

Uma imagem com alimentação

Descrição gerada automaticamente

**Relatório de ASIST**

**SPRINT 3**

**Turma 3DGH \_ Grupo 02**

1191008 Rodrigo Rodrigues

1201564 Jorge Ferreira

1201566 Rafael Leite

1201568 Rui Pina

**Data: 08/01/2023**

Índice

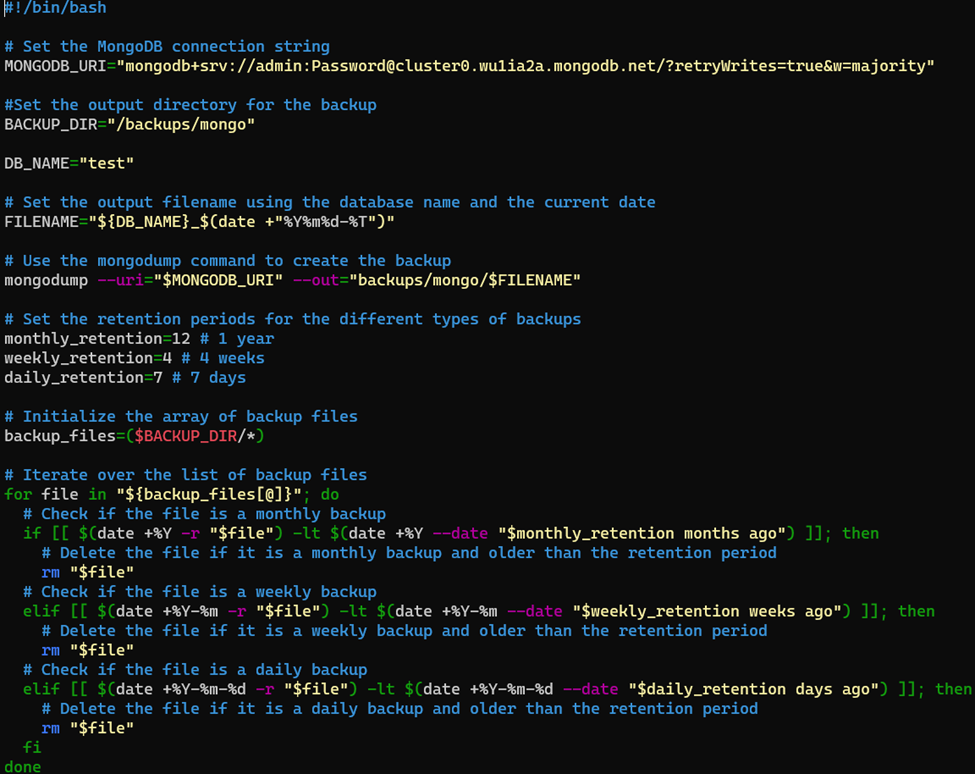
[**10. Como administrador de sistemas quero que o administrador tenha um acesso SSH à máquina virtual, apenas por certificado, sem recurso a password. 1201564 6**](#_Toc122188456)

# 3. 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 \_yyyymmdd sendo 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. 1201568

# Uma imagem com texto Descrição gerada automaticamente

1. Estou a estabelecer uma ligação à base de dados MongoDB com uma string de ligação e um nome de utilizador e senha.
2. Estou a definir um diretório de backup para onde os backups da base de dados serão guardados.
3. Estou a usar o comando "mongodump" para criar um backup da base de dados e a guardá-lo no diretório de backup com um nome que inclui o nome da base de dados e a data atual.

# 4. 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. 1201568



1. Estou a definir períodos de retenção para diferentes tipos de backups (mensais, semanais e diários).
2. Estou a inicializar um array de ficheiros de backup com todos os ficheiros no diretório de backup.
3. Estou a iterar sobre a lista de ficheiros de backup e a verificar se cada um deles é um backup mensal, semanal ou diário.
4. Se o ficheiro for mais velho do que o período de retenção correspondente, estou a apagar o ficheiro.

# 5 .Como administrador de sistemas quero que o processo da US C3 seja mantido no log do Linux, num contexto adequado, e alertado o administrador no acesso à consola se ocorrer uma falha grave neste processo. 1201566

Uma imagem com texto

Descrição gerada automaticamente

Para a realização desta US peguei no script criado para a USC3 e adicionei logs ao script, através da utilização do comando ‘logger’, neste caso para avisar o administrador utilizei a facility user para todas as mensagens, para avisar o administrador no caso de erro utilizei o severity level alert, e para os outros utilizei o severity level info.



