



HPE Aruba Networking ClearPass Advanced Workshop H38GHS

HPE course number	H38GHS
Course length	5 days
Delivery mode	ILT/VILT
View schedule, local pricing, and register	View now
View related courses	View now

This course prepares participants with foundational skills in network access control using the ClearPass product portfolio. This course includes both instructional modules and labs to teach participants about the major features of the ClearPass portfolio. Participants learn how to set up ClearPass as an AAA server, and configure the Policy Manager, Guest, OnGuard and Onboard feature sets. In addition, this course covers integration with external Active Directory servers and monitoring and reporting, as well as deployment best practices. The student gains insight into authentication configuration with ClearPass on both wired and wireless networks.

Why HPE Education Services?

- Comprehensive worldwide [HPE technical, IT industry and personal development training](#)
- [Training and certification preparation](#) for ITIL®, Security, VMware®, Linux, Microsoft and more
- Innovative [training options](#) that match individual learning styles
- Anytime, anywhere remote learning via [HPE Digital Learner](#) subscriptions
- Verifiable [digital badges](#) for proof of training, skill recognition and career development
- Simplified purchase options with [HPE Training Credits](#)

Audience

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

Prerequisites

- Any current Aruba ClearPass certification
- Aruba ClearPass Configuration course

Course objectives

After successful completion of this course, you should be able to:

- Design a ClearPass cluster
- Design a high availability solution with virtual IP addresses following 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 alerts

Detailed 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 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 ArubaOS-S
- User roles configuration in ArubaOS-CX
- Web federation
- Multi-service ports
- Downloadable user roles enforcement profiles
- Downloadable user roles configuration and validation

Wired 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

Learn more at

hpe.com/ww/learnnetworking

Follow us:

