

Mis à jour le 02/10/2026

S'inscrire

Formation Certification SUSE Certified Engineer in SUSE Linux

5 jours (35 heures)

Présentation

SUSE Linux Enterprise Server est une distribution Linux d'entreprise conçue pour exploiter des infrastructures fiables et sécurisées. Avec YaST et Snapper ainsi que ses outils de réseau, de stockage et d'automatisation, elle permet de maîtriser les opérations système avancées et de développer les compétences attendues pour la certification officielle SUSE Certified Engineer in SUSE Linux Enterprise Server.

Notre Formation Certification SUSE Certified Engineer in SUSE Linux vous permettra d'aller au-delà des fondamentaux pour préparer l'examen de niveau Engineer et consolider votre expertise sur SUSE Linux Enterprise Server 15.

Vous apprendrez à diagnostiquer les performances, à sécuriser les échanges, à automatiser les tâches avec Bash et à configurer les réseaux avancés, le stockage partagé et l'authentification centralisée.

À l'issue de la formation, vous serez en mesure de gérer les paquets, les dépôts et les mises à jour, de déployer des configurations avec Salt et de justifier vos choix techniques face aux situations couvertes par l'examen.

Cette préparation associe ateliers pratiques et examen blanc pour identifier vos axes de progression. Le passage de l'examen officiel est proposé, selon les modalités de réservation, afin de valoriser les compétences validées par la certification.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Préparer les domaines de l'examen SUSE Certified Engineer in SUSE Linux Enterprise Server et analyser des questions de certification
- Diagnostiquer les performances et maîtriser la récupération système avec Snapper
- Automatiser les opérations d'administration avec Bash et Salt
- Configurer les réseaux avancés, le stockage iSCSI et les chemins multiples
- Sécuriser les échanges et intégrer une authentification centralisée avec PAM et SSSD
- Construire et signer des paquets RPM puis administrer les dépôts et leur réplication avec RMT

Public visé

- Administrateur système Linux
- Ingénieur systèmes Linux
- Ingénieur DevOps
- Consultant infrastructure
- Ingénieur de production

Pré-requis

- Expérience opérationnelle de l'administration de SUSE Linux Enterprise Server 15 ou compétences équivalentes
- Maîtrise de la ligne de commande Linux et des commandes usuelles de Bash
- Pratique du partitionnement, des permissions et de la gestion des utilisateurs sous Linux
- Connaissance de la configuration réseau et de la gestion des services avec systemd
- Pratique de la gestion des paquets et des dépôts avec RPM et Zypper

Pré-requis techniques

- Poste équipé de 16 Go de mémoire vive minimum, de 100 Go libres et d'un processeur avec virtualisation matérielle activée
- Hyperviseur KVM ou VirtualBox installé, avec droits permettant de créer des réseaux virtuels et des disques supplémentaires
- Trois machines virtuelles sous SUSE Linux Enterprise Server 15 SP7 avec accès administrateur et images préparées pour les ateliers
- Connexion Internet stable autorisant les dépôts logiciels, les téléchargements et l'accès à la plateforme de formation
- Compte SUSE Customer Center avec droits d'évaluation ou souscription adaptés aux exercices de réplication des dépôts

Programme de notre formation SUSE Certified Engineer in SUSE Linux

[Jour 1 - Matin]

Administration avancée et récupération système

- Positionnement de la Formation Certification SUSE Certified Engineer in SUSE Linux et cartographie des domaines de SUSE Certified Engineer in SUSE Linux Enterprise Server
- Consolidation des acquis administrateur : permissions, utilisateurs, services et gestion des paquets
- Paramétrage des politiques locales avec le module de sécurité YaST
- Gestion des instantanés Btrfs avec Snapper et distinction entre instantané et sauvegarde
- Analyse des changements, restauration de fichiers et conditions d'un retour arrière système
- Atelier pratique : Sécuriser une machine de laboratoire, provoquer une erreur de configuration puis restaurer un état fonctionnel avec Snapper.

[Jour 1 - Après-midi]

Diagnostic, performances et matériel

- Méthodologie de diagnostic : symptômes, hypothèses, mesures et validation des corrections
- Analyse de la consommation CPU, de la mémoire et des entrées-sorties avec les outils système
- Gestion des cgroups et limitation des ressources des services avec systemd
- Inventaire matériel, identification des pilotes et gestion des modules du noyau
- Résolution des dépendances de bibliothèques avec ldd et ldconfig, collecte des journaux et de supportconfig
- Atelier pratique : Diagnostiquer un service dégradé, appliquer une limitation de ressources et constituer un dossier de preuves techniques.

