Ubuntu Server: Política de Segurança com a Suite PAM

No Ubuntu Server, a **Pluggable Authentication Modules (PAM)** é a suite responsável por gerir e aplicar as políticas de segurança de autenticação (como regras de passwords, bloqueio de contas e restrições de acesso).

As configurações do PAM ficam localizadas na diretoria `/etc/pam.d/`.

📂 Principais Ficheiros de Configuração

Em vez de alterar as regras aplicação por aplicação, o Ubuntu utiliza ficheiros comuns que afetam todo o sistema:

- **`/etc/pam.d/common-password`**: Define a complexidade e histórico das passwords.
- **`/etc/pam.d/common-auth`**: Trata da verificação da identidade (sucesso/falha no login) e bloqueio de contas.
- **`/etc/pam.d/common-account`**: Verifica se a conta do utilizador é válida (se não expirou ou se tem permissões de acesso).
- **`/etc/pam.d/common-session`**: Configura o ambiente que é aberto após o login (limites de recursos, montagem de pastas, etc.).

⚙️ Verificar as Políticas existentes

Antes de fazer alterações, verifique as configurações atuais da validade da password para um utilizador com o comando de chage. Este vai mostrar todos os detalhes de expiração de senha e conta de uma só vez.

Para tal corra o comando:

sudo chage -l username (altere o username pelo nome do utilizador)

```
Last password change                                    : Mar 22, 2026
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
```

1. Forçar Complexidade de Passwords (`pam_pwquality`)

Para garantir que os utilizadores criam passwords fortes, instale o módulo de qualidade:

```
sudo apt update && sudo apt install libpam-pwquality -y
```

Edite o ficheiro `/etc/pam.d/common-password` e procure pela linha `pam_pwquality.so`. Pode configurá-la para exigir regras rígidas:

```
password requisite pam_pwquality.so retry=3 minlen=12 ucredit=-1
lcredit=-1 dcredit=-1 ocredit=-1
```

- `minlen=12`: Tamanho mínimo de 12 caracteres.
- `ucredit=-1`, `lcredit=-1`, `dcredit=-1`, `ocredit=-1`: Exige pelo menos 1 maiúscula, 1 minúscula, 1 dígito e 1 carácter especial.
- `enforce_for_root`: Aplica as regras **inclusive** ao utilizador *root*.

2. Bloqueio de Conta após Falhas de Login (`pam_faillock`)

Para proteger o servidor contra ataques de força bruta, configure o bloqueio temporário no ficheiro `/etc/pam.d/common-auth`:

Adicione as seguintes linhas **antes** de qualquer outra regra de autenticação:

```
auth required pam_faillock.so preauth silent audit deny=5 unlock_time=900
fail_interval=900
```

E adicione a seguinte linha no final do ficheiro `/etc/pam.d/common-account`:

```
account required pam_faillock.so
```

- `deny=5`: Bloqueia a conta após 5 tentativas falhadas.
- `unlock_time=900`: O bloqueio dura 15 minutos (900 segundos).
- `fail_interval=900`: Tempo (em segundos) que a conta permanece bloqueada antes de ser desbloqueada automaticamente. Se definido para 0 ou omitido com certas configurações, o bloqueio pode exigir intervenção manual do administrador. 15 minutos → (900 segundos).
- `audit`: Ativa registos de auditoria detalhados para os eventos de falha e sucesso

3. Impedir a Reutilização de Passwords Antigas (`pam_pwhistory`)

Para evitar que os utilizadores alternem entre as mesmas passwords, edite `/etc/pam.d/common-password` e adicione à linha do módulo `pam_pwhistory.so` (ou crie-a caso não exista):

```
password required pam_pwhistory.so remember=5
```

- `remember=5`: O sistema lembra-se das últimas 5 passwords e impede a sua reutilização.

4. Validade de Passwords (/etc/login.defs)

Para colocar a validade nas passwords, edite o ficheiro `(/etc/login.defs)` procure pela seção "Password aging controls":

```
90 #
91 # Password aging controls:
92 #
93 #        PASS_MAX_DAYS   Maximum number of day
94 #        PASS_MIN_DAYS   Minimum number of day
95 #        PASS_WARN_AGE   Number of days warnin
96 #
97 PASS_MAX_DAYS   99999
98 PASS_MIN_DAYS   0
99 PASS_WARN_AGE   7
100
```

- PASS_MAX_DAYS: validade máxima das passwords (em dias). Mude para 90
- PASS_MIN_DAYS: validade mínima das passwords. Mude para 1
- PASS_WARN_AGE: para avisar que a password vai expirar (em dias)

🛠️ Comandos de Diagnóstico e Gestão

Se um utilizador legítimo for bloqueado pela política do `pam_faillock`, use os seguintes comandos como administrador:

- **Verificar tentativas de login falhadas:**

```
sudo faillock --user <nome_do_utilizador>
```

- **Desbloquear uma conta manualmente:**

```
sudo faillock --user <nome_do_utilizador> --reset
```

🛠️ Forçar o utilizador a alterar a senha no próximo login

Depois de criar uma nova conta ou redefinir uma password, vamos forçar o utilizador a definir uma nova password no próximo login. Esta é uma prática padrão ao provisionar contas. **Comando:**

sudo chage -d 0 ***username*** ***(altere o username pelo nome do utilizador)***

Verificar a mudança forçada está definida:

sudo chage -l *username* *(altere o username pelo nome do utilizador)*

