

Relatório de ASIST

SPRINT B

JOÃO RODRIGUES (1210817) GABRIEL SILVA (1210808)
MATEUS FERNANDES (1210821) RICARDO VENÂNCIO
(1210828))

Índice

| | |
|----------------------------------|----|
| Índice de Figuras | 4 |
| Introdução..... | 5 |
| User Story 1..... | 6 |
| Requisitos..... | 6 |
| Esclarecimentos do cliente | 6 |
| Análise..... | 6 |
| Identificação do problema | 6 |
| Testes ao requisito..... | 6 |
| Desenho | 7 |
| Módulo Ideal..... | 7 |
| Deployment Automático..... | 7 |
| Plano de Testes | 7 |
| Notas..... | 7 |
| Logs | 7 |
| Workflow..... | 7 |
| User Story 2..... | 9 |
| Requisitos..... | 9 |
| Esclarecimentos do Cliente..... | 9 |
| Implementação | 9 |
| User Story 3..... | 11 |
| Requisitos..... | 11 |
| Implementação | 11 |
| User Story 4..... | 12 |
| Requisitos..... | 12 |

| | |
|---|----|
| Implementação | 12 |
| User Story 5 | 13 |
| Requisitos | 13 |
| Esclarecimentos do cliente | 13 |
| Análise | 14 |
| Recovery Point Objective | 14 |
| <i>Maximum Downtown Tolerable</i> | 15 |
| Desenho | 15 |
| Contexto do sistema | 15 |
| Criticidade dos dados | 15 |
| Custo da baixa do sistema | 15 |
| Tecnologias da infraestrutura | 16 |
| Conclusão | 16 |
| Cópia de segurança | 17 |
| Execução | 17 |
| Localização | 17 |
| User Story 6 | 18 |
| Requisitos | 18 |
| Objetivo | 18 |
| Problema | 18 |
| Resolução do Problema | 19 |
| Backup do Projeto | 19 |
| Backup da Base de Dados | 21 |
| User Story 7 | 22 |
| Requisitos | 22 |
| Esclarecimentos do cliente | 22 |
| Análise | 22 |

| | |
|---------------------------------|----|
| Implementação | 22 |
| User Story 8..... | 25 |
| Requisitos..... | 25 |
| Análise | 25 |
| Identificação do Problema | 25 |
| Resolução do Problema | 25 |
| Implementação | 25 |

Índice de Figuras

| | |
|--|----|
| Figura 1 - Workflow. | 8 |
| Figura 2 - Regras default na iptables. | 9 |
| Figura 3 - Configurações salvas iptables..... | 10 |
| Figura 4- Script rules.sh..... | 11 |
| Figura 5- Modelo de matriz de risco | 12 |
| Figura 6 - Informações a incluir no ficheiro smb.conf..... | 23 |
| Figura 7 - Conexão à máquina pretendida onde se encontra a pasta pública. | 24 |
| Figura 8 - Pasta public. | 24 |

Introdução

No presente relatório vamos apresentar o trabalho desenvolvido pelo grupo relativo à implementação das *User Stories* pretendidas para a unidade curricular de Administração de Sistemas. Será apresentada uma abordagem de como foram implementadas, bem como os respetivos desafios na realização.

Ao implementarmos uma melhor administração e segurança em Linux, permitimos que os administradores do sistema tenham um melhor controlo das ferramentas do sistema, bem como a facilidade de alteração de funcionalidades relacionadas com os utilizadores e o sistema operativo.

User Story 1

Requisitos

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

Esclarecimentos do cliente

Questão:

Could you clarify the user story 640: "As the system administrator I want the deployment of one of the RFP modules on a DEI VM to be systematic, validating in a scheduled manner with the test plan. (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)

Should I write request for proposal of one of the 'modules' of RoboDroneGo project or some of our virtual machine? What is the meaning module?

Resposta:

You should implement a way of automatically deploying one of the RFP modules on a DEI VM (to which you have access, regardless of whether it is VCenter3 or the DEI private cloud), taking into account the remaining part of the US: should the deployment take place every day or only when there are changes to the module?

Was the deployment successful? By "module" you should understand as any other component of LAPR5, connected to ALGAV, ARQSI, SGRAI.

Análise

Identificação do problema

Qual o módulo "ideal" para ser deployed para uma VM do DEI? Como implementar o "deployment automático"? O que é o plano de testes?

