

HP.HPE6-A81.v2022-07-01.q20

試験コード : HPE6-A81
試験名称 : Aruba Certified ClearPass Expert Written Exam
認証ベンダー : HP
無料問題の数 : 20
バージョン : v2022-07-01
ページの閲覧量 : 333
問題集の閲覧量 : 1506

<https://www.jpnsiken.com/shiken/HP.HPE6-A81.v2022-07-01.q20.html>

質問: 1

お客様は19.940IoTデバイスをネットワークに接続しており、[すべてのMac認証を許可]を使用してユーザーを認証し、デバイスの指紋の詳細で定義された条件に基づいてアクションを実行したいと考えています。デバイスのアクセスを決定するためにどの認証ソースを使用しますか？

- A. クリアパスプロファイラーデータベース
- B. ゲストデバイスデータベース
- C. エンドポイントデータベース
- D. ローカルユーザーデータベース

正解: ([正解を表示します](#))

質問: 2

ある顧客が、独自のActiveDirectoryインフラストラクチャを持つ別の会社を買収しました。802 1X PEAP認証は、お客様の元のActive Directoryサーバーで機能しますが、お客様は、買収した会社のユーザーも認証したいと考えています。

この要求をサポートするには、認証ソースに関してどのような手順が必要ですか？ 2つ選択してください。)

- A. 新しい認証ソースを作成します。GenericLDAP」と入力します。
- B. ClearPassサーバーを新しいADドメインに参加させます。
- C. 新しい認証ソースを作成し、ActiveDirectoryと入力します。
- D. ClearPassを新しいADドメインに参加させる必要はありません。
- E. 新しいADサーバーをバックアップとして既存の認証ソースに追加します。

正解: ([正解を表示します](#))

質問: 3

サービスルール条件を構成する際に、有線認証と無線認証のサービスを区別するためにどのNAS-Port-Type値を使用する必要がありますか？

- A. イーサネット 0)およびWireless-802 11 1)
- B. イーサネット 19)およびワイヤレス-80211 18)
- C. イーサネット 5)およびワイヤレス-80211 9)

D. イーサネット 15)およびワイヤレス-80211 19)

正解: ([正解を表示します](#))

質問: 4

顧客は、グループポリシーの結果を使用してOnGuard Agtntsをプッシュすることにより、すべての企業デバイスにOnGuardソリューションを展開しました。ネットワーク管理者は、エージェントの相馬がDMZにあるClearPassサーバーと通信していると不満を言っています。ファイアウォールの外側ネットワーク管理者は、すべてのエージェントのシステムヘルス検証トラフィックが管理サブネット内にとどまるようにします。

ClearPass管理者は、トラフィックをClearPass管理ポートにのみ移動するために何ができますか？

- A.** ファイアウォールでTCPポート6658をフィルタリングし、OnGuardエージェントにClearPass管理ポートの使用を強制します。
- B.** クライアントにデプロイされているagent.confファイルを編集して、SHVの更新にClearPass管理ポートを使用します
- C.** 正しいOnGuard Agentインストーラーを選択し、クライアントの管理ポート用に構成されたインストーラーを使用します。
- D.** OnGuardエージェントが管理ポートIPを使用するようにポリシーマネージャーゾーンマッピングを構成します。

正解: **A** ([コメントを発表する](#))

質問: 5

CPPMのGuestself-registrationに利用規約ページを追加するには、どのような構成手順に従う必要がありますか？ 2つ選択してください)。

- A.** 領収書ページのcreatoraccepttermsフォームフィールドを編集し、アップロードされたHTMLファイルへのハイパーリンクをポイントしてHTMLセクションを変更します
- B.** カスタムの契約条件を使用してHTMLページを作成し、ClearpassGuest->構成->コンテンツマネージャーの下のパブリックファイルにアップロードします
- C.** 領収書ページのaccept_termsフォームフィールドを編集し、ゲストマネージャーにアップロードされたHTMLファイルへのハイパーリンクをポイントしてHTMLセクションを変更します
- D.** カスタムの契約条件を使用してHTMLページを作成し、ClearpassGuest->構成->コンテンツマネージャーの下プライベートファイルにアップロードします
- E.** 登録ページのcreetoraccepitermsフォームフィールドを編集し、アップロードされたHTMLファイルへのハイパーリンクをポイントしてHTMLセクションを変更します

