



Rocky Enterprise Linux 9.2 Manual Pages on command 'nsec3hash.8'

\$ man nsec3hash.8

NSEC3HASH(8) BIND 9 NSEC3HASH(8)

NAME

nsec3hash - generate NSEC3 hash

SYNOPSIS

nsec3hash {salt} {algorithm} {iterations} {domain}

nsec3hash -r {algorithm} {flags} {iterations} {salt} {domain}

DESCRIPTION

nsec3hash generates an NSEC3 hash based on a set of NSEC3 parameters.

This can be used to check the validity of NSEC3 records in a signed zone.

If this command is invoked as nsec3hash -r, it takes arguments in order,

matching the first four fields of an NSEC3 record followed by the

domain name: algorithm, flags, iterations, salt, domain. This makes it

convenient to copy and paste a portion of an NSEC3 or NSEC3PARAM record

into a command line to confirm the correctness of an NSEC3 hash.

ARGUMENTS

salt This is the salt provided to the hash algorithm.

algorithm

This is a number indicating the hash algorithm. Currently the only supported hash algorithm for NSEC3 is SHA-1, which is indicated by the number 1; consequently "1" is the only useful value for this argument.

flags This is provided for compatibility with NSEC3 record presentation format, but is ignored since the flags do not affect the hash.

iterations

This is the number of additional times the hash should be performed.

domain This is the domain name to be hashed.

SEE ALSO

BIND 9 Administrator Reference Manual, RFC 5155.

AUTHOR

Internet Systems Consortium

COPYRIGHT

2021, Internet Systems Consortium

9.16.23-RH

NSEC3HASH(8)