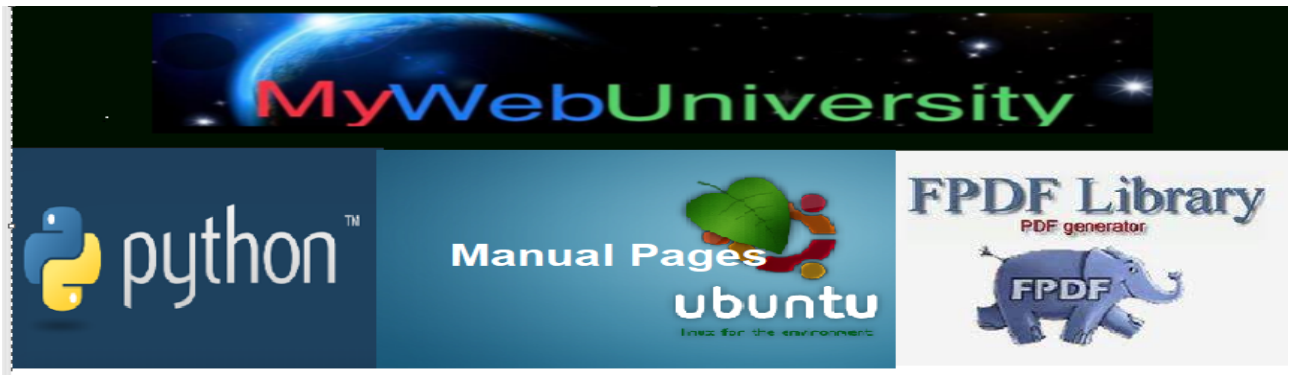

Full credit is given to the above companies including the OS that this PDF file was generated!

Linux Ubuntu 26.04 Manual Pages on command 'nsupdate.1'

$ man nsupdate.1

NSUPDATE(1) BIND 9 NSUPDATE(1)

NAME

nsupdate - dynamic DNS update utility

SYNOPSIS

nsupdate [-d] [-D] [-i] [-L level] [[-g] | [-o] | [-l] | [-y [hmac:]keyname:secret] | [-k keyfile]] [[-S] [-K tlskeyfile] [-E tlscertfile] [-A tlscafile] [-H tlshostname] [-O]] [-t timeout] [-u udptimeout] [-r udpretries] [-v] [-T] [-P] [-V] [[-4] | [-6]] [filename]

DESCRIPTION

nsupdate is used to submit Dynamic DNS Update requests, as defined in RFC 2136 <https://datatracker.ietf.org/doc/html/rfc2136.html>, to a name server. This allows resource records to be added or removed from a zone without manually editing the zone file. A single update request can contain requests to add or remove more than one resource record.

Zones that are under dynamic control via nsupdate or a DHCP server should not be edited by hand. Manual edits could conflict with dynamic updates and cause data to be lost.

The resource records that are dynamically added or removed with nsupdate must be in the same zone. Requests are sent to the zone's primary server, which is identified by the MNAME field of the zone's SOA record.

Transaction signatures can be used to authenticate the Dynamic DNS updates. These use the TSIG resource record type described in RFC 2845 <https://datatracker.ietf.org/doc/html/rfc2845.html>, the SIG(0) record described in RFC 2535 <https://datatracker.ietf.org/doc/html/rfc2535.html> and RFC 2931 <https://datatracker.ietf.org/doc/html/rfc2931.html>, or GSS-TSIG as described in RFC 3645 <https://datatracker.ietf.org/doc/html/rfc3645.html>.

TSIG relies on a shared secret that should only be known to nsupdate and the name server.

For instance, suitable key and server statements are added to /etc/bind/named.conf so that the name server can associate the appropriate secret key and algorithm with the IP address of the client application that is using TSIG authentication. ddns-confgen <# std-iscman-ddns-confgen> can generate suitable configuration fragments. nsupdate uses the -y or -k options to provide the TSIG shared secret; these options are mutually exclusive.

SIG(0) uses public key cryptography. To use a SIG(0) key, the public key must be stored in a KEY record in a zone served by the name server.

