

Contents

OPNSense and CloudDNS2

Home Assistant and CloudDNS4

Proxmox and CloudDNS.....5

OPNSense and ClouDNS

1. Install ACME Plugin
2. After installation go to **Services > ACME Client > Settings** and enable plugin
3. After enabling plugin go to **Services > ACME Client > Accounts** and create account used for Let's Encrypt. See image OPNSense_LetsEncrypt.png

Edit Account full help

Enabled ☒

Name

Description

NOTE: Settings below must not be changed after account registration.

E-Mail Address

ACME CA

Optional EAB Credentials

Key Identifier

HMAC Key

Cancel Save

4. After registration Let's Encrypt go to **Services > ACME Client > Challenge Types** and configure CloudDNS. See image OPNSense_Challenge_CloudDNS.png

Edit Challenge Type full help

Enabled ☒

Name

Description

Challenge Type

DNS-01

DNS Service

DNS Sleep Time

CloudDNS

Auth ID

Sub Auth ID

Auth Password

Cancel Save

5. After setting up Challenge Types go to **Services > ACME Client > Certificates** and configure the certificate you want to use and select the previous created Challenge Type and Renew Webinterface automation. See image OPNS_Certificate.png

Edit Certificate

full help

Certificate Options

Enabled

☒

Common Name

Description

Alt Names

Clear All

Copy

ACME CA Settings

ACME Account

Challenge Type

Auto Renewal

☒

Renewal Interval

Security Settings

Key Length

OCSP Must Staple

☐

Advanced Settings

Automations

Clear All

Copy

DNS Alias Mode

Cancel

Save

6. Select the **Issue or Renew certificate** command. See image OPNSense_RequestRenewCertificate.png

Services: ACME Client: Certificates

Introduction Certificates							
Enabled	Common Name	Multi-Domain (SAN)	Description	Issue/Renewal Date	Last ACME Status	Last ACME Run	Commands
<input checked="" type="checkbox"/>	*.domain.com		Wildcard	15/02/2024, 02:56:43	OK	15/02/2024, 02:56:43	<div><div>Issue/Renew All Certificates</div></div>

3

Home Assistant and CloudDNS

1. ¹Install the **Let's Encrypt** add-on in Home Assistant
2. Configure the **Let's Encrypt** add-on using DNS Challenge and CloudDNS as provider. See image HASS_CloudDNS.png

[Info](#) [Documentation](#) [Configuration](#) [Log](#)

Let's Encrypt

Options

homeassistant.domain.com ✕

Domains

The domain names to issue certificates for, use "*" for wildcard certificates.

Email*

The email address that will be registered for the certificate.

Private Key File*

privkey.pem

Path to where the Private Key File will be placed.

Certificate File*

fullchain.pem

Path to where the Certificate File will be placed.

Challenge

☒ dns

☐ http

The type of challenge used to validate the domain.

Key Type

☒ ecdsa

☐ rsa

Select the certificate key type. If unset, will auto-detect based on the key type of the existing certificate or default to ecdsa.

Elliptic Curve

☒ secp256r1

☐ secp384r1

Elliptic curve for ECDSA keys. This option must be used with Key Type set to ECDSA. If unset the Certbot default will be used.

DNS

```
1 provider: dns-cloudns
2 cloudns_sub_auth_user: xxxxxxxxxxxxxx
3 cloudns_auth_password: xxxxxxxxxxxxxx
4
```

