Relatório de aprovisionamento do cenário da Unidade Curricular de Infraestruturas Seguras

Data	Versão	Autor	Observações
04/05/2025	1.0	Tiago Cruz (tjcruz@dei.uc.pt)	Versão inicial
23/05/2025	1.1	Tiago Cruz (tjcruz@dei.uc.pt)	Correção do diagrama da topologia

A infraestrutura de suporte à unidade curricular de Infraestruturas Seguras assenta num cenário simples, composto por 5 VMs que suportam o contexto de trabalho + 1 VM por cada grupo/aluno (o número a aprovisionar dependerá dos recursos disponíveis). O cenário encontra-se ilustrado na próxima figura:

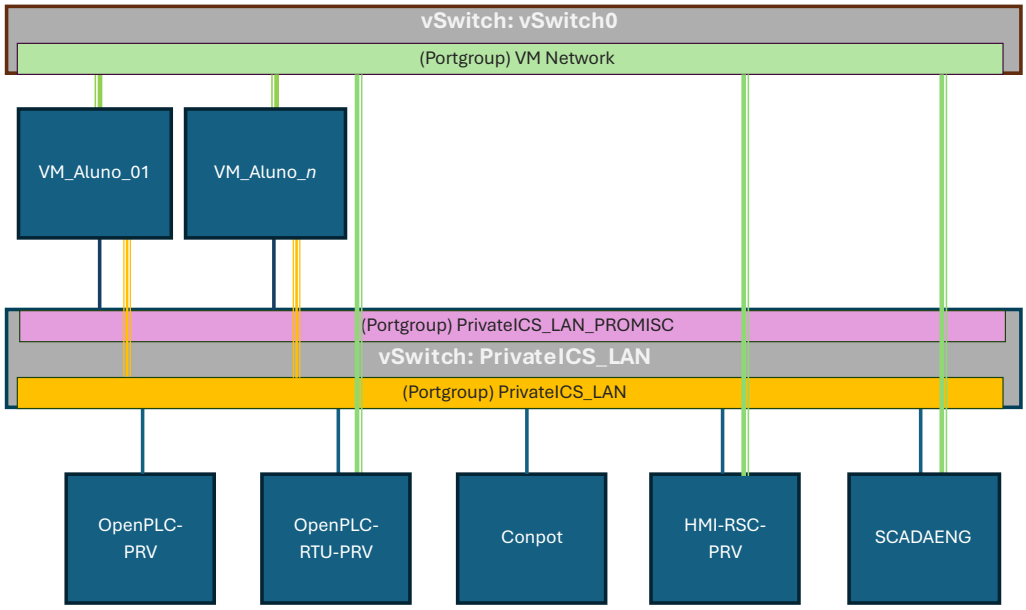

Figura 1 - Arquitetura do cenário

1. Configurações de rede

O cenário inclui um *vSwitch* privado onde estará ligado o cenário de testes/trabalho (PrivateICS_LAN). Este *vSwitch* tem de estar configurado para aceitar *Forged transmits* e *MAC changes*, nos seus parâmetros de segurança, não possuindo nenhum uplink (trata-se portanto de um *vSwitch* isolado). Este *vSwitch* inclui ainda 2 *portgroups*:

- O *PrivateICS_LAN*, que hospeda a LAN do cenário (todas as VM devem ter uma interface lá) e herdará a configurações de segurança do *vSwitch* que o hospeda (ver Figura 2). A gama utilizada nesta rede é a 172.27.224.0/24.
- O *PrivateICS_LAN_PROMISC*, que será adicionalmente configurado com a opção *Allow promiscuous mode* (ver Figura 3). Este último *portgroup* foi criado para permitir que todas as VMs dos alunos tenham uma terceira interface com acesso a um *mirror* de todo o tráfego da rede de ensaios, para teste da instalação de um IDS em modo passivo. Nenhuma interface nesta VM deverá ter IP configurado.

Adicionalmente, o *vSwitch0* (*vSwitch* por defeito) irá hospedar o porgroup *VM Nework* – todas as VMs com acesso à LAN da UNICV deverão ter uma interface neste *portgroup*.

