPC\_POLICY\_NAME structure](#section_c97d6de9ddf44579bdece242bccb349d) 189

[DNS\_RPC\_RECORD structure](#section_ac7939811c6043b8be59cdbb5c4ecb8a) 59

[DNS\_RPC\_RECORD\_A packet](#section_117c2ff9909445b283c25e44518e0bac) 46

[DNS\_RPC\_RECORD\_AAAA packet](#section_ee33fef16e8242d081070f6d21be072a) 53

[DNS\_RPC\_RECORD\_ATMA packet](#section_446e2032fdb3451c8cd62d02f728ff2f) 54

[DNS\_RPC\_RECORD\_DATA structure](#section_38b873927f614e3092639f0fb832d084) 45

[DNS\_RPC\_RECORD\_DHCID packet](#section_55976e1fbac54db0acee4697167465d4) 52

[DNS\_RPC\_RECORD\_DNSKEY packet](#section_a9d25f0622b8468c944a5ec60a801a45) 53

[DNS\_RPC\_RECORD\_DS packet](#section_ea58fdc5daae41569a00c76a9062b060) 52

[DNS\_RPC\_RECORD\_KEY packet](#section_24a91f50455b441fbfd9e3cd4fb115b6) 52

[DNS\_RPC\_RECORD\_MAIL\_ERROR packet](#section_a85308bb3c1449d3a425603325a328d9) 49

[DNS\_RPC\_RECORD\_NAME\_PREFERENCE packet](#section_f647d39166144c3eb38b4df971590eb6) 49

[DNS\_RPC\_RECORD\_NAPTR packet](#section_76c17fe1379e417d8be12f6bf4071b88) 55

[DNS\_RPC\_RECORD\_NODE\_NAME packet](#section_8f986756f1514f5bbfcf0d85be8b0d7e) 46

[DNS\_RPC\_RECORD\_NSEC packet](#section_e018dd4b239d4dda8ee5d3b994084a24) 51

[DNS\_RPC\_RECORD\_NSEC3 packet](#section_559c3fd9043444cd9e0da905777b12cf) 57

[DNS\_RPC\_RECORD\_NSEC3PARAM packet](#section_5dc72f3a14c54ca989071ffd05b4570b) 58

[DNS\_RPC\_RECORD\_NULL packet](#section_308da71d67db4a0b96b1d0120aaf0017) 47

[DNS\_RPC\_RECORD\_NXT packet](#section_f8589ea319ae47968aa1c052a51de9c8) 53

[DNS\_RPC\_RECORD\_RRSIG packet](#section_20db056266f04dd4b38d19ec0885d48c) 50

[DNS\_RPC\_RECORD\_SIG packet](#section_2576da09c94d4a629c33afdd9d8a21e6) 50

[DNS\_RPC\_RECORD\_SOA packet](#section_dcd3ec16d6bf4bb491286172f9e5f066) 46

[DNS\_RPC\_RECORD\_SRV packet](#section_db37cab7f12143ba81c5ca0e198d4b9a) 54

[DNS\_RPC\_RECORD\_STRING packet](#section_69166ff536c14542924313b8931fa447) 48

[DNS\_RPC\_RECORD\_TS packet](#section_def7736add094b4ab8d66a702a7ecde0) 57

[DNS\_RPC\_RECORD\_WINS packet](#section_a3ab32de38ce4c55a11fbbd9d508f535) 56

[DNS\_RPC\_RECORD\_WINSR packet](#section_ba27d6f970ec4119b8bdb6e73773ff21) 56

[DNS\_RPC\_RECORD\_WKS packet](#section_bd24d852ca2f4275822dcf645fd31d29) 48

[DNS\_RPC\_SERVER\_INFO](#section_12233dd4dd644b1c95fd6a566e529ac9) 76

[DNS\_RPC\_SERVER\_INFO structure](#section_ac444baf4bf94f36912e3041d4c46361) 70

[DNS\_RPC\_SERVER\_INFO\_DOTNET structure](#section_84f3331d499d49fe9f61ab4c5dde6377) 74

[DNS\_RPC\_SERVER\_INFO\_LONGHORN structure](#section_12233dd4dd644b1c95fd6a566e529ac9) 76

[DNS\_RPC\_SERVER\_INFO\_W2K structure](#section_130bd2ca07644ea6996553ca15dd6ed2) 70

[DNS\_RPC\_SIGNING\_VALIDATION\_ERROR structure](#section_b9b7d8ba458b4c589ae5c9616a52aa4a) 109

[DNS\_RPC\_SKD structure](#section_f7b0ad424cae40fd87c882af83824639) 100

[DNS\_RPC\_SKD\_LIST structure](#section_6a715b5cf8c24b26923bca23cca2bd57) 102

[DNS\_RPC\_SKD\_STATE structure](#section_b211f98844044c14b293bafd114b0eb6) 102

[DNS\_RPC\_SKD\_STATE\_EX structure](#section_4578b2654ff9429492d505dbaa845037) 111

[DNS\_RPC\_TRUST\_ANCHOR structure](#section_3ac97d1e7f7b4cd3aa24ccbde00ef0be) 107

[DNS\_RPC\_TRUST\_ANCHOR\_LIST structure](#section_b70ad9a4fb654fea80f3eef09cbc54b9) 108

[DNS\_RPC\_TRUST\_POINT structure](#section_4bcc003085254d94bc79c057e3f650d1) 105

[DNS\_RPC\_TRUST\_POINT\_LIST structure](#section_4a950c7f5f734b0eb0d2c467dde70976) 106

[DNS\_RPC\_UNICODE\_STRING\_LIST structure](#section_ad7d4230cccf41589287328eb753e716) 35

[DNS\_RPC\_USE\_ALL\_PROTOCOLS](#section_cbae04989a604455977845476f7331f5) 32

[DNS\_RPC\_USE\_LPC](#section_cbae04989a604455977845476f7331f5) 32

[DNS\_RPC\_USE\_NAMED\_PIPE](#section_cbae04989a604455977845476f7331f5) 32

[DNS\_RPC\_USE\_TCPIP](#section_cbae04989a604455977845476f7331f5) 32

[DNS\_RPC\_UTF8\_STRING\_LIST structure](#section_8c593fe61a074140992c71f97f929ba3) 34

[DNS\_RPC\_ZONE](#section_64c5005d2a5546cc8453af393bb27bb9) 81

[DNS\_RPC\_ZONE structure](#section_f22773cabfbf46a58042fbda1f3c4ad2) 80

[DNS\_RPC\_ZONE\_CHANGE\_DP structure](#section_6dc9428b7a6f4112a3dc7d250d2b06b4) 117

