



Relatório de ASIST

Sprint C

Ricardo Freitas (1210828)
Gabriel Silva (1210808)
João Rodrigues (1210817)
Mateus Fernandes (1210821)

Índice

| | |
|---|-------------------------------------|
| User Story 1..... | 5 |
| Requisitos..... | 5 |
| Esclarecimentos do cliente..... | 5 |
| Desenho..... | 5 |
| Definição de desastre..... | 5 |
| Propósito..... | 5 |
| Contatos de emergência..... | 6 |
| Rede de Notificação..... | 6 |
| Formas de contato interno e externo..... | 6 |
| Direcionamento..... | 6 |
| Backup e Dados..... | 7 |
| User Story 2..... | 8 |
| Requisitos..... | 8 |
| Esclarecimentos do cliente..... | Erro! Marcador não definido. |
| Desenho..... | 8 |
| Solução..... | 8 |
| User Story 3..... | 10 |
| Requisitos..... | 10 |
| Esclarecimentos do cliente..... | 10 |
| Desenho..... | 10 |
| Resolução do Problema..... | 10 |
| User Story 4..... | 12 |
| Requisitos..... | 12 |
| Esclarecimentos do cliente..... | 12 |
| Desenho..... | 12 |
| Resolução do Problema..... | 12 |
| User Story 5..... | 15 |
| Requisitos..... | 15 |
| Identificação do Problema..... | 15 |
| Desenho..... | 15 |
| Implementação..... | 15 |
| Alteração do Script de Backup..... | 15 |
| Criação de Script checkUpdates..... | 15 |
| Iniciar o Script sempre que for efetuado login..... | 15 |

| | |
|---|----|
| User Story 6..... | 16 |
| Requisitos | 16 |
| Esclarecimentos do cliente | 16 |
| Desenho | 16 |
| Resolução do Problema | 16 |
| User story 7 | 17 |
| Requisitos | 17 |
| Esclarecimentos do cliente | 17 |
| Desenho | 17 |
| User Story 8..... | 21 |
| Requisitos | 21 |
| Esclarecimentos do Cliente | 21 |
| Desenho | 21 |
| User story 9 | 24 |
| Requisitos | 24 |
| Esclarecimentos do cliente | 24 |
| Desenho | 24 |
| Sistemas e ferramentas | 24 |
| Número de servidores + backup | 24 |
| Algoritmo de balanceamento | 24 |
| Ficheiro de configuração HAProxy | 25 |
| User Story 10..... | 26 |
| Requisitos | 26 |
| Esclarecimentos do cliente | 26 |
| Desenho | 26 |
| User Story 11..... | 27 |
| Requisitos | 27 |
| Esclarecimentos do Cliente | 27 |
| Desenho | 27 |
| Implementação | 27 |
| Instalação do Package ACL..... | 27 |
| Criação de grupos e utilizadores para testar funcionalidade | 27 |
| Alteração de passwords dos utilizadores..... | 27 |
| Definir lista de controlo de acesso através do setfac1 | 28 |
| Executar o getfac1 | 28 |
| Alteração do ficheiro smb.conf..... | 28 |

Reiniciar o serviço28

Verificar conexões à pasta partilhada29

User Story 12.....30

Requisitos.....30

Esclarecimentos do Cliente30

Desenho30

Resolução do problema.....30

Índice de figuras

| | |
|--|----|
| Figura 1 - Redede Notificação..... | 6 |
| Figura 2 - Exemplificação através de esquema das stages e das respetivas diretrizes. | 8 |
| Figura 3 - Script de renomeação do ficheiro de backup da base de dados. | 11 |
| Figura 4- Extrato 1 script us850..... | 13 |
| Figura 5- Extrato 2 script us850..... | 14 |
| Figura 6 - Configurações a adicionar no final do script. | 15 |
| Figura 7 - Script que verifica a falha do backup. | 15 |
| Figura 8 - Exemplo de Last Login realizado anteriormente noutra US. | 22 |
| Figura 9 - Auth.log, que mantém o histórico de autenticação dos utilizadores. | 22 |
| Figura 10 - Exemplo de estrutura do aspeto di ficheiro shadow. | 22 |
| Figura 11 - Utilização da Role para cumprir o parâmetro de autorização de acesso. | 23 |
| Figura 12 - Ficheiro de configuração HAProxy | 25 |
| Figura 13 - Demonstração por acesso a SSH sem password. | 26 |
| Figura 14 - Getfacl, mostrando as permissões de cada grupo de utilizadores para a pasta partilhada. | 28 |
| Figura 15 - Configurações no ficheiro smb.conf para a realização da US. | 28 |
| Figura 16 - Acesso negado a escrita para utilizadores que sejam gestores de Campus. | 29 |
| Figura 17- Extrato script us930..... | 30 |

User Story 1

Requisitos

Como administrador da organização quero um plano de recuperação de desastre que satisfaça o MBCO definido no sprint B.

Esclarecimentos do cliente

Questão:

Resposta:

Desenho

É impossível para uma organização evitar todas as ameaças a desastres, porém é possível precaverem-se. De qualquer das formas, o futuro é incerto e qualquer empresa está sujeita a este tipo de situações. É uma excelente prática e fortemente aconselhável que exista um *DRP (Disaster Recovery Plan)* para haver uma agilização na recuperação e restauração após uma situação destas.

Definição de desastre

Um desastre é qualquer tipo de evento que impeça a utilização do setor de IT durante um período de tempo. São esses eventos:

- Sistema não funcional;
- Robôs/Drones não funcionais;
- Módulo(s) do sistema não funciona(l/is).

Para que aconteçam os desastres acima mencionados, segue uma lista de eventos com a capacidade de os fazer concretizar:

- Ciberataques;
- Catástrofes ambientais;
- Erros humanos;
- Falhas de energia;
- Falhas de hardware;
- Falhas de software.

Propósito

Este plano tem como objetivo:

- Manter o negócio ativo face um evento disruptivo;
- Minimizar o *downtime*;
- Estabelecer meios alternativos de operar em avanço;
- Minimizar o impacto das consequências negativas;
- Prevenção de perda de recursos da empresa (hardware, dados...).

Contatos de emergência

| Primeiro Nome | Último Nome | Título | Tipo Contato | Informação Contato |
|---------------|-------------|--|--------------|--|
| Ricardo | Venâncio | Coordenador DRP | Email | 1210828@isep.ipp.pt |
| Gabriel | Silva | Analista de Recuperação de Dados | Email | 1210808@isep.ipp.pt |
| João | Rodrigues | Network Engineering | Email | 1210817@isep.ipp.pt |
| Mateus | Fernandes | Especialista em Segurança | Email | 1210821@isep.ipp.pt |

Rede de Notificação

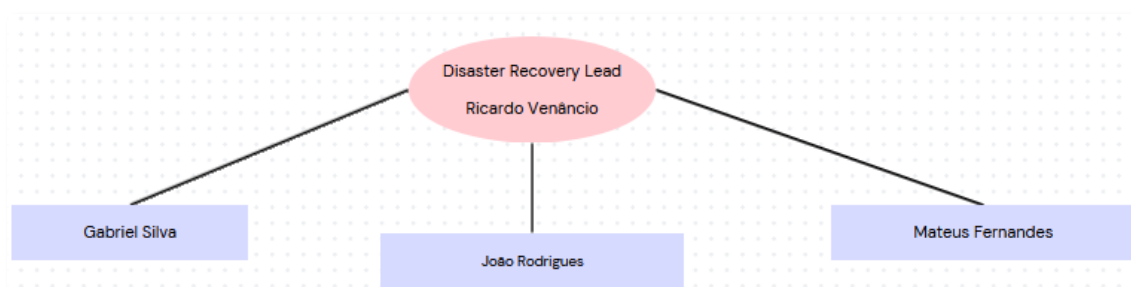


Figura 1 - Rede de Notificação.

Formas de contato interno e externo

Na condição dos sistemas estarem todos em baixo, é necessário seguir os seguintes passos para estabelecer comunicação interna:

- Mensagens de texto (SMS);
- Comunicações rádio;
- Aplicações que os trabalhadores utilizem na generalidade.

É também necessário e importante a transparência com o externo, mais concretamente, os *stakeholders*. Como tal, segue a lista de meios alternativos de comunicação externa:

- Redes Sociais;
- Mensagens de texto (SMS).

Direcionamento

Este plano dirige-se às seguintes áreas tecnológicas:

- Infraestrutura de rede;
- Servidores da infraestrutura;
- Capacidade de armazenamento e sistemas de backup;
- Sistemas de base de dados.

Backup e Dados

A próxima tabela vai demonstrar onde é que os dados do sistema RobDroneGo são persistidos também o onde estão as cópias de segurança. É relevante utilizar esta informação para localizar e restaurar dados numa situação desastrosa.

Dados por ordem de criticidade

| Rank | Informação | Tipo de dado | Freq. Cópia de segurança | Local. Cópia de segurança |
|------|--------------------------|------------------|--------------------------|--------------------------------------|
| 1 | Dados de alunos/docentes | Dados pessoais | Diária | vs510.dei.isep.ipp.pt (Cloud do DEI) |
| 2 | Informação do campus | Dados do sistema | 3 em 3 dias | vs510.dei.isep.ipp.pt (Cloud do DEI) |

APIs por ordem de importância

A seguinte tabela ordena as APIs deste sistema por ordem de criticidade.

| Rank | API | Componentes do sistema |
|------|--|---------------------------------|
| 1 | Master Data Gestão de Dispositivos API | Gestão de dados de dispositivos |
| 1 | Master Data Gestão de Tarefas API | Gestão de dados de tarefas |
| 1 | Frontend API | Interface do utilizador |
| 2 | Planeamento API | Planeamento |
| 3 | Visualização 3D API | Visualização de gráficos 3D |

Plano de testes e Manutenção

É extremamente difícil apontar todos os problemas a uma organização, já que se encontra constantemente em atualizações e adaptações. À medida que a empresa vai mudando, o DRP deve ser atualizado.

Este **plano** deverá ser **atualizado** com uma **frequência de um mês** ou sempre que haja uma grande atualização ou *upgrade* de um sistema.

Para que a manutenção seja eficaz é necessário assegurar que:

- todas as equipas estão atualizadas;
- as instruções do plano ainda têm nexos para empresa;
- o plano está de acordo a lei.

Através de testes ao plano, vai ser possível verificar se é realmente funcional ou não. Os testes que devem ser executados para garantir eficácia são:

- membros da equipa experimentarem seguir o DRP e tentarem descobrir erros, falta de informação, *bottlenecks* e outras fraquezas;
- de forma isolada, colocar servidores e sistemas online para verificar que todos os sistemas de operação estão a correr como esperado e sem quaisquer problemas.

User Story 2

Requisitos

Como administrador da organização quero que me seja apresentada de forma justificada a ou as alterações a realizar na infraestrutura por forma a assegurar um MTD (Maximum Tolerable Downtime) de 20 minutos.

Desenho

É importante que qualquer organização estude qual é o seu MTD, para que as perdas que possa vir a ter sejam minimizadas ou até mesmo nulas. Para isso, é importante perceber o que é o MTD antes de apresentar formas como a empresa ou organização consiga repor os seus serviços ou protegê-los antes do tempo máximo ser esgotado e isso lhe traga prejuízos.

Solução

O MTD (Maximum Tolerable Downtime) é o período durante o qual uma empresa ou organização, pode ficar sem acesso a um sistema ou serviço crítico antes que isso cause danos à operação da mesma. Para além disso o MTD, é um parâmetro importante, quando se fala em implementação de medidas de proteção e tolerância a falhas, como sistemas altamente disponíveis e backups, sendo por isso um indicador do investimento necessário a ser feito pela organização.

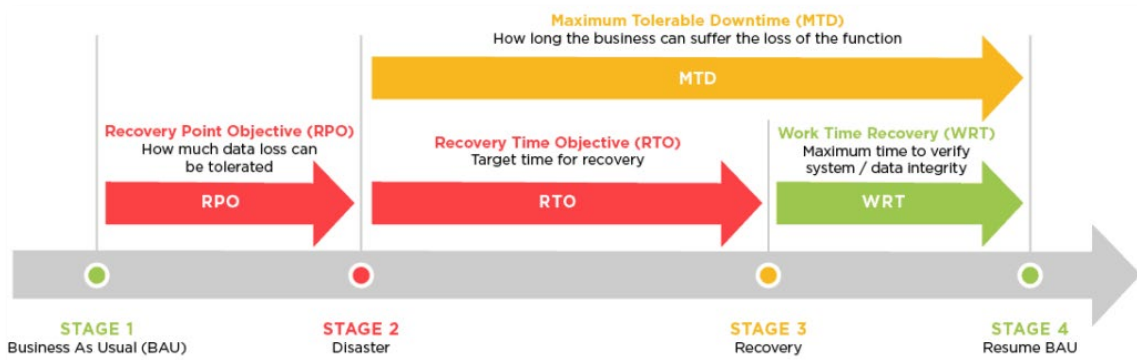


Figura 2 - Exemplificação através de esquema das stages e das respetivas diretrizes.

Para se poder garantir um MTD de 20 minutos, é preciso implementar medidas de proteção e tolerância a falhas, em todas as camadas da infraestrutura da organização.

Como é possível verificar na figura acima apresentada, o MTD é a soma entre o tempo de recuperação dos sistemas (RPO) e os testes de funcionamento e integridade destes mesmos (WRT), que já foram explorados e abordados anteriormente. O MTD, varia de acordo com as necessidades e prioridades da organização, e pode até variar entre departamentos e sistemas utilizados pela organização, o que significa que dentro da própria empresa, poderão existir diferentes MTD's para cada operação.

Para se escolher um MTD, deverão ser seguidos alguns passos como por exemplo:

- Avaliação de impacto nos negócios;
- Identificação de ativos críticos;
- Conversas com partes interessadas (Executivos, Departamentos, Equipas de Operações, ...);

- Identificar regulamentações e requisitos do setor;
- Avaliar custos;
- Identificar risco toleráveis;
- Considerações estratégicas;
- Executar testes e simulações.

Para ser possível garantir um MTD tão baixo exige altos custos, e investimento em tecnologias e soluções como as seguintes:

- Investimento em infraestrutura redundante;
- Tecnologias e soluções de backups avançadas;
- Atualizações e manutenção constantes;
- Monitorização e gerenciamento proativo;
- Treinamento e capacitação da equipa;
- Alocação de tempo e recursos para planeamento e testes;
- Contratos de suporte e serviços especializados.

No caso, para a nossa infraestrutura, destas soluções, as que se deveriam adotar para conseguir um MTD de 20 minutos seriam:

- Utilizar sistemas de backup e recuperação de desastres e anomalias, garantindo a proteção de **dados** críticos (informação da base de dados e a aplicação em si) e possibilitando a rápida recuperação em caso de falha;
- Implementar sistemas altamente disponíveis, como clusters que permitem com o que o sistema continue a funcionar, em caso de falha, ao redirecionar para outro servidor/máquina a tarefa ou tarefas que o equipamento que falhou estaria a executar;
- Realizar e produzir novos testes de *failover*, para garantir que os sistemas de backup funcionam corretamente e que caso haja necessidade de transição para estes sistemas, esta seja feita sem imprevistos e de forma suave;
- Formar a equipa para proteger os sistemas de falhas humanas;
- **Manter** os softwares atualizados, para prevenir falhas de segurança e do próprio software.
- Praticar políticas que obriguem a atualização regular dos equipamentos e softwares, que contenham correções de falhas e melhorias para minimizar a probabilidade de falhas;



User Story 3

Requisitos

Como administrador de sistemas quero que seja realizada uma cópia de segurança da(s) DB(s) para um ambiente de Cloud através de um script que a renomeie para o formato <nome_da_db>_yyyymmdd sendo <nome_da_db> o nome da base de dados, yyyy o ano de realização da cópia, mm o mês de realização da cópia e dd o dia da realização da cópia.

Esclarecimentos do cliente

Questão

Perante o caso de uso 120, que sugere o apagamento dos dados do utilizador, existe um possível conflito com os casos de uso 840, 850 e 870 (relacionados com backups). Sendo que é necessário persistir 1 backup por mês no último ano, 1 backup por semana no último mês e backup por dia na última semana, como seria a abordagem desejada para tratar os backups que contêm informações de utilizadores que já solicitaram o apagamento dos seus dados.

Resposta

Essa é uma excelente questão. Poderão propor uma metodologia para em caso de reposição de um backup validar os pedidos de apagamento que surgiram, entretanto.

Desenho

É importante que qualquer organização organize bem os seus backups, com a correta nomenclatura, no local indicado, para que quando exista necessidade de os usar ou modificar algo relacionado com os backups, ser fácil para o administrador de sistemas se localizar e agir o mais rapidamente perante uma necessidade, seja esta uma emergência ou não. De salientar, que uma boa gestão dos backups, pode significar uma poupança de milhares para a empresa.

Resolução do Problema

Para resolver este problema, foi bastante simples, necessitando apenas de fazer algumas alterações ao script de backups feito no Sprint anterior.

```

GNU nano 5.4                                     mongo_backup_total.sh
#!/bin/bash

#Dates
DATE=$(date +%Y%m%d)

#Names
DBNAME="test"

# 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="/root/bin/mongodumtotal"
BACKUP_DIR2="/root/bin/mongodumtotal2"

#Output file
BACKUP_FILE="$BACKUP_DIR/${DBNAME}_${DATE}"
BACKUP_FILE2="$BACKUP_DIR2/${DBNAME}_${DATE}"

# Log file to record backup status
LOG_FILE="/root/backup_logs.log"

# Ensure the backup directory exists; create if not
mkdir -p "$BACKUP_DIR"
mkdir -p "$BACKUP_DIR2"

# Run mongodump with the specified URI and log the output
if ./bin/mongodump --uri "$MONGO_URI" --out "$BACKUP_FILE" >> "$LOG_FILE" 2>&1; then
    echo "$(date): MongoDB backup successful" >> "$LOG_FILE"
else
    echo "$(date): MongoDB backup failed" >> "$LOG_FILE"
fi

```

Figura 3 - Script de renomeação do ficheiro de backup da base de dados.

Como é possível observar na figura acima apresentada, as alterações que foram feitas para cumprir com a nomenclatura dos ficheiros de backup, são referentes ao “BACKUP_FILE” que especifica tanto onde é que irá ser guardado, bem como o nome que lhe será dado. No início do script foi criada tanto uma variável de data, bem como uma variável com o nome da base de dados, que posteriormente são utilizados na construção da variável “BACKUP_FILE”, que cumpre com a nomenclatura “<nome_da_db>_yyyymmdd”.

User Story 4

Requisitos

Como administrador de sistemas quero que utilizando o Backup elaborado na US C3, seja criado um script que faça a gestão dos ficheiros resultantes desse backup, no seguinte calendário. 1 Backup por mês no último ano, 1 backup por semana no último mês, 1 backup por dia na última semana.

Esclarecimentos do cliente

Questão: O que é que é pretendido por "a gestão dos ficheiros resultantes desse backup" no contexto desta US?

Resposta: O texto completo da US é : "Como administrador de sistemas quero que utilizando o Backup elaborado na US 840, seja criado um script que faça a gestão dos ficheiros resultantes desse backup, no seguinte calendário. 1 Backup por mês no último ano, 1 backup por semana no último mês, 1 backup por dia na última semana". Na US 840 são realizadas cópias de segurança de acordo com um dado critério. Com "gestão" pretende-se a eliminação dos backups que não obedecem aos princípios enunciados.

Desenho

Na US C3 é criado um backup com um dado critério, neste caso {nome da bd}_{data de realização do backup}. O objetivo da US C4 é verificar se o backup realizado se encontra de acordo com o pedido na gestão de ficheiros. Caso contrário, esse backup será descartado. Os ficheiros aceites serão apenas os que cumprem um ou mais dos seguintes requisitos:

- 1 Backup por mês no último ano;
- 1 Backup por semana no último mês;
- 1 Backup por dia na última semana;

Resolução do Problema

De modo a satisfazer o requisito da US C4 foi elaborado um script para realizar a filtragem dos backups realizados.

No script apresentado cada backup será guardado numa pasta. Para a gestão dos backups um ciclo for percorre cada pasta de backups e analisa a data desse mesmo. Caso a data não corresponda ao pedido, essa mesma pasta e os seus ficheiros serão eliminados. O mesmo será realizado na base de dados relacional de MySQL.

```

folder_path="/root/bin/mongodumtotal"
mysql_folder_path="/root/bin/mysqldumtotal"
log_file="/root/us850_logs.log"

# Function to check if a folder follows the specified criteria
check_folder() {
    local folder_name=$1
    local test=0

    # Extract the date part
    date_part=${folder_name#test_}

    # Check if it's the first day of the month
    if [ "$(date -d "$date_part" +%d)" -eq 28 ]; then
        echo "Folder '$folder_name' is a backup for the 28th of the month. Keeping it." >> "$log_file"
        ((test++))
    fi

    # Check if it is the month of december and it is the first day of the week
    if [ "$(date -d "$date_part" +%m)" -eq 12 ] && [ "$(date -d "$date_part" +%u)" -eq 1 ]; then
        echo "Folder '$folder_name' is a backup for the first day of December. Keeping it." >> "$log_file"
        ((test++))
    fi

    # Check if it's the last week of the year
    if [ "$(date -d "$date_part" +%W)" -eq 52 ]; then
        echo "Folder '$folder_name' is a backup for the last week of the year. Keeping it." >> "$log_file"
        ((test++))
    fi

    if [ $test -eq 0 ]; then
        echo "Deleting folder '$folder_name' because it does not follows the specificied criteria." >> "$log_file"
        rm -rf "$folder_path/$folder_name"
    fi
}

check_sql_file() {
    local file_name=$1
    local test2=0

    # Extract the date part
    date_part=${file_name#sem5_pi_}
    date_part=${date_part%.sql}

    # Check if it's the first day of the month
    if [ "$(date -d "$date_part" +%d)" -eq 28 ]; then
        echo "File '$file_name' is a backup for the 28th of the month. Keeping it." >> "$log_file"
        ((test2++))
    fi
}

