"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

Which authentication methods can ClearPass use to validate user credentials? (Select two.)

A. EAP-TLS
B. PAP
C. PEAP
D. CHAP

Answer: A, C

Explanation:

ClearPass supports EAP-TLS for certificate-based authentication and PEAP for password-based authentication over a secure tunnel. PAP and CHAP are outdated and less secure, making them unsuitable for enterprise environments.

Question: 2

Which policy enforcement feature in ClearPass ensures that devices comply with security requirements before accessing the network?

A. Role Mapping
B. Posture Assessment
C. Guest Access
D. MAC Caching

Answer: B

Explanation:

Posture Assessment evaluates a device's security compliance, such as antivirus updates and firewall settings, before granting access. Role Mapping assigns roles but does not assess compliance.

Question: 3

What is the primary function of the ClearPass Policy Manager?

A. Managing wireless access points

B. Enforcing network access policies
C. Configuring VLANs
D. Blocking unauthorized devices

Answer: B

Explanation:

ClearPass Policy Manager enforces policies based on user authentication, device posture, and contextual information, ensuring secure network access. It does not directly manage APs or VLAN configurations.

Question: 4

Which authentication protocol is recommended for organizations that require certificate-based authentication?

A. EAP-TLS
B. PEAP-MSCHAPv2
C. EAP-GTC
D. CHAP

Answer: A
Explanation:

EAP-TLS provides secure, certificate-based authentication, ensuring mutual authentication between clients and the network. PEAP-MSCHAPv2 is password-based and less secure than EAP-TLS.

Question: 5

Which methods does ClearPass support for guest user authentication? (Select two.)

A. Social login authentication
B. Static pre-shared keys
C. SMS/email verification
D. 802.1X authentication

Answer: A, C
Explanation:

ClearPass allows guest authentication via social logins (e.g., Google, Facebook) and SMS/email verification. 802.1X is used for enterprise authentication, not guest access.

Question: 6

Which component in ClearPass allows administrators to manage authentication requests?

A. Policy Manager
B. OnGuard
C. Guest Manager
D. Insight

Answer: A
Explanation:

ClearPass Policy Manager is responsible for handling authentication requests, applying policies, and enforcing security rules based on identity and context.

Question: 7

What is the primary purpose of ClearPass OnGuard?

A. Managing guest access
B. Enforcing endpoint compliance
C. Configuring SSIDs
D. Assigning VLANs

Answer: B
Explanation:

OnGuard ensures endpoint devices comply with security policies, such as antivirus status and operating system patches, before granting network access.

Question: 8

Which feature allows ClearPass to integrate with third-party security solutions?

A. Active Directory Integration
B. REST API
C. MAC Address Bypass
D. RADIUS Authentication

Answer: B
Explanation:

ClearPass provides REST API capabilities, enabling integration with third-party security tools for policy enforcement, automation, and enhanced visibility.

Question: 9

Which type of authentication is commonly used with 802.1X authentication for wired and wireless networks?

A. Certificate-based authentication
B. PSK authentication
C. Open authentication
D. Captive portal authentication

Answer: A
Explanation:

802.1X authentication often uses certificate-based authentication (EAP-TLS) for secure device verification. PSK and captive portal methods are not ideal for enterprise networks.

Question: 10

Which component is responsible for policy decision-making in a ClearPass environment?

A. OnGuard
B. Policy Manager
C. Guest Manager
D. Device Insight

Answer: B
Explanation:

ClearPass Policy Manager makes authentication decisions based on configured policies, ensuring secure access control and network enforcement.

Question: 11

Which security measure prevents unauthorized devices from accessing a network?

A. MAC Authentication Bypass
B. Role-Based Access Control
C. Dynamic VLAN Assignment
D. MAC Address Filtering

Answer: B
Explanation:

Role-Based Access Control (RBAC) restricts access to network resources based on user identity and context, preventing unauthorized devices from gaining access.

Question: 12

Which ClearPass feature allows administrators to generate network access reports?

A. OnGuard
B. Guest Manager
C. Insight
D. Device Manager

Answer: C
Explanation:

ClearPass Insight provides reporting and analytics, allowing administrators to track authentication events, user access patterns, and security incidents.

Question: 13

What happens when a device fails a ClearPass posture check?

A. It is granted full network access
B. It is redirected to a remediation network
C. It is disconnected permanently
D. It is assigned a random VLAN

Answer: B
Explanation:

If a device fails a posture check, ClearPass can redirect it to a quarantine VLAN or captive portal for remediation before allowing full network access.

Question: 14

Which authentication protocol allows authentication via external identity providers such as Google or Facebook?

A. OAuth
B. LDAP
C. TACACS+
D. RADIUS

Answer: A
Explanation:

OAuth is commonly used for authentication via third-party identity providers, enabling single sign-on (SSO) for web and mobile applications.

Question: 15

Which policy enforcement feature in ClearPass assigns different access levels based on user identity?

A. MAC Caching
B. Role-Based Access Control
C. Guest Manager
D. OnGuard

Answer: B
Explanation:

Role-Based Access Control (RBAC) ensures that users receive appropriate network access permissions based on their role, such as employee or guest.

Question: 16

Which type of authentication does ClearPass use for machine authentication?

A. 802.1X with EAP-TLS
B. Guest Authentication
C. MAC Authentication Bypass
D. PSK Authentication

Answer: A
Explanation:

Machine authentication typically uses 802.1X with EAP-TLS, allowing secure access based on client certificates rather than passwords.

Question: 17

Which network security feature allows a device to access the network temporarily without full authentication?

A. MAC Caching
B. Captive Portal
C. Posture Assessment
D. RADIUS Proxy

Answer: A
Explanation:

MAC Caching enables previously authenticated devices to reconnect without re-authentication for a predefined period, enhancing user experience.

Question: 18

Which protocol does ClearPass use for network access enforcement?

A. SNMP
B. RADIUS
C. ICMP
D. SMTP

Answer: B
Explanation:

ClearPass primarily uses RADIUS for authentication, authorization, and accounting (AAA) services to enforce network access policies.

Question: 19

Which ClearPass feature enables self-registration for guests?

A. Insight
B. Guest Manager
C. Policy Manager
D. OnGuard

Answer: B
Explanation:

ClearPass Guest Manager allows self-registration, enabling guests to obtain network access credentials via email, SMS, or sponsor approval.

Question: 20

Which encryption method is recommended for protecting authentication traffic in ClearPass?

A. SSL/TLS
B. DES
C. MD5
D. SHA-1

Answer: A
Explanation:

SSL/TLS encryption ensures secure transmission of authentication credentials, preventing interception and unauthorized access.

Question: 21

Which authentication protocol is best suited for securing wireless network access with certificates?

A. PEAP-MSCHAPv2
B. EAP-TLS

C. EAP-FAST
D. EAP-GTC

Answer: B
Explanation:

EAP-TLS is the most secure authentication protocol as it uses client and server certificates to establish mutual authentication, eliminating the need for passwords. It prevents credential theft and offers robust security.

Question: 22

Which component in ClearPass is responsible for profiling network devices?

A. Guest Manager
B. Device Insight
C. Policy Manager
D. OnGuard

Answer: B
Explanation:

ClearPass Device Insight collects information about network-connected devices, categorizes them, and enables administrators to enforce access policies based on device type and behavior.

Question: 23

Which ClearPass feature allows for adaptive policy enforcement based on real-time user and device context?

A. Posture Assessment
B. Dynamic Role Assignment
C. Static VLAN Assignment
D. MAC Address Filtering

Answer: B
Explanation:

Dynamic Role Assignment enables ClearPass to change user access privileges based on contextual factors such as authentication method, location, and device compliance, improving security.

Question: 24

Which protocol does ClearPass use to communicate with network access devices for authentication?

A. RADIUS
B. SSH
C. SNMP
D. SMTP

Answer: A
Explanation:

RADIUS is an authentication, authorization, and accounting (AAA) protocol used by ClearPass to enforce security policies and validate users and devices accessing the network.

Question: 25

Which feature allows ClearPass to integrate with external security tools for automated threat response? (Select two.)

A. REST API
B. Syslog Integration
C. Captive Portal
D. MAC Caching

Answer: A, B
Explanation:

The REST API allows ClearPass to integrate with SIEM, firewall, and endpoint security tools, while Syslog integration enables event logging and real-time security monitoring.

Question: 26

Which authentication method allows employees to use a single sign-on (SSO) experience with ClearPass?

A. OAuth
B. SAML
C. LDAP
D. RADIUS

Answer: B
Explanation:

SAML (Security Assertion Markup Language) enables Single Sign-On (SSO) integration, allowing employees to authenticate once and gain access to multiple applications without re-entering credentials.

Which ClearPass component is primarily responsible for handling authentication requests?

A. Policy Manager

Question: 27

B. Guest Manager
C. Insight
D. OnGuard

Answer: A
Explanation:

ClearPass Policy Manager acts as the core authentication engine, processing authentication requests, applying policies, and enforcing network access control.

Question: 28

Which protocol does ClearPass use to securely authenticate administrative users logging into network devices?

A. TACACS+
B. FTP
C. SNMP
D. RADIUS

Answer: A
Explanation:

TACACS+ provides enhanced authentication and authorization controls for administrative access to network devices, offering greater flexibility and security than RADIUS.

Question: 29

Which authentication method should be used for securing IoT devices in a ClearPass environment?

A. MAC Authentication Bypass (MAB)
B. PEAP-MSCHAPv2
C. EAP-TTLS
D. Static PSK

Answer: A
Explanation:

MAC Authentication Bypass (MAB) allows ClearPass to authenticate IoT devices that lack 802.1X support, providing identity-based access control without user interaction.

Question: 30

Which feature in ClearPass allows enforcement of different access policies based on device posture compliance?

A. VLAN Assignment
B. Posture-Based Access Control
C. Role Mapping
D. Static ACLs

Answer: B
Explanation:

Posture-Based Access Control evaluates device compliance (e.g., antivirus, OS updates) before granting access, ensuring only secure devices connect to the network.

Question: 31

Which two factors does ClearPass consider when dynamically assigning roles? (Select two.)

A. User authentication method
B. Device type
C. IP address
D. VLAN assignment

Answer: A, B
Explanation:

ClearPass dynamically assigns roles based on authentication methods (e.g., 802.1X, MAC authentication) and device type, ensuring appropriate access control based on security policies.

Question: 32

Which technology does ClearPass use to provide guest users with time-limited access?

A. MAC Authentication Bypass
B. Captive Portal
C. 802.1X Authentication
D. TACACS+

Answer: B
Explanation:

Captive portals allow guests to access the network temporarily by authenticating through a web page, ensuring controlled access while maintaining security.

Which two authentication methods use certificates for authentication? (Select two.)

Question: 33

A. EAP-TLS
B. PEAP-MSCHAPv2
C. EAP-TTLS
D. PAP

Answer: A, C
Explanation:

EAP-TLS and EAP-TTLS use certificates for secure authentication, reducing password reliance. PEAP-MSCHAPv2 and PAP use credentials, making them less secure.

Question: 34

Which ClearPass feature enhances security by automatically revoking network access from compromised devices?

A. Guest Manager
B. Enforcement Profiles
C. Policy Manager
D. Endpoint Compliance

Answer: D
Explanation:

Endpoint Compliance dynamically restricts or revokes network access if a device is detected as compromised or non-compliant, ensuring network security.

Question: 35

Which authentication mechanism is used for device onboarding in ClearPass?

A. Secure SSID with PSK
B. 802.1X with EAP-TLS
C. Open SSID with Captive Portal
D. MAC Address Filtering

Answer: B
Explanation:

802.1 X with EAP-TLS enables secure onboarding by authenticating devices with digital certificates, ensuring strong identity verification without passwords.

Question: 36

Which protocol does ClearPass OnGuard use to assess device health status?

A. SNMP
B. RADIUS
C. HTTPS
D. TCP

Answer: B
Explanation:

ClearPass OnGuard communicates health posture information using RADIUS, allowing Policy Manager to enforce access restrictions based on compliance status.

Question: 37

Which two security measures does ClearPass use to protect against unauthorized network access? (Select two.)

A. Role-Based Access Control
B. MAC Address Filtering
C. Policy Enforcement with Posture Checks
D. DHCP Snooping

Answer: A, C
Explanation:

ClearPass ensures secure access using Role-Based Access Control and Posture Enforcement, dynamically restricting unauthorized devices based on security policies.

Question: 38

Which ClearPass feature provides real-time visibility into authentication and network access events?

A. Policy Manager
B. Insight
C. OnGuard
D. TACACS+

Answer: B
Explanation:

ClearPass Insight offers real-time monitoring, logs, and analytics on authentication events, enabling administrators to detect security incidents and anomalies.

Which feature allows an administrator to define network access based on device operating system and type?

Question: 39

A. Device Profiling
B. Role Mapping
C. Captive Portal
D. RADIUS Authentication

Answer: A
Explanation:

Device Profiling enables ClearPass to identify and categorize devices based on OS, manufacturer, and other attributes, enforcing appropriate access policies.

Question: 40

Which two logging mechanisms does ClearPass use for event tracking and security audits? (Select two.)

A. Syslog
B. Local Logging
C. LDAP Queries
D. DHCP Requests

Answer: A, B
Explanation:

ClearPass logs authentication events locally and sends Syslog messages to external monitoring tools, ensuring detailed tracking of security-related activities.

Question: 41

Which ClearPass component is responsible for enforcing network access policies?

A. Guest Manager
B. Policy Manager
C. Insight
D. OnGuard

Answer: B
Explanation:

ClearPass Policy Manager is the core component responsible for defining and enforcing network access policies. It evaluates authentication requests and applies security policies dynamically.

Which ClearPass module is used for endpoint health and compliance checks?

A. Insight
B. OnGuard
C. Policy Manager
D. Guest Manager

Question: 42

Answer: B
Explanation:

ClearPass OnGuard assesses endpoint health by verifying compliance with security policies such as antivirus status, OS updates, and firewall settings before granting network access.

Question: 43

Which authentication protocol does ClearPass Policy Manager support for secure user authentication? (Select two.)

A. EAP-TLS
B. PAP
C. PEAP-MSCHAPv2
D. HTTP Basic Authentication

Answer: A, C
Explanation:

EAP-TLS and PEAP-MSCHAPv2 are secure authentication protocols supported by ClearPass Policy Manager. PAP and HTTP Basic Authentication are insecure and not recommended for enterprise environments.

Question: 44

Which ClearPass module provides real-time monitoring and reporting?

A. Guest Manager
B. OnGuard
C. Insight
D. Policy Manager

Answer: C
Explanation:

ClearPass Insight provides real-time visibility into authentication events, user activity, and policy enforcement logs, helping administrators monitor network access and security trends.

Question: 45

Which ClearPass feature enables self-registration and authentication for guest users?

A. Device Insight
B. Guest Manager
C. OnGuard
D. Policy Manager

Answer: B
Explanation:

Guest Manager allows organizations to provide self-registration portals and authentication mechanisms for guest users while ensuring network security and compliance.

Question: 46

Which authentication method is recommended for machine authentication in ClearPass?

A. MAC Authentication Bypass (MAB)
B. EAP-TLS
C. PEAP-MSCHAPv2
D. PSK

Answer: B
Explanation:

EAP-TLS uses client certificates for machine authentication, ensuring secure and automatic authentication without relying on user credentials.

Question: 47

Which module allows administrators to create policies based on user roles and device types?

A. Insight
B. Policy Manager
C. Guest Manager
D. OnGuard

Answer: B
Explanation:

Policy Manager enables administrators to define access control rules based on contextual information such as user identity, role, and device type.

Question: 48

Which feature in ClearPass provides integration with third-party security solutions?

A. API and Extensions
B. VLAN Assignment
C. Captive Portal Authentication
D. SNMP Traps

Answer: A
Explanation:

ClearPass supports API and Extensions to integrate with third-party security platforms such as SIEM, firewalls, and endpoint protection solutions for enhanced security enforcement.

Question: 49

Which authentication method allows ClearPass to validate user credentials against external identity providers?

A. SAML
B. LDAP
C. OAuth
D. RADIUS

Answer: A
Explanation:

SAML (Security Assertion Markup Language) allows ClearPass to authenticate users via external identity providers such as Okta, Azure AD, and Google.

Question: 50

Which ClearPass component allows administrators to configure authentication sources?

A. Guest Manager
B. Policy Manager
C. Insight
D. OnGuard

Answer: B
Explanation:

Policy Manager provides the ability to configure authentication sources such as Active Directory,

RADIUS, and LDAP to validate user credentials during authentication requests.

Question: 51

Which ClearPass module is responsible for handling endpoint profiling?

A. Device Insight
B. Policy Manager
C. OnGuard
D. Insight

Answer: A
Explanation:

ClearPass Device Insight collects data on devices connecting to the network, identifying them based on attributes like OS, manufacturer, and MAC address to enforce security policies.

Question: 52

Which ClearPass feature allows authentication requests to be forwarded to another authentication server?

A. RADIUS Proxy
B. MAC Caching
C. Guest Access
D. VLAN Steering

Answer: A
Explanation:

RADIUS Proxy allows ClearPass to forward authentication requests to an external authentication server, enabling centralized authentication management.

Question: 53

Which type of authentication does ClearPass Guest Manager support? (Select two.)

A. Social Media Authentication
B. Certificate-Based Authentication
C. SMS Verification
D. Static PSK

Answer: A, C
Explanation:

ClearPass Guest Manager supports social media login (e.g., Google, Facebook) and SMS verification to

authenticate guest users while ensuring security and ease of access.

Question: 54

Which feature enables administrators to assign different network privileges based on authentication policies?

A. Role-Based Access Control
B. Static VLAN Assignment
C. MAC Filtering
D. DHCP Snooping

Answer: A
Explanation:

Role-Based Access Control (RBAC) in ClearPass dynamically assigns access levels based on user authentication, device type, and contextual information.

Question: 55

Which component provides a web-based interface for configuring ClearPass modules?

A. CLI
B. Policy Manager
C. ClearPass Web UI
D. Guest Manager

Answer: C
Explanation:

The ClearPass Web UI provides a centralized graphical interface for configuring Policy Manager, Guest Manager, OnGuard, and other ClearPass modules.

Question: 56

Which protocol is used by ClearPass to provide authentication, authorization, and accounting (AAA)?

A. SNMP
B. RADIUS
C. SSH
D. FTP

Answer: B
Explanation:

RADIUS is the primary AAA protocol used by ClearPass for authentication, authorization, and

accounting, ensuring secure network access control.

Question: 57

Which feature allows ClearPass to dynamically assign VLANs based on authentication policies?

A. Dynamic VLAN Assignment
B. Static IP Mapping
C. SNMP Traps
D. MAC Filtering

Answer: A
Explanation:

Dynamic VLAN Assignment in ClearPass enables the automatic assignment of VLANs based on user authentication, role, and security policies.

Question: 58

Which authentication sources can ClearPass integrate with for user validation? (Select two.)

A. Active Directory
B. LDAP
C. HTTP
D. DHCP

Answer: A, B
Explanation:

ClearPass integrates with identity providers such as Active Directory and LDAP for centralized user authentication and policy enforcement.

Question: 59

Which feature in ClearPass OnGuard ensures endpoints comply with security policies before network access?

A. Posture Assessment
B. Guest Registration
C. SNMP Polling
D. VLAN Steering

Answer: A
Explanation:

Posture Assessment evaluates endpoint security status, ensuring compliance with policies like antivirus

updates, OS patches, and firewall settings before granting access.

Question: 60

Which ClearPass module allows security teams to generate network access reports?

A. Policy Manager
B. Guest Manager
C. Insight
D. Device Insight

Answer: C
Explanation:

ClearPass Insight provides detailed reports and analytics on authentication events, network access trends, and security enforcement policies.

Question: 61

Which feature in ClearPass Policy Manager allows administrators to create rules based on multiple identity attributes?

A. Role Mapping
B. Static VLAN Assignment
C. Captive Portal Authentication
D. MAC Filtering

Answer: A
Explanation:

Role Mapping enables administrators to dynamically assign user roles based on authentication attributes such as device type, location, and security compliance. This allows for granular policy enforcement and tailored access control.

Question: 62

Which ClearPass component provides centralized visibility into authentication logs and access trends?

A. OnGuard
B. Insight
C. Guest Manager
D. Policy Manager

Answer: B
Explanation:

ClearPass Insight collects and analyzes authentication data, providing detailed reports on user access, failed login attempts, and security threats. This helps administrators monitor network health and troubleshoot authentication issues efficiently.

Question: 63

Which authentication method does ClearPass Policy Manager support for seamless user authentication via cloud identity providers?

A. TACACS+
B. SAML
C. SNMP
D. PEAP-MSCHAPv2

Answer: B
Explanation:

SAML allows ClearPass to integrate with cloud identity providers like Azure AD, Okta, and Google, providing Single Sign-On (SSO) for seamless authentication across multiple enterprise applications and services.

Question: 64

Which protocol does ClearPass use to communicate authentication decisions to network devices?

A. RADIUS
B. FTP
C. SMTP
D. ICMP

Answer: A
Explanation:

RADIUS is the primary protocol used by ClearPass for authentication, authorization, and accounting (AAA). It enables network devices such as switches and access points to enforce security policies based on authentication responses.

Question: 65

Which ClearPass module is used for endpoint security posture checks?

A. Guest Manager
B. OnGuard
C. Insight
D. Policy Manager

Answer: B
Explanation:

OnGuard evaluates endpoint compliance with security policies such as antivirus software, OS patches, and firewall status. It ensures that only compliant devices are granted network access, reducing security risks.

Question: 66

Which feature allows ClearPass to apply different access policies based on user location and device type?

A. Adaptive Policy Enforcement
B. VLAN Steering
C. SNMP Traps
D. Pre-Shared Keys

Answer: A
Explanation:

Adaptive Policy Enforcement dynamically adjusts access policies based on real-time contextual data, such as the user's location and device profile. This improves security by restricting access based on risk factors.

Question: 67

Which authentication source can ClearPass integrate with for user credential validation? (Select two.)

A. Active Directory
B. LDAP
C. SNMP
D. FTP

Answer: A, B
Explanation:

ClearPass integrates with Active Directory and LDAP to authenticate users against existing directory services. These integrations enable centralized authentication and role-based access control across the network.

Question: 68

Which two features of ClearPass OnGuard help enforce endpoint security compliance? (Select two.)

A. Posture Assessment
B. Role Mapping
C. Network Quarantine
D. SNMP Polling

Answer: A, C

Explanation:

Posture Assessment verifies whether a device meets security policies before granting network access, while Network Quarantine isolates non-compliant devices in a restricted environment for remediation.

Question: 69

Which ClearPass component enables administrators to track and manage guest access logs?

A. Policy Manager
B. OnGuard
C. Guest Manager
D. Insight

Answer: C

Explanation:

Guest Manager provides a platform for managing guest accounts, including access logs, expiration times, and authentication methods. This ensures secure and controlled guest access management.

Question: 70

Which feature in ClearPass enables the integration of security alerts and logs with external SIEM solutions?

A. Syslog Forwarding
B. MAC Caching
C. SNMP Traps
D. Pre-Shared Keys

Answer: A

Explanation:

Syslog Forwarding allows ClearPass to send authentication logs, security alerts, and access data to external SIEM platforms like Splunk and ArcSight. This enhances security monitoring and compliance auditing.

Question: 71

Which protocol is most commonly used for AAA services in ClearPass?

A. FTP
B. RADIUS
C. SNMP
D. HTTP

Answer: B
Explanation:

RADIUS is the primary protocol used for Authentication, Authorization, and Accounting (AAA) in ClearPass. It allows network devices to communicate with authentication servers for secure access control.

Question: 72

Which AAA function verifies user identity before granting network access?

A. Authorization
B. Authentication
C. Accounting
D. Encryption

Answer: B
Explanation:

Authentication is the process of verifying a user's identity using credentials such as usernames, passwords, or certificates before granting network access.

Question: 73

Which authentication protocol provides the highest level of security in a ClearPass AAA environment?

A. PAP
B. PEAP
C. EAP-TLS
D. CHAP

Answer: C
Explanation:

EAP-TLS provides the highest level of security as it uses mutual authentication with digital certificates,

eliminating password-based vulnerabilities.

Question: 74

Which protocol does ClearPass use to send accounting records to external logging systems?

A. SNMP
B. Syslog
C. RADIUS Accounting
D. DHCP

Answer: C
Explanation:

RADIUS Accounting collects and sends session-related data, such as connection time and data usage, to external logging systems for auditing and monitoring.

Question: 75

Which AAA function determines the network resources a user can access after authentication?

A. Accounting
B. Authentication
C. Authorization
D. Encryption

Answer: C
Explanation:

Authorization controls what resources a user or device can access based on policies, ensuring that only permitted actions are performed after authentication.

Question: 76

Which ClearPass feature allows administrators to define role-based access control policies?

A. Insight
B. OnGuard
C. Policy Manager
D. Guest Manager

Answer: C
Explanation:

Policy Manager in ClearPass allows administrators to configure role-based access policies based on user

attributes, device type, and authentication methods.

Question: 77

Which protocol does ClearPass support for centralized administrator authentication on network devices?

A. RADIUS
B. TACACS+
C. LDAP
D. SNMP

Answer: B
Explanation:

TACACS+ is used for authenticating administrators accessing network devices, offering granular control over command-level authorization and logging.

Question: 78

Which authentication method uses username/password credentials encrypted within a secure tunnel?

A. EAP-TLS
B. PEAP-MSCHAPv2
C. MAC Authentication Bypass
D. CHAP

Answer: B
Explanation:

PEAP-MSCHAPv2 encrypts user credentials inside a secure TLS tunnel, improving security compared to protocols that transmit passwords in plaintext.

Question: 79

Which AAA function tracks user activity and generates logs for auditing purposes?

A. Authentication
B. Authorization
C. Accounting
D. Encryption

Answer: C
Explanation:

Accounting records user activity, such as login times, session duration, and resource usage, enabling

auditing and security monitoring.

Question: 80

Which two authentication sources does ClearPass typically use for user validation? (Select two.)

A. Active Directory
B. LDAP
C. SMTP
D. SNMP

Answer: A, B
Explanation:

ClearPass integrates with Active Directory and LDAP as authentication sources to validate user credentials, ensuring secure access management.

Question: 81

Which protocol does ClearPass use for AAA communication with network devices?

A. RADIUS
B. DHCP
C. SSH
D. ICMP

Answer: A
Explanation:

RADIUS is the primary protocol for authentication, authorization, and accounting in ClearPass, facilitating secure communication between network devices and authentication servers.

Question: 82

Which authentication method allows user login without requiring credentials on subsequent connections?

A. MAC Authentication Bypass (MAB)
B. EAP-TLS
C. PSK Authentication
D. PEAP-MSCHAPv2

Answer: A
Explanation:

MAC Authentication Bypass (MAB) enables devices to authenticate based on their MAC address,

eliminating the need for user credentials but providing limited security.

Question: 83

Which AAA component is responsible for validating identity before assigning a network role?

A. Authentication
B. Authorization
C. Accounting
D. Policy Mapping

Answer: A
Explanation:

Authentication verifies user identity using credentials, certificates, or other identity mechanisms before assigning network access policies.

Question: 84

Which protocol does ClearPass use to forward authentication requests to external identity providers?

A. TACACS+
B. RADIUS Proxy
C. LDAP
D. SNMP

Answer: B
Explanation:

RADIUS Proxy enables ClearPass to forward authentication requests to external RADIUS servers, allowing integration with remote authentication services.

Question: 85

Which authentication method requires both a user certificate and a server certificate for mutual authentication?

A. EAP-TLS
B. PEAP
C. MAC Authentication Bypass
D. CHAP

Answer: A
Explanation:

EAP-TLS provides mutual authentication between client and server using digital certificates, eliminating the risk of password-based attacks.

Question: 86

Which two authentication protocols support password-based authentication over a secure tunnel? (Select two.)

A. PEAP
B. EAP-TTLS
C. PAP
D. CHAP

Answer: A, B
Explanation:

PEAP and EAP-TTLS use a secure TLS tunnel to encrypt user credentials during authentication, enhancing security compared to unencrypted methods like PAP and CHAP.

Question: 87

Which ClearPass feature allows network access based on device type and security posture?

A. Policy Manager
B. Role Mapping
C. Adaptive Policy Enforcement
D. MAC Filtering

Answer: C
Explanation:

Adaptive Policy Enforcement dynamically modifies access privileges based on user, device, and real-time posture assessment, improving security.

Question: 88

Which component of the AAA model determines what actions an authenticated user can perform?

A. Authentication
B. Authorization
C. Accounting
D. Policy Enforcement

Answer: B
Explanation:

Authorization controls access to network resources by applying policies that dictate the actions a user or device can perform after authentication.

Question: 89

Which authentication method is preferred for secure, passwordless network authentication?

A. EAP-TLS
B. PEAP
C. MAC Authentication Bypass
D. CHAP

Answer: A
Explanation:

EAP-TLS is a certificate-based authentication method that eliminates password vulnerabilities by requiring digital certificates for mutual authentication.

Question: 90

Which ClearPass component allows the enforcement of granular access policies based on authentication results?

A. Insight
B. Policy Manager
C. Guest Manager
D. Device Insight

Answer: B
Explanation:

Policy Manager enables administrators to define and enforce authentication-based policies, dynamically adjusting network access based on user identity and security posture.

Question: 91

Which ClearPass feature allows administrators to apply different levels of network access based on authentication attributes?

A. Role-Based Access Control
B. Static VLAN Assignment
C. Guest Self-Registration
D. Pre-Shared Key Authentication

Answer: A
Explanation:

Role-Based Access Control (RBAC) assigns access levels dynamically based on authentication attributes such as user identity, device type, and security posture. This ensures users receive appropriate permissions

while maintaining security.

Question: 92

Which two authentication protocols use encrypted tunnels to protect user credentials during authentication? (Select two.)

A. PEAP
B. EAP-TTLS
C. PAP
D. CHAP

Answer: A, B

Explanation:

PEAP and EAP-TTLS establish encrypted tunnels before transmitting user credentials, enhancing security by preventing credential interception. PAP and CHAP are outdated and transmit credentials in less secure ways.

Question: 93

Which component of AAA is responsible for logging network access details such as session duration and data usage?

A. Authentication
B. Authorization
C. Accounting
D. Identity Mapping

Answer: C

Explanation:

Accounting logs user session details, including login/logout times, duration, and data consumption, providing visibility for auditing, compliance, and security analysis.

Question: 94

Which authentication protocol provides mutual authentication using client and server certificates?

A. PEAP

B. EAP-TLS
C. EAP-TTLS
D. MSCHAPv2

Answer: B
Explanation:

EAP-TLS provides mutual authentication, requiring both client and server certificates to validate each other's identity, offering the highest level of security in enterprise environments.

Question: 95

Which authentication method does ClearPass use to authenticate IoT devices that lack 802.1X support?

A. MAC Authentication Bypass (MAB)
B. PEAP-MSCHAPv2
C. EAP-TLS
D. OAuth

Answer: A
Explanation:

MAC Authentication Bypass (MAB) allows devices without 802.1X capabilities to authenticate based on their MAC addresses. While convenient for IoT, it provides limited security and should be combined with other controls.

Question: 96

Which authentication method allows ClearPass to use external identity providers such as Google and Azure AD?

A. SAML RADIUS TACACS+ LDAP
B.
C. **Answer: A**
D. **Explanation:**

Security Assertion Markup Language (SAML) enables Single Sign-On (SSO) with cloud-based identity providers, allowing users to authenticate via external services such as Google and Azure AD.

Question: 97

Which AAA function allows network administrators to control which VLANs users are assigned to after

authentication?

A. Authentication
B. Authorization
C. Accounting
D. Adaptive Enforcement

Answer: B
Explanation:

Authorization determines what resources users can access, including VLAN assignment, role-based policies, and access control lists (ACLs) based on authentication results.

Question: 98

Which two authentication sources are commonly integrated with ClearPass for user validation? (Select two.)

A. Active Directory
B. LDAP
C. SNMP
D. ICMP

Answer: A, B
Explanation:

ClearPass integrates with Active Directory and LDAP to authenticate users against directory services, enabling centralized authentication, policy enforcement, and role mapping for enterprise environments.

Question: 99

Which feature in ClearPass ensures that authentication requests from specific devices or users are forwarded to external authentication servers?

A. RADIUS Proxy B. MAC Filtering C. Captive Portal D. VLAN Steering

Answer: A
Explanation:

RADIUS Proxy enables ClearPass to forward authentication requests to external RADIUS servers, allowing authentication load balancing and integration with third-party authentication systems.

Question: 100

Which function of AAA ensures that user activities are logged and monitored for auditing purposes?

A. Authentication
B. Authorization
C. Accounting
D. Identity Profiling

Answer: C
Explanation:

Accounting records user authentication events, access history, and resource usage, allowing organizations to monitor user activity, detect anomalies, and comply with security policies.

Question: 101

Which ClearPass component is responsible for handling authentication requests?

A. Policy Manager
B. Insight
C. Guest Manager
D. OnGuard

Answer: A
Explanation:

ClearPass Policy Manager processes authentication requests and applies access control policies based on user identity, device type, and security posture. It enforces role-based network access rules dynamically.

Question: 102

Which protocol does ClearPass use for secure authentication and authorization?

A. SNMP
B. RADIUS
C. SMTP
D. FTP

Answer: B
Explanation:

RADIUS is the primary protocol used by ClearPass for Authentication, Authorization, and Accounting (AAA). It facilitates secure communication between network access devices and authentication servers.

Question: 103

Which authentication source can be integrated into ClearPass for user validation? (Select two.)

A. Active Directory
B. LDAP

C. DHCP
D. Syslog

Answer: A, B
Explanation:

ClearPass supports Active Directory and LDAP as authentication sources to validate user credentials and retrieve user attributes. These integrations enable centralized authentication and policy enforcement.

Question: 104

Which ClearPass feature allows authentication requests to be forwarded to an external RADIUS server?

A. RADIUS Proxy
B. MAC Caching
C. Captive Portal
D. VLAN Steering

Answer: A
Explanation:

RADIUS Proxy enables ClearPass to forward authentication requests to an external RADIUS server, allowing for authentication delegation and centralized identity management.

Question: 105

Which authentication method is best suited for certificate-based authentication in ClearPass?

A. PEAP
B. EAP-TLS
C. CHAP
D. PAP

Answer: B
Explanation:

EAP-TLS provides secure certificate-based authentication by using client and server certificates. It eliminates password-based vulnerabilities and ensures mutual authentication.

Question: 106

Which authentication method allows ClearPass to authenticate devices that do not support 802.1X?

A. MAC Authentication Bypass (MAB)
B. PEAP-MSCHAPv2
C. EAP-TTLS

D. OAuth

Answer: A
Explanation:

MAC Authentication Bypass (MAB) authenticates devices based on their MAC addresses when 802.1X authentication is not possible. While convenient for IoT devices, it has limited security.

Question: 107

Which ClearPass feature allows administrators to enforce different access policies based on authentication attributes?

A. Role Mapping
B. Static VLAN Assignment
C. MAC Filtering
D. SNMP Traps

Answer: A
Explanation:

Role Mapping dynamically assigns roles based on authentication attributes such as device type, authentication method, and user group, allowing granular access control.

Question: 108

Which authentication method allows guest users to self-register in ClearPass?

A. SAML
B. OAuth
C. Captive Portal
D. EAP-TLS

Answer: C
Explanation:

A Captive Portal provides a web-based authentication mechanism for guest users, allowing them to self-register and gain controlled network access. It integrates with social logins and SMS verification.

Question: 109

Which ClearPass module is responsible for generating authentication and policy enforcement reports?

A. OnGuard
B. Guest Manager
C. Insight

D. Policy Manager

Answer: C
Explanation:

ClearPass Insight provides detailed reports on authentication events, policy enforcement actions, and security incidents. It helps administrators analyze trends and improve security posture.

Question: 110

Which authentication method is recommended for securing network access using user credentials over an encrypted tunnel?

A. PEAP-MSCHAPv2
B. PAP
C. MAC Authentication Bypass
D. CHAP

Answer: A
Explanation:

PEAP-MSCHAPv2 provides encrypted authentication by encapsulating user credentials inside a secure TLS tunnel, preventing password interception and replay attacks.

Question: 111

Which service type should be configured in ClearPass to support 802.1X authentication for wired and wireless networks?

A. RADIUS Enforcement
B. TACACS+ Authentication
C. Guest Access Service
D. DHCP Relay

Answer: A
Explanation:

The RADIUS Enforcement service in ClearPass handles 802.1X authentication requests for wired and wireless networks, enforcing policies and granting appropriate access permissions.

Question: 112

Which ClearPass feature dynamically assigns VLANs based on authentication results?

A. Adaptive Policy Enforcement
B. MAC Filtering

C. VLAN Steering
D. Pre-Shared Keys

Answer: C
Explanation:

VLAN Steering dynamically assigns users and devices to specific VLANs based on authentication attributes, ensuring appropriate network segmentation and access control.

Question: 113

Which protocol does ClearPass use to provide centralized authentication and authorization for administrators accessing network devices?

A. RADIUS
B. TACACS+
C. LDAP
D. FTP

Answer: B
Explanation:

TACACS+ provides centralized authentication and authorization for network device administration. It allows granular command-level authorization and detailed logging of administrator actions.

Question: 114

Which two authentication methods allow ClearPass to validate user credentials against an external identity provider? (Select two.)

A. SAML
B. RADIUS Proxy
C. SNMP
D. FTP

Answer: A, B
Explanation:

SAML and RADIUS Proxy enable ClearPass to authenticate users via external identity providers, facilitating Single Sign-On (SSO) and integration with third-party authentication servers.

Question: 115

Which ClearPass service is required to integrate with an external multi-factor authentication (MFA) provider?

A. RADIUS Proxy
B. Guest Manager
C. TACACS+ Service D. Syslog Forwarding

Answer: A
Explanation:

RADIUS Proxy allows ClearPass to forward authentication requests to an external multi-factor authentication provider, enabling additional security layers beyond passwords.

Question: 116

Which authentication method does ClearPass recommend for securing administrator logins to network devices?

A. TACACS+
B. RADIUS
C. MAC Authentication Bypass
D. Open Authentication

Answer: A
Explanation:

TACACS+ provides secure authentication for administrators, supporting granular authorization policies and encrypted communications for command execution.

Question: 117

Which two authentication sources are commonly used with ClearPass for user authentication? (Select two.)

A. Active Directory
B. LDAP
C. SNMP
D. DHCP

Answer: A, B
Explanation:

Active Directory and LDAP are commonly used authentication sources in ClearPass, enabling integration with enterprise identity directories for user authentication and access control.

Question: 118

Which authentication feature in ClearPass allows administrators to enforce security policies based on

device posture compliance?

A. OnGuard
B. Guest Manager
C. Insight
D. VLAN Steering

Answer: A
Explanation:

ClearPass OnGuard assesses device compliance with security policies, ensuring that only devices meeting security requirements (e.g., antivirus, OS updates) are granted network access.

Question: 119

Which feature in ClearPass allows authentication and authorization based on user location and time of day?

A. Adaptive Policy Enforcement
B. Pre-Shared Keys
C. Static VLAN Assignment
D. MAC Caching

Answer: A
Explanation:

Adaptive Policy Enforcement dynamically adjusts access policies based on contextual factors such as user location, time of access, and device security posture.

Question: 120

Which ClearPass feature ensures that unauthorized devices are redirected to a remediation portal?

A. Captive Portal Enforcement
B. VLAN Steering
C. MAC Filtering
D. Role Mapping

Answer: A
Explanation:

Captive Portal Enforcement redirects non-compliant or unauthorized devices to a remediation portal, requiring users to take corrective actions before obtaining network access.

Question: 121

Which authentication protocol should be used in ClearPass for secure authentication with both username and password over an encrypted tunnel?

A. PAP
B. PEAP-MSCHAPv2
C. CHAP
D. EAP-TLS

Answer: B
Explanation:

PEAP-MSCHAPv2 secures authentication by encrypting credentials inside a TLS tunnel, preventing password exposure during transmission. It is widely used for secure wireless authentication in enterprise networks.

Question: 122

Which ClearPass feature allows the enforcement of access policies based on device type and security posture?

A. Guest Manager
B. Insight
C. OnGuard
D. TACACS+

Answer: C
Explanation:

OnGuard performs real-time posture assessments to verify if a device meets security compliance requirements, such as antivirus installation or OS patching, before granting network access.

Which ClearPass component is primarily used for creating and enforcing authentication rules?

A. Insight

Question: 123

B. Policy Manager
C. Device Insight
D. OnGuard

Answer: B
Explanation:

Policy Manager enables administrators to define authentication policies, enforce role-based access control, and dynamically apply network policies based on user identity and device security.

Question: 124

Which feature in ClearPass enables guest users to receive network credentials via email or SMS?

A. Guest Manager
B. OnGuard
C. RADIUS Proxy
D. Insight

Answer: A
Explanation:

Guest Manager allows self-service registration and credential delivery via email or SMS, ensuring secure and controlled guest access while simplifying authentication management.

Question: 125

Which ClearPass authentication source allows integration with cloud-based identity providers like Azure AD?

A. LDAP
B. RADIUS Proxy
C. SAML
D. TACACS+

Answer: C
Explanation:

SAML enables ClearPass to integrate with cloud identity providers, allowing Single Sign-On (SSO) authentication and seamless user access to enterprise applications.

Which ClearPass feature assigns different levels of access based on authentication results?

A. Role Mapping
B. Static VLAN Assignment
C. MAC Authentication Bypass
D. DHCP Snooping

Question: 126

Answer: A
Explanation:

Role Mapping dynamically assigns user roles based on authentication attributes, such as device type and user identity, allowing enforcement of different security policies.

Question: 127

Which authentication method does ClearPass recommend for IoT devices that lack 802.1X support?

A. MAC Authentication Bypass (MAB)
B. EAP-TLS
C. PEAP-MSCHAPv2
D. OAuth

Answer: A
Explanation:

MAB enables ClearPass to authenticate devices that cannot support 802.1X by using their MAC address, though it is less secure and should be combined with additional security measures.

Question: 128

Which feature in ClearPass enables administrators to quarantine non-compliant devices?

A. Posture Enforcement
B. RADIUS Proxy
C. TACACS+ Authorization
D. Captive Portal

Answer: A
Explanation:

Posture Enforcement ensures that devices failing security checks, such as outdated antivirus or OS patches, are quarantined in a restricted network until they meet compliance requirements.

Question: 129

Which protocol does ClearPass use for centralized authentication and accounting?

A. SNMP
B. RADIUS
C. SMTP
D. FTP

Answer: B
Explanation:

RADIUS provides authentication, authorization, and accounting (AAA) functions, allowing ClearPass to manage network access control securely across wired and wireless networks.

Question: 130

Which ClearPass module provides real-time analytics and authentication event logs?

A. Guest Manager
B. Insight
C. Policy Manager
D. OnGuard

Answer: B
Explanation:

Insight collects and analyzes authentication events, policy enforcement actions, and network access trends, providing administrators with visibility into security and compliance issues.

Question: 131

Which ClearPass feature allows authentication policies to be adjusted dynamically based on user behavior?

A. Adaptive Policy Enforcement
B. Static ACLs
C. Pre-Shared Keys
D. SNMP Traps

Answer: A
Explanation:

Adaptive Policy Enforcement modifies access policies dynamically based on user activity, security posture, and contextual attributes, improving overall network security.

Which authentication method provides passwordless authentication in ClearPass?

A. EAP-TLS
B. PEAP
C. MAC Authentication Bypass
D. MSCHAPv2

Answer: A
Explanation:

EAP-TLS uses client and server certificates for authentication, eliminating password vulnerabilities while ensuring secure, mutual authentication between endpoints and the network.

Question: 132

Question: 133

Which ClearPass service enables integration with external multi-factor authentication (MFA) providers?

A. RADIUS Proxy
B. Guest Manager
C. TACACS+
D. Insight

Answer: A
Explanation:

RADIUS Proxy allows ClearPass to forward authentication requests to external MFA providers, adding an additional security layer beyond passwords and improving user authentication security.

Question: 134

Which protocol does ClearPass use to provide authentication for network device administrators?

A. TACACS+
B. LDAP
C. SNMP
D. DHCP

Answer: A
Explanation:

TACACS+ authenticates and authorizes network device administrators, providing centralized control over access and logging of command execution for security auditing.

Question: 135

Which ClearPass feature allows role-based access control based on authentication attributes?

A. Policy Manager
B. Insight
C. Device Profiling
D. OnGuard

Answer: A
Explanation:

Policy Manager enforces role-based access control by assigning user roles dynamically based on authentication attributes, ensuring security and compliance across network access points.

Question: 136

Which authentication protocol allows for seamless Single Sign-On (SSO) with external identity providers?

A. SAML
B. RADIUS
C. EAP-TLS
D. TACACS+

Answer: A
Explanation:

SAML enables ClearPass to authenticate users through external identity providers, providing a seamless Single Sign-On (SSO) experience across multiple applications and services.

Question: 137

Which feature in ClearPass allows guest users to be redirected to an authentication page before gaining network access?

A. Captive Portal
B. VLAN Steering
C. MAC Filtering
D. Static IP Mapping

Answer: A
Explanation:

Captive Portal redirects unauthenticated users to a login page where they can register, authenticate, or agree to terms before being granted network access.

Question: 138

Which authentication method allows devices to connect to the network without user intervention?

A. MAC Authentication Bypass
B. PEAP
C. OAuth
D. PAP

Answer: A
Explanation:

MAC Authentication Bypass (MAB) authenticates devices using their MAC addresses, enabling automated network access for devices that do not support 802.1X authentication.

Question: 139

Which ClearPass feature allows authentication requests to be forwarded to an external authentication server?

A. RADIUS Proxy
B. TACACS+
C. SNMP
D. DHCP Relay

Answer: A
Explanation:

RADIUS Proxy enables ClearPass to forward authentication requests to external authentication servers, facilitating centralized authentication across multiple environments.

Question: 140

Which ClearPass feature dynamically restricts network access based on a device's security posture?

A. OnGuard Posture Assessment
B. Captive Portal Enforcement
C. RADIUS Proxy
D. SNMP Polling

Answer: A
Explanation:

OnGuard Posture Assessment checks device security compliance, such as antivirus status and OS

updates, dynamically restricting or granting access based on compliance status.

Question: 141

What is the primary function of Dynamic User Roles in ClearPass?

A. Assigning static VLANs to devices
B. Dynamically enforcing access policies based on user authentication
C. Configuring predefined firewall rules for all users
D. Assigning MAC addresses to user devices

Answer: B
Explanation:

Dynamic User Roles allow ClearPass to enforce network access policies based on authentication factors such as user identity, device type, and security posture, enabling adaptive security controls.

Question: 142

Which two components are required for implementing Dynamic Segmentation in ClearPass? (Select two.)

A. Aruba Policy Enforcement Firewall (PEF)
B. VLAN Trunking Protocol (VTP)
C. ClearPass Policy Manager
D. Layer 3 Routing Protocol

Answer: A, C
Explanation:

Aruba PEF applies role-based access controls, while ClearPass Policy Manager defines authentication and authorization policies, together enabling Dynamic Segmentation.

Question: 143

Which feature allows ClearPass to enforce different levels of access based on authentication results?

A. Role Mapping
B. VLAN Steering
C. Guest Self-Registration
D. MAC Authentication Bypass

Answer: A
Explanation:

Role Mapping dynamically assigns access levels based on authentication factors, ensuring that users

receive appropriate permissions based on their identity and security posture.

Question: 144

Which protocol does ClearPass use to enforce Dynamic User Role-based policies?

A. RADIUS
B. HTTP
C. SSH
D. SNMP

Answer: A
Explanation:

RADIUS is used by ClearPass to authenticate users and enforce Dynamic User Roles by assigning policies to devices based on authentication results.

Question: 145

Which ClearPass feature enables per-user access control without requiring VLAN changes?

A. Role-Based Firewall Policies
B. Port-Based Access Control
C. Static VLAN Assignment
D. Network Address Translation (NAT)

Answer: A
Explanation:

Role-Based Firewall Policies allow user access control at the device level without modifying VLAN configurations, ensuring flexibility and security in network segmentation.

Question: 146

Which two criteria can be used for Dynamic User Role assignment in ClearPass? (Select two.)

A. User Identity
B. Device Type
C. IP Address Subnet
D. DHCP Lease Time

Answer: A, B
Explanation:

Dynamic User Roles can be assigned based on user authentication credentials and device type, allowing

granular access control for different users and endpoints.

Question: 147

Which ClearPass component is responsible for dynamically assigning VLANs and firewall rules based on user roles?

A. Policy Manager
B. Insight
C. OnGuard
D. Guest Manager

Answer: A
Explanation:

ClearPass Policy Manager enforces role-based network segmentation by dynamically assigning VLANs, firewall policies, and access permissions based on authentication results.

Question: 148

Which benefit does ClearPass Dynamic Segmentation provide over traditional VLAN-based segmentation?

A. Reduces the need for static VLAN assignments
B. Requires manual network configuration for each user
C. Assigns the same access level to all users
D. Only applies to wired networks

Answer: A
Explanation:

Dynamic Segmentation allows ClearPass to enforce security policies without static VLAN assignments, making network access more flexible and scalable.

Question: 149

Which ClearPass feature allows a device to be assigned a role before authentication is complete?

A. Pre-Authentication Role Mapping
B. MAC Authentication Bypass (MAB)
C. Captive Portal Enforcement
D. 802.1X Supplicant Enforcement

Answer: A
Explanation:

Pre-Authentication Role Mapping assigns a temporary role to a device before full authentication, allowing restricted network access until the authentication process is complete.

Question: 150

Which authentication method is most commonly used to implement Dynamic User Roles in ClearPass?

A. 802.1X Authentication
B. MAC Authentication Bypass (MAB)
C. Pre-Shared Keys (PSK)
D. Web-based Captive Portal

Answer: A
Explanation:

802.1 X Authentication enables ClearPass to apply Dynamic User Roles by verifying user credentials and assigning access policies dynamically.

Question: 151

Which two technologies are commonly integrated with ClearPass for Dynamic Segmentation? (Select two.)

A. Aruba Switches
B. Aruba Gateways
C. Layer 3 Routing Protocols
D. VLAN Spanning Tree Protocol

Answer: A, B
Explanation:

Aruba switches and gateways integrate with ClearPass to enforce Dynamic Segmentation, allowing access control policies to be applied without requiring VLAN changes.

Question: 152

Which component enables automatic role enforcement for IoT devices in ClearPass?

A. ClearPass Device Insight
B. Aruba Central
C. VLAN Trunking
D. RADIUS Proxy

Answer: A

Explanation:

ClearPass Device Insight identifies and classifies IoT devices, allowing automatic role assignment and policy enforcement based on predefined security profiles.

Question: 153

Which ClearPass feature ensures that only authorized users can access the network?

A. Role-Based Access Control
B. Static VLAN Assignment
C. Manual ACL Configuration
D. SNMP Polling

Answer: A

Explanation:

Role-Based Access Control dynamically enforces access policies based on authentication factors, ensuring that only authorized users receive appropriate network permissions.

Question: 154

Which two authentication sources can ClearPass use for Dynamic User Role enforcement? (Select two.)

A. Active Directory
B. LDAP
C. DHCP Server
D. SNMP

Answer: A, B

Explanation:

Active Directory and LDAP provide identity verification and user attributes that ClearPass uses to enforce Dynamic User Roles and apply security policies.

Question: 155

Which component in ClearPass enables role-based firewall enforcement?

A. Aruba Policy Enforcement Firewall (PEF)
B. OnGuard
C. Guest Manager
D. DHCP Server

Answer: A

Explanation:

Aruba Policy Enforcement Firewall (PEF) applies firewall rules dynamically based on user roles, ensuring adaptive security enforcement across the network.

Question: 156

Which ClearPass feature allows guest users to be assigned a temporary role before authentication?

A. Pre-Authentication Role
B. Captive Portal Role
C. MAC Caching
D. SNMP Enforcement

Answer: A
Explanation:

Pre-Authentication Role assigns a restricted network role to guest users before authentication, ensuring limited access until verification is complete.

Question: 157

Which protocol is commonly used to communicate Dynamic User Role assignments to Aruba switches?

A. RADIUS Change of Authorization (CoA)
B. SNMP
C. HTTPS
D. FTP

Answer: A
Explanation:

RADIUS Change of Authorization (CoA) allows ClearPass to dynamically update user roles and enforce policy changes without requiring re-authentication.

Question: 158

Which two enforcement actions can ClearPass take based on Dynamic User Roles? (Select two.)

A. Assign VLANs
B. Apply Access Control Lists (ACLs)
C. Disable Physical Switch Ports
D. Change Switch Management IP

Answer: A, B

Explanation:

ClearPass can dynamically assign VLANs and apply ACLs based on user roles, ensuring appropriate

access control without manual configuration.

Question: 159

Which method allows returning users to retain their previous access role without re-authentication?

A. MAC Caching
B. 802.1X Authentication
C. Pre-Shared Key (PSK) Assignment
D. SNMP Role Mapping

Answer: A
Explanation:

MAC Caching stores device information and role assignments, allowing returning users to regain previous network access permissions without repeated authentication.

Question: 160

Which security feature in ClearPass prevents unauthorized role elevation for users?

A. Role Hierarchy Enforcement
B. Captive Portal Authentication
C. Guest VLAN Assignment
D. SNMP Access Control

Answer: A
Explanation:

Role Hierarchy Enforcement ensures that users cannot escalate privileges beyond their assigned roles, maintaining strict access control across the network.

Question: 161

Which benefit does Dynamic Segmentation provide in a network?

A. Eliminates the need for static VLAN assignments
B. Requires manual role-based configuration
C. Prevents user authentication
D. Only applies to wired networks

Answer: A

Explanation:

Dynamic Segmentation allows ClearPass to enforce security policies dynamically without requiring static VLAN assignments, making network access more flexible and scalable.

Question: 162

Which ClearPass feature allows network segmentation based on device posture and user authentication?

A. ClearPass Policy Manager
B. ClearPass OnGuard
C. Guest Manager
D. Static VLAN Mapping

Answer: B

Explanation:

ClearPass OnGuard assesses device posture and user authentication status, dynamically assigning network segmentation policies to enhance security.

Question: 163

Which two methods are commonly used in ClearPass to assign user roles dynamically? (Select two.)

A. Role Mapping
B. Policy Enforcement Firewall (PEF)
C. MAC Address Filtering
D. SNMP-Based Authentication

Answer: A, B

Explanation:

Role Mapping assigns access levels based on authentication attributes, while Policy Enforcement Firewall (PEF) applies firewall policies dynamically to enforce security rules.

Question: 164

Which feature in ClearPass enables automatic VLAN assignments based on user roles?

A. VLAN Steering
B. Static VLAN Assignment
C. SNMP VLAN Trunking
D. Guest Self-Registration

Answer: A

Explanation:

VLAN Steering dynamically assigns VLANs based on user authentication and security posture, eliminating the need for manual VLAN configurations.

Question: 165

Which two authentication protocols support Dynamic User Role enforcement in ClearPass? (Select two.)

A. EAP-TLS
B. PEAP-MSCHAPv2
C. FTP
D. SNMP

Answer: A, B
Explanation:

EAP-TLS and PEAP-MSCHAPv2 are widely used for secure authentication in ClearPass, enabling the enforcement of Dynamic User Roles and access policies.

Question: 166

Which component enables ClearPass to apply policy-based role enforcement on Aruba switches?

A. Policy Enforcement Firewall (PEF)
B. VLAN Trunking Protocol (VTP)
C. DNS-Based Routing
D. Static Access Control Lists

Answer: A
Explanation:

Aruba Policy Enforcement Firewall (PEF) integrates with ClearPass to apply security policies dynamically, ensuring flexible and role-based network access control.

Question: 167

Which enforcement action can ClearPass take based on Dynamic Segmentation?

A. Assign VLANs dynamically
B. Block non-compliant devices
C. Enable DHCP Snooping
D. Change user MAC addresses

Answer: A

Explanation:

ClearPass can dynamically assign VLANs based on authentication and device compliance, ensuring that users and devices are placed in the correct network segment.

Question: 168

Which two criteria can ClearPass use to assign dynamic roles? (Select two.)

A. User Group Membership
B. Device Type
C. IP Address Reservation
D. SNMP Configuration

Answer: A, B
Explanation:

Dynamic roles in ClearPass can be assigned based on User Group Membership from Active Directory and Device Type detected through profiling mechanisms.

Question: 169

Which feature in ClearPass allows dynamic segmentation without changing VLAN configurations?

A. Role-Based Firewall Policies
B. Pre-Shared Keys
C. MAC Filtering
D. Spanning Tree Protocol

Answer: A
Explanation:

Role-Based Firewall Policies enforce network segmentation without requiring VLAN changes, providing security and flexibility in dynamic access control.

Question: 170

Which protocol is commonly used to assign Dynamic User Roles in ClearPass?

A. RADIUS
B. SNMP
C. HTTP SSH
D.

Answer: A

Explanation:

RADIUS is used by ClearPass to assign Dynamic User Roles by communicating authentication, authorization, and accounting (AAA) data to network devices.

Question: 171

Which ClearPass feature allows role-based access control for unmanaged IoT devices?

A. Device Insight
B. Policy Manager
C. Guest Manager
D. SNMP Authentication

Answer: A
Explanation:

ClearPass Device Insight enables role-based access control for IoT devices by identifying and classifying unmanaged endpoints dynamically.

Question: 172

Which security mechanism in ClearPass ensures that a user cannot elevate privileges beyond their assigned role?

A. Role Hierarchy Enforcement
B. Static VLAN Assignment
C. Manual Access Control Lists
D. SNMP Polling

Answer: A
Explanation:

Role Hierarchy Enforcement ensures users cannot gain unauthorized access to higher-privilege roles, preventing security breaches and maintaining strict access control.

Question: 173

Which ClearPass feature prevents unauthorized access by dynamically segmenting non-compliant devices?

A. Quarantine VLANs
B. DHCP Snooping
C. Static Role Assignment
D. Load Balancing

Answer: A
Explanation:

Quarantine VLANs isolate non-compliant or untrusted devices from the production network, enforcing security policies until compliance is restored.

Question: 174

Which enforcement method in ClearPass ensures that authenticated users receive different policies based on their roles?

A. Role-Based Access Control (RBAC)
B. VLAN Trunking
C. Dynamic DNS Resolution
D. Static ACLs

Answer: A
Explanation:

Role-Based Access Control (RBAC) allows different users and devices to receive appropriate policies based on their authentication status and security posture.

Question: 175

Which feature in ClearPass dynamically adjusts network access policies based on user behavior?

A. Adaptive Policy Enforcement
B. Static Policy Mapping
C. SNMP-Based Enforcement
D. Pre-Shared Key Assignment

Answer: A
Explanation:

Adaptive Policy Enforcement dynamically adjusts network access policies in response to changing user behavior and security posture, ensuring real-time protection.

Question: 176

Which two conditions can ClearPass use to dynamically adjust firewall policies? (Select two.)

A. User Identity
B. Device Health Posture
C. DNS Server Configuration
D. MAC Address Duplication

Answer: A, B
Explanation:

User Identity and Device Health Posture allow ClearPass to adjust firewall policies dynamically, ensuring

access control is based on real-time security assessments.

Question: 177

Which protocol does ClearPass use to enforce Dynamic User Role changes on an Aruba switch?

A. RADIUS Change of Authorization (CoA)
B. SNMP Traps
C. LDAP Queries
D. FTP Transfers

Answer: A
Explanation:

RADIUS Change of Authorization (CoA) allows ClearPass to dynamically modify user roles and apply updated access policies without requiring re-authentication.

Question: 178

Which enforcement action can be applied when ClearPass detects a non-compliant device?

A. Redirect to a Remediation Portal
B. Assign a Restricted Role
C. Block All Network Traffic
D. Reassign to a Lower-Priority VLAN

Answer: A, B
Explanation:

ClearPass can redirect non-compliant devices to a remediation portal or assign a restricted role, limiting their access until compliance requirements are met.

Question: 179

Which component in ClearPass enables administrators to view role assignments and segmentation policies?

A. Insight
B. OnGuard
C. Guest Manager
D. DHCP Server

Answer: A
Explanation:

Insight provides reporting and analytics on role assignments, policy enforcement actions, and network

segmentation, offering visibility into access control.

Question: 180

Which security feature ensures that IoT devices receive the appropriate network segmentation policy?

A. Device Profiling
B. Static IP Addressing
C. SNMP-Based Authentication
D. DNS Load Balancing

Answer: A
Explanation:

Device Profiling enables ClearPass to identify IoT devices dynamically and assign them to the correct security policies, ensuring controlled network segmentation.

Question: 181

Which ClearPass component is responsible for onboarding devices securely?

A. ClearPass Onboard
B. ClearPass Guest
C. ClearPass Insight
D. ClearPass OnGuard

Answer: A
Explanation:

ClearPass Onboard automates device provisioning by securely enrolling and configuring devices with certificates, ensuring seamless and secure network access.

Question: 182

Which authentication method does ClearPass Onboard use for secure device provisioning?

A. EAP-TLS
B. PEAP-MSCHAPv2
C. MAC Authentication
D. Pre-Shared Keys

Answer: A
Explanation:

EAP-TLS is commonly used in ClearPass Onboard for secure authentication, leveraging certificates to provide strong, identity-based authentication without passwords.

Question: 183

Which two security policies can ClearPass enforce based on posture assessment? (Select two.)

A. Quarantine non-compliant devices
B. Restrict access based on antivirus status
C. Assign a static IP address
D. Change the MAC address dynamically

Answer: A, B

Explanation:

ClearPass OnGuard assesses endpoint posture (e.g., antivirus, OS updates) and can quarantine non-compliant devices or restrict access until security requirements are met.

Question: 184

Which ClearPass component is used for real-time device health enforcement?

A. OnGuard
B. Onboard
C. Guest Manager
D. Insight

Answer: A

Explanation:

OnGuard continuously evaluates endpoint security posture and enforces policies dynamically, ensuring compliance before granting or maintaining network access.

Question: 185

Which posture enforcement method allows ClearPass to restrict network access based on endpoint security status?

A. Role-based enforcement
B. MAC Filtering
C. SNMP Polling
D. DNS Filtering

Answer: A

Explanation:

Role-based enforcement dynamically assigns access permissions based on device posture, ensuring non-compliant devices receive restricted access or remediation steps.

Question: 186

Which two attributes can ClearPass check when performing posture enforcement? (Select two.)

A. Antivirus status
B. Operating system version
C. VLAN ID
D. Subnet Mask

Answer: A, B
Explanation:

ClearPass can assess the antivirus status and operating system version of endpoints, ensuring that only compliant devices are granted full network access.

