Sparks

0 805 950 800 · appel gratuit
demande@sparks-formation.com

Formation Keycloak : administration et exploitation

Réf. SF34726

Déployez, configurez et faites vivre une plateforme Keycloak fiable et sécurisée : de la fédération de vos annuaires au cluster haute disponibilité supervisé.

3 j Durée	2 100 € HT Inter / participant	0 Sessions à venir

Objectifs pédagogiques

✓ Déployer Keycloak en mode production avec une base de données externe, TLS et un reverse proxy

✓ Configurer des flux d'authentification sécurisés : authentification multifacteur, politiques de mot de passe, protection contre la force brute

✓ Administrer les realms, clients, utilisateurs et rôles, y compris la délégation d'administration

✓ Mettre en place un cluster Keycloak haute disponibilité et durci

✓ Fédérer les identités de l'entreprise via LDAP/Active Directory, Kerberos et des fournisseurs d'identité externes OIDC ou SAML

✓ Superviser, sauvegarder, mettre à jour et automatiser une plateforme Keycloak en production

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux, Ingénieurs DevOps

Prérequis- Pratique de l'administration Linux et de la ligne de commande - Bonnes bases réseau : HTTP, DNS, TLS et certificats, reverse proxy - Notions de bases de données relationnelles et de conteneurs (Docker ou Podman) - Notions d'annuaire LDAP / Active Directory ; une première approche d'OAuth 2.0 / OpenID Connect est un plus

Programme détaillé

Architecture et concepts de Keycloak

– Gestion des identités et des accès : rôle d’un fournisseur d’identité, SSO et centralisation de l’authentification en entreprise
– Keycloak et Red Hat build of Keycloak : positionnement, écosystème et rythme de publication
– OpenID Connect et OAuth 2.0 côté administrateur : flux recommandés, jetons d’accès, d’identité et de rafraîchissement, flux hérités à désactiver
– SAML 2.0 côté administrateur : fournisseur d’identité et fournisseur de service, métadonnées, assertions signées
– Modèle de Keycloak : realms, clients, utilisateurs, groupes, rôles et client scopes
– Architecture du serveur : moteur Quarkus, base de données, cache Infinispan, console d’administration et endpoints exposés

Activités pratiques :

– Suivi d’une authentification de bout en bout : redirections, endpoints sollicités et décodage des jetons émis
– Exploration de la console d’administration et du discovery endpoint d’un realm

Installation et configuration du serveur

– Modes de distribution : archive, image conteneur, déploiement sur Kubernetes avec le Keycloak Operator
– Mode développement et mode production : différences de comportement, build optimisé et options fixées au build
– Configuration du serveur : fichier de configuration, variables d’environnement, ligne de commande et gestion des secrets
– Base de données externe : PostgreSQL, MariaDB ou Oracle, paramétrage du pool de connexions
– Exposition du service : nom d’hôte, TLS et certificats, reverse proxy et en-têtes transmis
– Interface de management : health checks et métriques séparés du trafic public
– Import et export de realms : initialiser une instance et transférer une configuration entre environnements

Activités pratiques :

– Déploiement de Keycloak en mode production avec une base PostgreSQL externe, derrière un reverse proxy TLS

© 2026 Sparks Formation. Tous droits réservés. Fiche générée depuis https://www.sparks-formation.com/formation/keycloak-administration-exploitation/

– Export d’un realm depuis une instance de développement et import dans l’instance de production

Administration des realms, clients et utilisateurs

– Realm master et realms applicatifs : isolement, comptes d’administration et bonnes pratiques
– Stratégies de segmentation : realm par environnement, par client ou par périmètre métier, Organizations pour le multitenant
– Clients OpenID Connect et SAML : clients publics et confidentiels, URI de redirection, secrets et rotation, comptes de service
– Client scopes et mappers : contrôler les informations et les rôles transmis dans les jetons et les assertions
– Utilisateurs, groupes et rôles : profil utilisateur, rôles de realm et de client, rôles composites, actions requises
– Sessions et jetons : durées de vie, sessions hors ligne, révocation, impersonation encadrée
– Clés de realm : fournisseurs de clés et rotation des clés de signature
– Délégation d’administration : permissions d’administration fines pour confier un périmètre à une équipe

Activités pratiques :

– Création d’un realm d’entreprise avec groupes, rôles et politiques de session
– Mise en SSO sans développement de deux applications, l’une en OpenID Connect, l’autre en SAML, via un reverse proxy
– Délégation de la gestion des utilisateurs d’un périmètre à un administrateur restreint

Fédération d'identités

– User federation LDAP et Active Directory : connexion à l’annuaire, recherche des utilisateurs, modes d’édition
– Mappers LDAP : récupérer attributs, groupes et rôles depuis l’annuaire
– Synchronisation : complète ou incrémentale, périodique ou à la demande
– Kerberos et SPNEGO : SSO transparent pour les postes Windows du domaine
– Identity brokering : déléguer l’authentification à un fournisseur OIDC ou SAML (Microsoft Entra ID, ADFS, autre Keycloak, fournisseurs sociaux)
– Première connexion via un fournisseur externe : first broker login flow, liaison avec les comptes existants, mappers d’IdP
– Déconnexion globale : back-channel logout OpenID Connect et Single Logout SAML