Testes ao requisito

É necessário existirem testes para verificar que a nova atualização cumpre com os requisitos mínimos para produção. Como tal, testes como **compilação**, **unidade** e **integração** são essenciais.

Desenho

Módulo Ideal

A equipa optou por escolher o módulo de front-end para dar o deployment automático para uma VM do DEI. É um módulo simples e fácil de configurar para correr corretamente.

Deployment Automático

Para a implementação do deployment automático, a equipa pensou num bash script que seria adicionado ao crontab do servidor para que conseguisse ser executado com uma frequência X.

Plano de Testes

O plano de testes vai consistir em 2 pontos:

Testes de compilação + runtime;

Testes de unidade + integração.

Testes de compilação + runtime vão perceber se a aplicação está com algum problema que leve a uma interrupção inesperada. Enquanto os testes de unidade + integração vão tentar verificar se as regras de negócio e os diferentes componentes isolados e integrados estão a ser seguidas e a funcionar devidamente.

Notas

Logs

Existe um ficheiro designado "audit_log.txt" que vai armazenar todas as informações de sucesso/insucesso ao longo de uma semana. Após esse tempo, é feito um *refresh* e apagado todo o conteúdo para não o sobrecarregar com informação "desnecessária".

Workflow

A aplicação vai seguir o workflow da seguinte figura (ponto inicial S0):

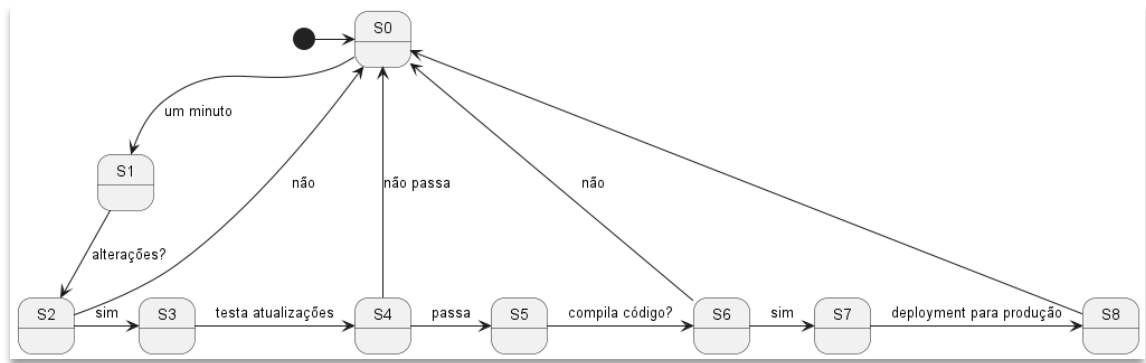


Figura 1 - Workflow.

A equipa optou por passar as novas atualizações do módulo escolhido para produção, apenas depois de garantir que nada "estragado" vai ser posto em produção, daí o passo intermédio de "compila código?"

Implementação do [script](#).

User Story 2

Requisitos

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

Esclarecimentos do Cliente

Questão:

Relativamente à US650, onde refere que pretende que apenas os clientes da rede interna do DEI (cabo ou VPN) acessem, tem já alguma gama de IP's pré-definida, ou devemos extrapolar?

Resposta:

Sempre que nos ligamos à rede interna do DEI (cabo ou VPN) obtemos um endereço atribuído dinamicamente por DHCP. A gama de endereços IP são todos esses. Duvido que tenha noção da gama completa, pelo que recomendo que para prova de conceito possa alterar o(s) endereço(s) a partir de um ficheiro de texto.

Implementação

Passo 1:

Para garantirmos que não existem nenhuma regras anteriores, limpamos as entries com o comando:

iptables -F

Ao fazer isto, o -F dá flush, eliminando todas as regras uma a uma. Se fizermos **iptables -S** verificamos que só ficaram as default:

```
root@vs857:/etc/iptables# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
```

Figura 2 - Regras default na iptables.

