Caçadores de Logs

Desvendando Segredos da Rede com graylog

SEMANA CAPACITAÇÃO NIC.BR
23 DE SETEMBRO DE 2025
MICHAEL SOARES

AGENDA

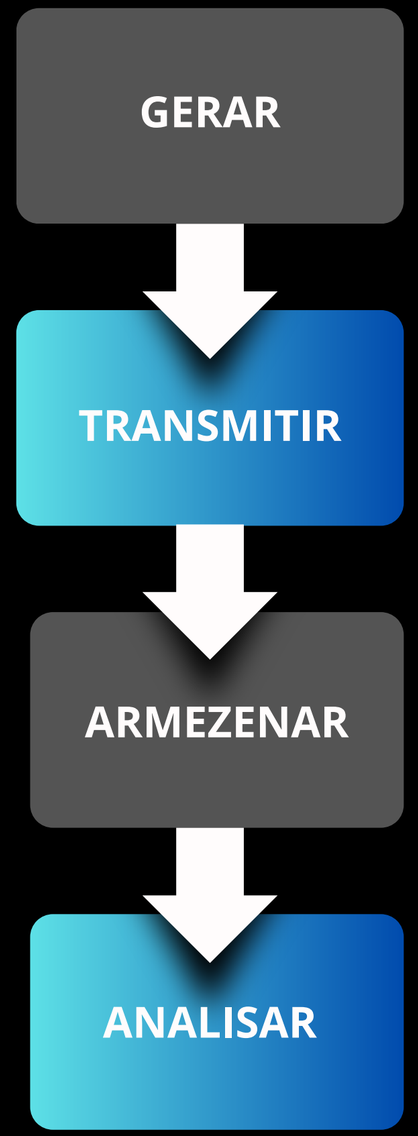
- Conceitos de logs **01**
- Por que Graylog? **02**
- Arquitetura e instalação **03**
- Coleta e análise de logs **04**
- Laboratório prático **05**

CONCEITOS DE

Logs

- REGISTROS AUTOMATIZADOS DE EVENTOS EM SISTEMAS E REDES
- TIPOS: AUDITORIA, TRANSAÇÃO, EVENTO, ERRO, MENSAGEM E SEGURANÇA
- CAMPOS: DATA/HORA, USUÁRIO, DISPOSITIVO, ID DO EVENTO E DESCRIÇÃO

Ciclo de vida de um log



SYSLOG E

Severidade

- PROTOCOL STANDARD IETF (RFC 5424)
- PORTA UDP 514 E TPC 6514 (TLS)
- MENSAGENS ENVIADAS A UM SERVIDOR CENTRAL

Severidade	Descrição
Emergência	Sistema inutilizável
Alerta	Ação imediata para estabilidade do sistema
Crítico	Falhas de sistemas importantes
Erro	Erro que requer atenção em um determinado período
Aviso	Um erro pode ocorrer se nada for feito
Notificação	Condição normal, como uma transição de rede
Informativo	Mensagens informacionais
Depuração	Mensagens de debug

