

Mis à jour le 08/10/2026

S'inscrire

Formation HPE Aruba Networking ClearPass Configuration (CPC)

5 jours (35 heures)

Présentation

HPE Aruba Networking ClearPass est une solution de contrôle d'accès au réseau permettant de sécuriser les connexions des utilisateurs et des appareils en entreprise. Avec Policy Manager et les fonctionnalités Guest, OnGuard et Onboard, ClearPass permet de centraliser l'authentification, les politiques d'accès, le contrôle de posture et le provisionnement des appareils.

Notre formation HPE Aruba Networking ClearPass Configuration vous permettra de développer vos connaissances fondamentales du portefeuille ClearPass et de les mobiliser dans des configurations concrètes adaptées aux réseaux d'entreprise.

Vous apprendrez à configurer les services AAA et les sources d'authentification, à exploiter le profilage des points de terminaison, à définir les rôles et à mettre en œuvre des contrôles d'accès cohérents.

À l'issue de la formation, vous serez en mesure de déployer une solution d'accès réseau ClearPass et de configurer les accès invités, l'authentification câblée, les politiques de posture OnGuard et le provisionnement Onboard.

Cette formation aborde également la gestion des certificats et les opérations administratives, les sauvegardes, la collecte des journaux et les rapports ClearPass Device Insight afin de vous aider à résoudre les problèmes rencontrés en exploitation.

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

Objectifs

- Mettre en œuvre une solution d'accès réseau ClearPass en entreprise
- Concevoir et mettre en œuvre des services et des contrôles efficaces dans ClearPass
- Résoudre les problèmes liés à une solution ClearPass en exploitation

Public visé

- Administrateur réseau
- Ingénieur réseau
- Technicien réseau

Pré-requis

- Un à deux ans d'expérience professionnelle réseau au minimum conseillés
- Expérience du déploiement de solutions réseau
- Pratique de ces déploiements en environnement d'entreprise

Pré-requis techniques

- Poste informatique équipé d'un navigateur compatible avec les interfaces de ClearPass utilisées pendant les ateliers
- Connexion réseau stable permettant l'accès à l'environnement pédagogique
- Compte d'accès à l'environnement de travaux pratiques ClearPass avec les droits nécessaires aux configurations

Programme de notre formation HPE Aruba Networking ClearPass Configuration (CPC)

[Jour 1 - Matin]

Fondamentaux de ClearPass et architecture AAA

- Introduction à HPE Aruba Networking ClearPass et au portefeuille de produits
- Principes du contrôle d'accès au réseau et cas d'utilisation de ClearPass
- Organisation du système ClearPass et repérage des fonctions de configuration
- Modèle AAA : authentification, autorisation et comptabilisation
- Sources d'authentification et articulation avec les demandes d'accès
- Atelier pratique : explorer le système ClearPass et configurer une source d'authentification pour un scénario d'accès réseau.

[Jour 1 - Après-midi]

Appareils externes et profilage des terminaux

- Intégration des appareils externes dans une solution ClearPass
- Configuration des appareils d'accès au réseau et de leurs échanges avec ClearPass
- Paramétrage des services de messagerie
- Rôle des serveurs de contexte externes dans les informations disponibles
- Introduction au profilage des points de terminaison et fonctionnement du collecteur de profilage
- Atelier pratique : déclarer un appareil d'accès au réseau et examiner les informations collectées pour profiler un terminal.

[Jour 2 - Matin]

Rôles, services et application des politiques

- Organisation des services ClearPass dans le traitement des demandes d'accès
- Définition des rôles ClearPass et exploitation des informations d'authentification
- Principes d'application des politiques et articulation entre rôles et contrôles
- Configuration des règles de sélection des services et analyse de leur ordre
- Création de services associant authentification, rôles et contrôles d'accès
- Atelier pratique : créer un service, configurer ses règles de sélection et vérifier l'application des contrôles selon le rôle obtenu.

[Jour 2 - Après-midi]

Services web et authentification des invités

- Configuration des services web et utilisation du gestionnaire de contenu
- Personnalisation des skins avec l'éditeur de page web
- Processus de portail captif et configuration des connexions web
- Création et utilisation des comptes invités
- Accès invité avec authentification MAC et articulation avec le portail
- Atelier pratique : personnaliser un portail invité, créer un compte et vérifier les parcours d'authentification web et MAC.

[Jour 3 - Matin]

Autonregistrement des accès invités

- Principes de l'autonregistrement d'accès invité et place dans le parcours d'accès
- Analyse de l'expérience d'autonregistrement du point de vue de l'utilisateur
- Configuration de l'autonregistrement et des pages associées
- Déroulement du processus d'autonregistrement jusqu'à l'authentification de l'invité
- Atelier pratique : configurer un parcours d'autonregistrement et tester la création du compte puis la connexion de l'invité.

[Jour 3 - Après-midi]

Authentification et contrôle des accès câblés

- Principes de l'authentification câblée et cheminement d'une demande d'accès
- Configuration de l'accès câblé avec les services ClearPass
- Définition de l'application des politiques sur les accès câblés selon les rôles
- Collecte et exploitation du profilage sur les ports câblés
- Atelier pratique : configurer un accès câblé, vérifier le profilage du terminal et corriger une règle empêchant l'application du contrôle attendu.

[Jour 4 - Matin]

Posture et application des politiques OnGuard

- Introduction à ClearPass OnGuard et au contrôle de posture
- Configuration des politiques de posture et interprétation des résultats
- Mise en œuvre de l'agent logiciel OnGuard et surveillance de son fonctionnement
- Analyse du workflow OnGuard entre collecte, évaluation et décision d'accès
- Intégration d'OnGuard dans l'application des politiques de contrôle d'accès
- Atelier pratique : configurer une politique de posture, tester l'agent OnGuard et vérifier les contrôles appliqués à un terminal conforme puis non conforme.

[Jour 4 - Après-midi]

Provisionnement des appareils avec Onboard

- Principes du provisionnement ClearPass Onboard et déroulement du parcours utilisateur
- Configuration des autorités de certification nécessaires au provisionnement
- Paramétrage du portail Onboard et du parcours de provisionnement
- Configuration des services Onboard et articulation avec le portail
- Atelier pratique : configurer une autorité de certification, un portail et les services Onboard pour provisionner un appareil de test.

[Jour 5 - Matin]

Administration Onboard et maintenance de ClearPass

- Administration du logiciel ClearPass Onboard et gestion des utilisateurs et des appareils
- Gestion des certificats et suivi de leur cycle de vie
- Révocation des certificats et contrôle de leur statut avec OCSP
- Opérations administratives : licences, certificats, mises à jour et améliorations
- Gestion des sauvegardes et collecte des journaux pour l'analyse des problèmes
- Atelier pratique : révoquer un certificat Onboard, vérifier son statut, réaliser une sauvegarde et collecter les journaux d'un incident simulé.

[Jour 5 - Après-midi]

Accès administratifs, rapports et diagnostic

- Configuration de l'accès administrateur aux appareils d'accès au réseau ou NAD
- Gestion de l'accès administrateur au Policy Manager
- Configuration des connexions opérateur invité
- Administration de ClearPass Device Insight et exploitation des alertes et des rapports
- Atelier pratique : configurer les accès administratifs et les connexions opérateur invité, puis exploiter les alertes, les rapports et les journaux pour diagnostiquer un problème ClearPass.

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.