

# Gabriel Santos

Concluiu seus estudos em 19 de agosto de 2020 o curso  
516 - Auditoria de Logs  
ministrado pela empresa 4Linux e  
cumprindo a carga horária de 20 horas.



**RODOLFO GOBBI**

DIRETOR GERAL

Para validar a autenticidade deste certificado  
acesse [aia.4linux.com.br/admin/tool/certificate/index.php](http://aia.4linux.com.br/admin/tool/certificate/index.php)  
e digite o código: **2902618243GS**

# Ementa de Curso

Gabriel Santos  
Concluiu os estudos em 19 de agosto de 2022  
no curso 516 - Auditoria de Logs  
ministrado pela empresa 4Linux e  
cumprindo a carga horária de 20 horas.

A autenticidade deste documento pode ser verificada em:  
[aia.4linux.com.br/admin/tool/certificate/index.php](http://aia.4linux.com.br/admin/tool/certificate/index.php)  
digitando o código: [2902618243GS](#)

-----

## Conteúdo Programático

### Preparando o ambiente do Curso

- Instalar e configurar o Virtualbox
- Instalar o Ansible
- Instalar o Git
- Instalar o Vagrant
- Obter arquivos do curso

### Introdução ao Sistema de Logs

- Conhecer as diferenças entre syslog, syslog-ng, rsyslog
- Configuração padrão de rsyslog em Ubuntu, Debian e Centos
- Entendendo o que são os facilities e os severity levels
- Localização padrão de arquivos de logs
- Gerencia de arquivos de logs, permissões, tamanho com o logrotate
- Procurando, analisando e resolvendo problemas através de logs

### Auditoria de acesso ao Sistema

- Instalação e configuração do auditd
- Criação de regras de auditoria para acesso e alteração de arquivos

- Criação de regras para execução de syscalls
- Visualização e busca de eventos com o ausearch e aureport
- Auditando o que foi digitado em um terminal com pam\_tty\_audit
- Encaminhando eventos para o syslog através do audispd-plugins

## **Gerenciar Logs Remoto**

- Configuração de armazenamento de logs
- Log remoto utilizando a criptografia TLS
- Planejamento de capacidade e backup
- Armazenando logs no MySQL
- Planejamento de capacidade e backup do mysql

## **Centralização de Logs com Graylog**

- Instalação e configuração do Graylog (Graylog + Elastic + MongoDB)
- Configurando e entendendo os Inputs disponíveis
- Coletando logs dos hosts pelo Rsyslog
- Coletando logs de Containers
- Criando extratores baseados em Regex
- Realizando buscas
- Criando dashboards
- Criando alertas (Email e RocketChat)

## **Centralização de Logs com ELK**

- Instalação e configuração da pilha ELK (Elastic, Logstash e Kibana)
- Ingerindo e filtrando logs com o Logstash
- Utilizando o FileBeat para envio de arquivos logs
- Realizando buscas
- Criando dashboards

## **Gerenciar Logs na AWS com o Cloudwatch**

- Criar conta gratuita na AWS
- Introdução ao Cloudwatch
- Criar função CloudWatchFullAccess
- Criar instância na AWS
- Acessar instância na AWS
- Instalar e configurar Cloudwatch Agent

- Visualizar logs da instância no console do Cloudwatch
- Configurar e visualizar logs de um servidor Web
- Configurar e visualizar logs de containers

## **Gerenciar Logs na GCP com o Stackdriver**

- Criar conta gratuita na GCP
- Introdução ao Stackdriver
- Criar instância na GCP
- Acessar instância na GCP
- Instalar e configurar o agente do Cloud Logging
- Visualizar logs da instância no console da GCP
- Configurar e visualizar logs de um servidor Web
- Configurar e visualizar logs de containers