Segurança

Este capítulo reúne as políticas, práticas e mecanismos de segurança que você pode aplicar em seu Cloud Server da SafeArmor.

- Como Gerar uma Chave SSH
- Como Criar Senhas Seguras
- Visualizando e analisando logs no Cloud Server

Como Gerar uma Chave SSH

As chaves SSH permitem acessar servidores e serviços de forma segura, sem a necessidade de senha.
Siga este guia para criar uma chave SSH no Linux, macOS ou Windows.

---

1. Verificar se já existe uma chave SSH

Antes de criar uma nova, veja se já existem chaves no seu computador:

```
ls ~/.ssh
```

Se aparecerem arquivos como:

- id_rsa e id_rsa.pub
- id_ed25519 e id_ed25519.pub

então você já possui chaves SSH.

Se não existir, prossiga para criar uma nova.

2. Criar uma nova chave SSH

```
ssh-keygen -t ed25519 -C "seu-email@exemplo.com"
```

Durante o processo, será perguntado:

1. Local do arquivo da chave

Aperte Enter para usar o padrão:

```
~/.ssh/id_ed25519
```

1. Criar uma senha (passphrase) Recomendado inserir uma senha. Se não quiser, apenas aperte Enter.

3. Verificando a chave gerada

Após gerar, confira os arquivos:

```
ls ~/.ssh/id_ed25519*
```

Você deverá ver:

- id_ed25519 → chave privada (NUNCA compartilhe)
- id_ed25519.pub → chave pública (pode ser enviada)

4. Copiar a chave pública

Para copiar a chave pública:

```
cat ~/.ssh/id_ed25519.pub
```

Copie o conteúdo completo, algo como:

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAI... seu-email@exemplo.com
```

5. Adicionar a chave no servidor

Edite o arquivo authorized_keys no servidor:

```
mkdir -p ~/.ssh
nano ~/.ssh/authorized_keys
```

Cole a chave pública dentro do arquivo e salve.

Corrija as permissões (muito importante!):

```
chmod 700 ~/.ssh
chmod 600 ~/.ssh/authorized_keys
```

5.1 (ALTERNATIVA) Copiar a chave pública com `ssh-copy-id`

A forma mais prática e segura de enviar sua chave pública para um servidor Linux é usando o comando:

```
ssh-copy-id usuario@servidor
```

Como Criar Senhas Seguras

Ter uma senha forte é fundamental para proteger suas contas e arquivos na Safearmor. Siga estas recomendações:

1. Use comprimento adequado

- Prefira **no mínimo 12 caracteres**.
- Senhas mais longas são muito mais seguras.

2. Misture diferentes tipos de caracteres

- Letras maiúsculas (A*Z)
- Letras minúsculas (a*z)
- Números (0*9)
- Símbolos (!@#$%^&*()_+=[]{})

Exemplo: `S3gur@Saf3Armor!`

3. Evite senhas óbvias

- Nomes, datas de nascimento, palavras comuns ou sequências (`123456`, `senha`, `abcdef`).
- Frases famosas ou nomes de times também são fáceis de adivinhar.

4. Use frases ou combinações

- Combine palavras aleatórias para criar uma **passphrase** fácil de lembrar, mas difícil de adivinhar.
- Exemplo: `Gato$Livro7Céu!Sol`

5. Crie senhas localmente ou com o SafeVault

- Prefira criar senhas **mentalmente ou usando gerenciadores de senha confiáveis**
- Evite usar geradores de senha online, pois elas podem ser armazenadas em bancos de dados de terceiros.
- Com o **SafeVault**, você pode **gerar senhas seguras** diretamente na plataforma. As senhas geradas **são descartadas após uso**, garantindo privacidade total.

6. Não reutilize senhas

- Cada serviço deve ter uma senha **única**.
- Se uma senha vazar, outras contas não serão comprometidas.

7. Utilize gerenciadores de senha

- Ferramentas como **SafeVault, KeepassXC** ajudam a gerar e armazenar senhas complexas com segurança.
- Não anote senhas em papel ou arquivos desprotegidos.

8. Ative autenticação em dois fatores (2FA) sempre que possível

- Um código extra além da senha aumenta significativamente a segurança da sua conta.

Seguindo estas dicas, suas contas e dados na Safearmor ficarão muito mais protegidos contra acesso não autorizado.

Visualizando e analisando logs no Cloud Server

Este guia explica como acessar e interpretar logs no seu Cloud Server da Safearmor, uma etapa essencial para diagnóstico de problemas e auditoria do sistema.

---

1. O que são logs

Logs são registros automáticos gerados pelo sistema e pelos serviços em execução no servidor.

Eles registram eventos como:

- Tentativas de login
- Erros de aplicações
- Reinicializações de serviços
- Uso de recursos e falhas do sistema

---

2. Onde os logs ficam

Em servidores Linux, os principais logs ficam em:

- `/var/log/syslog` ou `/var/log/messages` (logs gerais do sistema)
- `/var/log/auth.log` (acessos e autenticação)
- Logs específicos de serviços (ex: web, banco de dados, Nextcloud, etc.)

---

3. Como visualizar logs em tempo real

Você pode acompanhar os logs ao vivo com o comando:

```
tail -f /var/log/syslog
```

Isso é útil para monitorar o sistema enquanto o problema acontece.

---

4. Como buscar erros específicos

Para filtrar apenas erros:

```
grep "error" /var/log/syslog
```

Ou para autenticação:

```
grep "failed" /var/log/auth.log
```

---

5. O que observar nos logs

Fique atento a:

- Mensagens de erro repetidas
- Falhas de autenticação
- Uso excessivo de recursos
- Serviços reiniciando constantemente

---

6. Boas práticas

- Verifique logs antes de abrir chamados
- Sempre anote o horário do problema
- Evite apagar logs sem necessidade
- Use logs para identificar padrões de falha

Conclusão

A análise de logs é uma das formas mais eficientes de diagnosticar problemas em um Cloud Server. O uso correto dessas informações reduz o tempo de resolução de incidentes e melhora a estabilidade do ambiente.