Cisco.350-401J.v2026-08-13.q184

試験コード：	350-401J
試験名称：	Implementing and Operating Cisco Enterprise Network Core Technologies (350-401日本語版)
認証ベンダー：	Cisco
無料問題の数：	184
バージョン：	v2026-08-13
ページの閲覧量：	102
問題集の閲覧量：	1983

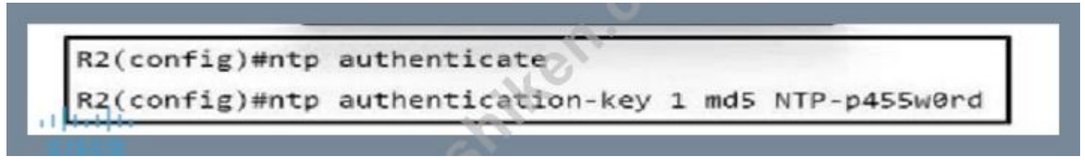
https://www.jpnshiken.com/shiken/Cisco.350-401J.v2026-08-13.q184.html

質問: **1**
エンタープライズ キャンパス設計におけるレイヤー 2 の安定性を向上させるには、どのネットワーク設計原則に従う必要がありますか?
A. すべてのユーザーVLANをコア層全体に拡張する
B. アクセス層全体に必要なユーザーVLANのみを拡張する
C. すべてのユーザーVLANをアクセス層全体に拡張します
D. 必要なユーザーVLANのみを集約層全体に拡張する
正解: **(**正解を表示します**)**

質問: **2**
エッジ ノードが担当する 2 つの機能はどれですか? (2 つ選択してください。)
A. ファブリックトラフィックの複数の入口と出口ポイントを提供します
B. エンドポイントを認証する
C. ファブリックトラフィックのデフォルトの出口ポイントを提供します
D. ファブリックトラフィックのデフォルトのエントリポイントを提供します
E. エンドポイントIDを現在の場所にマッピングするホストデータベースを提供します
正解: **(**正解を表示します**)**

質問: **3**
どの AP モードがスペクトルを分析して干渉源を検出しますか?
A. モニター
B. 不正検出機能
C. SEコネクト
D. スニファー
正解: **(**正解を表示します**)**

質問: **4**



図を参照してください。R2はNTPマスターとして構成されており、ローカル接続されたインターフェース10.1.1.1からNTPパケットを送信しています。構成を完了するために、他にどのような構成が必要ですか？
A. NTPサーバー 10.1.1.1 キー NTP-p455w0rd
B. NTP 信頼済みキー NTP-p455w0rd
C. NTPサーバー 10.1.1.1 キー 1
D. NTP信頼済みキー 1
正解: **(**正解を表示します**)**
The correct answer is D. NTP trusted-key 1.
ntp authenticate
ntp authentication-key 1 md5 NTP-p455w0rd
To fully enable NTP authentication, three components are required:
* Enable authentication globally
ntp authenticate
* Define the authentication key
ntp authentication-key < key-id > md5 < password >
* Trust the key
ntp trusted-key < key-id >
* The configuration already defines key 1
* The missing step is to mark this key as trusted
* Without ntp trusted-key 1 , the router will not use the key, even if it is defined
* A. NTP server 10.1.1.1 key NTP-p455w0rd Incorrect syntax. The key must be referenced by key ID (number), not password.
* B. NTP trusted-key NTP-p455w0rd Incorrect. Trusted-key uses the key ID, not the password.
* C. NTP server 10.1.1.1 key 1 This command is used on a client, not required to complete authentication on the server itself in this context.
For NTP authentication, always remember:
authenticate # authentication-key # trusted-key
If any of these three are missing, authentication will not work properly.

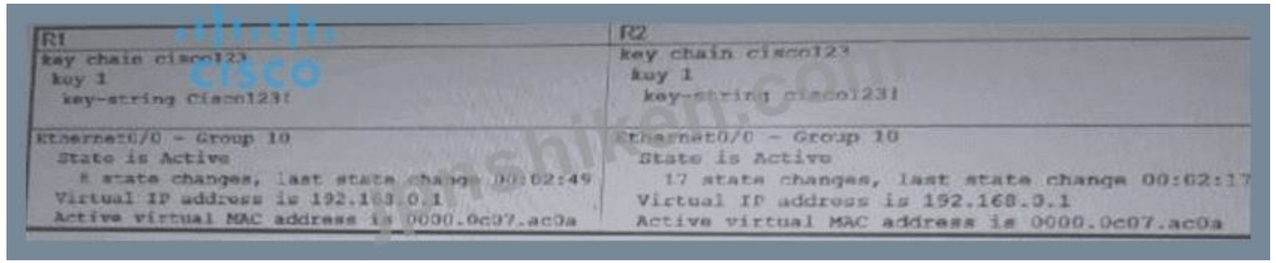
質問: **5**
ルート プロセッサに障害が発生した後、コントロール プレーンが回復するまでパケットの転送を継続するために SSO と連携する機能はどれですか。
A. NSF
B. RSVP
C. ECMP
D. HSRP
正解: **A (**コメントを発表する**)**

質問: **6**
Cisco Catalyst SD-WAN は、コントロール プレーン通信を保護するためにどのプロトコルを使用しますか?
A. DTLS
B. IPsec
C. OMP
D. STUN
正解: **(**正解を表示します**)**

質問: **7**
サードパーティ アプリケーションに HTTP サービスへの制限付きアクセスを許可する認証フレームワークはどれですか?
A. GRE
B. 基本認証
C. OAuth 2.0
D. IPsec
正解: (正解を表示します)

質問: **8**
Cisco DNA Center サウスバウンド API の機能は何ですか?
A. Cisco DNA Center からシスコ以外のデバイスを管理するためのサポートが追加されました。
B. ServiceNow などの 10 個の ITSM サービスに接続します。
C. 管理者が Cisco DNA Center への API 呼び出しを行うことを許可します。
D. アラートがトリガーされると、Cisco DNA CenterからWebhookを送信します。
正解: (正解を表示します)

質問: **9**



エンジニアが冗長構成で新しいルーターのペアを設置しています。ハードウェア障害が発生した場合でもトラフィックが中断されないことを保証するプロトコルはどれですか？
A. HSRPv1
B. VRRP
C. GLBP
D. HSRPv2
正解: (正解を表示します)

質問: **10**

```
import json
from requests import get

Headers = { "Content-Type" : "application/yang-data+json",
            "Accept" : "application/yang-data+json" }

Devices = open("devices.txt", "r")

for Device in Devices.readlines():
  Hostname, IP, Login, Pass = Device.strip().split(",")
  URL = f"https://{IP}/restconf/data/Cisco-IOS-XE-native:native"
  Creds = (Login, Pass)
  Response = get(URL, auth = Creds, headers = Headers, verify = False)
```

展示を参照してください。各デバイスの構成がデバイス名でJSON形式のファイルに保存されるように、スクリプトをどのように記述すればよいですか？

Insert after the for loop:

```
with open(f"{Hostname}.json", "w") as OutFile:
  OutFile.write(Response)
```

Insert after the for loop:

```
with open(f"{Hostname}.json", "w") as OutFile:
  OutFile.write(json.dumps(Response.text))
```

Append to the body of the for loop:

```
with open(f"{Hostname}.json", "w") as OutFile:
  OutFile.write(Response.text)
```

Insert immediately before the for loop:

```
with open(f"{Hostname}.json", "w") as OutFile:
  OutFile.write(json.load(Devices))
```