[DNS\_RPC\_ZONE\_CREATE\_INFO](#section_5646cf31c0d242d88ef8ab2b69feb37b) 96

[DNS\_RPC\_ZONE\_CREATE\_INFO structure](#section_f79e7455e26643d3ab2bf8e75aacfefa) 92

[DNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET structure](#section_f0a445761d3f43ccbece07ae958f5b36) 95

[DNS\_RPC\_ZONE\_CREATE\_INFO\_LONGHORN structure](#section_5646cf31c0d242d88ef8ab2b69feb37b) 96

[DNS\_RPC\_ZONE\_CREATE\_INFO\_W2K structure](#section_780eba2615ea43d3a2b377ed9ab00690) 92

[DNS\_RPC\_ZONE\_DATABASE](#section_05778fae86d1414dbdf799479bb1ac15) 92

[DNS\_RPC\_ZONE\_DATABASE structure](#section_fc8b181af8b84953992e8102008d23cd) 91

[DNS\_RPC\_ZONE\_DATABASE\_DOTNET structure](#section_05778fae86d1414dbdf799479bb1ac15) 92

[DNS\_RPC\_ZONE\_DATABASE\_W2K structure](#section_660c4d3d6049422b912a7bf9129e7ed6) 91

[DNS\_RPC\_ZONE\_DNSSEC\_SETTINGS structure](#section_a6027a0db9364702b72c51bc0634ed19) 109

[DNS\_RPC\_ZONE\_DOTNET structure](#section_64c5005d2a5546cc8453af393bb27bb9) 81

[DNS\_RPC\_ZONE\_EXPORT\_INFO structure](#section_563518e385464d3c88c8f9b001beaa6e) 97

[DNS\_RPC\_ZONE\_INFO](#section_23a085bfd81445e3943f8bbdc32a5dae) 88

[DNS\_RPC\_ZONE\_INFO structure](#section_5e6b44a913c44c3aa7a2b5576016c3cf) 84

[DNS\_RPC\_ZONE\_INFO\_DOTNET structure](#section_45b100df57c24c8486de00b69d742372) 86

[DNS\_RPC\_ZONE\_INFO\_LONGHORN structure](#section_23a085bfd81445e3943f8bbdc32a5dae) 88

[DNS\_RPC\_ZONE\_INFO\_W2K structure](#section_e86515440fbb40388232375ff2d8a55e) 84

[DNS\_RPC\_ZONE\_LIST](#section_24366c193f664ddab3a533a79417661f) 83

[DNS\_RPC\_ZONE\_LIST structure](#section_e43b2e88e3d54e909c0708d2f2dc57ed) 82

[DNS\_RPC\_ZONE\_LIST\_DOTNET structure](#section_24366c193f664ddab3a533a79417661f) 83

[DNS\_RPC\_ZONE\_LIST\_W2K structure](#section_f457cf9e14e04195a8fd2c93bc7f1f6d) 83

[DNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1 structure](#section_cbe779f029b94a6199fba1d9115d590f) 181

[DNS\_RPC\_ZONE\_SCOPE\_INFO\_V1 structure](#section_7dc5c61adb9b4704a287a9713f24b0c6) 181

[DNS\_RPC\_ZONE\_SECONDARIES](#section_bf91cfc1da7c48f4bb5ff708ad305f3c) 91

[DNS\_RPC\_ZONE\_SECONDARIES structure](#section_2e5897350d8943c4a463212857482882) 89

[DNS\_RPC\_ZONE\_SECONDARIES\_DOTNET structure](#section_f3f440eb6ff5419ca9ff7ed6aafc937a) 90

[DNS\_RPC\_ZONE\_SECONDARIES\_LONGHORN structure](#section_bf91cfc1da7c48f4bb5ff708ad305f3c) 91

[DNS\_RPC\_ZONE\_SECONDARIES\_W2K structure](#section_0961e81f542f48c78043bd420d104101) 90

[DNS\_RPC\_ZONE\_SKD structure](#section_f8f3c7949bb946dcb39bcd853d65b3f1) 111

[DNS\_RPC\_ZONE\_STATS\_V1 structure](#section_d0ac5580a8464e5aa526c5e17c00e15d) 180

[DNS\_RPC\_ZONE\_W2K structure](#section_6b6e834ae08e432ca9a78ced1422a688) 80

[DNS\_SYSTEMTIME packet](#section_fc487ec46e26482ca9944f019afe0e4c) 124

[DNS\_TYPE\_A](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_AAAA](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_AFSDB](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_ALL](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_ATMA](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_CNAME](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_DHCID](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_DNAME](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_DNSKEY](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_DS](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_HINFO](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_ISDN](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_KEY](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_LOC](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_MB](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_MD](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_MF](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_MG](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_MINFO](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_MR](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_MX](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_NAPTR](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_NS](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_NSEC](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_NSEC3](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_NSEC3PARAM](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_NULL](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_NXT](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_PTR](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_RP](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_RRSIG](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_RT](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_SIG](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_SOA](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_SRV](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_TXT](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_WINS](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_WINSR](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_WKS](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_X25](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_TYPE\_ZERO](#section_39b03b89226440638198d62f62a6441a) 40

[DNS\_ZONE\_TYPE\_CACHE](#section_27e138a7110c44a4afcbb95f35f00306) 77

[DNS\_ZONE\_TYPE\_FORWARDER](#section_27e138a7110c44a4afcbb95f35f00306) 77

[DNS\_ZONE\_TYPE\_PRIMARY](#section_27e138a7110c44a4afcbb95f35f00306) 77

[DNS\_ZONE\_TYPE\_SECONDARY](#section_27e138a7110c44a4afcbb95f35f00306) 77

[DNS\_ZONE\_TYPE\_SECONDARY\_CACHE](#section_27e138a7110c44a4afcbb95f35f00306) 77

