User Stories

US 1. Como administrador do sistema quero que o deployment de um dos módulos do RFP numa VM do DEI seja sistemático, validando de forma agendada com o plano de testes.

Clone script

```
#!/bin/bash

GREEN='\033[0;32m'
YELLOW='\033[1;33m'
NC='\033[0m'

echo -e "\n${YELLOW}cd /home/asist/${NC}"
cd /home/asist/

echo -e "\n${YELLOW}git clone${NC}\n"
git clone
https://x-token-auth:LVgy4UfvZZB93qMBn8po@bitbucket.org/hhacarvalho/spa-g70-2022.git

echo -e "\n${YELLOW}cd spa-g70-2022/${NC}"
cd spa-g70-2022/

echo -e "\n${YELLOW}npm install${NC}\n"
npm install

echo -e "\n${GREEN}Clone complete.${NC}\n"
```

- Mudamos de diretório para a pasta do user *asist*;
- Clonamos o repositório
- Mudamos de diretório para a pasta do módulo SPA;
- Instalamos as bibliotecas.

Deployment script

```
#!/bin/bash

GREEN='\033[0;32m'
YELLOW='\033[1;33m'
NC='\033[0m'

echo -e "\n${GREEN}Closing application...${NC}\n"
fuser -k 4200/tcp

echo -e "\n${YELLOW}cd /home/asist/spa-g70-2022/${NC}"
cd /home/asist/spa-g70-2022/

echo -e "\n${YELLOW}git pull${NC}\n"
git pull

echo -e "\n${YELLOW}npm install${NC}\n"
npm install

echo -e "\n${YELLOW}npm test${NC}\n"
npm test

echo -e "\n${YELLOW}ng serve --host 0.0.0.0${NC}\n"
ng serve --host 0.0.0.0
```

- Começamos por desligar a aplicação;
- Mudamos de diretório para a pasta do módulo SPA;
- Damos pull do projeto;
- Instalamos as bibliotecas caso existam novas;
- Executamos os testes;
- Iniciamos a aplicação.

Start script (Opcional)

```
#!/bin/bash

GREEN='\033[0;32m'
YELLOW='\033[1;33m'
NC='\033[0m'

echo -e "\n${YELLOW}cd /home/asist/spa-g70-2022/${NC}"
cd /home/asist/spa-g70-2022/

echo -e "\n${YELLOW}ng serve --host 0.0.0.0${NC}\n"
ng serve --host 0.0.0.0
```

- Mudamos de diretório para a pasta do módulo SPA;
- Iniciamos a aplicação.

Agendar o deploy:

- **nano /etc/crontab**

Adicionar a seguinte linha:

```
# [minute] [hours] [day of month] [month] [day of the week]

0 22 * * * root /bin/bash /home/asist/scripts/deploy.sh
```

Às 22:00, todos os dias (0 22 * * *) o script deploy.sh será executado.

US 2. Como administrador do sistema quero que apenas os clientes da rede interna do DEI (cablada ou via VPN) possam aceder à solução.

```
#!/bin/bash

# Flush rules
iptables -F

# Accept every connection
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT

# Block SAMBA for people outside the DEI ip range
iptables -A INPUT -p tcp --dport 445 -m iprange --src-range 0.0.0.0-10.8.0.0 -j DROP
iptables -A INPUT -p tcp --dport 445 -m iprange --src-range 10.9.255.255-255.255.255.255 -j DROP

# Block SPA port for everyone
iptables -A INPUT -p tcp --dport 4200 -j DROP

# Save rules
netfilter-persistent save
```

- Dá flush (apaga) as atuais regras;
- Aceita todas as conexões;
- Bloqueia a porta 445 (Samba) para todas as conexões com origem fora da rede do DEI;
- Bloqueia a porta 4200 por completo
- Guarda as alterações

US 3. Como administrador do sistema quero que os clientes indicados na user story anterior possam ser definidos pela simples alteração de um ficheiro de texto.

- **nano /etc/samba/smb.conf**

```
[asist]
        path = /home/asist/
        read only = no
        valid users = @sambaShare
        inherit permissions = yes
```

Com esta configuração estamos a partilhar a pasta /home/asist (path) onde é possível editar ficheiros (read only = no) e que apenas utilizadores que pertencem ao grupo “sambaShare” (valid users) podem aceder. As permissões dos ficheiros criados irão ser herdadas da pasta pai (inherit permissions).

Para criar um utilizador e definir a sua password na base de dados do samba:

- **smbpasswd -a asist** (O utilizador tem de existir no sistema)

Para remover um utilizador da base de dados do samba:

- **smbpasswd -x asist**

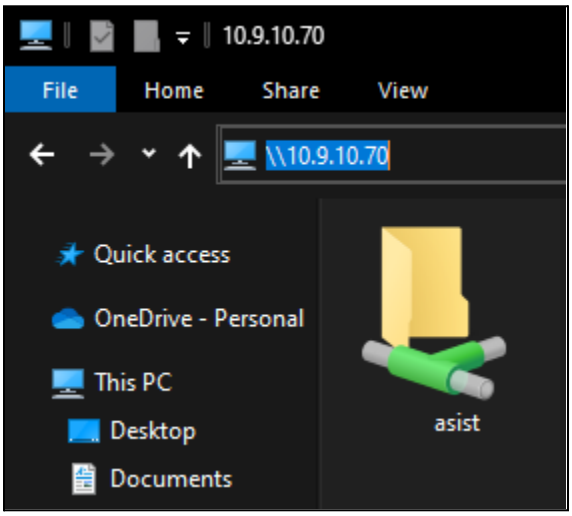
Criar um grupo no sistema:

- **Groupadd sambaShare**

Adicionar utilizador ao grupo:

- **usermod -a -G sambashare asist**

Para testar a ligação abre-se uma janela do windows explorer e introduz se o IP da máquina linux:



Foi também criado o seguinte script para ler o conteúdo do ficheiro "/home/asist/allow.txt" que irá conter os IPs dos utilizadores que poderão aceder à página do projeto SPA cujo deploy foi realizado na US 1.

```
#!/bin/bash

# Reset rules
/home/asist/scripts/ip_rules.sh

# Add the IPs included in the file
file="/home/asist/allow.txt"

while read -r ip
do
  echo "Added $ip to the expection list."
  iptables -I INPUT -p tcp --dport 4200 -s $ip -j ACCEPT
done < "$file"
```

O ficheiro é lido linha a linha, em que cada linha contém um ip, e esse ip é adicionado como exceção através do comando “iptables”.

Agendar a atualização dos IPs:

- **nano /etc/crontab**

Adicionar a seguinte linha:

```
# [minute] [hours] [day of month] [month] [day of the week]

* * * * * root /bin/bash /home/asist/scripts/update_rules.sh
```

A cada minuto (* * * * *) o script update_rules.sh será executado.

US 4. Como administrador quero identificar e quantificar os riscos envolvidos na solução preconizada

A solução preconizada não é a solução ideal e tem alguns riscos associados, isto porque, estamos a pôr algo que devia ser acedido apenas pelo root (administrador) numa partilha semi-privada, esta solução permite de certa forma “trapacear”, e isto não é correto. Alguns erros associados à solução são:

- Ter um comando que corre em root a ir buscar um ficheiro partilhado por um grupo de pessoas;
- Há grande probabilidade de alguém se enganar ao realizar as configurações;
- Podem acontecer erros de crontab e por consequência o ficheiro que está a ser editado, quando gravado, pode não conseguir ter acesso;
- Se o ficheiro for criado em windows (crlf) o linux(lf) não o conseguirá ler;
- Na US 2 não é ideal permitir o acesso a todas as portas;
- O script de deploy só funciona se o repositório do projeto já estiver clonado;
- Podem ocorrer falhas de segurança;
- Ataques informáticos;
- Falhas de hardware, de rede e elétricas;
- As aplicações que usamos, no nosso caso apenas o SPA, e as bases de dados podem falhar.

Das situações mencionadas, as mais prováveis de acontecer são as falhas nas aplicações e os erros provocados por enganos.

Nas situações mais críticas inserem-se, a da criação do ficheiro em windows que por consequência o linux não irá conseguir ler, os ataques informáticos e as falhas de hardware, rede e elétricas.