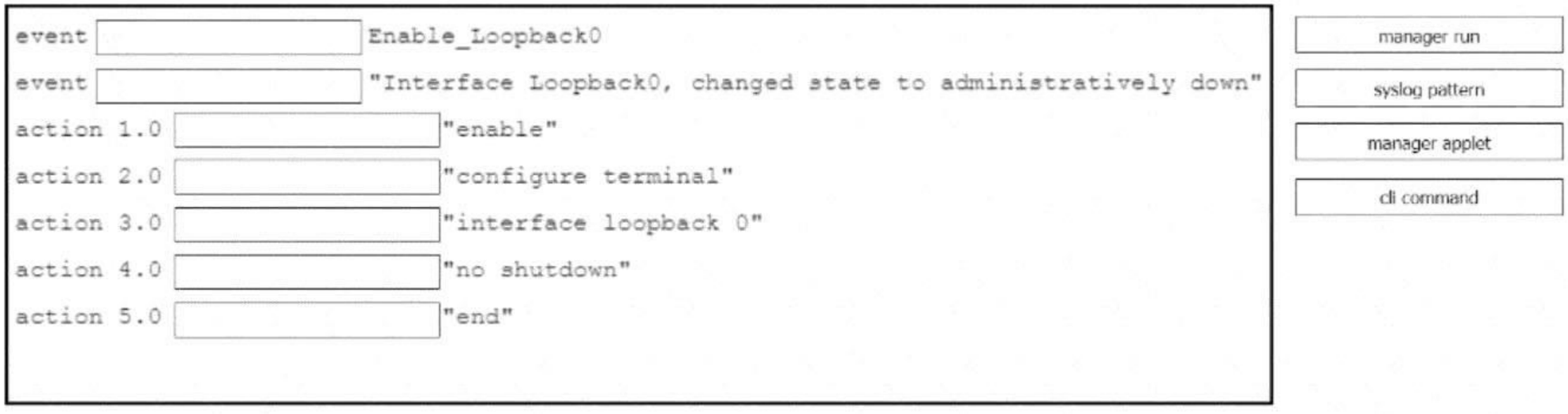
A. オプションC

B. オプションB

C. オプションD
D. オプションA
正解: **(**正解を表示します**)**

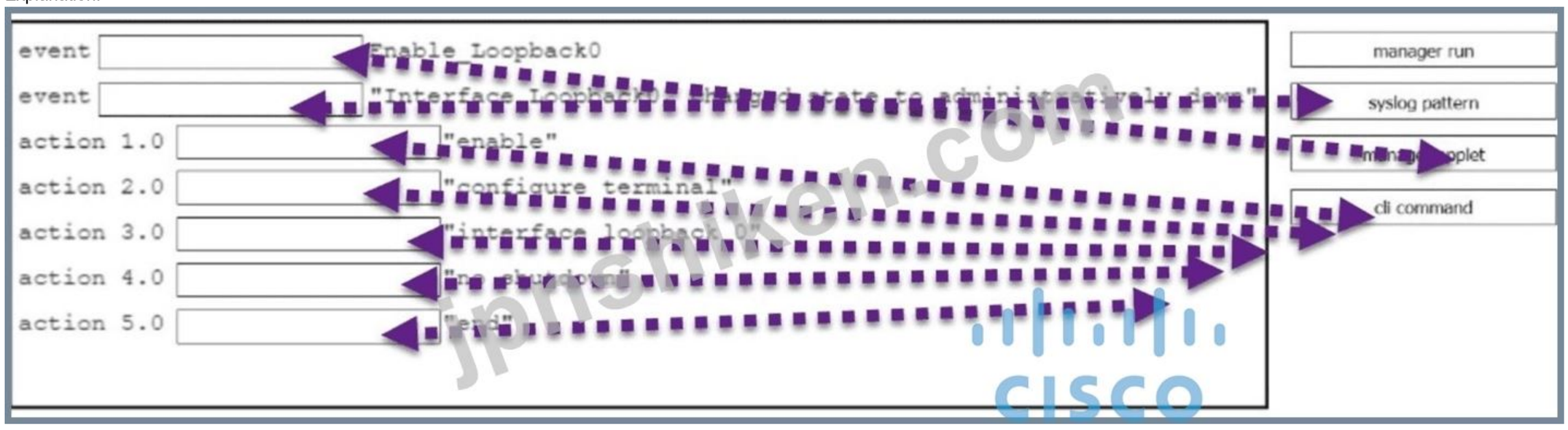
質問: **11**
トラフィックが LISP 対応サイトに送信されるときに、EID から RLOC へのマッピングを見つける役割を担うデバイスはどれですか。
A. マップサーバー
B. 入力トンネルルータ
C. マップリゾルバ
D. 出力トンネルルータ
正解: **(**正解を表示します**)**

質問: **12**
右側のコマンド スニペットをボックスにドラッグ アンド ドロップして、ログ メッセージ 「nterface LoopbackO. changed state to Administratively down」を受信したときにインターフェイス LoopbackO を有効にする EEM アプレットを作成します。すべてのコマンドが使用されるわけではなく、一部のコマンドは複数回使用されます。



正解:

Explanation:



質問: **13**

異なるモビリティ グループを使用している 2 つの WLC 間でコントローラ間レイヤ 3 ローミングが実行される場合に、クライアントの IP アドレスを維持するために必要な機能はどれですか。

A. 自動アンカー

B. RFグループ

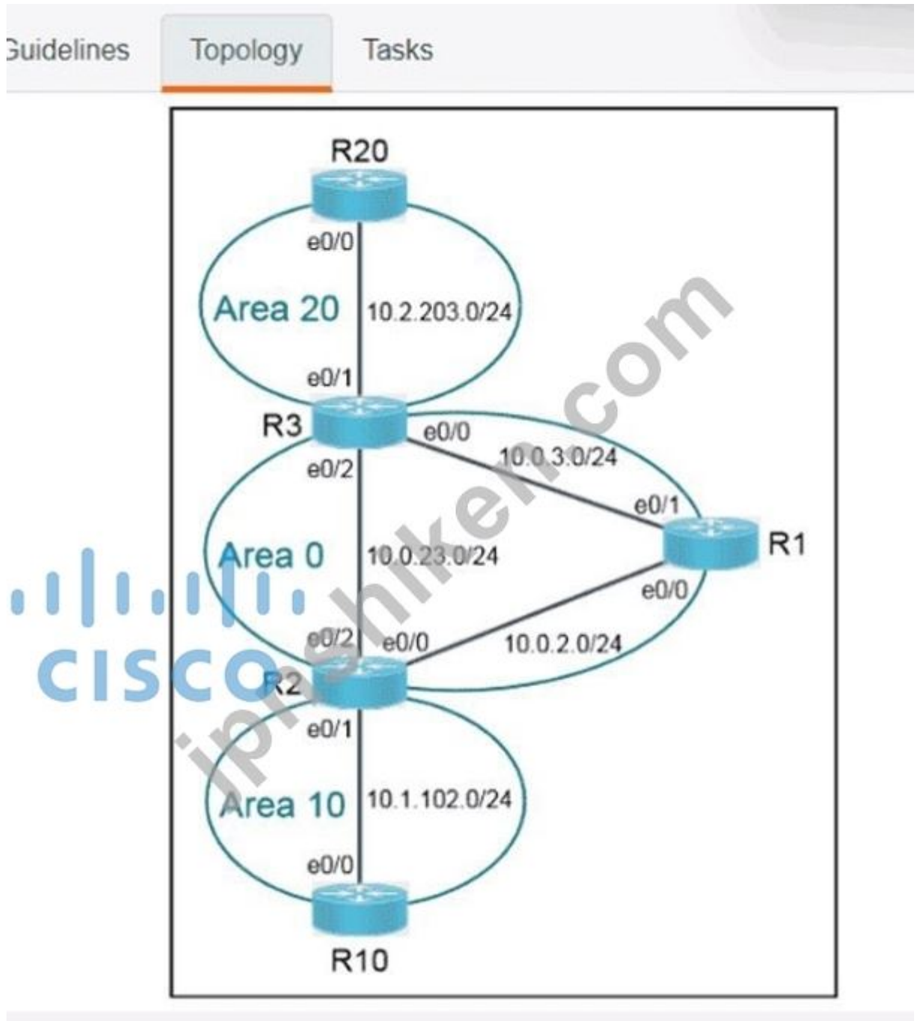
C. AAAオーバーライド

D. インターフェースグループ

正解: **A** (コメントを発表する)

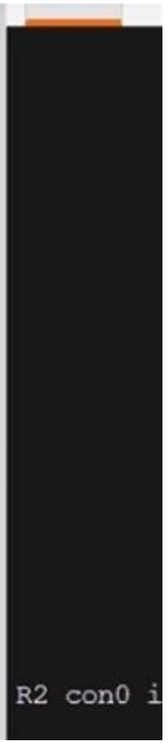
質問: **14**
PIM デンス モードはネットワーク内でどのような 2 つの方法で機能しますか? (2 つ選択してください。)
A. 下流ルータが転送停止を要求するまで、すべてのインターフェースでマルチキャスト トラフィックを転送します。
B. 下流ルータがトラフィックを要求するまで、マルチキャスト トラフィックの転送を待機します。
C. プッシュ方式を使用し、RP 情報が失われた場合にフォールバックが発生します。
D. 指定されたフォワーダーの選択を利用して、マルチキャスト パケット ループを回避します。
E. 1 つのリバース パス フォワーディング インターフェイスからのみトラフィックを受信します。
正解: **(**正解を表示します**)**

質問: **15**



OSPF is partially configured. Complete the OSPF configurations on the ABR routers to achieve these goals:

1. The route for R1 Loopback 0 should not be advertised into Area 10. Use the partially configured prefix list to accomplish the task. Do not use the **area 0** command under the **router ospf** configuration section to accomplish the task.
2. The route for R20 loopback 0 should not be advertised out of area 20. Use the partially configured prefix list to accomplish this task. Do not use the **area 0** command under the **router ospf** configuration section to accomplish this task.



