

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
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
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
4. Como administrador quero identificar e quantificar os riscos envolvidos na solução preconizada. - 1191008.....	6

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

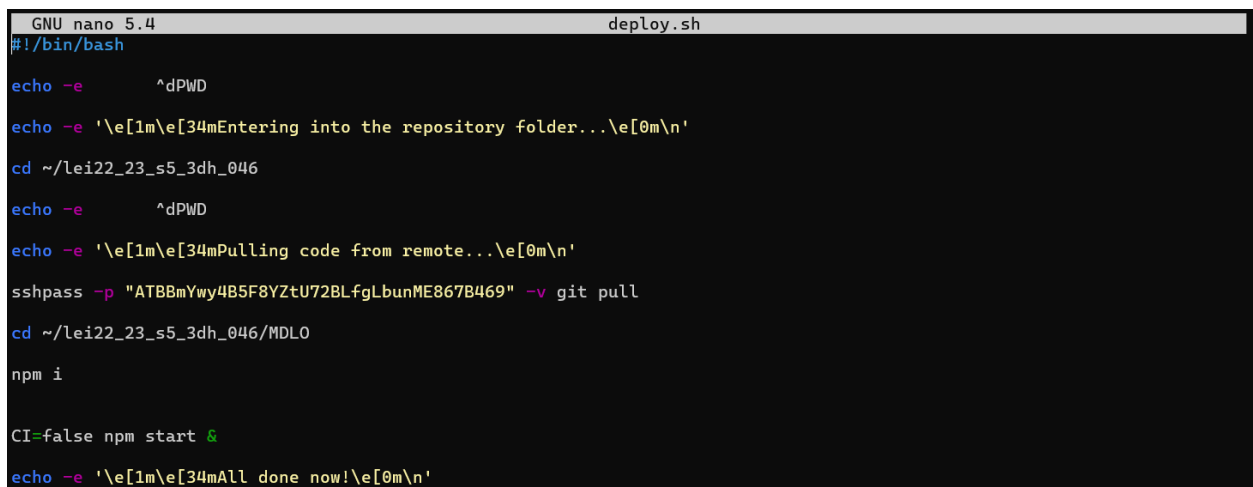
A cada commit feito, o repositório corre a pipeline definida no ficheiro bitbucket-pipelines.yml.

```
- step:
  name: Deploy to production
  deployment: production
  script:
    - echo "Deploying to production environment"
    - pipe: atlassian/ssh-run:0.2.2
      variables:
        PORT: '10367'
        SSH_USER: 'root'
        SERVER: 'vsgate-ssh.dei.isep.ipp.pt'
        COMMAND: 'lei22_23_s5_3dh_046/deploy.sh'
```

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.



Depois 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.

	Branch	Pipeline	Schedule
	master	default	Every Fri at ~11pm

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 Storrie anterior foi realizado na porta 3000, daí as regras serem aplicadas a essa porta, de forma a gerir esse acesso.

```
iptables -A INPUT -p tcp -s 10.8.0.0/16 --dport 3000 -j ACCEPT
```

- 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.

```
iptables -A INPUT -p tcp -s 10.4.0.0/16 --dport 3000 -j ACCEPT
```

- Fornece acesso ao intervalo de IPs 10.4.0.0/16 (Rede dos Gabinetes).
- Engloba todos os restantes espaços do DEI.

```
iptables -A INPUT -p tcp -s dei.isep.ipp.pt --dport 3000 -j ACCEPT
```

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

```
root@vs367:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination          tcp dpt:3000
ACCEPT     tcp  --  10.8.0.0/16            anywhere             tcp dpt:3000
ACCEPT     tcp  --  10.4.0.0/16            anywhere             tcp dpt:3000
ACCEPT     tcp  --  frodo.dei.isep.ipp.pt anywhere             tcp dpt:3000

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

- 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.

```
touch iptableslist.txt
```

- Cria um ficheiro de texto chamado iptableslist.

```
iptables-save > iptableslist.txt
```

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

```
iptables-restore < iptableslist.txt
```

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

```
# Generated by iptables-save v1.8.7 on Fri Dec  2 14:39:35 2022
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -s 10.8.0.0/16 -p tcp -m tcp --dport 3000 -j ACCEPT
-A INPUT -s 10.4.0.0/16 -p tcp -m tcp --dport 3000 -j ACCEPT
-A INPUT -s 193.136.62.2/32 -p tcp -m tcp --dport 3000 -j ACCEPT
COMMIT
# Completed on Fri Dec  2 14:39:35 2022
# Generated by iptables-save v1.8.7 on Fri Dec  2 14:39:35 2022
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A PREROUTING -p tcp -m tcp --dport 2222 -j DNAT --to-destination :22
COMMIT
# Completed on Fri Dec  2 14:39:35 2022
```

- 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, recorreremos 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:

Risco	Probabilidade	Impacto	Nível de Risco
Interrupção ou atraso na resposta da Cloud do DEI torna os serviços/componentes lentos e/ou indisponíveis	3	3	9
Devido a um erro na lista de utilizadores autorizados, existem utilizadores não autorizados com acesso à aplicação	2	4	8
Devido a um erro na lista de utilizadores autorizados, existem utilizadores autorizados sem acesso à aplicação	1	2	2
Manutenção semanal à Cloud do DEI causa que os serviços fiquem indisponíveis	4	2	8
Falha na execução de um serviço, devido a um erro não testado	2	3	6
Falha na execução de um módulo	2	5	10

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

		Impacto				
Probabilidade	x	1	2	3	4	5
	5					
	4		1			
	3			1		
	2			1	1	1
	1		1			