Passo 2:

Agora iremos bloquear o tráfego da porta 4200, que é a porta para a aplicação de “Node.js”. Para poder fazer isto, iremos executar o seguinte comando:

iptables -A INPUT -p tcp -destination-port 4200 -j DROP

- -A: Append, ou seja adicionar o “INPUT”, que toda a máquina recebe
- -p: serve para definir o protocolo, neste caso tcp
- -destination-port: a porta a que vamos aplicar, neste caso a 4200
- -j: comando que dá jump, neste caso ao DROP

Passo 3:

Como estas regras não são persistidas, temos de instalar o iptables persistence, através do comando:

sudo apt-get install iptables-persistence

Após a instalação, e de aceitar as regras para os ficheiros criados, o rules.v4 e o rules.v6

Passo 4:

Por último, salvamos com o comando iptables-save, para salvarmos as alterações realizadas:

```
root@vs857:/etc/iptables# iptables-save
# Generated by iptables-save v1.8.9 (nf_tables) on Sat Nov 25 23:57:05 2023
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -p tcp -m tcp --dport 4200 -j DROP
COMMIT
# Completed on Sat Nov 25 23:57:05 2023
```

Figura 3 - Configurações salvas iptables.

User Story 3

Requisitos

Como administrador do sistema quero que os clientes indicados na user story 2 possam ser definidos pela simples alteração de um ficheiro de texto.

Implementação

Passo 1

Criação do ficheiro de texto ips.txt na pasta /home e adicionar os ips que poderão aceder à solução.

Passo 2

Criação do script rules.sh e adicionar as regras necessárias ao iptables. Começamos por criar as variáveis utilizadas no script que serão: caminho para o iptables, porta usada na solução e o caminho para o ficheiro txt com os ips. Verificamos se o ficheiro de texto existe e lemos linha a linha. Para cada ip adicionamos a regra de permitir aceder a porta estipulada, no caso em estudo a 4200 que dará acesso ao módulo de front end. Posteriormente bloqueamos o acesso a qualquer outro utilizador que não esteja definido no ficheiro txt. A ordem das regras importa pois será necessário dar accept e posteriormente drop.

Passo 3

Atribuir permissão de executar através de chmod +x rules.sh.

Passo 4

Executar o script através do comando ./rules.sh.

```
#!/bin/bash

IPTABLES=/sbin/iptables
PORTA=4200
ALLOWED_IPS=/home/ips.txt

$IPTABLES -F

if [ -f "$ALLOWED_IPS" ]; then
    while read -r IP; do
        $IPTABLES -A INPUT -p tcp --dport $PORTA -s $IP -j ACCEPT
    done < "$ALLOWED_IPS"
    $IPTABLES -A INPUT -p tcp --destination-port $PORTA -j DROP
    echo "Regras atualizadas com IPs do ficheiro: $ALLOWED_IPS"
else
    echo "O arquivo $ALLOWED_IPS não foi encontrado"
fi
```

Figura 4- Script rules.sh

User Story 4

Requisitos

Como administrador do sistema quero identificar e quantificar os riscos envolvidos na solução preconizada.

Implementação

Baseando num modelo de matriz de risco.

| | | CONSEQUÊNCIA* | | | | |
|----------------------------|--------------------|--------------------|--------------|-----------------|--------------|----------------------|
| | | Desprezível (1) | Menor (2) | Moderada (4) | Maior (8) | Catastrófica (16) |
| PROBABILIDADE (frequência) | Quase Certo (5) | 5 | 10 | 20 | 40 | 80 |
| | Provável (4) | 4 | 8 | 16 | 32 | 64 |
| | Possível (3) | 3 | 6 | 12 | 24 | 48 |
| | Improvável (2) | 2 | 4 | 8 | 16 | 32 |
| | Raro (1) | 1 | 2 | 4 | 8 | 16 |

Figura 5- Modelo de matriz de risco

| Ameaça | Probabilidade | Consequência | Risco |
|--|---------------|--------------|-------|
| Desempenho da máquina | 3 | 2 | 6 |
| Perda de dados | 2 | 8 | 16 |
| Falha de Segurança | 2 | 16 | 32 |
| Falha da VM | 2 | 8 | 16 |
| Má utilização da VM | 3 | 8 | 24 |
| Requisitos não compreendidos por parte da equipa | 3 | 1 | 3 |

- Desempenho da máquina- Fraco desenvolvimento por parte da máquina, lentidão;
- Perda de dados- Irá ser feito um deployment para a máquina de dados importantes do projeto, uma ameaça será a perda desses mesmos dados.
- Falha de segurança- Tentativa de acesso por terceiros, membros não constituintes do grupo;
- Falha da VM- Devido à falha dos servidores do DEI;
- Má utilização da VM- Não conhecimento do funcionamento da VM por parte dos elementos do grupo;
- Requisitos não compreendidos por parte da equipa- Má interpretação do resultado pedido por parte dos elementos do grupo.

User Story 5

Requisitos

Como administrador do sistema quero que seja definido o MBCO (Minimum Business Continuity Objective) a propor aos stakeholders.

Esclarecimentos do cliente

Questão 1:

Neste contexto, pretende-se que o sistema esteja operacional o máximo de tempo possível. Sendo assim, é aceite algum período de indisponibilidade? Se sim, de quanto tempo? O sistema deverá apresentar funcionalidades parciais durante este período? Além disso, existe algum máximo de tempo que o sistema, após interromper/paralisar os serviços, deverá voltar a recuperar os dados?

Resposta 1:

Como descrito na US800 "quero que seja definido o MBCO (Minimum Business Continuity Objective) a propor aos stakeholders" o que implica que terá que definir as funcionalidades que lhe parecem mais importantes que sejam mantidas em caso de desastre. As cópias de segurança (US810) são necessárias e podem implicar a inoperacionalidade da solução. A estratégia implementada nas cópias têm implicação no RPO e no WRT, pelo que terá de definir a mais apropriada. Sim, é aceite algum tempo de indisponibilidade mas que terá de ser justificado e, claro, o menor possível.

Questão 2:

Pode indicar-nos qual a escala horária estabelecida para efeitos de utilização do sistema? É espectável que, para efeitos de backup, haja uma breve interrupção do serviço, no entanto, poderemos recorrer a qualquer período do dia para este efeito. Neste sentido, gostávamos de saber qual a altura mais favorável do dia para esta breve interrupção.

Resposta 2:

Atendendo aos termos e exemplo do RFP, quer o robisep quer o droneisep podem executar tarefas que não pressupõem ocupação humana (vigilância, limpeza, por exemplo). Já outras tarefas (buscar/entregar um item, por exemplo) pressupõem ocupação humana. Deverá definir face ao tempo estimado de indisponibilidade do sistema a melhor altura para a breve interrupção face às funções planeadas para os dispositivos. Em suma, é aceitável uma breve interrupção de serviço, mas a altura da indisponibilidade deverá ser proposta por quem responde ao RFP.

Análise

Como se pode verificar na seguinte figura, existem 4 pontos que têm de ser delimitados:

- *Recovery Point Objective (RPO)*;
- *Recovery Time Objective (RTO)*;
- *Work Recovery Time (WRT)*;
- *Maximum Tolerable Downtime (MTD)*.

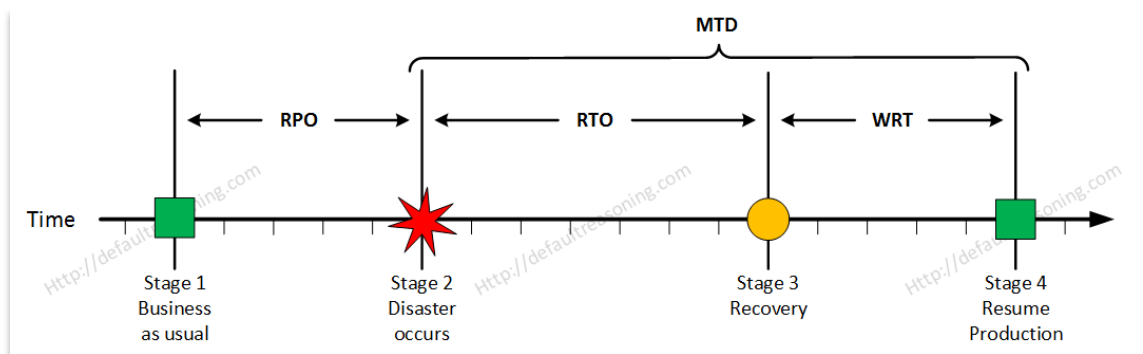


Figure 1 - Business Continuity and Disaster Recovery.

Nota: Imagem figurativa e não se encontra à escala da solução apresentada.

Recovery Point Objective

Para definir o RPO, é preciso responder à(s) pergunta(s):

- Qual é o máximo de tempo em que se pode perder informação?

- Quando (frequência e altura do dia (manhã/noite)) é que faz sentido executar cópias de segurança?

Maximum Downtown Tolerable

Para definir o MDT, é preciso responder à(s) pergunta(s):

- Qual é o máximo de tempo que desde a perda de dados até o regresso à normalidade pode durar?

Desenho

Este é um requisito onde as exigências do cliente são cruciais (como qualquer outro use case, mas este especialmente) e vão redigir a proposta MBCO.

