4·Linux Open Software Specialists™

CERTIFICADO

Certificate

Lucas Freitas Santos

Concluiu seus estudos no curso **704 - Linux Network Engineer: Análise de Logs e Segurança com IA** ministrado pela empresa 4Linux e cumprindo a carga horária de 40 horas.

7 de outubro de 2026



RODOLFO GOBBI

DIRETOR GERAL

Para validar a autenticidade deste certificado acesse aia.4linux.com.br/admin/tool/certificate/ e digite o código: 9922893054LF

Ementa de Curso

Lucas Freitas Santos
Concluiu seus estudos no curso **704 - Linux Network Engineer: Análise de Logs e Segurança com IA** ministrado pela empresa 4Linux e cumprindo a carga horária de 40 horas.
7 de outubro de 2026

A autenticidade deste documento pode ser verificado em aia.4linux.com.br/admin/tool/certificate/ digitando o código 9922893054LF

Aula 01 — Preparação do Ambiente Cloud e IA

Competências da Aula

- Compreender o papel da **cloud computing** no contexto de atuação de um **Linux Network Engineer**.
- Reconhecer, em nível prático, as diferenças entre os modelos **IaaS**, **PaaS** e **SaaS**.
- Entender por que o curso utiliza a **Google Cloud Platform (GCP)** como ambiente de laboratório para simular uma infraestrutura corporativa distribuída.
- Validar ou criar uma conta na **Google Cloud Platform** e acessar o **Console da GCP** e o **Google Cloud Shell**.
- Identificar os principais componentes de rede utilizados no curso, como **VPC**, sub-redes, endereçamento IP, regras de firewall, rotas, **Cloud Router** e **Cloud NAT**.
- Compreender que a **VPC** é um recurso global, enquanto sub-redes, **Cloud Router** e **Cloud NAT** são recursos regionais.
- Entender o uso de múltiplas regiões da GCP nos laboratórios e o papel do file-server em uma região distinta.
- Compreender a diferença entre conectividade interna, exposição externa e acesso de saída para a internet.
- Entender a arquitetura do projeto integrador **OpsCenter - Portal de Engenharia** e o papel dos principais servidores da infraestrutura.
- Compreender o uso do domínio interno empresa.lan no ambiente de laboratório.
- Entender como a IA será utilizada como **copiloto operacional**, aplicando o fluxo de validação baseado em evidências técnicas.
- Conhecer o papel do **Goose** como ferramenta de apoio para terminal, troubleshooting e

documentação técnica.
- Validar ou criar acesso ao **Google AI Studio**, gerar uma chave de API para modelos Gemini e adotar boas práticas de segurança no tratamento de credenciais.

Aula 02 — Provisionamento de Infraestrutura com Terraform

Competências da Aula

- Compreender o conceito de **Infrastructure as Code**, ou **IaC**;
- Entender por que IaC é importante para ambientes escaláveis, reproduzíveis e auditáveis;
- Reconhecer o papel do **Terraform** no provisionamento de infraestrutura cloud;
- Entender a estrutura básica da linguagem **HCL - HashiCorp Configuration Language**;
- Identificar os principais blocos usados em arquivos Terraform:
    - terraform;
    - provider;
    - resource;
    - variable;
    - output;
- Instalar ou validar o **Terraform CLI** no **Google Cloud Shell**;
- Configurar o **Provider da Google Cloud**;
- Compreender o papel do **Terraform State**;
- Criar uma primeira instância simples usando Terraform;
- Listar recursos criados na GCP;
- Acessar uma instância via SSH;
- Remover recursos com terraform destroy;
- Criar uma VPC customizada;
- Criar uma sub-rede regional;
- Criar IP externo estático;
- Criar regra de firewall para acesso HTTP;
- Criar uma instância conectada à VPC customizada;
- Usar metadata_startup_script para instalar o NGINX automaticamente;
- Validar acesso à aplicação usando o IP externo.

