

KTest

更に上のクオリティ 更に上のサービス



問題集

<http://www.ktest.jp>

1年で無料進級することに提供する

Exam : **210-260**

Title : Implementing Cisco
Network Security

Version : DEMO

1. クラウドネットワークを定義する 2 つのサービスはどれですか？（2 つを選択してください）

- A. サービスとしてのインフラ
- B. サービスとしてのプラットフォーム
- C. サービスとしてのセキュリティ
- D. サービスとしての計算
- E. サービスとしてのテナント

Answer: A,B

Explanation:

NIST のクラウドコンピューティングの定義では、サービスモデルを[2] + サービスとしてのソフトウェア（SaaS）と定義しています。コンシューマに提供される機能は、クラウドインフラストラクチャ上で実行されているプロバイダのアプリケーションを使用することです。アプリケーションは、ウェブブラウザ（例えば、ウェブベースの電子メール）のようなシンクライアントインタフェースまたはプログラムインタフェースを介して、様々なクライアントデバイスからアクセス可能である。ユーザーは、ネットワーク、サーバー、オペレーティングシステム、ストレージ、さらには個別のアプリケーション機能など、基盤となるクラウドインフラストラクチャを管理または制御することはできませんが、ユーザー固有のアプリケーション構成の設定は限られています。

+ サービスとしてのプラットフォーム（PaaS）。コンシューマに提供される機能は、プロバイダがサポートするプログラミング言語、ライブラリ、サービス、およびツールを使用して作成されたコンシューマが作成または取得したクラウドインフラストラクチャに展開することです。コンシューマは、ネットワーク、サーバー、オペレーティングシステム、ストレージなどの基盤となるクラウドインフラストラクチャを管理または制御することはありませんが、展開されたアプリケーションやアプリケーションホスト環境の構成設定を制御します。

+ サービスとしてのインフラストラクチャ（IaaS）。消費者に提供される機能は、消費者がオペレーティングシステムおよびアプリケーションを含む任意のソフトウェアを展開して実行できる、処理、ストレージ、ネットワーク、およびその他の基本的なコンピューティングリソースを提供することである。コンシューマは、基盤となるクラウドインフラストラクチャを管理または制御するのではなく、オペレーティングシステム、ストレージ、および展開されたアプリケーションを制御します。（例えば、ホストファイアウォール）の制御が制限される可能性がある。

Source: https://en.wikipedia.org/wiki/Cloud_computing#Service_models

2. アウトオブバンド管理を使用する 2 つの状況はどれですか？（2 つを選択してください）

- A. ネットワークデバイスがパケットを転送できない場合
- B. ROMMON アクセスが必要なとき
- C. 管理アプリケーションがデバイスに同時にアクセスする必要がある場合
- D. 複数の場所からの管理者アクセスが必要な場合
- E. コントロールプレーンが応答しないとき

Answer: A,B

Explanation:

OOB 管理は、本社のデバイスで使用され、デバイス上の専用管理ポートまたは予備イーサネットポートを、管理および監視アプリケーションおよびサービスをホストする専用の OOB 管理ネットワークに直接接続することによって実行されます。OOB 管理ネットワークは、専用ハードウェアの集合として実装することも、VLAN 分離に基づいて実装することもできます。

Source:

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg/chap9.html

3. TACACS プロトコルと RADIUS の 3 つの方法は異なりますか。 (3 つ選択してください)

- A. TACACS は TCP を使用して NAS と通信します。
- B. TACACS は、NAS に送信されるパケット全体を暗号化できます。
- C. TACACS はコマンド単位の認可をサポートします。
- D. TACACS は同時に認証と承認を行い、送信するパケットの数を減らします。
- E. TACACS は UDP を使用して NAS と通信します。
- F. TACACS は、認証パケット内のパスワードフィールドのみを暗号化します。

Answer: A,B,C

4. シスコのベストプラクティスによれば、有線 BYOD デバイスが有効なクレデンシャルを供給してネットワークに接続できるようにするために、アクセスポートでデフォルトの ACL が許可する 3 つのプロトコルはどれですか? (3 つ選択してください)

- A. BOOTP
- B. TFTP
- C. DNS
- D. MAB
- E. HTTP
- F. 802.1x

Answer: A,B,C

Explanation:

ACL は、キャンパス内の有線デバイスのアクセスレイヤスイッチでポリシーの施行が行われる主要な方法です。

ACL-DEFAULT - この ACL はアクセスレイヤスイッチ上で設定され、ポート上のデフォルト ACL として使用されます。その目的は、許可されていないアクセスを防ぐことです。

キャンパスアクセスレイヤスイッチのデフォルト ACL の例を以下に示します。

拡張 IP アクセスリスト ACL-DEFAULT

```
10 許可 udp 任意の eq bootpc 任意の eq bootps ログ(2604 マッチ)20 許可 udp 任意のホスト 10.230.1.45 eq ドメイン
```

30 は ICMP を許可します

40 は任意の eq tftp を udp に許可します

すべてのログを拒否した場合は 50 回 (40 回)

上の出力からわかるように、ACL-DEFAULT は DHCP、DNS、ICMP、および TFTP トラフィックを許可し、その他すべてを拒否します。

出典: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_Wired.html

MAB はシスコが提供するアクセス制御技術であり、MAC 認証バイパスと呼ばれています。

5. シスコで推奨される次の 2 つの暗号化アルゴリズムはどれですか? (2 つを選択してください)

- A. AES
- B. 3DES
- C. DES
- D. MD5
- E. DH-1024

F.HAA-384

Answer: A,F

Explanation:

Suite B の次世代暗号化（**NGE**）には、認証された暗号化、デジタル署名、鍵の確立、および暗号化ハッシュアルゴリズムが含まれています。

+楕円曲線暗号（**ECC**）は、動作のガロア/カウンタモード（**GCM**）で **RSA** シグネチャを **ECDSA** アルゴリズム+**AES** で置き換えます

+ **ECC** デジタル署名アルゴリズム

+ **SHA-256**、**SHA-384**、および **SHA-512**

出典：シスコ公認ガイド、次世代暗号化プロトコル、p.97