

FICHE FORMATION

ARUBA MOBILITY BOOTCAMP, REV. 20.11

Description du cours

Cette formation enseigne les connaissances, les compétences et l'expérience pratique nécessaires pour installer et configurer un réseau WLAN Aruba en utilisant l'architecture et les fonctionnalités de l'OS 8.X. Ce cours BOOTCAMP fournit les connaissances et compétences techniques importantes des deux cours Aruba :

- Aruba Mobility Fundamentals, Rev 20.11
- Implementing Aruba Mobility, Rev 20.11

Avec des cours théoriques et des travaux pratiques, les participants apprendront comment utiliser le matériel Aruba et ArubaOS pour installer et construire un réseau de WLAN complet et sécurisé avec plusieurs SSID. Ce cours fournit le matériel de base nécessaire pour préparer les candidats aux certifications ACMA et ACMP

Durée	5 jours
Niveau de Compétences	Intermédiaire
Langues du cours	Français
Langues du support	English
Instructeur	Certifié
Certifications liées	Aruba Certified Mobility Associate (ACMA) Aruba Certified Mobility Professional (ACMP)
Divers	Salle équipée Déjeuner inclus

Contenu

- **Principes de base du réseau local sans fil (WLAN)**

Description des principes fondamentaux du 802.11, fréquences et canaux RF

Explication des modèles RF et de la couverture, y compris le rapport SNR

Normes d'itinérance et exigences en matière de QOS

- **Architecture Mobile First**

Introduction aux produits Aruba, y compris les types et modes de contrôleurs

Architecture et fonctionnalités d'OS 8.X

Types de licences et distribution

- **Mobility Master Redundancy**

Expliquer la mise en place du protocole VRRP

Expliquer la procédure de synchronisation des bases de données et sa validation.

Expliquer le processus de failover des MMs

- **Fonctionnement et Configuration du Mobility Master Mobility Controller**

Comprendre les groupes et sous-groupes

Différentes méthodes pour joindre MC avec MM

Présentation de la configuration hiérarchique

- **Sécurité WLAN**

Description de la découverte, de l'authentification et de l'association 802.11

Exploration des différentes méthodes d'authentification, 802.1x avec WPA/WPA2, Mac. Description de la communication du serveur d'authentification

Explication des clés symétriques et asymétriques, méthodes de chiffrement

Le WIPS est décrit ainsi que la découverte et la protection des rogue.

- **Accès invité**

Présentation des solutions d'Aruba pour Guest Access et le processus du portail Captive

Configuration de l'accès sécurisé des invités via le portail interne Captive

La configuration d'un portail captif utilisant Clearpass et ses avantages

Création d'un compte de provisionnement invité

Dépannage de l'accès invité

- **Dérivation des Rôles**

Revoir les politiques et les règles Firewall

Expliquer la dérivation de rôle à l'aide des VSA

Description des règles utilisateur

Description des rôles d'authentification par défaut

Expliquer comment dépanner la dérivation dynamique des rôles.

- **Options avancées de la sécurité**

Se familiariser avec les concepts et la configuration de mécanismes de sécurité avancés.

Comprendre comment et quand utiliser la terminaison RADIUS et EAP

Explorez l'authentification machine et la liste noire des clients

Comprenez les meilleures pratiques lors de l'utilisation de certificats.

- **Introduction au clustering MC**

Décrire les avantages du clustering des Contrôleurs de Mobilité

Le processus d'élection du cluster leader

L'assignation des APs et users aux membres du cluster

Les prérequis pour un avoir cluster failover transparent

Le load-balancing des APs et users dans un cluster

- **Gestion RF dynamique**

Démonstration de l'étalonnage du réseau par ARM pour la sélection des canaux et des paramètres de puissance.
Exploration du nouvel OS 8.X Airmatch pour calibrer le réseau
Appariement entre Client Match et Client Insight pour orienter les clients vers de meilleurs AP.

- **Configuration WLAN sécurisée**

Identification des exigences WLAN telles que le nom SSID, le cryptage, l'authentification, etc.
Explication de la structure et des profils des groupes AP
Configuration du WLAN à l'aide de l'interface graphique Mobility Master

- **Provisioning AP**

Description de la communication entre le AP et le Mobility controller
Explication de la séquence de démarrage de l'AP et des conditions requises
Exploration des mécanismes de découverte des APs
Explication de la façon de sécuriser la communication AP vers le contrôleur à l'aide de CPsec.
Description de l'approvisionnement et des opérations AP

- **Rôles et politiques du pare-feu**

Introduction aux rôles et politiques des pare-feu
Explication du pare-feu basé sur l'identité d'Aruba
Configuration des stratégies et des règles, y compris les alias
Répartition des rôles entre les utilisateurs

- **Options avancées du clustering MC**

Se familiariser avec les fonctionnalités avancées du clustering.
Savoir utiliser la fonction de déplacement AP et l'interaction avec le serveur d'autorisation
Être en mesure d'effectuer les étapes de dépannage du cluster.

- **Mobilité**

Expliquer le standard 802.11r
Décrire la mobilité dans des architectures single et multi-controller
Définir les avantages de la mobilité dans un cluster

- **Administration**

Expliquer le management des comptes et mots de passes
Configuration des comptes guest provisioning
L'utilisation de l'authentification RADIUS et TACACS
Décrire comment désactiver l'accès console

- **Operations**

Expliquer le processus de mise à jour
Décrire le mécanisme d'AP preloading
Expliquer la mise à jour en-service dans le cadre du clustering
Auto roll backs de la configuration

- **Surveillance du réseau et dépannage**

Utilisation du tableau de bord MM pour surveiller et diagnostiquer les problèmes clients, WLAN et AP
Analyse du trafic à l'aide d'APPrf avec capacités de filtrage

Objectifs

- Expliquer comment les solutions de réseau sans fil d'Aruba répondent aux besoins des clients
- Expliquer les technologies WLAN fondamentales, les concepts RF, les normes 802.11 et la réglementation dans les réseaux Wifi
- Apprendre à concevoir et configurer des réseaux WLAN Aruba multi-contrôleurs pour contrôler l'accès des employés et des invités au réseau.
- Décrire la redondance donnant à l'utilisateur un basculement en douceur
- Contrôler l'accès sécurisé au réseau local sans fil à l'aide des politiques et des rôles du pare-feu d'Aruba
- Expliquer comment les rôles sont assignés aux utilisateurs sans fil ou câblés.
- Configurer et optimiser les fonctions ARM, AirMatch et Client Match d'Aruba
- Expliquer les utilisations et les avantages du clustering
- Décrire la mobilité des utilisateurs dans le spectre sans fil
- Exécuter les fonctions de management, de surveillance et de dépannage du réseau.

Merci de nous contacter pour plus d'informations.