Aula 03 — Infraestrutura do OpsCenter e Conectividade Inicial

Competências da Aula

- Compreender a infraestrutura base do projeto **OpsCenter - Portal de Engenharia**;
- Identificar os principais recursos criados na Google Cloud;
- Navegar pelos arquivos Terraform do projeto;
- Provisionar a infraestrutura usando Terraform;
- Validar VPC, sub-redes, firewall, IPs, Cloud Router, Cloud NAT e instâncias;
- Diferenciar instâncias públicas e privadas;
- Testar conectividade entre servidores da mesma VPC;
- Acessar o linux-client como estação interna de validação;
- Usar comandos Linux para análise de rede, rotas e portas;
- Instalar e testar o **Goose** como copiloto operacional no terminal.

Aula 04 — Firewall Local, Firewall Cloud e Modelo de Segurança

Competências da Aula

- Compreender o conceito de firewall em múltiplas camadas no ambiente **OpsCenter - Portal de Engenharia**;
- Diferenciar firewall cloud, firewall local, regras da aplicação e controles de proxy;
- Revisar as regras de firewall da Google Cloud criadas via Terraform;
- Entender a diferença entre conectividade liberada, acesso controlado, política de segurança e exposição pública;
- Criar uma matriz inicial de comunicação entre os servidores do projeto OpsCenter;
- Introduzir o **nftables** como ferramenta de firewall local em distribuições baseadas em Debian;
- Compreender os conceitos de tabelas, chains, regras, hooks, prioridades e políticas padrão no nftables;
- Diferenciar tráfego de entrada, saída, local, encaminhado e entre servidores;
- Compreender os conceitos de filtro de pacotes, NAT, DNAT, SNAT, masquerade e redirecionamento de portas;
- Aplicar uma política de bloqueio padrão nos servidores Linux do laboratório;
- Configurar regras locais com nftables para liberar apenas os acessos necessários;
- Configurar redirecionamento controlado da porta 2222 da bastion-host para o SSH do linux-client;
- Ajustar regras de firewall cloud da GCP para permitir acesso controlado à porta alta da bastion;
- Validar o acesso ao linux-client por meio da bastion-host usando o Google Cloud Shell;
- Validar o acesso externo ao linux-client usando chave SSH privada e usuário do OS Login.

Aula 05 — Bastion Host e VPN com OpenVPN

Competências da Aula

- Compreender o papel do **Bastion Host** no acesso administrativo seguro;
- Diferenciar acesso via IP público, Bastion Host, VPN e rede interna;
- Compreender o modelo de VPN **host-to-gateway**;
- Instalar e configurar o **OpenVPN** no bastion-host;
- Criar uma autoridade certificadora interna com **Easy-RSA**;
- Gerar certificados para o servidor VPN e para o cliente analista01;
- Configurar parâmetros básicos do servidor OpenVPN;
- Definir o pool de endereços da VPN;
- Habilitar **IP forwarding** no Linux;
- Ajustar regras locais com nftables para permitir o tráfego da VPN;
- Liberar a porta 1194/UDP no firewall cloud da Google Cloud;
- Gerar e baixar o perfil VPN analista01.ovpn;
- Conectar o desktop do aluno à VPN;
- Validar acesso à rede privada usando endereços IP;
- Acessar o linux-client por meio do túnel VPN;
- Diagnosticar problemas comuns de conexão, rotas, firewall, NAT e autenticação;
- Revogar certificados de clientes VPN usando CRL.

Aula 06 — DNS com BIND9

Competências da Aula

- Compreender o papel do **DNS** em ambientes Linux, cloud e redes internas;
- Diferenciar domínio, zona, registros DNS e resolução direta/reversa;
- Entender o papel do infra-core-server como DNS interno do projeto **OpsCenter - Portal de Engenharia**;

- Instalar e configurar o **BIND9** no infra-core-server;
- Configurar as opções globais do BIND9 em named.conf.options;
- Criar e declarar a zona direta empresa.lan;
- Criar e declarar a zona reversa 0.10.10.in-addr.arpa;
- Configurar registros A, CNAME, MX, NS e PTR;
- Validar configurações com named-checkconf e named-checkzone;
- Testar resolução DNS com dig, host e nslookup;
- Liberar consultas DNS nas portas 53/UDP e 53/TCP;
- Ajustar regras locais com nftables;
- Configurar clientes Linux para usar o DNS interno com systemd-resolved;
- Usar ~empresa.lan para rotear consultas diretas ao DNS interno;
- Usar ~0.10.10.in-addr.arpa para rotear consultas reversas ao DNS interno;
- Integrar o DNS interno aos clientes conectados via OpenVPN;
- Validar resolução de nomes internos a partir da VPN;
- Diagnosticar problemas comuns envolvendo BIND9, zonas, firewall, VPN e DNS do cliente;
- Usar o Goose para apoiar a criação de checklists de diagnóstico.