GSS-TSIG uses Kerberos credentials. Standard GSS-TSIG mode is switched on with the -g flag. A non-standards-compliant variant of GSS-TSIG used by Windows 2000 can be switched on with the -o flag.

OPTIONS

-4 This option sets use of IPv4 only.

-6 This option sets use of IPv6 only.

-A tlscafile

This option specifies the file of the certificate authorities (CA) certificates (in PEM format) in order to verify the remote server TLS certificate when using DNS-over-TLS (DoT), to achieve Strict or Mutual TLS. When used, it will override the certificates from the global certificates store, which are otherwise used by default when -S is enabled. This option can not be used in conjuction with -O, and it implies -S.

-C Overrides the default resolv.conf file. This is only intended for testing.

-d This option sets debug mode, which provides tracing information about the update re? quests that are made and the replies received from the name server.

-D This option sets extra debug mode.

-E tlscertfile

This option sets the certificate(s) file for authentication for the DNS-over-TLS (DoT) transport to the remote server. The certificate chain file is expected to be in PEM format. This option implies -S, and can only be used with -K.

-g This option enables standard GSS-TSIG mode.

-H tlshostname

This option makes nsupdate use the provided hostname during remote server TLS cer? tificate verification. Otherwise, the DNS server name is used. This option implies -S.

-i This option forces interactive mode, even when standard input is not a terminal.

-k keyfile

This option indicates the file containing the TSIG authentication key. Keyfiles may be in two formats: a single file containing a named.conf <#std-iscman-named.conf>-format key statement, which may be generated automatically by ddns-confgen <#std-iscman-ddns-confgen>; or a pair of files whose names are of the format K{name}.+157.+{random}.key and K{name}.+157.+{random}.private, which can be generated by dnssec-keygen <#std-iscman-dnssec-keygen>. The -k option can also be used to specify a SIG(0) key used to authenticate Dynamic DNS update requests. In this case, the key specified is not an HMAC-MD5 key.

-K tlskeyfile

This option sets the key file for authenticated encryption for the DNS-over-TLS (DoT) transport with the remote server. The private key file is expected to be in PEM format. This option implies -S, and can only be used with -E.

-l This option sets local-host only mode, which sets the server address to localhost (disabling the server so that the server address cannot be overridden). Connections to the local server use a TSIG key found in /run/session.key, which is automatically generated by named <#std-iscman-named> if any local primary zone has set update-policy to local. The location of this key file can be overridden with the -k option.

-L level

This option sets the logging debug level. If zero, logging is disabled.

-o This option is deprecated. Previously, it enabled a non-standards-compliant variant of GSS-TSIG that was used by Windows 2000. Since that OS is now long past its end of life, this option is now treated as a synonym for -g.

-O This option enables Opportunistic TLS. When used, the remote peer's TLS certificate will not be verified. This option should be used for debugging purposes only, and it is not recommended to use it in production. This option can not be used in conjuction with -A, and it implies -S.

-p port

This option sets the port to use for connections to a name server. The default is 53.

-P This option prints the list of private BIND-specific resource record types whose format is understood by nsupdate. See also the -T option.

-r udpretries

This option sets the number of UDP retries. The default is 3. If zero, only one up? date request is made.

-S This option indicates whether to use DNS-over-TLS (DoT) when querying name servers specified by server servername port syntax in the input file, and the primary server discovered through a SOA request. When the -K and -E options are used, then the spec? ified TLS client certificate and private key pair are used for authentication (Mutual TLS). This option implies -v.

-t timeout

This option sets the maximum time an update request can take before it is aborted. The default is 300 seconds. If zero, the timeout is disabled for TCP mode. For UDP mode, the option -u takes precedence over this option, unless the option -u is set to zero, in which case the interval is computed from the -t timeout interval and the number of UDP retries. For UDP mode, the timeout can not be disabled, and will be rounded up to 1 second in case if both -t and -u are set to zero.

-T This option prints the list of IANA standard resource record types whose format is understood by nsupdate. nsupdate exits after the lists are printed. The -T option can be combined with the -P option.

