ANÁLISE DE LOGS (SYSTEMD/JOURNALCTL)

Responsável: João Pedro Toledo Gonçalves

Data: 26/01/2026

MANUAL TÉCNICO - ANÁLISE DE LOGS (SYSTEMD/JOURNALCTL)

Código: ITGENG 0011/26 | **Classificação:** RESTRITO
Responsável: João Pedro Toledo Gonçalves | **Data:** 26/01/2026

1. HISTÓRICO DE REVISÃO

Data	Versão	Descrição	Autor
26/01/2026	**1.0**	**Criação Inicial**	**João Pedro Toledo Gonçalves**

2. OBJETIVO

Capacitar a engenharia na extração, filtro e análise de logs centralizados do `systemd` via comando `journalctl`, substituindo a leitura manual de arquivos texto dispersos.

3. PRÉ-REQUISITOS

[ ] Servidor rodando Systemd (Todas as distros modernas listadas).
[ ] Acesso root ou usuário no grupo `systemd-journal`.
---

4. USO BÁSICO E FILTRAGEM

O `journalctl` exibe logs de todos os serviços unificados.

Filtrar por Serviço (Unit)

A forma mais comum de debug.

```
journalctl -u nginx
journalctl -u ssh
journalctl -u docker
```

Visualizar em Tempo Real (Follow)

Igual ao `tail -f`.

```
journalctl -u nginx -f
```

Filtrar por Tempo (Since / Until)

Essencial para incidentes ("O que aconteceu ontem às 14h?").

```
journalctl --since "2023-10-20 14:00:00" --until "2023-10-20 14:30:00"
journalctl --since "1 hour ago"
journalctl --since "today"
```

Filtrar por Prioridade (Erro/Crítico)

Isola apenas problemas reais.

- 0: emerg
- 1: alert
- 2: crit
- 3: err
- 4: warning

```
journalctl -p err -b 0
```

(`-b 0` limita ao boot atual, ignorando reboots passados)

---

5. PERSISTÊNCIA DE LOGS

Por padrão, muitas distros configuram o journald como **Volátil** (memória RAM), perdendo logs ao reiniciar.

1. [x] Verifique o armazenamento:

```
    cat /etc/systemd/journald.conf | grep Storage
```

2. [x] Para ativar persistência:

- Opção A (Automática): Crie a pasta de logs.

```
        sudo mkdir -p /var/log/journal
        sudo systemd-tmpfiles --create --prefix /var/log/journal
        sudo systemctl restart systemd-journald
```

- Opção B (Config): Edite `/etc/systemd/journald.conf` e defina `Storage=persistent`.

6. LIMPEZA E MANUTENÇÃO (VACUUM)

Logs binários podem crescer muito. Limpe-os seguramente:

- **Manter apenas 1GB:**

```
journalctl --vacuum-size=1G
```

- **Manter apenas os últimos 10 dias:**

```
journalctl --vacuum-time=10d
```

7. EXPORTAÇÃO DE DADOS

Para enviar logs para devs ou anexar em chamados.

- **Sem paginação (Texto Puro):**

```
journalctl -u servico --no-pager > log_exportado.txt
```

- **Formato JSON (Para ELK/Splunk):**

```
journalctl -u servico -o json-pretty
```

8. ALPINE LINUX (SEM SYSTEMD)

> **IMPORTANTE**
>
> **ATENÇÃO:** O Alpine Linux usa **OpenRC** e não Systemd. Portanto, o comando `journalctl` **NÃO EXISTE**.

No Alpine, os logs são arquivos de texto tradicionais (Syslog):

- **Log Principal:** `/var/log/messages` (Tudo vai para cá).
- **Kernel:** `/var/log/dmesg`.
- **Auth (SSH):** `/var/log/messages` (ou `/var/log/auth.log` se configurado).

Comandos Substitutos:

- Ver em tempo real: `tail -f /var/log/messages`
- Buscar erro: `grep "error" /var/log/messages`

9. VALIDAÇÃO FINAL

[ ] O comando `journalctl` retorna dados (em distros Systemd)?
[ ] Os logs persistem após um reboot?
[ ] A rotação de logs (Vacuum) está funcionando para não lotar o disco?