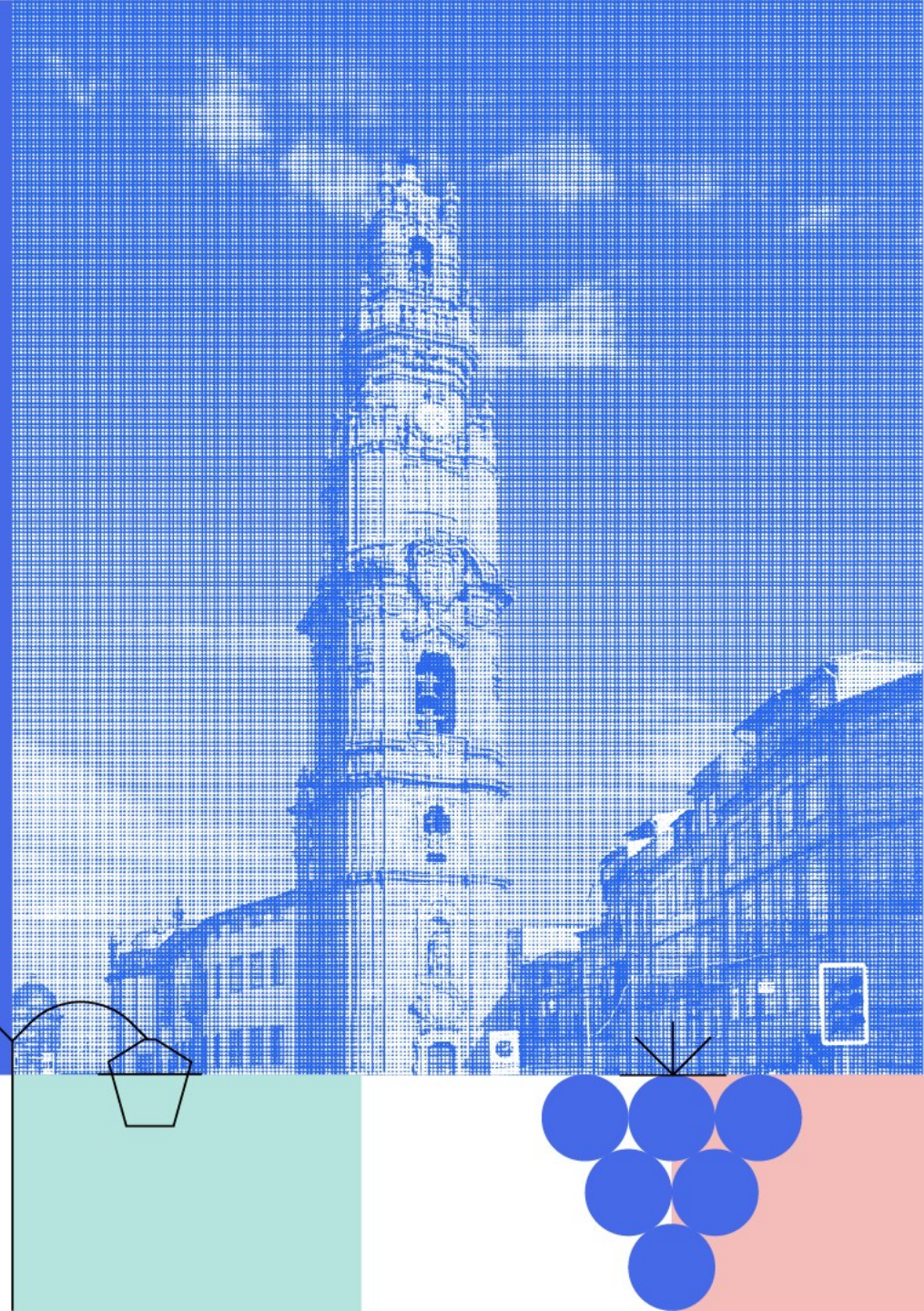
jornadas FCCN

Ludus para automação de criação de Cyber Ranges

Instituto Politécnico de Bragança

Jorge Loureiro

jorge.loureiro@ipb.pt

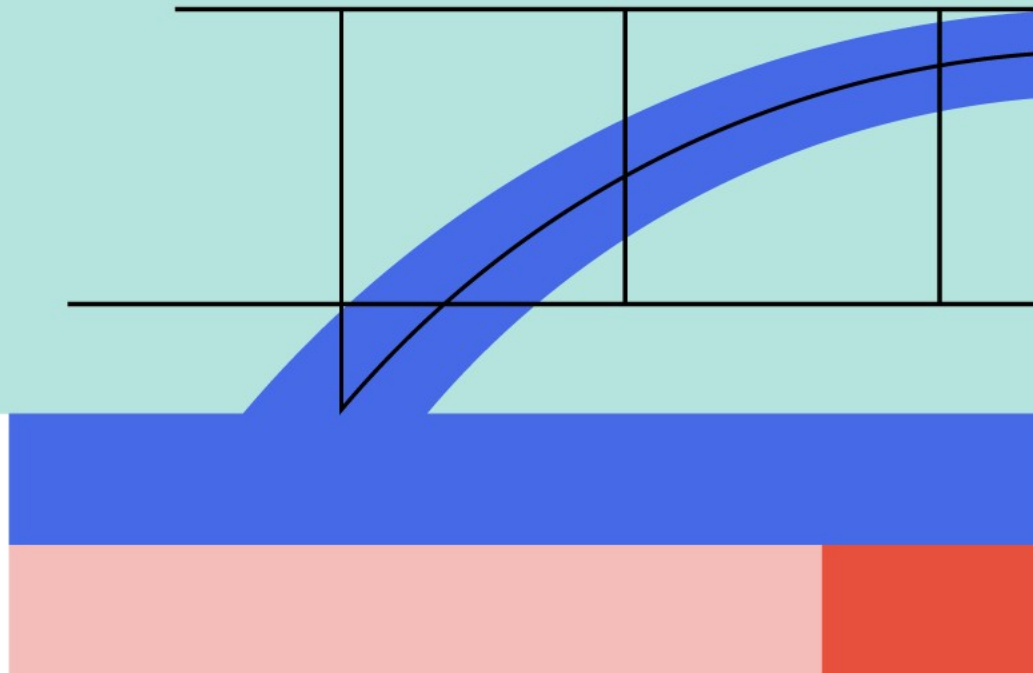


FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

jornadas FCCN

Agenda

- Cyber Ranges
- Ludus
  - Componentes
  - Implementação
  - Templates
  - Ranges
  - Benefícios
  - Limitações
- Ludus 2



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

Cyber Ranges

- Cyber Ranges são ambientes controlados e isolados que simulam infraestruturas reais de IT, utilizados para treino, testes e simulação de cenários de cibersegurança.

- São essenciais para que as equipas de cibersegurança pratiquem a resposta a desafios cibernéticos, sem o risco de causar impacto em sistemas em produção.

- Podem também ser utilizados para testar e validar provas de conceito (POCs).

jornadas FCCN

- O Ludus Cyber Range é uma plataforma que permite criar, gerir e automatizar cyber ranges, ou seja, ambientes de cibersegurança simulados para treino e testes.

- Facilita a implementação de infraestruturas completas (máquinas, redes e serviços) de forma automatizada, isolada e segura, permitindo reproduzir cenários realistas de ataque e defesa.

- Desenvolvido pela Bad Sector Labs, o Ludus surgiu da identificação de uma necessidade recorrente de uma forma mais flexível e automatizada de construir laboratórios de testes.

Componentes

Proxmox VE é uma plataforma de virtualização que permite gerir máquinas virtuais e containers através de uma interface web, sendo baseada em Debian e nas tecnologias KVM e LXC.

