jornadas FCCN

RCTS Certificados

Workshop

Renovação Automática de Certificados - Hands On

João Guerreiro – joao.guerreiro@fccn.pt

jornadas.fccn.pt

FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | arditi agência regional para o desenvolvimento da investigação tecnologia e inovação | SIH | UNIVERSIDADE da MADEIRA

Motivação – Alteração da Validade

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

2023/03/03

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

- **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?

- **A**utomated **C**ertificate **M**anagement **E**nvironment
- 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

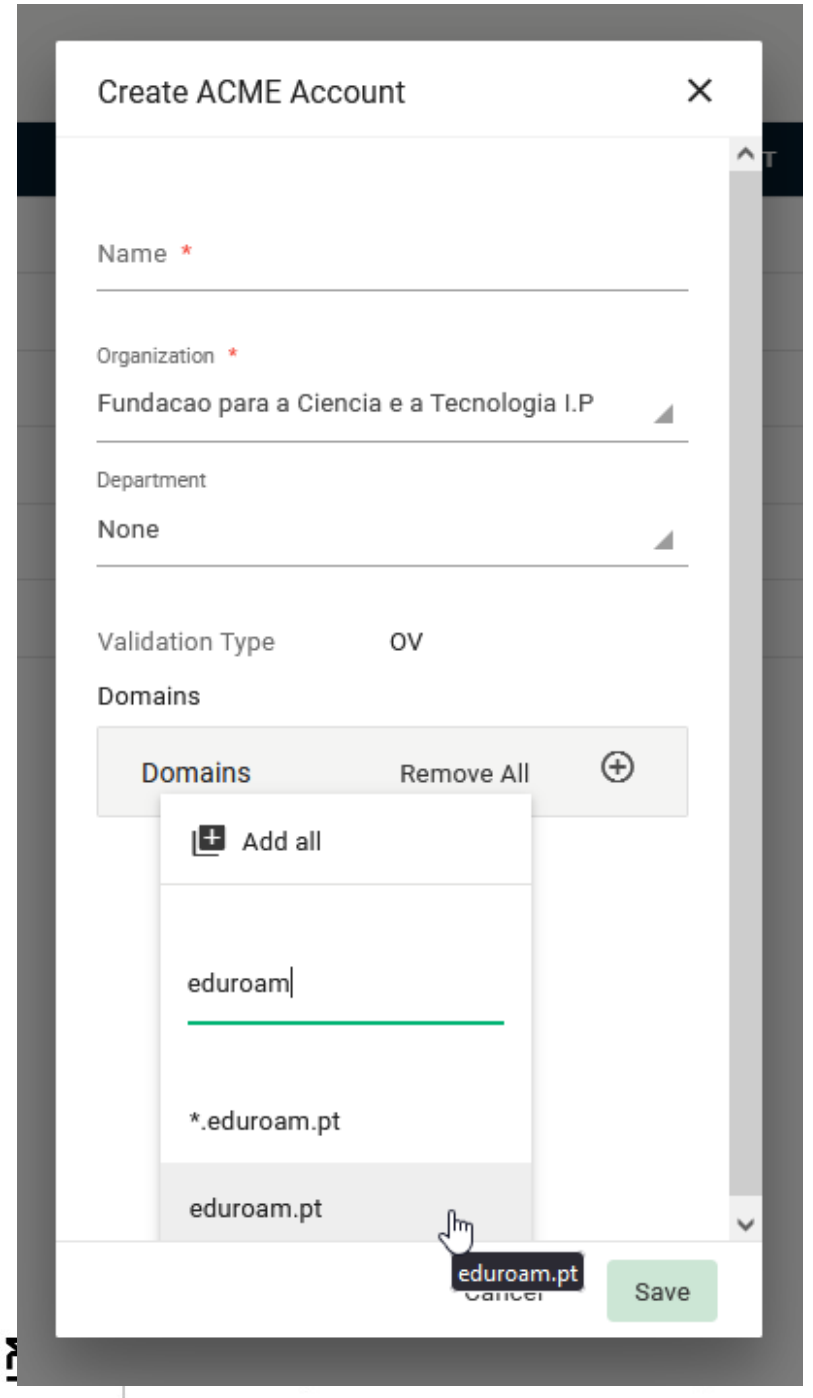
<u>Administradores de Certificados da Instituição</u>

- 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



Hands-On
Pacote Ansible – ACME

- **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)