Question: 187

Which feature in ClearPass Onboard enables self-service device provisioning?

A. Self-Registration Portal
B. Role Mapping
C. Network Access Control (NAC)
D. SNMP Authentication

Answer: A
Explanation:

The Self-Registration Portal allows users to enroll their own devices securely through ClearPass Onboard, streamlining device provisioning with minimal administrative overhead.

Question: 188

Which enforcement action can be applied when ClearPass OnGuard detects a non-compliant device?

A. Redirect to a remediation portal
B. Assign a restricted access role
C. Allow full network access
D. Change the device's MAC address

Answer: A, B
Explanation:

OnGuard can redirect non-compliant devices to a remediation portal or assign a restricted role, limiting access until security requirements are met.

Question: 189

Which certificate authority is commonly used in ClearPass Onboard for device authentication?

A. Internal ClearPass CA
B. Let's Encrypt
C. Self-Signed Certificates
D. DNS-Based Certificates

Answer: A
Explanation:

ClearPass Onboard generates and manages its own internal CA, providing secure certificate-based authentication for enrolled devices.

Question: 190

Which network enforcement technique does ClearPass use to isolate non-compliant devices?

A. VLAN Steering
B. DNS Redirection
C. RADIUS Change of Authorization (CoA)
D. SNMP ACLs

Answer: C
Explanation:

RADIUS Change of Authorization (CoA) allows ClearPass to dynamically modify user access based on real-time posture assessment results.

Question: 191

Which ClearPass feature ensures that a device remains compliant after onboarding?

A. Periodic Posture Reassessment
B. Static Role Assignment
C. VLAN Stacking
D. Pre-Shared Keys

Answer: A
Explanation:

Periodic Posture Reassessment continuously evaluates device compliance to ensure that security policies remain enforced throughout the session.

Question: 192

Which technology is commonly used in ClearPass Onboard to distribute unique device credentials?

A. Digital Certificates
B. Pre-Shared Keys
C. MAC Address Filtering
D. RADIUS Proxy

Answer: A
Explanation:

Digital Certificates are provisioned via ClearPass Onboard, enabling secure, identity-based authentication without the need for shared passwords.

Question: 193

Which authentication method is recommended for enterprise device provisioning with ClearPass Onboard?

A. 802.1X with EAP-TLS
B. Captive Portal with MAC Authentication
C. PEAP with MSCHAPv2
D. Open Authentication

Answer: A
Explanation:

EAP-TLS with 802.1X is recommended for enterprise provisioning, providing the highest level of security using certificate-based authentication.

Question: 194

Which ClearPass feature can revoke a device's certificate if it becomes non-compliant?

A. Certificate Revocation List (CRL)
B. VLAN Steering
C. SNMP Polling
D. Static Role Mapping

Answer: A
Explanation:

Certificate Revocation Lists (CRL) allow ClearPass to invalidate previously issued certificates, preventing non-compliant devices from authenticating.

Question: 195

Which two criteria can be used for role assignment in ClearPass Onboard? (Select two.)

A. Device Ownership (BYOD vs. Corporate)
B. User Group Membership
C. Subnet Mask
D. DHCP Lease Duration

Answer: A, B
Explanation:

ClearPass Onboard can assign roles based on device ownership (e.g., BYOD vs. corporate) and user group membership, enforcing different security policies accordingly.

Question: 196

Which encryption protocol does ClearPass Onboard use for secure device communication?

A. TLS
B. FTP
C. SNMPv1
D. Telnet

Answer: A
Explanation:

TLS (Transport Layer Security) encrypts communication between devices and ClearPass Onboard, ensuring secure certificate provisioning and authentication.

Question: 197

Which two enforcement actions can ClearPass take if a device fails a posture check? (Select two.)

A. Assign a remediation VLAN
B. Block network access
C. Modify device MAC address
D. Change device hostname

Answer: A, B
Explanation:

ClearPass can assign a remediation VLAN for security updates or block network access entirely until the device meets compliance standards.

Question: 198

Which ClearPass feature enables guest devices to be onboarded securely?

A. ClearPass Guest with Onboard
B. OnGuard
C. Device Insight
D. SNMP Polling

Answer: A
Explanation:

ClearPass Guest with Onboard allows guest users to securely enroll their devices, ensuring controlled and authenticated network access.

Question: 199

Which ClearPass component integrates with mobile device management (MDM) solutions for compliance enforcement?

A. OnGuard
B. Insight
C. Onboard
D. Policy Manager

Answer: D
Explanation:

Policy Manager integrates with MDM solutions to verify device compliance and enforce access control policies dynamically.

Question: 200

Which two conditions trigger a posture reassessment in ClearPass OnGuard? (Select two.)

A. User logoff and logon
B. Network interface change
C. DNS Query Resolution
D. MAC Address Spoofing

Answer: A, B
Explanation:

Posture reassessment occurs when users log off and log back on or change network interfaces, ensuring continuous compliance checks.

Question: 201

Which component in ClearPass Onboard helps ensure device provisioning is secure?

A. Internal Certificate Authority (CA)
B. Static MAC Address Lists
C. SNMP Authentication
D. VLAN Trunking

Answer: A
Explanation:

The Internal Certificate Authority (CA) in ClearPass Onboard generates and manages unique digital certificates, providing secure authentication for enrolled devices.

Question: 202

Which ClearPass feature ensures that only compliant devices can access the network after onboarding?

A. Posture Assessment with OnGuard
B. VLAN Assignment
C. MAC Address Filtering
D. DNS-Based Filtering

Answer: A
Explanation:

OnGuard continuously assesses the security posture of onboarded devices, enforcing compliance before granting or maintaining network access.

Question: 203

Which two factors can be used to define posture policies in ClearPass? (Select two.)

A. OS Patch Level
B. Antivirus Status
C. User Session Timeout
D. VLAN Assignment

Answer: A, B
Explanation:

Posture policies in ClearPass enforce security compliance based on factors like OS Patch Level and Antivirus Status, ensuring endpoints meet security requirements.

Question: 204

Which method does ClearPass Onboard use to distribute Wi-Fi credentials securely?

A. Digital Certificates
B. Pre-Shared Keys
C. Manual Configuration
D. Static MAC Addressing

Answer: A
Explanation:

Digital Certificates issued through ClearPass Onboard provide secure, identity-based Wi-Fi authentication, eliminating the risks associated with shared passwords.

Question: 205

Which two enforcement actions can ClearPass take if a device becomes non-compliant? (Select two.)

A. Redirect to a remediation page
B. Assign a quarantine VLAN
C. Enable static MAC filtering
D. Change device hostname

Answer: A, B
Explanation:

ClearPass can redirect non-compliant devices to a remediation page or assign them to a quarantine VLAN, restricting access until compliance is restored.

Question: 206

Which authentication protocol does ClearPass Onboard primarily use for device enrollment?

A. EAP-TLS
B. PAP
C. CHAP
D. PEAP-MSCHAPv2

Answer: A
Explanation:

EAP-TLS is the preferred authentication method for ClearPass Onboard, as it leverages digital certificates for strong security without using passwords.

Question: 207

Which ClearPass feature automatically revokes network access for devices that fail posture checks?

A. RADIUS Change of Authorization (CoA)
B. Manual VLAN Reassignment
C. Guest Self-Registration
D. Static Access Control Lists

Answer: A
Explanation:

RADIUS Change of Authorization (CoA) allows ClearPass to dynamically revoke or modify network access when a device fails a posture assessment.

Question: 208

Which enforcement policy in ClearPass ensures that devices remain compliant even after initial onboarding?

A. Continuous Posture Assessment
B. VLAN Trunking
C. Static Firewall Rules
D. Manual Role Mapping

Answer: A
Explanation:

Continuous Posture Assessment ensures that devices remain compliant with security policies throughout their session, triggering enforcement actions if compliance status changes.

Question: 209

Which enforcement action does ClearPass OnGuard take when an endpoint's antivirus is out of date?

A. Restricts network access until antivirus is updated
B. Assigns a static IP address
C. Moves the device to a guest VLAN
D. Disconnects the user session immediately

Answer: A
Explanation:

OnGuard detects outdated antivirus software and can restrict access until the device updates its security software, maintaining a secure network environment.

Question: 210

Which authentication source does ClearPass Onboard use for verifying users before enrolling devices?

A. Active Directory
B. SNMP Server
C. DHCP Server
D. DNS Resolver

Answer: A
Explanation:

Active Directory (AD) is commonly used in ClearPass Onboard to verify user credentials before allowing device enrollment, ensuring secure and authenticated access.

Question: 211

Which ClearPass component is responsible for managing authentication requests?

A. Policy Manager
B. OnGuard
C. Insight
D. Onboard

Answer: A
Explanation:

Policy Manager is the core ClearPass component responsible for handling authentication requests, enforcing policies, and integrating with external identity sources like Active Directory.

Question: 212

Which two authentication protocols does ClearPass support for network access control? (Select two.)

A. EAP-TLS
B. PEAP-MSCHAPv2
C. SNMPv2
D. HTTPS

Answer: A, B
Explanation:

EAP-TLS and PEAP-MSCHAPv2 are commonly used authentication protocols in ClearPass, providing secure user and device authentication over 802.1X.

Question: 213

Which feature allows ClearPass administrators to monitor system health and authentication logs?

A. Insight
B. OnGuard
C. Guest Manager
D. RADIUS Proxy

Answer: A
Explanation:

ClearPass Insight provides reporting, logging, and analytics on system health, authentication trends, and policy enforcement actions for administrators.

Question: 214

Which protocol does ClearPass use to communicate authentication requests to external directories like Active Directory?

A. LDAP
B. SNMP
C. FTP
D. TCP

Answer: A
Explanation:

LDAP (Lightweight Directory Access Protocol) allows ClearPass to query user credentials and attributes from external identity stores like Active Directory.

Question: 215

Which two types of user authentication sources can be configured in ClearPass? (Select two.)

A. Active Directory
B. RADIUS Server
C. DNS Resolver
D. Syslog Server

Answer: A, B
Explanation:

Active Directory and RADIUS Servers are common authentication sources in ClearPass, enabling secure user authentication for network access.

Question: 216

Which feature in ClearPass enables role-based access control for administrative users?

A. Admin Access Control Lists (ACLs)
B. Operator Profiles
C. Role-Based VLAN Assignment
D. SNMP Authentication

Answer: B
Explanation:

Operator Profiles define role-based access control for ClearPass administrators, restricting access to specific features based on assigned privileges.

Question: 217

Which ClearPass component is responsible for system backups and configuration management?

A. Administration UI
B. Insight
C. Cluster Manager
D. Policy Manager

Answer: C
Explanation:

Cluster Manager handles system backups, software updates, and configuration synchronization across multiple ClearPass appliances.