正解: **A,B** ([コメントを発表する](#))

質問: 6

複数のArubaNetworksモビリティコントローラーを使用している顧客向けに、ゲスト機能を備えたCleat PassPolicyManagerを導入します。お客様は、ゲストアクセス中のSSLエラーを回避した

いと考えていますが、会社のセキュリティポリシーにより、ClearPassまたはコントローラーでワイルドカード証明書を使用することはできません。

顧客のゲストソリューションを構成するための最も効率的な方法は何ですか？ 2つ選択してください。)

- A. コントローラー（会社のドメイン）のベンダー設定を使用して1つのWebログインページを作成します
- B. 各コントローラーに異なる共通名を持つ複数の公開証明書をインストールします
- C. 各コントローラーにベンダー設定を構成して複数のWebログインページを作成します
- D. captiveportal-controller（会社のドメイン）のベンダー設定を使用して1つのWebログインページを作成します
- E. 共通名「controller.{companydomain}」のすべてのコントローラーに同じ公開証明書をインストールします

正解: ([正解を表示します](#))

質問: 7

展示を参照してください。





お客様が新しいClearPassのインストールを行っており、6.8.6バージョンを実行している2台のClearPassサーバー間にクラスタリングを設定しています。ClearPassサーバーはサブスクライバーノードの追加に失敗しました。顧客は、クラスタのセットアップ時に使用したのと同じCLIパスワードを使用してClearPassサーバーのコンソールにログインできました。顧客からサポートを求めるスクリーンショットが送信されました。サブスクライバーノードを追加しようとして失敗し、そのエラーが表示されなかったのはなぜですか。

A. パブリッシャーサーバーで使用されるデフォルトのデータベース証明書は有効な証明書ではありません

- B. サブスクリायバーのデータと時刻がNTPサーバーと同期されていませんでした
 - C. サブスクリायバーサーバーは、公開署名および信頼されたHTTPS証明書を使用して実行されています
 - D. サブスクリायバサーバーはデフォルトの自己署名HTTPS証明書で実行されています
- 正解: ([正解を表示します](#))

質問: 8

お客様は、OnGuardクライアントアクティビティのトラブルシューティングを行っており、[ライブモニタリング]->[OnGuardアクティビティ]セクションを調べています。このクライアントを表すステータスフィールドは何ですか？



- A. クライアントは正常にプロファイリングされました
 - B. クライアントのヘルスステータスはHEALTHYです
 - C. クライアントは正常に認証されました
 - D. クライアントはオンラインであり、キープアライブメッセージを送信します
- 正解: A ([コメントを發表する](#))

質問: 9

顧客は、これから作成されるすべての新しいページの「テンプレート」として使用したいゲスト自己登録ページを作成しました。彼らの目標は、すべてのページのヘッダーとフッターが同じであり、それらに加えられた編集がすべての自己登録ページに自動的に反映されるようにすることです。

この要求を実行するには、何を構成する必要がありますか？

- A. 「テンプレート」ページをマスター自己登録ページとして保存します。
- B. 新しい自己登録ページを作成するときに子ページを作成し、親として「テンプレート」を選択します。
- C. この「テンプレート」ページを新しいスキンとして保存して、他の自己登録ページで使用するようにします。
- D. 「テンプレート」ページをコピーして、新しい自己登録ページが必要になるたびに編集します。

正解: ([正解を表示します](#))

質問: 10

展示を参照してください。

Please login to the network using your username and password.

To create a new account click [Create Account](#).

Login

Username:
Invalid username or password

Password:

Terms: ☒ I accept the terms of use

Log In

Contact a staff member if you are experiencing difficulty logging in.

