

Mis à jour le 13/08/2025

S'inscrire

Formation Zimbra

2 jours (14 heures)

Présentation

Zimbra est une plateforme de messagerie et collaboration d'entreprise bâtie sur des standards ouverts, offrant messagerie, calendriers, contacts et partage avec un contrôle total sur la souveraineté des données. Cette solution on-prem ou cloud hybride s'appuie sur des composants éprouvés (Postfix, Nginx, LDAP, antivirus/antispam) et un client web moderne.

Notre formation Zimbrae vous permet d'installer et configurer Zimbra, de sécuriser la chaîne d'envoi (SPF/DKIM/DMARC), d'activer les services clients (IMAP/POP/CalDAV/CardDAV/ActiveSync) et d'industrialiser l'exploitation (sauvegardes, supervision, mises à jour).

Vous serez capable de dépanner efficacement, de gérer la conformité et d'optimiser l'expérience utilisateur.

À la suite de cette formation, vous serez en mesure d'installer et configurer Zimbra Collaboration, d'en comprendre l'architecture et de conduire une mise en production fiable et sécurisée.

Comme toutes nos formations, celle-ci couvre la dernière version stable [v10.1.11 de Zimbra](#).

Objectifs

- Déployer une plateforme Zimbra en production
- Mettre en place SPF/DKIM/DMARC et TLS
- Administrer comptes, COS, domaines, ressources
- Activer les protocoles clients et optimiser l'UX
- Organiser sauvegardes, supervision et patching

Public visé

- Administrateurs systèmes
- DevOps
- Ingénieurs réseau
- Équipes IT

Pré-requis

- Bases Linux
- Notions SMTP/IMAP/POP/HTTP[S]
- Connaissances TLS, certificats et DNS

Programme de notre formation Zimbra

Architecture & composants Zimbra

- Panorama Zimbra Collaboration (Daffodil) : Mailbox, MTA (Postfix), Proxy (Nginx), LDAP, MariaDB, Zimlets
- Topologies mono-serveur vs multi-serveurs ; prérequis système et réseau
- Ports, services et flux (SMTP/IMAP/POP/HTTP[S]/CalDAV/CardDAV)
- Console Admin vs CLI : zmcontrol, zmprov, journaux
- Maintenance : patches, restarts, vérifications santé
- Atelier : cartographier une infra et valider les prérequis

Installation & configuration initiale

- Préparation OS, comptes, DNS, certificats TLS
- Installation Daffodil et post-install ; configuration domains & COS
- Création comptes, alias, listes ; GAL et ressources
- Politiques de mots de passe, quotas, HSM (concepts), rétention
- Personnalisation Web Client, Zimlets
- Atelier : déployer un domaine pilote avec 3 comptes et 1 COS

Sécurité messagerie & conformité

- Chaîne sécurisée : SPF, DKIM, DMARC ; MTA-STS/TLS-RPT
- Anti-spam/AV : Amavis, ClamAV, SpamAssassin, règles
- S/MIME utilisateurs & annuaires, TLS opportuniste/strict
- 2FA et délégation d'admin, audit
- Journalisation, rétention & legal hold
- Atelier : activer DKIM, tester DMARC et vérifier TLS

Services & clients

- Protocoles IMAP/POP/SMTP, CalDAV/CardDAV, ActiveSync
- Zimbra Web Client : options, filtres, partages

- Connecteurs : ZCO, mobiles, intégrations tierces
- Briefcase, tâches, partages et délégations
- Bonnes pratiques UX & productivité
- Atelier : configurer un poste type et des règles de tri

Sauvegarde, supervision & dépannage

- Sauvegardes NG Backup & alternatives OSE ; restauration
- Supervision : logs, métriques, alertes
- Outils CLI et scripts ; gestion quotas & files MTA
- Diagnostic : SMTP, auth, proxy, perfs
- Capacité : stockage, IOPS, HSM/archives
- Atelier : simuler une panne et restaurer une boîte

Exploitation avancée & mises en production

- Patching & upgrades, compatibilité OS
- Split en rôles, scénarios HA & PRA
- Branding Modern UI & bannière légale
- Automatisation et durcissement CSP
- Check-list Go-Live et rollback
- Atelier : check-list de mise en prod + rollback

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.