Ansible é uma ferramenta de automação que permite configurar sistemas, gerir infraestruturas e automatizar tarefas de forma simples e declarativa, através de playbooks em YAML e SSH.

HashiCorp Packer é uma ferramenta usada para criar imagens de máquinas de forma automatizada e consistente, como templates para máquinas virtuais, cloud ou containers. Permite definir um processo único que gera imagens prontas a usar, garantindo uniformidade entre ambientes.

Implementação

- Fornece documentação para a implementação da solução em seis infraestruturas diferentes:
  - Azure, Google Cloud Platform (GCP), Proxmox, bare metal, Hyper-V e VMware Fusion.
- Suporta apenas dois métodos de instalação: Debian 12/13 (recomendado) ou Proxmox 8/9.
- Fornece um script de instalação que automatiza o processo. Os ficheiros de configuração encontram-se disponíveis em /opt/ludus.
- Durante o processo de instalação, é criado um utilizador com permissões para criar e gerir Ranges.

Templates

- Inclui 5 templates integrados:
  - Debian 11 e 12, Kali, Windows 11 22h2 Enterprise e Windows Server 2022.
- No repositório oficial do Ludus, encontram-se presentes templates adicionais. Estes incluem:
  - Debian 10, Rocky 9, Ubuntu Server 20.04 e 22.04, Windows 10 21h1 Enterprise, Windows 11 23h2 Enterprise, Windows Server 2012r2, Windows server 2016, Windows server 2019, CommandoVM, Flare-VM e Remnux.
- Suporta a criação de templates customizados.

Ranges

- As Ranges são criadas via Ludus CLI (cliente). Requer um ficheiro de configuração YAML, onde se encontra definida a Range.
- As ranges funcionam com base em pools do Proxmox.
- Para cada Range é criada uma VM (Router), que fornece rede privada e acesso remoto via WireGuard.
- As Ranges podem ser configuradas para utilizar redes em produção, sendo necessário garantir que o Proxmox tem acesso a essa rede.

Ranges

```
user@ludus:~$ export LUDUS_API_KEY='JD._7Gx2T5kTUSD%uTWZ*lFi=Os6MpFR^OrG+yT94Xt'
```