[DNS\_ZONE\_TYPE\_STUB](#section_27e138a7110c44a4afcbb95f35f00306) 77

[dnsProperty packet](#section_445c7843e4a142228c0f630c230a4c80) 192

[dnsRecord packet](#section_6912b33854724f59b9120edb536b6ed8) 195

[dnsserver interface](#section_bdac51424baf4b62bcced49eafc9c3e6) 203

[DNSSRV\_DNSSEC\_STATS packet](#section_c56e41c88d99475db497fbc59593880a) 136

[DNSSRV\_DS\_STATS packet](#section_02cbf8802d26454499d773294b664a78) 149

[DNSSRV\_MASTER\_STATS packet](#section_80779ec12b52499eaecc7018d0cf58a1) 136

[DNSSRV\_MEMTAG\_STATS packet](#section_0fbecaa99f8e4e9a8e94e0dd94d87710) 153

[DNSSRV\_QIERY2\_STATS packet](#section_538b073821f247e5b2120b4b858fdaca) 127

[DNSSRV\_QUERY\_STATS packet](#section_3fe0d4da23f74371854bbb480fb21586) 126

[DNSSRV\_RECURSE\_STATS packet](#section_402dd0cf46f646fda58a088fddc04a73) 129

[DNSSRV\_SECONDARY\_STATS packet](#section_e047d72501084f7f857f8665c1021694) 139

[DNSSRV\_SKWANSEC\_STATS packet](#section_8a9bf38fcda6485083bc6fa59936c988) 147

[DNSSRV\_STAT structure](#section_c4dd5c55f4344b968bb59d69e28ec7c2) 124

[DNSSRV\_STAT\_HEADER structure](#section_271b57b1759c4c5c8238912cd1b3be2a) 123

[DNSSRV\_STATID\_CACHE](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_DBASE](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_DNSSEC](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_DS](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_ERRORS](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_MASTER](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_MEMORY](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_NBSTAT](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_NONWIRE\_UPDATE](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_PACKET](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_PRIVATE](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_QUERY](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_QUERY2](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_RECORD](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_RECURSE](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_SECONDARY](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_SKWANSEC](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_TIME](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_TIMEOUT](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_WINS](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_STATID\_WIRE\_UPDATE](#section_6e5f45dfbf644c53867b2a1157472523) 122

[DNSSRV\_TIME\_STATS packet](#section_238b54f6bfdf4bb891ccc5ddbde6e7ac) 125

[DNSSRV\_TYPEID\_ADDRARRAY](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ANY](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_AUTOCONFIGURE](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_BUFFER](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_DP\_ENUM](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_DP\_INFO](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_DP\_LIST](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_DWORD](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ENLIST\_DP](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ENUM\_ZONES\_FILTER](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_FORWARDERS](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_FORWARDERS\_DOTNET](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_FORWARDERS\_W2K](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_IP\_VALIDATE](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_IPARRAY](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_LPSTR](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_LPWSTR](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_NAME\_AND\_PARAM](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_NULL](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_SCOPE\_ENUM](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_SERVER\_INFO](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_SERVER\_INFO\_DOTNET](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_SERVER\_INFO\_W2K](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_SIGNING\_VALIDATION\_ERROR](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_SKD](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_SKD\_LIST](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_SKD\_STATE](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_STATS](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_TRUST\_ANCHOR\_LIST](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_TRUST\_POINT\_LIST](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_UNICODE\_STRING\_LIST](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_UTF8\_STRING\_LIST](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_CHANGE\_DP](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_CREATE](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_CREATE\_DOTNET](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_CREATE\_W2K](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_DATABASE](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_DATABASE\_W2K](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_EXPORT](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_INFO](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_INFO\_DOTNET](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_INFO\_W2K](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_LIST](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_LIST\_W2K](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_RENAME](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_SCOPE\_CREATE](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_SCOPE\_ENUM](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_SCOPE\_INFO](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_SECONDARIES](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_SECONDARIES\_DOTNET](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_SECONDARIES\_W2K](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_SIGNING\_SETTINGS](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_STATS](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_TYPE\_RESET](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_TYPE\_RESET\_DOTNET](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_TYPE\_RESET\_W2K](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_TYPEID\_ZONE\_W2K](#section_c49b8142a36441c8914a7675a573b5e4) 28

[DNSSRV\_UPDATE\_STATS packet](#section_3c28e68edae6444b93a5416607d9002a) 143

[DNSSRV\_VERSION packet](#section_abf93ed679384564b21486762a1c4dea) 69

[DNSSRV\_WINS\_STATS packet](#section_49da9ba8b2df42aa93cb6ad7f8eb287f) 143

[DNSSRV\_ZONE\_QUERY\_STATS structure](#section_dd33a1852f5545cc99da57394db76f9f) 178

[DNSSRV\_ZONE\_TIME\_STATS structure](#section_76bf861ff1f74894a451be0f1a2e6794) 178

[DNSSRV\_ZONE\_TRANSFER\_STATS structure](#section_d1956dca7de742979ecdfcacf53df672) 179

[DNSSRV\_ZONE\_UPDATE\_STATS structure](#section_48a92670d0df4261a1281e3d63af1a62) 179

[DSPROPERTY\_ZONE\_AGING\_ENABLED\_TIME](#section_3af638710cc44179916c5caade55a8f3) 193

[DSPROPERTY\_ZONE\_AGING\_STATE](#section_3af638710cc44179916c5caade55a8f3) 193

[DSPROPERTY\_ZONE\_ALLOW\_UPDATE](#section_3af638710cc44179916c5caade55a8f3) 193

[DSPROPERTY\_ZONE\_AUTO\_NS\_SERVERS](#section_3af638710cc44179916c5caade55a8f3) 193

[DSPROPERTY\_ZONE\_AUTO\_NS\_SERVERS\_DA](#section_3af638710cc44179916c5caade55a8f3) 193

[DSPROPERTY\_ZONE\_DCPROMO\_CONVERT](#section_3af638710cc44179916c5caade55a8f3) 193

[DSPROPERTY\_ZONE\_DELETED\_FROM\_HOSTNAME](#section_3af638710cc44179916c5caade55a8f3) 193

[DSPROPERTY\_ZONE\_MASTER\_SERVERS](#section_3af638710cc44179916c5caade55a8f3) 193

[DSPROPERTY\_ZONE\_MASTER\_SERVERS\_DA](#section_3af638710cc44179916c5caade55a8f3) 193

[DSPROPERTY\_ZONE\_NODE\_DBFLAGS](#section_3af638710cc44179916c5caade55a8f3) 193

[DSPROPERTY\_ZONE\_NOREFRESH\_INTERVAL](#section_3af638710cc44179916c5caade55a8f3) 193

[DSPROPERTY\_ZONE\_REFRESH\_INTERVAL](#section_3af638710cc44179916c5caade55a8f3) 193

[DSPROPERTY\_ZONE\_SCAVENGING\_SERVERS](#section_3af638710cc44179916c5caade55a8f3) 193

[DSPROPERTY\_ZONE\_SCAVENGING\_SERVERS\_DA](#section_3af638710cc44179916c5caade55a8f3) 193

[DSPROPERTY\_ZONE\_SECURE\_TIME](#section_3af638710cc44179916c5caade55a8f3) 193

[DSPROPERTY\_ZONE\_TYPE](#section_3af638710cc44179916c5caade55a8f3) 193

**E**

[ECDSA\_P256 Key Pair packet](#section_2520414ed4f1483784696eb771c64992) 172

[ECDSA\_P384 Key Pair packet](#section_ed7dcb2f37794814b548ae37bb82653a) 173

[Elements - directory service schema](#section_74db40e109174ecb863d9bce5165ebf3) 190

[Enumerating client subnet records example](#section_d0507a147e4947aa818fb3c501a0b71d) 304

[Enumerating policies example](#section_47a4747ad33d4d0792c8d75cdf0bb6e1) 303

[Enumerating zone scopes](#section_27b59a12df5c4261be0fe02542634722) 300

[Enumerating zone scopes example](#section_27b59a12df5c4261be0fe02542634722) 300

[Enumerating zones example](#section_0c06b63ee544498789e67d674d719a14) 297

[ERROR\_SUCCESS](#section_f9f3901a862f4bdba7c4963dae44c13e) 64

[EVENT\_LOG\_ERROR\_TYPE](#section_9422eb05ebf54b86ac1be79ebf2e3b37) 121

[EVENT\_LOG\_INFORMATION\_TYPE](#section_9422eb05ebf54b86ac1be79ebf2e3b37) 121

[EVENT\_LOG\_SUCCESS](#section_9422eb05ebf54b86ac1be79ebf2e3b37) 121

[EVENT\_LOG\_WARNING\_TYPE](#section_9422eb05ebf54b86ac1be79ebf2e3b37) 121

Events

local

[directory server security descriptors reading and caching](#section_22c0c227816b4cc88a60644a7985a8ce) 288

[dnsRecord in directory server](#section_6ad921057d2b4350ae8f80e99c09013e) 288

[modifying directory server security descriptors](#section_fb192c0d664b4dddb490af241b664f8c) 288

[three-phase authorization test](#section_7ba0801d74f1499e81a300231ef31952) 287

[timer - server](#section_9b5fc445302b47419fdf0df895053ead) 287

Examples

[creating a client subnet record](#section_7232d384985a4562b858441d97ced9ec) 303

[creating a new zone](#section_8c30ab9a4ca64a3fb1930d2a32ce4229) 297

[creating a policy](#section_0a6660e099e941feba462146226b95db) 301

[creating a zone scope](#section_64b8e0369b6f4ef7a7fd593340538e60) 299

[creating and deleting a dns record](#section_c87b1caf904d4d8aa7d13a6908112cd3) 298

[creating and deleting a dns record in a zone scope](#section_2a406d47dd3c4dd4a8129cc15d23cd02) 300

[creating and deleting DNS record](#section_c87b1caf904d4d8aa7d13a6908112cd3) 298

[creating new zone](#section_8c30ab9a4ca64a3fb1930d2a32ce4229) 297

[deleting a client subnet record](#section_c1b4a31cd44344d5b995631994aa4563) 304

[deleting a policy](#section_0438e532a71141d8bdd4795e7f4e2695) 302

[deleting a zone scope](#section_729d57f33f0249a882d0962d7f2a7935) 299

[enumerating client subnet records](#section_d0507a147e4947aa818fb3c501a0b71d) 304

[enumerating policies](#section_47a4747ad33d4d0792c8d75cdf0bb6e1) 303

[enumerating zone scopes](#section_27b59a12df5c4261be0fe02542634722) 300

[enumerating zones](#section_0c06b63ee544498789e67d674d719a14) 297

[modifying a dns server dword property](#section_cafe3ebce69448688d66385443499856) 296

[modifying DNS server DWORD property](#section_cafe3ebce69448688d66385443499856) 296

[querying a dns server dword property](#section_77373ee29cfa426eaa087005a6ab939f) 296

[querying DNS server DWORD property](#section_77373ee29cfa426eaa087005a6ab939f) 296

[updating a policy](#section_45189bb6b17a4a2489a83c13c20b1184) 302

[ExportedKeyPair packet](#section_820903b3170440b6b977ac9154a90ffd) 176

**F**

[Fields - vendor-extensible](#section_293edac2617740d7b860ecf654e6bf3a) 25

[Full IDL](#section_83136c8ef5ea4ec5bf332134053d33bd) 307

**G**

[Glossary](#section_a95b05daf1fd4db394b4817fdaa1f642) 10

**I**

[IDL](#section_83136c8ef5ea4ec5bf332134053d33bd) 307

[Implementer - security considerations](#section_082cc4b5e01e41589042b63c2c12a06e) 306

[IMPORT\_STATUS\_CHANGED](#section_c5e7283c001242c98d693aa1529fa772) 100

[IMPORT\_STATUS\_NOOP](#section_c5e7283c001242c98d693aa1529fa772) 100

[IMPORT\_STATUS\_SIGNING\_READY](#section_c5e7283c001242c98d693aa1529fa772) 100

[IMPORT\_STATUS\_UNSIGNING\_READY](#section_c5e7283c001242c98d693aa1529fa772) 100

[Index of security parameters](#section_e029f962bc7644669db5a52210720008) 306

[Informative references](#section_881efeaa605a4c538ca70540caed9fb7) 21

[Initialization](#section_007efcd2295546dda59ef83ae88f4678) 229

[server](#section_007efcd2295546dda59ef83ae88f4678) 229

Interfaces - server

[dnsserver](#section_bdac51424baf4b62bcced49eafc9c3e6) 203

[Introduction](#section_a340b0e1172b4e54b338488291550e95) 10

[IP4\_ARRAY structure](#section_588ae29671bf402f999686ecee39dc29) 65

**L**

Local events

[directory server security descriptors reading and caching](#section_22c0c227816b4cc88a60644a7985a8ce) 288

[dnsRecord in directory server](#section_6ad921057d2b4350ae8f80e99c09013e) 288

[modifying directory server security descriptors](#section_fb192c0d664b4dddb490af241b664f8c) 288

[three-phase authorization test](#section_7ba0801d74f1499e81a300231ef31952) 287

**M**

[Message processing](#section_bdffbbf3e31b49ba8b8d8abde125a9d8) 233

[server](#section_bdffbbf3e31b49ba8b8d8abde125a9d8) 233

Messages

[common data types](#section_1d88a0dea17a46f0b002b0cb7b50c793) 28

[transport](#section_09591e5ada87438cb70e2ec62dd82314) 27

Methods

[R\_DnssrvComplexOperation (Opnum 2)](#section_864a6971f66447b9b012826fd2b0a409) 267

[R\_DnssrvComplexOperation2 (Opnum 7)](#section_d28e3ba85742417dad6d2e0139ab2ad9) 281

[R\_DnssrvEnumRecords (Opnum 3)](#section_d0251c9b9e3e4eecbcc5eb6b995b6108) 276

[R\_DnssrvEnumRecords2 (Opnum 8)](#section_0d236e5899444cdfae98f92460202e29) 282

[R\_DnssrvEnumRecords3 (Opnum 11)](#section_d7d4a3ac79954d419fcf1826cce95e2c) 284

[R\_DnssrvOperation (Opnum 0)](#section_9500a7e8165d4b13be860ddc43100eef) 235

[R\_DnssrvOperation2 (Opnum 5)](#section_8c0522b197fb4fa7b4e22c55c0afb0e7) 280

[R\_DnssrvOperation3 (Opnum 12)](#section_54044c364e9e44fb80dfffb026939b8b) 284

[R\_DnssrvQuery (Opnum 1)](#section_b0419a70ac0b40baab941510992bc574) 265

[R\_DnssrvQuery2 (Opnum 6)](#section_a90a44f0f64e44b09e35a7fc49f6adea) 281

[R\_DnssrvQuery3 (Opnum 13)](#section_0cb4d9cee08c40e6b4d55603b3fbc880) 286

[R\_DnssrvUpdateRecord (Opnum 4)](#section_37eea10100b8495899ebde8cda4b8417) 278

[R\_DnssrvUpdateRecord2 (Opnum 9)](#section_8f50ae96d87f4fdb85265a86cea25837) 283

[R\_DnssrvUpdateRecord3 (Opnum 10)](#section_12279f8cddaf47b8890591d7635cdfea) 283

[Modifying a dns server dword property example](#section_cafe3ebce69448688d66385443499856) 296

[Modifying DNS server DWORD property example](#section_cafe3ebce69448688d66385443499856) 296

[msDNS-SigningKeyDescriptors packet](#section_44a58c972ee948ff8ecc4744e62328cf) 197

[msDNS-SigningKeys packet](#section_ae475e07d7d34acaaa82c1dfb44a1703) 196

**N**

[Normative references](#section_2483e88025824594bdfb7fcfb1b4ae62) 18

**O**

[Overview (synopsis)](#section_4181e2e1dd6245ba8ed2e7129585302c) 21

**P**

[Parameter index - security](#section_e029f962bc7644669db5a52210720008) 306

[Parameters - security index](#section_e029f962bc7644669db5a52210720008) 306

[PDNS\_ADDR](#section_835c236a4d354a1ebc4cf5eb27bfb06d) 65

[PDNS\_ADDR\_ARRAY](#section_56ba5fabf304486699a44f1c1f9247a3) 67

[PDNS\_FLAT\_RECORD](#section_ac7939811c6043b8be59cdbb5c4ecb8a) 59

[PDNS\_RPC\_AUTOCONFIGURE](#section_414cf6fba8884c5591a46f77dff66cbe) 120

[PDNS\_RPC\_BUFFER](#section_cd4d047c3e894bc2b1651dc60ba538d5) 34

[PDNS\_RPC\_CLIENT\_SUBNET\_RECORD](#section_c8b7e015035f424d90bef1c5f0b60eab) 186

[PDNS\_RPC\_CRITERIA](#section_be16f14ddf7440fe892c0718ebd32e84) 188

[PDNS\_RPC\_DP\_ENUM](#section_324a939828c6463f93f68505904dc738) 116

[PDNS\_RPC\_DP\_INFO](#section_bd2a817d6a6940d3befc0c198a9c6e80) 114

[PDNS\_RPC\_DP\_LIST](#section_56b1d38f78964632b7dc0913ff3ef9b1) 116

[PDNS\_RPC\_DP\_REPLICA](#section_9528535cd6a444a29c6f964e8adefa56) 115

[PDNS\_RPC\_ENLIST\_DP](#section_7f445256e1694f1ea244d4223fbdf604) 116

[PDNS\_RPC\_ENUM\_SCOPE\_LIST](#section_eb2f8d9cf68e44389fddd7e9ec1a52bd) 182

[PDNS\_RPC\_ENUM\_ZONE\_SCOPE\_LIST](#section_fe6fb7243db047ba9b00852703f430c4) 180

[PDNS\_RPC\_ENUM\_ZONES\_FILTER](#section_b2c763771c5042f483c6b514a1a7e65e) 97

[PDNS\_RPC\_ENUMERATE\_POLICY\_LIST](#section_e1c7065259a844eb844a1cda0b1453b8) 190

[PDNS\_RPC\_FORWARDERS](#section_2b015323fedd4bf8bcc40df5da06450f) 99

[PDNS\_RPC\_FORWARDERS\_DOTNET](#section_4356fa2462664bb2ac5e519b6afe9237) 98

[PDNS\_RPC\_FORWARDERS\_LONGHORN](#section_2b015323fedd4bf8bcc40df5da06450f) 99

[PDNS\_RPC\_FORWARDERS\_W2K](#section_7c71bbd3a46d4f8ebca79bc9e153454f) 98

[PDNS\_RPC\_IP\_VALIDATE](#section_2a367e0b5a8245d6aa77fbf407ed8d61) 67

[PDNS\_RPC\_NAME\_AND\_PARAM](#section_408e91b91e534631a0515e097394f8d8) 35

[PDNS\_RPC\_POLICY](#section_89be092dec014ab384e45a56622f9de8) 188

[PDNS\_RPC\_POLICY\_CONTENT](#section_dd2e4ce56eea4dc4b9f7058eb9703381) 187

[PDNS\_RPC\_POLICY\_CONTENT\_LIST](#section_5e1af43060b242a6958e5e7c661ab99d) 187

[PDNS\_RPC\_POLICY\_NAME](#section_c97d6de9ddf44579bdece242bccb349d) 189

[PDNS\_RPC\_RECORD](#section_ac7939811c6043b8be59cdbb5c4ecb8a) 59

[PDNS\_RPC\_SERVER\_INFO](#section_12233dd4dd644b1c95fd6a566e529ac9) 76

[PDNS\_RPC\_SERVER\_INFO\_DOTNET](#section_84f3331d499d49fe9f61ab4c5dde6377) 74

[PDNS\_RPC\_SERVER\_INFO\_LONGHORN](#section_12233dd4dd644b1c95fd6a566e529ac9) 76

[PDNS\_RPC\_SERVER\_INFO\_W2K](#section_130bd2ca07644ea6996553ca15dd6ed2) 70

[PDNS\_RPC\_SIGNING\_VALIDATION\_ERROR](#section_b9b7d8ba458b4c589ae5c9616a52aa4a) 109