正解:

See the solution below in Explanation:

Explanation:

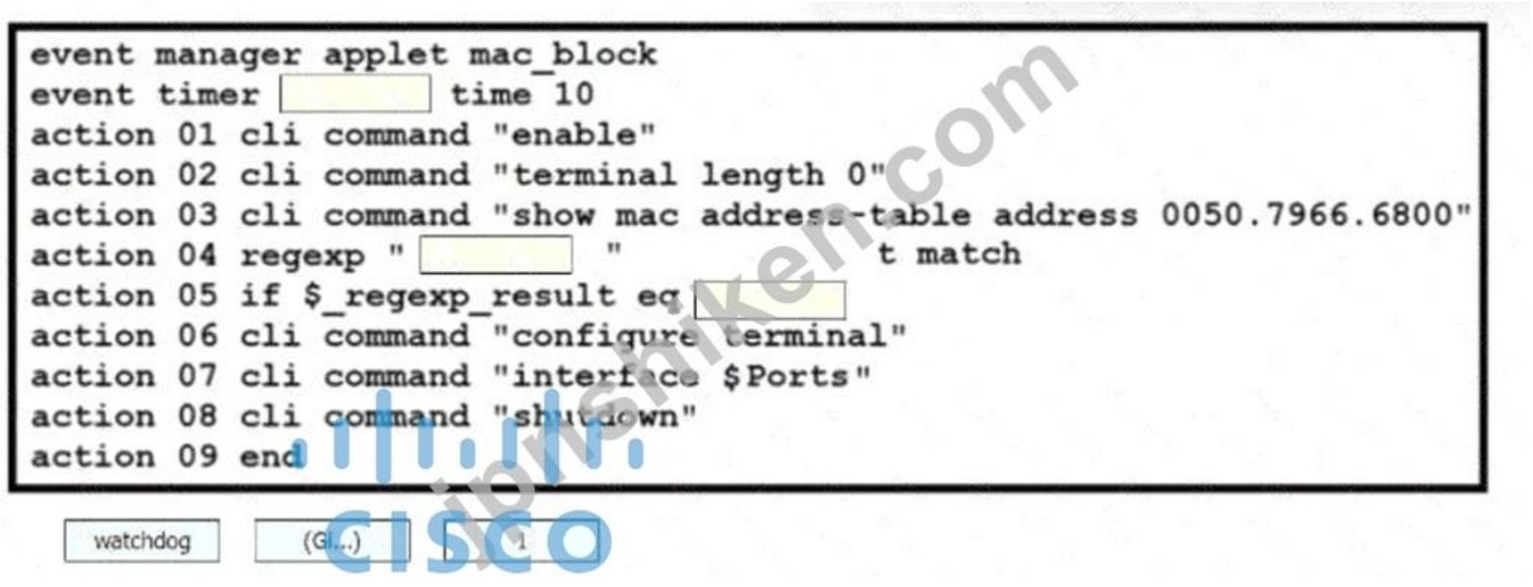
Solution:

R2

R3

質問: **16**
構成と状態データをモデル化するために使用できる言語はどれですか?
A. XDR
B. JSON
C. YANG
D. XML
正解: **(**正解を表示します**)**

質問: **17**
スニペットをコード内の空白にドラッグ アンド ドロップして、MAC アドレスをブロックするスクリプトを作成します。



正解:

```
event manager applet mac_block
event timer watchdog time 10
action 01 cli command "enable"
action 02 cli command "terminal length 0"
action 03 cli command "show mac address-table address 0050.7966.6800"
action 04 regexp " (Gi...) " t match
action 05 if $_regexp_result eq 1
action 06 cli command "configure terminal"
action 07 cli command "interface $Ports"
action 08 cli command "shutdown"
action 09 end
```

watchdog (Gi...) 1

Explanation:

```
event manager applet mac_block
 event timer watchdog time 10
action 01 cli command "enable"
action 02 cli command "terminal length 0"
action 03 cli command "show mac address-table address 0050.7966.6800"
action 04 regexp " (Gi...) " $_cli_result match
action 05 if $_regexp_result eq 1
 action 06 set Ports "$_cli_result"
 action 07 cli command "configure terminal"
 action 08 cli command "interface $Ports"
 action 09 cli command "shutdown"
action 10 end
```


質問: **18**

顧客から、GLBPをFHRPとして含む設計の依頼がありました。ネットワーク設計者は、GLBPグループのメンバーのスループット能力が異なることを発見しました。この環境をサポートするGLBPロードバランシング方式はどれですか？

A. ラウンドロビン

B. ホスト依存

C. 最小接続

D. 重み付け
正解: **(**正解を表示します**)**

質問: **19**
クライアントが Web 認証状態にあり、モビリティ トンネルを使用して 2 つのコントローラ間をローミングする場合、クライアントは何と見なされますか?
A. 新しい
B. モバイル
C. 外国人
D. アンカー
正解: **(**正解を表示します**)**

質問: **20**
Cisco Trust Sec アーキテクチャでユーザーにセキュリティ グループ タグを割り当てるために使用される 2 つの方法はどれですか。
（2つ選択してください。）
A. モジュラーQoS
B. IEEE 802.1x
C. ポリシールーティング
D. DHCP
E. ウェブ認証
正解: **(**正解を表示します**)**

質問: **21**
REST API によって実行されるステートレス呼び出しがクラウド アプリケーションで役立つのはなぜですか?
A. 再デプロイや拡張が簡単です。
B. 呼び出しにはサーバー上に保存されたデータに依存します。
C. すべての呼び出しを実装するために HTTPS を使用します。
D. URL デコードを制御します。
正解: **(**正解を表示します**)**

質問: **22**
ファブリック対応ワイヤレスの Cisco SD-Access プレーン機能について説明している文はどれですか。
A. コントロール プレーン トラフィックは CAPWAP トンネルを介して WLC に送信され、データ プレーン トラフィックは VXLAN を介して AP からファブリック エッジ スイッチに送信されます。
B. コントロール プレーン トラフィックは VXLAN を介して WLC に送信され、データ プレーン トラフィックは CAPWAP トンネルを介して WLC に送信されます。
C. コントロール プレーン トラフィックとデータ プレーン トラフィックは、VXLAN を介して WLC に送信されます。
D. コントロール プレーン トラフィックとデータ プレーン トラフィックは、CAPWAP トンネルを介して WLC に送信されます。
正解: **A (**コメントを発表する**)**

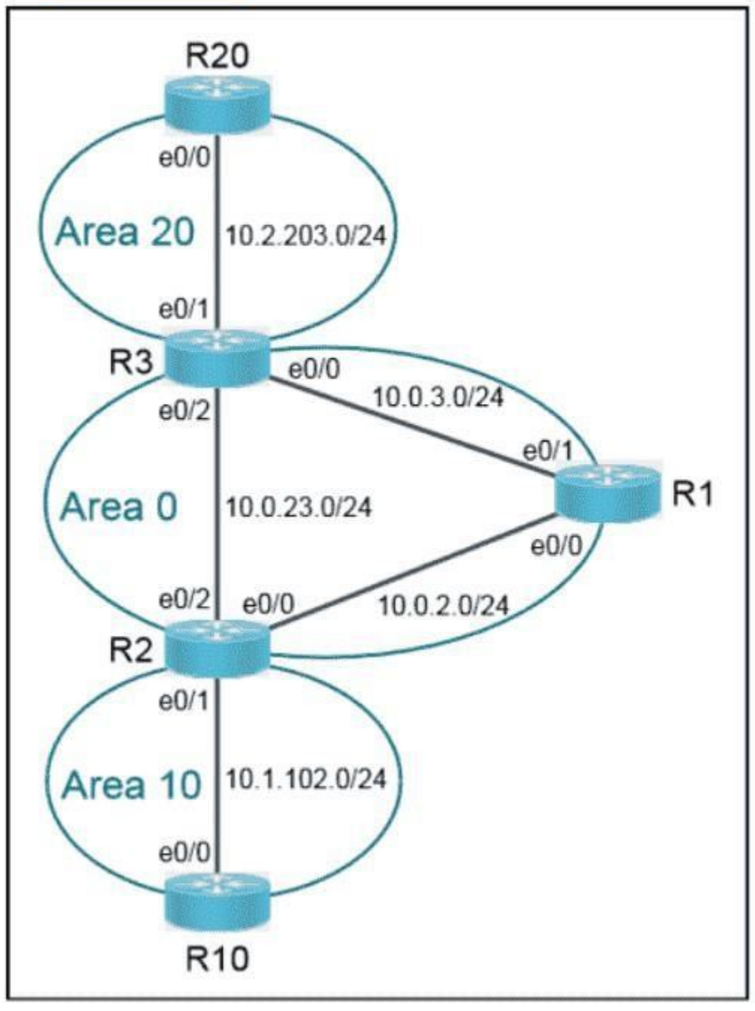
質問: **23**
タイプ 1 ハイパーバイザーとは何ですか?
A. 物理サーバー上で直接実行され、以前にインストールされたオペレーティングシステムに依存します。

B. 仮想サーバー上で実行され、既にインストールされているオペレーティングシステムに依存します。
C. 仮想サーバー上で実行され、独自のオペレーティングシステムが含まれています
D. 物理サーバー上で直接実行され、独自のオペレーティングシステムが含まれています
正解: **D** (コメントを発表する)

質問: **24**
Cisco Cyber Threat Defenseソリューションのどのコンポーネントが、ユーザおよびフローコンテキスト分析を提供しますか。
A. Ciscoステルスウォッチシステム
B. 高度なマルウェア保護
C. CiscoFirepowerおよびFireSIGHT
D. CiscoWebセキュリティアプライアンス
正解: (正解を表示します)

質問: **25**

Guidelines | Topology | Tasks



R2 | R3 | R1 | R10 | R20

```
R2>
```

Guidelines Topology Tasks

OSPF is partially configured. Complete the OSPF configurations to achieve these goals:

1. Configure R3 and R20 so they do not participate in a DR/BDR election process in Area 20.
2. Configure R10 so it is always the DR for Area 10. Do not change the router ID.

R2 R3 R1 R10 R20

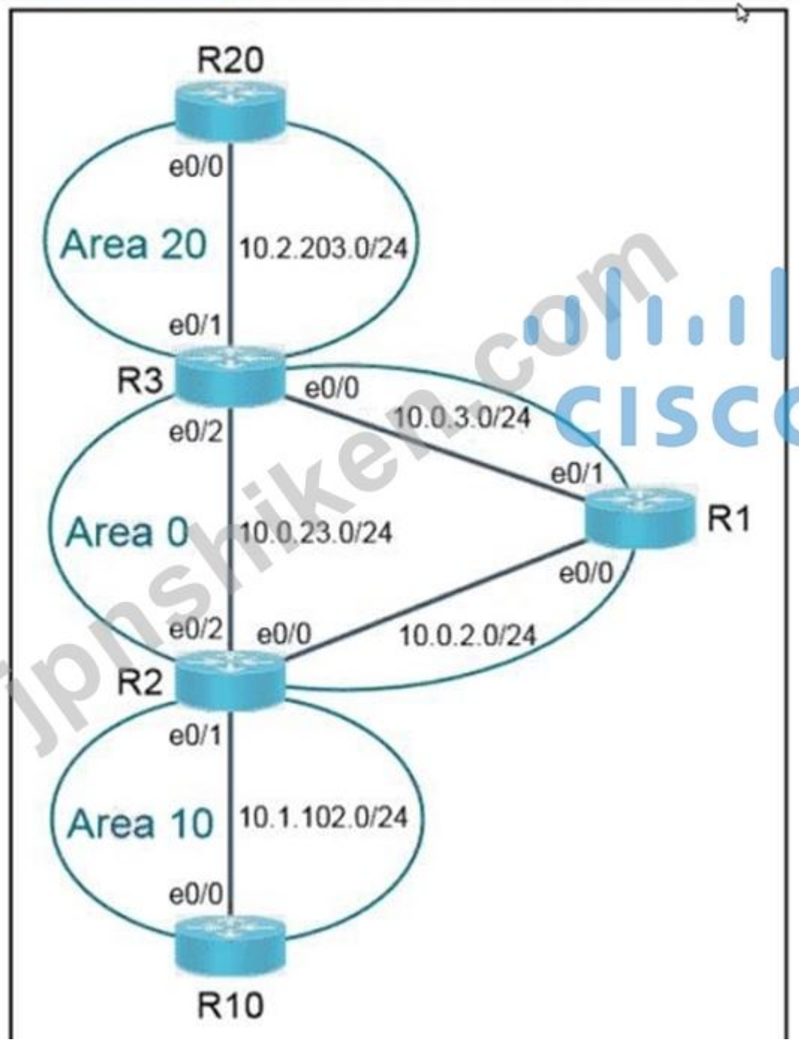
R2>

Guidelines Topology Tasks

OSPF is partially configured. Complete the OSPF configurations to achieve these goals:

1. Configure R3 and R20 so they do not participate in a DR/BDR election process in Area 20.
2. Configure R10 so it is always the DR for Area 10. Do not change the router ID.

Guidelines | Topology | Tasks



正解:

See the solution below in Explanation:

Explanation:

Solution:

```
R20#sh run int e0/0
Building configuration...

Current configuration : 112 bytes
!
interface Ethernet0/0
 ip address 10.2.203.20 255.255.255.0
 ip ospf network point-to-point
 duplex auto
end
```

Copy run start

```
R3#sh run int e0/1
Building configuration...

Current configuration : 111 bytes
!
interface Ethernet0/1
 ip address 10.2.203.3 255.255.255.0
 ip ospf network point-to-point
 duplex auto
end
```

Copy run start

```
R10#sh run  int e0/0
Building configuration...

Current configuration : 102 bytes
!
interface Ethernet0/0
 ip address 10.1.102.10 255.255.255.0
 ip ospf priority 255
 duplex auto
end
```

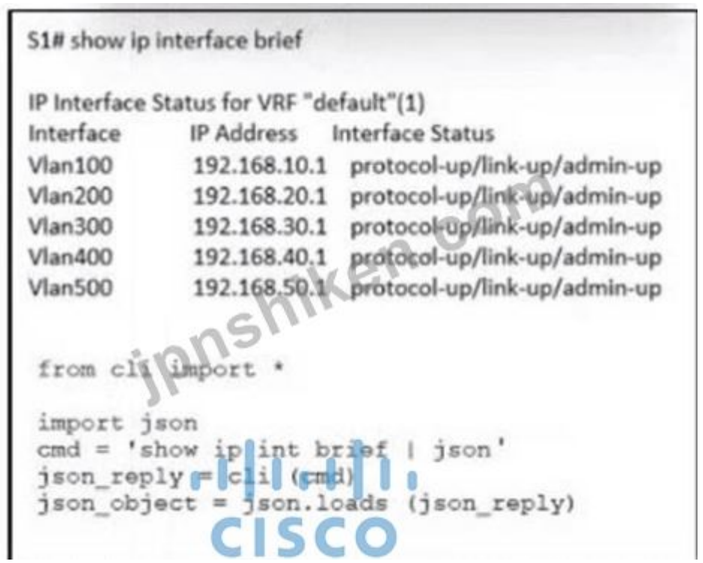
Copy run start

Verification:-

```
R10#
R10#clear ip ospf process
Reset ALL OSPF processes? [no]: yes
R10#
*Nov 17 10:21:39.702: %OSPF-5-ADJCHG: Process 10, Nbr 10.0.
1.2 on Ethernet0/0 from FULL to DOWN, Neighbor Down: Interf
ace down or detached
*Nov 17 10:21:39.703: %OSPF-5-ADJCHG: Process 10, Nbr 10.0.
1.2 on Ethernet0/0 from LOADING to FULL, Loading Done
R10#
```

OR

質問: 26



図を参照してください。エンジニアは、ネットワーク内の複数のデバイスからインターフェースの詳細を取得し、JSON応答に基づいてデバイスの管理IPアドレスを出力する必要があります。VLAN 100はすべてのスイッチに存在し、管理に使用されます。どのコード行を適用する必要がありますか？

A. print(json.dumps[" TABLE_intf "][" ROW_intf "][" prefix "])

B. print(json.dumps[" TABLE_intf "][" ROW_intf "][2] [" prefix "])

C. print(json_object[" TABLE_intf "][" ROW_intf "][1] [" prefix "])

D. print(json_object[" TABLE_intf "][" ROW_intf "][0] [" prefix "])

正解: **(**正解を表示します**)**

The correct answer is D. print(json_object[" TABLE_intf "][" ROW_intf "][0] [" prefix "]).

* Parsing JSON output from Cisco devices

* Using Python to extract structured data

* Understanding how CLI output is converted into JSON format

* The command used:

show ip int brief | json

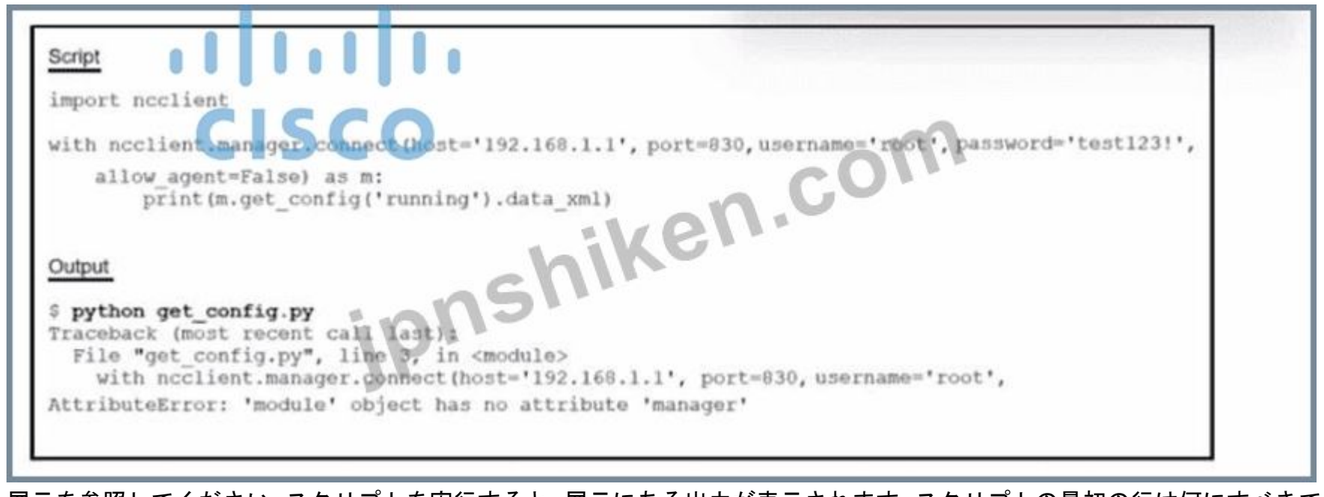
returns structured JSON data.

* The JSON hierarchy shown in the exhibit:

{

" TABLE_intf " : {
" ROW_intf " : [
{ " intf-name " : " Vlan100 " , " prefix " : " 192.168.10.1 " , ... },
{ " intf-name " : " Vlan200 " , " prefix " : " 192.168.20.1 " , ... },
...
]
}
}
* Important Observations:
* ROW_intf is a list (array) of interface objects.
* Each object contains fields like " prefix " (IP address).
* VLAN 100 is used for management and appears first in the list.
* Python Code Analysis:
* json.loads() converts JSON string into a Python dictionary # json_object
* To access VLAN100 IP:
json_object[" TABLE_intf "][" ROW_intf "][0] [" prefix "]
* Why Option D is Correct:
* Uses the correct variable (json_object)
* Correctly navigates dictionary # list # element # key
* Index [0] corresponds to Vlan100 (management VLAN)
* A & B: Use json.dumps incorrectly (this function converts Python # JSON, not for accessing data)
* C: Uses index [1] , which refers to Vlan200, not VLAN100
When working with Cisco JSON output:
* Identify list vs dictionary
* Use indexing for lists ([0])
* Use keys for dictionaries ([" key "])
Correct Pattern:
json_object[" parent "][" child "][index] [" field "]

質問: 27



展示を参照してください。スクリプトを実行すると、展示にある出力が表示されます。スクリプトの最初の行は何にすべきでしょうか？

A. インポートマネージャー

B. ncclientインポートマネージャーから

C. ncclient マネージャーのインポート

D. ncclient からのインポート *

正解: **(**正解を表示します**)**

質問: **28**

LISP マップ サーバーの役割は何ですか?

A. EIDをRLOCにマッピングするETRから情報を受信する

B. EIDをRLOCにマッピングするETRからの情報を送信します。

C. EID から RLOC への解決要求に応答します。

D. EIDからRLOCへの解決要求を送信します

正解: **(**正解を表示します**)**

質問: **29**

Cisco Catalyst Center (旧 DNA Center) から発信され、ファブリック アンダーレイ スイッチで終了するサウスバウンド インターフェイスはどれですか (2 つ選択してください)。

A. UDP67 DHCP

B. UDP 162 SNMP

C. UDP6007 ネットフロー

D. TCP 23 テルネット

E. ICMP検出

正解: **D,E (**コメントを発表する**)**

質問: **30**

図を参照してください。ネットワークエンジニアはNETCONFを設定する必要があります。設定後、エンジニアはshow lineコマンドからは出力を取得できますが、show running-configからは出力を取得できません。どのコマンドで設定を完了できますか？

A. Device(config)# no netconf ssh acl 1
B. Device(config)# netconf lock-time 500
C. Device(config)# netconf max-sessions 100
D. Device(config)# netconf max-message 1000
正解: **(**正解を表示します**)**

質問: **31**
ある会社が、Cisco SD-Access Fabric 有線ネットワーク内で新しい OTT ワイヤレス ソリューションを設計するためにネットワーク アーキテクトを雇っています。アーキテクトは、トラフィックを集中的に切り替えられるように、アクセス ポイントを WLC に登録したいと考えています。設計にはどの AP モードを含める必要がありますか?
A. ファブリック
B. フレックスコネクト
C. ブリッジ
D. ローカル
正解: **(**正解を表示します**)**

質問: **32**
クライアントがワイヤレス コントローラ間でレイヤー 2 ローミングを実行できるようにする機能はどれですか。
A. SSO
B. N+1の高可用性
C. RFグループ化
D. モビリティグループ
正解: **(**正解を表示します**)**

質問: **33**
キャンパス ネットワーク設計において、障害検出に BFD を使用する 2 つの利点は何ですか? (2 つ選択してください。)
A. BFDはメモリとCPUの使用量を削減する効率的な方法です
B. BFDにより、ネットワークピアは再起動時にパケットの転送を継続できます。
C. BFD はルーティングの収束時間を短縮します
D. BFDは、複数のルータを単一の仮想ルータとして表示できるようにすることで、耐障害性を提供します。
E. BFDは1秒未満でパス障害検出を提供します
正解: **C,E (**コメントを発表する**)**

質問: **34**
サポートされている AP が WLAN クライアントのように機能し、クライアントの接続の問題を関連付けて識別できるようにする AP モードはどれですか。
A. センサーモード

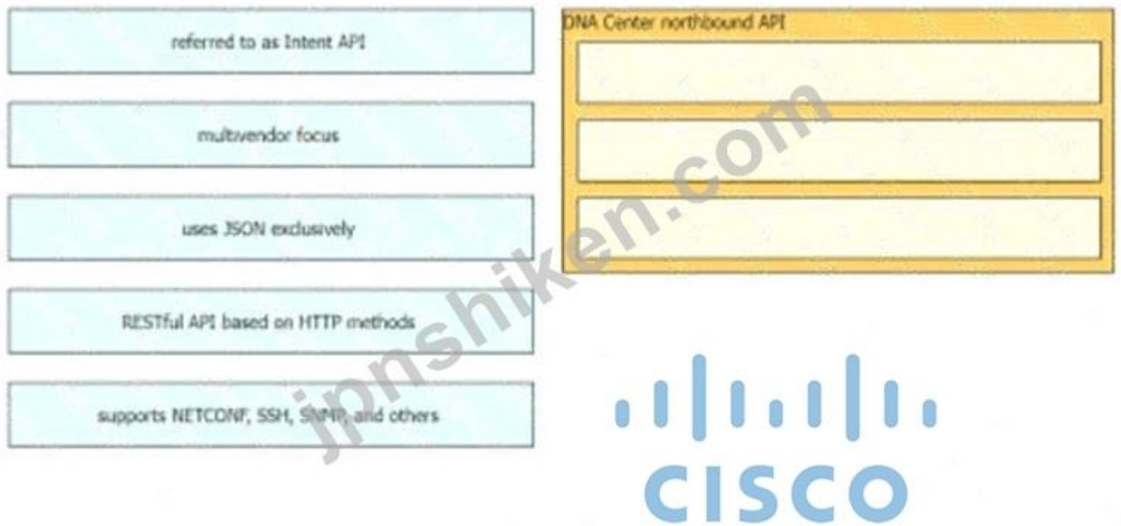
B. SE接続モード
C. スニファーモード
D. クライアントモード
正解: **(**正解を表示します**)**

質問: **35**

図を参照してください。IP SLAはルータに設定されています。エンジニアは、IP SLAに問題が発生した場合にインターフェースをシャットダウンし、再起動するためのEEMアプレットを設定する必要があります。エンジニアはどの設定を使用すべきでしょうか？
A. イベントマネージャアプレット EEM_IP_SLAevent sla 10 状態到達不能
B. イベントマネージャアプレット EEM_IP_SLAevent トラック 10 状態到達不能
C. イベントマネージャアプレット EEM_IP_SLAevent sla 10 状態ダウン
D. イベントマネージャアプレット EEM_IP_SLAevent トラック 10 状態ダウン
正解: **(**正解を表示します**)**

質問: **36**
接続されたメンバーまたは下流のネイバーが存在しない場合に、どのマルチキャスト動作モードがソースにプルーニング メッセージを送信しますか。
A. IGMPv2
B. IGMPv3
C. PIMデンスモード
D. PIMスパースモード
正解: **(**正解を表示します**)**

質問: **37**
Cisco DNA Centerのノースバウンドapi特性を左から右にドラッグアンドドロップします。すべてのオプションが使用されるわけではありません。



正解:

Explanation:


referred to as Intent API
multivendor focus
uses JSON exclusively
RESTful API based on HTTP methods
supports NETCONF, SSH, SNMP, and others
DNA Center northbound API
jpnshiken.com
CISCO

質問: 38

```
from pythonping import ping
import paramiko
import sys

s= "%s %s" % (sys.argv[1],'')
s1=s.replace(' ','')
ip= s1
t= "%s %s" % (sys.argv[2],'')
r= ping(s1, count=7)
r1= r.success()
if r1 != True:
   exit()
client= paramiko.SSHClient()
client.load_system_host_keys()
client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
client.connect(ip, port= 22, username= usr, password= pswd)
stdin, stdout, stderr = client.exec_command(t + '\n')
time.sleep(3)
print(t)
for u in stdout:
   print(u)
client.close()
```


図を参照してください。Pythonスクリプトを実行すると、どのようなアクションが発生しますか？

A. そのデバイスで入力されたコマンドの出力を表示します

B. そのデバイスで入力されたコマンドの出力を1行で表示します。

C. そのデバイスに手動で入力されたIPアドレスにSSH接続します

D. そのデバイスで入力されたコマンドのフォーマットされていない出力を表示します。

正解: **(**正解を表示します**)**

質問: **39**

エンドユーザーのデバイスとデータを未知のファイルの動作から保護するために使用される手法はどれですか?