Aula 07 — Aplicação Web e NGINX Proxy Reverso

Competências da Aula

- Compreender o papel da aplicação web no projeto **OpsCenter - Portal de Engenharia**;
- Entender o papel do application-server como servidor da aplicação;
- Entender o papel do proxy-server como ponto de entrada HTTP do portal;
- Diferenciar servidor web, aplicação backend, proxy reverso e balanceador de carga;
- Realizar o deploy inicial da aplicação **Python/Flask** no application-server;
- Executar a aplicação com **Gunicorn**;
- Configurar a aplicação como serviço do sistema com **systemd**;
- Utilizar arquivo .env para definir o estágio da aplicação no curso;
- Configurar a aplicação no estágio da Aula 07 com OPSCENTER_COURSE_STAGE=7;
- Validar a aplicação localmente no application-server;
- Instalar e configurar o **NGINX** no proxy-server;
- Configurar o NGINX como **proxy reverso HTTP**;
- Criar o virtual host para portal.empresa.lan;
- Encaminhar requisições do proxy-server para o backend app.empresa.lan:8000;
- Ajustar o DNS interno para resolver portal.empresa.lan;
- Entender a diferença entre acessar o portal por IP e por nome DNS;
- Configurar firewall local no Oracle Linux com **firewalld**;
- Criar uma zona dedicada chamada opscenter no firewalld;
- Liberar SSH e HTTP apenas para a rede interna e para a rede VPN;
- Compreender o papel do **SELinux** no controle de ações de processos;
- Permitir que o NGINX acesse backends remotos com httpd_can_network_connect;
- Validar acesso ao portal a partir da VPN;
- Analisar logs da aplicação e do NGINX;
- Diagnosticar falhas básicas envolvendo HTTP, DNS, backend, proxy reverso, systemd, firewall e SELinux;
- Usar o Goose para apoiar a criação de checklists de troubleshooting;
- Encerrar as instâncias do laboratório para reduzir consumo de créditos.

Aula 08 — HTTPS e Publicação Segura

Competências da Aula

- Compreender a evolução da publicação do portal de **HTTP** para **HTTPS**;
- Entender a diferença entre HTTP, HTTPS, SSL e TLS;
- Compreender o conceito de **TLS termination** no proxy reverso;
- Identificar o papel do proxy-server como ponto de terminação HTTPS;
- Entender que o backend continua privado em app.empresa.lan:8000;
- Compreender a função de certificados digitais, chave pública, chave privada, CSR e SAN;
- Criar uma **CA interna** para uso no laboratório;
- Gerar chave privada, CSR e certificado para portal.empresa.lan;
- Criar e organizar a estrutura de certificados em /etc/nginx/ssl/;
- Configurar o NGINX para escutar em 443/TCP com TLS;
- Configurar redirecionamento de HTTP para HTTPS na porta 80/TCP;
- Manter o NGINX como proxy reverso para o backend Flask/Gunicorn;
- Configurar regras de firewall local para liberar HTTPS apenas para redes autorizadas;
- Ajustar a zona opscenter no firewalld para comportamento semelhante a policy drop;
- Atualizar o estágio da aplicação para OPSCENTER_COURSE_STAGE=8;
- Validar HTTPS com curl, curl -k, curl --cacert e openssl s_client;
- Instalar a CA interna no linux-client para confiar no certificado do portal;
- Validar o acesso ao portal sem ignorar a verificação do certificado;
- Verificar cabeçalhos básicos de segurança HTTP;
- Analisar logs HTTP e HTTPS do NGINX;
- Diagnosticar falhas básicas envolvendo certificado, porta 443, proxy reverso, backend, firewall e SELinux.

Aula 09 — OpenLDAP, Kerberos e Login no Portal OpsCenter

Competências da Aula

- Compreender o conceito de diretório e identidade centralizada;
- Entender o modelo LDAP e sua estrutura hierárquica;
- Diferenciar identidade, autenticação e autorização;
- Entender o papel do infra-core-server como servidor central de identidade;
- Instalar e configurar o **OpenLDAP** no infra-core-server;
- Criar a base LDAP dc=empresa,dc=lan;
- Criar unidades organizacionais para usuários e grupos;
- Criar usuários LDAP para o ambiente OpsCenter;
- Criar grupos LDAP com membros associados;
- Utilizar arquivos **LDIF** para administrar objetos LDAP;
- Pesquisar usuários e grupos com ldapsearch;
- Testar autenticação LDAP com ldapwhoami;
- Modificar objetos LDAP com ldapmodify;
- Criar e remover objetos de teste no LDAP;
- Compreender o papel do **Kerberos** em autenticação centralizada;
- Instalar e configurar o **MIT Kerberos KDC**;
- Criar o realm Kerberos EMPRESA.LAN;
- Criar principals de usuários e serviços;
- Criar principal administrativo do Kerberos;
- Gerar e validar keytabs de serviço;
- Testar tickets Kerberos com kinit, klist e kdestroy;
- Compreender a dependência entre Kerberos, DNS e sincronização de horário;
- Configurar regras de firewall para LDAP e Kerberos;

- Validar LDAP e Kerberos a partir do linux-client;
- Atualizar a aplicação OpsCenter para o estágio da Aula 09;
- Configurar variáveis LDAP no .env da aplicação;
- Validar o login no portal https://portal.empresa.lan;
- Diagnosticar falhas comuns de DNS, LDAP, Kerberos, firewall e aplicação.

Aula 10 — Banco de Dados para Aplicação

Competências da Aula

- Compreender o papel do banco de dados na arquitetura do **OpsCenter - Portal de Engenharia**;
- Entender como a aplicação passa a consumir dados persistentes e estruturados a partir do MariaDB;
- Identificar o fluxo de comunicação entre application-server e database-server;
- Diferenciar os conceitos de:
    - banco local;
    - banco remoto;
    - autenticação local;
    - autenticação remota;
    - permissão de banco;
    - permissão de rede;
- Reconhecer o papel dos comandos SQL nos grupos:
    - DDL, DML, DQL, DCL;
- Configurar regras de firewall cloud na GCP para permitir acesso ao MariaDB somente a partir do application-server;
- Configurar firewall local no database-server usando firewalld;
- Instalar e configurar o **MariaDB** no database-server;
- Executar a configuração inicial segura do MariaDB;
- Configurar o bind-address para permitir acesso remoto controlado ao banco;
- Criar o banco de dados opscenter;
- Criar usuários MariaDB para a aplicação e para backup;
- Aplicar permissões específicas ao usuário da aplicação;
- Restringir o acesso remoto ao banco por origem autorizada;
- Configurar resolução DNS interna para o alias db.empresa.lan;
- Validar conectividade TCP/3306 entre application-server e database-server;
- Testar o acesso remoto ao banco usando cliente MariaDB;
- Atualizar o arquivo .env da aplicação com OPSCENTER_COURSE_STAGE=10;
- Configurar a variável DATABASE_URL para integração da aplicação com o MariaDB;
- Inicializar as tabelas da aplicação OpsCenter;
- Popular o inventário inicial da aplicação;
- Reiniciar e validar o serviço da aplicação;
- Validar o portal em https://portal.empresa.lan exibindo **Banco de dados: OK**;
- Confirmar que o inventário é carregado a partir do banco MariaDB;
- Executar consultas SQL básicas no inventário da aplicação;
- Inserir, consultar e remover registros de teste no banco;
- Realizar backup da base opscenter usando dump;
- Restaurar a base de dados a partir de um arquivo .sql;
- Criar uma base separada para teste de restore;
- Diagnosticar falhas comuns envolvendo DNS, rede, firewall, serviço MariaDB, permissões, credenciais, DATABASE_URL, backup e restore.