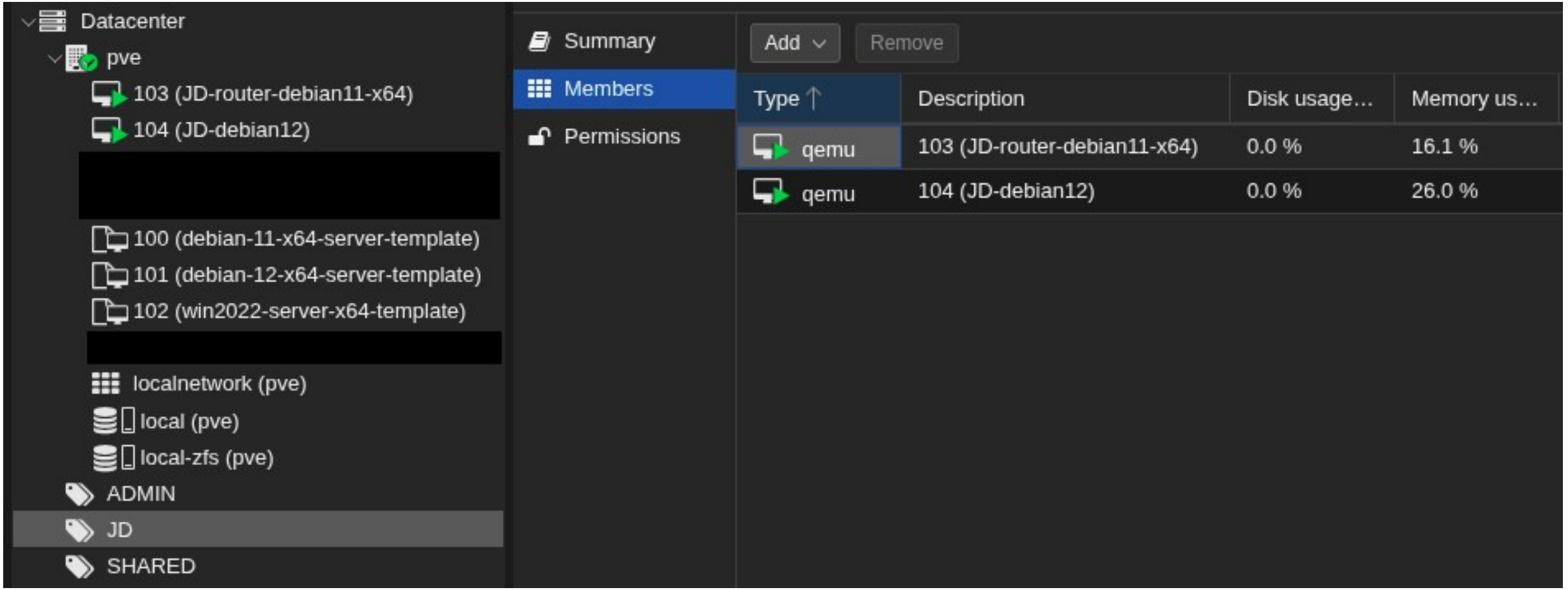
```
root@pve:~# ludus range config get
# yaml-language-server: $schema=https://docs.ludus.cloud/schemas/range-config.json
ludus:
  - vm_name: "{{ range_id }}-debian12"
    hostname: "{{ range_id }}-debian12"
    template: SecGen-setuid-pwnable-binary-example-reverse-mes
    full_clone: true
    vlan: 10
    ip_last_octet: 11
    ram_gb: 4
    cpus: 2
    linux: true
    testing:
      snapshot: false
      block_internet: false

  - vm_name: "{{ range_id }}-kali"
    hostname: "{{ range_id }}-kali"
    template: kali-s
    full_clone: true
    vlan: 10
    ip_last_octet: 12
    force_ip: true
    ram_gb: 4
    cpus: 4
    linux: true
    testing:
      snapshot: false
      block_internet: false

network:
  external_default: ACCEPT
  inter_vlan_default: REJECT
  rules: []
```

Ranges

```
user@ludus:~$ ludus range deploy
[INFO]  range deploy started
```

```
user@ludus:~$ ludus range status
+---------+---------------+------------------+---------------+--------------------+------------------+
| USER ID | RANGE NETWORK | LAST DEPLOYMENT  | NUMBER OF VMS | DEPLOYMENT STATUS | TESTING ENABLED |
+---------+---------------+------------------+---------------+--------------------+------------------+
|   JD    |  10.2.0.0/16  | 2023-12-31 18:42 |       4       |      SUCCESS       |      FALSE       |
+---------+---------------+------------------+---------------+--------------------+------------------+
+------------+-------------------------------------+-------+-------------+
| PROXMOX ID |               VM NAME               | POWER |     IP      |
+------------+-------------------------------------+-------+-------------+
|    107     | JD-router-debian11-x64              |  On   | 10.2.10.254 |
|    109     | JD-ad-dc-win2019-server-x64         |  On   | 10.2.10.11  |
|    113     | JD-ad-win11-22h2-enterprise-x64-1 |  On   | 10.2.10.21  |
|    114     | JD-kali                             |  On   | 10.2.99.1   |
+------------+-------------------------------------+-------+-------------+
```

Ranges


Datacenter
pve
103 (JD-router-debian11-x64)
104 (JD-debian12)
100 (debian-11-x64-server-template)
101 (debian-12-x64-server-template)
102 (win2022-server-x64-template)
localnetwork (pve)
local (pve)
local-zfs (pve)
ADMIN
JD
SHARED
Summary
Members
Permissions
Add
Remove
Type
Description
Disk usage…
Memory us…
qemu
103 (JD-router-debian11-x64)
0.0 %
16.1 %
qemu
104 (JD-debian12)
0.0 %
26.0 %

Benefícios

- Open Source.
- Fácil de implementar.
- Boa documentação e suporte.
- Fácil criar ou modificar Templates.
- Maquinas podem ser adicionadas as Ranges, sem recorrer a Templates.
- Gestão intuitiva via Ludus CLI ou interface web do Proxmox.