A. ファイルハッシュ計算を使用した暗号ファイルランサムウェア保護

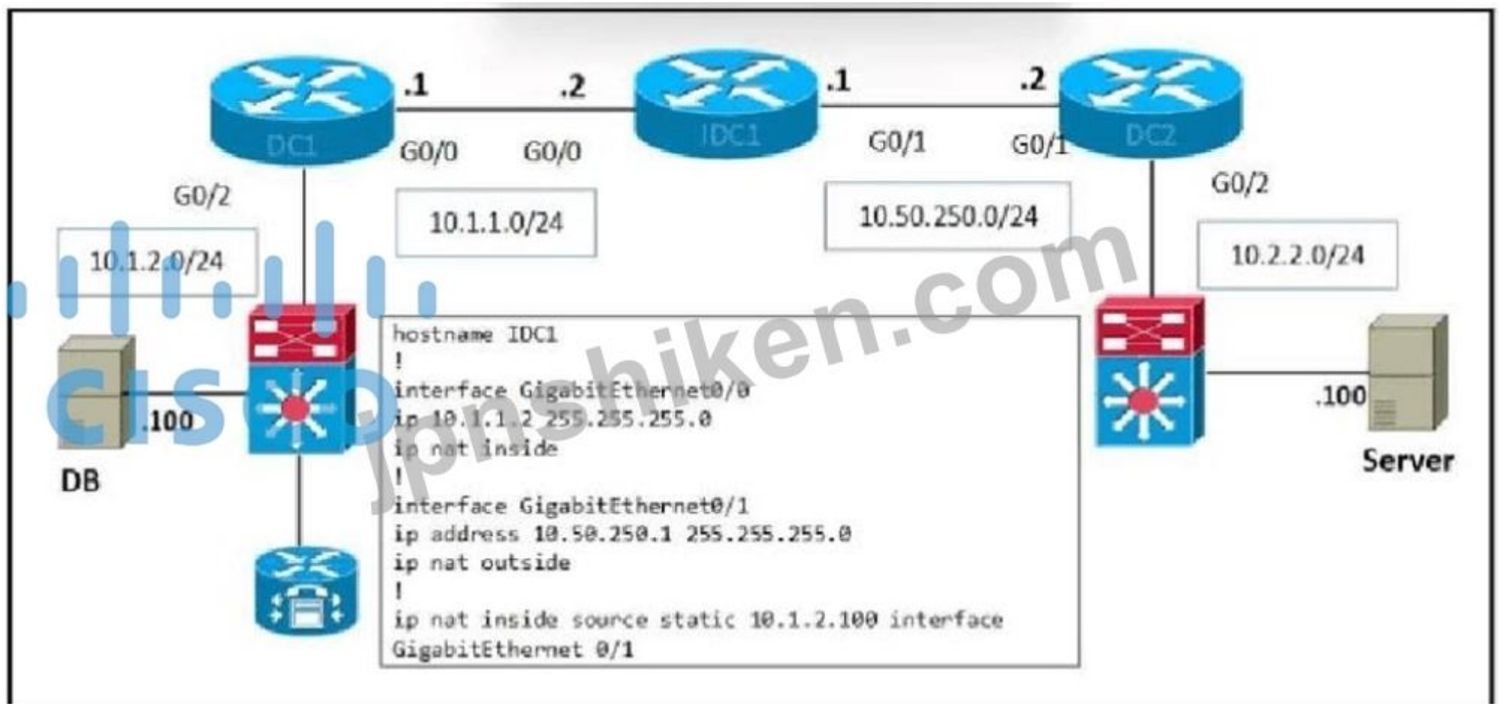
B. 添付ファイルを保存するための内部環境を使用したフィッシングファイルの隔離

C. 継続的なスキャンと分析を使用したファイルの遡及調査

D. 保護された環境を使用して未知のファイルの動作を分析およびシミュレートするファイルサンドボックス

正解: **D (**コメントを発表する**)**

質問: **40**



図を参照してください。DC2 のサーバーは、DC1 のデータベースからのトラフィックがソースネットワーク 10.50.250.0/24 を使用することを想定しています。サーバーは最初の要求を送信します。内部グローバル IP は次のように構成されています。

10.50.250.1. この設定の結果はどうなりますか？

A. 通信を開始できるのはサーバーのみです。

B. 通信を開始できるのはデータベースのみです。

C. サーバーとデータベースが通信できません。

D. サーバーとデータベースは通信を開始できます。

正解: **B** (コメントを発表する)

The correct answer is B. Only the database can initiate communication.

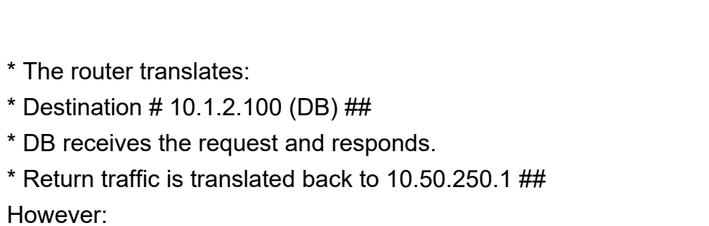
From the exhibit:

ip nat inside source static 10.1.2.100 interface GigabitEthernet0/1

* Inside local (DB): 10.1.2.100
* Inside global (translated IP): 10.50.250.1 (Gi0/1 interface)
* NAT type: Static NAT
* Static NAT creates a permanent one-to-one mapping between inside local and inside global IP.
* It allows bidirectional communication, but only if traffic is properly addressed.
* The server initiates the connection
* The server expects the DB to appear as 10.50.250.0/24 (translated network)
* The server sends traffic to 10.50.250.1 (inside global IP).

* The router translates:
* Destination # 10.1.2.100 (DB) ##
* DB receives the request and responds.
* Return traffic is translated back to 10.50.250.1 ##
However:
* The NAT rule only defines source translation for traffic originating from inside (DB).
* It does not fully support proper session handling when initiated from outside unless routing/NAT symmetry is correct.
* In this topology, the expectation and flow mismatch causes only inside-initiated sessions to work reliably.
* The database (inside) can initiate connections outward using NAT ##
* The server (outside) initiating may fail due to NAT direction and expectation mismatch #
* A. Only the server can initiate communication Incorrect - NAT favors inside-initiated traffic.
* C. No communication possible Incorrect - inside-initiated traffic still works.
* D. Both can initiate communication Incorrect - would only be true with correct bidirectional NAT design.
* Static NAT = bidirectional mapping, BUT
* Always check:
* Who initiates traffic
* Which side is inside vs outside
* Whether NAT rules match expected traffic flow
Exam trick:
If NAT is configured as inside source , it primarily supports inside # outside initiation.

質問: **41**



展示を参照してください。プログラマーはAPI呼び出しで受信したVLANのリストにどのようにアクセスすればよいでしょうか？

A. VlanNames(0)

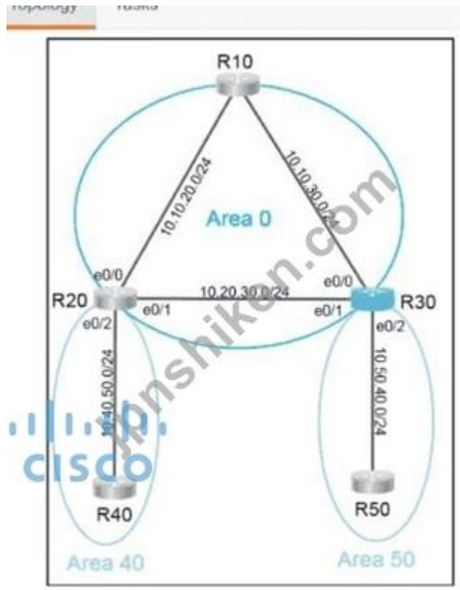
B. VlanName['response']

C. VlanName[Vlan1']

D. list(VlanNames)

正解: **(**正解を表示します**)**

質問: **42**



Guidelines Topology Tasks

OSPF is preconfigured on all devices except R30. Configure R30 to complete these tasks.

Task 1:

Configure OSPF according to the topology using these requirements:

- Use Process ID 100.
- Use Loopback0 for the Router ID.
- Advertise all networks into OSPF.
  - Use **network** statements under the OSPF process to accomplish this task.

Task 2:

Configure a /18 summary route for Area 50.

正解:

See the solution below in Explanation:

Explanation:

Solution:

R30

Config t
router ospf 100
router-id 10.0.1.30
int ran lo0 , e0/0-1
ip ospf 100 a 0
exit
int et0/2
ip ospf 100 a 50
exit
router ospf 30
area 50 range 10.10.0.0 255.255.192.0
area 50 range 10.50.0.0 255.255.192.0
end
wr

質問: **43**
信号が無線、アンテナケーブル、およびアンテナを通過した後の信号の放射電力を測定するために使用される計算は何ですか？
A. mW
B. EIRP
C. dBi
D. dBm
正解: **B** (コメントを発表する)

質問: **44**
Cisco SD-Accessソリューションにおいて、ファブリックエッジノードの役割は何ですか？
A. フュージョンルーターをSD-Accessファブリックに接続する
B. 有線エンドポイントをSD-Accessファブリックに接続する
C. ファブリックIPアドレス空間を外部ネットワークにアドバタイズする
D. 外部レイヤ3ネットワークをSD-Accessファブリックに接続する
正解: (正解を表示します)
The correct answer is B. to connect wired endpoints to the SD-Access fabric.
In Cisco SD-Access, the fabric edge node is the device that provides access for endpoints into the fabric. It is the point where user devices such as PCs, phones, printers, and access points attach to the SD-Access network. The edge node handles endpoint onboarding into the fabric and applies the appropriate segmentation and policy.
A fabric edge node is specifically responsible for:
* Connecting wired endpoints to the fabric
* Serving as the access-layer entry point into the SD-Access fabric
* Enforcing policy and segmentation for connected endpoints
* Extending the fabric to end hosts
This is the main role of the edge node in the SD-Access architecture.
* A. to connect the fusion router to the SD-Access fabric This is not the role of the fabric edge node. The fusion router is used outside the fabric to provide connectivity between the fabric and external networks.

* C. to advertise fabric IP address space to external networks This function is associated with the border node, not the edge node. The border node connects the fabric to external domains and exchanges reachability information.
* D. to connect external Layer 3 networks to the SD-Access fabric This is also the function of the border node, not the edge node.
Remember these SD-Access node roles clearly:
* Edge node = connects endpoints
* Border node = connects to external networks
* Control-plane node = maintains endpoint-to-location mappings
* Fusion router = external routing/services outside the fabric
Edge node = endpoint access into the fabric

質問: **45**

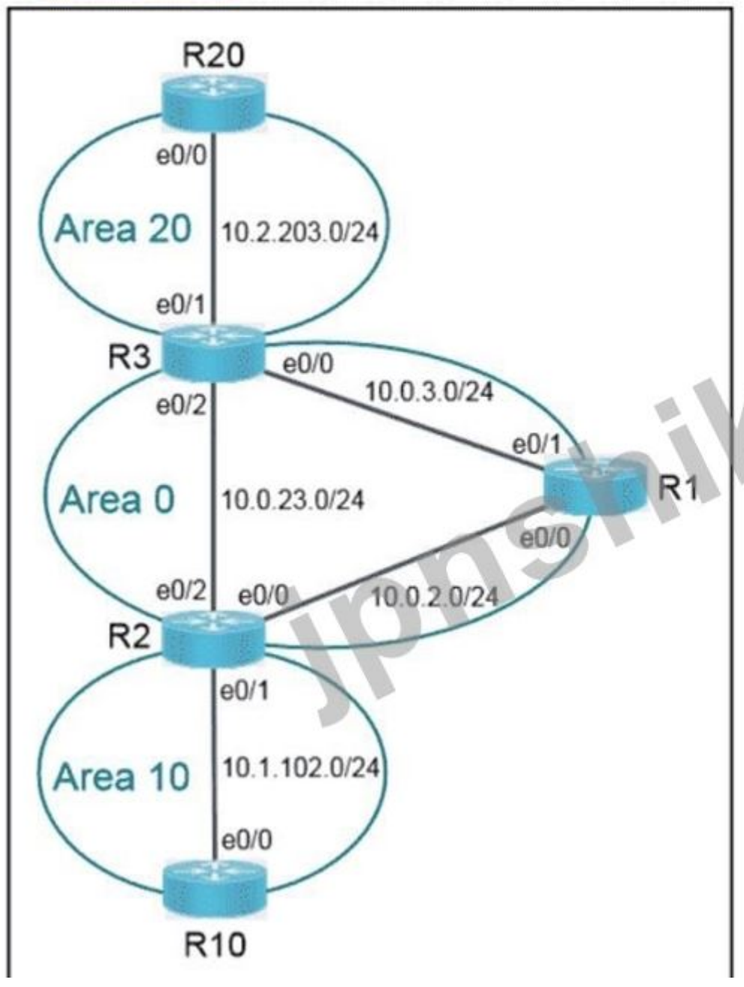
展示を参照してください。コード実行後の変数リストの値は何ですか？
A. [3,6]
B. [1,2] * 3
C. [1,2.1.2.1,2]
D. [1,2]. [1.2]. [1,2]
正解: (正解を表示します)

質問: **46**
Cisco SD-Access ワイヤレス ソリューションでは、無線リソース管理はどこで実行されますか?
A. ワイヤレスコントローラー
B. コントロールプレーンノード
C. Cisco CMX
D. DNAセンター
正解: (正解を表示します)

質問: **47**

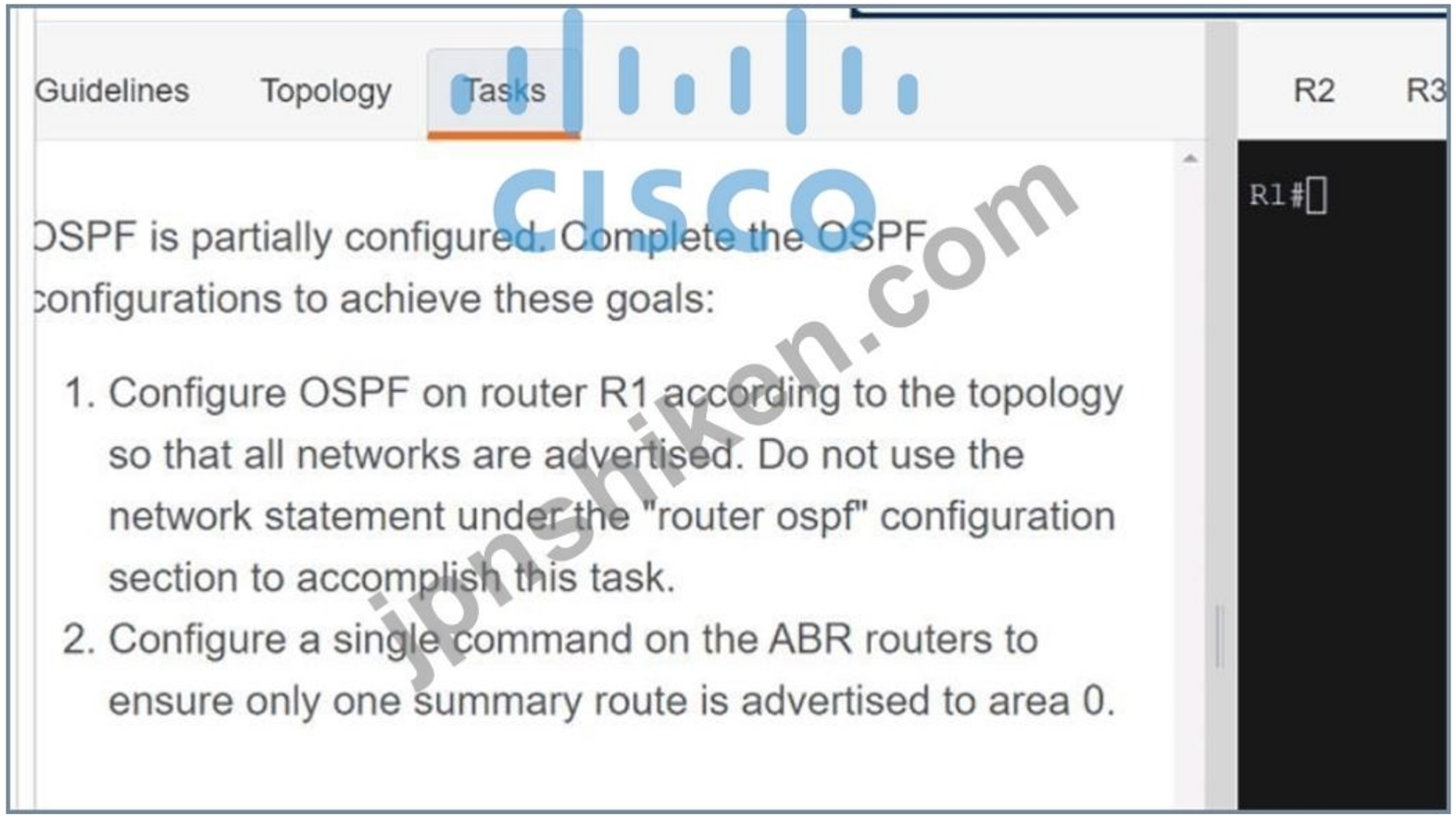
Recording

Guidelines | Topology | Tasks



R2 | R3 | R1 | R10 | R20

R1#



正解:

See the solution below in Explanation:

Explanation:

Solution:

R1

en

Conf t

Router ospf 10

Router-id 10.x.x.x - lo0 address

Int range lo0, e0/0-1

Ip ospf 10 area 0

Exit

wr

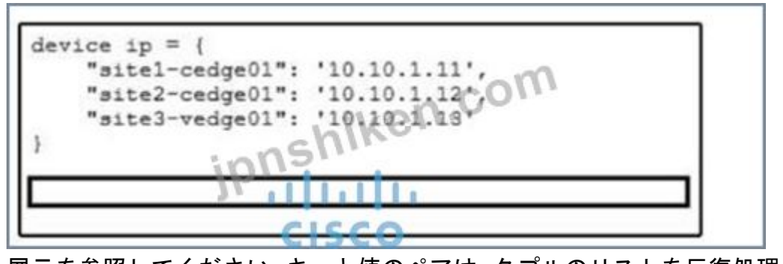
R2

Router ospf 10

Area 10 range 10.1.0.0 255.255.0.0

exit
wr
R3
Router ospf 10
Area 10 range 10.2.0.0 255.255.0.0
Exit
Wr
OR

質問: **48**
REST APIでは、OAuthフレームワークはどのように使用されますか？
A. 外部アプリケーションにアカウントへのアクセスを許可するトークンを提供することによって
B. REST URL内のセキュリティ情報を隠蔽するためのフレームワークとして
C. REST URL内のセキュリティ情報をハッシュ化するためのフレームワークとして
D. 外部アプリケーションにユーザー認証情報を提供することにより
正解: **(**正解を表示します**)**
The correct answer is A. by providing the external application a token that authorizes access to the account.
In REST APIs, OAuth is used as an authorization framework. Instead of giving the external application the user's actual username and password, the user or authorization server provides the application with an access token. That token allows the application to access specific resources based on the permissions granted.
This is the main purpose of OAuth:
* Authorize access
* Use tokens instead of exposing credentials
* Allow controlled, limited access to resources
* B. as a framework to hide the security information in the REST URL OAuth does not work by hiding information in the URL. It is an authorization framework based on tokens.
* C. as a framework to hash the security information in the REST URL OAuth is not a URL-hashing mechanism. Hashing and OAuth are different concepts.
* D. by providing the user credentials to the external application This is the opposite of OAuth's purpose.
OAuth is designed so that the external application does not need the user's credentials.
Remember this difference:
* Basic Authentication # sends username/password
* OAuth # uses token-based authorization
OAuth = token-based delegated access