Other types can be entered using TYPEXXXXX where XXXXX is the decimal value of the type with no leading zeros. The rdata, if present, is parsed using the UNKNOWN rdata format, (<backslash> <hash> <space> <length> <space> <hexstring>).

-u udptimeout

This option sets the UDP retry interval. The default is 3 seconds. If zero, the in? terval is computed from the timeout interval and number of UDP retries.

-v This option specifies that TCP should be used even for small update requests. By de? fault, nsupdate uses UDP to send update requests to the name server unless they are too large to fit in a UDP request, in which case TCP is used. TCP may be preferable when a batch of update requests is made.

-V This option prints the version number and exits.

-y [hmac:]keyname:secret

This option sets the literal TSIG authentication key. keyname is the name of the key, and secret is the base64 encoded shared secret. hmac is the name of the key algo? rithm; valid choices are hmac-md5, hmac-sha1, hmac-sha224, hmac-sha256, hmac-sha384, or hmac-sha512. If hmac is not specified, the default is hmac-md5, or if MD5 was dis?

abled, hmac-sha256.

NOTE: Use of the -y option is discouraged because the shared secret is supplied as a command-line argument in clear text. This may be visible in the output from ps1 or in a history file maintained by the user's shell.

INPUT FORMAT

nsupdate reads input from filename or standard input. Each command is supplied on exactly one line of input. Some commands are for administrative purposes; others are either update instructions or prerequisite checks on the contents of the zone. These checks set conditions that some name or set of resource records (RRset) either exists or is absent from the zone. These conditions must be met if the entire update request is to succeed. Updates are re? jected if the tests for the prerequisite conditions fail.

Every update request consists of zero or more prerequisites and zero or more updates. This allows a suitably authenticated update request to proceed if some specified resource records are either present or missing from the zone. A blank input line (or the send command) causes the accumulated commands to be sent as one Dynamic DNS update request to the name server.

The command formats and their meanings are as follows:

server servername port

This command sends all dynamic update requests to the name server servername. When no server statement is provided, nsupdate sends updates to the primary server of the correct zone. The MNAME field of that zone's SOA record identify the primary server for that zone. port is the port number on servername where the dynamic update re? quests are sent. If no port number is specified, the default DNS port number of 53 is used.

Note:

This command has no effect when GSS-TSIG is in use.

local address port

This command sends all dynamic update requests using the local address. When no local statement is provided, nsupdate sends updates using an address and port chosen by the system. port can also be used to force requests to come from a specific port. If no port number is specified, the system assigns one.

zone zonename

This command specifies that all updates are to be made to the zone zonename. If no zone statement is provided, nsupdate attempts to determine the correct zone to update

based on the rest of the input.

class classname

This command specifies the default class. If no class is specified, the default class is IN.

ttl seconds

This command specifies the default time-to-live, in seconds, for records to be added. The value none clears the default TTL.

key hmac:keyname secret

This command specifies that all updates are to be TSIG-signed using the keyname-se? cret pair. If hmac is specified, it sets the signing algorithm in use. The default is hmac-md5; if MD5 was disabled, the default is hmac-sha256. The key command overrides any key specified on the command line via -y or -k.

gsstsig

This command uses GSS-TSIG to sign the updates. This is equivalent to specifying -g on the command line.

oldgsstsig

This command is deprecated and will be removed in a future release. Previously, it caused nsupdate to use the Windows 2000 version of GSS-TSIG to sign updates. It is now treated as a synonym for gsstsig.

realm [realm_name]

When using GSS-TSIG, this command specifies the use of realm_name rather than the de? fault realm in krb5.conf. If no realm is specified, the saved realm is cleared.

check-names [boolean]

This command turns on or off check-names processing on records to be added. Check-names has no effect on prerequisites or records to be deleted. By default check-names processing is on. If check-names processing fails, the record is not added to the UPDATE message.

check-svbc [boolean]

This command turns on or off check-svcb processing on records to be added. Check-svcb has no effect on prerequisites or records to be deleted. By default check-svcb processing is on. If check-svcb processing fails, the record is not added to the UPDATE message.

lease time [keytime]

Set the EDNS Update Lease (UL) option to value to time and optionally also set the key lease time to keytime in seconds. If time is none the lease times are cleared.