Contact a staff member if you are experiencing difficulty logging in.

Request Details

Summary | Input | Output | Alerts

Login Status:	REJECT
Session Identifier:	W00000000-01-5d88e82b
Date and Time:	Sep 23, 2019 11:43:40 EDT
End-Host Identifier:	-
Username:	accx@exam.com
Access Device IP/Port:	-/-
System Posture Status:	-

Policies Used -

Service:	-
Authentication Method:	Not applicable
Authentication Source:	-
Authorization Source:	-
Roles:	-
Enforcement Profiles:	-
Service Monitor Mode:	-
Online Status:	Not Available

Showing 1 of 1-16 records »

[Show Configuration](#) [Export](#) [Show Logs](#) [Close](#)

Request Details

Summary Input Output **Alerts**

Error Code: 204
 Error Category: Authentication failure
 Error Message: Failed to classify request to service

Alerts for this Request

WebAuthService: ServiceClassification failed (No service matched)

Configuration > Services > Edit - ACCX Guest Access

Services - ACCX Guest Access

Summary **Service** Authentication Rules Enforcement

Service:

Name: ACCX Guest Access
 Description: To authenticate guest users logging in via captive portal. Guests must re-authenticate after their session ends.
 Type: RADIUS Enforcement (Generic)
 Status: Enabled
 Monitor Mode: Disabled
 More Options: -

Service Rule

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	Calling-Station-Id	EXISTS	
2. Connection	Client-Mac-Address	NOT_EQUALS	%(Radius:IETF:User-Name)
3. Radius:Aruba	Aruba-Essid-Name	EQUALS	guest-labtest

Authentication:

Authentication Methods: 1. [PAP]
 2. [MSCHAP]
 3. [CHAP]
 Authentication Sources: [Guest User Repository]
 Strip Username Rules: -
 Service Certificate: -

Roles:

Role Mapping Policy: [Guest Roles]

Enforcement:

Use Cached Results: Disabled
 Enforcement Policy: Accx Guest Access Enforcement Policy

Home > Configuration > Pages > Web Logins

Web Login (ACCX_LabTest)

Use this form to make changes to the Web Login ACCX_LabTest.

Use this form to make changes to the Web Login **ACCX_LabTest**.

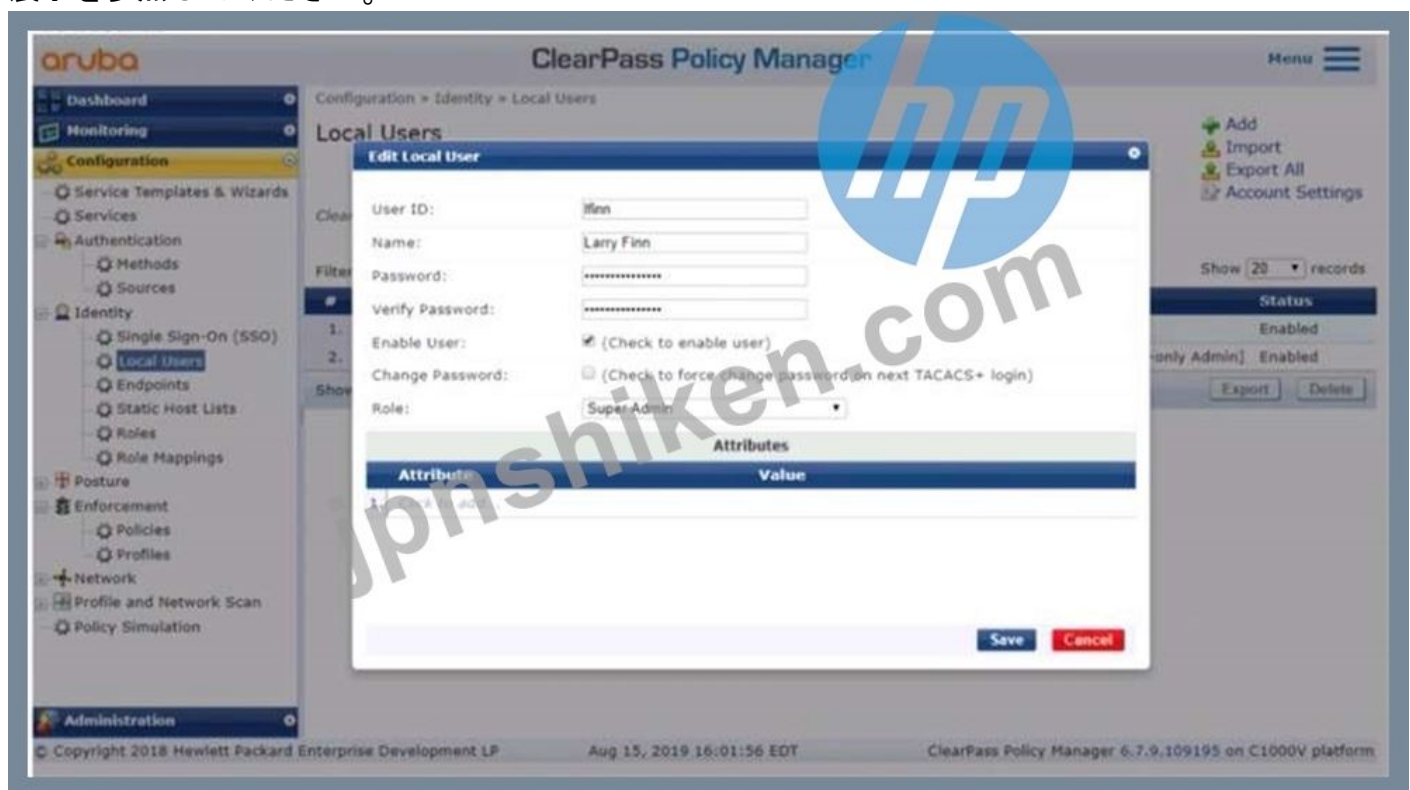
一年前。お客様は、IAPクラスターでホストされているゲストSSID用にAruba ClearPass Policy Managerサーバーを展開しました。お客様は、以前のWebログインページが新しいWebログインページでテストに失敗し、お客様から上記のスクリーンショットが転送されました。

問題を解決するためにお客様にどのような推奨事項を提供しますか？

- A. 顧客は、ゲスト管理アカウントを使用して、ユーザー名accxCdlexam.comのパスワードをリセットする必要があります。
 - B. 設定されているサービスタイプが正しくありません。ゲスト認証は、アプリケーション認証タイプのサービスである必要があります。
 - C. WebLoginPre-AuthCheckがArubaApplicationAuthenticationに設定されているため、ポリシーマネージャーで個別のアプリケーションサービスが必要です。
 - D. WebLoginベンダー設定でファイルされたアドレスが正しく構成されていません。インスタントに設定する必要があります、Aruba Networks com、
- 正解: ([正解を表示します](#))

質問: 11

展示を参照してください。



表示されたユーザーが、[Policy Manager Admin NetworkLoginService]を使用して管理者のClearPassサーバーにログインできないとお客さんから苦情がありました。この理由は何でしょうか？

- A. 作成されたアカウントはこの目的に適合しません。
 - B. ユーザーはTACACS認証に使用される可能性があります。
 - C. ローカルユーザー認証が無効になっている可能性があります。
 - D. 役割のマッピングを[RADIUSスーパー管理者]に変更する必要があります
- 正解: ([正解を表示します](#))

質問: 12

Arubaのダウンロード可能なユーザーロールについて正しい説明はどれですか？ 3つ選択してください

- A. Arubaのダウンロード可能なユーザーロールは、ClearPassに組み込まれている施行テンプレートです。
- B. Arubaのダウンロード可能なユーザーロールは、環境全体で広く利用できます。
- C. ClearPassによって認証されたポートまたはWLANユーザーにのみ適用できます。
- D. これらの結果は、ClearPassを含まない他の認証方法に使用できます。
- E. 大企業では、ダウンロード可能なユーザーロールの管理が難しい場合があります。
- F. ダウンロード可能なロール名はArubaスイッチまたはコントローラーで定義する必要があります。