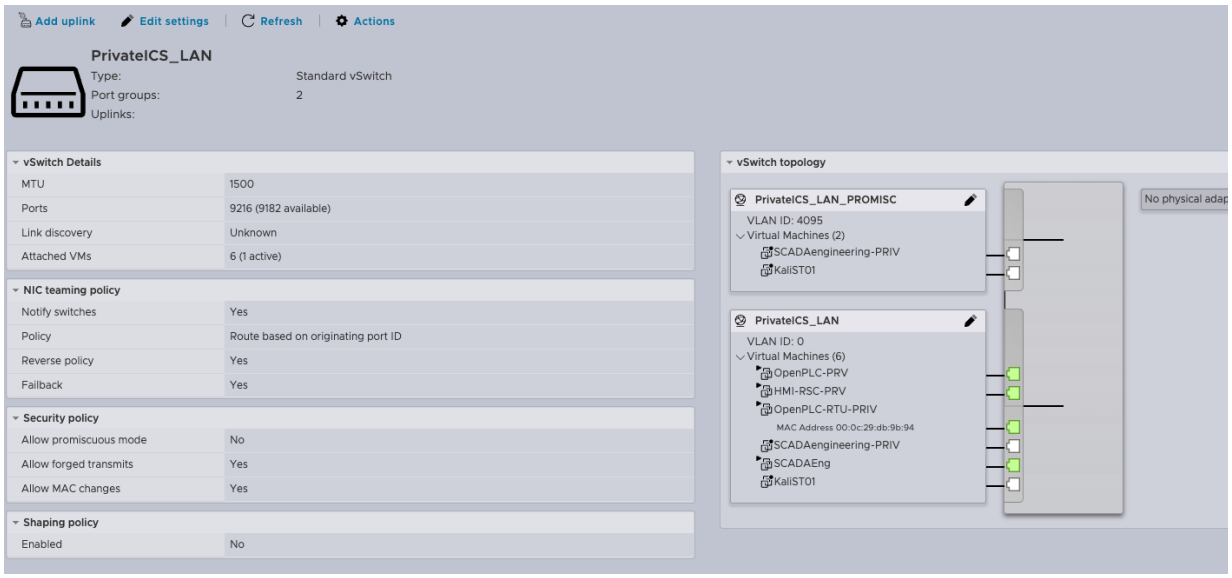

Figura 2 - Configuração do portgroup PrivateICS_LAN

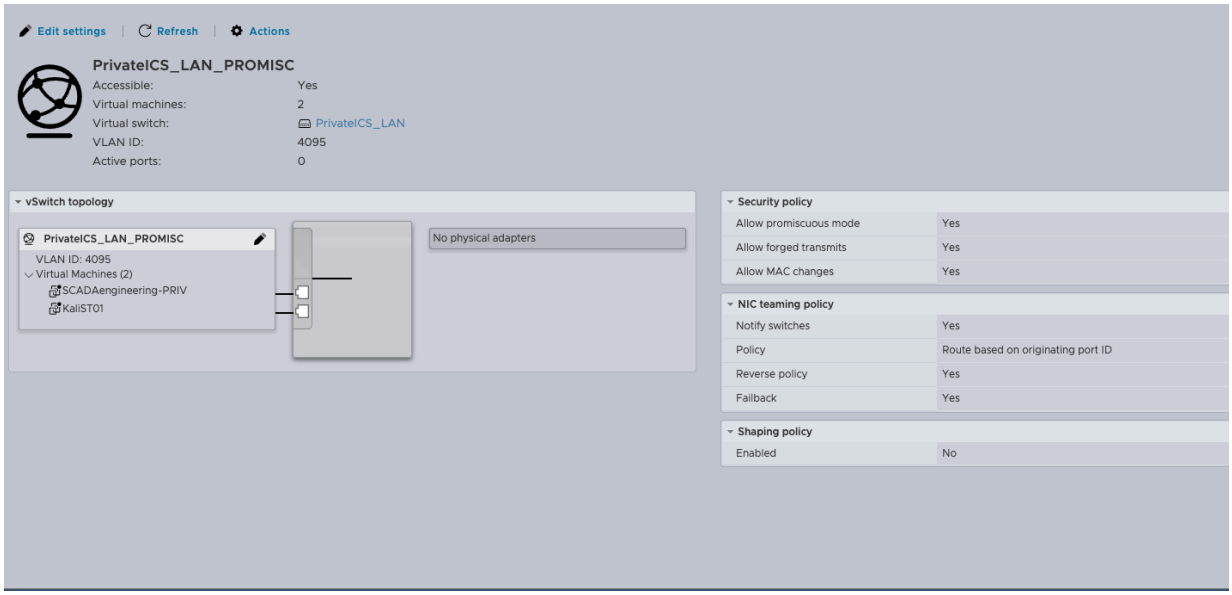

Figura 3 - Configuração do portgroup PrivateICS_LAN_PROMISC

2. Propriedades das VMs

As VMs do cenário encontram-se esquematizadas na parte inferior da Figura 1. Todas estão ligadas ao *portgroup PrivateICS_LAN*, sendo que duas possuem também uma interface no *portgroup VM Network*.