[PDNS\_RPC\_SKD](#section_f7b0ad424cae40fd87c882af83824639) 100

[PDNS\_RPC\_SKD\_LIST](#section_6a715b5cf8c24b26923bca23cca2bd57) 102

[PDNS\_RPC\_SKD\_STATE](#section_b211f98844044c14b293bafd114b0eb6) 102

[PDNS\_RPC\_SKD\_STATE\_EX](#section_4578b2654ff9429492d505dbaa845037) 111

[PDNS\_RPC\_TRUST\_ANCHOR](#section_3ac97d1e7f7b4cd3aa24ccbde00ef0be) 107

[PDNS\_RPC\_TRUST\_ANCHOR\_LIST](#section_b70ad9a4fb654fea80f3eef09cbc54b9) 108

[PDNS\_RPC\_TRUST\_POINT](#section_4bcc003085254d94bc79c057e3f650d1) 105

[PDNS\_RPC\_TRUST\_POINT\_LIST](#section_4a950c7f5f734b0eb0d2c467dde70976) 106

[PDNS\_RPC\_UNICODE\_STRING\_LIST](#section_ad7d4230cccf41589287328eb753e716) 35

[PDNS\_RPC\_UTF8\_STRING\_LIST](#section_8c593fe61a074140992c71f97f929ba3) 34

[PDNS\_RPC\_ZONE](#section_64c5005d2a5546cc8453af393bb27bb9) 81

[PDNS\_RPC\_ZONE\_CHANGE\_DP](#section_6dc9428b7a6f4112a3dc7d250d2b06b4) 117

[PDNS\_RPC\_ZONE\_CREATE\_INFO](#section_5646cf31c0d242d88ef8ab2b69feb37b) 96

[PDNS\_RPC\_ZONE\_CREATE\_INFO\_DOTNET](#section_f0a445761d3f43ccbece07ae958f5b36) 95

[PDNS\_RPC\_ZONE\_CREATE\_INFO\_LONGHORN](#section_5646cf31c0d242d88ef8ab2b69feb37b) 96

[PDNS\_RPC\_ZONE\_CREATE\_INFO\_W2K](#section_780eba2615ea43d3a2b377ed9ab00690) 92

[PDNS\_RPC\_ZONE\_DATABASE](#section_05778fae86d1414dbdf799479bb1ac15) 92

[PDNS\_RPC\_ZONE\_DATABASE\_DOTNET](#section_05778fae86d1414dbdf799479bb1ac15) 92

[PDNS\_RPC\_ZONE\_DATABASE\_W2K](#section_660c4d3d6049422b912a7bf9129e7ed6) 91

[PDNS\_RPC\_ZONE\_DNSSEC\_SETTINGS](#section_a6027a0db9364702b72c51bc0634ed19) 109

[PDNS\_RPC\_ZONE\_DOTNET](#section_64c5005d2a5546cc8453af393bb27bb9) 81

[PDNS\_RPC\_ZONE\_EXPORT\_INFO](#section_563518e385464d3c88c8f9b001beaa6e) 97

[PDNS\_RPC\_ZONE\_INFO](#section_23a085bfd81445e3943f8bbdc32a5dae) 88

[PDNS\_RPC\_ZONE\_INFO\_DOTNET](#section_45b100df57c24c8486de00b69d742372) 86

[PDNS\_RPC\_ZONE\_INFO\_LONGHORN](#section_23a085bfd81445e3943f8bbdc32a5dae) 88

[PDNS\_RPC\_ZONE\_INFO\_W2K](#section_e86515440fbb40388232375ff2d8a55e) 84

[PDNS\_RPC\_ZONE\_LIST](#section_24366c193f664ddab3a533a79417661f) 83

[PDNS\_RPC\_ZONE\_LIST\_DOTNET](#section_24366c193f664ddab3a533a79417661f) 83

[PDNS\_RPC\_ZONE\_LIST\_W2K](#section_f457cf9e14e04195a8fd2c93bc7f1f6d) 83

[PDNS\_RPC\_ZONE\_SCOPE\_CREATE\_INFO\_V1](#section_cbe779f029b94a6199fba1d9115d590f) 181

[PDNS\_RPC\_ZONE\_SCOPE\_INFO\_V1](#section_7dc5c61adb9b4704a287a9713f24b0c6) 181

[PDNS\_RPC\_ZONE\_SECONDARIES](#section_bf91cfc1da7c48f4bb5ff708ad305f3c) 91

[PDNS\_RPC\_ZONE\_SECONDARIES\_DOTNET](#section_f3f440eb6ff5419ca9ff7ed6aafc937a) 90

[PDNS\_RPC\_ZONE\_SECONDARIES\_LONGHORN](#section_bf91cfc1da7c48f4bb5ff708ad305f3c) 91

[PDNS\_RPC\_ZONE\_SECONDARIES\_W2K](#section_0961e81f542f48c78043bd420d104101) 90

[PDNS\_RPC\_ZONE\_SKD](#section_f8f3c7949bb946dcb39bcd853d65b3f1) 111

[PDNS\_RPC\_ZONE\_STATS\_V1](#section_d0ac5580a8464e5aa526c5e17c00e15d) 180

[PDNS\_RPC\_ZONE\_W2K](#section_6b6e834ae08e432ca9a78ced1422a688) 80

[PDNSSRV\_STAT](#section_c4dd5c55f4344b968bb59d69e28ec7c2) 124

[PDNSSRV\_STAT\_HEADER](#section_271b57b1759c4c5c8238912cd1b3be2a) 123

[PDNSSRV\_STATS](#section_c4dd5c55f4344b968bb59d69e28ec7c2) 124

[PDNSSRV\_ZONE\_QUERY\_STATS](#section_dd33a1852f5545cc99da57394db76f9f) 178

[PDNSSRV\_ZONE\_TIME\_STATS](#section_76bf861ff1f74894a451be0f1a2e6794) 178

[PDNSSRV\_ZONE\_TRANSFER\_STATS](#section_d1956dca7de742979ecdfcacf53df672) 179

[PDNSSRV\_ZONE\_UPDATE\_STATS](#section_48a92670d0df4261a1281e3d63af1a62) 179

[PIP4\_ARRAY](#section_588ae29671bf402f999686ecee39dc29) 65

[Preconditions](#section_3bf8092ae6d54433ae0288a6c31b0df2) 24

[Prerequisites](#section_3bf8092ae6d54433ae0288a6c31b0df2) 24

Processing rules

[constructing exported key](#section_33a9931f7e064a44b29214541ad39c84) 289

[importing exported key](#section_9fb68ee30b244878a2804c03ea572c78) 291

[Product behavior](#section_4a9a3ba310eb430eb1571fed0aaf85a5) 339

[Protection\_Key\_Identifier packet](#section_98a575daca484afdba79f77a8bed4e4e) 174

Protocol Details

[overview](#section_00838343c85e4843a3c45f50a6a720fa) 203

**Q**

[Querying a dns server dword property example](#section_77373ee29cfa426eaa087005a6ab939f) 296

[Querying DNS server DWORD property example](#section_77373ee29cfa426eaa087005a6ab939f) 296

**R**

[R\_DnssrvComplexOperation (Opnum 2) method](#section_864a6971f66447b9b012826fd2b0a409) 267

[R\_DnssrvComplexOperation method](#section_864a6971f66447b9b012826fd2b0a409) 267

[R\_DnssrvComplexOperation2 (Opnum 7) method](#section_d28e3ba85742417dad6d2e0139ab2ad9) 281

[R\_DnssrvComplexOperation2 method](#section_d28e3ba85742417dad6d2e0139ab2ad9) 281

[R\_DnssrvEnumRecords (Opnum 3) method](#section_d0251c9b9e3e4eecbcc5eb6b995b6108) 276

[R\_DnssrvEnumRecords method](#section_d0251c9b9e3e4eecbcc5eb6b995b6108) 276

[R\_DnssrvEnumRecords2 (Opnum 8) method](#section_0d236e5899444cdfae98f92460202e29) 282

[R\_DnssrvEnumRecords2 method](#section_0d236e5899444cdfae98f92460202e29) 282

[R\_DnssrvEnumRecords3 (Opnum 11) method](#section_d7d4a3ac79954d419fcf1826cce95e2c) 284

[R\_DnssrvEnumRecords3 method](#section_d7d4a3ac79954d419fcf1826cce95e2c) 284

[R\_DnssrvOperation (Opnum 0) method](#section_9500a7e8165d4b13be860ddc43100eef) 235

[R\_DnssrvOperation method](#section_9500a7e8165d4b13be860ddc43100eef) 235

[R\_DnssrvOperation2 (Opnum 5) method](#section_8c0522b197fb4fa7b4e22c55c0afb0e7) 280

[R\_DnssrvOperation2 method](#section_8c0522b197fb4fa7b4e22c55c0afb0e7) 280

[R\_DnssrvOperation3 (Opnum 12) method](#section_54044c364e9e44fb80dfffb026939b8b) 284

[R\_DnssrvOperation3 method](#section_54044c364e9e44fb80dfffb026939b8b) 284

[R\_DnssrvQuery (Opnum 1) method](#section_b0419a70ac0b40baab941510992bc574) 265

[R\_DnssrvQuery method](#section_b0419a70ac0b40baab941510992bc574) 265

[R\_DnssrvQuery2 (Opnum 6) method](#section_a90a44f0f64e44b09e35a7fc49f6adea) 281

[R\_DnssrvQuery2 method](#section_a90a44f0f64e44b09e35a7fc49f6adea) 281

[R\_DnssrvQuery3 (Opnum 13) method](#section_0cb4d9cee08c40e6b4d55603b3fbc880) 286

[R\_DnssrvQuery3 method](#section_0cb4d9cee08c40e6b4d55603b3fbc880) 286

[R\_DnssrvUpdateRecord (Opnum 4) method](#section_37eea10100b8495899ebde8cda4b8417) 278

[R\_DnssrvUpdateRecord2 (Opnum 9) method](#section_8f50ae96d87f4fdb85265a86cea25837) 283

[R\_DnssrvUpdateRecord2 method](#section_8f50ae96d87f4fdb85265a86cea25837) 283

[R\_DnssrvUpdateRecord3 (Opnum 10) method](#section_12279f8cddaf47b8890591d7635cdfea) 283

[R\_DnssrvUpdateRecord3 method](#section_12279f8cddaf47b8890591d7635cdfea) 283

[References](#section_fa683319801741858c77120ff9512d97) 17

[informative](#section_881efeaa605a4c538ca70540caed9fb7) 21

[normative](#section_2483e88025824594bdfb7fcfb1b4ae62) 18

[Relationship to other protocols](#section_ac2f389a2ba4454b8667e42e0b9740f4) 22

[RSA Key Pair packet](#section_244cca32e77a4d8a951d6fd918d55a98) 171

**S**

[Schema elements - directory service](#section_74db40e109174ecb863d9bce5165ebf3) 190

Security

[implementer considerations](#section_082cc4b5e01e41589042b63c2c12a06e) 306

[parameter index](#section_e029f962bc7644669db5a52210720008) 306

[Sequencing rules](#section_bdffbbf3e31b49ba8b8d8abde125a9d8) 233

[server](#section_bdffbbf3e31b49ba8b8d8abde125a9d8) 233

Server

[abstract data model](#section_e72286df3e4c45359a0ce9cc944248c2) 203

[dnsserver interface](#section_bdac51424baf4b62bcced49eafc9c3e6) 203

[initialization](#section_007efcd2295546dda59ef83ae88f4678) 229

[message processing](#section_bdffbbf3e31b49ba8b8d8abde125a9d8) 233

[overview](#section_bdac51424baf4b62bcced49eafc9c3e6) 203

[R\_DnssrvComplexOperation (Opnum 2) method](#section_864a6971f66447b9b012826fd2b0a409) 267

[R\_DnssrvComplexOperation2 (Opnum 7) method](#section_d28e3ba85742417dad6d2e0139ab2ad9) 281

[R\_DnssrvEnumRecords (Opnum 3) method](#section_d0251c9b9e3e4eecbcc5eb6b995b6108) 276

[R\_DnssrvEnumRecords2 (Opnum 8) method](#section_0d236e5899444cdfae98f92460202e29) 282

[R\_DnssrvEnumRecords3 (Opnum 11) method](#section_d7d4a3ac79954d419fcf1826cce95e2c) 284

[R\_DnssrvOperation (Opnum 0) method](#section_9500a7e8165d4b13be860ddc43100eef) 235

[R\_DnssrvOperation2 (Opnum 5) method](#section_8c0522b197fb4fa7b4e22c55c0afb0e7) 280

[R\_DnssrvOperation3 (Opnum 12) method](#section_54044c364e9e44fb80dfffb026939b8b) 284

[R\_DnssrvQuery (Opnum 1) method](#section_b0419a70ac0b40baab941510992bc574) 265

[R\_DnssrvQuery2 (Opnum 6) method](#section_a90a44f0f64e44b09e35a7fc49f6adea) 281

[R\_DnssrvQuery3 (Opnum 13) method](#section_0cb4d9cee08c40e6b4d55603b3fbc880) 286

[R\_DnssrvUpdateRecord (Opnum 4) method](#section_37eea10100b8495899ebde8cda4b8417) 278