Limitações

- Ranges estão associadas a utilizadores, sendo necessário criar utilizadores adicionais para ter múltiplas ranges ativas.
- Para utilizar a VPN nativa, é necessário que o Proxmox tenha acesso a uma interface, VLAN ou IP público, ou configurar regras de NAT, dependendo da infraestrutura.

Ludus 2

- A Bad Sector Labs lançou recentemente a versão 2 do Ludus.
- Inclui melhorias na arquitetura e documentação, reforço da segurança da API e melhorias na gestão de redes.
- Mitigou a limitação das Ranges, sendo agora possível um único utilizador criar e gerir múltiplas Ranges.

Referencias

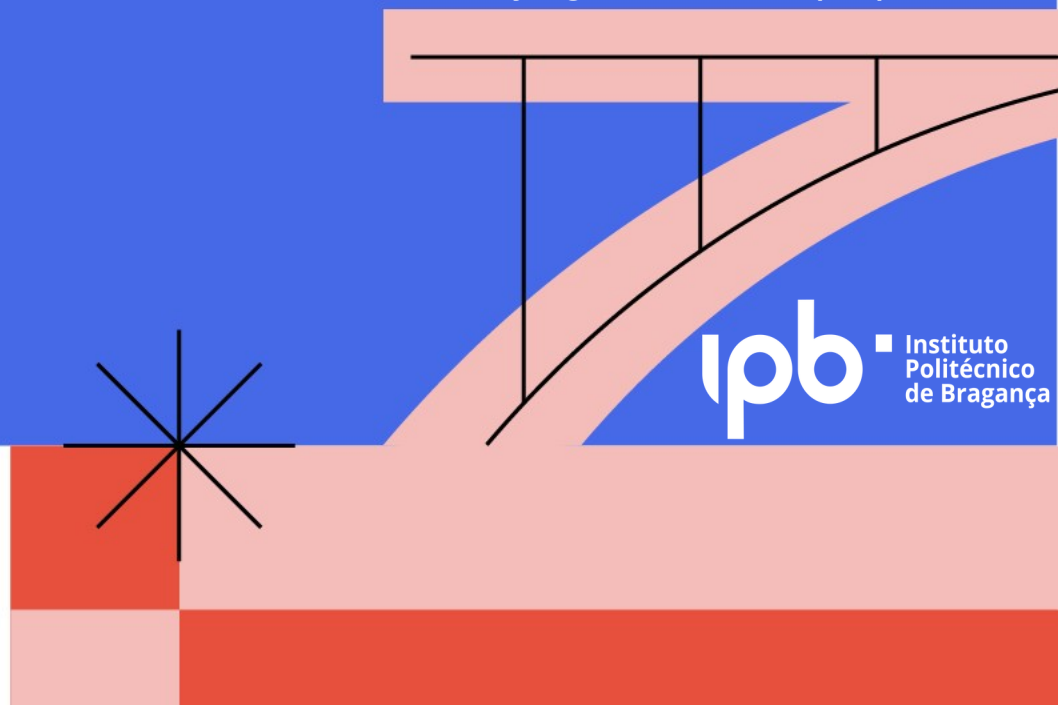
- Website oficial: https://ludus.cloud/
- Gitlab: https://gitlab.com/badsectorlabs/ludus
- Documentação: https://docs.ludus.cloud/docs/intro/

jornadas FCCN

Obrigado!

jornadas.fccn.pt | fccn.pt

Jorge Loureiro
jorge.loureiro@ipb.pt



ipb Instituto Politécnico de Bragança

FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO