

Juniper Junos Pulse Access Control (JPAC)

Code: ACBE-JUN-JPAC

Days: 3

Course Description:

This three-day course provides detailed coverage of the configuration of the Junos Pulse Access Control Service offered by Juniper Networks. Students will work with the solution elements—the Junos Pulse Access Control Service, the SRX Series Services Gateway as a firewall enforcer, Junos Pulse, and the Odyssey Access Client (OAC)—to configure secured access to network resources. Key topics include Junos Pulse Access Control Service deployment, basic implementation, and element configuration. Students will have the opportunity to apply their knowledge in several hands-on labs. This course is based on Junos Pulse Access Control Service Release 4.1R3.

Course Summarize:

Day 1

Chapter 1: Course Introduction

Chapter 2: The Junos Pulse Access Control Service

- The Need for Access Control
- Junos Pulse Access Control Service Components
- Junos Pulse Access Control Service Component Interaction
- Sample Junos Pulse Access Control Service Deployments

Chapter 3: Initial Configuration

- Junos Pulse Access Control Service Initial Configuration: Console
- Junos Pulse Access Control Service Initial Configuration: Admin UI
- Firewall Enforcer Initial Configuration
- Verification and Troubleshooting
- Lab 1: Initial Configuration

Chapter 4: The Access Management Framework

- Access Management Framework Elements

Chapter 5: Roles

- Configuring User Roles
- Role Mapping
- Configuring Sign-In Policies
- Lab 2: Roles

Chapter 6: Client Access Methods

- Client Access Methods
- Configure Agent Access
- Configure Agentless Access
- Lab 3: Client Access

Day 2

Chapter 7: Firewall Enforcement

- Resource Policy Overview
- Firewall Enforcement Overview
- Configure Firewall Enforcement
- Captive Portal
- Lab 4: Firewall Enforcement

Chapter 8: Layer 2 Enforcement

- 802.1X Operations
- RADIUS Elements
- MAC Authentication

Chapter 9: Configuring Layer 2 Enforcement

- Configuring an 802.1X Authenticator
- Configuring 802.1X Support on the Junos Pulse Access Control Service
- Configure MAC Authentication
- Lab 5: Policy Configuration Using 802.1X

Chapter 10: Endpoint Defense

- What Is Host Checker?
- Host Checker Configuration
- Enhanced Endpoint Security (EES) Configuration
- Enforcing Policies
- Lab 6: Endpoint Security

Day 3

Chapter 11: Authentication Options

- Authentication Process Review
- Configuring Authentication Servers
- Configuring Authentication Realms
- Lab 7: Authentication Options

Chapter 12: Management and Troubleshooting

- Logging
- System Monitoring
- Troubleshooting Component Communications
- Troubleshooting User Interactions
- Configuration File Management

- Working with JTAC
- Lab 8: Logging and Troubleshooting

Chapter 13: High Availability

- Describe High Availability
- Junos Pulse Access Control Service Clustering
- Firewall Options
- Lab 9: Junos Pulse Access Control Service Clustering

Chapter 14: Junos Pulse Access Control Service Integration

- IF-MAP Federation
- NSM Integration
- STRM Integration
- IDP Integration

Appendix A: Junos Pulse Gateway Chassis Management

- CMC Benefits
- Configure CMC

Appendix B: ScreenOS Enforcers

- ScreenOS Policies
- Configure Firewall Enforcement
- Verify Operations