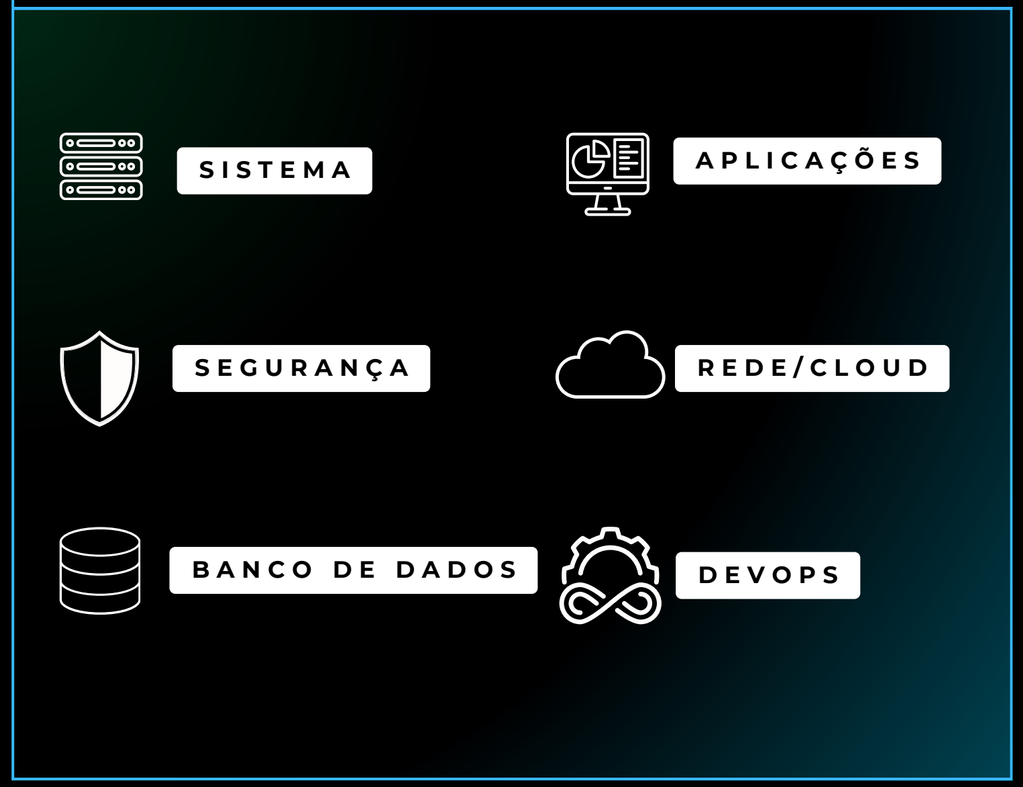
CENTRALIZAÇÃO E

Ciclo de Logs

- UNIFICA FORMATOS VARIADOS DE LOGS
- PERMITE CORRELAÇÃO DE EVENTOS COMPLEXOS
- GARANTE ALERTAS DE ALTA FIDELIDADE
- RETENÇÃO RECOMENDADA ≥ 1 ANO

TIPOS DE LOGS E FORMATOS

Diversas categorias e formatos exigem estratégias distintas



Categoria	Exemplos
Estruturado	JSON, XML
Semi-estruturado	CSV, Syslog
Proprietário	CEF, Avro, Parquet

Normalização

- PADRONIZAR CAMPOS E TIPOS DE DADOS
- REMOVER REDUNDÂNCIAS E CONSOLIDAR REGISTROS
- CRIAR IDENTIFICADORES ÚNICOS
- CONSULTAS MAIS RÁPIDAS E MENOR ARMAZENAMENTO
- DESAFIOS: FONTES DIVERSAS E ALTO VOLUME
- DASHBOARDS E CORRELAÇÕES COESAS

Enriquecimento

- ADICIONAR GEOLOCALIZAÇÃO POR IP
- RESOLVER IDENTIDADE DE USUÁRIO E HOST
- ATRIBUIR PONTUAÇÃO DE RISCO E CONTEXTO
- SIDECAR GERENCIA COLETORES REMOTOS

Maturidade em **Gestão de Logs**

EVOLUA DA COLETA BÁSICA PARA AUTOMAÇÃO E MELHORIA CONTÍNUA.

CADA NÍVEL ADICIONA VALOR POR MEIO DE CORRELAÇÕES, DASHBOARDS, AUTOMAÇÃO E APRENDIZADO, CULMINANDO EM ADAPTAÇÃO CONTÍNUA.

NÍVEL 1:

COLETA BÁSICA E ALERTAS MANUAIS

NÍVEL 2:

CORRELAÇÕES, DASHBOARDS E RELATÓRIOS

NÍVEL 3:

AUTOMAÇÃO DE RESPOSTAS E WORKFLOWS

NÍVEL 4:

MODELAGEM DE RISCO E MACHINE LEARNING

NÍVEL 5:

INTEGRAÇÃO E MELHORIA CONTÍNUA

Boas Práticas de Logging

Utilize formatos estruturados (JSON, XML) para facilitar o processamento

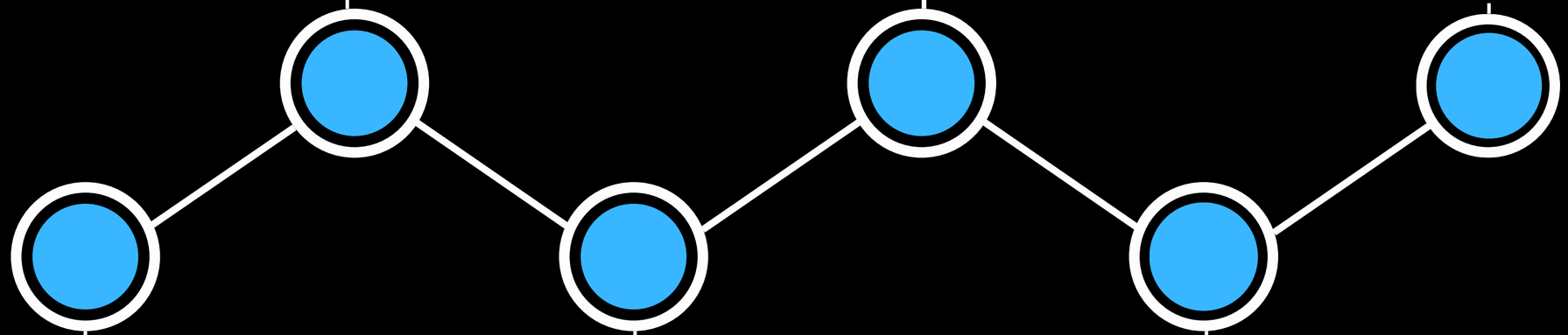
Inclua contexto: timestamps, IDs, IP, host e requisição

Evite registrar dados sensíveis (PII, senhas, financeiras)

Capture logs de aplicativos, servidores, dispositivos e nuvem

Aplique filtros/pipelines para reduzir ruído e indexe eficientemente

Implemente políticas de retenção e rotação por compliance



SEGURANÇA & Conformidade

- Proteger integridade: hashing, assinaturas e controles de acesso
- Monitorar, correlacionar e enriquecer logs para caçar ameaças
- Implementar File Integrity Monitoring para auditoria
- Criptografar logs em trânsito e em repouso
- Cumprir normas (GDPR, HIPAA, SOC 2, PCI) e políticas internas
- Nunca registrar dados confidenciais; aplicar mascaramento/redação

POR QUE graylog

Ingestão ilimitada e gerenciamento centralizado

Alertas configuráveis e relatórios

Pesquisa rápida e em tempo real

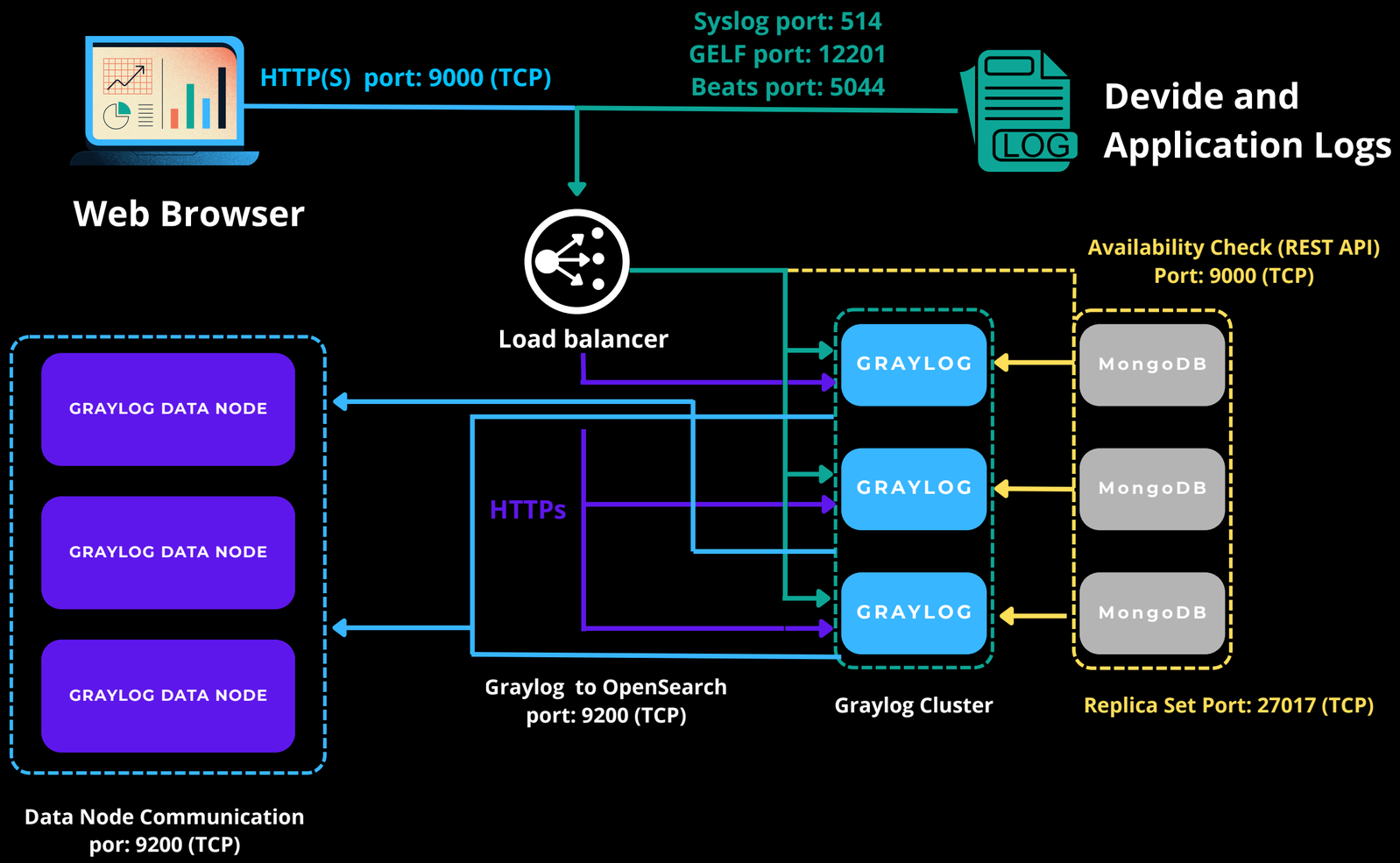
Dashboards personalizáveis

Novidades da versão 6.3

- INTEGRAÇÃO DO GOOGLE CLOUD STORAGE (GCS)
- PROCEDIMENTOS DE EVENTOS E COMPARTILHAMENTO DE RELATÓRIOS
- AUTENTICAÇÃO SAML
- INTEGRAÇÃO MIMECAST V2.0