As VMs dos Alunos terão sempre 3 interfaces: uma na rede da UNICV (portgroup *VM Nework*), uma na rede do cenário (*portgroup PrivateICS_LAN*) e outra no *portgroup* do modo promíscuo (*PrivateICS_LAN_PROMISC*).

Todas as VMs são importadas a partir das imagens proporcionadas com o nome correspondente, sendo que as VMs dos alunos serão cópias da VM *KaliST01.ova*.

3. Importação das VMs

As VMs foram importadas usando a ferramenta *ovftool* da VMware, com as seguintes opções:

SCADAENG:

```
./ovftool --noSSLVerify --name="SCADAENG" --datastore="datastore1" --net:"VM Network=VM Network" --net:"PrivateICS_LAN=PrivateICS_LAN" --net:"PrivateICS_LAN_PROMISC=PrivateICS_LAN_PROMISC" --diskMode=thin ../IMAGES/SCADAengineering-PRIV.ova "vi://172.16.16.200"
```

HMI-RSC-PRV:

```
./ovftool --noSSLVerify --name="HMI-RSC-PRV" --datastore="datastore1" --net:"VM Network=VM Network" --net:"PrivateICS_LAN=PrivateICS_LAN" --diskMode=thin ../IMAGES/HMI-RSC-PRV.ova "vi://172.16.16.200"
```

OpenPLC-PRV:

```
./ovftool --noSSLVerify --name="OpenPLC-PRV" --datastore="datastore1" --net:"VM Network=VM Network" --net:"PrivateICS_LAN=PrivateICS_LAN" --diskMode=thin  ../IMAGES/OpenPLC_PRV.ova "vi://172.16.16.200"
```

OpenPLC-RTU-PRV:

```
./ovftool --noSSLVerify --name="OpenPLC-RTU-PRV" --datastore="datastore1" --net:"VM Network=VM Network" --net:"PrivateICS_LAN=PrivateICS_LAN" --diskMode=thin ../IMAGES/OpenPLC-RTU-PRIV.ova "vi://172.16.16.200"
```

Conpot:

```
./ovftool --noSSLVerify --name="Conpot" --datastore="datastore1" --net:"PrivateICS_LAN=PrivateICS_LAN" --diskMode=thin  ../IMAGES/Conpot.ova "vi://172.16.16.200"
```

KaliST01:

```
./ovftool --noSSLVerify --name="KaliST01" --datastore="datastore1" --net:"VM Network=VM Network" --net:"PrivateICS_LAN=PrivateICS_LAN" --net:"PrivateICS_LAN_PROMISC=PrivateICS_LAN_PROMISC" --diskMode=thin ../IMAGES/KaliST01.ova "vi://172.16.16.200"
```

Todas as linhas de comando incluem as instruções para mapear os *portgroups* originais nos *portgroups* de destino utilizados no servidor ESXi configurado na UNICV.

4. Credenciais das VMs

VM	**User**	**Password**
Conpot	`unicvadm`	`Unicv%25`
OpenPLC-RTU-PRV	`unicvadm`	`Unicv%25`
OpenPLC-PRV	`unicvadm`	`unicvadm`
SCADAENG	`unicvadm`	`Unicvadm`
HMI-RSC-PRV	`x`	`cdis0000!`
VMs dos alunos (KaliST01)	`unicvst`	**`UnicvST#33`**

No caso das VMs dos alunos (criadas por cópia a partir da KaliST01), sugere-se a mudança de credenciais depois de atribuídas as VMs.

