Relatório de ASIST

SPRINT 3

Turma 3DE _ Grupo 032
1200616 - João Silva
1190519 – Diogo Marques
1191606 – Pedro Marques
1202054 – Tiago Ribeiro

Data: 08/01/2023

User Stories:

- **1**

Objetivo:

"Como administrador da organização quero um plano de recuperação de desastre que satisfaça o MBCO definido na US B5."

Resolução:

Um plano de recuperação de desastre (DRP) é um documento que descreve as ações a serem tomadas em caso de interrupção dos negócios devido a um desastre. O objetivo do plano de DRP é garantir que a empresa possa retomar as atividades o mais rapidamente possível, como demonstrado na US B5, a nossa organização apenas irá considerar desastre que possam acontecer na aplicação. Este plano está elaborado em várias partes:

- Métricas relativas ao tempo: Recovery Point Objective (RPO) e Recovery Time Objective (RTO);
- Registo de pessoas responsáveis no plano;
- Listagem dos aplicativos e/ou equipamentos necessários para um funcionamento correto da organização;
- Procedimentos de backup;
- Procedimentos de recuperação de serviços;
- Locais para a recuperação dos desastres;
- Procedimentos de restauro.

No primeiro ponto estas duas métricas são fundamentais para o DRP. O Recovery Point Objective (RPO) é uma métrica que mede a quantidade de dados que podem ser perdidos durante uma interrupção antes que isso tenha um impacto significativo na empresa. Portanto a nossa aplicação regista um RPO de 4 horas, isso significa que o sistema pode perder até 4 horas de dados sem causar danos significativos à empresa. O Recovery Time Objective (RTO) é uma métrica que mede o tempo que leva para restaurar um sistema ou serviço após uma interrupção, a fim de atender às necessidades da empresa. A nossa aplicação tem um RTO de 1 horas, isso significa que o sistema deve

ser restaurado dentro de 1 horas após uma interrupção para atender às necessidades da empresa.

No segundo ponto, as pessoas responsáveis por este plano são as que fazem parte deste grupo. A equipa realiza 1 teste de DRP por ano em conjunto. Através desta testagem é possível criar um plano bem definido com todos os procedimentos e alternativas para a recuperação dos serviços da organização.

Relativamente ao terceiro ponto a nossa organização necessita de vários equipamentos e aplicativos como é o caso de serviço de nuvem que são necessários para uma operação diária, como o uso de computadores, routers, base de dados principal e secundária e serviços da app da organização.

Relativamente ao quarto ponto, os procedimentos de backup contam com os dispositivos, pastas e arquivos e a forma como a recuperação deve ser feita através da base de dados de suporte. Os trabalhadores com permissões de administração desta base de dados tratam da transferência de todos os dados desde o último backup. De acordo com o MBCO, é possível utilizar 90% dos dados totais.

Relativamente ao quinto ponto, os procedimentos de recuperação de serviços tratam da recuperação das componentes da aplicação. Para isso, a nossa organização em conjunto implementou um sistema de failover em cluster- cluster ativo/passivo. Assim, na falha de algum serviço do servidor/aplicação principal, o servidor/aplicação de failover assume e executa as suas funcionalidades estando em constante monotorização.

Por fim, e relativamente ao sétimo ponto, os procedimentos de restauro podem ser diferentes mediante os contextos de desastre.

- **2**

  Objetivo:

  "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."

  Resolução:

  Para assegurar um *Maximum Tolerable Downtime* de 20 minutos, existem várias alterações que podem ser consideradas na infraestrutura. Exemplos de alterações que devem ser efetuadas:

  - Implementação de sistemas de backup e recuperação de desastres, que permitem recuperar rapidamente os serviços em caso de falha.
  - Adotar uma arquitetura de alta disponibilidade para minimizar o tempo de inatividade e garantir a disponibilidade contínua dos serviços. Como, por exemplo, a implementação de um sistema de balanceamento de carga para efetuar a sua distribuição entre os vários servidores e garantir que haja sempre um servidor disponível para atender às necessidades requeridas.
  - Realização de testes de recuperação de desastres regularmente para garantir que os sistemas de backup e recuperação de desastres estão a funcionar corretamente e garantir que os procedimentos de recuperação são eficientes.
  - Monitorização da infraestrutura de forma proativa para ajudar a identificar problemas antes que eles ocorram e tomar medidas preventivas para evitar falhas, isto é, utilizar ferramentas de monitorização de rede e sistemas para identificar potenciais problemas e corrigi-los antes que estes causem interrupções.

- **3**

Objetivo:

“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.”

Resolução:

Para criar um script que realizasse uma cópia de segurança de uma base de dados MySQL e uma base de dados MongoDB e as enviasse para um ambiente de Cloud no Azure, um possível caminho seria:

Criar um script utilizando o comando ‘mysqldump’ para realizar a cópia de segurança da base de dados MySQL:

```
# Warehouse Database backup
mysqldump -u node -p node123 --databases mysqldb > mysqldb_backup.sql
```

Criar um script utilizando o comando ‘mongodump’ para realizar a cópia de segurança da base de dados MongoDB:

```
# Logistics Database backup
mongodump -u node -p node123 -d mongodb -o mongodb_backup
```

Adicionar ao script uma etapa que renomeie as cópias de segurança com o formato desejado, utilizando o nome da DB, o ano, o mês e o dia da realização da cópia de segurança. Isso pode ser feito, por exemplo, utilizando o comando "mv" do shell para renomear o arquivo de backup gerado:

```
# Rename backups with current date
DATE=$(date +%Y%m%d)
mv mysqldb_backup.sql mysqldb_$DATE.sql
mv mongodb_backup mongobd_$DATE
```

Adicionar ao script uma etapa que envie as cópias de segurança renomeada para o ambiente de cloud. Isso pode ser feito, por exemplo, utilizando a ferramenta rsync para sincronizar o arquivo de backup com uma pasta no ambiente de cloud:

```
# Send to Cloud
rsync -avz --port=10743 mysqldb_$DATE.sql root@vsgate-ssh.dei.isep.ipp.pt:/db_backups/mysql

rsync -avz --port=10743 mongodb_$DATE root@vsgate-ssh.dei.isep.ipp.pt:/db_backups/mongodb
```

- **4**

Objetivo:

“Como administrador de sistemas quero que utilizando o Backup elaborado na US C3, seja criado um script quer 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.”

Resolução:

Para fazer a gestão dos ficheiros resultantes usamos o crontab que é uma ferramenta utilizada para agendar tarefas no sistema. Inicialmente, para abrir o crontab usamos o seguinte comando: crontab -e. De seguida adicionamos ao ficheiro as seguintes linhas:

```
# Backup mensal no último ano
0 0 1 */1 * /db_backups/mysql
0 0 1 */1 * /db_backups/mongodb

# Backup semanal no último mês
0 0 * */1 * /db_backups/mysql
0 0 * */1 * /db/backups/mongodb

# Backup diário na última semana
0 0 * * */1 /db_backups/mysql
0 0 * * */1 /bd_backups/mongodb
```

Portanto, serão agendados os devidos backups para cada base dados.

- **6**

Objetivo:

“Como administrador de sistemas quero que a cópia de segurança da US C3 tenha um tempo de vida não superior a 7 (sete) dias exceto no indicado na US C4.

Resolução:

Para garantir que as cópias de segurança anteriores tenham um tempo de vida não superior a 7 dias, um possível caminho seria adicionar uma etapa ao script que remova as cópias de segurança mais antigas. Isso pode ser feito, por exemplo, utilizando o comando "find" do shell para localizar os arquivos de backup mais antigos que 7 dias e o comando "rm" para removê-los.

Para remover as cópias de segurança do MySQL que tenham mais de 7 dias, a etapa poderia ser assim:

```
#Delete 7 day old copies
find /db_backups/mysql -name "mysql_*" -mtime +7 -delete
```

Para remover as cópias de segurança do MongoDB que tenham mais de 7 dias, a etapa poderia ser assim:

```
find /db_backups/mongodb -name "mongodb_*" -mtime +7 -delete
```

O comando "find" procura por arquivos ou pastas no caminho especificado cujo nome comece com "nome_da_db_" e que tenham sido modificados há mais de 7 dias (-mtime +7). O comando "-delete" remove esses arquivos ou pastas encontradas.

- **8**

Objetivo:

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

Resolução:

Existem várias maneiras de implementar uma gestão de acessos eficiente e segura. Uma delas é definir políticas de senhas fortes. Para criar políticas de senhas fortes, usamos a ferramenta "pwquality" para verificar a força das senhas dos usuários.

Pwquality é uma ferramenta de linha de comando que pode ser usada para validar a força de senhas. É comumente utilizada em sistemas Linux e pode ser usada para garantir que os usuários definam senhas fortes e seguras.

Para usar a ferramenta pwquality tivemos primeiro de a instalar na máquina virtual.

```
isep@isep-scomp2018:~$ sudo apt-get install libpwquality-tools
[sudo] password for isep:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  libpwquality-tools
0 upgraded, 1 newly installed, 0 to remove and 191 not upgraded.
Need to get 9348 B of archives.
After this operation, 86,0 kB of additional disk space will be used.
Get:1 http://pt.archive.ubuntu.com/ubuntu xenial/universe amd64 libpwquality-too
ls amd64 1.3.0-0ubuntu1 [9348 B]
Fetched 9348 B in 0s (93,4 kB/s)
Selecting previously unselected package libpwquality-tools.
(Reading database ... 212963 files and directories currently installed.)
Preparing to unpack .../libpwquality-tools_1.3.0-0ubuntu1_amd64.deb ...
Unpacking libpwquality-tools (1.3.0-0ubuntu1) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up libpwquality-tools (1.3.0-0ubuntu1) ...
isep@isep-scomp2018:~$
```

Se a senha for considerada forte, o código de saída será uma percentagem de quão forte será a password e nenhuma mensagem de erro será exibida. Se a senha não for forte o suficiente, será exibida uma mensagem de erro explicando o problema.

Para testar a password usamos o comando “pwscore”.

```
isep@isep-scomp2018:~$ pwscore
minhasenha123
78
isep@isep-scomp2018:~$ pwscore
MinhaSenha!"$43
100
```

Se a senha for inválida apresenta uma imagem de erro como mostra a figura.

```
isep@isep-scomp2018:~$ pwscore
hello
Password quality check failed:
 The password is shorter than 8 characters
isep@isep-scomp2018:~$ pwscore
qwertyui
Password quality check failed:
 The password fails the dictionary check - it is based on a dictionary word
```

- **10**

  Objetivo:

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

  Resolução:

  Primeiro geramos um par de chaves publica/privada usando o comando:

  ssh-keygen –t rsa

A opção -t significa type e o RSA é o protocolo utilizado. A chave é de 2048 bits. O administrador deve escolher uma senha para proteger a chave privada, mas essa senha não será necessária para a conexão SSH.

A segunda etapa é usar o comando ssh-copy-id:

```
ssh-copy-id root@localhost
```

Uma vez que a autenticação seja sucedida a chave publica do ssh gerada será adicionada ao arquivo de chaves autorizada da máquina, ssh/authorized_keys.

Edite o arquivo de configuração do SSH na máquina virtual para desabilitar a autenticação por senha. Para fazer isso, abra o arquivo /etc/ssh/sshd_config e altere a seguinte linha: PasswordAuthentication no

Reinicie o serviço SSH na máquina virtual para que as alterações entrem em vigor. Isso pode ser feito com o comando: systemctl restart ssh.

Para testar uso o comando: ssh root@localhost e o login será feito sem a necessidade de usar a password.

- **11**

  Objetivo:

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

  Resolução:

  Foi escolhido o formato NFS para partilha de pastas.

