NAME

ldns-verify-zone - read a DNSSEC signed zone and verify it.

SYNOPSIS

ldns-verify-zone *ZONEFILE*

DESCRIPTION

ldns-verify-zone reads a DNS zone file and verifies it.

RRSIG resource records are checked against the DNSKEY set at the zone apex.

Each name is checked for an NSEC(3), if appropriate.

If ZONEMD resource records are present, one of them needs to match the zone content.

OPTIONS

-h Show usage and exit

-a Apex only, check only the zone apex

-e *period*
Signatures may not expire within this period. Default no period is used.

-i *period*
Signatures must have been valid at least this long. Default signatures should just be valid now.

-k *file*
A file that contains a trusted DNSKEY or DS rr. This option may be given more than once.

Alternatively, if **-k** is not specified, and a default trust anchor (/usr/local/etc/unbound/root.key) exists and contains a valid DNSKEY or DS record, it will be used as the trust anchor.

-p *[0-100]*
Only check this percentage of the zone. Which names to check is determined randomly. Defaults

to 100.

-S Chase signature(s) to a known key. The network may be accessed to validate the zone's DNSKEYs. (implies -k)

-t *YYYYMMDDhhmmss | [+|-]offset*
Set the validation time either by an absolute time value or as an offset in seconds from the current time.

-v Show the version and exit

-V *number*
Set the verbosity level (default 3):

0: Be silent
1: Print result, and any errors
2: Same as 1 for now
3: Print result, any errors, and the names that are being checked
4: Same as 3 for now
5: Print the zone after it has been read, the result, any errors, and the names that are being checked

-Z Requires a valid ZONEMD RR to be present. When given once, this option will permit verifying only the ZONEMD RR of an unsigned zone. When given more than once, the zone needs to be validly DNSSEC signed as well.

-ZZZ
When three times a **-Z** option is given, the ZONEMD RR to be verified is considered "detached" and does not need to have valid signatures.

*period*s are given in ISO 8601 duration format:
P[n]Y[n]M[n]DT[n]H[n]M[n]S

If no file is given standard input is read.

FILES

/usr/local/etc/unbound/root.key

The file from which trusted keys are loaded for signature chasing, when no **-k** option is given.

SEE ALSO

unbound-anchor(8)

AUTHOR

Written by the ldns team as an example for ldns usage.

REPORTING BUGS

Report bugs to <ldns-team@nlnetlabs.nl>.

COPYRIGHT