Aula 11 — NFS, Samba, SFTP e Documentação Técnica do OpsCenter

Competências da Aula

- Compreender o papel de um servidor de arquivos em ambientes Linux e cloud;
- Diferenciar os protocolos NFS, SMB/CIFS, SFTP, FTP e FTPS;
- Entender quando utilizar NFS para compartilhamento Linux-to-Linux;
- Instalar e configurar o serviço NFS no file-server;
- Criar exports NFS para acesso controlado pelo application-server;
- Montar compartilhamentos NFS manualmente e via /etc/fstab;
- Compreender o uso do Samba/SMB para compartilhamento com clientes internos;
- Instalar e configurar o Samba no file-server;
- Criar compartilhamentos acessíveis pelo linux-client;
- Aplicar permissões POSIX usando usuários e grupos centralizados;
- Integrar permissões de arquivos com grupos vindos do LDAP/SSSD;
- Configurar acesso SFTP seguro para upload de documentos técnicos;
- Criar áreas de entrada, publicação e colaboração de documentos do OpsCenter;
- Validar acesso, leitura, montagem e permissões nos compartilhamentos;
- Ajustar regras de firewall cloud e firewall local para NFS, SMB e SFTP;
- Diagnosticar problemas envolvendo DNS, NFS, Samba, SFTP, permissões e grupos.

Aula 12 — Servidor de E-mail com Postfix e Dovecot

Competências da Aula

- Compreender o fluxo de e-mail em ambientes Linux;
- Diferenciar os papéis de MTA, MDA, MUA, SMTP e IMAP;
- Identificar a função do Postfix como servidor de envio, recebimento e entrega de mensagens;
- Identificar a função do Dovecot como serviço de acesso às caixas postais via IMAP/IMAPS;
- Preparar o mail-server como servidor de e-mail interno do projeto OpsCenter;
- Configurar registros DNS necessários para e-mail, incluindo registros A e MX;
- Ajustar regras de firewall cloud e firewall local para serviços de e-mail;
- Integrar o mail-server com usuários centralizados via SSSD, LDAP e Kerberos;
- Criar diretórios Maildir para usuários do ambiente;
- Instalar e configurar o Postfix no mail-server;
- Configurar parâmetros principais do Postfix, como domínio, hostname, redes confiáveis e entrega local;
- Habilitar armazenamento de mensagens no formato Maildir;
- Criar certificado TLS de laboratório para uso nos serviços de e-mail;
- Preparar o Postfix para autenticação SASL via Dovecot;
- Habilitar o serviço Submission na porta 587/TCP;
- Instalar e configurar o Dovecot no mail-server;
- Configurar o Dovecot para acesso IMAP e IMAPS;
- Configurar autenticação plain e login com proteção por TLS;
- Configurar o socket de autenticação do Dovecot para integração com o Postfix;
- Testar envio local de mensagens no próprio mail-server;
- Testar envio e leitura de e-mails a partir do linux-client;
- Validar comunicação SMTP, Submission, IMAP e IMAPS;
- Ler mensagens via IMAP usando openssl s_client;
- Criar aliases de e-mail no Postfix para notificações do OpsCenter;
- Validar entrega de mensagens para múltiplos usuários por meio de aliases;

- Consultar logs do Postfix e do Dovecot para diagnóstico;
- Localizar mensagens nos logs por remetente, destinatário, status e ID de fila;
- Verificar e reprocessar a fila de mensagens do Postfix;
- Gerar falhas controladas para análise de logs e troubleshooting;
- Atualizar a configuração da aplicação OpsCenter para envio de notificações por e-mail;
- Validar o envio de e-mails pela interface web do OpsCenter;
- Diagnosticar problemas envolvendo DNS, MX, firewall, Postfix, Dovecot, SSSD, TLS, Maildir, autenticação, logs e fila de e-mails.