正解: ([正解を表示します](#))

質問: 13

Allow All MAC AUTHを使用しているのはどれですか？どの認証ソースをサービスにマップする必要がありますか？

- A. 静的ホストリスト
- B. 任意の認証ソース
- C. ゲストデバイスデータベース
- D. エンドポイントデータベース

正解: A ([コメントを發表する](#))

質問: 14

お客様には次の要件があります。

*MAC認証を使用する2.000IoTエンドポイント

*ユーザー名/パスワードと証明書（企業BYOD）ベースの認証を組み合わせる使用する6.000エンドポイント

*ゲストの自己登録を使用するピーク使用時の1.000ゲストエンドポイント

*ユーザーあたり3デバイスと推定される1500BYODデバイス \$500ユーザー)

* OnGuardがインストールされ、毎日接続されている2.500エンドポイント顧客の要件を満たすには、どのライセンスをインストールする必要がありますか？

- A. 9.000アクセス。500オンボード。2.500 OnGuard
- B. 11.500アクセス。500オンボード。2.500 OnGuard
- C. 11.500アクセス。1.500オンボード。2.500 OnGuard
- D. 13.000アクセス。1.500オンボード。2.500 OnGuard

正解: ([正解を表示します](#))

質問: 15

お客様は、HOJの場所から「マネージャー」の称号を持つADユーザーのみに個人用デバイスのオンボードを許可したいと考えています。他のADユーザーは、最初のデバイスプロビジョニングページを超えて通過することを許可されるべきではありません。この要件を実装するためにどのオンボードサービスを使用しますか？

- A. オンボードCPログインサービス

- B. オンボード認証サービス
- C. オンボードプロビジョニングサービス
- D. オンボード事前認証サービス

正解: ([正解を表示します](#))

質問: 16

1つのサイトに2台のサーバーが配置されている企業のClearPassクラスターには、管理ポートとデータポートの両方のIPアドレスが構成されています。管理ポートIPはDataCenterネットワークサブネットにあり、データポートIPはDMZにあります。AAAトラフィックに1つの仮想IPを使用することと、各サーバーの物理IPにAAA要求を送信することの違いは何ですか？ 2つ選択してください。

- A. 1つの仮想IPを個々のサーバーIPと一緒に使用して、負荷分散を行うことができます。
- B. フェイルオーバーは仮想IPを使用することによってのみ達成できます
- C. 仮想IPを使用することにより、フェイルオーバーの待機時間は、個々のサーバーIPを使用するよりも速くなります。
- D. 個々のIPは、フェイルオーバーと負荷分散を提供できます。
- E. 1つの仮想IPを使用すると、フェイルオーバーを提供できます。

正解: ([正解を表示します](#))

有効的な**HPE6-A81**問題集はJPNTest.com提供され、**HPE6-A81**試験に合格することに役に立ちます！JPNTest.comは今最新**HPE6-A81**試験問題集を提供します。JPNTest.com HPE6-A81試験問題集はもう更新されました。ここで**HPE6-A81**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/HPE6-A81-mondaishu> **60問、30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 17

展示を参照してください。

Configuration > Services > Edit > HS-Guest MAC Authentication

Services - HS-Guest User Authentication with MAC Caching

Summary Service Authentication Authorization Roles Enforcement

Service:

Name: HS-Guest User Authentication with MAC Caching

Description: Captive Portal authentication with MAC Caching

Type: RADIUS Enforcement (Generic)

Status: Enabled

Monitor Mode: Disabled

More Options: Authorization

Service Rule

Match ANY of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	Calling-Station-Id	EXISTS	
2. Connection	Client-Mac-Address	NOT_EQUALS	%{Radius:IETF:User-Name}
3. Radius:Aruba	Aruba-Essid-Name	BELONGS_TO	guest-HS-5007,Instantguest-HS-5007

Authentication:

Authentication Methods: 1. [PAP]
2. [MSCHAP]
3. [CHAP]

Authentication Sources: [Guest User Repository]

Strip Username Rules: -

Service Certificate: -

Authorization:

Authorization Details: 1. [Endpoints Repository]
2. [Time Source]

Roles:

Role Mapping Policy: HS-Guest User Authentication with MAC Caching Role Mapping

Enforcement:

Use Cached Results: Disabled

Enforcement Policy: HS-Guest User Authentication with MAC Caching Enforcement Policy

ArubaControllerと統合されたArubaClearPassとInstantAccessPoint Guest Mac Caching機能を使用してACCX試験準備用のホームラボをセットアップしました。ArubaControllerのゲストSSIDに対してのみ構成され、共通のWebログインページが両方のNADデバイスに対して構成されています。クライアントをArubaControllerのゲストSSIDに接続して、クライアントのMacキャッシュ機能を確認しました。

クライアントをArubaControllerのゲストSSIDから切断し、Instant APのゲストSSIDに接続するとどうなりますか？

- A. クライアントはキャプティブポータルページにリダイレクトされ、Web認証を完了します。
- B. クライアントは、MAC認証を完了することにより、キャプティブポータル認証をバイパスします。
- C. クライアントはMac認証に失敗し、キャプティブポータルページにリダイレクトされます。
- D. 再接続がすぐに行われたため、クライアントは認証を完了する必要はありません。

正解: B ([コメントを发表する](#))

質問: 18

展示を参照してください。

Configuration > Services > Edit > HPE-Aruba Wired Mac auth

Services - HPE-Aruba Wired Mac auth

Summary Service Authentication Authorization Roles Enforcement Profiles

Services:

Name: HPE-Aruba Wired Mac auth
Description: MAC-based Authentication Service
Type: MAC Authentication
Status: Enabled
Monitor Mode: Disabled
More Options: 1. Authorization
2. Profile Endpoints

Service Rule

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet(15)
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)
3. Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
4. Radius:IETF	NAS-IP-Address	BELONGS_TO_GROUP	HPE-Aruba Switches

Authentication:

Authentication Methods: [Allow All MAC AUTH]
Authentication Sources: [Local User Repository]
Strip Username Rules: -

Authorization:

Authorization Details: [Endpoints Repository]

Roles:

Role Mapping Policy: HS_Building Role Mapping Policy

Enforcements:

Use Cached Results: Disabled
Enforcement Policy: HPE-ArubaOS Mac auth policy

Profiles:

Endpoint Classification: ANY
RADIUS CoA Action: [ArubaOS Switching - Bounce Switch Port]

Back to Services

Disable Copy Save Cancel

Configuration > Services > Edit > HS_Building Aruba 802.1x service

Services - HS_Building Aruba 802.1x service

Summary Service Authentication Authorization Roles Enforcement Profiles

Role Mapping Policy: HS_Building Role Mapping Policy Modify Add New Role Mapping Policy

Role Mapping Policy Details

Description:
Default Role: [Other]
Rules Evaluation Algorithm: first-applicable

Conditions	Role
1. (Connection:Client-Mac-Address BELONGS_TO_GROUP VIP User MAC)	VIP User
2. (Authorization:Corp SQL:MAC EXISTS)	Corp SQL Tablet
3. (Authorization:[Endpoints Repository]:Category EQUALS VoIP Phone)	IP Phone
4. (Authorization:[Endpoints Repository]:Category EQUALS SmartDevice)	Personal SmartDevice
5. (Authorization:[Endpoints Repository]:Category EQUALS Point of Sale devices)	Vending Machine
6. AND (Authorization:[Endpoints Repository]:Category EQUALS Printer) AND (Authorization:[Endpoints Repository]:MAC Vendor EQUALS CANON)	Printer
7. AND (Authorization:[Endpoints Repository]:Category EQUALS Network Camera) AND (Authorization:[Endpoints Repository]:MAC Vendor EQUALS Axis Communications AB)	IP Camera