Acesso consola web do Open PLC (http://172.27.224.250:8080)

`user: openplcAdmin`	**`pass: Unicv%25`**

5. Inicialização do cenário

Todas as VMs inicializam os serviços automaticamente aquando do seu arranque, com a exceção da VM *OpenPLC-RTU-PRV*. No caso desta, o procedimento de inicialização é simples:

1. abrir uma sessão no terminal gráfico, para o user *unicvadm*
2. abrir um terminal e arrancar o script *./init.sh* (ver Figura 4)
3. se tudo correr como esperado, o script irá provocar a execução de uma instância de browser Web com uma interface simples que controla as temperaturas no cenário simulado
4. para sair bastará deixar a sessão do utilizador bloqueada (não fazer *logoff*)

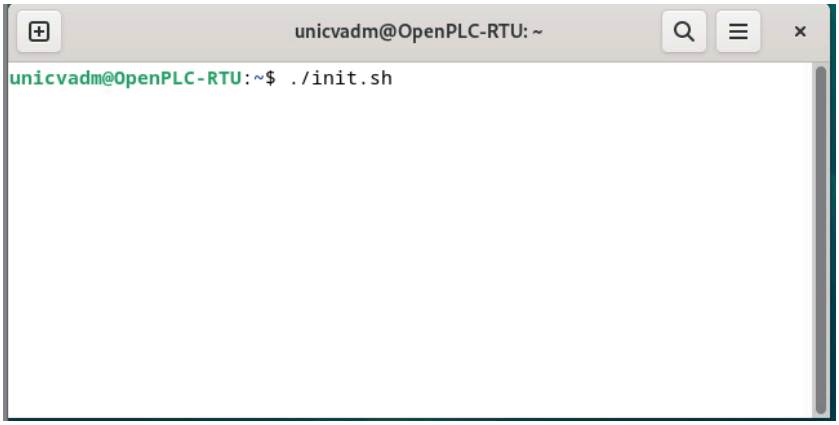

Figura 4 - Script de inicialização para a VM OpenPLC-RTU-PRV

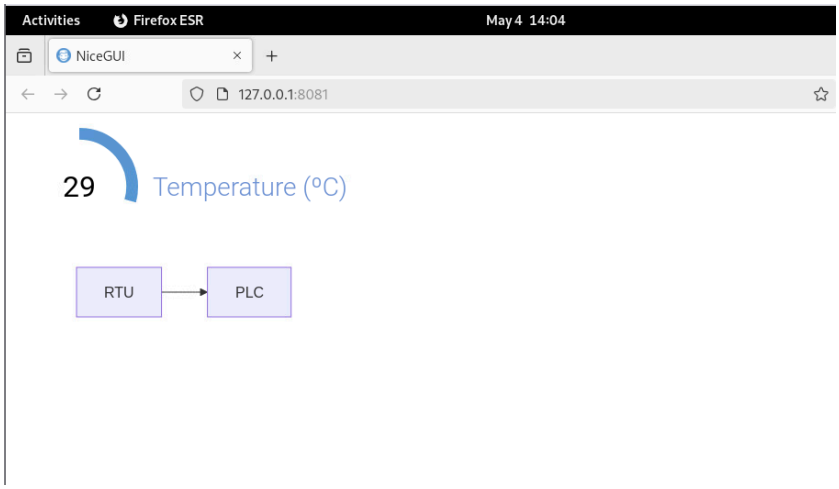

Figura 5 - Interface de operação da VM OpenPLC-RTU-PRV

6. Sugestões de âmbito operacional

No início da unidade curricular, é aconselhado fazer snapshot ao estado inicial das VMs do cenário de testes, de modo a poder recuperar de quaisquer danos infligidos pelos alunos.

Adicionalmente, tem sido hábito criar um utilizador no ESXi para os alunos (*unicvst*), com um *role* específico associado, de modo a que os alunos apenas vejam as VMs dos alunos e não as do cenário. As configurações do role são as seguintes:

Figura 6 - Configurações do role para os alunos

Na sequência deste ajuste, todas as VMs dos alunos são configuradas com as seguintes permissões:

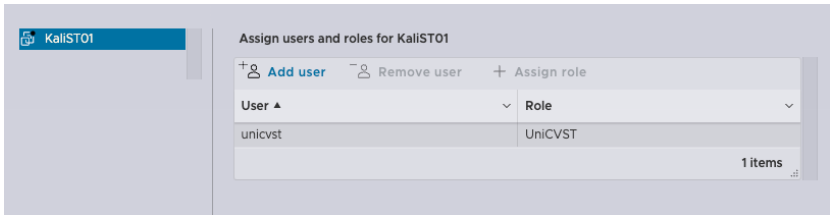

Figura 7 - Permissões para as VMs dos alunos

Deste modo, ao entrarem no ESXi os alunos apenas irão ver as VMs de aluno, ficando as restantes ocultas.

Finalmente, a VM *SCADAENG* deverá ser mantida desligada, visto apenas existir para programação do autómato (PLC – Programmable Logic Controller) emulado na VM *OpenPLC-PRV.*