Updated on 13/08/2025

Sign up

Zimbra training

2 days (14 hours)

Overview

Zimbra is an enterprise messaging and collaboration platform built on open standards, offering messaging, calendaring, contacts and sharing with total control over data sovereignty. This on-prem or hybrid cloud solution is based on proven components (Postfix, Nginx, LDAP, antivirus/antispam) and a modern web client.

Our Zimbrae training course will enable you to install and configure Zimbra, secure the sending chain (SPF/DKIM/DMARC), activate client services (IMAP/POP/CalDAV/CardDAV/ActiveSync) and industrialize operations (backups, supervision, updates).

You'll be able to troubleshoot effectively, manage compliance and optimize the user experience.

Following this training, you'll be able to install and configure Zimbra Collaboration, understand its architecture and conduct a reliable and secure production launch.

As with all our training courses, this one covers the latest stable version v10.1.11 of Zimbra.

Objectives

- Deploy a Zimbra platform in production
- Implement SPF/DKIM/DMARC and TLS
- Manage accounts, COS, domains and resources
- Activate client protocols and optimize UX
- Organize backups, supervision and patching

Target audience

- System administrators
- DevOps
- Network engineers
- IT teams

Prerequisites

- Linux basics
- SMTP/IMAP/POP/HTTP[S] basics
- Knowledge of TLS, certificates and DNS

Our Zimbra training program

Zimbra architecture & components

- Zimbra Collaboration overview (Daffodil) : Mailbox, MTA (Postfix), Proxy (Nginx), LDAP, MariaDB, Zimlets
- Single-server vs. multi-server topologies; system and network requirements
- Ports, services and flows (SMTP/IMAP/POP/HTTP[S]/CalDAV/CardDAV)
- Admin console vs. CLI: zmcontrol, zmprov, logs
- Maintenance: patches, restarts, health checks
- Workshop: mapping an infrastructure and validating prerequisites

Installation & initial configuration

- OS preparation, accounts, DNS, TLS certificates
- Daffodil installation and post-installation; domains & COS configuration
- Account creation, aliases, lists; GAL and resources
- Password policies, quotas, HSM (concepts), retention
- Web Client customization, Zimlets
- Workshop: deploying a pilot domain with 3 accounts and 1 COS

Mail security & compliance

- Secure chain: SPF, DKIM, DMARC; MTA-STS/TLS-RPT
- Anti-spam/AV: Amavis, ClamAV, SpamAssassin, rules
- S/MIME users & directories, opportunistic/strict TLS
- 2FA and admin delegation, auditing
- Logging, retention & legal hold
- Workshop: DKIM activation, DMARC testing and TLS verification

Services & clients

- IMAP/POP/SMTP protocols, CalDAV/CardDAV, ActiveSync
- Zimbra Web Client: options, filters, shares

- Connectors: ZCO, mobile, third-party integrations
- Briefcase, tasks, sharing and delegation
- UX & productivity best practices
- Workshop: configuring a typical workstation and sorting rules

Backup, monitoring & troubleshooting

- NG Backup & OSE alternatives; restoration
- Supervision: logs, metrics, alerts
- CLI tools and scripts; quota & MTA file management
- Diagnostics: SMTP, auth, proxy, perfs
- Capacity: storage, IOPS, HSM/archives
- Workshop: simulate a failure and restore a box

Advanced operation & production releases

- Patching & upgrades, OS compatibility
- Split into roles, HA & PRA scenarios
- Modern UI & legal banner branding
- Automation and CSP hardening
- Go-Live checklist and rollback
- Workshop: go-live checklist + rollback

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming training course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire is used to check that skills have been correctly acquired.

Certification

A certificate will be awarded to each trainee who completes the training course.