

Uma imagem com alimentação

Descrição gerada automaticamente

**Relatório de ASIST**

**SPRINT 2**

**Turma 3DGH \_ Grupo 02**

1191008 Rodrigo Rodrigues

1201564 Jorge Ferreira

1201566 Rafael Leite

1201568 Rui Pina

**Data: 01/12/2022**

Índice

[**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 - 1201568 3**](#_Toc121060854)

[**2. Como administrador do sistema quero que apenas os clientes da rede interna do DEI (cablada ou via VPN) possam aceder à solução. - 1201564 4**](#_Toc121060855)

[**3. Como administrador do sistema quero que os clientes indicados na US 2 possam ser definidos pela simples alteração de um ficheiro de texto. - 1201566 5**](#_Toc121060856)

[**4. Como administrador quero identificar e quantificar os riscos envolvidos na solução preconizada. -1191008 6**](#_Toc121060857)

## 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 - 1201568

A cada commit feito, o repositório corre a pipeline definida no ficheiro bitbucket-pipelines.yml.

Uma imagem com texto

Descrição gerada automaticamente

Isto, faz uma ligação ssh na porta 10367, porta pública de ssh da máquina virtual do DEI, e entra como root através de uma public key authentication, definida no ficheiro ~/.ssh/authorized\_keys. Sendo que pusemos a public key que geramos no bitbucket dentro deste ficheiro.



Uma imagem com texto

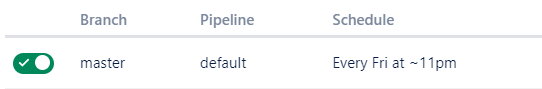
Descrição gerada automaticamenteDepois da conexão ser feita corremos os comandos que estão definidos no ficheiro lei\_22\_23\_s5\_3dh\_046/deploy.sh:

Entramos no ficheiro que tem o repositório e fazemos pull através do uso do sshpass, que foi instalado na máquina virtual e passamos a password de uma conta que foi criada especificamente para este deployment. Esta solução parece-nos vulnerável e, portanto, seria uma boa ideia melhorá-la através de outro método de dar pull.

Após isso instalamos as dependências do Node, que podem ter sido mudadas e damos start ao programa através do comando npm start e o módulo e as suas endpoints já ficam disponíveis no url <https://vs367:3000>, apenas para redes do DEI.

Para fazermos isto de forma sistemática, o Bitbucket habilita a funcionalidade de scheduling que implementa o Crontab. No nosso caso, caso fossemos fazer manualmente seria facilmente feito com o comando **crontab -e,** que após abrir o ficheiro de configuração, poríamos, na notação cron, 0 23 \* \* FRI /lei22\_23\_s5\_3dh\_046/deploy.sh

Escolhemos apenas fazer na sexta-feira, por motivos de poupança de tempo de execução de pipelines e por representar o fim da semana de trabalho. Poderia ser qualquer outra cadência a escolher.



## 2**. Como administrador do sistema quero que apenas os clientes da rede interna do DEI (cablada ou via VPN) possam aceder à solução. - 1201564**

Como na US anterior o deployment é realizado numa máquina virtual do DEI, apenas é possível aceder à solução se estivermos ligados à VPN do DEI, porém é necessário usarmos o comando iptables e inserimos regras para gerir a permissão de acesso à solução.

O deployment da User Storie anterior foi realizado na porta 3000, daí as regras serem aplicadas a essa porta, de forma a gerir esse acesso.

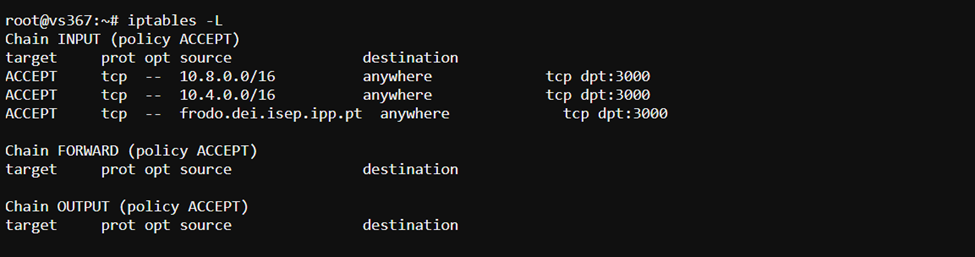
• Fornece acesso ao intervalo de IPs 10.8.0.0/16 (Rede dos Laboratórios).

• Engloba todos os espaços do DEI que estão livremente acessíveis aos alunos.



• Fornece acesso ao intervalo de IPs 10.4.0.0/16 (Rede dos Gabinetes).

• Engloba todos os restantes espaços do DEI.

* Fornece acesso ao DNS em vez dos IPs, como nas duas anteriores.

• Lista com as regras iptables atuais.

## 3. Como administrador do sistema quero que os clientes indicados na US 2 possam ser definidos pela simples alteração de um ficheiro de texto. - 1201566

É possível guardar as regras definidas na US anterior num ficheiro de texto, e caso necessário, podemos alterá-lo e de seguida aplicar as regras desse mesmo ficheiro.

• Cria um ficheiro de texto chamado iptableslist.

****• Guarda as regras iptables atuais no ficheiro de texto criado, e caso necessário, podemos alterá-las neste ficheiro com o comando nano.

• Restaura as regras iptables atuais, que serão agora o conteúdo do ficheiro iptableslist.txt.

Uma imagem com texto

Descrição gerada automaticamente

• Ficheiro de Texto com regras iptables após iptables-save -> iptableslist.txt. Pode ser alterado de acordo com os nossos desejos.

## 4. Como administrador quero identificar e quantificar os riscos envolvidos na solução preconizada. -1191008

Para tal, recorremos a uma matriz de risco para nos ajudar a não só quantificar como avaliar os potenciais riscos na solução.

Numa matriz de risco, cada item tem associado um impacto e uma probabilidade estimado, sendo que o valor do risco é obtido através do produto dos mesmos. Para tal usamos uma escala de 1 a 5 para ambas as escalas; sendo que: o impacto no valor 1 seria negligente; o impacto no valor 5 seria catastrófico; a probabilidade no valor 1 seria improvável; e a probabilidade no valor 5 seria muito frequente.

* Sendo assim, a tabela de riscos obtida foi esta:

Uma imagem com mesa

Descrição gerada automaticamente

* A partir desta tabela conseguimos obter a seguinte matriz de risco:

