
certbot-dns-linode Documentation

Release 0

Certbot Project

Jul 11, 2019

Contents:

1	API Documentation	1
1.1	certbot_dns_linode.dns_linode	1
2	Named Arguments	3
3	Credentials	5
4	Examples	7
5	Indices and tables	9
	Python Module Index	11
	Index	13

1.1 certbot_dns_linode.dns_linode

DNS Authenticator for Linode.

class `certbot_dns_linode.dns_linode.Authenticator` (*args, **kwargs)
Bases: `certbot.plugins.dns_common.DNSAuthenticator`

DNS Authenticator for Linode

This Authenticator uses the Linode API to fulfill a dns-01 challenge.

classmethod `add_parser_arguments` (add)
Add plugin arguments to the CLI argument parser.

NOTE: If some of your flags interact with others, you can use `cli.report_config_interaction` to register this to ensure values are correctly saved/overridable during renewal.

Parameters `add` (*callable*) – Function that proxies calls to `argparse.ArgumentParser.add_argument` prepending options with unique plugin name prefix.

`_setup_credentials` ()
Establish credentials, prompting if necessary.

`_perform` (*domain*, *validation_name*, *validation*)
Performs a dns-01 challenge by creating a DNS TXT record.

Parameters

- **`domain`** (*str*) – The domain being validated.
- **`validation_domain_name`** (*str*) – The validation record domain name.
- **`validation`** (*str*) – The validation record content.

Raises `errors.PluginError` – If the challenge cannot be performed

`__cleanup` (*domain*, *validation_name*, *validation*)

Deletes the DNS TXT record which would have been created by `__perform_achall`.

Fails gracefully if no such record exists.

Parameters

- **domain** (*str*) – The domain being validated.
- **validation_domain_name** (*str*) – The validation record domain name.
- **validation** (*str*) – The validation record content.

class `certbot_dns_linode.dns_linode._LinodeLexiconClient` (*api_key*, *api_version*)

Bases: `certbot.plugins.dns_common_lexicon.LexiconClient`

Encapsulates all communication with the Linode API.

The `dns_linode` plugin automates the process of completing a `dns-01` challenge (DNS01) by creating, and subsequently removing, TXT records using the Linode API.

CHAPTER 2

Named Arguments

<code>--dns-linode</code>	Linode credentials INI file. (Required)
<code>--dns-linode-p</code>	The number of seconds to wait for DNS to propagate before asking the ACME server to verify the DNS record. (Default: 1200 because Linode updates its first DNS every 15 minutes and we allow 5 more minutes for the update to reach the other 5 servers)

Credentials

Use of this plugin requires a configuration file containing Linode API credentials, obtained from your Linode account's [Applications & API Tokens page \(legacy\)](#) or [Applications & API Tokens page \(new\)](#).

Listing 1: Example credentials file:

```
# Linode API credentials used by Certbot
dns_linode_key = 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ64
dns_linode_version = [<blank>|3|4]
```

The path to this file can be provided interactively or using the `--dns-linode-credentials` command-line argument. Certbot records the path to this file for use during renewal, but does not store the file's contents.

Caution: You should protect these API credentials as you would the password to your Linode account. Users who can read this file can use these credentials to issue arbitrary API calls on your behalf. Users who can cause Certbot to run using these credentials can complete a `dns-01` challenge to acquire new certificates or revoke existing certificates for associated domains, even if those domains aren't being managed by this server.

Certbot will emit a warning if it detects that the credentials file can be accessed by other users on your system. The warning reads "Unsafe permissions on credentials configuration file", followed by the path to the credentials file. This warning will be emitted each time Certbot uses the credentials file, including for renewal, and cannot be silenced except by addressing the issue (e.g., by using a command like `chmod 600` to restrict access to the file).

Examples

Listing 1: To acquire a certificate for `example.com`

```
certbot certonly \  
  --dns-linode \  
  --dns-linode-credentials ~/.secrets/certbot/linode.ini \  
  -d example.com
```

Listing 2: To acquire a single certificate for both `example.com` and `www.example.com`

```
certbot certonly \  
  --dns-linode \  
  --dns-linode-credentials ~/.secrets/certbot/linode.ini \  
  -d example.com \  
  -d www.example.com
```

Listing 3: To acquire a certificate for `example.com`, waiting 1000 seconds for DNS propagation (Linode updates its first DNS every 15 minutes and we allow some extra time for the update to reach the other 5 servers)

```
certbot certonly \  
  --dns-linode \  
  --dns-linode-credentials ~/.secrets/certbot/linode.ini \  
  --dns-linode-propagation-seconds 1000 \  
  -d example.com
```


CHAPTER 5

Indices and tables

- `genindex`
- `modindex`
- `search`

C

`certbot_dns_linode`, 2

`certbot_dns_linode.dns_linode`, 1

Symbols

`_LinodeLexiconClient` (class in *certbot_dns_linode.dns_linode*), 2
`_cleanup()` (*certbot_dns_linode.dns_linode.Authenticator* method), 1
`_perform()` (*certbot_dns_linode.dns_linode.Authenticator* method), 1
`_setup_credentials()` (*certbot_dns_linode.dns_linode.Authenticator* method), 1

A

`add_parser_arguments()` (*certbot_dns_linode.dns_linode.Authenticator* class method), 1
`Authenticator` (class in *certbot_dns_linode.dns_linode*), 1

C

`certbot_dns_linode` (module), 2
`certbot_dns_linode.dns_linode` (module), 1