Configuration > Services > Edit > HPE-Aruba Wired Mac auth



エンドポイントプロファイリングデータを使用して有線MAC認証サービスの実施条件を設定しました。mac認証ベースのクライアントがネットワークに接続すると、ClearPassは拒否アクセスプロファイルを割り当てます。お客様から上記のスクリーンショットが送信されました。問題をどのように解決しますか？

- A. TypeとoperatorをAuthorization [Endpoint Repository] :Category NOT_EXISTSとして、DHCPサービスのみを許可する制限付きアクセスプロファイルとしてアクションを使用して、最初の位置に新しい条件を作成します。
- B. TypeとoperatorをTips :Role EQUALS [User Authenticated]として、すべてのサービスとポートにプロファイリングを許可するアクセスプロファイルを許可するアクションを使用して、最後の位置に新しい条件を作成します。
- C. HPE ArubaOS Mac認証ポリシーの施行ポリシーのルール評価アルゴリズムを「すべての一致を選択」に変更し、プロファイラタブのHPEバウンススイッチポートとしてCoAアクションを追加します。
- D. タイプと演算子を承認として、最初の位置に新しい条件を作成します[エンドポイントリポジトリ]カテゴリNOT_EXISTS、アクションを制限付きアクセスプロファイルとして、ArubaOSワイヤレス終了セッション

正解: [\(正解を表示します\)](#)

質問: 19

Secure SSIO（別名シングルSSID）OnBoardデプロイメントサービスワークフローとは何ですか？

- A. RADIUSサービスのプロビジョニング。オンボードの事前認証RADIUSサービス。オンボード認証アプリケーションサービス。オンボードプロビジョニングRADIUSサービス。
- B. オンボード認証RADIUSサービス。オンボード事前認証アプリケーションサービス。オンボードプロビジョニングRADIUSサービス。オンボードプロビジョニングRADIUSサービス。オンボードPrt-Authアプリケーションサービス。

- C. オンボードプロビジョニングRADIUSサービス、オンボード認証アプリケーションサービス、オンボード事前認証アプリケーションサービス。オンボードプロビジョニングRADIUSサービス
オンボードプロビジョニングRADIUSサービス、
- D. オンボード認証アプリケーションサービス。オンボードプロビジョニングRADIUSサービス
オンボード

正解: ([正解を表示します](#))

質問: 20

お客様は、1台のArubaコントローラーと1台のClearPassサーバーを使用してインフラストラクチャにマシンとユーザーの認証を実装することを計画しています。このソリューションを設計する際に、顧客は何を考慮する必要がありますか？ 3つ選択してください。）

- A. Aruba Controllerはマシンの状態をキャッシュしないため、お客様はマルチマスターキャッシュの存続可能性を有効にする必要があります。
- B. ユーザーとマシンの認証を行うには、オンボードを使用して個人用デバイスに証明書をインストールする必要があります。
- C. ClearPassサーバーのマルチマスターキャッシュに24時間書き込まれたマシン認証ステータスrs
- D. マシン認証はEAPTLSのみを使用します。そのため、マシン認証用にPKIインフラストラクチャを導入する必要があります。
- E. コントローラーはマシンの状態もキャッシュするため、お客様はマルチマスターキャッシュの存続可能性について心配する必要はありません。
- F. Windowsユーザーはログオフする必要があります。キャッシュの有効期限が切れる前に、マシンを再起動または切断して、マシン認証を開始します。

正解: ([正解を表示します](#))

有効的なHPE6-A81問題集はJPNTTest.com提供され、HPE6-A81試験に合格することに役に立ちます！JPNTTest.comは今最新HPE6-A81試験問題集を提供します。JPNTTest.com HPE6-A81試験問題集はもう更新されました。ここでHPE6-A81問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/HPE6-A81-mondaishu> 60問、30%ディスカウント、特別な割引コード: **JPNshiken**」