```

Figura 4- Extrato 1 script us850

```

fi
# Check if it is the month of december and it is the first day of the week
if [ "$(date -d "$date_part" +%m)" -eq 12 ] && [ "$(date -d "$date_part" +%u)" -eq 1 ]; then
    echo "File '$file_name' is a backup for the first day of December. Keeping it." >> "$log_file"
    ((test2++))
fi
# Check if it's the last week of the year
if [ "$(date -d "$date_part" +%W)" -eq 52 ]; then
    echo "File '$file_name' is a backup for the last week of the year. Keeping it." >> "$log_file"
    ((test2++))
fi
if [ $test2 -eq 0 ]; then
    echo "Deleting file '$file_name' because it does not follows the especificied criteria." >> "$log_file"
    rm -rf "$mysql_folder_path/$file_name"
fi
}

# Check if the folder exists
if [ -d "$folder_path" ]; then
    echo "Checking folders in $folder_path..."

    # Loop through each subfolder in the specified path
    for subfolder in "$folder_path"/*; do
        # Extract the folder name
        folder_name=$(basename "$subfolder")

        # Check the folder against the criteria
        check_folder "$folder_name"
    done
else
    echo "Error: Folder $folder_path does not exist."
fi

# Check if the folder exists
if [ -d "$mysql_folder_path" ]; then
    echo "Checking files in $mysql_folder_path..."

    for sql_file in "$mysql_folder_path"/*.sql; do
        # Extract the file name
        file_name=$(basename "$sql_file")

        # Check the file against the criteria
        check_sql_file "$file_name"
    done
else
    echo "Error: Folder $mysql_folder_path does not exist."
fi

```

Figura 5- Extrato 2 script us850

User Story 5

Requisitos

Como administrador de sistemas quero que o processo da US da cópia de segurança da DB seja mantido no log do Linux, num contexto adequado, e alertado o administrador no acesso à consola se ocorrer uma falha grave neste processo

Identificação do Problema

De que forma iremos notificar quando existir um problema grave no backup da base de dados

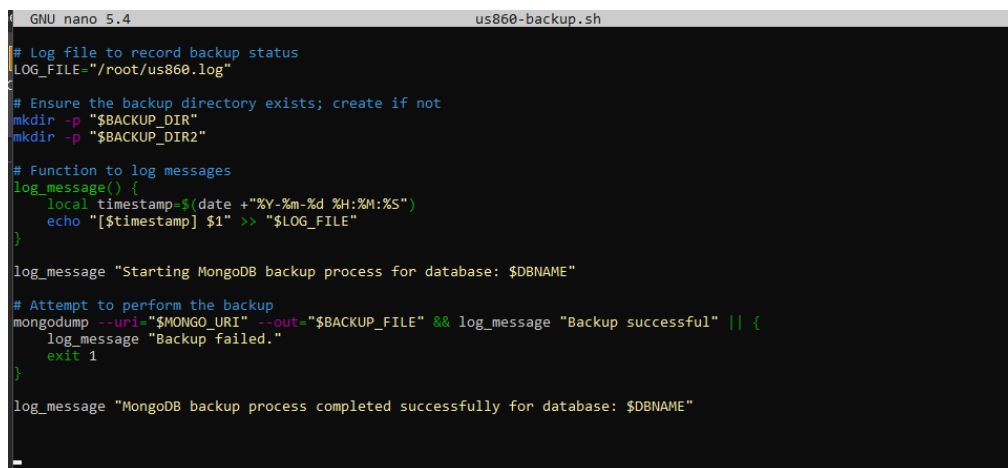
Desenho

Para a resolução deste problema iremos utilizar o script realizado para a UC840, que se trata do backup à base de dados, e iremos adicionar um script para verificar o conteúdo dos logs para efetivamente mostrar quando o administrador der login se houve alguma falha no backup.

Implementação

Alteração do Script de Backup

Para isto, adicionamos no final do ficheiro:



```
GNU nano 5.4 us860-backup.sh
# Log file to record backup status
LOG_FILE="/root/us860.log"

# Ensure the backup directory exists; create if not
mkdir -p "$BACKUP_DIR"
mkdir -p "$BACKUP_DIR2"

# Function to log messages
log_message() {
    local timestamp=$(date +"%Y-%m-%d %H:%M:%S")
    echo "[$timestamp] $1" >> "$LOG_FILE"
}

log_message "Starting MongoDB backup process for database: $DBNAME"

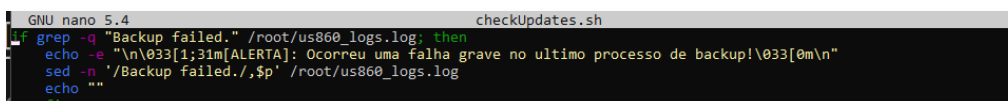
# Attempt to perform the backup
mongodump --uri="$MONGO_URI" --out="$BACKUP_FILE" && log_message "Backup successful" || {
    log_message "Backup failed."
    exit 1
}

log_message "MongoDB backup process completed successfully for database: $DBNAME"
```

Figura 6 - Configurações a adicionar no final do script.

Criação de Script checkUpdates

Este script irá verificar se o backup falhou, e se assim for, emitir uma notificação após o administrador realizar login no sistema:



```
GNU nano 5.4 checkUpdates.sh
if grep -q "Backup failed." /root/us860_logs.log; then
    echo -e "\n\033[1;31m[ALERTA]: Ocorreu uma falha grave no ultimo processo de backup!\033[0m\n"
    sed -n '/Backup failed./,p' /root/us860_logs.log
    echo ""
fi
```

Figura 7 - Script que verifica a falha do backup.

Iniciar o Script sempre que for efetuado login

Para isto acontecer, escrevemos no **.profiles** o caminho para o script, que seria: **/root/checkUpdates.sh**

User Story 6

Requisitos

Como administrador de sistemas quero que a cópia de segurança da US da cópia de segurança da DB tenha um tempo de vida não superior a 7 (sete) dias exceto no indicado na US de retenção das cópias mensais e anuais

Esclarecimentos do cliente

Questão: O que é que é pretendido por "a gestão dos ficheiros resultantes desse backup" no contexto desta US?

Resposta: O texto completo da US é: "Como administrador de sistemas quero que utilizando o Backup elaborado na US 840, seja criado um script que faça a gestão dos ficheiros resultantes desse backup, no seguinte calendário. 1 Backup por mês no último ano, 1 backup por semana no último mês, 1 backup por dia na última semana". Na US 840 são realizadas cópias de segurança de acordo com um dado critério. Com "gestão" pretende-se a eliminação dos backups que não obedeçam aos princípios enunciados.

Desenho

É importante que qualquer organização organize bem os seus backups, e que tenha os que realmente necessita disponíveis, porque ter backups além dos necessários, significa uma maior dificuldade na organização dos mesmos, e significa também maiores custos de armazenagem, o que para qualquer organização é negativo.

Resolução do Problema

Para resolver este problema, foi utilizado o script feito na User Story 4, uma vez que este já elimina todos os ficheiros de backup, que não foram realizados pelo próprio script. Uma outra forma de resolver este problema era criando um script que procurava dentro da pasta onde estão guardados os backups, aqueles que já haviam sido criados há mais de 7 dias, existindo uma condição "if" que ao fazer a distinção dos backups criados inicialmente e aqueles criados pela User Story 4, apenas apagaria os criados pelo script feito no sprint anterior. Para isto seria utilizado o comando "rm".

User story 7

Requisitos

Como administrador da organização quero que me seja apresentado um BIA (Business Impact Analysis) da solução final, adaptando se e onde aplicável o(s) risco(s) da US B4.

Esclarecimentos do cliente

Desenho

Este Business Impact Analysis (BIA) foi desenvolvido como parte do processo de planeamento de contingência para o sistema RobDroneGo. Foi concluído a 28 de dezembro de 2023.

Baseia-se no modelo NIST SP 800-34 Rev1.

1. Descrição do sistema

O sistema RobDroneGo gere uma frota de robots que executa tarefas no interior de um campus universitário, sendo as mesmas vigilância e entrega de objetos, seguindo um critério de otimização de modo a reduzir ao máximo a deslocação do robot dentro dos edifícios.,

Os servidores e as bases de dados encontram-se nas instalações do ISEP.

