Uma imagem com Tipo de letra, Gráficos, design gráfico, captura de ecrã

Descrição gerada automaticamente

**Relatório Sprint 1&2**

**Turma 3DD - Grupo 23**

**1220879 – Rafael Brandao**

**Professor:**

André Moreira, ASC

**Unidade Curricular:**

Arquitetura de Sistemas

Índice

[Sprint 1 3](#_Toc186748943)

[User Story 4 3](#_Toc186748944)

[User Story 7 5](#_Toc186748946)

[Sprint 2 6](#_Toc186748948)

[User Story 6 6](#_Toc186748949)

[User Story 8 8](#_Toc186748951)

# Sprint 1

## User Story 4

Requisitos: “*Como administrador do sistema quero implementar uma gestão de quotas no sistema Windows para que uma pasta de partilha de ficheiros (que deve ser criada) não possa conter mais do que 10MB de informação, avisando-me por email se estiver prestes a ser alcançado esse limite.”*

Começamos por ativar o Quota Management no disco pretendido (C:):

Uma imagem com texto, captura de ecrã, software, Software de multimédia

Descrição gerada automaticamente

Foi então criada a pasta, “pasta\_partilhada” dentro do disco em que ativamos o Quota Management. De seguida adicionamos o File Server Resource Manager para podermos fazer a configuração das quotas na pasta que pretendemos.

Uma imagem com texto, captura de ecrã, software, Software de multimédia

Descrição gerada automaticamente

Adicionamos também o SMTP Server, para o ADMIN ser avisado quando estiver perto de ultrapassar o limite definido de quota.

Uma imagem com texto, captura de ecrã, software, Software de multimédia

Descrição gerada automaticamente

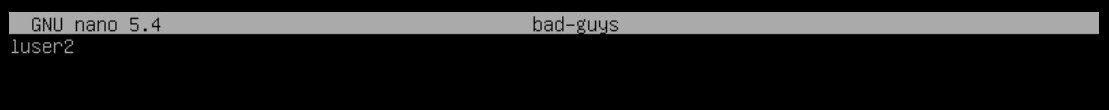
Uma imagem com texto, captura de ecrã, software, Software de multimédia

Descrição gerada automaticamente

## User Story 7

Requisitos: “*Como administrador do sistema quero usar no sistema Linux o módulo PAM “pam\_listfile.so” para condicionar o acesso ao sistema, negando o acesso ao sistema aos utilizadores (um por linha) listados no ficheiro (que deve ser criado) /etc/bad-guys.”*

Primeiro passo, deveremos criar o ficheiro /etc/bad-guys.



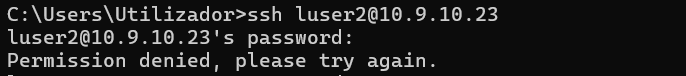
Após listar os users aos quais pretendemos negar o acesso devemos configurar o arquivo PAM no ficheiro /etc/pam.d/sshd.



Significado dos parâmetros utilizados:

* onerr = succeed: No caso de surgir erros, como, por exemplo, se o arquivo ‘/etc/bad-guys’ não existir, a autenticação será bem-sucedida.
* item=user: Especifica que o item a ser verificado é um user.
* sense=deny: Indica que o acesso deve ser negado caso o utilizador esteja na lista especificada.
* file=/etc/bad-guys: Este é o caminho para o ficheiro que contém a lista de utilizadores indesejados.

Se um user que tenha sido incluído no ficheiro /etc/bad-guys tentar efetuar login, não irá conseguir aceder ao sistema após estas alterações.



# Sprint 2

## User Story 6

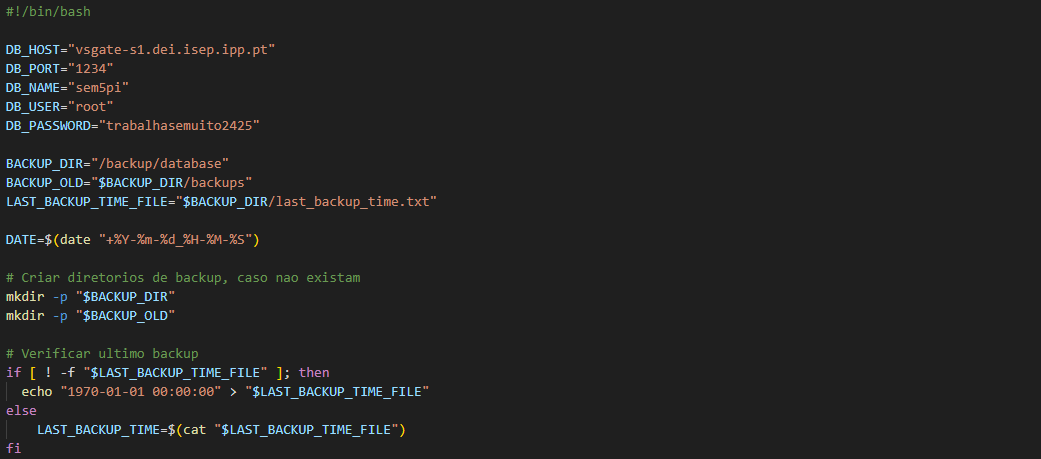
Requisitos: “*Como administrador do sistema quero que seja proposta, justificada e implementada uma estratégia de cópia de segurança que minimize o RPO (Recovery Point Objective) e o WRT (Work Recovery Time).”*

