

HP.HPE6-A88.v2026-06-20.q62

Exam Code:	HPE6-A88
Exam Name:	HPE Aruba Networking ClearPass Exam
Certification Provider:	HP
Free Question Number:	62
Version:	v2026-06-20
# of views:	103
# of Questions views:	620
https://www.freecram.net/torrent/HP.HPE6-A88.v2026-06-20.q62.html	

NEW QUESTION: 1

An IT administrator attempts to join a ClearPass server to an Active Directory domain. They notice that the system clocks of the ClearPass server and the AD domain are not in sync. The ClearPass server is 10 minutes behind the AD domain. As a best practice, what should the administrator do?

- A. The administrator should manually set the ClearPass server clock to match the AD domain.
- B. The administrator should sync the ClearPass server and the AD domain to the same time source.
- C. The administrator should proceed with the join.

Answer: (SHOW ANSWER)

Active Directory authentication relies on Kerberos, which is highly sensitive to time differences. Synchronizing both the ClearPass server and the Active Directory domain to the same reliable time source ensures proper Kerberos operation and prevents authentication and domain join failures.

NEW QUESTION: 2

An IT administrator is setting up a captive portal for a company's network and needs to ensure that the SSL certificate is compatible with the Aruba Instant device they are using. Which type of certificate should the administrator install to meet this requirement?

- A. CER certificate
- B. PEM certificate
- C. DER certificate

Answer: B (LEAVE A REPLY)

The PEM certificate format is required for Aruba Instant devices when configuring SSL on a captive portal. PEM files contain the base64-encoded certificate and private key, making them compatible with Aruba devices for secure HTTPS communication during guest authentication.

NEW QUESTION: 3

An IT administrator is configuring ClearPass to send guest receipts for registrations. They want to ensure that guests receive these receipts through both email and SMS simultaneously. What steps should the administrator follow to achieve this configuration?

- A. Configure both the email relay and SMS gateway in the Messaging Setup menu.
- B. Navigate to Administration > External Servers > Guest Setup to configure messaging.
- C. Use the REST API to manually send emails and SMS messages.

Answer: A ([LEAVE A REPLY](#))

To send guest receipts via both email and SMS, the administrator must configure the email relay and SMS gateway in the Messaging Setup menu. This enables ClearPass Guest to deliver registration notifications through multiple communication channels simultaneously.

NEW QUESTION: 4

Which of the following is an example of a ClearPass Authorization Rule?

- A. Allowing a device based on its MAC address
- B. Assigning a specific IP address to a device
- C. Blocking access to specific websites
- D. Configuring routing protocols for a network

Answer: (SHOW ANSWER)

Authorization rules in ClearPass are used to control access to the network, based on different criteria, such as MAC addresses, user roles, or device types.

NEW QUESTION: 5

A network administrator wants to ensure that users see their company's logo when accessing the guest network. They have already uploaded the logo as a JPEG file into the Content Manager. What is the next step they should take to display this logo on the custom web pages?

- A. Enable public access for the uploaded logo file.
- B. Apply a skin that includes the uploaded logo to the web pages.
- C. Edit the ClearPass Guest configuration to include the logo in the default template.

Answer: B ([LEAVE A REPLY](#))

After uploading the company logo to the Content Manager, the administrator must apply a skin that includes the uploaded logo to the guest web pages. Skins define the visual appearance of ClearPass Guest portals, and applying one with the logo ensures the branding appears consistently across all guest-facing pages.

NEW QUESTION: 6

A company implements a drop-down list of valid sponsors for their guest network access. What is a significant advantage of this approach?

- A. It reduces the number of required fields in the registration form.
- B. It allows guests to bypass email verification.
- C. It simplifies the sponsor selection process for the guest user.

Answer: ([SHOW ANSWER](#))

Providing a drop-down list of valid sponsors simplifies the sponsor selection process by allowing guests to choose from predefined, authorized sponsors. This reduces user errors, ensures sponsor validity, and streamlines the guest registration workflow.

NEW QUESTION: 7

A network administrator needs to revoke a certificate for a lost device to ensure it no longer has network access. They navigate to the Certificate Authorities section in ClearPass Onboard. What next step should they take to ensure the certificate is properly revoked and the device is blocked?

- A.** Select the certificate authority, edit the retention policy to store only metadata, and then revoke the certificate.
- B.** Select the certificate authority, view the issued certificates, and revoke the specific certificate associated with the lost device.
- C.** Select the certificate authority, view the trust chain, and manually revoke the certificate from the list.

Answer: ([SHOW ANSWER](#))

The administrator should select the certificate authority, view the issued certificates, and revoke the specific certificate associated with the lost device. This action immediately invalidates the certificate, ensuring that the lost device can no longer authenticate or gain access to the network.

NEW QUESTION: 8

What is the purpose of ClearPass Onboard?