Exemplo de logs gerados pelo script, localizados no ficheiro user.log em /var/log



Regra adicionada ao rsyslog.conf de forma a que o utilizador root ou admin receba uma mensagem caso haja um erro.

# 6 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. 1201566



Para realizar esta US utilizei o crontab que às 00:00 H realiza um script que apaga os backups que foram criados à 7 dias ou mais.

Uma imagem com texto

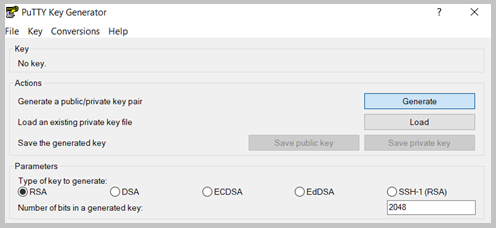
Descrição gerada automaticamente

O script encontra todos os ficheiros com 7 dias ou mais e apaga-os

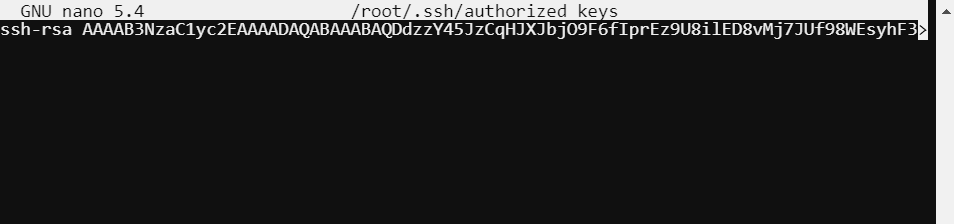
# 10. Como administrador de sistemas quero que o administrador tenha um acesso SSH à máquina virtual, apenas por certificado, sem recurso a password. 1201564

Para resolver esta User Story, recorri ao PuTTY pois facilita o meu trabalho, já que tem uma interface gráfica e uma funcionalidade de gerar keys.

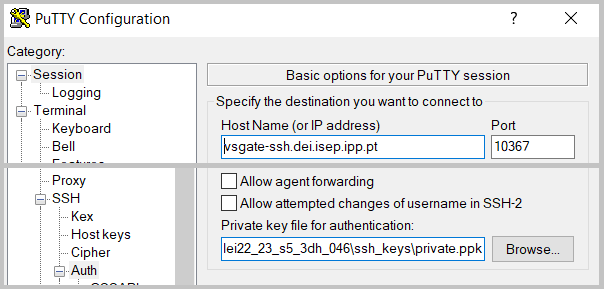
**1. Gerar e guardar um par de chaves pública/privada (Generate) -> (Save public key & Save private key).**

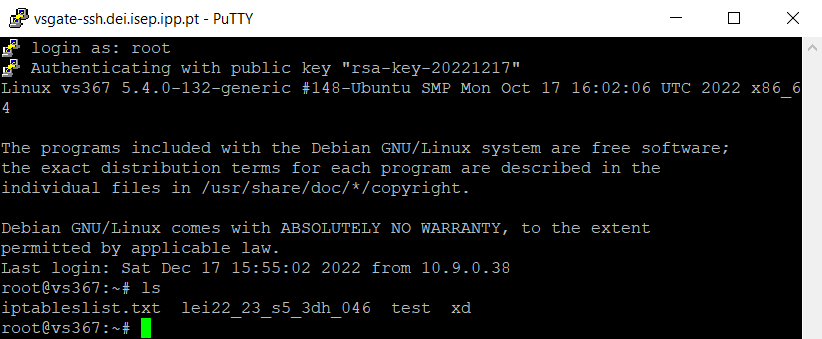


**2. Inserir a chave pública no arquivo ssh/authorized\_keys da VM do DEI.**

****O arquivo authorized\_keys especifica as chaves SSH que podem ser usadas para fazer login na conta do utilizador para a qual o arquivo está configurado, neste caso **root**.

**3. Iniciar sessão SSH.**

Inserir IP e Port corretas da máquina virtual do DEI e nas definições SSH -> utilizar a chave privada para a autenticação.