Contexto do sistema

Este sistema contém drones e robôs que executam, fundamentalmente, tarefas de vigilância, entrega de objetos e limpeza.

Criticidade dos dados

Neste sistema é importante que todos os processos que envolvam as funções dos robôs/drones estejam "sempre" operáveis, sendo considerado o mais crítico a vigilância e a limpeza.

Este sistema trata-se um **sistema não crítico** por conter funcionalidades dispensáveis ao negócio.

Custo da baixa do sistema

Sem o sistema, em média, existem custos como:

- Cerca de 15 minutos por dia com a tarefa de busca de objetos;
- Limpezas por fazer;
- Sistema de vigilância sofre vulnerabilidades.

Relativamente à busca de objetos, são 75 minutos por semana que cada pessoa perde, resultando, para 100 pessoas, um acumular de 7500 minutos semanais de produtividade. Se por cada 15 minutos as pessoas gerarem 10eur para a empresa:

- Sem o sistema, cada pessoa trabalha cerca de 40h semanais (2400 minutos), dispensando 75 minutos para este tipo de tarefas, resulta em 2325 minutos de produtividade (1550eur). Numa escala de 100 pessoas, são 155 000eur.
- Com o sistema, cada pessoa dispõe de 2400 minutos de produtividade (1600eur). Numa escala de 100 pessoas, são 160 000eur.

Se se optasse por uma solução menos arriscada, ou seja, com execução de cópias de segurança mais frequentes como por exemplo, diariamente, teria um **custo de cerca de 10 000eur** por exigir equipamentos mais sofisticados, mais espaço, etc. Se se optasse por uma solução mais arriscada com uma frequência de três dias, teria um **custo de cerca de 3333eur**.

Conclui-se então que se se optasse por um sistema de recuperação mais sofisticado, com mais frequência e mais rápido seria um valor de $160\,000\text{eur} - 10\,000\text{eur} = 150\,000\text{eur}$, e por outro lado $155\,000\text{eur} - 3333\text{eur} = 151667\text{eur}$. É mais vantajoso, financeiramente falando, o sistema de 3 dias de frequência.

As perdas ocorrem **apenas** quando o sistema está em baixo, ou seja, a perda de dados de um dia, em princípio, não afetará, financeiramente, o negócio. Isto significa que se a base de dados sofrer um problema que a nível físico que estrague o computador, no pior caso, ou seja, a minutos de chegar o 3º dia de executar a cópia de segurança, o tempo que se perdeu de dados não vai ser fundamental, isto por o teor do conteúdo que se armazena não ser financeiramente prejudicial e não impedir progressos.

Relativamente à limpeza e à vigilância, o seu impacto não seria a nível financeiro, porém teria, obviamente, consequências negativas.

Nota: Os valores utilizados são completamente figurativos, mas, eventualmente, com proporção direta para os valores reais.

Em suma, o sistema RobDroneGo não se define como crítico, é algo que apenas auxilia os seus utilizadores e que não impede que as funções dos próprios sejam executadas. O risco pode ser mais elevado tendo isto consequências positivas, como não necessitar de soluções de recuperação mais sofisticadas e dispendiosas.

Tecnologias da infraestrutura

Este projeto não dispõe de tecnologias de ponta, rede banda larga medíocre e soluções de armazenamento escassas.

Conclusão

Apontados os fatores que sustentam a decisão do RPO, a equipa considerou que **3 dias é a frequência necessária e suficiente**. Para o MDT considerou-se **6 horas**.

Cópia de segurança

Execução

Sendo que este processo reduz eficiência ao sistema ou até inoperacionalidade, a melhor altura do dia para executar backups é de madrugada, onde a probabilidade de atividade por parte dos utilizadores é baixa.

Localização

É fortemente sugerido que os backups sejam armazenados numa cloud ou num servidor distinto. Isto por serem e estarem fisicamente distintos e distantes. Em caso de desastre no servidor, esta solução salvaguarda o backup.

User Story 6

Requisitos

Como administrador do sistema quero que seja proposta, justificada e implementada uma estratégia de cópia de segurança que minimize o RPO (Recovery Point Objective) e o WRT (Work Recovery Time).

Objetivo

Criar e implementar uma política de backups para o projeto e respetiva base de dados.

Problema

Para prevenir a perda de dados cruciais, seja funcionalidades do programa, ou dados que ele consome, é crucial efetuar uma política de Backups, que permita numa situação de emergência, a recuperação total ou parcial dos dados que foram perdidos, apagados ou alterados de forma inesperada.

Para escolher a melhor Política de Backups, foi analisado o documento onde é feito o estudo do WRT (Work Recovery Time) e do RPO (Recovery Point Objective), onde se chegou à conclusão que a frequência de backups deveria de ser de 3 em 3 dias para garantir o RPO estudado e escolhido.

Tendo esta informação em conta, foram então analisadas as possibilidades de backups que poderiam ser feitas: total, incremental ou diferencial e concluiu-se que no dado momento (SPRINT B) a informação que é armazenada e a quantidade de alterações feitas diariamente não justificavam a necessidade de ser feito um backup incremental ou diferencial. O projeto tem na sua grande maioria, dados estáticos e não tem qualquer automatização que implique que certos dados estejam disponíveis para ser executada, ou seja, qualquer ação feita no programa, será feita após um input de um utilizador e não triggered automaticamente.

Caso se justifique no SPRINT C, podem ser sempre acrescentadas novas políticas de backup que se adequem às novas funcionalidades ou dados armazenados. Isto significa um novo estudo, porque a implementação de backups diferenciais ou incrementais, implicavam um maior cuidado com a cronologia de backups, uma vez que ambos dependem do backup total para guardarem a informação correta.

Backup incremental

Um backup incremental é um tipo de cópia de segurança que registra apenas as alterações efetuadas nos dados desde o último backup realizado. Por exemplo, se um backup completo foi

feito no domingo, o backup incremental feito na segunda-feira incluiria apenas as mudanças feitas desde esse backup de domingo. Na terça-feira, o backup incremental conteria apenas as modificações ocorridas desde o backup realizado na segunda-feira. Esse método de backup economiza espaço de armazenamento ao capturar apenas as alterações mais recentes nos dados, em vez de duplicar todo o conjunto de informações a cada backup.

Backup diferencial

Uma estratégia de backup diferencial regista apenas os dados novos e alterados desde o último backup completo. Se o último backup completo foi feito no domingo, um backup diferencial realizado na segunda-feira conteria todas as modificações desde o domingo. Da mesma forma, um backup feito na terça-feira também incluiria todas as alterações desde o último backup completo, realizado no domingo. Conforme novos backups diferenciais são feitos, o tamanho do arquivo de backup aumenta progressivamente até que seja realizado um novo backup completo.

Resolução do Problema

Para resolver este problema, foi necessário utilizar o scp para fazer uma cópia do projeto da máquina local e enviá-la para uma máquina remota. Utilizou-se também o mongodump, mas para fazer o backup da base de dados, na máquina remota. Depois foram feitos 2 scripts, um para cada um destes comandos, que os executavam, dando-lhes os dados necessários para fazer a comunicação entre máquinas e adicionado ao crontab uma regra para executar o script de 3 em 3 dias, às 2 da manhã.

Backup do Projeto

Inicialmente, tem de ser feita a conexão das duas máquinas, e partilhar uma key entre elas, para que ao correr o script não seja exigido o login ao utilizador, mas este ser feito automaticamente. Para isto, executa-se o seguinte comando ``ssh-keygen -t rsa -b 2048``, que irá gerar uma key, que terá de ser partilhada com a máquina remota através do comando ``ssh-copy-id -i /path/to/private_key root@vs510.dei.isep.ipp.pt``.

É também criado um ficheiro para logs, que conterá os registos e possíveis erros da execução do script, através do comando ``touch ~/backup_logs.log``. Após isto, o script já pode fazer a conexão entre as duas máquinas sem necessitar de login, porque elas partilham uma key e já poderá também guardar as informações acerca da execução do script num ficheiro de logs. O script terá o seguinte formato:

```
#!/bin/bash
```

Caminho do ficheiro de logs

```
LOG_FILE="/root/backup_logs.log"
```

Caminho da pasta onde se encontra o projeto na máquina local

```
SOURCE_DIR="/root/RobDroneGo"
```

//Caminho da pasta onde se quer armazenar o backup na máquina remota

```
REMOTE_USER="root"
```

```
REMOTE_HOST="vs510.dei.isep.ipp.pt"
```

```
REMOTE_DIR="/root/RobDroneGo"
```

Mensagem de informação de execução do script (sem ainda ter iniciado o processo de transferência)

```
echo "Transferring files..."
```