Serão feitos backups seguindo o RPO estabelecido, numa máquina virtual do DEI. Existe um sistema de autenticação e autorização permitindo aos utilizadores apenas executar as tarefas que lhes competem.

2. Recolha de dados BIA

2.1 Determinar processo e criticidade do sistema

| Missão/Processo de Negócios | Descrição |
|------------------------------------|---|
| Guardar backups das bases de dados | Fazer uma cópia dos dados do sistema para no caso de uma falha, ser possível repor os mesmos. |
| Visualizar percurso do Robot | Ter acesso visual ao trajeto percorrido pelo robot aquando na realização de determinada tarefa |
| Calcular percurso do Robot | Calcular de forma otimizada de modo a reduzir custos do robot, sejam eles energéticos como bateria ou a nível de hardware como o desgaste do mesmo. |
| Visualizar dados do negócio | Obter acesso aos edifícios, pisos, etc. e permitir a criação ou atualização dos mesmos. |
| Vigilância do campus | Vigilância do campus através de câmaras incorporadas nos robots. |
| Entrega de objetos | Entrega de objetos requisitados pelos docentes. |
| Limpeza dos pisos | Manter a higiene do campus. |

2.1.1 Identificar impactos de interrupções e downtime estimado

| Riscos | Desempenho da máquina | Perda de dados | Falha de segurança | Falha da VM | Má utilização da VM | Requisitos não compreendidos |
|------------|-----------------------|----------------|--------------------|-------------|---------------------|------------------------------|
| Categorias | | | | | | |

| | | | | | | |
|--------------|---|---|---|---|---|---|
| Operacional | | | | | | |
| Financeiro | | | | | | |
| Reputação | x | x | | x | | x |
| Segurança | | | x | x | x | |
| Clientes | x | x | x | x | | |
| Regulamentos | | | | | | |
| Desempenho | x | | | | x | x |
| Dados | | x | x | | | |
| Tempo | | | | | | |

Existem diversas categorias de impacto, mas de modo a selecionar as mais pertinentes foram utilizados os riscos da US B4 e a sua possível coligação.

Categorias de impacto:

- Reputação;
- Segurança;
- Clientes;
- Desempenho;
- Dados.

Valores de impacto:

- Severo- Irá envolver custos elevados tanto monetários como temporais, obtendo como exemplo a perda de dados, afetando assim a reputação da empresa afetando o seu estatuto podendo levar à falência da mesma. (Ex: 100000€)
- Moderado- Algo considerável que irá envolver algum trabalho por parte da equipa, mas será exequível. Podemos tomar como exemplo o desempenho do robô, irá envolver custos na sua melhoria, mas sem a melhoria o mesmo encontra-se funcional. (Ex: 25000€)
- Mínimo- Pequenos detalhes na aplicação como por exemplo validação de regras de negócio. (Ex: 1000€)

| Missão/Processo de negócios | Categorias de Impacto | | | | | Impacto |
|------------------------------------|-----------------------|-----------|----------|------------|--------|----------|
| | Reputação | Segurança | Clientes | Desempenho | Dados | |
| Guardar backups das bases de dados | Severo | Severo | Severo | Severo | Severo | Severo |
| Visualizar percurso do robot | Mínimo | Mínimo | Moderado | Moderado | Mínimo | Mínimo |
| Calcular percurso do robot | Moderado | Mínimo | Moderado | Moderado | Mínimo | Moderado |
| Visualizar dados do negócio | Severo | Mínimo | Moderado | Severo | Severo | Severo |

| | | | | | | |
|----------------------|--------|--------|----------|----------|--------|----------|
| Vigilância do campus | Mínimo | Severo | Mínimo | Mínimo | Mínimo | Mínimo |
| Entrega de objetos | Severo | Mínimo | Severo | Moderado | Mínimo | Moderado |
| Limpeza dos pisos | Mínimo | Mínimo | Moderado | Mínimo | Mínimo | Mínimo |

Definição:

MTD (Maximum Tolerable Downtime) – Quantidade total de tempo que os gestores estão dispostos a aceitar para uma interrupção de um processo de negócio.

RTO (Recovery Time Objective) – Período máximo que um recurso do sistema pode permanecer indisponível antes de haver um impacto inaceitável noutros recursos do sistema.

RPO (Recovery Point Objective) – Ponto no tempo, antes de uma interrupção no sistema, para o qual os dados do processo de negócio devem ser recuperados.

| Missão/Processo de Negócios | MTD | RTO | RPO |
|------------------------------------|----------|---------|----------|
| Guardar backups das bases de dados | 1/3 hora | ½ hora | ½ hora |
| Visualizar percurso do robot | 6 horas | 6 horas | 6 horas |
| Calcular percurso do robot | 3 horas | 3 horas | 3 horas |
| Visualizar dados do negócio | 2 horas | 1 horas | 1 hora |
| Vigilância do campus | 6 horas | 8 horas | 6 horas |
| Entrega de objetos | 2 horas | 1 hora | 1 hora |
| Limpeza dos pisos | 6 horas | 6 horas | 10 horas |

2.2 Identificar os requisitos de recursos

| Recurso/Componente do sistema | Plataforma/OS/Versão (conforme aplicável) |
|---------------------------------------|---|
| Base de dados de informação do campus | MongoDB 7.0.3 |
| Base de dados de utilizadores | MySQL 8 |
| Base de dados de tarefas | MongoDB 7.0.3 |
| Máquina virtual backups | Debian 12 |
| Máquina virtual deployment 1 | Debian 12 |
| Máquina virtual deployment 2 | Debian 12 |
| Máquina virtual Cluster | Debian 12 |
| Computadores pessoais | Windows e Linux |

2.3 Identificar prioridades de recuperação dos recursos do sistema

| Prioridade | Objetivo do tempo de recuperação |
|---------------------------------------|----------------------------------|
| Base de dados de informação do campus | ½ hora |
| Base de dados de utilizadores | ½ hora |
| Base de dados de tarefas | ½ hora |
| Máquina virtual backups | ½ hora |

| | |
|------------------------------|---------|
| Máquina virtual deployment 1 | 1 hora |
| Máquina virtual deployment 2 | 1 hora |
| Máquina virtual Cluster | 1 hora |
| Computadores pessoais | 4 horas |

2.4 Matriz de permissões com utilizadores do sistema e as suas tarefas

Existem 5 utilizadores de sistema, cada um com tarefas distintas. Existe um controlo de autorização e autenticação, isto é, o utilizador necessita de estar registado e ao efetuar o login irá ser gerado um JWT (Json Web Token) com a informação correspondente ao seu registo (email, cargo). Para verificar se tem permissões irá ser extraído o seu cargo do token e comparado com o seu role atribuído. Para executar determinadas tarefas necessita de aceder ao website e entrar no menu respetivo. Como mencionado anteriormente existem várias tarefas então apenas serão mencionadas as essenciais.

| Utilizadores | Tarefas |
|------------------------|--|
| Gestor de Utilizadores | Criar utilizador de sistema |
| Gestor de Utilizadores | Aprovar registos de utentes |
| Gestor de Campus | Criar um edifício |
| Gestor de Campus | Atualizar informação de um piso |
| Gestor de Campus | Listar passagens entre edifícios |
| Gestor de Tarefas | Aprovar ou recusar tarefas |
| Gestor de Tarefas | Obter uma sequência das tarefas a serem executadas |
| Gestor de Frota | Criar um robo |
| Gestor de Frota | Listar robots da frota |
| Utente | Download de um ficheiro JSON com os dados pessoais |
| Utente | Atualizar informações do utilizador |
| Utente | Eliminar conta do utilizador |

User Story 8

Requisitos

Como administrador da organização quero que seja implementada uma gestão de acessos que satisfaça os critérios apropriados de segurança.

Esclarecimentos do Cliente

Questão

Relativamente à US890 é pedido para "...implementar uma gestão de acessos que satisfaça os critérios apropriados de segurança", queria pedir informação sobre quais os critérios apropriados a ter em conta.

Resposta

Há tipos diferentes de utilizadores, pertencentes a grupos distintos. Cada grupo terá inerentemente um critério de segurança (tríade CIA) diferente, por certo - ainda que alguns possam ser iguais ou similares.

Deve implementar os mecanismos apropriados para assegurar os critérios para cada utilizador/grupo.

Questão

Quando refere gestão de acessos, é exatamente ao quê? A uma pasta? A um módulo da aplicação? Por exemplo, o administrador tem acesso a todos os módulos enquanto o Gestor de Campus tem acesso somente ao módulo de Gestão de Campus?

Resposta

A gestão de acessos é aos componentes do UI, pastas, dados, etc... Também é para os clientes internos (colaboradores) que possuem credenciais locais.

Como planeiam criar a ligação à(s) base(s) de dados? Sempre com as mesmas credenciais que tudo permitem ou credenciais diferentes? Como planeiam controlar e monitorizar os acessos internos às pastas e informação on store?

Desenho

Para a realização desta mesma, o cliente esclarece com uma das questões que cada utilizador tem um critério CIA diferente, critério este que envolve Confidencialidade, Integridade e Disponibilidade. Estes critérios são fundamentais para orientar as estratégias de segurança da informação.

Com base nos esclarecimentos obtidos, o grupo assumiu então que estes critérios de segurança se baseiam nestes 3 pontos principais.

Durante a realização do projeto, desde o Sprint A até este mesmo, já foram implementados alguns mecanismos de segurança que de acordo com os critérios CIA.

Alguns deles já implementados envolvem a configuração com o módulo PAM, bem como algumas user stories realizadas no Sprint B que condicionam o acesso à solução.

Outros mecanismos podem envolver manter o histórico de logins dos utilizadores, encriptação de passwords e realização de backups, também realizada em US do Sprint B e no Sprint C.

O exemplo do Last Login quando um utilizador faz conexão por ssh é um exemplo da utilização do histórico de logins:

```
C:\Users\Gabriel>ssh root@vs857.dei.isep.ipp.pt
root@vs857.dei.isep.ipp.pt's password:
Linux vs857 5.4.0-132-generic #148-Ubuntu SMP Mon Oct 17 16:02:06 UTC 2022 x86_64

Debian GNU/Linux 12

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Dec 11 19:41:33 WET 2023 from 10.8.211.146 on pts/1
Last login: Mon Dec 11 20:06:38 2023 from 10.8.211.150
root@vs857:~#
```

Figura 8 - Exemplo de Last Login realizado anteriormente noutra US.

Relativamente ao histórico de login dos utilizadores e à encriptação de passwords, o sistema é responsável por estes mesmos.

Para acedermos aos logs de autenticação acedemos a **/var/log/auth.log**:

```
GNU nano 7.2 var/log/auth.log
2023-12-10T00:02:01.282289+00:00 vs857 CRON[125797]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2023-12-10T00:02:02.06661+00:00 vs857 CRON[125797]: pam_unix(cron:session): session closed for user root
2023-12-10T00:04:01.067279+00:00 vs857 CRON[125814]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2023-12-10T00:04:01.787792+00:00 vs857 CRON[125814]: pam_unix(cron:session): session closed for user root
2023-12-10T00:06:01.795370+00:00 vs857 CRON[125831]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2023-12-10T00:06:02.821436+00:00 vs857 CRON[125831]: pam_unix(cron:session): session closed for user root
2023-12-10T00:08:01.829736+00:00 vs857 CRON[125849]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2023-12-10T00:08:02.672056+00:00 vs857 CRON[125849]: pam_unix(cron:session): session closed for user root
2023-12-10T00:10:01.676164+00:00 vs857 CRON[125866]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2023-12-10T00:10:02.434390+00:00 vs857 CRON[125866]: pam_unix(cron:session): session closed for user root
2023-12-10T00:12:01.442330+00:00 vs857 CRON[125932]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2023-12-10T00:12:02.297726+00:00 vs857 CRON[125932]: pam_unix(cron:session): session closed for user root
2023-12-10T00:14:01.303790+00:00 vs857 CRON[125951]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2023-12-10T00:14:02.084382+00:00 vs857 CRON[125951]: pam_unix(cron:session): session closed for user root
2023-12-10T00:16:01.160799+00:00 vs857 CRON[125968]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2023-12-10T00:16:02.034464+00:00 vs857 CRON[125968]: pam_unix(cron:session): session closed for user root
2023-12-10T00:17:01.042649+00:00 vs857 CRON[125985]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2023-12-10T00:17:01.047235+00:00 vs857 CRON[125985]: pam_unix(cron:session): session closed for user root
2023-12-10T00:18:01.055194+00:00 vs857 CRON[125988]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2023-12-10T00:18:01.036346+00:00 vs857 CRON[125988]: pam_unix(cron:session): session closed for user root
2023-12-10T00:20:01.043688+00:00 vs857 CRON[126006]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2023-12-10T00:20:02.695808+00:00 vs857 CRON[126006]: pam_unix(cron:session): session closed for user root
2023-12-10T00:22:01.703938+00:00 vs857 CRON[126023]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2023-12-10T00:22:02.429695+00:00 vs857 CRON[126023]: pam_unix(cron:session): session closed for user root
2023-12-10T00:24:01.436253+00:00 vs857 CRON[126040]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2023-12-10T00:24:02.256376+00:00 vs857 CRON[126040]: pam_unix(cron:session): session closed for user root
```

Figura 9 - Auth.log, que mantém o histórico de autenticação dos utilizadores.

A encriptação de passwords é feita pelo sistema também, encontra-se em **etc/shadow**:

```
GNU nano 7.2 shadow
root:$y$j9T$FDxQbY8j4Mk2.K48EM0w1$XuEvX88sGa16LsrXdfbgcRkEcOm877EHqHCR4MuYt0:19675:0:99999:7:::
daemon:*:19628:0:99999:7:::
bin:*:19628:0:99999:7:::
sys:*:19628:0:99999:7:::
sync:*:19628:0:99999:7:::
games:*:19628:0:99999:7:::
man:*:19628:0:99999:7:::
lp:*:19628:0:99999:7:::
mail:*:19628:0:99999:7:::
news:*:19628:0:99999:7:::
uucp:*:19628:0:99999:7:::
proxy:*:19628:0:99999:7:::
www-data:*:19628:0:99999:7:::
backup:*:19628:0:99999:7:::
list:*:19628:0:99999:7:::
irc:*:19628:0:99999:7:::
lapt:*:19628:0:99999:7:::
nobody:*:19628:0:99999:7:::
messagebus:!:19628:0:99999:7:::
systemd-network:!:19628:0:99999:7:::
systemd-resolve:!:19628:0:99999:7:::
sshd:!:19629:0:99999:7:::
Debian-exim:!:19671:0:99999:7:::
gestorFrota1:$y$j9T$QNEvt6P/ENqbcLwDXTX0$6IdfC0x.iReVtva7uUgHCAP6Q2u/3xMySEf1N1E01:19691:0:99999:7:::
gestorFrota2:!:19691:0:99999:7:::
gestorFrota3:!:19691:0:99999:7:::
```

Figura 10 - Exemplo de estrutura do aspeto di ficheiro shadow.

Para além destas regras implementadas, no nosso projeto também aplicamos o parâmetro de autorização de acesso, onde cada utilizador só tem acesso às funcionalidades que necessita consoante a sua função, ou seja, uma Role.

```
public async Task<RoleDto> AddAsync(CreatingRoleDto dto)
{
    try
    {
        var role = new Role(await GenerateId(), dto.Name);
        await this._repo.AddAsync(role);
        await this._unitOfWork.CommitAsync();

        return new RoleDto(role.Id.toInt(), role.Name.toString());
    }
    catch (BusinessRuleValidationException ex)
    {
        throw new BadRequestException(ex.Message);
    }
}
```

Figura 11 - Utilização da Role para cumprir o parâmetro de autorização de acesso.

Já para as políticas de acesso, estabelece-se algumas regras para a utilização dos recursos na organização, de entre elas destacam-se, por exemplo, não utilizar em circunstância alguma a conta de outro funcionário da empresa; se encontrar algum problema técnico, informar um administrador para que este possa contactar a equipa de desenvolvimento do projeto; Em caso de algum problema de conexão com um dos servidores, contactar a equipa de manutenção.

User story 9

Requisitos

Como administrador da organização quero que seja implementado de forma justificada um sistema de *clustering* entre os sistemas que implementam o SPA.

Esclarecimentos do cliente

Questão

Could you clarify the purpose of the clustering system US900 requirement?

Resposta

It seems to me that if SPA fails, everything fails, as users will no longer be able to access the user interface. As so, clustering must be configured to avoid that SPOF. It can be in failover or load balancing, however some clustering method should be deployed.

Desenho

Sistemas e ferramentas

Os servidores utilizados têm o sistema operativo Debian, isto por serem sistemas mais leves (CLI) e com ferramentas muito mais avançadas e sofisticadas que as do Windows. Como tal optou-se por usar *HAProxy* como controlador do *cluster*.

Número de servidores + backup

A equipa optou por utilizar dois servidores para distribuir o trabalho e caso um dos servidores esteja em baixo, o outro servirá de backup.

Algoritmo de balanceamento

O algoritmo selecionado foi o *Round Robin*, que vai redirecionar os pedidos, sequencialmente, para cada um dos servidores. Foi escolhido este método devido à capacidade similar de processamento dos servidores.

Ficheiro de configuração HAProxy

```
listen http_proxy

    maxconn 10
    log /dev/log local0
    bind *:5432
    stats enable
    mode http
    option httpclose
    option forwardfor
    balance roundrobin

    # timeout client 10s
    # timeout server 30s
    # timeout connect 5s

    server S1 vs857.dei.isep.ipp.pt:4200 check
    server S2 vs721.dei.isep.ipp.pt:4200 check
```

Figura 12 - Ficheiro de configuração HAProxy

É utilizado o url “<http://10.9.22.42:5432/haproxy?stats>” para analisar estatísticas.

User Story 10

Requisitos

Como administrador de sistemas quero que o administrador tenha um acesso SSH à máquina virtual, apenas por certificado, sem recurso a password.

Esclarecimentos do cliente

Questão: By "access to the virtual machine, only through a certificate", do you mean utilizing SSH Key Pair or something else?

Resposta: Yes, the SSH Key Pair

Desenho

Para solucionar este requisito, foi necessário recorrer a um comando que executa um algoritmo de cifragem. Segue agora uma lista de passos da resolução deste problema.

1. Na máquina do administrador, gerar um par de chave pública e privada com o comando: `"ssh-keygen -t rsa"` e definir a palavra-passe para a utilização deste certificado (que no caso é "uc10");
2. Como foi especificado um diretório personalizado, vai ser necessário alterar as permissões (apenas para `root`) destes ficheiros por motivos de segurança, através dos comandos:
 - a. `"sudo chown root:root ~/openssh_keys/key";`
 - b. `"sudo chown root:root ~/openssh_keys/key.pub";`
 - c. `"sudo chmod 700 ~/openssh_keys/key";`
 - d. `"sudo chmod 700 ~/openssh_keys/key.pub".`
3. No diretório `"/.ssh/"` existe um ficheiro designado por `"authorized_keys"` (contém todas as `keys` com permissão para fazer `ssh` através de um certificado) deve ser colocada a chave pública gerada pela máquina do administrador;
4. Como neste caso foi optado por guardar as chaves geradas num diretório personalizado é necessário especificar o caminho para a chave privada ao executar o comando `"ssh"` e utilizar a `flag` de "ficheiro de identidade", ou seja: `"sudo ssh -i ~/openssh_key/key root@vs857.dei.isep.ipp.pt"`, finalmente, insere-se a palavra-passe definida e mencionada no 1º passo. Nota: Esta palavra-passe é opcional na geração da chave, porém é fortemente aconselhada por motivos de segurança.

```
richard22@DESKTOP-P73C7UR:~/openssh_key$ sudo ssh -i ~/openssh_key/key root@vs857.dei.isep.ipp.pt
Enter passphrase for key '/home/richard22/openssh_key/key':
Linux vs857 5.4.0-132-generic #148-Ubuntu SMP Mon Oct 17 16:02:06 UTC 2022 x86_64

Debian GNU/Linux 12

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Nov 30 15:23:20 2023 from 10.8.198.20
root@vs857:~#
```

Figura 13 - Demonstração por acesso a SSH sem password.

User Story 11

Requisitos

Como administrador de sistemas quero que para agilização entre as várias equipas seja criada uma partilha pública de ficheiros, formato SMB/CIFS ou NFS.

Esclarecimentos do Cliente

Questão

A pasta pública CIFS/SMB que pretende que seja criada, deverá ser de leitura apenas, ou pretende que os utilizadores (presume-se que qualquer pessoa não administrativa) possa aceder e escrever novos conteúdos na pasta?

Resposta

A US é (propositadamente) omissa nesse ponto. O que imaginam que será colocado na pasta partilhada? Instruções de funcionamento do jogo e/ou da aplicação, ou algo similar (avisos aos utilizadores registados, etc.)? Se sim, deverá ser apenas de escrita.

Desenho

Para a resolução deste problema foi pensado no formato SMB, visto que já existe conhecimento prévio sobre o mesmo, para atribuir diferentes permissões às equipas, com recurso também às extended libraries do Linux (ACL).

Utilizaremos também a pasta pública criada no Sprint B, e efetuaremos as respetivas alterações na mesma para estar de acordo com o pedido pelo cliente.

Implementação

Instalação do Package ACL

Para esta instalação, tudo o que necessitamos fazer é:

sudo apt-get install acl

Criação de grupos e utilizadores para testar funcionalidade

São criados 3 grupos para a demonstração com os respetivos nomes:

- gestoresCampus
- gestoresFrota
- administradoresSistema

Para cada um destes grupos, vamos ter 1 utilizador de teste por grupo, por exemplo:

- gestorCampus1
- gestorFrota1
- adminSist1

Alteração de passwords dos utilizadores

Configuramos as passwords através do comando:

smbpasswd utilizadorPretendido

Definir lista de controlo de acesso através do setfacl

Agora que os utilizadores se encontram configurados, definimos as permissões para cada grupo através do setfacl para a pasta pretendida (já criada no sprint B):

```
setfacl -m g:gestoresFrota:r /public
```

```
setfacl -m g:gestoresCampus:rx /public
```

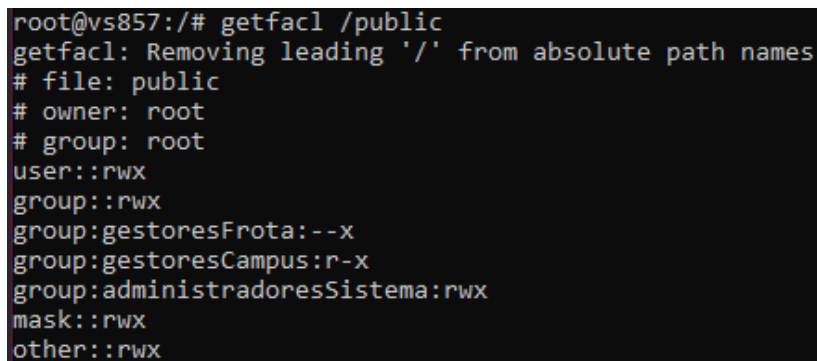
```
setfacl -m g:administradoresSistema:rwx /public
```

Cada grupo tem permissões diferentes.