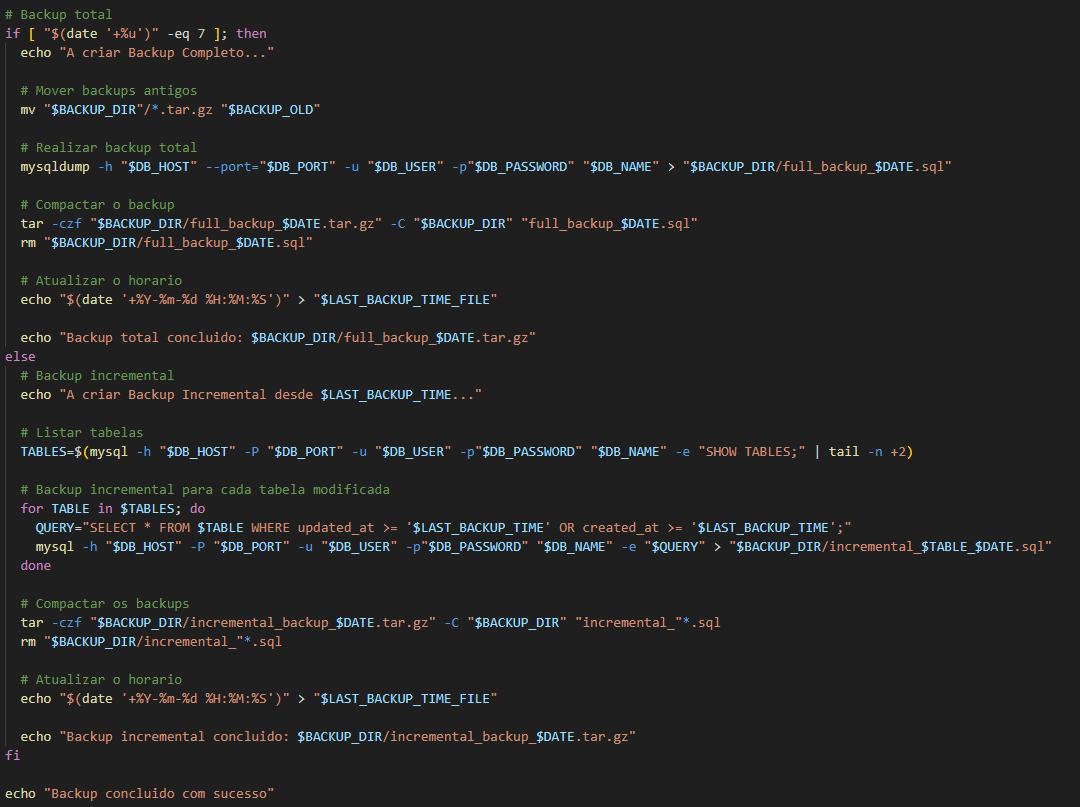
**Estratégia e Justificação**

1. Backup Total ao Domingo:
   * Garante a criação de um backup completo, o que facilita a restauração rápida de todo o sistema em caso de qualquer falha severa.
   * Realizamos o backup às 15:00h de modo a minimizar o impacto no sistema durante horas críticas.
2. Backups Incrementais Diários:
   * Registam-se apenas as alterações realizadas desde o último backup de modo a garantir que apenas essas sejam perdidas em situações de falha, reduzindo significativamente o RPO.
   * Reduz o tempo de recuperação (WRT) do backup diário pois complementam os dados restaurados sem necessidade de processamento intensivo.
3. Automação via Crontab:
   * Permite uma execução automática e sem intervenção humana, de modo a garantir alguma consistência no processo de backup.

