

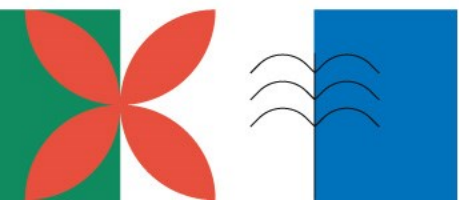
# RCTS Certificados

## Workshop

Renovação Automática de Certificados - Hands On

João Guerreiro – [joao.guerreiro@fccn.pt](mailto:joao.guerreiro@fccn.pt)

[jornadas.fccn.pt](http://jornadas.fccn.pt)



# Motivação – Alteração da Validade

<https://www.chromium.org/Home/chromium-security/root-ca-policy/moving-forward-together/>

In a future policy update or CA/Browser Forum Ballot Proposal, we intend to introduce:

2023/03/03

- **a reduction of TLS server authentication subscriber certificate maximum validity from 398 days to 90 days.** Reducing certificate lifetime encourages automation and the adoption of practices that will drive the ecosystem away from baroque, time-consuming, and error-prone issuance processes. These changes will allow for faster adoption of emerging security capabilities and best practices, and promote the agility required to transition the ecosystem to quantum-resistant algorithms quickly. Decreasing certificate lifetime will also reduce ecosystem reliance on “[broken](#)” revocation checking solutions that [cannot fail-closed](#) and, in turn, offer incomplete protection. Additionally, shorter-lived certificates will decrease the impact of unexpected Certificate Transparency Log disqualifications.

- **Validade máxima de 90 dias** (antes: 1 ano)



# ACME – O que é?



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



# ACME – Vantagens



- **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 (*Sectigo*)
  - Protocolo ACME
- Instalado + configurado:
  - Obtenção e renovação automática de certificados SSL



# Hands-on Criação de Conta ACME

## Administradores de Certificados da Instituição

- Criar conta(s) ACME
- Associar domínios da instituição ligados a uma conta
- **Obter credenciais da conta**

## Recomendações

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

Ver documentação em:

<https://share.fccn.pt/sites/rctscertificados/ACME/acme/#page-toc-10>

Create ACME Account

Name \*

Organization \*  
Fundacao para a Ciencia e a Tecnologia I.P.

Department  
None

Validation Type OV

Domains

Domains Remove All +

+ Add all

eduroam|

\*eduroam.pt

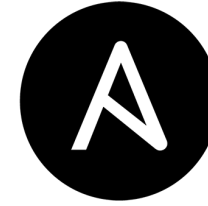
eduroam.pt

eduroam.pt

Save

# Hands-On

## Pacote Ansible – ACME



ANSIBLE

### • Pré-requisitos:

- Conta ACME já criada
- Instalar dependências:

```
> sudo apt install -y ansible unzip
> wget --no-check-certificate
https://share.fccn.pt/sites/rctscertificados/assets/acme/certbot_playbook_
1.1.11.zip
> unzip certbot_playbook_1.1.11.zip -d certbot_ansible
> cd certbot_ansible
```

Ver documentação em:

<https://share.fccn.pt/sites/rctscertificados/ACME/acme/#page-toc-11>



# Hands-On

## Pacote Ansible – ACME



- **Pré-requisitos:**

- Configurar Inventário com credenciais
- Utilizar *Ansible-Vault* para encriptar credenciais

Ver documentação em:

<https://share.fccn.pt/sites/rctscertificados/ACME/acme/#page-toc-11>





# Hands-On

## Pacote Ansible – ACME



- Executar playbook

```
> sudo ansible-playbook playbook_acme_ssl.yml --ask-vault-pass --extra-  
vars "option_credentials_file='defaults/credentials.yml'  
option_acme_account_name='idp-workshop'  
option_common_names_list='workshop05.idp.fccn.pt'  
option_multi_domain='single-domain' option_post_hook='service apache2  
reload'"
```

Ver documentação em:

<https://share.fccn.pt/sites/rctscertificados/ACME/acme/#page-toc-11>



# Hands-On

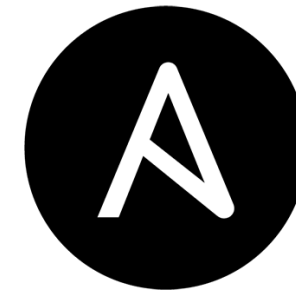
## Pacote Ansible – ACME

- **Pré-requisitos:**

- Conta ACME já criada

- **Funcionalidades**

- Instala *certbot*
- Regista Cliente ACME na CA (Sectigo)
- Faz pedido de certificado(s)
- Transfere certificado(s)
- Confirma se certificados ainda estão válidos (periodicamente)



A N S I B L E

Ver documentação em:

<https://share.fccn.pt/sites/rctscertificados/ACME/acme>



# Infraestrutura Simples

## Exemplo 1

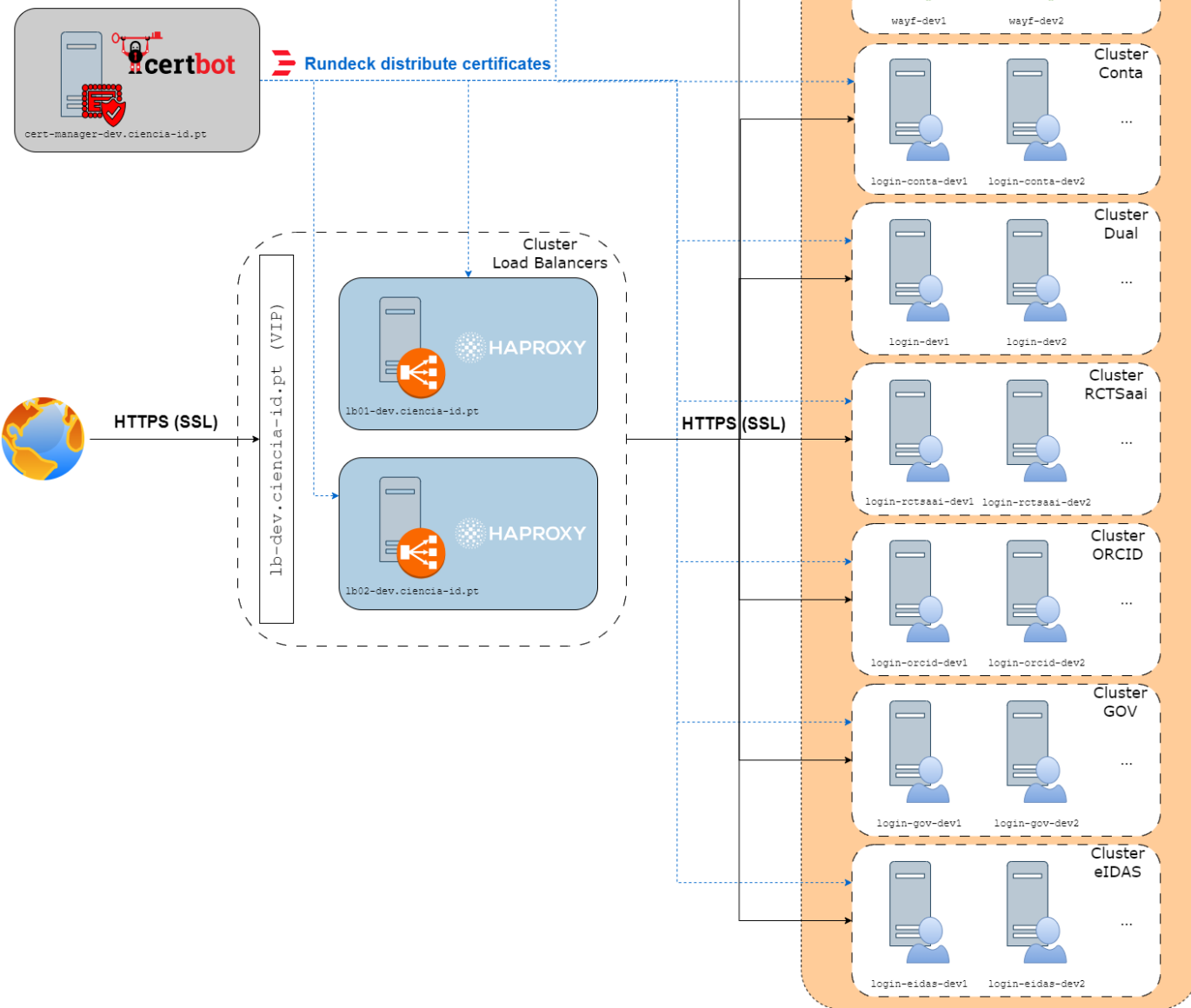
- **Servidor *web*** (*apache, nginx, etc.*)
- **certbot junto do servidor *web***
  - Certificados/chave privada no local de destino



# Infraestrutura complexa

## Exemplo 2

- **Infraestrutura mais complexa (eg., CIÊNCIA ID)**
  - *Load-balancers* com redundância
  - Servem vários certificados SSL
  - Mesmos certificados nos 2 LBs
- **Novo servidor (*cert-manager*)**
  - Com agente *certbot*
  - Mantém certificados atuais
  - Certificados e chave privada copiados para os locais necessários



# Windows

Cliente: Win-acme

<https://www.win-acme.com/>

- Fácil de executar
- Pode configurar certificados directamente no IIS

```

I:\Git\Repos\win-acme\src\main\bin\Release\netcoreapp3.1\wacs.exe

A simple Windows ACMEv2 client (WACS)
Software version 2.1.2.0 (RELEASE, TRIMMED)
IIS version 10.0
Running with administrator credentials
Scheduled task looks healthy
Please report issues at https://github.com/PKISharp/win-acme

N: Create new certificate (simple for IIS)
M: Create new certificate (full options)
R: Run scheduled renewals [0 currently due]
A: Manage renewals [0 renewals with 0 errors]
O: More options...
Q: Quit

Please choose from the menu:
  
```





# LeGo CertHub

- <https://www.legocerthub.com/>
- Para Linux e Windows
  - Também pode correr em *containers*
- Permite configurar diferentes contas ACME
- Certificados/Chaves podem ser obtidos acedendo à API de forma segura

The screenshot shows the LeGo CertHub dashboard. On the left is a navigation menu with options: Dashboard, Private Keys, ACME Accounts, Certificates, Order Queue, Logs, Providers, ACME Servers, and Settings. The main content area displays a table of certificates under the heading 'Dashboard'.

Name	Subject	Flags	Expiration (Remaining)
r210ii-1	r210ii-1		01/17/2024 42 Days
vcenter.c	vcenter		01/20/2024 45 Days
r320-1-e	r320-1		01/20/2024 45 Days
r220-1-e	r220-1		01/20/2024 45 Days
edge-sw	edge-s	Legacy API	01/22/2024 47 Days
vm-unifi	vm-unifi		01/24/2024 49 Days
vm-adgu	vm-adg		01/26/2024 51 Days
vm-med	vm-me		01/29/2024 54 Days
vm-zone	vm-zon		01/30/2024 55 Days
r320-1-ic	r320-1		02/08/2024 64 Days
vm-pfse	vm-pfs		02/18/2024 74 Days

© 2023 Greg T. Wallace





**A** Pacote Ansible e documentação em [share.fccn.pt](https://share.fccn.pt)

<https://share.fccn.pt/sites/rctscertificados/ACME/acme>

## Questões?

Esmeralda Pires – [epires@fccn.pt](mailto:epires@fccn.pt)

Filipe Santana – [filipe.santana@fccn.pt](mailto:filipe.santana@fccn.pt)

João Guerreiro – [joao.guerreiro@fccn.pt](mailto:joao.guerreiro@fccn.pt)

Pedro Simões – [psimoes@fccn.pt](mailto:psimoes@fccn.pt)

[jornadas.fccn.pt](https://jornadas.fccn.pt)

