SAYCON CONSULTORIA

RSYSLOG

COLETA, PROCESSAMENTO E ROTEAMENTO INTELIGENTE DE LOGS

Centralização de logs para segurança, auditoria, observabilidade e continuidade operacional

Solução open source para centralização e transporte confiável de eventos

1. O QUE É O RSYSLOG?

RSyslog é uma plataforma open source de alto desempenho para coleta, filtragem, normalização, armazenamento e encaminhamento de logs. Compatível com Linux, aplicações, firewalls, switches, roteadores e diversos dispositivos.

Ele cria uma base confiável para segurança, auditoria, troubleshooting e observabilidade, reduzindo a dispersão de logs e aumentando o controle da infraestrutura.

Com arquitetura modular, filas resilientes e suporte a múltiplos protocolos, o RSyslog garante entrega segura, ordenada e persistente dos eventos ao destino certo.

2. FLUXO DE TRATAMENTO DOS LOGS

1. **COLETA** — Recebe logs de arquivos locais, journal, rede e aplicações
2. **PROCESSAMENTO** — Aplica parsing, filtros, templates e normalização
3. **FILAS E PROTEÇÃO** — Usa filas em memória e disco para reduzir perda de eventos
4. **ENTREGA** — Encaminha para arquivos, SIEM, Wazuh, Grafana Loki, Elastic/OpenSearch, Kafka e mais

ARQUIVOS LOCAIS | JOURNAL | SYSLOG | SIEM | NUVEM | OUTROS DESTINOS

SEGURANÇA E RASTREABILIDADE | AUTOMAÇÃO E CONTROLE | ALTA PERFORMANCE | FILAS RESILIENTES | INTEGRAÇÃO COM SIEM | ESCALÁVEL ON-PREM OU CLOUD

3. COMPONENTES DA PLATAFORMA

A — COLETORES E INPUTS
- imuxsock e imjournal
- imfile para arquivos locais
- imudp, imtcp e imelp
- Coleta local e remota

B — FILTROS E RULESETS
- Regras por origem e severidade
- Separação por aplicação
- Redução de ruído
- Priorização de eventos críticos

C — PARSING E TEMPLATES
- RFC3164 e RFC5424
- JSON e formatação customizada
- Normalização de mensagens
- Enriquecimento para análise

D — FILAS E CONFIABILIDADE
- Filas em memória
- Filas em disco
- Retry e buffer em falhas
- Continuidade do fluxo

E — OUTPUTS E ACTIONS
- Arquivos locais
- Relay centralizado
- Encaminhamento seguro
- Integração com plataformas externas

4. INTEGRAÇÕES E DESTINOS

FONTES — Linux, aplicações, firewalls, switches, roteadores

PROTOCOLOS — UDP, TCP, TLS, RELP

PLATAFORMAS — Wazuh, Grafana Loki, Elastic / OpenSearch, Kafka, SIEM

DESTINOS — Arquivos, servidor central, data lake, observabilidade

AMBIENTES — On-premises, cloud ou híbrido

5. RECURSOS TÉCNICOS AVANÇADOS

FILTROS AVANÇADOS — Por host, severity, programa e conteúdo

POLÍTICAS E REGRAS — Roteamento inteligente e regras por contexto

AUDITORIA E RETENÇÃO — Histórico, organização e rastreabilidade

TRANSPORTE SEGURO — TLS criptografado e RELP confiável

ALTA PERFORMANCE — Leve, estável e eficiente

ESCALABILIDADE — Suporte a ambientes maiores e distribuídos

6. DIFERENCIAIS DO RSYSLOG

- ✓ Open source maduro e estável
- ✓ Excelente desempenho em Linux
- ✓ Forte compatibilidade com syslog tradicional
- ✓ Arquitetura modular e flexível
- ✓ Menor consumo de recursos
- ✓ Ótimo custo-benefício
- ✓ Ideal para centralização, auditoria e observabilidade

RSYSLOG VS OUTRAS PLATAFORMAS

RECURSO	RSYSLOG	OUTRAS SOLUÇÕES
Leveza e desempenho	✓	⊖
Filas persistentes	✓	⊖
Transporte TLS	✓	⊖
Suporte a RELP	✓	✗
Roteamento flexível	✓	⊖
Integração com SIEM	✓	✓
Custo-benefício	✓	✗

7. RESULTADOS PARA SUA EMPRESA

- ✓ Mais visibilidade e controle
- ✓ Redução de riscos e perda de logs
- ✓ Mais produtividade na análise de eventos
- ✓ Menos retrabalho e maior agilidade
- ✓ Base sólida para auditoria e compliance
- ✓ Ambiente preparado para crescer

TENHA CONTROLE TOTAL SOBRE SEUS LOGS.

COLETE. ORGANIZE. ENCAMINHE.

Conte com a Saycon Consultoria para planejar, implantar e integrar o RSyslog ao seu ambiente.

saycon.com.br | (11) 98053-9425 | @sayconconsultoria | SAYCON CONSULTORIA