https://dominandoograylog.com.br/

Arquitetura do graylog



- GRAYLOG UTILIZA OPENSEARCH/ELASTICSEARCH PARA INDEXAÇÃO
- MONGODB ARMAZENA METADADOS E CONFIGURAÇÃO
- VÁRIAS INSTÂNCIAS DE GRAYLOG PODEM SER BALANCEADAS

https://dominandoograylog.com.br/

Coleta de **Logs**

Fontes suportadas:

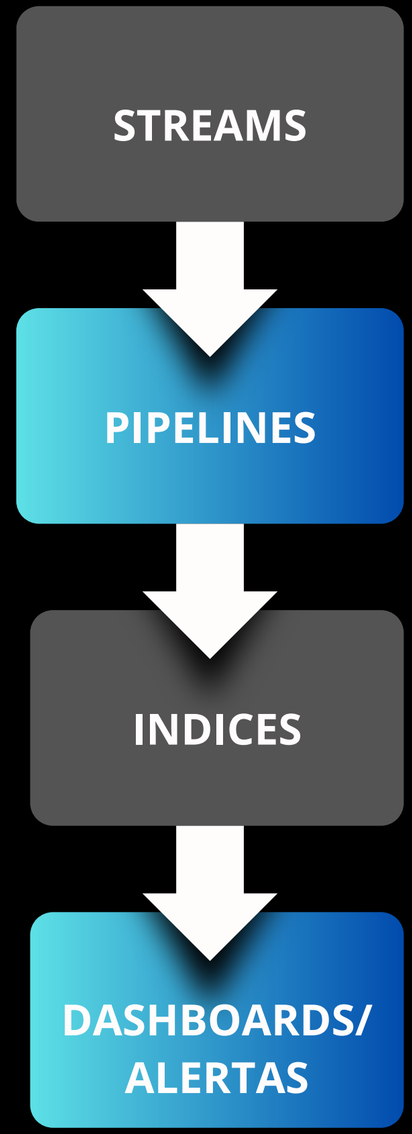
- Syslog (UDP/TCP)
- GELF via HTTP/UDP
- Beats/Logstash
- AWS CloudWatch/CloudTrail
- NetFlow/IPFIX
- CEF, JSON e texto bruto

Protocolo	Porta
Syslog (TCP/UDP)	514
Syslog (TCP/TLS)	6514
GELF (TCP/UDP)	12201
Beats	5044

STREAMS, PIPELINES E

Dashboards

- STREAMS: ROTEIAM MENSAGENS PARA DIFERENTES CATEGORIAS
- PIPELINES: APLICAM REGRAS DE LIMPEZA E ENRIQUECIMENTO
- INDICES: ONDE OS LOGS SÃO ARMAZENADOS
- DASHBOARDS: VISUALIZAÇÕES INTERATIVAS DOS DADOS
- ALERTAS: GATILHOS CONFIGURÁVEIS BASEADOS EM CONDIÇÕES



CONCLUSÃO

Logs são essenciais para segurança, desempenho e conformidade

Centralização e normalização possibilitam detectar padrões e responder a incidentes de forma eficiente

Graylog oferece uma solução poderosa, escalável e amigável para provedores e administradores de redes

Continue explorando e adaptando as práticas de observabilidade às suas necessidades.

https://dominandoograylog.com.br/

AMBIENTE DE LABORATÓRIO

UTILIZAREMOS ORACLE VIRTUALBOX PARA O LABORATÓRIO

1. Baixar VirtualBox para Windows, macOS ou Linux
2. Importar as VMs: pfSense, Graylog e Web Server
3. Validar a configuração das VMs de acordo com o seu ambiente
4. Inicializar as VMs e garantir conectividade com Internet e acesso entre as VMs

Exercícios **Práticos**

- Configurar as VMs e instalar o Graylog
- Criar Inputs no Graylog para recepcionar os logs e liberar portas no firewall
- Configurar o monitoramento de logs de um servidor web Nginx
- Configurar o monitoramento de logs de um firewall pfSense
- Criar um dashboard no Graylog com as informações coletadas