LPI 202 - Konfiguracja usług serwerowych i ich bezpieczeństwo (kod: LPI-202 (autoryzowane))

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Najbliższe terminy
2026-11-30 (Zdalnie)
2026-11-30 (Warszawa)

Opis i cel szkolenia

Pięć dni szkoleniowych na temat usług, które administrator Linuksa typowo uruchamia i utrzymuje w firmowej sieci.

Konfigurujemy serwer DNS w BIND, serwery WWW (Apache i Nginx) z obsługą HTTPS, udostępniamy pliki przez Sambę i NFS, ustawiamy DHCP oraz logowanie użytkowników różnymi metodami (PAM, SSSD i OpenLDAP), a potem pocztę w Postfixie i Dovecocie. Ostatnia część to bezpieczeństwo: zapora i NAT, SSH, FTP, fail2ban i OpenVPN. Pracujemy w konsoli.

Po szkoleniu:

- skonfigurujesz serwer DNS dla własnych stref i zabezpieczysz go,
- uruchomisz witryny w Apache i Nginx z certyfikatami HTTPS, a Nginx ustawisz jako reverse proxy,
- udostępnisz pliki przez Sambę i NFS i poznasz dołączanie serwera Samba do domeny Active Directory,
- skonfigurujesz DHCP i centralne logowanie użytkowników przez LDAP,
- uruchomisz serwer poczty z filtrowaniem wiadomości i szyfrowanym dostępem IMAP,
- zabezpieczysz serwer i sieć (zapora, NAT, SSH z kluczami, VPN) i przygotujesz się do egzaminu LPIC-2 202.

Program szkolenia odpowiada celom egzaminu **LPIC-2 202**. ALX jest autoryzowanym partnerem **Linux Professional Institute**. Certyfikat ***LPIC-2 Linux Engineer*** uzyskuje się po zdaniu dwóch egzaminów, 201 i 202 (do pierwszego przygotowuje szkolenie LPI 201); warunkiem jest aktywny certyfikat LPIC-1. Egzamin - dla chętnych - zazwyczaj zdaje się online.

Szkolenie przyda się administratorom systemów Linux i sieci, inżynierom infrastruktury, DevOps i SRE, osobom utrzymującym serwery WWW, pocztowe i plikowe, a także wszystkim, którzy przygotowują się do certyfikacji LPIC-2. Kto chce pogłębić tylko jedną usługę, np. DNS, pocztę albo Sambę, znajdzie odpowiednie "dedykowane" szkolenia wśród naszych kursów i szkoleń Linux.

Czas trwania

5 dni, 9:00 - 17:00

Program

1. Serwer DNS: BIND
   - serwer autorytatywny i buforujący, rndc, logowanie
   - strefy proste i odwrotne, rekordy, delegowanie, named-checkzone
   - bezpieczeństwo: praca bez uprawnień roota, chroot, forwardery, TSIG
   - rzut okiem na DNSSEC, DANE, dnsmasq i PowerDNS
2. Serwer WWW: Apache
   - konfiguracja Apache, logi, hosty wirtualne, przekierowania
   - ograniczanie dostępu, uwierzytelnianie klientów, .htaccess
   - moduły i PHP, limity procesów i klientów
   - HTTPS: klucze prywatne, CSR, certyfikaty własne i z urzędu certyfikacji, certyfikaty pośrednie, SNI
   - wyłączanie słabych protokołów i szyfrów

3. Nginx i Squid
   — Nginx jako serwer WWW i reverse proxy
   — Squid jako serwer proxy z buforowaniem: ACL, uwierzytelnianie klientów
4. Udostępnianie plików
   — Samba: serwer samodzielny i członek domeny Active Directory, udziały plikowe i drukarki
   — mapowanie użytkowników, diagnostyka, klienci Linux: smbclient, mount.cifs
   — NFS: eksporty, opcje montowania, kontrola dostępu; rzut okiem na NFSv4
5. Zarządzanie klientami sieci
   — serwer DHCP: podsieci, pule adresów, dzierżawy; rzut okiem na DHCPv6 i radvd
   — PAM: konfiguracja i moduły, nsswitch
   — SSSD i uwierzytelnianie przez LDAP
   — klient LDAP: wyszukiwanie, modyfikacja, zmiana hasła
   — serwer OpenLDAP: konfiguracja cn=config, schematy, LDIF, kontrola dostępu
6. Poczta elektroniczna
   — Postfix: konfiguracja, podstawy SMTP, TLS, aliasy, logi; rzut okiem na Sendmail i Exim
   — filtrowanie poczty regułami Sieve, autoresponder; rzut okiem na Procmail
   — Dovecot: dostęp IMAP i POP3, TLS
7. Bezpieczeństwo systemu
   — Linux jako router: przekazywanie pakietów, NAT, przekierowanie portów
   — reguły filtrowania iptables i ip6tables, zapisywanie i odtwarzanie reguł; rzut okiem na nftables
   — SSH: konfiguracja serwera OpenSSH, ograniczenia logowania, logowanie kluczem
   — serwery FTP: vsftpd i Pure-FTPd, tryb aktywny i pasywny
   — skanowanie portów (nmap), fail2ban, źródła informacji o podatnościach; rzut okiem na OpenVAS i Snort
8. OpenVPN
   — połączenia punkt–punkt i między sieciami

Dla grup na zamówienie możemy rozłożyć akcenty inaczej, np. więcej czasu poświęcić Sambie i integracji z Active Directory, poczcie albo bezpieczeństwu, i dopasować przykłady do dystrybucji używanej w firmie (Red Hat, Ubuntu, Debian, SUSE).

Przeznaczenie i wymagania

Szkolenie jest przeznaczone przede wszystkim dla:
— administratorów systemów Linux i sieci,
— osób, które utrzymują serwery WWW, pocztowe, plikowe i katalogowe,
— inżynierów infrastruktury, DevOps i SRE,
— osób przygotowujących się do certyfikacji LPIC-2.

Od uczestników oczekujemy swobody w podstawowej administracji Linuksem, mniej więcej na poziomie LPIC-1, oraz ogólnej orientacji w sieciach TCP/IP. Taką wiedzę można zdobyć w pracy albo na szkoleniach LPI 101 i LPI 102. Udział w szkoleniu LPI 201 nie jest warunkiem.

Certyfikaty

Uczestnicy szkolenia otrzymują imienne certyfikaty sygnowane przez ALX.

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Najbliższe terminy
2026-11-30 (Zdalnie)
2026-11-30 (Warszawa)

Lokalizacje

— Warszawa – ul. Jasna 14/16A
— Zdalnie – zajęcia realizowane poprzez platformę Zoom
— Kraków – ul. św. Filipa 23
— Warsaw (English) – Jasna 14/16A
— Online (English) – your home, office or wherever you want
— na życzenie dowolne miejsce w Polsce, lub UE (zajęcia prowadzone w języku angielskim)

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Cena szkolenia

3990 PLN netto (VAT 23%)

W cenę szkoleń organizowanych w naszej siedzibie wliczone są:

— autorskie materiały szkoleniowe,
— indywidualne stanowisko komputerowe do pracy podczas zajęć,
— certyfikaty ukończenia szkolenia,
— drobny poczęstunek oraz ciepłe i zimne napoje,
— możliwość jednorazowego kontaktu z instruktorem (instruktorami) po szkoleniu i zadawania pytań dotyczących materiału szkolenia.

Cena szkolenia nie zawiera obiadów. Można je dokupić w cenie 35 zł netto za obiad.

Najbliższe terminy
2026-11-30 (Zdalnie)
2026-11-30 (Warszawa)