BIT - AUDITORIA DE ATIVIDADES DE USUÁRIOS EM GRUPO

Professor: Marcos Brandão

Versão: 2026

Registrar atividades dos usuários de um grupo

Este procedimento configura o **auditd** para registrar atividades dos usuários pertencentes ao grupo `turma_informatica_2026` e cria o comando `log_turma` para consultar essas informações.

> **Atenção:** o `auditd` registra execuções de programas e eventos do sistema. Ele não representa necessariamente, de forma literal, tudo que o usuário digitou no terminal.

---

1. Primeiro, confira a lista de usuários

Execute:

getent group turma_informatica_2026

O resultado deve apresentar o grupo e seus usuários, por exemplo:

turma_informatica_2026:x:1042:asantos,abrito,cramos,...

Para visualizar somente os usuários, execute:

getent group turma_informatica_2026 | cut -d: -f4 | tr ',' '\n'

---

2. Instale o sistema de auditoria

Execute:

sudo apt update
sudo apt install auditd audispd-plugins -y

Depois ative o serviço:

sudo systemctl enable --now auditd

Confira:

sudo systemctl status auditd --no-pager

O esperado é:

Active: active (running)

---

3. Crie as regras de auditoria para a turma

O comando abaixo cria automaticamente uma regra para cada usuário do grupo:

```
sudo bash -c '
for usuario in $(getent group turma_informatica_2026 | cut -d: -f4 | tr "," " "); do
    uid=$(id -u "$usuario")
    echo "-a always,exit -F arch=b64 -S execve -F auid=$uid -k turma_informatica_2026"
done > /etc/audit/rules.d/turma_informatica_2026.rules
'
```

Confira o arquivo:

```
sudo cat /etc/audit/rules.d/turma_informatica_2026.rules
```

---

4. Carregue as regras

Execute:

```
sudo augenrules --load
```

Depois confira:

```
sudo auditctl -l | grep turma_informatica_2026
```

Deverão aparecer regras semelhantes a:

```
-a always,exit -F arch=b64 -S execve -F auid=1073 -F key=turma_informatica_2026
```

O número depois de `auid=` corresponde ao UID do usuário.

Para verificar:

```
id ateste
```

---

5. Teste a auditoria

Entre no servidor com um usuário da turma e execute alguns comandos:

```
whoami
pwd
ls
date
id
mkdir teste_auditoria
```

Depois, como `professor`, consulte os eventos:

```
sudo ausearch -ua $(id -u ateste) -m EXECVE -i
```

Também é possível consultar pela chave:

```
sudo ausearch -k turma_informatica_2026 -i
```

> **Importante:** se a sessão do usuário já estava aberta antes da configuração da auditoria, faça logout e login novamente para realizar o teste.

---

6. Criar o comando `log_turma`

O comando `log_turma` facilita a consulta das informações da turma.

Ele permite:

log_turma

Consultar todos os usuários.

log_turma ateste

Consultar somente um usuário.

log_turma hoje

Consultar as atividades da turma realizadas hoje.

log_turma ateste hoje

Consultar somente as atividades de hoje de um usuário.

O relatório apresenta informações como:

- usuário;
- UID;
- situação da conta;
- último login;
- sessão atual;
- atividades registradas pelo `auditd`.

---

7. Exemplo de relatório

```
------------------------------------------------------------
USUÁRIO: ateste
UID:     1073
STATUS:  ATIVO

ÚLTIMO LOGIN:
  ateste pts/3 ::1 Tue Aug 25 11:42 - 11:47

SESSÃO ATUAL:
  Nenhuma sessão ativa.

ATIVIDADES DO USUÁRIO:
------------------------------------------------------------
  11:42:14  whoami
  11:42:18  ls --color=auto
  11:42:26  date
  11:42:30  id
  11:42:30  mkdir teste_audit
```

---

8. Consultar diretamente o auditd

Para consultar as atividades de um usuário:

sudo ausearch -ua 1073 -m EXECVE -i

Para consultar pelo nome do usuário:

sudo ausearch -ua ateste -m EXECVE -i

Para consultar as atividades registradas pela chave da turma:

sudo ausearch -k turma_informatica_2026 -i

---

9. Ver usuários conectados

Para verificar quem está conectado atualmente:

who

Ou:

w

Para consultar o histórico de logins:

last

Para consultar o histórico de um aluno específico:

last ateste

---

10. Verificar o status de um usuário

Para saber se a conta está ativa ou bloqueada:

sudo passwd -S ateste

Exemplo de usuário ativo:

ateste P 2026-08-25 0 99999 7 -1

Exemplo de usuário bloqueado:

ateste L 2026-08-25 0 99999 7 -1

P = senha ativa.

L = senha bloqueada.

---

11. Bloquear temporariamente um usuário

Para bloquear:

sudo passwd -l ateste

Para desbloquear:

sudo passwd -u ateste

Esse procedimento permite suspender temporariamente o acesso sem excluir a conta do usuário.

---

12. Manutenção das regras

Se novos usuários forem adicionados ao grupo depois que as regras forem criadas, é necessário atualizar as regras de auditoria para incluir os novos UIDs.

Confira os usuários:

getent group turma_informatica_2026

Depois recrie as regras:

```
sudo bash -c '
for usuario in $(getent group turma_informatica_2026 | cut -d: -f4 | tr "," " "); do
    uid=$(id -u "$usuario")
    echo "-a always,exit -F arch=b64 -S execve -F auid=$uid -k turma_informatica_2026"
done > /etc/audit/rules.d/turma_informatica_2026.rules
'
```

Carregue novamente:

sudo augenrules --load

E confira:

sudo auditctl -l | grep turma_informatica_2026

Resumo dos principais comandos

Objetivo	Comando
Ver usuários da turma	`getent group turma_informatica_2026`
Ver somente os usuários	`getent group turma_informatica_2026 | cut -d: -f4 | tr ',' '\n'`
Ver status do auditd	`sudo systemctl status auditd`
Ver regras	`sudo auditctl -l | grep turma_informatica_2026`
Consultar auditoria	`sudo ausearch -k turma_informatica_2026 -i`
Ver usuários conectados	`who`
Ver histórico de login	`last`
Relatório da turma	`log_turma`
Relatório de um aluno	`log_turma ateste`
Relatório de hoje	`log_turma hoje`

Relatório de um aluno hoje	`log_turma ateste hoje`
Bloquear usuário	`sudo passwd -l usuario`
Desbloquear usuário	`sudo passwd -u usuario`

Resultado

Após a implementação, o servidor passa a ter uma estrutura básica de **auditoria das atividades da turma**, permitindo ao professor acompanhar os acessos e as execuções de programas dos usuários sem precisar consultar manualmente os arquivos de log do Linux.