Question: 218

Which logging feature in ClearPass helps troubleshoot failed authentication attempts?

A. Access Tracker
B. Guest Manager C. Event Viewer
D. SNMP Trap Logs

Answer: A
Explanation:

Access Tracker provides detailed logs for authentication requests, including success and failure reasons, aiding in troubleshooting access issues.

Question: 219

Which two factors should be considered when configuring ClearPass server redundancy? (Select two.)

A. High Availability (HA) Clustering
B. Licensing Synchronization
C. SNMP Polling
D. VLAN Trunking

Answer: A, B

Explanation:

High Availability (HA) Clustering ensures failover between ClearPass servers, while Licensing Synchronization prevents disruptions in user authentication services.

Question: 220

Which ClearPass feature allows administrators to assign different privileges to users based on group membership?

A. Role Mapping
B. VLAN Trunking
C. Static IP Assignment
D. SNMP Group Policies

Answer: A

Explanation:

Role Mapping dynamically assigns users to specific roles based on authentication attributes such as Active Directory group membership.

Question: 221

Which command is used to restart ClearPass services from the CLI?

A. service restart all
B. restart clearpass
C. system reboot
D. clearpass -reload

Answer: A

Explanation:

The service restart all command is used in the CLI to restart ClearPass services without rebooting the entire appliance.

Question: 222

Which two authentication methods does ClearPass support for administrator logins? (Select two.)

A. Local User Authentication
B. Active Directory Authentication
C. RADIUS Proxy Authentication
D. SNMP-Based Authentication

Answer: A, B
Explanation:

ClearPass allows local user authentication and Active Directory authentication for administrator logins, enforcing secure access controls for management.

Question: 223

Which feature in ClearPass helps detect configuration changes and logs them for auditing?

A. Configuration Change Tracker
B. Role-Based Logging
C. Insight Access Logs
D. SNMP Configuration

Answer: A
Explanation:

Configuration Change Tracker logs changes made to ClearPass settings, enabling administrators to audit modifications and ensure compliance.

Question: 224

Which database is primarily used in ClearPass for storing authentication logs and system data?

A. PostgreSQL
B. MySQL
C. Oracle DB
D. MongoDB

Answer: A
Explanation:

PostgreSQL is the backend database used by ClearPass to store authentication logs, system configurations, and policy enforcement data.

Question: 225

Which ClearPass feature allows integration with third-party security solutions for policy enforcement?

A. REST APIs
B. Static Access Control Lists
C. DNS-Based Filtering
D. SNMP Polling

Answer: A
Explanation:

ClearPass REST APIs allow integration with third-party security solutions, enabling automated policy enforcement and external system interactions.

Question: 226

Which two features improve ClearPass server performance in high-load environments? (Select two.)

A. Load Balancing
B. Policy Caching C. VLAN Trunking D. SNMP Polling

Answer: A, B
Explanation:

Load Balancing distributes authentication requests across multiple ClearPass servers, while Policy Caching speeds up policy enforcement for frequent requests.

Question: 227

Which encryption standard is used for securing ClearPass administrative access via the web UI?

A. TLS
B. FTP
C. Telnet
D. SNMPv1

Answer: A
Explanation:

TLS (Transport Layer Security) encrypts communications for ClearPass administrative access, preventing unauthorized interception of management data.

Question: 228

Which ClearPass feature prevents unauthorized changes to system configurations?

A. Role-Based Access Control (RBAC)
B. Guest Self-Registration
C. VLAN Assignment Policies
D. DNS Blacklisting

Answer: A
Explanation:

Role-Based Access Control (RBAC) ensures only authorized administrators can modify system settings, preventing unauthorized changes to ClearPass configurations.

Question: 229

Which method ensures system updates do not disrupt authentication services in ClearPass clusters?

A. Rolling Upgrades
B. Manual System Reboots
C. Disabling High Availability (HA)
D. VLAN Steering

Answer: A
Explanation:

Rolling Upgrades allow ClearPass updates to be applied incrementally across cluster nodes, ensuring continuous authentication services without downtime.

Question: 230

Which best practice should be followed for securing ClearPass administrative access?

A. Enforcing Multi-Factor Authentication (MFA)
B. Allowing open Telnet connections
C. Using a default password for all admin accounts
D. Disabling HTTPS access

Answer: A
Explanation:

Enforcing Multi-Factor Authentication (MFA) adds an extra security layer for administrative access, reducing the risk of unauthorized logins.

Which ClearPass feature allows administrators to track and analyze authentication events?

Question: 231

Which two backup methods are supported in ClearPass for configuration recovery? (Select two.)

A. Manual Backup via Web UI
B. Automated Scheduled Backups
C. FTP Backup Sync
D. Telnet Backup

Answer: A, B
Explanation:

ClearPass supports manual backups via the web UI and automated scheduled backups, ensuring administrators can restore system configurations when needed.

Question: 232

Which command is used to check system health status in the ClearPass CLI?

A. system health
B. show system-status
C. check-server-status
D. health monitor

Answer: B
Explanation:

show system-status provides detailed health metrics, including CPU, memory usage, and database status, allowing administrators to monitor system performance.

Question: 233

Which protocol is used for external log forwarding from ClearPass to SIEM systems?

A. Syslog
B. SNMP
C. LDAP
D. FTP

Answer: A
Explanation:

Syslog is commonly used for log forwarding from ClearPass to external SIEM systems, enabling centralized log analysis and security monitoring.

Question: 234

Which two methods can be used to update ClearPass software versions? (Select two.)

A. Web UI Software Update
B. CLI-Based Upgrade
C. SNMP Firmware Push
D. Manual File Copy via SCP

Answer: A, B

Explanation:

ClearPass supports software updates via the web UI and CLI-based upgrades, ensuring administrators can apply patches and new versions securely.

Question: 235

Which ClearPass feature allows administrators to generate reports on authentication trends?

A. Insight Reporting
B. Configuration Change Tracker
C. Syslog Event Monitoring
D. SNMP Alerts

Answer: A

Explanation:

ClearPass Insight Reporting provides authentication trends, failed login attempts, and policy enforcement summaries, helping administrators analyze network access patterns.

Question: 236

Which service must be running on ClearPass for authentication requests to be processed?

A. Policy Service
B. NTP Service
C. SNMP Service
D. DHCP Server

Answer: A

Explanation:

Policy Service is the core authentication engine in ClearPass, responsible for evaluating access policies and processing authentication requests.

Question: 237

Which two authentication sources can ClearPass integrate with for user verification? (Select two.)

A. Microsoft Active Directory
B. Google LDAP
C. SNMP Traps
D. DNS Server

Answer: A, B

Explanation:

ClearPass integrates with Active Directory and Google LDAP, enabling organizations to use centralized authentication sources for user verification.

Question: 238

Which feature ensures ClearPass services continue running if one server fails in a cluster?

A. High Availability (HA)
B. Static Role Assignments
C. SNMP Polling
D. VLAN Trunking

Answer: A

Explanation:

High Availability (HA) ensures redundancy by enabling failover between ClearPass servers, maintaining continuous authentication services.

Question: 239

Which feature in ClearPass prevents unauthorized modifications to policy settings?

A. Operator Profiles
B. Role-Based VLAN Assignment
C. SNMP Configuration Control
D. Static IP Addressing

Answer: A

Explanation:

Operator Profiles enforce role-based access control for administrators, restricting who can modify policy settings to enhance security.

Question: 240

Which command is used to reboot a ClearPass appliance from the CLI?

A. system reboot
B. restart clearpass
C. shutdown -r now
D. reboot system

Answer: A
Explanation:

The system reboot command safely restarts the ClearPass appliance, ensuring services are properly stopped and restarted.

Question: 241

Which two ClearPass features provide proactive system monitoring? (Select two.)

A. System Health Alerts
B. Access Tracker Logging
C. VLAN Assignment Policies
D. SNMP Traps

Answer: A, D
Explanation:

System Health Alerts notify administrators of potential system issues, while SNMP Traps enable integration with external monitoring tools for proactive health checks.

Question: 242

Which database optimization technique improves ClearPass performance?

A. Indexing Logs
B. Increasing RADIUS Timeouts
C. Disabling Syslog Forwarding
D. VLAN Tagging

Answer: A
Explanation:

Indexing logs improves ClearPass database performance by speeding up search and query operations, reducing authentication latency.

Question: 243

Which feature in ClearPass enables automated responses to security incidents?

A. Adaptive Policy Enforcement
B. Guest Self-Registration
C. SNMP ACLs
D. Manual Role Mapping

Answer: A
Explanation:

Adaptive Policy Enforcement dynamically adjusts access policies in response to security threats, automating incident response for enhanced security.

Question: 244

Which feature in ClearPass allows integration with external multi-factor authentication (MFA) providers?

A. RADIUS Proxy
B. DHCP Relay
C. VLAN Steering
D. SNMPv2

Answer: A
Explanation:

RADIUS Proxy enables ClearPass to integrate with external MFA providers, enhancing authentication security with additional verification steps.

Question: 245

Which two factors should be monitored to maintain ClearPass system health? (Select two.)

A. CPU Utilization
B. Disk Space Usage
C. VLAN ID Assignment
D. IP Address Range

Answer: A, B
Explanation:

CPU utilization and disk space usage should be monitored to ensure ClearPass operates efficiently, preventing performance bottlenecks and service disruptions.

Question: 246

Which feature in ClearPass enables real-time synchronization between multiple servers?

A. Cluster Synchronization
B. VLAN Trunking
C. SNMP Polling
D. Static Role Assignments

Answer: A
Explanation:

Cluster Synchronization ensures configuration consistency across multiple ClearPass servers, allowing real-time replication of policies and authentication settings.

Question: 247

Which best practice should be followed when assigning administrative roles in ClearPass?

A. Using the principle of least privilege
B. Assigning all users full administrator rights
C. Disabling role-based access control
D. Allowing password sharing between administrators

Answer: A
Explanation:

The principle of least privilege ensures administrators only have the minimum access required for their tasks, reducing security risks.

Question: 248

Which feature in ClearPass allows automatic detection of configuration issues?

A. Configuration Validation
B. Static Policy Enforcement
C. VLAN ID Assignment
D. DNS-Based Routing

Answer: A
Explanation:

Configuration Validation detects misconfigurations in ClearPass settings, helping administrators identify and resolve issues proactively.

Question: 249

Which ClearPass feature enables secure backup storage?

A. Encrypted Backup Files
B. Guest Self-Registration
C. VLAN Spanning Tree
D. DNS Forwarding

Answer: A

Explanation:

Encrypted Backup Files protect ClearPass configuration backups, ensuring sensitive system data remains secure during storage and restoration.