

**Sprint 1**

**Turma 3NA-Grupo 76**

1200618 – Jorge Cunha

**Professor:**

Dílio Ribeiro, DAR

**Unidade Curricular:**

ADMINISTRAÇÃO DE SISTEMAS (ASIST)

**Data: 29/10/2023**

**Índice**

[**Índice** 0](#_Toc148222126)

[**Introdução** 1](#_Toc148222127)

[**User Story 1** 2](#_Toc148222128)

[**User Story 2** 3](#_Toc148222129)

[**User Story 5** 7](#_Toc148222130)

[**User Story 6** 7](#_Toc148222130)

# **Introdução**

O presente relatório foi escrito no âmbito do Sprint 1 da unidade curricular Administração de Sistemas.

Neste relatório iremos demonstrar as Us, que nos foram pedidas para desenvolver, como também a sua explicação e como foi desenvolvida. Também apresentaremos imagens que comprovam que as user stories foram adicionadas a máquina virtual.

# **User Story 1**

1. Como administrador do sistema quero alterar a informação apresentada no terminal

do sistema Linux antes de me autenticar, alterando a informação por omissão por

uma mais criativa que contenha obrigatoriamente a data e o número de utilizadores

ativos.

Para personalizar a mensagem pré-login, é possível modificar o arquivo "/etc/issue" e incluir informações como a data atual, a hora atual, e o número de usuários ativos.

Isso pode ser feito utilizando sequências como "\d" para a data, "\t" para a hora, "\n" para o nome do host e "\u" para o número de usuários ativos no momento.

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

Descrição gerada automaticamente

# 

# **User Story 2**

2. Como administrador do sistema quero alterar a informação apresentada no terminal

do sistema Linux após me autenticar, alterando a informação por omissão por uma

mais criativa que contenha obrigatoriamente a data e o nome do utilizador.

Assim, para personalizar a mensagem de pós-login, é necessário editar o arquivo "/etc/profile" e incluir informações sobre o nome de usuário que fez login e a data. Isso pode ser feito usando o comando "echo" para exibir texto no terminal, com a opção "-e" habilitando o uso do caractere "\n".

Para adicionar uma nova linha, utilizamos "\n". Para exibir o nome do usuário conectado no momento, usamos "$(whoami)", que é um comando que retorna o nome do usuário atualmente ligado. Para mostrar a data e hora do sistema, usamos "$(date)" e podemos definir o formato desejado, como "dia (%d), mês (%m), ano (%Y)".

Uma imagem com texto, software, Software de multimédia, Software gráfico

Descrição gerada automaticamente

**User Story 3**

3. Como administrador do sistema quero implementar uma gestão de quotas no sistema Linux para que os utilizadores não possam exceder 300 ficheiros na sua área de trabalho (home directory)

Começamos por verificar os home dirs de cada user presente na máquina virtual:

Uma imagem com texto, Tipo de letra, captura de ecrã, preto

Descrição gerada automaticamente

Verificamos se o ficheiro /etc/fstab já contém a habilitação da quota para o diretório /home com o comando nano /etc/fstab:

Uma imagem com texto, captura de ecrã, Tipo de letra

Descrição gerada automaticamente

Em seguida, verificamos o estado das quotas dos users, com o comando quotacheck no diretório /home (caso estivessem desativadas, poderíamos ativar as quotas com o comando quotaon /home):

Uma imagem com texto, captura de ecrã, preto, Tipo de letra

Descrição gerada automaticamente

Com o comando setquota estabelecemos um valor de soft limit e hard limit para o luser1 e repetimos o processo para os restantes utilizadores:

setquota -u luser1 0 0 300 350 /home

Uma imagem com texto, captura de ecrã, Tipo de letra, preto

Descrição gerada automaticamente

Para os restantes utilizadores:

Uma imagem com texto, captura de ecrã, Tipo de letra, preto

Descrição gerada automaticamente

Neste momento, temos então o limite de 300 ficheiros (inodes) para todos os utilizadores, analisando com o comando repquota:

Uma imagem com texto, captura de ecrã, preto, Tipo de letra

Descrição gerada automaticamente

**User Story 5**

5. Como administrador do sistema quero usar no sistema Linux o módulo PAM

“***pam\_succeed\_if.so***” para condicionar o acesso ao sistema, permitindo acesso

apenas aos utilizadores com UID inferior a 7000 e que pertençam ao grupo

**lasistgrupo**.

Para restringir o acesso apenas a utilizadores com UID abaixo de 7000 que fa√ßam parte do grupo "lasistgrupo", procedemos √† edi√ß√£o do ficheiro "/etc/pam.d/sshd" e acrescentamos o seguinte:

Ao executar o comando "cat /etc/passwd", notamos que existem utilizadores com "uid" acima de 7000 que estão associados aos grupos com "gid" 6003 e 6004.

No comando "cat /etc/group," podemos verificar que os "gid" 6003 e 6004 correspondem aos grupos "lgrupo1" e "lasistgrupo," respetivamente.

Para abranger todas as possibilidades, consideramos os utilizadores "luser2," "luser3," e "luser5," com os seguintes critérios:

"luser2" possui um "uid" inferior a 7000 e pertence ao grupo "lasistgrupo," portanto, é permitido o login.

"luser3" tem um "uid" inferior a 7000, mas faz parte do grupo "lgrupo1," o que impede o login.

"luser5" possui um "uid" superior a 7000, mesmo sendo membro do grupo "lasistgrupo," o que também impede o login.

Nas capturas de ecrã que se seguem, iremos demonstrar todos os passos mencionados anteriormente.

Uma imagem com texto, software, Software de multimédia, Website

Descrição gerada automaticamenteUma imagem com texto, captura de ecrã

Descrição gerada automaticamenteUma imagem com texto, captura de ecrã, software

Descrição gerada automaticamente

# **User Story 6**

6. Como administrador do sistema quero usar no sistema Linux o módulo PAM

“***pam\_listfile.so***” para condicionar o acesso ao sistema, permitindo acesso apenas às

máquinas remotas (uma por linha) que constem do ficheiro (que deve ser criado)

**/etc/remote-hosts**.

Com o objetivo de restringir o acesso ao servidor apenas a um conjunto específico de utilizadores, aqueles que foram atribuídos IPs fixos ou endereços estáticos, implementamos uma instrução que concede acesso exclusivamente a utilizadores cujos IPs estejam listados no documento denominado "/etc/remote-hosts".

Esta instrução orienta o sistema Linux a empregar o módulo "pam\_listfile.so" para fazer referência ao ficheiro "remote-hosts", que contém os IPs com autorização para aceder ao servidor. O sistema verifica se o IP do host que solicita acesso corresponde a algum dos IPs listados no ficheiro em questão.

O procedimento inicial envolve a criação do ficheiro e a inclusão do IP do host que deseja acessar o servidor. Em seguida, tentamos efetuar o login com as credenciais de um utilizador do servidor, e o acesso é concedido sem problemas se o IP estiver autorizado.



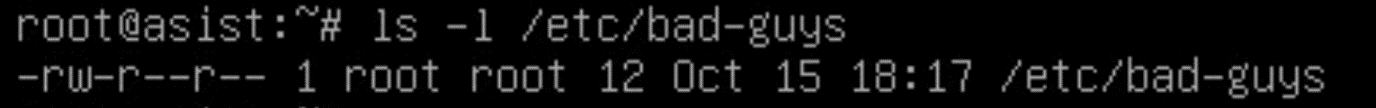
Uma imagem com texto, captura de ecrã, software, Software de multimédia

Descrição gerada automaticamente

# **User Story 7**

7. 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.

Comecemos por criar o ficheiro /etc/bad-guys e adicionamos o luser1 para testar o acesso ao sistema:



Uma imagem com texto, captura de ecrã, Tipo de letra, preto

Descrição gerada automaticamente

Para modificarmos no arquivo PAM de autenticação, atualizamos o ficheiro /etc/pam.d/sshd com a linha apresentada abaixo:

auth required pam\_listfile.so onerr=fail item=user sense=deny file=/etc/bad-guys

Assim sendo, podemos ver o login com sucesso do luser2:

Uma imagem com texto, captura de ecrã, Tipo de letra, preto

Descrição gerada automaticamente

E a falha do login do luser1:

Uma imagem com texto, Tipo de letra, captura de ecrã, preto

Descrição gerada automaticamente