

Sécurité Red Hat : gestion des identités et authentification avec Examen (EX362)

Durée: 5 Jours Réf de cours: RH363 Méthodes d'apprentissage: Intra-entreprise & sur-mesure

Résumé:

Sécuriser les services de gestion des identités centralisés afin de coordonner l'authentification et l'autorisation des utilisateurs avec les systèmes clients, les services réseau et les domaines Windows.

Ce cours permet d'acquérir les compétences requises pour configurer et gérer IdM, la solution complète de gestion des identités fournie avec Red Hat Enterprise Linux.

Il a pour objectif de développer les compétences requises pour intégrer et centraliser la gestion du cycle de vie, pour mettre en œuvre et appliquer les politiques de sécurité, ainsi que pour exploiter ces processus de gestion unifiés avec d'autres outils de gestion des configurations d'entreprise de la gamme de produits Red Hat, tels que Red Hat Ansible Automation Platform et Red Hat Satellite Server.

Il aborde notamment les thèmes suivants : gestion centralisée et provisionnement des comptes d'utilisateur ; conception et installation de topologies de serveurs IdM ; exploitation des services intégrés de l'autorité de certification DNS et TLS ; gestion de l'authentification à deux facteurs, de l'authentification par carte à puce et du fonctionnement en tant que fournisseur d'authentification unique et unifiée ; intégration et gestion des approbations bidirectionnelles avec Active Directory, résolution des problèmes et planification de la récupération après sinistre.

Le cours explique également l'enregistrement des clients Linux auprès d'IdM et leur exploitation dans des environnements d'entreprise qui utilisent à la fois des clients et des serveurs Linux et Microsoft Windows.

Note : A partir de janvier 2026, ce package (cours + examen) n'existe qu'en présentiel (en classe) s'il est programmé ou sous forme de cours privé intra-entreprise. Nous contacter.

Mis à jour 20/01/2026

Formation intra-entreprise

Cette formation est délivrable en session intra-entreprise, dans vos locaux ou dans les nôtres. Son contenu peut être adapté sur-mesure pour répondre aux besoins de vos collaborateurs. Contactez votre conseiller formation Global Knowledge ou adressez votre demande à info@globalknowledge.fr.

Public visé:

Titulaires de la certification RHCE (Ingénieur système certifié Red Hat) qui souhaitent apprendre à provisionner et configurer des solutions de gestion centralisée des identités pour les clients Linux, et à les intégrer à d'autres services réseau et systèmes de gestion des identités Spécialistes ou ingénieurs de la gestion des identités Spécialistes ou ingénieurs de la gestion des accès

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
 - Concevoir une topologie de gestion des identités pour l'évolutivité et la résilience
 - Décrire les technologies clés utilisées par IdM, notamment SSSD, PAM, Kerberos et PKI
 - Installer des serveurs, des réplicas et des clients Identity Management (IdM) à l'aide de playbooks Ansible
 - Gérer des services IdM, y compris des services DNS et CA intégrés
 - Configurer et gérer des services d'authentification et de sécurité Kerberos
 - Configurer et gérer des certificats TLS
- Créer et gérer une relation de confiance avec Microsoft Active Directory
- Configurer un système d'authentification des utilisateurs sécurisé avec l'authentification à deux facteurs et l'authentification unique et unifiée
- Configurer et gérer des politiques Sudo, HBAC et RBAC
- Gérer des secrets, des coffres-forts, des certificats et des clés
- Résoudre des problèmes de gestion des identités
- Intégrer IdM à Satellite 6 et Red Hat Ansible Automation Platform
- Configurer un système de sauvegarde et de récupération pour IdM

Pré-requis:

- Être titulaire de la certification RHCE ou disposer de compétences équivalentes
- Il est vivement recommandé de passer l'évaluation gratuite pour s'assurer que le cours est adapté aux compétences du participant [Red Hat Skills Assessment](#)

Test et certification

- Examen Spécialiste certifié Red Hat en gestion des identités (EX362)

Contenu:

Identity Management dans Red Hat Enterprise Linux

- Présentation du composant Identity Management (IdM) dans Red Hat Enterprise Linux et de son architecture de haut niveau

Technologies de base d'Identity Management

- Description des technologies de base d'Identity Management (IdM) dans Red Hat Enterprise Linux

Installation d'Identity Management dans Red Hat Enterprise Linux

- Installer les serveurs, les réplicas et les clients Identity Management sur Red Hat Enterprise Linux 9

Mise en œuvre d'une topologie pour Identity Management

- Mettre en œuvre des fonctionnalités continues et une haute disponibilité des services IdM dans des topologies à site unique et distribuées géographiquement

Gestion de l'autorité de certification et des services DNS intégrés

- Gérer les services de l'autorité de certification (CA) et du système de noms de domaine (DNS) intégrés à Identity Management

Gestion des utilisateurs et contrôle des accès associés

- Configurer les utilisateurs autorisés à accéder aux services et aux ressources

Configuration des services d'authentification alternatifs

- Configurer et gérer l'authentification par carte à puce, les secrets et l'authentification à deux facteurs

Intégration d'Identity Management à Active Directory

- Mettre en œuvre une relation d'approbation entre les forêts Identity Management et Active Directory, et configurer des vues d'identifiants pour mettre les attributs POSIX en correspondance avec les utilisateurs Active Directory

Intégration d'Identity Management aux produits Red Hat

- Intégrer un déploiement d'Identity Management à Red Hat Satellite et Red Hat Ansible Automation Platform

Résolution des problèmes et planification de la récupération après sinistre pour IdM

- Résoudre les problèmes et préparer la récupération après sinistre avec Identity Management

Révision complète

- Créer une petite topologie résiliente pour Identity Management qui inclut plusieurs réplicas et clients, et contenant plusieurs utilisateurs, informations d'identification, politiques et droits d'accès

Méthodes pédagogiques :

Un support de cours officiel sera fourni aux participants.

Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

- Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
- Votre place sera confirmée à la réception d'un devis ou "booking form" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
- Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

- En cas de handicap : plus d'info sur globalknowledge.fr/handicap
- Le Règlement intérieur est disponible sur globalknowledge.fr/reglement