[Jour 2 - Matin]

Chiffrement et gestion des identités cryptographiques

- Principes de cryptographie symétrique et asymétrique, empreintes et signatures numériques
- Architecture TLS, chaîne de certification et vérification de l'identité des services
- Création de clés, demandes de certificat et contrôles avec OpenSSL
- Création, exportation, distribution et révocation de clés avec GPG
- Analyse de scénarios d'examen sur la confiance, la confidentialité et l'intégrité
- Atelier pratique : Créer une autorité de laboratoire, vérifier un certificat de service et signer puis contrôler un fichier avec GPG.

[Jour 2 - Après-midi]

Automatisation robuste avec Bash

- Maîtrise des expansions, de la protection des arguments et des redirections
- Construction de conditions, de boucles et de tests sur les fichiers et les valeurs
- Organisation des scripts avec fonctions, tableaux et variables locales
- Gestion des paramètres, saisies utilisateur et options avec getopt
- Traitement des codes de retour, journalisation, nettoyage avec trap et débogage
- Atelier pratique : Développer un script d'audit paramétrable qui contrôle plusieurs services et produit un rapport exploitable avec gestion des erreurs.

[Jour 3 - Matin]

Réseaux avancés et isolation

- Analyse des interfaces, des routes et de la résolution de noms avec ip et les outils de diagnostic
- Configuration de bridges et de segments VLAN, validation de la connectivité
- Création de paires veth et circulation des paquets entre interfaces virtuelles
- Isolation réseau avec les network namespaces et diagnostic des chemins de communication
- Adressage IPv6, découverte des voisins et résolution des incidents de routage
- Atelier pratique : Construire une topologie isolée avec namespaces, interfaces veth et bridge, puis diagnostiquer une rupture de connectivité IPv6.

[Jour 3 - Après-midi]

Stockage iSCSI et chemins multiples

- Architecture iSCSI : cibles, initiateurs, sessions, identifiants et unités logiques
- Configuration d'une cible LIO et présentation des volumes aux initiateurs
- Administration des initiateurs avec iscsiadm, authentification et persistance des connexions
- Configuration de Device Mapper Multipath, identification des périphériques et politiques de chemins
- Analyse des défaillances et contrôles de cohérence entre stockage, réseau et montages
- Atelier pratique : Présenter un volume iSCSI par deux chemins, configurer multipath et vérifier le comportement lors de la perte d'un chemin.

[Jour 4 - Matin]

Authentification centralisée et contrôle des accès

- Articulation entre identification, authentification, autorisation et résolution des comptes
- Organisation des piles PAM, catégories de modules et indicateurs de contrôle
- Configuration des politiques d'accès et analyse des effets d'une modification de PAM
- Architecture SSSD, fournisseurs d'identité et intégration à un annuaire de laboratoire
- Gestion du cache d'identité, comportements hors ligne et diagnostic des échecs de connexion
- Atelier pratique : Intégrer un serveur à l'annuaire fourni, valider les connexions avec SSSD et corriger une erreur de configuration PAM.

[Jour 4 - Après-midi]

Paquets, dépôts et réplication des mises à jour

- Analyse d'un paquet RPM, vérification de son intégrité et résolution des dépendances
- Construction d'un paquet avec rpmbuild, structure du fichier spec et signature avec GPG
- Création d'un dépôt RPM-MD avec createrepo et signature des métadonnées
- Gestion des dépôts, priorités et mises à jour avec Zypper et libzypp
- Installation de RMT, sélection des produits, réplication des dépôts et configuration des clients

- Atelier pratique : Construire et signer un paquet, le distribuer depuis un dépôt local et connecter un client à un serveur RMT préparé.

[Jour 5 - Matin]

Gestion de configuration avec Salt

- Architecture Salt, rôles master et minion, échanges et gestion des clés
- Installation des composants, association des nœuds et validation des communications
- Utilisation des modules d'exécution pour interroger et administrer les systèmes
- Description des configurations avec les states, syntaxe YAML et fichier top.sls
- Gestion des dépendances, ciblage des machines et vérification de l'idempotence
- Atelier pratique : Déployer un paquet, un fichier de configuration et un service sur plusieurs minions, puis vérifier la convergence après une modification manuelle.

[Jour 5 - Après-midi]

Consolidation et préparation finale à l'examen

- Synthèse transversale des domaines de SUSE Certified Engineer in SUSE Linux Enterprise Server
- Analyse de scénarios associant performances, réseau, stockage, sécurité et automatisation
- Méthode de lecture des questions, élimination des distracteurs et gestion du temps
- Organisation du passage proposé, vérification des conditions d'obtention et des exigences de surveillance à distance
- Construction d'un plan de révision individuel à partir des erreurs et des compétences à renforcer
- Atelier pratique : Réaliser un examen blanc chronométré avec des questions originales, analyser les réponses et reproduire en laboratoire les configurations mal maîtrisées.

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.