Comando scp com uso de keys SSH para um login sem password, com o output redirecionado para um ficheiro de logs

```
{  
echo "==== Start of File Transfer ====  
  
date +"%Y-%m-%d %H:%M:%S"  
  
scp -r -o "BatchMode yes" -i /root/backup_key "$SOURCE_DIR"  
"$REMOTE_USER@"$REMOTE_HOST":"$REMOTE_DIR"  
  
echo "==== End of File Transfer ====  
  
date +"%Y-%m-%d %H:%M:%S"  
  
}>>"$LOG_FILE" 2>&1
```

Verifica o status de término do comando scp e coloca a mensagem correspondente no ficheiro de logs

```
if [ $? -eq 0 ]; then  
echo "Files transferred successfully." >>"$LOG_FILE"  
  
else  
echo "Error transferring files." >>"$LOG_FILE"  
  
fi
```

Deve-se testar o script, executando-o, para garantir que a conexão entre as duas máquinas é feita e o backup é feito corretamente antes de adicionar uma nova regra no crontab. Caso seja positivo, acrescenta-se finalmente ao ficheiro de configuração do crontab uma nova regra de execução do script. Finalmente, deve-se acrescentar a regra ao ficheiro de configuração do crontab, através do comando `crontab -e`, que abrirá o ficheiro ao qual teremos de adicionar a seguinte regra: `0 2 * * * /root/backup_script.sh >> /root/backup_logs.log 2>&1`.

Backup da Base de Dados

Para o backup de base de dados, é necessário instalar o MongoDB Database Tools, e correr o comando `mongodump`. Igualmente, como no backup do projeto, cria-se um script e um ficheiro de logs e adiciona-se uma regra ao crontab. O script terá a seguinte estrutura:

```
#!/bin/bash
```

```
MongoDB URI for authentication and connection
```

```
MONGO_URI="mongodb://mongoadmin:aed0452dba3a82201f874542@vsgate-  
s1.dei.isep.ipp.pt:10242/"
```

```
Output directory for MongoDB dump
```

```
BACKUP_DIR="/path/to/backup/directory"
```

```
Log file to record backup status
```

```
LOG_FILE="/path/to/backup.log"
```

```
Ensure the backup directory exists; create if not
```

```
mkdir -p "$BACKUP_DIR"
```

```
Run mongodump with the specified URI and log the output
```

```
if mongodump --uri "$MONGO_URI" --out "$BACKUP_DIR" >> "$LOG_FILE" 2>&1; then
```

```
    echo "$(date): MongoDB backup successful" >> "$LOG_FILE"
```

```
else
```

```
    echo "$(date): MongoDB backup failed" >> "$LOG_FILE"
```

```
fi
```

Finalmente, deve-se acrescentar a regra ao ficheiro de configuração do crontab, através do comando `crontab -e`, que abrirá o ficheiro ao qual teremos de adicionar a seguinte regra : `0 2 * * * /root/mongo_backup_total.sh >> /root/backup_logs.log 2>&1`.

User Story 7

Requisitos

Como administrador do sistema quero definir uma pasta pública para todos os utilizadores registados no sistema.

Esclarecimentos do cliente

Questão:

Pretende que a pasta seja visível através da UI ou através do próprio sistema operativo dos utilizadores? Quando se refere a todos os utilizadores registados no sistema, isto inclui os users, campus managers, fleet managers, task managers que são criados via sign up pela nossa solução ou apenas o users já registados nas máquinas?

Ou pretende que a pasta seja de acesso publico apenas com permissões de leitura para o acesso geral, e apenas os managers (campus, fleet, task, system admins ou users registados nas máquinas) tenham de fazer login para terem as permissões de escrita e leitura?

Resposta:

Através da UI seria mais apelativo por nem todos saberão aceder vi sistema operativo, não concorda? Contudo, é aceitável que seja apenas nesta fase visível por sistema operativo. Relativamente às permissões note que a US é (propositadamente) omissa sobre isso. O que imagina que o cliente irá colocar na pasta? Instruções (pasta só de leitura para utilizadores "normais", leitura e escrita para internos)? Ou algo diferente que implique que qualquer utilizador tenha permissões de escrita?

Apresente e implemente de acordo com o princípio que considerarem - o máximo que pode acontecer é o cliente dizer na reunião final "Ah, mas não era essa a minha ideia", tornando-se numa definição incorreta das especificações da exclusiva responsabilidade do cliente.