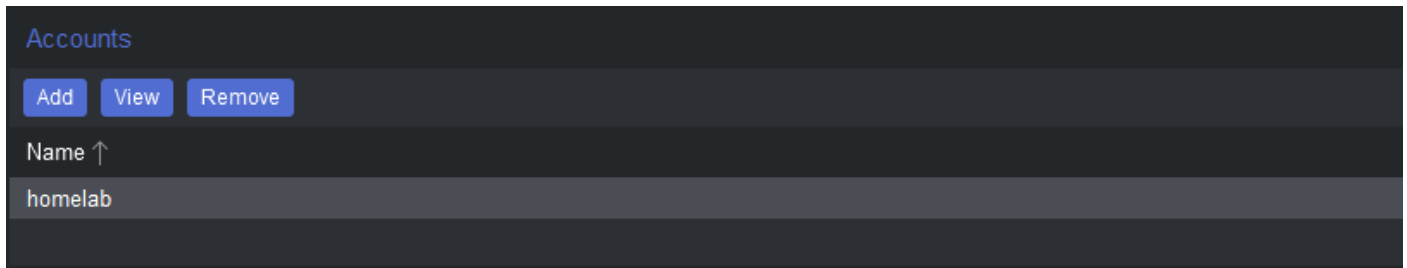
DNS Provider configuration

☐ Show unused optional configuration options

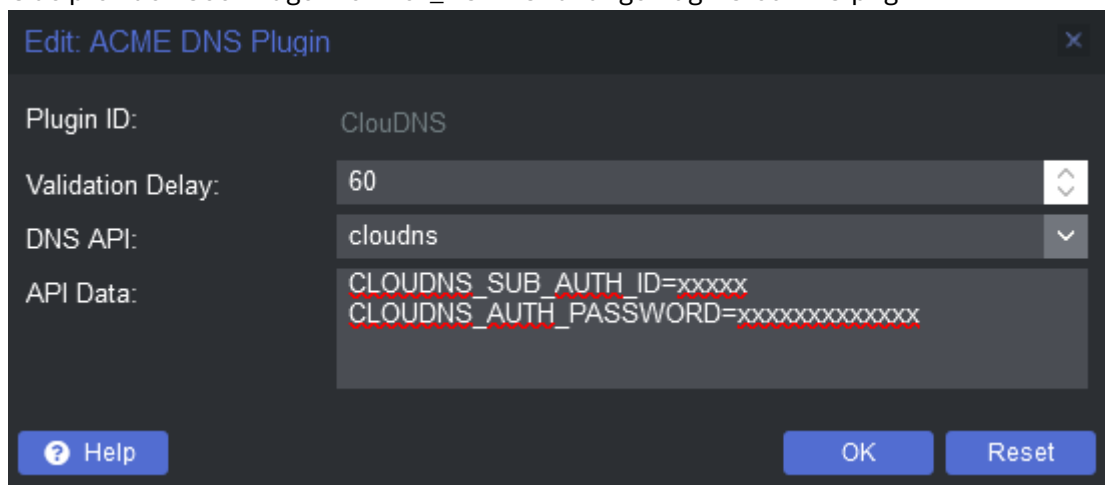
SAVE

Proxmox and CloudDNS

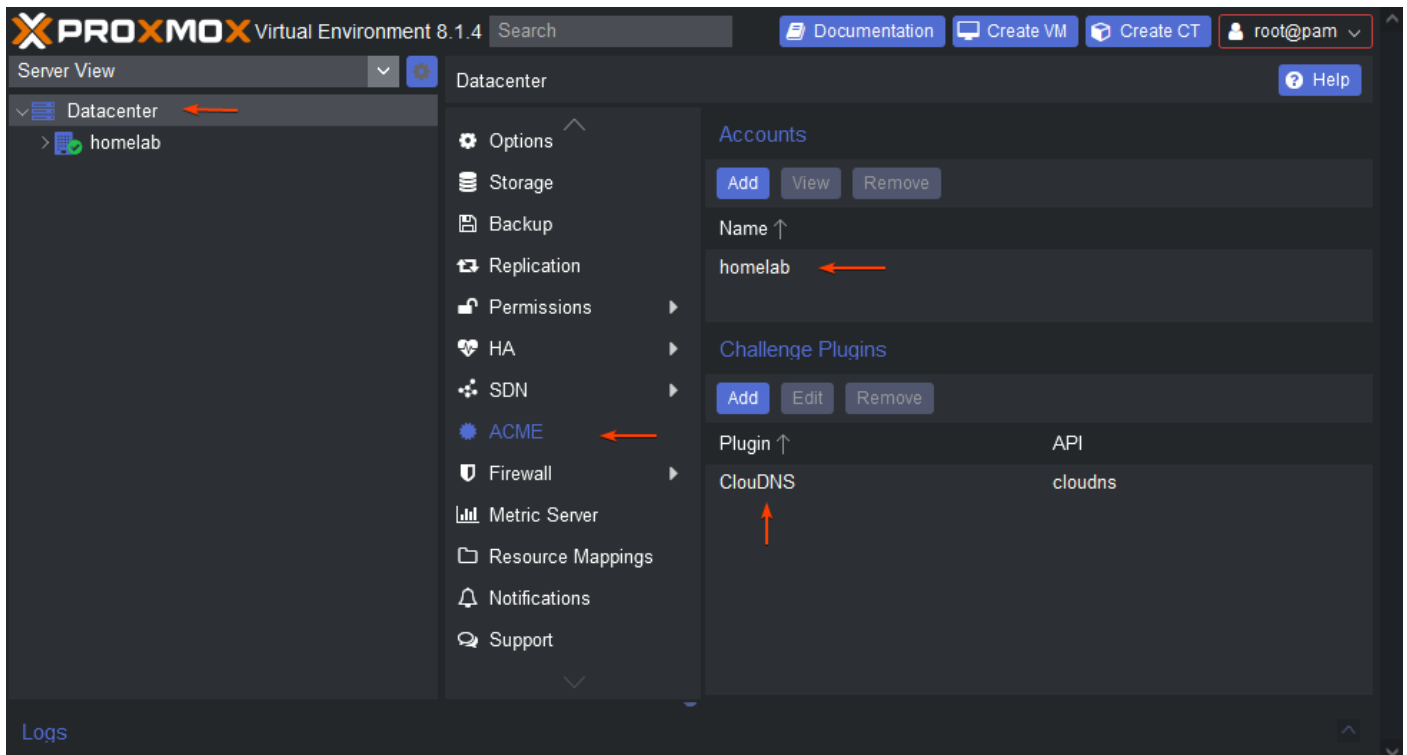
1. Install ACME Plugin if not already installed
2. After installation go to **Datacenter > ACME** and create account used for Let's Encrypt. See image Proxmox_ACMEClient_Overview.png



3. After creating Let's Encrypt account go to **Datacenter > ACME** and create Challenge Plugin using CloudDNS as provider. See image Proxmox_ACMEChallengePluginCloudDNS.png



It should look like this:



4. After creating Challenge Plugin go to **Node > Certificates** and add ACME Domain. Select DNS as challenge and the previous created Challenge Plugin and fill in the domain name. See image Proxmox_NodeCertificateACME.png