**4. A sessão SSH é iniciada, sem ser necessário inserir uma password, tal como era pretendido.**

# 11.   Como administrador de sistemas quero que para agilização entre as várias equipas seja criada uma partilha pública de ficheiros, formato SMB/CIFS ou NFS. 1201564

1. **Para resolver esta User Story, comecei por instalar o samba na máquina virtual**

sudo apt-get install samba

1. **Criei a pasta para partilha, com sub-pastas pública e privada.**

mkdir /media/samba

mkdir /media/samba/public

mkdir /media/samba/private

1. **Criei um grupo de utilizadores ao qual pertence a pasta private**

groupadd smbgrp

useradd user1

usermod -aG smbgrp user1

chgrp smbgrp /media/samba/private

smbpasswd -a user1 (para criar password)

1. **Alterei o ficheiro de configuração do samba nano /etc/samba/smb.conf para o desejado**

[global]

workgroup = WORKGROUP

security = user

map to guest = bad user

wins support = no

dns proxy = no

[public]

path = /media/samba/public

guest ok = yes

force user = nobody

browsable = ye

writable = yes

[private]

path = /media/samba/private

valid users = @smbgrp

guest ok = no

browsable = yes

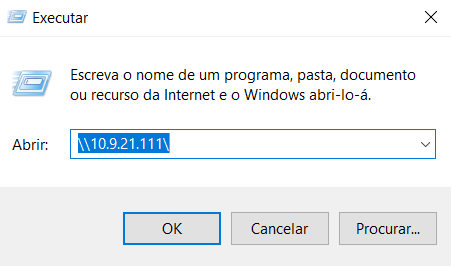
writable = yes

1. **Inicio/Paragem do serviço Samba**

sudo service smbd start

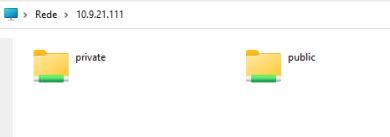
sudo service smbd stop

1. **Acesso via windows**

****

**Para aceder à pasta private, é necessário inserir password, já a pasta publica tem livre acesso.**

**É possível inserir ficheiros de forma a permitir a troca de informações entre a equipa.**

****

# 12. Como administrador da organização quero um plano de recuperação de desastre que satisfaça o MBCO. 1191008

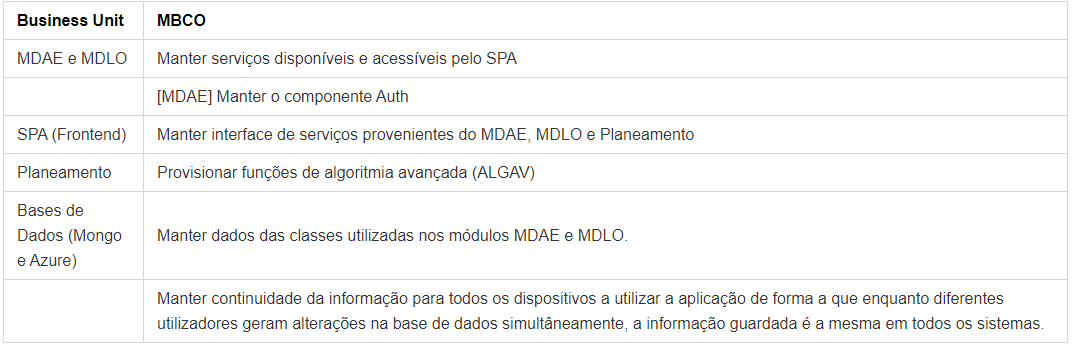
Para tal, primeiro necessitámos de definir o **MBCO** (Minimum Business Continuity Objective) aplicado à solução final.

A função do MBCO é identificar todas as unidades do negócio (**Business Unit**) e, de acordo com a solução pretendida, mencionar para cada um o objetivo mínimo da unidade de negócio de forma que possamos ter continuidade do bom funcionamento da solução. Após a analise da solução conseguimos identificar que as unidades de negócio críticas da solução são:

* MDAE;
* MDLO;
* Bases de Dados (MongoDB e Azure);
* Planeamento;
* SPA (Frontend).

Embora os módulos MDAE e MDLO sejam independentes e distintos, as suas funcionalidades são semelhantes, assim como as suas soluções, então decidimos agrupá-los na mesma unidade para evitar redundâncias.

Sendo assim, traçamos a seguinte tabela onde identificamos as mesmas e os devidos objetivos essenciais para o bom desempenho da solução respetivos a cada uma:



Com isto podemos fazer a traçagem de o **BCP** (Business Continuity Plan), ou seja, plano de recuperação. Tipicamente, na traçagem do BCP, são definidas equipas dedicadas a cada unidade de negócio, responsáveis pelo processo de recuperação em caso de desastre; devido ao âmbito e extensão da nossa solução, podemos ultrapassar esse passo, sendo que a manutenção da solução é delegada a todos os elementos do projeto.

Passamos então à definição do **BCS** (Business Continuity Strategy), onde definimos a estratégia de recuperação e as prioridades no caso de desastre.

A cadeia de prioridade das unidades de negócio é a seguinte (por ordem decrescente):

1. MDAE e MDLO;
2. Bases de Dados (MongoDB e Azure);
3. Planeamento;
4. SPA (frontend)

Geralmente, no caso de desastre o recurso mais eficiente de conseguir que a aplicação continue operacional é reverter a *build* da aplicação para uma *build* segura, previamente testada e confirmada como segura. Embora este recurso torna-se redundante no caso da nossa solução, visto que existem medidas para segurar que a *build* mais recente da aplicação seja segura. Não obstante, a opção recorrer a esta medida é uma mais-valia.

Sendo assim, a medida não é omnipotente, visto que muitas causas para desastre podem não ser provenientes do código em si, por isso delineamos alguns passos para ajudar a identificar e resolver o desastre:

1. Executar testes da aplicação;
2. Verificar a ligação com o servidor DEI;
3. Verificar se o acesso entre as unidades de negócio foi comprometido;
4. Desativar a funcionalidade afetada.

Com isto, no caso de desastre, a partir da informação provisionada pelos testes e a verificação das ligações das diferentes unidades de negócio, partimos do ponto que o desenvolvedor tenha informação suficiente para identificar o desastre, e corrigir o mesmo. Em tal caso que a informação ainda não seja suficiente, recomendasse a continua análise da solução fora da pipeline principal da solução.

# 13. Como administrador da organização quero que me seja apresentado um BIA (Business Impact Analysis) da solução final, adaptando se e onde aplicável os riscos definidos na matriz de riscos. 1191008

No que diz respeito a **BIA** (Business Impact Analysis), o objetivo é, para cada risco identificado, considerar o impacto realístico na solução e a sua duração no intuito de documentar o impacto potencial resultado na interrupção das funções do negócio e os seus processos, identificando a cadeia de prioridade por ordem de eventos. Com este final, recorremos à **matriz de riscos** preconizada no relatório anterior para identificar os potenciais riscos:

Uma imagem com mesa

Descrição gerada automaticamente

A partir da tabela anterior analisamos os riscos identificado. De seguida os riscos, por ordem decrescente de prioridade:

1. **Falha na execução de um módulo.**
   1. **Impacto:** Torna a solução potencialmente completamente inoperável; possibilidade de corrupção ou exclusão de dados.
   2. **Duração:** Indefinida; dependente da velocidade de reparação de desastre.
2. **Interrupção ou atraso na resposta da Cloud do DEI torna os serviços/componentes lentos e/ou indisponíveis.**
   1. **Impacto:** Torna a solução potencialmente inoperável.
   2. **Duração:** Período curto (menos de 1 hora).
3. **Manutenção semanal à Cloud do DEI causa que os serviços fiquem indisponíveis.**
   1. **Impacto:** Torna a solução inoperável.
   2. **Duração:** Período curto (menos de 1 hora).
4. **Devido a um erro na lista de utilizadores autorizados, existem utilizadores não autorizados com acesso à aplicação.**
   1. **Impacto:** Potencial vazamento de dados não autorizados guardados na solução.
   2. **Duração:** Dependente do período deteção do desastre.
5. **Falha na execução de um serviço, devido a um erro não testado.**
   1. **Impacto:** Parte da solução fica indisponível; severidade dependente do serviço afetado.
   2. **Duração:** Indefinida; dependente da velocidade de reparação de desastre.
6. **Devido a um erro na lista de utilizadores autorizados, existem utilizadores autorizados sem acesso à aplicação.**
   1. **Impacto:** Utilizador sem acesso à solução.
   2. **Duração:** Dependente do período deteção do desastre.