



Instituto Superior de  
**Engenharia** do Porto

## **Sprint 1**

### **Turma 3NA-Grupo 76**

1191448 – Rui Marinho

1200583 – João Carrinho

1200586 – Mário Borja

1200618 – Jorge Cunha

### **Professor:**

Dílio Ribeiro, DAR

### **Unidade Curricular:**

ADMINISTRAÇÃO DE SISTEMAS (ASIST)

**Data: 29/10/2023**

## Conteúdo

|                          |           |
|--------------------------|-----------|
| Conteúdo.....            | 0         |
| <b>Introdução .....</b>  | <b>1</b>  |
| <b>User Story 1.....</b> | <b>2</b>  |
| <b>User Story 2.....</b> | <b>3</b>  |
| <b>User Story 3.....</b> | <b>4</b>  |
| <b>User Story 4.....</b> | <b>6</b>  |
| <b>User Story 5.....</b> | <b>7</b>  |
| <b>User Story 6.....</b> | <b>11</b> |
| <b>User Story 7.....</b> | <b>12</b> |
| <b>User Story 8.....</b> | <b>14</b> |

# Introdução

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

Neste relatório temos a resolução das oito questões propostas no Sprint 1 da UC em questão. Além da resolução, temos também imagens que demonstram o fluxo de cada uma das questões apresentadas.

# User Story 1 1200618

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.

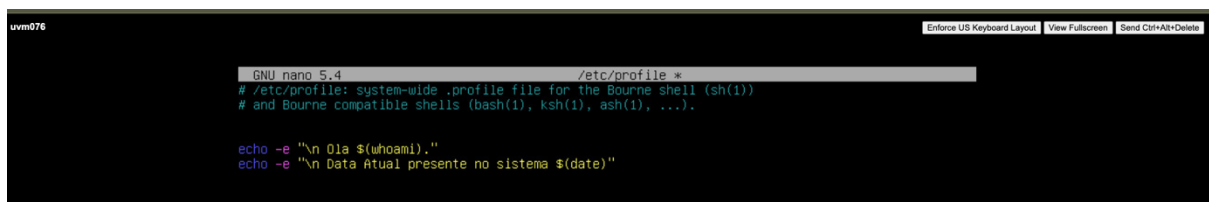
Isso pode ser feito utilizando sequências como `"\d"` para a data, `"\t"` para a hora, `"\n"` para o nome do host e `"\u"` para o número de usuários ativos no momento.

## User Story 2 1200586

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.

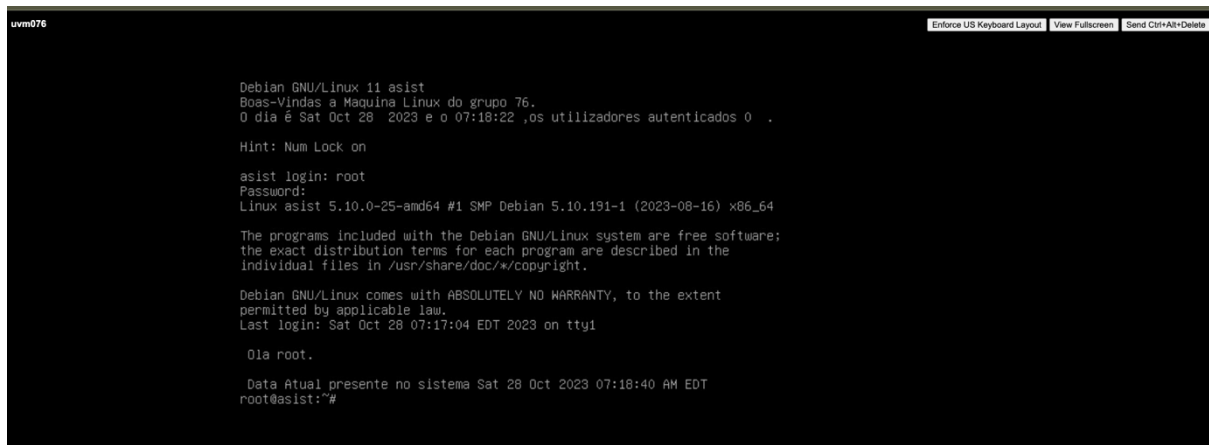
Assim, para personalizar a mensagem de pós-login, é necessário editar o arquivo `/etc/profile` e incluir informações sobre o nome de usuário que fez login e a data. Isso pode ser feito usando o comando `echo` para exibir texto no terminal, com a opção `-e` habilitando o uso do caractere `"\n"`.

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)"`.



```
GNU nano 5.4 /etc/profile *
# /etc/profile: system-wide .profile file for the Bourne shell (sh(1))
# and Bourne compatible shells (bash(1), ksh(1), ash(1), ...).

echo -e "\n Ola $(whoami)."
```



```
Debian GNU/Linux 11 asist
Boas-Vindas a Maquina Linux do grupo 76.
0 dia é Sat Oct 28 2023 e o 07:18:22 ,os utilizadores autenticados 0 .

Hint: Num Lock on

asist login: root
Password:
Linux asist 5.10.0-25-amd64 #1 SMP Debian 5.10.191-1 (2023-08-16) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Oct 28 07:17:04 EDT 2023 on tty1

Ola root.

Data Atual presente no sistema Sat 28 Oct 2023 07:18:40 AM EDT
root@asist: #
```

## User Story 3 1191448

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:

```
luser1:x:6000:7004::/home/luser1:/bin/sh
luser2:x:6001:7004::/home/luser2:/bin/sh
luser3:x:6002:7004::/home/luser3:/bin/sh
luser4:x:7000:7000::/home/luser4:/bin/sh
luser5:x:7001:7001::/home/luser5:/bin/sh
luser6:x:7002:7004::/home/luser6home:/bin/sh
```

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

```
# / was on /dev/sda1 during installation
UUID=797496a9-f15f-400b-8eab-49c65b8b9faa /          ext4      errors=remount-ro 0      1
# /home was on /dev/sda3 during installation
UUID=d6b391ce-1e06-48e4-8673-9b0b76da6b2b /home      ext4      defaults,usrquota,grpquota
# swap was on /dev/sda2 during installation
UUID=f571e8c4-0f68-4e20-9859-70cf7844352e none        swap      sw          0      0
/dev/sr0    /media/cdrom0  udf,iso9660 user,noauto 0      0
```

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`):

```
root@asist:~# quotacheck -cu /home
quotacheck: Quota for users is enabled on mountpoint /home so quotacheck might damage the file.
Please turn quotas off or use -f to force checking.
root@asist:~#
```

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
```

```
GNU nano 5.4 /tmp//EdP.a0VQF6v
Disk quotas for user luser1 (uid 6000):
Filesystem blocks soft hard inodes soft hard
/dev/sda3 4 0 0 1 280 300
```

Para os restantes utilizadores:

```
root@asist:~# setquota -u luser2 0 0 280 300 /home
root@asist:~# setquota -u luser3 0 0 280 300 /home
root@asist:~# setquota -u luser4 0 0 280 300 /home
root@asist:~# setquota -u luser5 0 0 280 300 /home
root@asist:~# setquota -u luser6 0 0 280 300 /home
root@asist:~# _
```

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

```
root@asist:~# repquota -a
*** Report for user quotas on device /dev/sda3
Block grace time: 7days; Inode grace time: 7days

```

|        |    | Block limits |      |      |       | File limits |      |      |       |
|--------|----|--------------|------|------|-------|-------------|------|------|-------|
| User   |    | used         | soft | hard | grace | used        | soft | hard | grace |
| root   | -- | 20           | 0    | 0    |       | 2           | 0    | 0    |       |
| asist  | -- | 20           | 0    | 0    |       | 5           | 0    | 0    |       |
| luser1 | -- | 4            | 0    | 0    |       | 1           | 280  | 300  |       |
| luser2 | -- | 4            | 0    | 0    |       | 1           | 280  | 300  |       |
| luser3 | -- | 4            | 0    | 0    |       | 1           | 280  | 300  |       |
| luser4 | -- | 4            | 0    | 0    |       | 1           | 280  | 300  |       |
| luser5 | -- | 4            | 0    | 0    |       | 1           | 280  | 300  |       |
| luser6 | -- | 4            | 0    | 0    |       | 1           | 280  | 300  |       |

## User Story 4 1200583

4. 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.

Inicialmente, começamos por criar uma nova pasta dentro do disco C:, denominada Pasta\_Partilhada. Para prosseguir com a questão, fomos ao File Server Resource Manager e criamos uma quota associada a esta pasta de forma que a mesma ficasse com 10MB de limite (hard quota) e enviasse um email de aviso ao administrador de sistema quando atingido 85% da capacidade máxima da quota.

Abaixo estão as imagens com a ordem do processo e o resultado final:

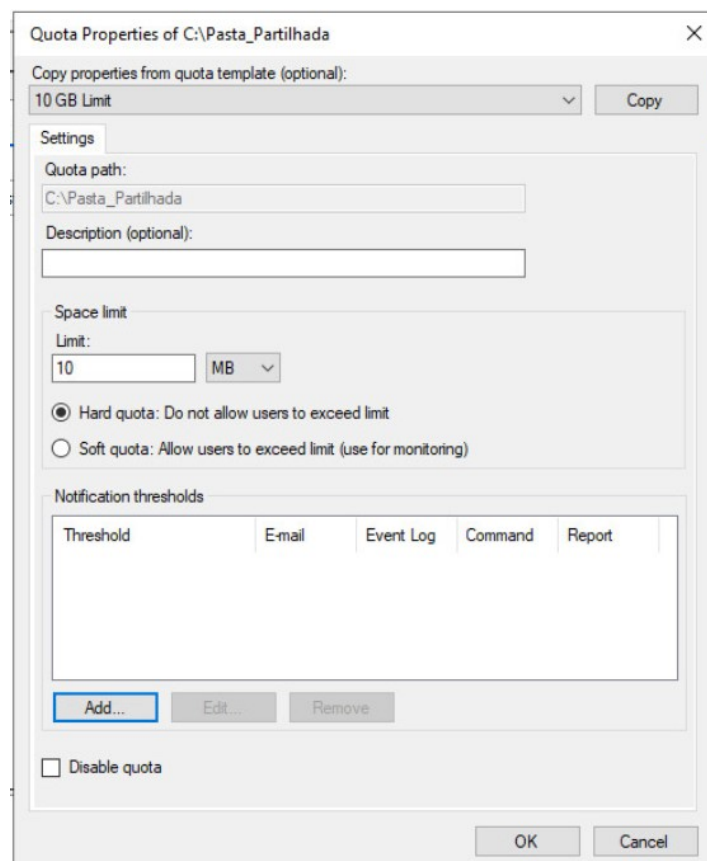


Figura 1 - Passo 1 Q4



**Add Threshold** [X]

Generate notifications when usage reaches (%):

E-mail Message | Event Log | Command | Report

☒ Send e-mail to the following administrators:  
  
 Format: account@domain. Use semicolons to separate accounts.

☐ Send e-mail to the user who exceeded the threshold

E-mail message  
 Type the text to use for the Subject line and message.  
 To identify the quota, limit, usage, or other information about the current threshold, you can use Insert Variable to insert a variable in your text.

Subject:

Message body:

Select variable to insert:

Inserts the e-mail addresses of the administrators who receive the e-mail.

Figura 2- Passo 2 Q4

**Quota Properties of C:\Pasta\_Partilhada** [X]

Copy properties from quota template (optional):

Settings

Quota path:

Description (optional):

Space limit  
 Limit:

☒ Hard quota: Do not allow users to exceed limit  
☐ Soft quota: Allow users to exceed limit (use for monitoring)

Notification thresholds

| Threshold     | E-mail | Event Log | Command | Report |
|---------------|--------|-----------|---------|--------|
| Warning (85%) | ✓      |           |         |        |

☐ Disable quota

Figura 3- Passo 3 Q4

## User Story 5 1200618

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 façam parte do grupo "lasistgrupo", procedemos à edição 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.

```
uvm076 /etc/pam.d/sshd *
GNU nano 5.4
# Print the message of the day upon successful login.
# This includes a dynamically generated part from /run/motd.dynamic
# and a static (admin-editable) part from /etc/motd.
session optional pam_motd.so motd=/run/motd.dynamic
session optional pam_motd.so noupdate

# Print the status of the user's mailbox upon successful login.
session optional pam_mail.so standard noenv # [1]

# Set up user limits from /etc/security/limits.conf.
session required pam_limits.so

# Read environment variables from /etc/environment and
# /etc/security/pam_env.conf.
session required pam_env.so # [1]
# In Debian 4.0 (etch), locale-related environment variables were moved to
# /etc/default/locale, so read that as well.
session required pam_env.so user_readenv=1 envfile=/etc/default/locale

# SELinux needs to intervene at login time to ensure that the process starts
# in the proper default security context. Only sessions which are intended
# to run in the user's context should be run after this.
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selinux.so open

# Standard Unix password updating.
@include common-password

# UID < 7000
auth required pam_succeed_if.so quiet uid < 7000

auth required pam_succeed_if.so quiet gid eq 7004

Help Write Out Where Is Cut Execute Location Undo
Exit Read File Replace Cut Paste Justify Go To Line Redo
```

```
uvm076 Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

nslcd:x:112:
root@asist:/# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110:/nonexistent:/usr/sbin/nologin
asist:x:1000:1000:asist,,:/home/asist:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
sshd:x:105:65534:/run/sshd:/usr/sbin/nologin
luser1:x:6000:7004:/home/luser1:/bin/sh
luser2:x:6001:7004:/home/luser2:/bin/sh
luser3:x:6002:7004:/home/luser3:/bin/sh
luser4:x:7000:7000:/home/luser4:/bin/sh
luser5:x:7001:7001:/home/luser5:/bin/sh
luser6:x:7002:7004:/home/luser6:/bin/sh

nslcd:x:106:112:nslcd name service LDAP connection daemon,,:/var/run/nslcd:/usr/sbin/nologin
```

```
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:asist
sasl:x:45:
plugdev:x:46:asist
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-timesync:x:101:
systemd-journal:x:102:
systemd-network:x:103:
systemd-resolve:x:104:
input:x:105:
kvm:x:106:
render:x:107:
crontab:x:108:
netdev:x:109:asist
messagebus:x:110:
ssh:x:111:
asist:x:1000:
systemd-coredump:x:999:
luser1:x:6000:
luser2:x:6001:
luser3:x:6002:
luser4:x:7000:
luser5:x:7001:
luser6:x:7002:
lgrupo1:x:7003:
lasistgrupo:x:7004:
lgrupo2:x:7005:luser1,luser2,luser3,luser4,luser5,luser6
nslcd:x:112:
root@asist:/#
```

## User Story 6 1191448

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.



The image consists of two screenshots of a terminal window. The top screenshot shows the GNU nano 5.4 editor editing the file /etc/pam.d/ssh. The content of the file is: @include common-password, auth required pam\_listfile.so item=rhost sense=allow file=/etc/remote-hosts onerr=succeed. The bottom screenshot shows the GNU nano 5.4 editor editing the file /etc/remote-hosts. The content of the file is: 192.168.5.76, 10.9.10.76, 10.9.10.78. The terminal window has a title bar that says 'uvvm076' and buttons for 'Enforce US Keyboard Layout', 'View Fullscreen', and 'Send Ctrl+Alt+Delete'.

```
GNU nano 5.4 /etc/pam.d/ssh *
@include common-password
auth required pam_listfile.so item=rhost sense=allow file=/etc/remote-hosts onerr=succeed
```

```
uvvm076 Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete
```

```
GNU nano 5.4 /etc/remote-hosts
192.168.5.76
10.9.10.76
10.9.10.78
```

## User Story 7 1200586

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:

```
root@asist:~# ls -l /etc/bad-guys
-rw-r--r-- 1 root root 12 Oct 15 18:17 /etc/bad-guys
```

```
GNU nano 5.4 /etc/bad-guys
luser1_
```

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:

```
Debian GNU/Linux 11 asist
Boas-Vindas a Maquina Linux do grupo 76.
O dia é Sun Oct 15 2023 e o 18:39:48 ,os utilizadores autenticados 0 .

asist login: luser2
Password:
Linux asist 5.10.0-25-amd64 #1 SMP Debian 5.10.191-1 (2023-08-16) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

E a falha do login do luser1:

```
asist login: luser1  
Password:
```

```
Login incorrect  
asist login:
```

## User Story 8 1200583

8. Como administrador do sistema quero usar no sistema Linux o módulo PAM “pam\_cracklib.so” para obrigar os utilizadores a terem uma palavra-chave complexa. O entendimento de complexa deve ser explicado na resposta a esta user story.

Definimos o seguinte como regras para as senhas:

- . Deve ter pelo menos 8 caracteres.
- . Deve conter pelo menos um dígito.
- . Deve conter pelo menos uma letra maiúscula.
- . Deve conter pelo menos um símbolo.

Estas regras foram traduzidas adicionando uma linha no ficheiro /etc/pam.d/common-password. A linha adicionada foi a seguinte:

```
#uc 8  
password requisite pam_cracklib.so retry=3 minlen=8 dcredit=1 ucredit=1 ocredit=1
```