Análise

Partilha de informações entre todos os utilizadores do sistema

Implementação

Para implementar a pasta pública, o grupo optou por utilizar o Samba, e para isso seguimos os respetivos passos:

Passo 1:

Instalar o Samba na máquina, para isso utilizar o comando:

sudo apt-get install samba

Passo 2:

Criar a pasta que vamos querer partilhar com todos os utilizadores, neste caso, a pasta vai ser criada com o nome “public”, para isso executamos o comando:

sudo mkdir public

Passo3:

Agora que a pasta “public” foi criada, iremos dar permissões de leitura, escrita e execução a todos os utilizadores, para tal, executamos o comando:

sudo chmod 777 public

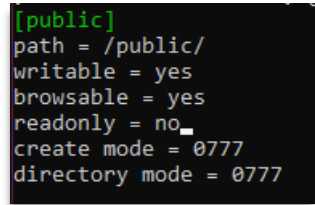
Passo 4:

Agora iremos editar o ficheiro de configuração do samba, para isso abrimos o ficheiro, para isso fazemos:

cd etc/samba

nano smb.conf

Dentro do ficheiro, inserimos no final as seguintes informações:



```
[public]
path = /public/
writable = yes
browsable = yes
readonly = no
create mode = 0777
directory mode = 0777
```

Figura 6 - Informações a incluir no ficheiro smb.conf

Passo 5:

Após estas alterações no ficheiro, temos de reiniciar o serviço, para isso fazemos:

service smbd restart

Passo 6:

Por último, verificamos se a conexão está a ser realizada e se a pasta está pública, para isso fazemos:

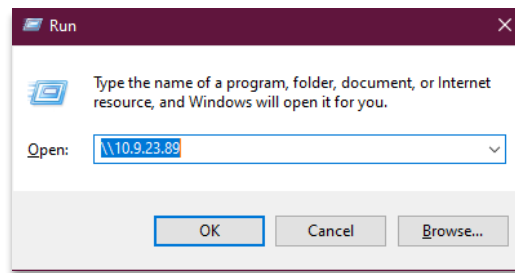


Figura 7 - Conexão à máquina pretendida onde se encontra a pasta pública.

E assim verificamos que a pasta se encontra publica:

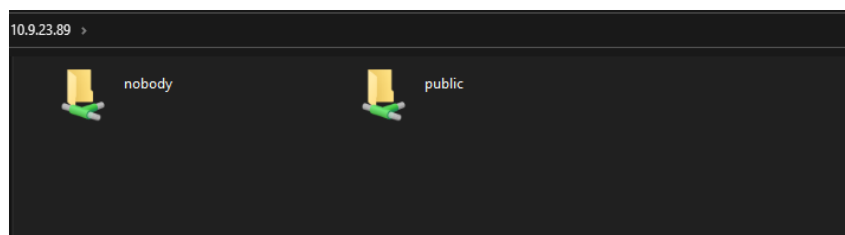


Figura 8 - Pasta public.

User Story 8

Requisitos

Como administrador do sistema quero obter os utilizadores com mais do que 3 acessos incorretos.

Análise

Identificação do Problema

Identificar os utilizadores com mais do que 3 acessos incorretos.

Resolução do Problema

Para resolver este problema, vai recorrer-se ao ficheiro de logs `/var/log/auth.log` para identificar os utilizadores cujo login foi falhado mais do que 3 vezes.

Implementação

Passo 1:

Primeiro instalaremos o módulo que vai guardar nos ficheiros ".log" a informação de logins incorretos. Para isso necessitamos de correr o seguinte comando:

\$ sudo apt -y install -y rsyslog

Após executar o comando, é necessário reiniciar a máquina para serem criados os ficheiros de logs, nos respetivos locais.

Passo 2:

Após a instalação do módulo, iremos aceder ao ficheiro `auth.log`.

Dentro deste ficheiro estão localizadas todos os logins válidos ou tentativas falhadas, que poderão ser filtradas posteriormente através de um comando, para serem mostrados os utilizadores com mais do que 3 tentativas falhadas no seu login.

Executar o comando de filtragem de utilizadores, sendo este:

``grep "Failed password" /var/log/auth.log | awk '{print $(NF-5)}' | sort | uniq -c | awk '$1 > 3 {print $2}'`, que irá filtrar os utilizadores com mais de 3 tentativas falhadas a fazer login. Todos os outros serão ignorados.