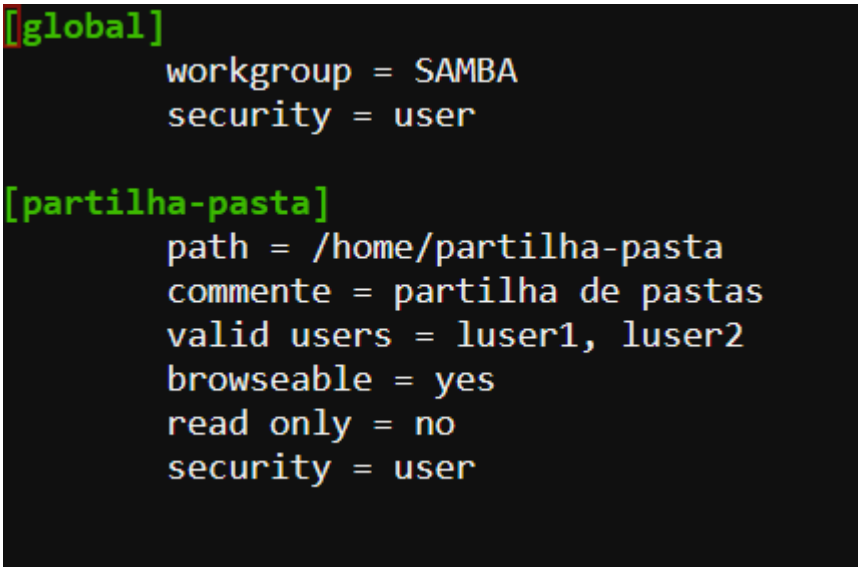
  - Para começar temos de instalar o Samba, usando o comando:

  apt install samba

  - De seguida executei o comando systemctl status smbd para ver se o Samba estava a funcionar.

  Apos ver que estava a funcionar vamos configurar.

- Foi para o diretirio /etc/samba com o comando cd /etc/samba
- Copiei o ficheiro smb.conf para poder ter um backup do ficheiro pois eu vou alterar o ficheiro smb.conf, a copia foi feita através do comando cp smb.conf smb.conf.backup
- Em seguida alterei o ficheiro smb.conf e coloqui o seguinte



Para explicar o path é o caminho da pasta partilhada, o comment é um comentário, valid users são os usuários que terão acesso, o browseable é para poder por a pasta visível, caso seja yes, ou não para o usuário, o read only é para dizer se só é de leitura ou se também se tem permissão de escrita e para terminar o security que diz que os usuários validos é que podem aceder a pasta.

- Em seguida fazemos um restart no serviço com o comando systemctl restart smbd
- Em seguida vou para o diretorio /home fazendo cd /home e crio a pasta partilha-pasta com o comando mkdir partilha-pasta
- Agora criamos os usuários dentro do samba através do comando smbpasswd –a luser1 e também para o usuário luser2 smbpasswd –a luser2
- Em seguida vou dar permissão para o usuário poder ter acesso a pasta partilha-pasta com o comando chown luser1: luser1 pasta-partilhada sendo o luser1 o usuario e o luser1 depois do dois pontos o grupo.

Neste passo o luser1 é um usuário do servidor Linux não é o Samba.

Pode criar o usuário através do comando adduser luser1.

- Volto a dar restart ao serviço

Resultado:

Eu testei no meu próprio computador. Pressionei a tecla Windows mais r e coloquei \\10.9.23.19 sendo o 10.9.23.19 o ip do servidor Linux, obtido através do comando ifconfig, pressiono ok e aparece uma janela a pedir para autêntica. Para autenticar eu usei o luser1 e a sua password para depois ser direcionado para a pasta partilhada, onde criei um ficheiro chamado teste que continha a seguinte frase: correu bem.

Em seguida no servidor Linux foi a diretório home/partilha-pasta e verifiquei que a o ficheiro teste estava lá e com o mesmo conteúdo como se pode ver nas imagens a seguir.