**Implementação**

1. Criamos um script nomeado de *backup.sh* que faz o seguinte:
   * Backup Total: Exporta todas as tabelas do banco de dados para um arquivo SQL e compacta-o. Arquivos da semana anterior são movidos para a pasta “backups”.
   * Backups Incrementais: Gera backups incrementais com base em alterações desde o último backup, utilizando as datas de modificação das tabelas. Também compacta os dados incrementais para minimizar espaço utilizado.

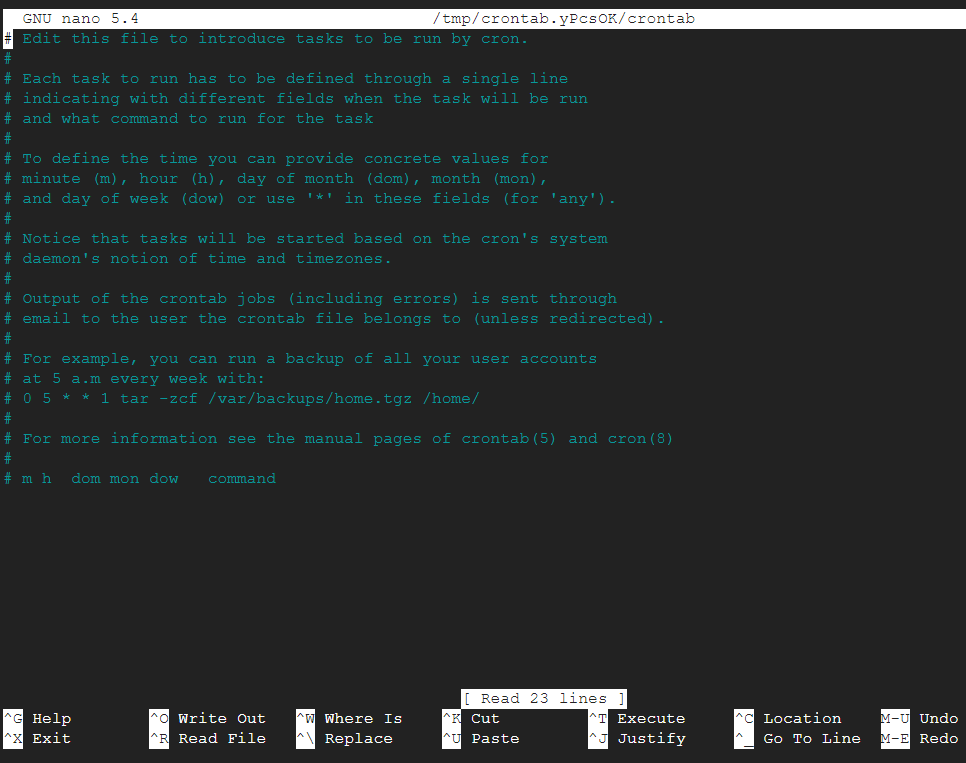




Após a criação do ficheiro tornamo-lo executável com o comando:



1. De seguida, usamos o Crontab na automatização diária:

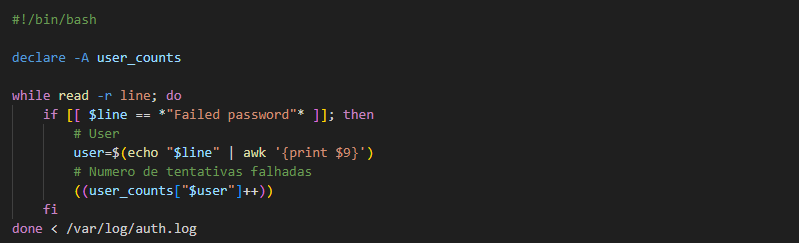


## User Story 8

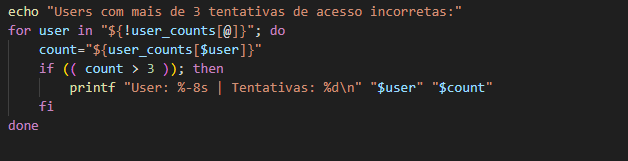
## Requisitos: *“Como administrador do sistema quero obter os utilizadores com mais do que 3 tentativas de acesso incorretas.”*

De modo a obter os usuários com mais de 3 tentativas de acesso incorretas a partir dos *logs* de autenticação do sistema, armazenados em /var/log/auth.log, temos de implementar um Shell script, neste caso chamado de *tentativas\_falhadas.sh.*

O script encontra o arquivo /var/log/auth.log e procede a filtrar as linhas com o texto "*Failed password*", que indicam tentativas de acesso incorretas.



De seguida, contando o número de falhas por usuário e mostra apenas os usuários com mais de 3 falhas de acesso.



Após tentarmos 3 vezes dar login com a conta luser1, se executarmos o script aparecerá por exemplo:

