certbot-dns-cloudflare Documentation

Release 0

Certbot Project

Apr 10, 2024

CONTENTS:

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

Note: The plugin is not installed by default. It can be installed by heading to certbot.eff.org, choosing your system and selecting the Wildcard tab.

ONE

NAMED ARGUMENTS

`--dns-cloudflare-credent:`	Cloudflare *credentials* INI file. (Required)
`--dns-cloudflare-propaga:`	The number of seconds to wait for DNS to propagate before asking the ACME server to verify the DNS record. (Default: 10)

CREDENTIALS

Use of this plugin requires a configuration file containing Cloudflare API credentials, obtained from your Cloudflare dashboard.

Previously, Cloudflare's "Global API Key" was used for authentication, however this key can access the entire Cloudflare API for all domains in your account, meaning it could cause a lot of damage if leaked.

Cloudflare's newer API Tokens can be restricted to specific domains and operations, and are therefore now the recommended authentication option.

The Token needed by Certbot requires `Zone:DNS:Edit` permissions for only the zones you need certificates for.

Using Cloudflare Tokens also requires at least version 2.3.1 of the `cloudflare` Python module. If the version that automatically installed with this plugin is older than that, and you can't upgrade it on your system, you'll have to stick to the Global key.

Listing 1: Example credentials file using restricted API Token (recommended):

```
# Cloudflare API token used by Certbot
dns_cloudflare_api_token = 0123456789abcdef0123456789abcdef01234567
```

Listing 2: Example credentials file using Global API Key (not recommended):

```
# Cloudflare API credentials used by Certbot
dns_cloudflare_email = cloudflare@example.com
dns_cloudflare_api_key = 0123456789abcdef0123456789abcdef01234
```

The path to this file can be provided interactively or using the `--dns-cloudflare-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 Cloudflare 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).

Note: Please note that the `cloudflare` Python module used by the plugin has additional methods of providing credentials to the module, e.g. environment variables or the `cloudflare.cfg` configuration file. These methods are not supported by Certbot. If any of those additional methods of providing credentials is being used, they must provide the same credentials (i.e., email and API key *or* an API token) as the credentials file provided to Certbot. If there is a discrepancy, the `cloudflare` Python module will raise an error. Also note that the credentials provided to Certbot will take precedence over any other method of providing credentials to the `cloudflare` Python module.

EXAMPLES

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

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

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

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

Listing 3: To acquire a certificate for `example.com`, waiting 60 seconds for DNS propagation

```
certbot certonly \
  --dns-cloudflare \
  --dns-cloudflare-credentials ~/.secrets/certbot/cloudflare.ini \
  --dns-cloudflare-propagation-seconds 60 \
  -d example.com
```

FOUR

API DOCUMENTATION

Certbot plugins implement the Certbot plugins API, and do not otherwise have an external API.

FIVE

INDICES AND TABLES

- genindex
- modindex
- search

PYTHON MODULE INDEX

C

certbot_dns_cloudflare, 1

C

certbot_dns_cloudflare
    module, 1

M

module
    certbot_dns_cloudflare, 1