

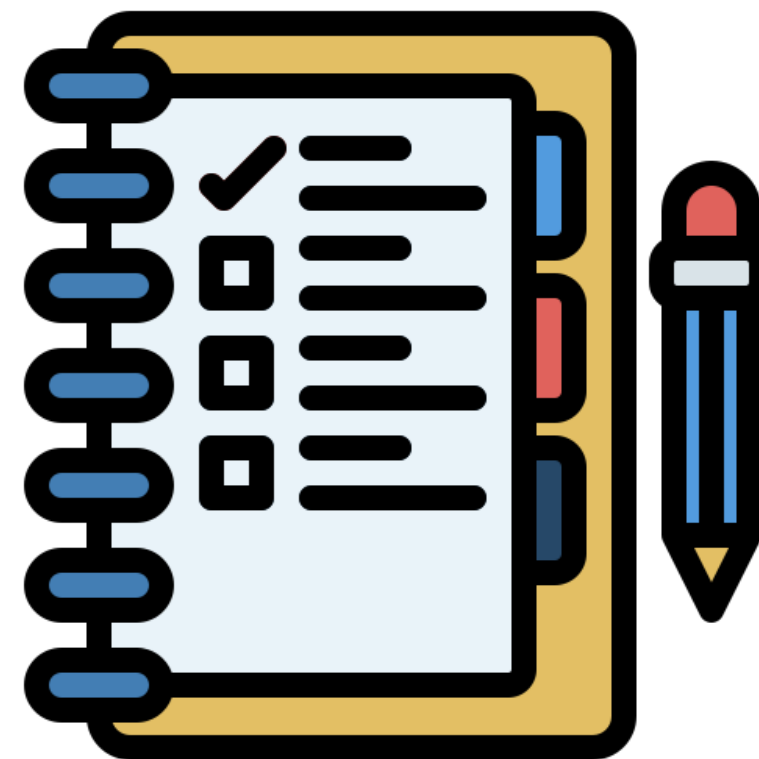
HARICA - ACME

Usar ACME no serviço de certificados
RCTS



HARICA - Agenda

- O que é o ACME
- Criar conta ACME
- Reciclar instalação ACME
- Nova instalação ACME
- Considerações gerais



O que é o ACME



- **Automated Certificate Management Environment**
- Protocolo de comunicação
 - Entre **Cliente** (nosso servidor) e **CA** (*HARICA*)
 - Seguro
- Permite:
 - Automatizar processo de obtenção (e renovação) de certificados SSL
 - **Sem intervenção manual**

O que é o ACME



- **Automático!!** (emissão, revocação, renovação, etc.)
- Mantém certificados **atualizados**
- **Reduz** hipóteses de **erro humano**
- **Melhor segurança**
- **Transversal às várias CAs** (vs. API)

Certbot – O que é?



- Ferramenta **grátis** e *open-source*
- **Cliente ACME**
 - Comunica com a CA (*HARICA*)
 - Protocolo ACME
- Instalado + configurado:
 - Obtenção e renovação automática de certificados SSL
- Clientes alternativos
 - Win-acme - <https://www.win-acme.com/>
 - LeGo CertHub - <https://www.legocerthub.com/>

Criar conta ACME



- Contas criadas por Admins
- Definir realms
- Obter credenciais

Recomendações

- O mais limitado possível
- Exemplo: Uma conta por serviço



Criar conta ACME – 1



- Aceder ao site da HARICA
- Escolher:
 1. Enterprise
 2. Admin
- Separador ACME
- Carregar em “Create”

The screenshot shows the 'Enterprise Manager' interface. At the top, there are navigation tabs: 'Enterprises', 'Users', 'Certificates', 'Bulk Certificates', and 'ACME'. The 'ACME' tab is selected. Below the tabs, there is a 'Create +' button with a red arrow pointing to it. Below the button is a search bar with the text 'educam' and a search icon. Below the search bar is a table with the following columns: 'Friendly Name', 'Organization', 'Created By', 'Created At', and 'Status'. The table contains one row of data:

Friendly Name	Organization	Created By	Created At	Status
ACME educam	Fundação para a Ciência e a Tecnologia I.P	psimoes@fccn.pt	24/06/2025	✔

Criar conta ACME – 2



1. Escolher Organização
2. Definir certificado (OV/DV)
3. Atribuir nome da conta
4. Aceitar as regras
5. Carregar “Create”

Create ACME EAB Account

The screenshot shows the 'Create ACME EAB Account' form with five numbered steps indicated by red arrows:

- 1 Choose Organization**: A dropdown menu is set to 'Fundação para a Ciência e a Tecnologia I.P.'
- 2 Choose Certificate Type**: A dropdown menu is set to 'SSL OV'.
- 3 Add Friendly Name**: A text input field contains 'Testes eduoam'.
- 4**: A checkbox is checked, indicating agreement with the terms and conditions.
- 5**: The 'Create' button is highlighted.

Additional form details include: Country: PT, State: Lisboa, Locality: Lisboa, Name: Fundação para a Ciência e a Tecnologia I.P., and Domains: pubin.pt, perma.pt, gigapix.pt, ticsociedade.pt. A note at the bottom states: 'Please note: You can define specific rules for each domain that will be included in this ACME EAB account later.'

Criar conta ACME – 4



- Aceder a “Domains”
- Escolher a conta criada
- “+” em domínios pretendidos
 - Escolher 1 ou vários

Details Certificates Domains

Allow All Domains

Available Domains

Domain	Validity
+ pubin.pt	09/08/2026
+ perma.pt	08/01/2025
+ gigapix.pt	08/01/2025
+ ticsociedade.pt	08/01/2025
+ eduroam.pt	10/02/2026
+ cienciaid.pt	08/01/2025
+ gridcomputing.pt	08/01/2025
+ fct.pt	17/02/2026
+ gtaedes.pt	09/08/2026
+ linguateca.pt	08/01/2025
+ ciencia-id.pt	14/07/2026

Active Rules (Explicit denial takes precedence over allowance)

Domain	Allowed	Rule applies to Subdomains

Inactive Rules

Domain	Allowed	Rule applies to Subdomains



Criar conta ACME – 5



- Para cada domínio:
 - Definir sub-domínios
 - “Deny” ou “Allow”
 - Autorizar sub-domínios
- Terminar com “Add”
- Podem depois reverter

Add New Rule

Domain: .eduroam.pt

Access Rule: Deny Allow

Applies also to subdomains?

4 →

Add

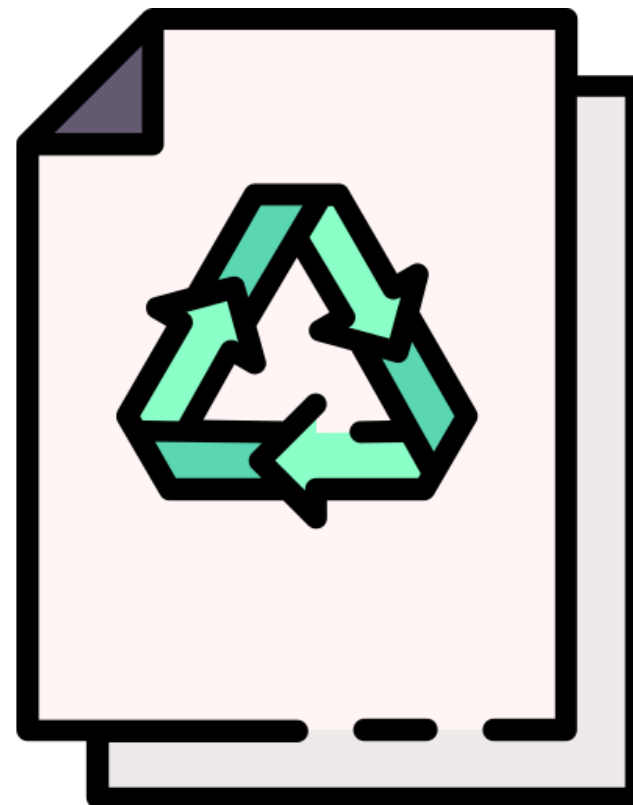
Close

Reciclar ACME



Processo

- Usar o novo ANSIBLE
- Configurar com novos dados
- Forçar a nova conta ACME

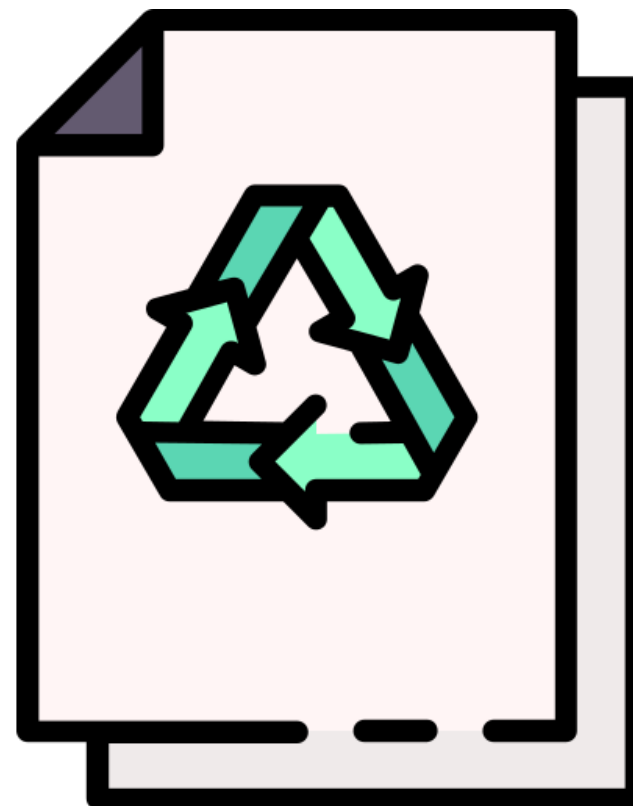


Reciclar ACME



Observações

- Obter dados da nova conta
 - `/etc/letsencrypt/accounts/`
- Alterar conta ACME
 - `/etc/letsencrypt/renewal/`
- Erro de chave?
 - `option_encryption_algorithm='rsa'`



Nova instalação ACME



- **Pré-requisitos:**

- Conta ACME já criada

- **Funcionalidades:**

- Instala *certbot*
- Faz pedido de certificado(s)
- Transfere certificado(s)
- Confirma se certificados estão válidos (periodicamente)



HARICA



Considerações gerais

Link do pacote Ansible

<https://github.com/fccn/asr-certbot>

Recomendações

- O mais compartimentado possível
- Exemplo: Conta por serviço (Apache, FTP, Mail)



Obrigado!

jornadas.fccn.pt

fccn.pt