- A.** To manage guest access to the network
- B.** To provide automatic device configuration and security
- C.** To monitor network traffic
- D.** To configure Aruba switches

Answer: **B** ([LEAVE A REPLY](#))

ClearPass Onboard enables automatic configuration and provisioning of devices, including security settings like certificates, for secure network access.

NEW QUESTION: 9

A network administrator is setting up ClearPass for a large organization and needs to ensure that user credentials are validated efficiently while also gathering rich context about the users. Which authentication source should the administrator prioritize to meet the need?

- A.** Active Directory
- B.** SQL Servers
- C.** Internal Database

Answer: ([SHOW ANSWER](#))

Active Directory should be prioritized because it allows ClearPass to efficiently validate user credentials and retrieve rich contextual information such as group membership, organizational

roles, and user attributes. This enhances both authentication accuracy and policy-based access control.

NEW QUESTION: 10

Which ClearPass feature enables administrators to create custom policies for specific users or devices?

- A. Role Mapping
- B. Policy Manager
- C. Device Profiling
- D. Access Control Lists (ACLs)

Answer: ([SHOW ANSWER](#))

The ClearPass Policy Manager allows administrators to create customized policies for specific users, devices, and groups.

NEW QUESTION: 11

A network engineer is reviewing the policy cache tab for an endpoint in the Identity: Endpoints Database. They notice the cache was updated three minutes ago. What can the engineer conclude about the current status of the endpoint's role or posture token?

- A. The endpoint's role or posture token has expired and needs to be reassigned immediately.
- B. The policy cache will not expire until the endpoint is disconnected from the network.
- C. The endpoint's role or posture token is still valid and will be updated if necessary within the next two minutes.

Answer: ([SHOW ANSWER](#))

A recent policy cache update indicates that the endpoint's role or posture token is still within its validity period. ClearPass will continue to treat the cached decision as valid and will refresh or update it as needed when the cache lifetime is reached.

NEW QUESTION: 12

An IT administrator needs to configure multiple profile collectors to gather endpoint context data for a diverse network. What is the primary benefit of using ClearPass for this task?

- A. It helps manage devices and their security levels by profiling client devices when they connect to the network.
- B. It automatically blocks non-corporate devices.
- C. It provides a single security policy for all devices.

Answer: ([SHOW ANSWER](#))

ClearPass allows the use of multiple profile collectors to gather endpoint context data, enabling device profiling as clients connect to the network. This helps administrators identify device types, manage their security posture, and apply appropriate network access policies based on profiling results.

NEW QUESTION: 13

A network engineer is tasked with creating enforcement profiles for a multi-vendor environment.

They want to minimize the number of enforcement profiles they need to write. Which approach should the engineer take?

- A. Enable SNMP services on all network devices.
- B. Utilize IETF attributes instead of vendor-specific attributes.
- C. Write separate enforcement profiles for each device vendor type.

Answer: B ([LEAVE A REPLY](#))

Using IETF-standard RADIUS attributes allows enforcement profiles to be applied consistently across different network device vendors. This avoids reliance on vendor-specific attributes and significantly reduces the number of enforcement profiles required in a multi-vendor environment.

NEW QUESTION: 14

An IT administrator is configuring a Web-Based Health Check service in ClearPass to enforce posture compliance for client endpoints. They need to ensure that the service can handle requests from various operating systems and networks. Which step should the administrator take to ensure the posture policy is applied correctly to the agent's System Health Validator report?

- A. Select the Posture Compliance option to add the Posture tab to the service.
- B. Configure the service without specifying the operating system for the agent.
- C. Assign multiple Posture Policies to the same client endpoint.

Answer: ([SHOW ANSWER](#)**)**

Selecting the Posture Compliance option enables the Posture tab within the service configuration. This allows ClearPass to evaluate the System Health Validator report generated by the web-based agent and correctly apply the defined posture policy across different operating systems and network environments.

NEW QUESTION: 15

When managing network access through ClearPass, an administrator notices that client status changes are causing repeated disconnections and re-authentications. The administrator wants to prevent the service from making the same enforcement decision without considering newly gathered information. What action should the administrator take?

- A. Enable automatic endpoint reconciliation.
- B. Increase the timeout period for client re-authentication.
- C. Select the option 'Use Cached Results' on the enforcement tab.

Answer: ([SHOW ANSWER](#)**)**

Enabling automatic endpoint reconciliation ensures that ClearPass updates endpoint attributes dynamically as new information is gathered. This prevents repeated disconnections and redundant enforcement decisions by allowing ClearPass to adapt to the latest endpoint context without reapplying identical policies unnecessarily.

NEW QUESTION: 16

To enhance the guest login experience, an administrator is configuring the Pre-Authentication Check on an Aruba controller. Where should the administrator edit these settings?

- A. In the network policies section of the controller.
- B. In the Login Form section of the web login page editor.
- C. In the certificate management section of the controller interface.

Answer: ([SHOW ANSWER](#))

Pre-Authentication Check behavior is controlled within the web login page configuration. Editing the Login Form section allows the administrator to define checks and logic that occur before credentials are submitted, improving the guest login experience.

Valid HPE6-A88 Dumps shared by EduDump.com for Helping Passing HPE6-A88 Exam! EduDump.com now offer the **newest HPE6-A88 exam dumps**, the EduDump.com HPE6-A88 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com HPE6-A88 dumps with Test Engine here:

<https://www.edudump.com/exams/HP/HPE6-A88/premium/> (**114 Q&As Dumps, 35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 17

A company uses ClearPass with Active Directory as both the authentication and authorization source. What is the advantage of this setup?

- A. It allows for both credential validation and account attribute retrieval.
- B. It simplifies the network topology by eliminating external servers.
- C. It ensures that only internal devices can access the network.

Answer: ([SHOW ANSWER](#))

Using Active Directory for both authentication and authorization allows ClearPass to validate user credentials and simultaneously retrieve directory attributes such as group membership. This enables consistent, attribute-based policy decisions without requiring a separate identity source.

NEW QUESTION: 18

A network administrator notices that a client device leaves the network and returns after ten minutes. Upon reconnecting, the device's posture token is unknown. What is the most likely reason for this behavior?

- A. The agent failed to send any updates to ClearPass during the ten-minute period.
- B. The posture token expired due to inactivity beyond the five-minute threshold.
- C. The endpoint profile information was permanently deleted from ClearPass.

Answer: ([SHOW ANSWER](#))

Posture tokens in ClearPass are time-bound and expire after a defined inactivity period. If the client disconnects longer than the allowed validity window, the token expires and is no longer recognized when the device reconnects, resulting in an unknown posture state.

NEW QUESTION: 19

An IT administrator is configuring ClearPass to authenticate users in a large organization. They set the Base DN to the OU containing user accounts but noticed that computer accounts are not authenticated. What could be the reason for this issue?

- A. The password for the service account has expired.
- B. The ClearPass account does not have write access to the directory.
- C. The Base DN is too narrow, excluding the OU with computer accounts.

Answer: C ([LEAVE A REPLY](#))

If the Base DN is set only to the OU containing user accounts, ClearPass will not search other OUs - such as those containing computer accounts - during authentication. Expanding the Base DN to a higher-level directory path that includes both user and computer OUs ensures all relevant objects are accessible for authentication.

NEW QUESTION: 20

A company's IT department is tasked with ensuring data replication across multiple ClearPass servers while maintaining redundancy and failover capabilities. They need to perform license management operations for the cluster. Where should these license management operations be performed to ensure they are properly applied across the cluster?

- A. On the server with the active Insights database
- B. On the publisher
- C. On a dedicated license server

Answer: ([SHOW ANSWER](#)**)**

In a ClearPass cluster, all license management operations must be performed on the publisher server. The publisher centrally manages configurations, licenses, and synchronization across all subscribers, ensuring consistent licensing and cluster functionality.

NEW QUESTION: 21

A security analyst is reviewing a ClearPass configuration and notices that the system is set to gather device location information from network device attributes. Which attribute is likely being used to gather this information?

- A. SSID
- B. Client-Domain-Name
- C. Network device attribute settings

Answer: ([SHOW ANSWER](#)**)**

ClearPass can derive device location context from attributes learned from the network access device, such as switch, port, AP name, or controller information. These network device attribute settings provide location awareness without relying on client-side information.

NEW QUESTION: 22

A network engineer is configuring a policy enforcement service on a wired network to minimize deployment effort. They choose a non-AAA enforcement method. What is the main benefit of this approach?

A. It does not require client configuration and requires minimal configuration on the actual switches.

B. It enables advanced security protocols such as 802.1X.

C. It allows dynamic VLAN assignment based on user roles.

Answer: ([SHOW ANSWER](#))

Non-AAA enforcement methods rely on network-side controls rather than client-based authentication mechanisms. This approach minimizes deployment effort because endpoints do not need to be configured and only minimal configuration is required on the switches to enforce access control.

NEW QUESTION: 23

An IT administrator is setting up a captive portal for a company's network and needs to ensure that the SSL certificate is compatible with the Aruba Instant device they are using. Which type of certificate should the administrator install to meet this requirement?

A. CER certificate

B. DER certificate

C. PEM certificate

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 24

An IT administrator is configuring ClearPass for a secure network. They have enabled the OCSP authentication method and are now deciding whether to enable the 'Override OCSP URL from Client' option. What will ClearPass do if the 'Enable' option is unchecked and the certificate includes an OCSP URL?

A. ClearPass will use the OCSP URL from the authentication method.

B. ClearPass will use the OCSP URL included in the certificate.

C. ClearPass will prompt the user for a valid OCSP URL.

Answer: ([SHOW ANSWER](#))

When the option to override the OCSP URL from the client is not enabled, ClearPass relies on the OCSP responder information embedded in the certificate itself. If the certificate includes an OCSP URL, ClearPass uses that URL to perform the certificate status validation.

NEW QUESTION: 25

A company is setting up a custom Enforcement Profile for operator logins in ClearPass. They decide to copy an existing operator login profile and modify the value of the admin_privileges attribute. What additional step must they take to properly assign this custom profile to the users?

A. Create a new role in the Admin User Repository and link it to the custom profile.

B. Create an application enforcement policy and modify the rules to include the new custom profile.

C. Assign the custom profile directly to users in the Local User Repository.

Answer: **A** ([LEAVE A REPLY](#))

Operator access and privileges in ClearPass are controlled through roles defined in the Admin User Repository. After creating a custom operator login enforcement profile, it must be linked to a new or existing admin role so that users assigned to that role receive the defined administrative privileges.

NEW QUESTION: 26

An IT administrator is setting up a network for a multinational company with multiple sites. They need to ensure that requests to different Active Directory servers are properly filtered. How should the administrator configure the network to meet this need?

- A.** Create multiple Network Device Groups and filter requests by belongs to group.
- B.** Rely on the default settings of the Active Directory servers for request filtering.
- C.** Use a single Network Device Group for all sites and filter requests by IP address.

Answer: ([SHOW ANSWER](#))

The administrator should create multiple Network Device Groups and configure ClearPass to filter requests using the "belongs to group" condition. This setup ensures that authentication requests from each site are directed to the correct Active Directory server, maintaining proper segmentation and efficient authentication handling across multiple locations.

NEW QUESTION: 27

An IT administrator is tasked with creating a self-service portal for guest users to request and maintain their own user identities. Which type of web page should they create using ClearPass Guest's Web Content Manager?

- A.** Web Logins
- B.** Self-Registrations
- C.** Web Pages

Answer: ([SHOW ANSWER](#))

Self-Registration pages allow guest users to create, manage, and maintain their own user identities through a self-service portal. ClearPass Guest's Web Content Manager provides this page type specifically for guest-driven account creation and lifecycle management.

NEW QUESTION: 28

A company wants to prevent corporate devices from accessing the guest network. They configure a ClearPass Entity Update Enforcement action to tag devices as corporate clients. What happens when a tagged device attempts to access the guest network?

- A.** The enforcement action is ignored, and the device accesses the guest network.
- B.** The guest access service reads the attribute and denies access to the guest network.
- C.** The corporate client is redirected to a different network.

Answer: ([SHOW ANSWER](#))

The ClearPass Entity Update Enforcement action adds an attribute that identifies the device as a corporate client. When the device attempts to use the guest network, the guest access service

evaluates this attribute during service selection and enforcement, and access is denied based on the service policy.

NEW QUESTION: 29

A security analyst needs to ensure that ClearPass sends a notification whenever a report is ready. They want to receive these notifications via SMS. What is the correct procedure to set this up?

- A. Set up an email relay and configure it to forward the emails as SMS messages.
- B. Configure the SMS Gateway under ClearPass Guest and ensure report notifications are enabled in Insight.
- C. Enable SMS notifications in the Administration > External Servers > Messaging Setup menu.

Answer: ([SHOW ANSWER](#))

ClearPass uses the SMS Gateway configuration within ClearPass Guest to send SMS messages. By configuring the SMS Gateway and enabling SMS notifications for reports in Insight, ClearPass can automatically notify the analyst via SMS when a report is ready.

NEW QUESTION: 30

When configuring a new custom Operator Profile in ClearPass, an administrator needs to ensure that the system properly assigns this profile to users based on their roles. What critical step must be taken to meet this need?

- A. Modify the Local User Repository to directly assign the custom profile to each user.
- B. Include the operator account's role evaluation in the enforcement policy to select the new custom Operator Profile.
- C. Edit the built-in Guest Operator Login policy to include the new custom profile.

Answer: ([SHOW ANSWER](#))

To ensure a new custom Operator Profile is properly assigned, the administrator must edit the built-in Guest Operator Login policy to include the new profile. This policy determines which operator profile applies based on user roles during login, enabling ClearPass to map the correct administrative permissions dynamically.

NEW QUESTION: 31

A network engineer is troubleshooting an issue where a factory default Aruba Network device is not redirecting DNS requests correctly. The device is supposed to intercept requests for 'securelogin.hpe.com' but is failing to do so. What is a likely cause of this issue?

- A. The device's IP address is not correctly configured in the ClearPass Guest settings.
- B. The common name in the HTTPS certificate does not match 'securelogin.hpe.com'.
- C. The Page Name for the web login page is missing from the URL.

Answer: ([SHOW ANSWER](#))

Aruba devices performing DNS-based captive portal redirection rely on the HTTPS certificate common name to match the intercepted hostname. If the certificate common name does not

match securelogin.hpe.com, the device cannot correctly intercept and redirect DNS requests to the captive portal.

Valid HPE6-A88 Dumps shared by EduDump.com for Helping Passing HPE6-A88 Exam!
EduDump.com now offer the **newest HPE6-A88 exam dumps**, the EduDump.com HPE6-A88 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com HPE6-A88 dumps with Test Engine here:

<https://www.edudump.com/exams/HP/HPE6-A88/premium/> (114 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 32

A company wants to prevent corporate devices from accessing the guest network. They configure a ClearPass Entity Update Enforcement action to tag devices as corporate clients. What happens when a tagged device attempts to access the guest network?

- A. The enforcement action is ignored, and the device accesses the guest network.
- B. The corporate client is redirected to a different network.
- C. The guest access service reads the attribute and denies access to the guest network.

Answer: ([**SHOW ANSWER**](#)**)**

NEW QUESTION: 33

An IT manager needs to ensure that a report generated using the Remote Copy option is automatically saved to a specific file location on the network without logging into Insight. What must they configure in the administration settings?

- A. Read/write permissions for Insight subsections
- B. Insight tab read/write/delete options
- C. Hostname or IP address, port number, SCP or SFTP, and user credentials

Answer: ([**SHOW ANSWER**](#)**)**

To enable automatic report saving through the Remote Copy option, the IT manager must configure the hostname or IP address, port number, transfer protocol (SCP or SFTP), and user credentials. These settings allow ClearPass Insight to securely transfer generated reports to the designated network location without requiring manual login.

NEW QUESTION: 34

A network administrator is configuring a corporate network enforcement policy. The policy includes rules for corporate-issued laptops, MDM-enabled tablets, and personal smart devices. However, the administrator notices that some clients are failing all rules due to a lack of profile data. What should the administrator do to ensure these unprofiled clients can access the profiler collectors and receive a profile using best practices?

- A. Add a rule that identifies clients without profiles and assigns them a role allowing limited access to the profiler.
- B. Increase the frequency of profile data updates from the endpoint profiler.
- C. Set the default enforcement profile to 'Allow Access' for all unprofiled clients.

Answer: ([SHOW ANSWER](#))

The best practice is to add a rule that detects unprofiled clients and assigns them a limited-access role that permits communication with the profiler collectors. This approach allows ClearPass to gather profiling data securely while preventing unverified devices from gaining unrestricted network access.

NEW QUESTION: 35

An IT administrator notices that a client endpoint has failed a health check and wants to send a notification that will not only inform the user but also force the client to re-authenticate. Which action should the administrator take?

- A. Send a message to disable the network interface.
- B. Send a notification to disable the network interface.
- C. Send a notification with an action to restart the session.

Answer: ([SHOW ANSWER](#))

The administrator should send a notification with an action to restart the session. This forces the client to re-authenticate after failing a health check, allowing ClearPass to reassess the device's compliance status and apply the appropriate enforcement policy based on the updated posture.

NEW QUESTION: 36

Which ClearPass feature helps manage guest access by providing self-registration?

- A. ClearPass Onboard
- B. ClearPass Guest
- C. ClearPass Profiler
- D. ClearPass Policy Manager

Answer: ([SHOW ANSWER](#))

ClearPass Guest helps organizations manage guest access, including self-registration for visitors to obtain network access.

NEW QUESTION: 37

An IT specialist is tasked with ensuring that guests receive their login credentials via SMS after completing the self-registration process. What configuration must be checked to guarantee that this feature is enabled?

- A. The network must disable email notifications to enable SMS notifications.
- B. ClearPass must be configured to send the guest account information via SMS.
- C. The guest's browser must support SMS messaging.

Answer: ([SHOW ANSWER](#))

ClearPass Guest must be configured with an SMS delivery option so that guest account credentials are sent via SMS after self-registration. This requires proper SMS gateway integration and enabling SMS as a credential delivery method within the guest workflow.

NEW QUESTION: 38

Which ClearPass component is responsible for performing device profiling?

- A. ClearPass Policy Manager
- B. ClearPass Onboard
- C. ClearPass Profiler
- D. ClearPass Guest

Answer: ([SHOW ANSWER](#))

ClearPass Profiler is used to identify and classify devices connected to the network based on various characteristics, such as device type, operating system, and other identifiers.

NEW QUESTION: 39

What is the main risk associated with evaluating posture in role mappings instead of enforcement rules?

- A. Potential conflicts between role mappings and enforcement rules.
- B. Increased processing time for posture evaluation.
- C. Evaluating against cached attributes instead of the most current attributes.

Answer: ([SHOW ANSWER](#))

When posture is evaluated in role mappings, ClearPass uses cached posture attributes rather than the most current ones. This can result in outdated or inaccurate posture assessments, leading to improper access decisions. Evaluating posture in enforcement rules ensures the system uses real-time attribute data.

NEW QUESTION: 40

An IT administrator is setting up ClearPass servers for a new network environment. They need to ensure that the RADIUS authentication will work seamlessly across all servers in the cluster. What crucial step must they take regarding the certificates?

- A. Share a single RadSec certificate across all servers
- B. Install a single certificate on the publisher server only
- C. Install certificates individually on every ClearPass server

Answer: ([SHOW ANSWER](#))

Each ClearPass server in a cluster terminates RADIUS and TLS connections independently. To ensure consistent and seamless RADIUS authentication across the cluster, valid certificates must be installed on every ClearPass server so that all nodes can securely handle authentication requests.

NEW QUESTION: 41

What is the primary function of Aruba ClearPass?

- A. Manage network switches
- B. Authenticate network devices and users
- C. Monitor network performance
- D. Optimize network throughput

Answer: ([SHOW ANSWER](#))

Aruba ClearPass is primarily used for network access control, allowing organizations to authenticate, authorize, and enforce policies for users and devices connecting to the network.

NEW QUESTION: 42

Which of the following is NOT a typical role of ClearPass in a network?

- A. Device authentication
- B. Network intrusion detection
- C. Policy enforcement
- D. Guest access management

Answer: ([SHOW ANSWER](#))

While ClearPass plays a crucial role in authentication, policy enforcement, and guest access management, it does not directly function as a network intrusion detection system (IDS).

NEW QUESTION: 43

A company needs to add a new field to an existing form and wants it to appear before a specific field already on the form. What is the correct sequence of actions to meet this need?

- A. Select the existing field in the forms editor and choose the 'Insert Before' option.
- B. Use the Customize Form Field workspace to drag and drop the new field before the existing one.
- C. Select the existing field in the forms editor and choose the 'Insert After' option.

Answer: ([SHOW ANSWER](#))

To insert a new field before an existing one in a ClearPass form, the administrator must select the existing field in the form editor and choose the 'Insert Before' option. This ensures the new field is positioned correctly in the desired order without disrupting the rest of the form layout.

NEW QUESTION: 44

What is the role of the ClearPass Policy Manager when used in conjunction with Aruba wireless access points?

- A. To manage user IP addresses
- B. To define access policies for wireless clients
- C. To configure SSID settings
- D. To manage security updates

Answer: ([SHOW ANSWER](#))

ClearPass Policy Manager integrates with Aruba wireless access points to define and enforce policies for wireless clients.

NEW QUESTION: 45

An IT manager is organizing files for upload to ClearPass Guest and wants to ensure they are easily identifiable later. What is the best practice they should follow before uploading the files?

- A. Upload the files first and then rename them within ClearPass Guest.
- B. Name the files logically in advance, as the system will use the filename for the file identity.
- C. Use the description field to identify the files rather than focusing on the filenames.

Answer: ([SHOW ANSWER](#))

The best practice is to name the files logically before uploading them, as ClearPass Guest uses the filename as the file's identity. Clear and descriptive filenames make it easier to locate and manage files later within the system.

NEW QUESTION: 46

What is the main purpose of the ClearPass Policy Manager?

- A. To provide a centralized point for policy enforcement
- B. To configure Aruba wireless access points
- C. To manage user traffic on the network
- D. To optimize the routing protocols in the network

Answer: ([SHOW ANSWER](#))

ClearPass Policy Manager allows administrators to create and enforce policies regarding user and device access to the network.

Valid HPE6-A88 Dumps shared by EduDump.com for Helping Passing HPE6-A88 Exam!

EduDump.com now offer the **newest HPE6-A88 exam dumps**, the EduDump.com HPE6-A88 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com HPE6-A88 dumps with Test Engine here:

<https://www.edudump.com/exams/HP/HPE6-A88/premium/> (114 Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 47

In a network utilizing ClearPass and RADIUS CoA, a client initially connects without profile data and is assigned limited access. How does ClearPass ensure that the client eventually gains full access?

- A. ClearPass uses the initial connection data to grant full access without further profiling.
- B. ClearPass profiles the client after receiving a DHCP request, terminates the session, and allows the client to re-authenticate with full access.
- C. ClearPass immediately grants full access upon receiving the DHCP request without terminating the session.

Answer: ([SHOW ANSWER](#))

ClearPass passively profiles the client after observing network activity such as a DHCP request.

Once sufficient profile data is collected, ClearPass sends a RADIUS Change of Authorization to terminate the existing session, forcing the client to re-authenticate so the updated profile can be evaluated and full access granted based on the new enforcement decision.

NEW QUESTION: 48

A network engineer is installing a new HTTPS certificate on a ClearPass server to replace the built-in self-signed certificate. They want to ensure the certificate is trusted and properly installed. What critical step must they remember to avoid installation issues?

- A. Install the certificate without specifying the subject alternative names
- B. Include the entire certificate bundle with root CA and intermediate CA trusts
- C. Only install the certificate for the publisher

Answer: ([SHOW ANSWER](#))

ClearPass requires the full certificate trust chain to validate and present the HTTPS certificate correctly. Including the server certificate along with all intermediate and root CA certificates ensures trust is established and prevents browser and service validation errors.

NEW QUESTION: 49

In Aruba ClearPass, what is a "role mapping" used for?

- A. To assign a user role based on device attributes
- B. To configure network switches
- C. To provide encryption for network traffic
- D. To determine the IP address range for users

Answer: A ([LEAVE A REPLY](#))

Role mappings are used to assign roles to users or devices based on their attributes. This helps to enforce network policies for different types of users and devices.

NEW QUESTION: 50

An organization wants to ensure that all devices accessing their network meet specific security criteria. They decide to use ClearPass OnGuard to monitor and enforce compliance. During the deployment, the IT team needs to understand how ClearPass evaluates the security status of clients. Which aspect of ClearPass OnGuard provides this functionality?

- A. Network access control
- B. Health Checks
- C. Security policies

Answer: ([SHOW ANSWER](#))

Health Checks in ClearPass OnGuard are responsible for evaluating the security status of client devices. They assess factors such as antivirus status, firewall settings, OS updates, and other compliance parameters to determine whether a device meets the organization's security requirements before granting full network access.

NEW QUESTION: 51

An IT specialist is trying to create a reliable profile for a new endpoint device using ClearPass. They want to ensure the profiling is as accurate as possible. What approach should they take?

- A. Interface multiple profiling collectors between the client device and ClearPass.
- B. Only the HTTP network function is used to detect device fingerprints.
- C. Rely solely on the DHCP network function for profiling.

Answer: ([SHOW ANSWER](#))

Using multiple profiling collectors allows ClearPass to gather a wider range of device characteristics and behaviors from different network interaction points. Correlating data from several collectors significantly improves profiling accuracy and reliability for new endpoint device types.

NEW QUESTION: 52

An organization wants to enforce role-based access policies across their entire network to ensure that users have appropriate access privileges regardless of their connection point. How does ClearPass facilitate this requirement?

- A. By providing detailed audit logs of all network activity
- B. By offering customizable user authentication methods
- C. By allowing the creation of individual user roles with associated privileges that applies anywhere on the network

Answer: ([SHOW ANSWER](#))

ClearPass enables role-based access control (RBAC) by allowing administrators to create individual user roles with defined privileges that are enforced consistently across wired, wireless, and VPN connections. This ensures that users maintain the same level of network access regardless of where or how they connect.

NEW QUESTION: 53

A facility manager is concerned about the security of their network after discovering that an attacker could potentially replace a wired IP camera with a laptop using the same MAC address. How does the ClearPass profiler mitigate this risk?

- A. By creating separate networks for each type of device to prevent unauthorized access.
- B. The network can distinguish between the camera and a spoofed device by comprehensively profiling the real client device type.
- C. By automatically blocking any device that attempts to connect with a MAC address already in use.

Answer: ([SHOW ANSWER](#))

ClearPass Profiler uses multiple device characteristics beyond the MAC address, such as DHCP fingerprinting, traffic behavior, and protocol usage, to accurately identify the true device type. This comprehensive profiling allows the network to distinguish a legitimate IP camera from a spoofed device attempting to use the same MAC address.

NEW QUESTION: 54

An IT administrator is setting up a new service in their company's configuration system. After selecting a service type and filling in the name and description, they need to modify the service selection rules.

They want to ensure that non-compliant end hosts are automatically remediated.

Which step should they take next?

- A. Select the Audit End-hosts check box and choose to perform an audit always.
- B. Select the Add new Posture Server link and configure a new server.
- C. Select the Posture Compliance check box, enable auto-remediation, and enter the Remediation URL.

Answer: ([SHOW ANSWER](#))

Enabling posture compliance with auto-remediation allows ClearPass to automatically trigger remediation actions for non-compliant end hosts. Configuring the remediation URL ensures affected devices are redirected to the appropriate remediation resources without manual intervention.

NEW QUESTION: 55

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

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

Answer: ([SHOW ANSWER](#))

ClearPass uses RADIUS (Remote Authentication Dial-In User Service) for authentication, authorization, and accounting in network access control.

NEW QUESTION: 56

An employee needs to access the office network using their company laptop, but the administrator wants to limit network access on the employee's personal tablet and smartphone. How can the administrator meet this need using ClearPass with little manual administrative work?

- A. Creating a service that includes role mapping and enforcement policies specific to the employee's devices.
- B. By using MAC address filtering to restrict access to the employee's personal devices.
- C. By configuring the employee's devices to use a guest network.

Answer: ([SHOW ANSWER](#))

ClearPass can dynamically evaluate user identity and device attributes to assign roles and apply enforcement policies per device type. This allows full access for the employee's company laptop while automatically limiting access on personal devices, without requiring ongoing manual administration.

NEW QUESTION: 57

An IT administrator needs to quickly identify all devices connected to a specific subnet within their network. They decide to use the search feature to find all IP addresses within the 10.0.0.0/8 subnet. Which search term should they use?

- A. 10.0.0.0/16
- B. 10.
- C. 10.0.0

Answer: B ([LEAVE A REPLY](#))

Using a partial IP string search allows ClearPass to match all addresses that begin with the specified value. Entering 10. matches all IP addresses within the 10.0.0.0/8 subnet, enabling quick identification of all connected devices in that range.

NEW QUESTION: 58

An IT administrator attempts to join a ClearPass server to an Active Directory domain. They notice that the system clocks of the ClearPass server and the AD domain are not in sync. The ClearPass server is 10 minutes behind the AD domain. What will be the likely outcome of this attempt to join the domain?

- A. The join will succeed but ClearPass will generate a warning about the clock skew.
- B. The join will succeed because ClearPass automatically adjusts the clock skew during the join process.
- C. The join will fail because Active Directory only allows a maximum of five minutes of clock skew.

Answer: ([SHOW ANSWER](#)**)**

The domain join will fail because Active Directory enforces a maximum allowable clock skew of five minutes between systems for Kerberos authentication. Since the ClearPass server is 10 minutes behind, the Kerberos ticket validation will fail, preventing the join operation.

NEW QUESTION: 59

A company is deploying new Cisco switches and wants to use SNMP enforcement for VLAN assignments. What requirement must be met for SNMP enforcement to work correctly in this scenario?

- A. Downloadable enforcement must be enabled for all devices.
- B. Vendor-specific attributes must be used for enforcement.
- C. SNMP services must be enabled on the Cisco switches.

Answer: ([SHOW ANSWER](#)**)**

For SNMP enforcement to function properly, SNMP services must be enabled on the Cisco switches. This allows ClearPass to communicate with the switches and dynamically apply VLAN assignments or other enforcement actions based on authentication and policy decisions.

NEW QUESTION: 60

In a scenario where the OSCP server replies with an 'unknown' status, what action will ClearPass take regarding the certificate-based authentication?

- A. ClearPass will retry the OSCP request.

- B. ClearPass will accept the authentication but log a warning.
- C. ClearPass will reject the authentication.

Answer: (SHOW ANSWER)

If the OSCP responder returns an unknown status, ClearPass cannot confirm the revocation state of the certificate. Because certificate validity cannot be reliably established, ClearPass rejects the authentication to maintain security.

NEW QUESTION: 61

A guest user has their registration receipt open in their browser when their sponsor approves their account. What then happens to the Log In button?

- A. The Log In button remains grayed out.
- B. The Log In button becomes active.
- C. The Log In button disappears.

Answer: (SHOW ANSWER)

When the sponsor approves the guest account, ClearPass dynamically updates the registration receipt. As a result, the Log In button becomes active, allowing the guest to immediately proceed with authentication without refreshing or restarting the registration process.

Valid HPE6-A88 Dumps shared by EduDump.com for Helping Passing HPE6-A88 Exam!

EduDump.com now offer the **newest HPE6-A88 exam dumps**, the EduDump.com HPE6-A88 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com HPE6-A88 dumps with Test Engine here:

<https://www.edudump.com/exams/HP/HPE6-A88/premium/> (114 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 62

A company has installed a wildcard certificate with the common name '*.mycompany.com' on their Aruba gateway. What must be configured on the web login page to ensure credential posts are directed to the correct gateway?

- A. The address should be set to 'login.mycompany.com'.
- B. The DNS resolution should be set to the controller's IP address directly.
- C. The address should be set to 'captiveportal-login.mycompany.com'.

Answer: (SHOW ANSWER)

When a wildcard certificate such as *.mycompany.com is used on the Aruba gateway, the web login page must post credentials to a hostname that matches the certificate. Configuring the address as login.mycompany.com ensures the hostname aligns with the wildcard certificate and directs authentication requests to the correct gateway securely.

Valid HPE6-A88 Dumps shared by EduDump.com for Helping Passing HPE6-A88 Exam!

EduDump.com now offer the **newest HPE6-A88 exam dumps**, the EduDump.com HPE6-A88 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com HPE6-A88 dumps with Test Engine here:

<https://www.edudump.com/exams/HP/HPE6-A88/premium/> (**114** Q&As Dumps, **35%OFF**

Special Discount Code: freecram)