Ver documentação em:
https://share.fccn.pt/sites/rctscertificados/ACME/acme

Infraestrutura Simples

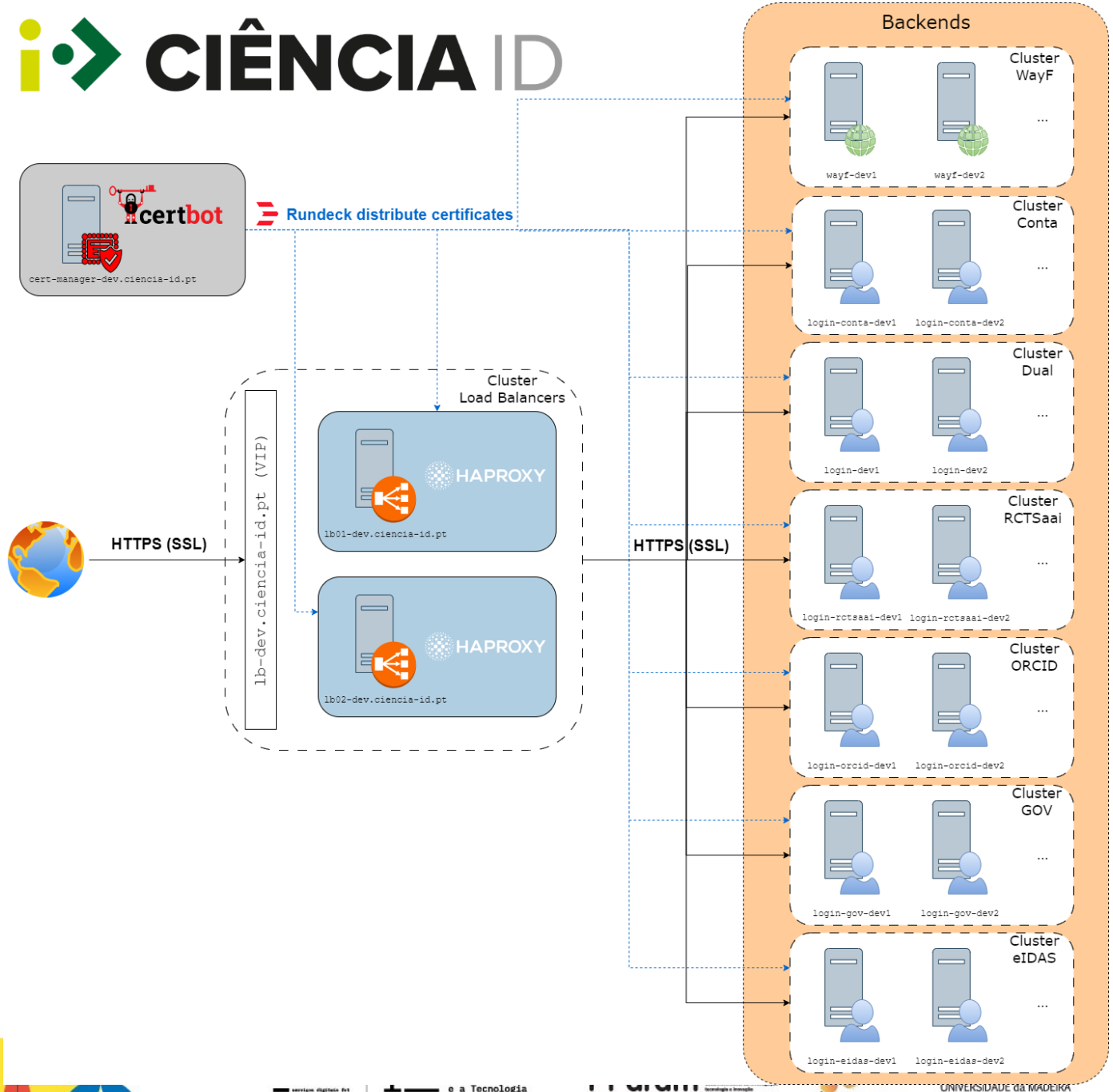
Exemplo 1

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

Infraestrutura complexa

Exemplo 2

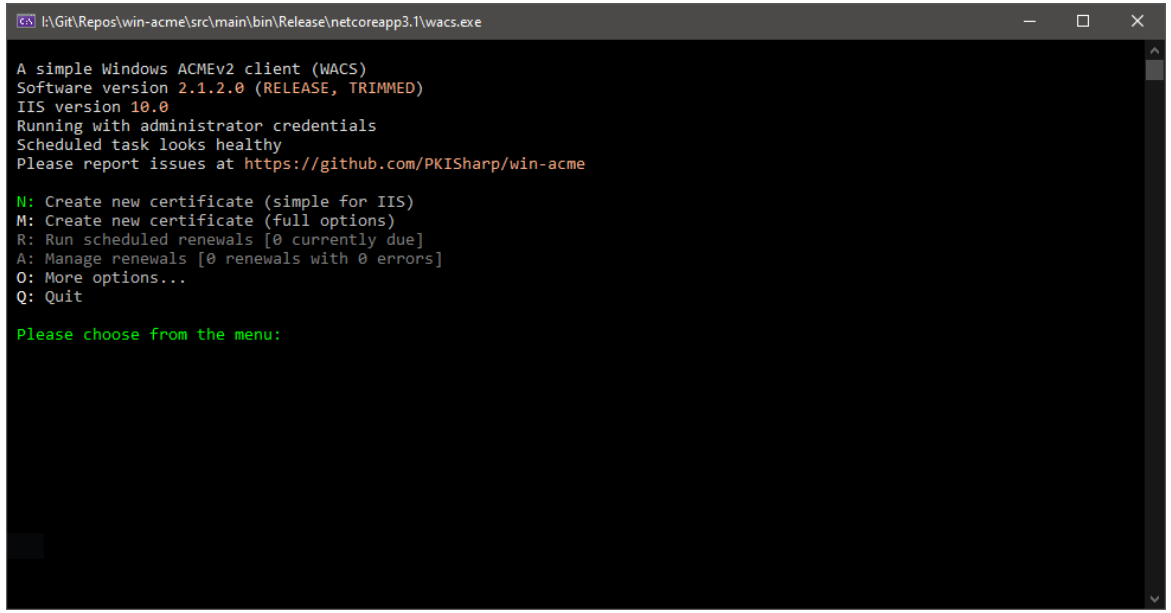
- **Infraestrutura mais complexa (eg., CIÊNCIA ID)**
  - *Load-balancers* com redundância
  - Servem vários certificados SSL
  - Mesmos certificados nos 2 LBs
- **Novo servidor** *(cert-manager)*
  - **Com agente *certbot***
  - Mantém certificados atuais
  - Certificados e chave privada copiados para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