Activités pratiques :

– Fédération d’un annuaire OpenLDAP et synchronisation des utilisateurs et des groupes
– Connexion d’un fournisseur d’identité externe (Microsoft Entra ID ou second Keycloak) et mapping des attributs reçus

Sécurisation de l'authentification

– Flux d’authentification : étapes, sous-flux, exécutions conditionnelles et flux spécifiques par client
– Authentification multifacteur : OTP, WebAuthn et passkeys, MFA conditionnel selon le rôle ou l’application
– Politiques de mot de passe : longueur, complexité, historique et algorithme de hachage
– Protection contre la force brute : verrouillage temporaire ou permanent des comptes
– Actions requises et parcours utilisateur : vérification d’e-mail, renouvellement du mot de passe, enrôlement OTP
– Événements utilisateurs et d’administration : activation, rétention et exploitation pour l’audit
– Thèmes : déploiement et sélection de l’habillage des pages de connexion et des e-mails

Activités pratiques :

– Durcissement d’un realm : politique de mot de passe, protection contre la force brute et test de verrouillage
– Mise en place d’un MFA conditionnel imposé aux seuls utilisateurs à privilèges
– Consultation et filtrage des événements de connexion et d’administration

Haute disponibilité et durcissement

– Architecture en cluster : cache distribué Infinispan, découverte des nœuds, sessions persistantes en base de données
– Répartition de charge : load balancer et reverse proxy (HAProxy, Nginx, Traefik), affinité de session, health checks
– Résilience de la base de données : haute disponibilité du SGBD et impact sur la disponibilité de Keycloak
– Dimensionnement : mémoire, CPU et pool de connexions selon la charge attendue
– Durcissement de l’exposition : restriction de la console et des endpoints d’administration, séparation des accès publics et internes
– Sécurité de l’administration : protection du realm master et des comptes administrateurs, désactivation des flux hérités
– Secrets, certificats et correctifs : gestion du cycle de vie et veille sur les vulnérabilités

Activités pratiques :

– Mise en place d’un cluster à deux nœuds derrière un load balancer et test de bascule sans perte de session
– Restriction de l’accès à la console d’administration au réseau interne via le reverse proxy

© 2026 Sparks Formation. Tous droits réservés. Fiche générée depuis https://www.sparks-formation.com/formation/keycloak-administration-exploitation/

Supervision et maintien en conditions opérationnelles

– Métriques : activation, indicateurs clés (authentifications, erreurs, caches, base de données) et collecte par Prometheus
– Tableaux de bord et alertes Grafana : détecter saturation, pics d’échecs d’authentification et dégradations
– Journaux : niveaux de verbosité, format structuré et centralisation
– Sauvegarde et restauration : base de données, export des realms, configuration et thèmes
– Montées de version : rythme des publications, migration automatique du schéma, procédure et retour arrière
– Diagnostic des incidents courants : nom d’hôte et proxy, erreurs de redirection, synchronisation LDAP, cluster

Activités pratiques :

– Supervision du cluster avec Prometheus et Grafana et création d’une alerte
– Sauvegarde puis restauration complète après une perte simulée
– Diagnostic d’incidents de configuration préparés par le formateur

Automatisation de l'administration

– Admin CLI kcadm.sh : authentification, opérations courantes et scripts d’administration
– Admin REST API : jeton d’administration via un compte de service et appels courants
– Configuration as code : Terraform, Ansible et outils d’import déclaratif de configuration
– Gestion multi-environnement : promotion de la configuration du développement à la production dans une chaîne CI/CD
– Checklist de mise en production : points de contrôle sécurité, disponibilité et exploitation

© 2026 Sparks Formation. Tous droits réservés. Fiche générée depuis https://www.sparks-formation.com/formation/keycloak-administration-exploitation/

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans d'expertise	1 068+ formations	11 178 apprenants formés/an	+67 Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Cybersécurité et Protection des Données : 4,9/5 — 13 avis

William B. — Prévoir l'envoie à chaque particiapnt du livre de CISS au moins un mois avant la formation.

Mickael L. — il est top Romain GARCIA

Ils nous font confiance

Cette année notre filière Sécurité Applicative (AppSec) a accompagné plus de 14 entreprises dont :

ACTIMAGE CONSULTING SAS AIGA ALCYOR ALDORIA BPO FOUR JS DEVELOPMENT TOOLS GIE AG2R GROUPE FDJ IT LINK FRANCE REGION HAUTS DE FRANCE +4 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.

Qualiopi processus certifié — RÉPUBLIQUE FRANÇAISE

ecovadis SILVER | Top 15% Sustainability Rating JAN 2026

Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com

© 2026 Sparks Formation. Tous droits réservés. Fiche générée depuis https://www.sparks-formation.com/formation/keycloak-administration-exploitation/