prereq nxdomain domain-name

This command requires that no resource record of any type exist with the name do? main-name.

prereq yxdomain domain-name

This command requires that domain-name exist (as at least one resource record, of any type).

prereq nxrrset domain-name class type

This command requires that no resource record exist of the specified type, class, and domain-name. If class is omitted, IN (Internet) is assumed.

prereq yxrrset domain-name class type

This command requires that a resource record of the specified type, class and do? main-name exist. If class is omitted, IN (internet) is assumed.

prereq yxrrset domain-name class type data

With this command, the data from each set of prerequisites of this form sharing a common type, class, and domain-name are combined to form a set of RRs. This set of RRs must exactly match the set of RRs existing in the zone at the given type, class, and domain-name. The data are written in the standard text representation of the re? source record's RDATA.

update delete domain-name ttl class type data

This command deletes any resource records named domain-name. If type and data are provided, only matching resource records are removed. The Internet class is assumed if class is not supplied. The ttl is ignored, and is only allowed for compatibility.

update add domain-name ttl class type data

This command adds a new resource record with the specified ttl, class, and data.

show This command displays the current message, containing all of the prerequisites and updates specified since the last send.

send This command sends the current message. This is equivalent to entering a blank line.

answer This command displays the answer.

debug This command turns on debugging.

version

This command prints the version number.

help This command prints a list of commands.

Lines beginning with a semicolon (;) are comments and are ignored.

EXAMPLES

The examples below show how nsupdate can be used to insert and delete resource records from the example.com zone. Notice that the input in each example contains a trailing blank line, so that a group of commands is sent as one dynamic update request to the primary name server for example.com.

```
# nsupdate
> update delete oldhost.example.com A
> update add newhost.example.com 86400 A 172.16.1.1
> send
```

Any A records for oldhost.example.com are deleted, and an A record for newhost.example.com with IP address 172.16.1.1 is added. The newly added record has a TTL of 1 day (86400 sec? onds).

```
# nsupdate
> prereq nxdomain nickname.example.com
> update add nickname.example.com 86400 CNAME somehost.example.com
> send
```

The prerequisite condition tells the name server to verify that there are no resource records of any type for nickname.example.com. If there are, the update request fails. If this name does not exist, a CNAME for it is added. This ensures that when the CNAME is added, it cannot conflict with the long-standing rule in RFC 1034 <https://datatracker.ietf .org/doc/html/rfc1034.html> that a name must not exist as any other record type if it exists as a CNAME. (The rule has been updated for DNSSEC in RFC 2535 <https://datatracker.ietf.org/ doc/html/rfc2535.html> to allow CNAMEs to have RRSIG, DNSKEY, and NSEC records.)

FILES

/etc/resolv.conf

Used to identify the default name server

/run/session.key

Sets the default TSIG key for use in local-only mode

K{name}.+157.+{random}.key

Base-64 encoding of the HMAC-MD5 key created by dnssec-keygen <# std-iscman-dnssec-keygen>.

K{name}.+157.+{random}.private

Base-64 encoding of the HMAC-MD5 key created by dnssec-keygen <#std-iscman-dnssec-keygen>.

SEE ALSO

RFC 2136 <https://datatracker.ietf.org/doc/html/rfc2136.html>, RFC 3007 <https://datatracker.ietf.org/doc/html/rfc3007.html>, RFC 2104 <https://datatracker.ietf.org/doc/html/rfc2104.html>, RFC 2845 <https://datatracker.ietf.org/doc/html/rfc2845.html>, RFC 1034 <https://datatracker.ietf.org/doc/html/rfc1034.html>, RFC 2535 <https://datatracker.ietf.org/doc/html/rfc2535.html>, RFC 2931 <https://datatracker.ietf.org/doc/html/rfc2931.html>, named(8) <#std-iscman-named>, dnssec-keygen(8) <#std-iscman-dnssec-keygen>, tsig-keygen(8) <#std-iscman-tsig-keygen>.

BUGS

The TSIG key is redundantly stored in two separate files. This is a consequence of nsupdate using the DST library for its cryptographic operations, and may change in future releases.

Author

Internet Systems Consortium

Copyright