

**Relatório Sprint 1**

**Turma 3DD-Grupo 23**

**1112250 – Luís Monteiro**

**1221251 – David Gonçalves**

**1220879 – Rafael Brandao**

**1201078 – Miguel Marques**

**Professor:**

André Moreira, ASC

**Unidade Curricular:**

Arquitetura de Sistemas

Índice

Introdução

User Story 1 – David Gonçalves

User Story 2 – Luís Monteiro

User Story 3 – Miguel Marques

User Story 4 – Rafael Brandão

User Story 5 – David Gonçalves

User Story 6 – Luís Monteiro

User Story 7 – Rafael Brandão

User Story 8 – Miguel Marques

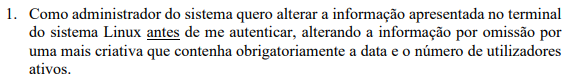
**Introdução**

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

Com este trabalho pretendemos aprender mais sobre esta unidade curricular e aplicar os métodos ensinados pelo Professor.

Iremos apresentar as User Stories que foram pedidas, seguida da sua explicação e como foi desenvolvida. Também apresentaremos imagens para evidenciar melhor o processo e comandos utilizados.

**User Story 1 – David Gonçalves**

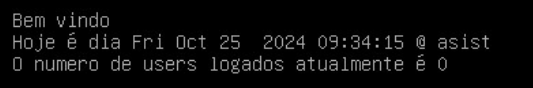


Para alterar a mensagem antes de dar o login temos de alterar o ficheiro ***“/etc/issue”*** e personalizar a mensagem com a data atual e o número de utilizadores. Escolhemos também adicionar uma saudação.

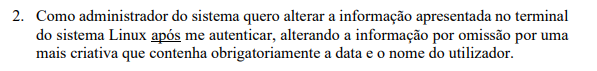


* **\d** – inserir a data atual;
* **\t** – obter o tempo atual;
* **\n** – obter o hostname;
* **\u** – obter o número de utilizadores ativos no momento;

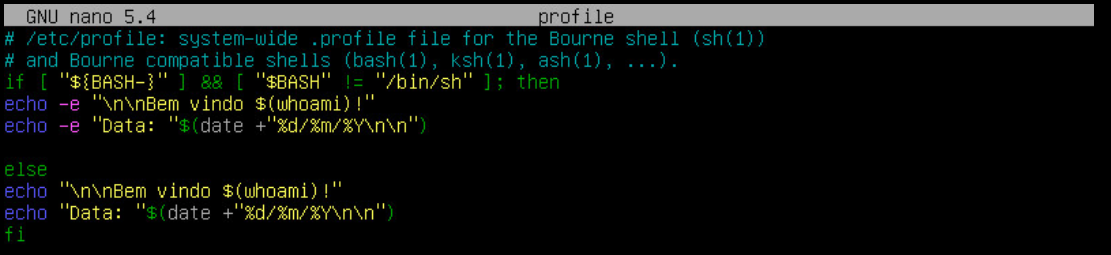
Depois de configurar é assim que fica o terminal quando acedemos ao servidor:



**User Story 2 – Luís Monteiro**



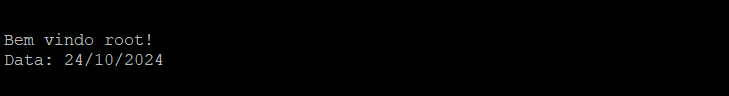
Para obter uma mensagem após a autenticação ter sucedido, é preciso alterar o ficheiro ***“/etc/profile”***:



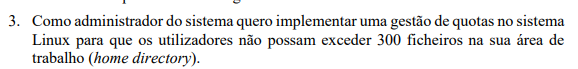
O comando “**echo**” imprime texto no terminal, a opção “**-e**” permite o uso do caráter “**\**”.

Usamos um if pois dependendo do user, (se é o root ou luser1, por exemplo) é utilizado um bash diferente, para o qual já não é preciso o -e.  
 O “**\n**” acrescenta uma nova linha, **$(whoami)** é um comando que apresenta o nome do utilizador conectado no momento. **$(date)** é um comando que mostra a data e hora do sistema, a seguir colocou-se o formato em que queremos visualizar a data, portanto: “**%d**” – dia, “**%m**” – mês e “**%Y**” – ano.

Resulta na seguinte frase quando autenticado como root:



**User Story 3 – Miguel Marques**



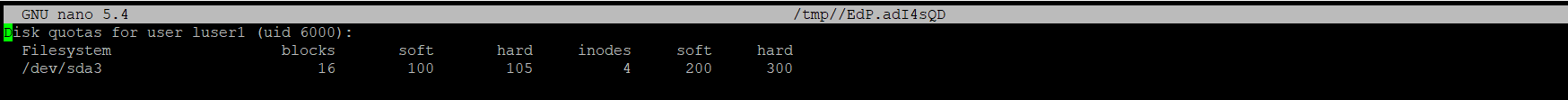
Primeiro instalamos os ficheiros necessários para usar as quotas:



Já instalado conseguimos modificar o limite de quotas de qualquer utilizador, desta maneira vamos mudar as quotas do user1 respetivamente:

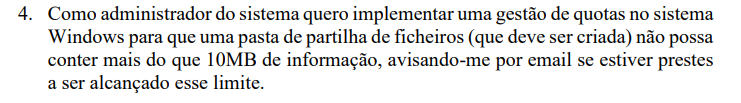


Para alterar o limite para 300 ficheiros, temos de mudar o hard block dos i-nodes, tal como está na imagem em baixo deste texto, sendo o soft limit o valor que quisermos, pois, este valor apenas mostra uma notificação quando ultrapassamos o armazenamento, mas com o requisito de ser menor que o valor que colocarmos no campo hard.

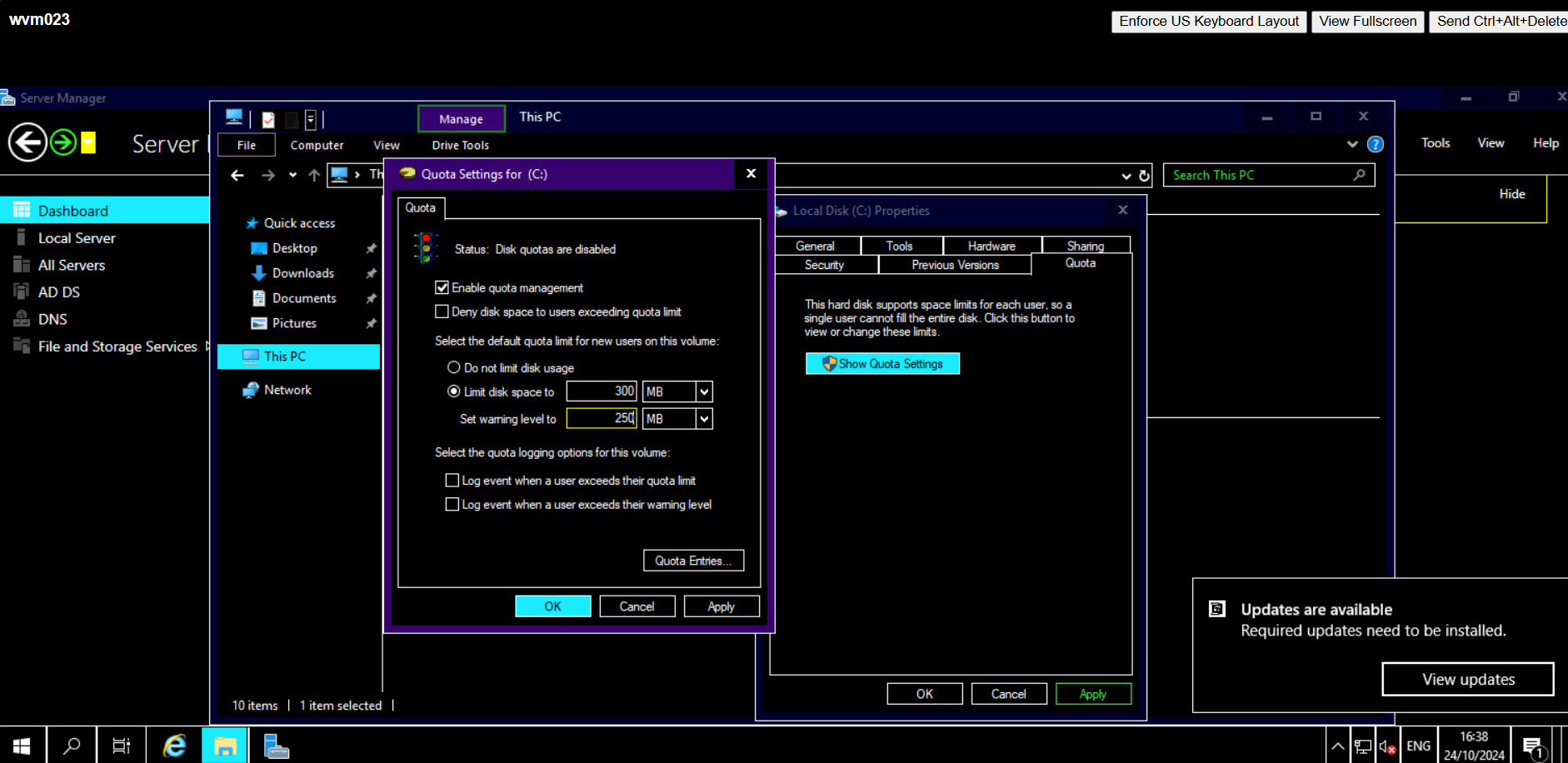


Agora temos de fazer isto para os restantes utilizadores, para mudar a gestão de quotas no sistema de cada um para não excederem 300 ficheiros na sua área de trabalho.

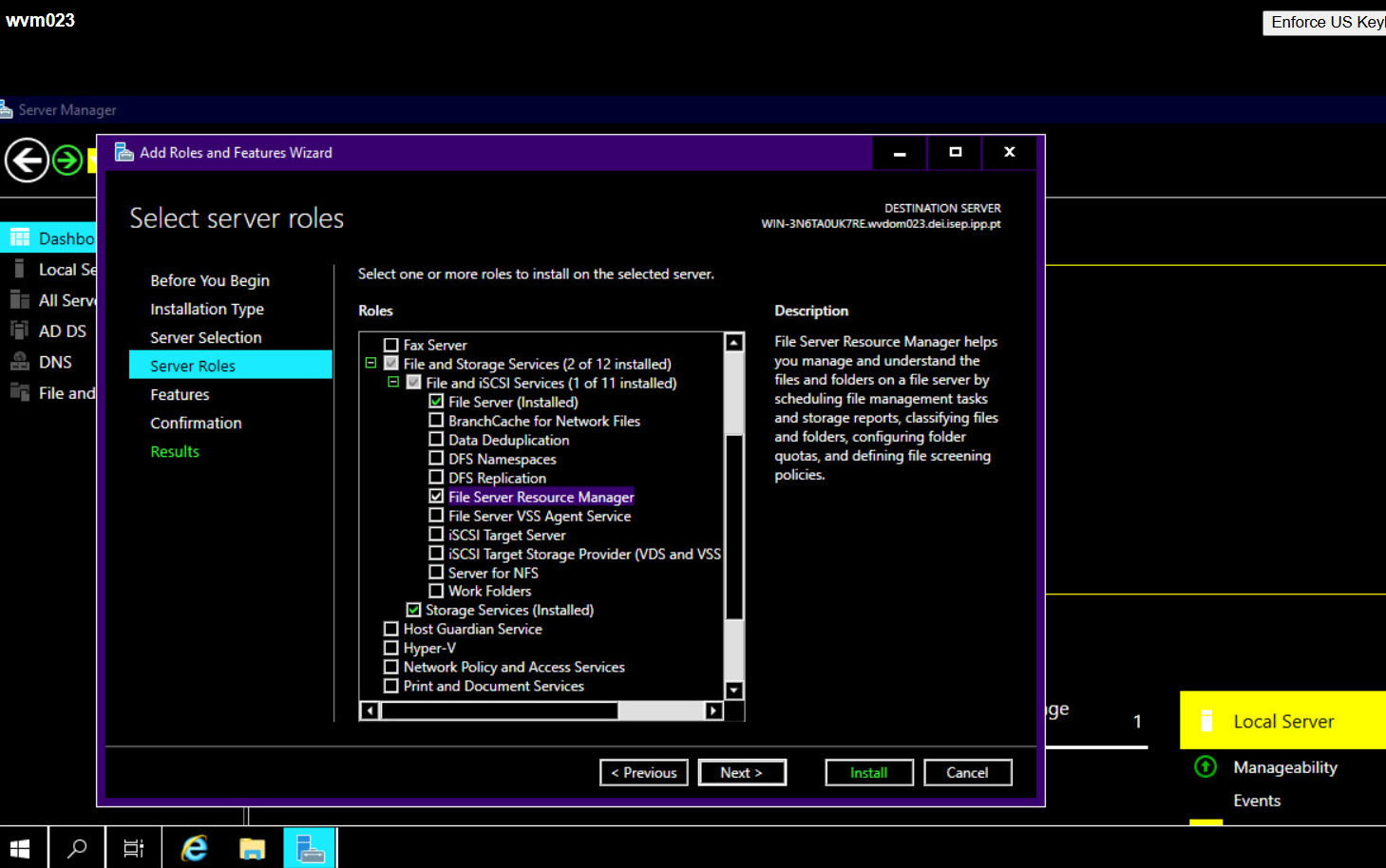
**User Story 4 – Rafael Brandão (WIP)**



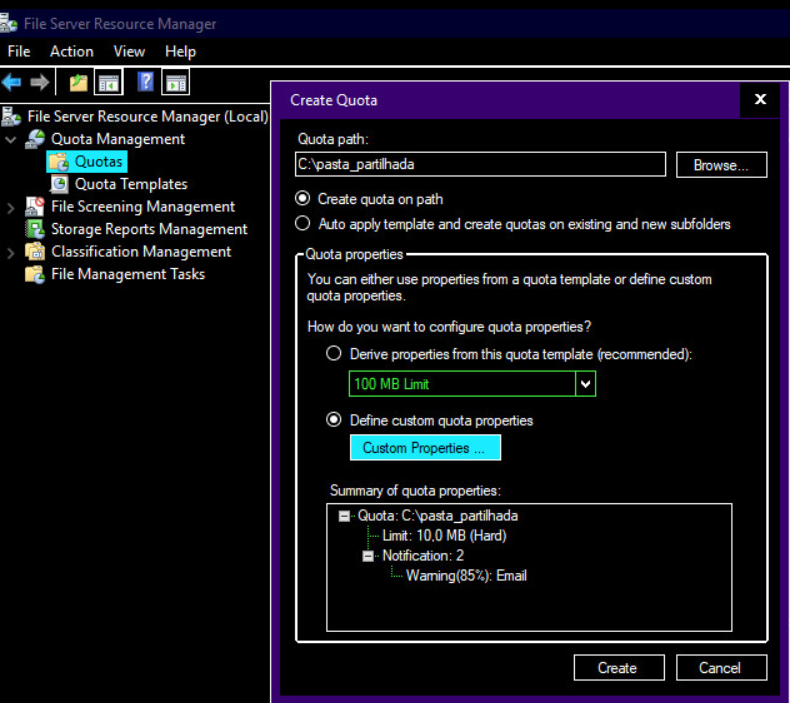
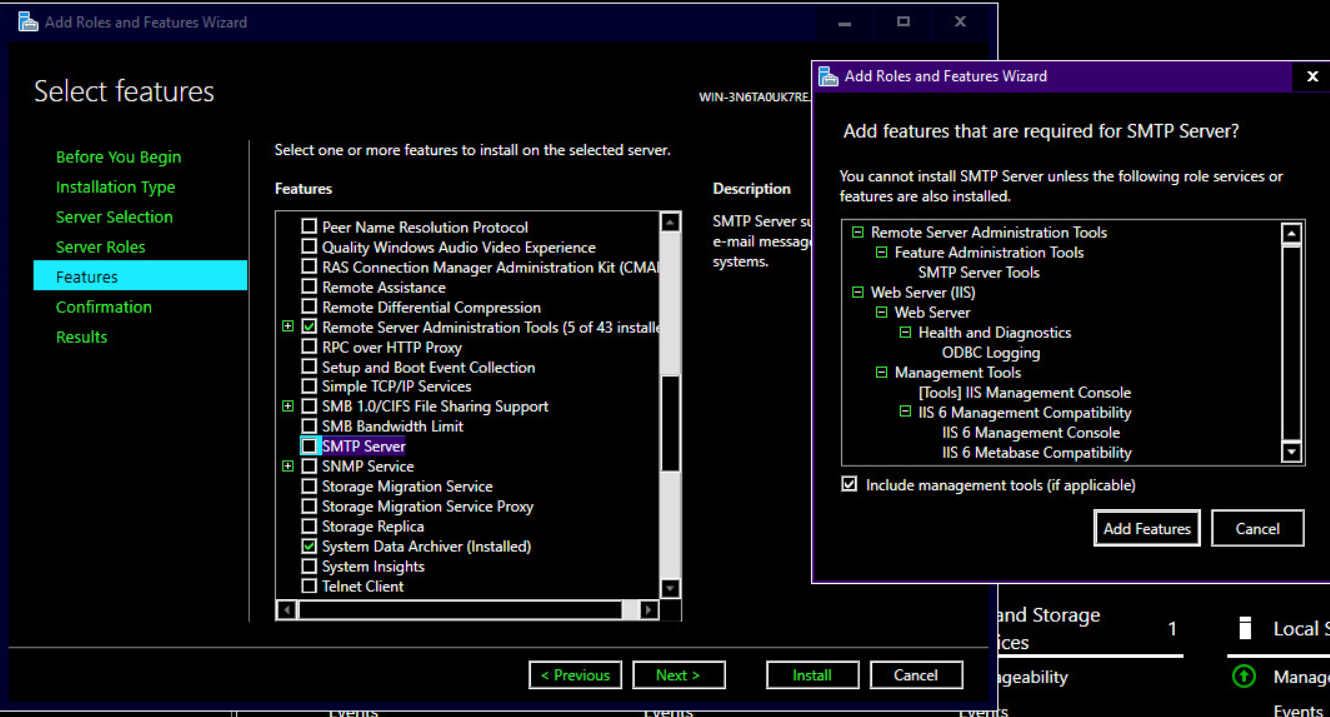
Começamos por ativar o Quota Management no disco pretendido (C: ):



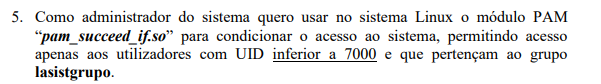
Foi então criada a pasta, “pasta\_partilhada” dentro do disco em que ativamos o Quota Management. De seguida adicionamos o File Server Resource Manager para podermos fazer a configuração das quotas na pasta que pretendemos.



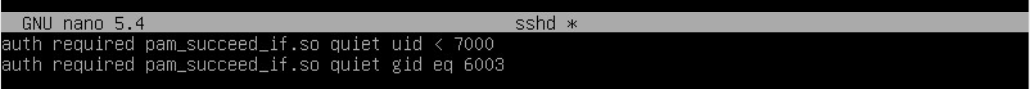
Adicionamos também o SMTP Server, para o ADMIN ser avisado quando estiver perto de ultrapassar o limite definido de quota.



**User Story 5 – David Gonçalves**



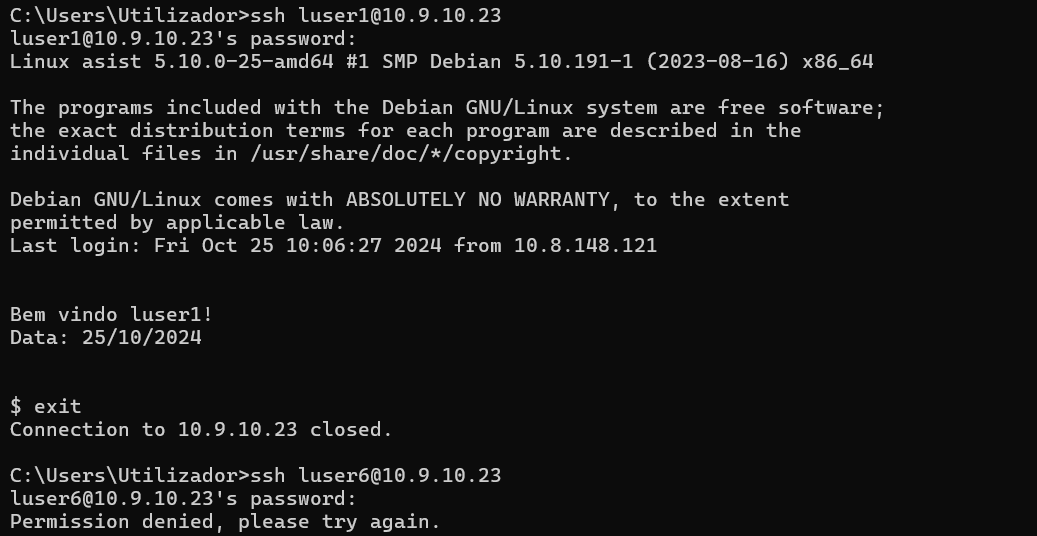
Para permitir apenas o acesso a utilizadores com UID inferior a 7000 e que pertençam ao grupo “lasistgrupo”, temos de editar o ficheiro “/etc/pam.d/sshd” e temos de acrescentar as seguintes linhas de código:



Usando o comando “cat /etc/passwd” examinar observar o UID dos utilizadores, observando que existe alguns com UID abaixo de 7000.

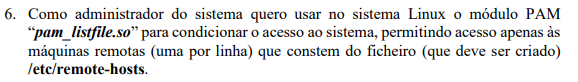
Através do comando “cat /etc/group” conseguimos observar que o UID do grupo “lasistgrupo” é 6003. Desta maneira metemos este número na linha de código que adicionamos acima.

Através deste procedimento apenas nos falta testar o login:



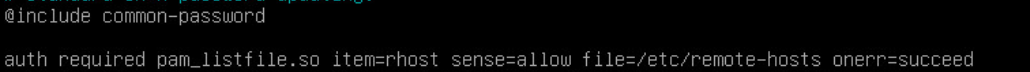
Desta maneira conseguimos ver que está a funcionar, pois os logins são feitos de maneira correta apenas para os que têm permissão para aceder ao sistema.

**User Story 6 – Luís Monteiro**



Para condicionar o acesso usando o módulo “pam\_listfile.so” temos de primeiro adicionar a instrução para utilizar o ficheiro remote-hosts para verificar que ips são autorizados e depois precisamos de criar esse ficheiro, adicionando os ips.

Para isso primeiro adicionamos ao ficheiro /etc/pam.d/sshd o seguinte:

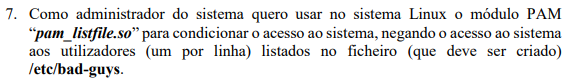


Depois criamos o ficheiro e colocamos lá o ***IP*** do ***host*** que pedirá acesso ao servidor.

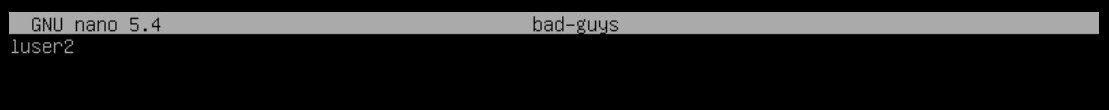


Se retirarmos o ip do remote-hosts, perdemos o acesso através do ssh, pois já não estamos autorizados.

**User Story 7 – Rafael Brandão (WIP)**



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



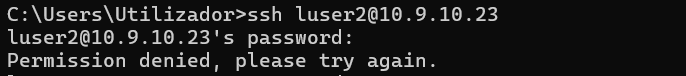
Após listar os users aos quais pretendemos negar o acesso devemos configurar o arquivo PAM no ficheiro /etc/pam.d/sshd.



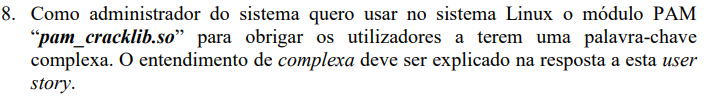
Significado dos parâmetros utilizados:

* onerr = succeed: I 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.



**User Story 8 – Miguel Marques**

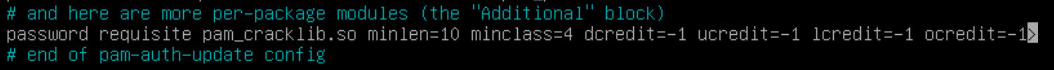


Para utilizarmos o módulo PAM “pam\_cracklib.so” para obrigar utilizadores a usar palavras-chave mais complexas começamos por editar o ficheiro de configuração /etc/pam.d/common-password. Neste ficheiro serão adicionadas as regras de palavra-passe que quisermos impor aos utilizadores. O módulo ‘pam\_cracklib.so’ possui diversas políticas já definidas entre as quais:

* minlen: comprimento mínimo da senha;
* minclass: número mínimo de classes de caracteres;
* minrepeat: número mínimo de caracteres repetidos;
* minsequence: número mínimo de caracteres em sequência;
* maxrepeat: número máximo de caracteres repetidos;
* difok: número mínimo de caracteres que devem ser diferentes da senha anterior;
* lcredit: crédito de letras minúsculas;
* ucredit: crédito de letras maiúsculas;
* dcredit: crédito de dígitos;
* ocredit: crédito de caracteres especiais.

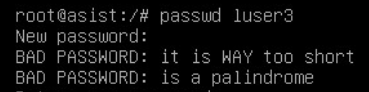
Determinamos que a palavra-chave devia incorporar no mínimo 10 caracteres e ter no mínimo 4 tipos de classes de caracter.

Para adicionar estas políticas colocamos a seguinte linha no ficheiro etc/pam.d/common-password:



Subtraimos os créditos para arranjar o tamanho mínimo.

Testando com a palavra-passe “92”.



Testando com a palavra-passe “aaaaaaaaab”.