Windows

Cliente: Win-acme

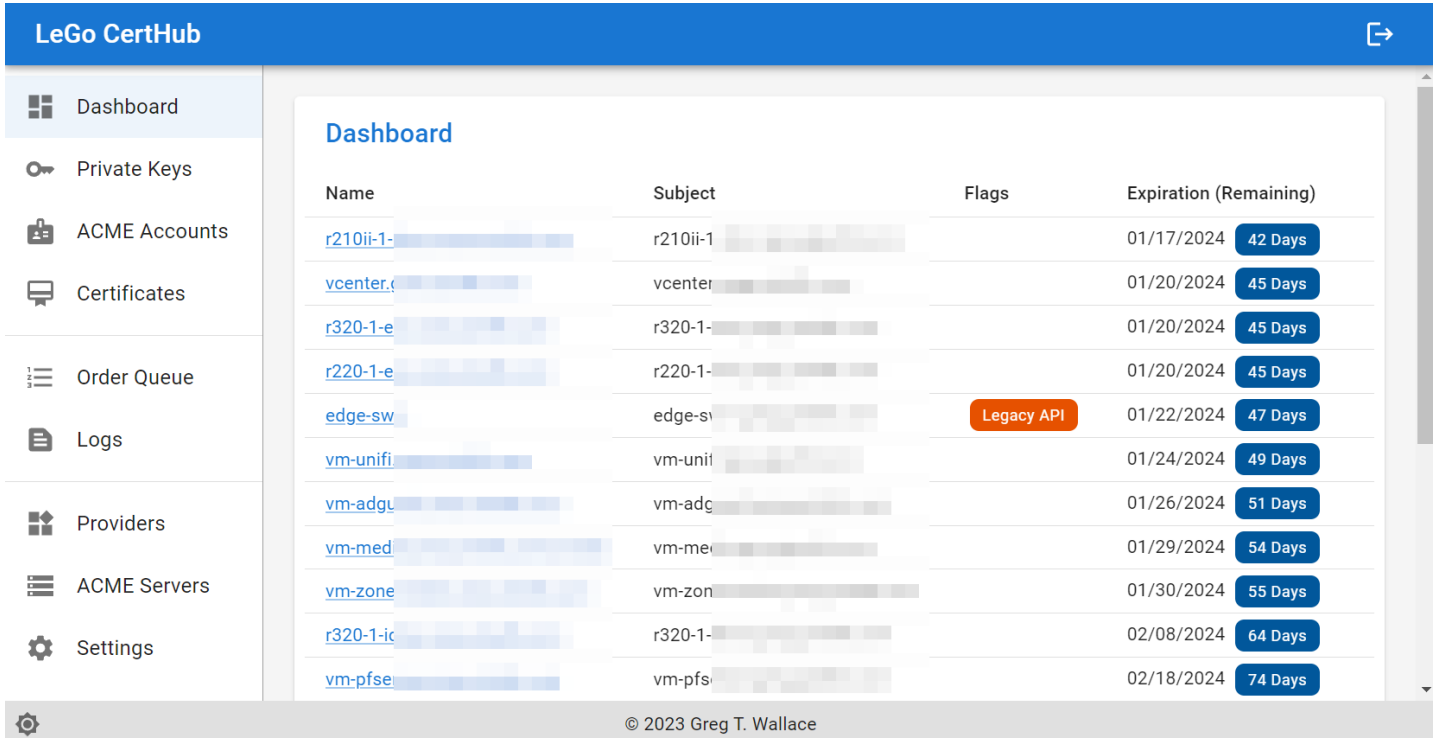
https://www.win-acme.com/



- Fácil de executar
- Pode configurar certificados directamente no IIS

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



jornadas FCCN

RCTS Certificados

Pacote Ansible e documentação em *share.fccn.pt*

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

Questões?

Esmeralda Pires – epires@fccn.pt

Filipe Santana – filipe.santana@fccn.pt

João Guerreiro – joao.guerreiro@fccn.pt

Pedro Simões – psimoes@fccn.pt