HPE Aruba Networking ClearPass Advanced Workshop (AR-CPA2)

Course Description

This advanced level course is taught as a workshop. Participants will be led through a real-world design and implementation scenario encompassing all aspects of the HPE Aruba Networking ClearPass security product. This 5-day course will cover the design, implementation, and troubleshooting of ClearPass solutions. The course is presented as a workshop, meaning that it is focused on student participation and hands-on labs to reinforce concepts through design exercises and lab debriefs, as well as planning and implementation of the design. This is not a course that relies on a step-by-step lab guide and you will be challenged to find creative solutions to the scenario. By the nature of this workshop, you will master troubleshooting techniques in ClearPass.

Course Duration:

5 days

Prerequisites:

- Configuring HPE Aruba Networking ClearPass course

Objectives:

After you successfully complete this course, expect to be able to:

- Design a ClearPass cluster
- Design a High availability solution with Virtual IP address following the best practices
- Describe Public Key Infrastructure and certificate format types
- Plan the certificates used by ClearPass
- Explain how Enrollment over Secure Transport can automate the certificate generation process
- Leverage RADIUS services to handle corporate wireless connections
- Deploy WEBAUTH services to handle health checks
- Describe the proposed RADIUS services that handles guest wireless connections
- Explain general guest considerations
- Design guest RADIUS services
- Describe the proposed Onboard services
- Describe the MPSK feature
- Leverage these features in your deployment
- Plan a successful wired access deployment
- Provide administrative access control to ClearPass modules and NADs
- Generate custom reports and alert

Course Outline:

- Network requirements
  - ClearPass goals
  - Network topology
  - List of available resources
  - Scenario analysis
  - Authentication requirements
  - Multiple user account databases
  - User account attributes
  - High level design
- PDI and digital certificates
  - Certificate types
  - PKI
  - Certificate trust
  - Certificate file formats
  - ClearPass as CA
  - Certificate use cases:
    - EAP
    - HTTPS
    - Service-based certificates
    - Onboarding
    - Clustering
    - RadSec
    - NAD captive portal
  - Installing certificates
  - Enrollment over secure transport
- Cluster design
  - ClearPass server placement
  - Determine the layout of the cluster
  - High availability schema
  - Design high availability
  - VIP failover
  - VIP mapping
  - Insight primary and secondary
- Network integration
  - Authentication sources
    - Local user repository
    - Endpoint repository
    - Admin user repository
    - Guest user repository
    - Guest device repository
    - Onboard device repository
    - Active Directory
    - SQL server
  - Define external servers
    - Unified endpoint management
    - Email server

    - Endpoint profiling
        - IF-MAP
        - Active scans (SNMP)
        - DHCP
        - HTTPS
    - Network devices
        - RadSec
        - Dynamic authorization
        - Logging of RADIUS accounting
        - Device-groups
        - Location attributes
    - Policy simulation
- Corporate access design
    - Define the requirements
    - High-level design
    - Services design
    - Plan TIPs roles
    - User authentication
    - Machine authentication
    - Tunneled EAP, EAP-TLS and protected EAP
    - One versus multiple services
    - Plan enforcement
    - Device-groups based enforcement
    - Service implementation
    - OnGuard design and implementation
        - Quarantine users
        - Remediation
    - Onboard design and implementation
        - User and device authorization
    - Informational pages
    - Authorization validation
    - Troubleshooting enforcement
    - Downloadable roles
- Guest access design
    - Guest network design
    - Captive portal flow
    - Design tasks
    - Define web pages
    - Guest services design
    - Guest services
    - Guest access controls
    - Configure network access devices
    - Guest account creation
    - Guest self registration
    - Guest sponsor approval
    - Self registration AD drop-down list
    - Requirements for guest enforcement

- Multi-pre shared key
  - Define the requirements
  - High-level design
  - Device authorization
  - Service design and implementation
- Wired access
  - AAA configuration
  - 802.1X and MAC auth
  - Using client profiling for authorization
  - Using conflict attribute for authorization
  - User roles configuration in AOS-S
  - User roles configuration in AOS-CX
  - Web redirection
  - Multi-service ports
  - Downloadable user roles enforcement profiles
  - Downloadable user roles configuration and validation
- Administrative access
  - TACACs+ based NAD administration
  - TACACs+ command authorization
  - Policy Manager administrators
  - Guest and Onboard operators
  - Register devices for MPSK
  - Insight operators
  - Insight reports and alerts

Who Should Attend

- Network Security Experts
- Individuals who implement network access control solutions.
- Network managers with HPE Aruba Network access device experience (wired and wireless).
- Network administrators who already own a ClearPass solution and are looking to deploy advanced features.