Aula 13 — Proxy Web com Squid

Competências da Aula

- Compreender o papel do **proxy web direto** em redes corporativas e diferenciá-lo do **proxy reverso** e do **proxy transparente**.
- Entender a utilização do proxy-server como **NGINX (proxy reverso)** e **Squid (proxy direto)** no ambiente OpsCenter.
- Instalar e configurar o serviço **Squid**, habilitando sua execução e definindo a porta 3128/TCP.
- Restringir o acesso ao proxy utilizando ACLs e redes autorizadas.
- Configurar listas de domínios permitidos e bloqueados, compreendendo a importância da ordem das regras http_access.
- Restringir portas e métodos HTTP, incluindo o método CONNECT.
- Validar a configuração do Squid e gerenciar o serviço com systemctl.
- Configurar regras do **firewalld** para proteger o acesso ao proxy.
- Evitar a exposição de um proxy aberto à internet.
- Configurar clientes Linux para utilização do Squid, incluindo variáveis http_proxy, https_proxy e no_proxy.
- Tornar a configuração de proxy persistente e utilizá-la também com o APT.
- Validar o funcionamento do proxy utilizando testes HTTP e HTTPS com curl.
- Analisar os principais logs do Squid e interpretar seus códigos de acesso.
- Diagnosticar falhas relacionadas a DNS, conectividade, firewall, ACLs, HTTPS e variáveis de ambiente.
- Reconhecer as limitações do Squid e compará-lo com soluções modernas de proxy e segurança web.
- Integrar o Squid ao **OpsCenter** por meio das variáveis de ambiente da aplicação.
- Validar o funcionamento do proxy no portal OpsCenter e executar testes controlados de falha.

Aula 14 — Operação Assistida por IA com Goose, MCP e Monitoramento

Competências da Aula

- Compreender o papel de um agente de IA na operação de ambientes Linux corporativos;
- Diferenciar o uso da IA para explicação, diagnóstico, execução assistida e correção controlada;
- Entender o papel do **Goose** como agente operacional local;
- Entender o papel do **MCP - Model Context Protocol** como camada de integração entre a IA e ferramentas do ambiente;
- Configurar uma extensão operacional controlada para o ambiente **OpsCenter**;
- Utilizar prompts estruturados para diagnóstico de serviços Linux;
- Utilizar prompts estruturados para correção automática com backup, validação e rollback;
- Provocar falhas controladas em serviços reais do laboratório;
- Diagnosticar e corrigir falhas em **NGINX**, **HTTPS/TLS**, **LDAP/Kerberos**, **MariaDB**, **NFS**,

Postfix/Dovecot, **Squid** e **OpsCenter**;
- Validar o ambiente após cada correção;
- Registrar evidências de troubleshooting.

Aula 15 — Capacity Planning e Troubleshooting Integrado

Competências da Aula

- Compreender a metodologia estruturada de troubleshooting.
- Diferenciar indisponibilidade, lentidão, saturação de recurso, erro de configuração, bloqueio de rede, falha de autenticação e falha de DNS.
- Revisar a arquitetura final do projeto **OpsCenter - Portal de Engenharia**.
- Mapear servidores, serviços, IPs, rotas, portas, DNS, firewall e dependências do ambiente.
- Levantar informações do sistema com comandos Linux básicos.
- Analisar processos, CPU, memória, disco, I/O, rede e conexões.
- Interpretar **Load Average** e relacioná-lo à quantidade de CPUs do servidor.
- Utilizar ferramentas como ps, top, htop, free, vmstat, mpstat, df, du, iostat, iotop, lsof, ss, ip, curl, ping, traceroute e nc.
- Instalar e configurar o pacote **sysstat**.
- Coletar e interpretar métricas históricas com sar.
- Realizar testes controlados de stress em CPU, memória, disco e I/O.
- Compreender os riscos de stress testing em ambiente cloud.
- Instalar e utilizar o **Netdata** como ferramenta leve de observabilidade.
- Diagnosticar falhas por camadas: rede, rotas, VPN, DNS, firewall, serviços, aplicação, banco, e-mail, proxy e HTTPS.
- Analisar logs do ambiente com journalctl e arquivos em /var/log.
- Consultar logs de serviços como OpenVPN, BIND9, LDAP, Kerberos, NFS, Samba, Postfix, Dovecot, MariaDB, NGINX, Squid e aplicação OpsCenter.
- Capturar tráfego de rede com tcpdump.
- Correlacionar sintomas, evidências e causa raiz.
- Usar ferramentas de apoio, como o **Goose**, com validação técnica antes de aplicar correções.
- Gerar documentação final da infraestrutura do OpsCenter.
- Registrar instâncias, IPs, DNS, portas, regras de firewall, serviços, certificados, volumes, dependências e pendências.
- Planejar e executar o descomissionamento da infraestrutura com Terraform.
- Validar a remoção de recursos na GCP para evitar cobranças residuais.