Executar o getfacl

Executamos este comando para verificar se as permissões foram corretamente atribuídas:

getfacl /public

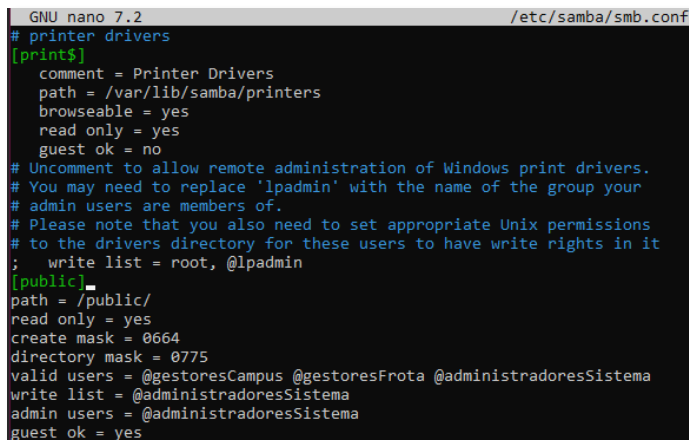


```
root@vs857:/# getfacl /public
getfacl: Removing leading '/' from absolute path names
# file: public
# owner: root
# group: root
user::rwx
group::rwx
group:gestoresFrota:--x
group:gestoresCampus:r-x
group:administradoresSistema:rwx
mask::rwx
other::rwx
```

Figura 14 - Getfacl, mostrando as permissões de cada grupo de utilizadores para a pasta partilhada.

Alteração do ficheiro smb.conf

Após a instalação do package, adicionamos no final do ficheiro as seguintes configurações:



```
GNU nano 7.2 /etc/samba/smb.conf
# printer drivers
[print$]
comment = Printer Drivers
path = /var/lib/samba/printers
browseable = yes
read only = yes
guest ok = no
# Uncomment to allow remote administration of Windows print drivers.
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
; write list = root, @lpadmin
[public]
path = /public/
read only = yes
create mask = 0664
directory mask = 0775
valid users = @gestoresCampus @gestoresFrota @administradoresSistema
write list = @administradoresSistema
admin users = @administradoresSistema
guest ok = yes
```

Figura 15 - Configurações no ficheiro smb.conf para a realização da US.

Reiniciar o serviço

Após guardarmos as alterações do ficheiro, reiniciamos o serviço através de:

service smb restart

Verificar conexões à pasta partilhada

Por último, verificamos o acesso de cada utilizador e as suas respectivas permissões à pasta.

Por exemplo, se efetuarmos login com o gestorCampus1, apenas temos permissões de leitura e execução, logo não podemos escrever na pasta, aparecendo a seguinte mensagem:

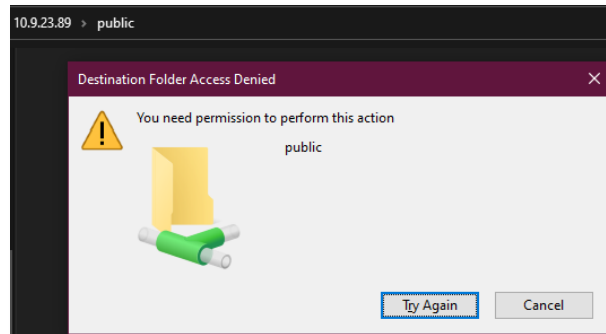


Figura 16 - Acesso negado a escrita para utilizadores que sejam gestores de Campus.

Para os Administradores de sistema, já é possível criar ficheiros dentro da pasta, bem como apagar outros ficheiros.

User Story 12

Requisitos

Como administrador de sistemas temos de garantir que em caso de necessidade os backups foram efetuados corretamente. Para isso devemos automatizar a sua reposição, validando no final o funcionamento do sistema (Ex. Base de Dados - executar uma query SQL com sucesso após reposição)

Esclarecimentos do Cliente

Questão: O que se pretende em concreto neste requisito? é relativo à US840? O objetivo é comparar o backup com a base de dados?

Resposta: Não exclusivamente. A menção à DB é apresentada como um exemplo. O pretendido é definir um procedimento para validar que em caso de necessidade de reposição não se obtém a surpresa desagradável de verificar que o backup não foi realizado com sucesso. Como exemplo - aliás, apresentado como tal na US - repor a DB ou parte dela para outro local e validar se os dados estão conformes. Claro que há outros métodos, como faz para verificar se o backup dos seus dados foi feito com sucesso?

Desenho

É necessário a reposição de dados através de um backup em caso de uma falha num sistema. Existem diversas maneiras, mas a mais eficiente será a execução de uma query à base de dados.

Resolução do problema

O primeiro passo foi instalar o mongodb server e mongodb shell de modo a ter acesso à base de dados e ser possível executar queries. O mesmo com a base de dados de mysql.

Para resolver este problema foi criado um script que irá fazer o restore da base de dados através do comando mongorestore. Este comando irá estar envolvido dentro de uma condição if e o seu valor de retorno determinará o sucesso ou insucesso da operação. Após sucesso da reposição dos dados uma query será feita através do comando mongosh. Ambos os resultados serão dispostos num ficheiro de logs. O mesmo será realizado na base de dados relacional de MySQL.

```
#!/bin/bash

# MongoDB connection details
COLLECTION="tarefas"
HOST="vsgate-s1.del.isep.ipp.pt"
PORT="10242"
USERNAME="mongoadmin"
PASSWORD="mcdb452db3a82201f874542"
BACKUP_FOLDER="/root/bin/mongodumptotal/test_20231228"
LOG_FILE="/root/us930_logs.log"

# MongoDB query
QUERY='{}'

# Execute the query using mongosh
if mongorestore --host "$HOST" --port "$PORT" --username "$USERNAME" --password "$PASSWORD" "$BACKUP_FOLDER" >> "$LOG_FILE" 2>&1; then
    result=$(mongosh --host "$HOST" --port "$PORT" --username "$USERNAME" --password "$PASSWORD" --quiet --eval "db.$COLLECTION.find($QUERY)")
    echo "Query result: $result" >> "$LOG_FILE"
    echo "Mongorestore success" >> "$LOG_FILE"
else
    echo "Mongorestore failed" >> "$LOG_FILE"
fi

# MySQL connection details
MYSQL_USER="root"
MYSQL_HOST="vsg1220.del.isep.ipp.pt"
DATABASE_NAME="sem5_pi"
MYSQL_PASSWORD="W/ISRoQWz33"
DUMP_FILE="/root/bin/mysqldumptotal/sem5_pi_20231228.sql"

if mysql -h "$MYSQL_HOST" -u "$MYSQL_USER" -p "$MYSQL_PASSWORD" "$DATABASE_NAME" < "$DUMP_FILE" >> "$LOG_FILE" 2>&1; then
    result=$(mysql -h "$MYSQL_HOST" -u "$MYSQL_USER" -p "$MYSQL_PASSWORD" "$DATABASE_NAME" -e "SELECT * FROM Pedidos")
    echo "Query result: $result" >> "$LOG_FILE"
    echo "MySQL restore success" >> "$LOG_FILE"
else
    echo "MySQL restore failed" >> "$LOG_FILE"
fi
```

Figura 17- Extrato script us930