[R\_DnssrvUpdateRecord2 (Opnum 9) method](#section_8f50ae96d87f4fdb85265a86cea25837) 283

[R\_DnssrvUpdateRecord3 (Opnum 10) method](#section_12279f8cddaf47b8890591d7635cdfea) 283

[sequencing rules](#section_bdffbbf3e31b49ba8b8d8abde125a9d8) 233

[timer events](#section_9b5fc445302b47419fdf0df895053ead) 287

[timers](#section_7eb0a1cd74a64850a67620d7291b585d) 229

[SIGN\_SCOPE\_ADD\_ONLY](#section_b67bcf7387b5449a91c9b470ea42b038) 99

[SIGN\_SCOPE\_ALL\_RECORDS](#section_b67bcf7387b5449a91c9b470ea42b038) 99

[SIGN\_SCOPE\_DEFAULT](#section_b67bcf7387b5449a91c9b470ea42b038) 99

[SIGN\_SCOPE\_DNSKEY\_ONLY](#section_b67bcf7387b5449a91c9b470ea42b038) 99

[SIGN\_SCOPE\_DO\_NOT\_PUBLISH](#section_b67bcf7387b5449a91c9b470ea42b038) 99

[SIGN\_SCOPE\_REVOKED](#section_b67bcf7387b5449a91c9b470ea42b038) 99

[Standards assignments](#section_5093503c687e4376912750504908fb91) 25

**T**

[Timer events](#section_9b5fc445302b47419fdf0df895053ead) 287

[server](#section_9b5fc445302b47419fdf0df895053ead) 287

[Timers](#section_7eb0a1cd74a64850a67620d7291b585d) 229

[server](#section_7eb0a1cd74a64850a67620d7291b585d) 229

[Tracking changes](#section_93cc65f1eebb4497ac5432bb745ecd71) 369

[Transport](#section_09591e5ada87438cb70e2ec62dd82314) 27

[TRUSTANCHOR\_STATE\_ADDPEND](#section_d84d1ece610a49118cfc8f93bc9a870e) 33

[TRUSTANCHOR\_STATE\_DSINVALID](#section_d84d1ece610a49118cfc8f93bc9a870e) 33

[TRUSTANCHOR\_STATE\_DSPENDING](#section_d84d1ece610a49118cfc8f93bc9a870e) 33

[TRUSTANCHOR\_STATE\_MISSING](#section_d84d1ece610a49118cfc8f93bc9a870e) 33

[TRUSTANCHOR\_STATE\_REVOKED](#section_d84d1ece610a49118cfc8f93bc9a870e) 33

[TRUSTANCHOR\_STATE\_VALID](#section_d84d1ece610a49118cfc8f93bc9a870e) 33

[TRUSTPOINT\_STATE\_ACTIVE](#section_0b73d83ca99d48a7a65dbe40f3e749e3) 33

[TRUSTPOINT\_STATE\_DELETE\_PENDING](#section_0b73d83ca99d48a7a65dbe40f3e749e3) 33

[TRUSTPOINT\_STATE\_DSPENDING](#section_0b73d83ca99d48a7a65dbe40f3e749e3) 33

[TRUSTPOINT\_STATE\_INITIALIZED](#section_0b73d83ca99d48a7a65dbe40f3e749e3) 33

**U**

[Updating a policy](#section_45189bb6b17a4a2489a83c13c20b1184) 302

[Updating a policy example](#section_45189bb6b17a4a2489a83c13c20b1184) 302

**V**

[Vendor-extensible fields](#section_293edac2617740d7b860ecf654e6bf3a) 25

[Versioning](#section_a9d5443512b8491d92c98c2c6c3aa667) 25

**Z**

[ZONE\_NOTIFY\_ALL\_SECONDARIES](#section_343f4212ad8a47908aa77c5bc15f7bd2) 78

[ZONE\_NOTIFY\_LIST\_ONLY](#section_343f4212ad8a47908aa77c5bc15f7bd2) 78

[ZONE\_NOTIFY\_OFF](#section_343f4212ad8a47908aa77c5bc15f7bd2) 78

[ZONE\_REQUEST\_AUTO](#section_f4cf1f3e7d134010a9155223dcabc15d) 78

[ZONE\_REQUEST\_CACHE](#section_f4cf1f3e7d134010a9155223dcabc15d) 78

[ZONE\_REQUEST\_CUSTOM\_DP](#section_f4cf1f3e7d134010a9155223dcabc15d) 78

[ZONE\_REQUEST\_DOMAIN\_DP](#section_f4cf1f3e7d134010a9155223dcabc15d) 78

[ZONE\_REQUEST\_DS](#section_f4cf1f3e7d134010a9155223dcabc15d) 78

[ZONE\_REQUEST\_FOREST\_DP](#section_f4cf1f3e7d134010a9155223dcabc15d) 78

[ZONE\_REQUEST\_FORWARD](#section_f4cf1f3e7d134010a9155223dcabc15d) 78

[ZONE\_REQUEST\_FORWARDER](#section_f4cf1f3e7d134010a9155223dcabc15d) 78

[ZONE\_REQUEST\_LEGACY\_DP](#section_f4cf1f3e7d134010a9155223dcabc15d) 78

[ZONE\_REQUEST\_NON\_DS](#section_f4cf1f3e7d134010a9155223dcabc15d) 78

[ZONE\_REQUEST\_PRIMARY](#section_f4cf1f3e7d134010a9155223dcabc15d) 78

[ZONE\_REQUEST\_REVERSE](#section_f4cf1f3e7d134010a9155223dcabc15d) 78

[ZONE\_REQUEST\_SECONDARY](#section_f4cf1f3e7d134010a9155223dcabc15d) 78

[ZONE\_REQUEST\_STUB](#section_f4cf1f3e7d134010a9155223dcabc15d) 78

[ZONE\_SECSECURE\_LIST\_ONLY](#section_751e1cf8c97f41c5ae499a674398d0f3) 77

[ZONE\_SECSECURE\_NO\_SECURITY](#section_751e1cf8c97f41c5ae499a674398d0f3) 77

[ZONE\_SECSECURE\_NO\_XFER](#section_751e1cf8c97f41c5ae499a674398d0f3) 77

[ZONE\_SECSECURE\_NS\_ONLY](#section_751e1cf8c97f41c5ae499a674398d0f3) 77

[ZONE\_UPDATE\_OFF](#section_d4b84209f00c478f80d78dd0f1633d9e) 99

[ZONE\_UPDATE\_SECURE](#section_d4b84209f00c478f80d78dd0f1633d9e) 99

[ZONE\_UPDATE\_UNSECURE](#section_d4b84209f00c478f80d78dd0f1633d9e) 99