質問: **49**


展示を参照してください。キーと値のペアは、タプルのリストを反復処理して抽出する必要があります。スニペットを完成させ、各キーと値のペアをタプルとして出力する文はどれですか？

A. デバイスの場合、値 device_ip.items() 内: print(device)
B. デバイスの場合、deviceip: print(device)
C. device_ip.items() 内のデバイスの場合: print(device)
D. device_ip.values() 内のデバイスの場合: print(device)
正解: **(**正解を表示します**)**

質問: **50**
ユーザーまたはデバイスの ID に基づいてネットワーク接続を許可または拒否する機能を提供する IEEE 標準はどれですか?
A. 802.1w
B. 802.1d
C. 802.1x
D. 802.1q
正解: **(**正解を表示します**)**

質問: **51**
マルチベンダー環境でデータ モデルを活用する利点は何ですか?
A. バイナリエンコードプロトコルによる通信セキュリティの向上
B. 構成と実行時状態データの区別を削除する
C. 構成と管理への統一されたアプローチの促進
D. 管理対象デバイスにかかるCPU負荷を軽減
正解: **(**正解を表示します**)**

質問: **52**
エンジニアは EAP を使用して RADIUS ベースの認証を構成しています。MS-CHAPv2 はクライアント デバイス上で構成されます。この認証タイプをサポートするには、ISE でどのアウター メソッド プロトコルを設定する必要がありますか?
A. LDAP
B. EAP-FAST
C. EAP-TLS
D. PEAP
正解: **(**正解を表示します**)**

質問: **53**
FHRP と SSO の違いは何ですか?
A. FHRP は帯域幅の割り当てに影響し、SSO はルーティングの決定に影響します。
B. FHRPはゲートウェイの冗長性を提供し、SSOは単一デバイス内でのフェイルオーバーを提供します。
C. FHRP は単一のデバイス内で状態情報を維持し、SSO は複数のデバイス間で状態情報を管理します。
D. FHRP は冗長性のために OTV を使用し、SSO は状態同期のために VXLAN を使用します。
正解: **(**正解を表示します**)**

質問: **54**

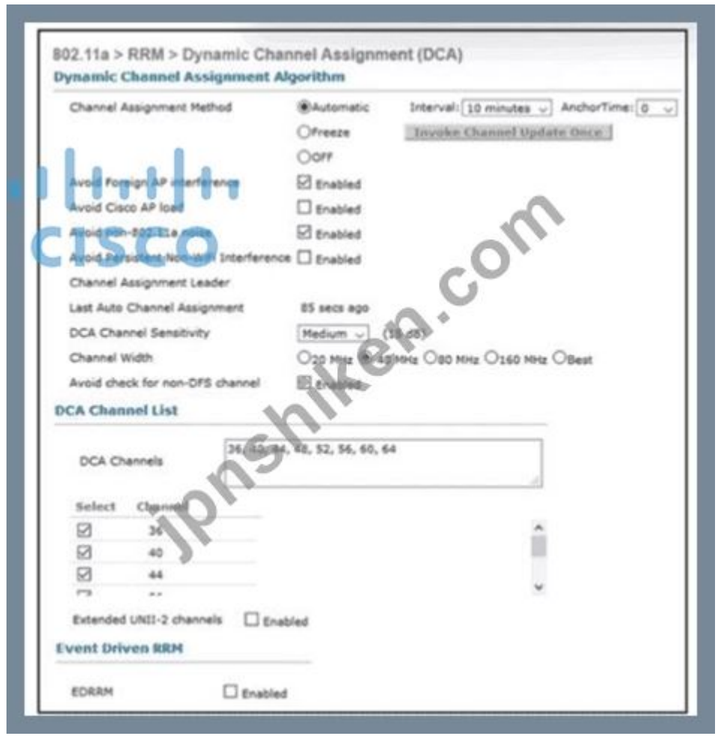
それぞれの特定の WLAN に適用されるプロパティを定義するタグはどれですか?
A. サイトタグ
B. APタグ
C. RFタグ
D. ポリシータグ
正解: **D** (コメントを発表する)

質問: **55**
プッシュ モデルで機能し、Python や Ruby などの言語をサポートし、ホストごとにエージェントをインストールする必要がないツールはどれですか。
A. アンシブル
B. ソルトスタック
C. 人形
D. シェフ
正解: **A** (コメントを発表する)

質問: **56**
Cisco Catalyst Center (旧 DNA Center) および vManage ノースバウンド API の特徴は何ですか?
A. 構成の変更をデバイスにプッシュします。
B. NETCONF プロトコルを実装します。
C. XML 形式のコンテンツを交換します。
D. RESTCONF プロトコルを実装します。
正解: (正解を表示します)

質問: **57**
ステートレス認証と承認は、REST API 呼び出しにどのセキュリティ機能を使用しますか?
A. クッキーベースのセッション認証
B. SSL/TLS 証明書の暗号化
C. OAuth 2 トークン
D. API キー
正解: (正解を表示します)

質問: **58**



展示を参照してください。エンジニアは、5 GHz 帯域での非 Wi-Fi 干渉に関する問題のトラブルシューティングを行っています。エンジニアは Cisco CleanAir を有効にし、適切なトラップを設定しましたが、AP は重大な干渉を検出してもチャネルを変更しません。どのアクションでこの問題を解決できますか。

A. イベント駆動型無線リソース管理オプションを有効にする

B. 持続的な非WiFi干渉を回避するオプションを有効にする

C. DCA感度オプションを高に変更します

D. 外部 AP 干渉を回避するオプションを無効にします。

正解: **A** (コメントを発表する)

質問: **59**

基本的なAPI認証において、スニファ攻撃から認証情報を保護するセキュリティオプションはどれですか？

A. クライアントとサーバー間のVPN接続

B. 通信にはTLSまたはSSLを使用します。

C. APIを認証するためのAAAサービス

D. 次世代ファイアウォール

正解: (正解を表示します)

The correct answer is B. TLS or SSL for communication.

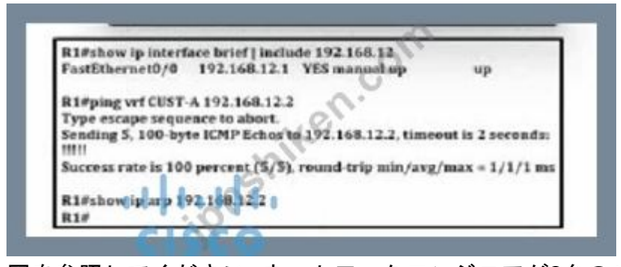
In basic API authentication, credentials (such as username and password) are often transmitted using Base64 encoding, which is not encrypted. This makes them vulnerable to sniffer (packet capture) attacks if sent over an unencrypted channel.

* TLS (Transport Layer Security) and its predecessor SSL provide encryption of the communication channel.

* This ensures that even if packets are captured, the credentials remain confidential and unreadable.

* Cisco documentation emphasizes that APIs (RESTCONF, HTTP-based APIs) should use HTTPS (HTTP over TLS) to secure credentials in transit.
* A. VPN connection between client and server While a VPN encrypts traffic, it is not specifically required for API authentication security. The standard and expected method is TLS/HTTPS.
* C. AAA services to authenticate the API AAA controls who can access, but it does not encrypt credentials in transit.
* D. next-generation firewall A firewall provides traffic filtering and threat protection but does not directly secure credential transmission in basic API authentication.
* Basic Authentication = NOT secure by itself
* Always pair it with HTTPS (TLS encryption)
Rule to remember:
If credentials travel over the network # encrypt with TLS

質問: **60**



図を参照してください。ネットワークエンジニアが2台のルーター間の接続性を確認しています。エンジニアはリモートエンドポイントにpingを実行できますが、ARPエントリを確認できません。ARPエントリが存在しないのはなぜですか？

A. インターフェイス FastEthernet0/0 は VRF CUST-A に設定されているため、ARP エントリもその VRF にあります。
B. VRF が使用される場合、グローバル ルーティング テーブルで ARP プロトコルが無効になります。
C. VRFを使用する場合、各VRFでARPプロトコルを有効にする必要があります。
D. ping コマンドはグローバルルーティングテーブルで実行する必要があります。
正解: **(**正解を表示します**)**
The correct answer is A. Interface FastEthernet0/0 is configured in VRF CUST-A, so the ARP entry is also in that VRF.
In Cisco VRF implementations, ARP entries are maintained separately per VRF, not in the global routing table. Cisco documentation states that with Multi-VRF CE, ARP entries are learned in separate VRFs, and the user can display them for a specific VRF. Cisco also documents the command show ip arp vrf < vrf-name > to display the ARP table for a specified VRF.
That means if the interface belongs to VRF CUST-A, a normal global show ip arp 192.168.12.2 may not display the entry, even though ping vrf CUST-A 192.168.12.2 succeeds. The ARP entry exists, but it is stored under the CUST-A VRF ARP table, not the global ARP table.
* B. When VRFs are used, ARP protocol is disabled in the global routing table. This is incorrect. ARP is not disabled; it is simply VRF-aware and tracked separately per VRF.
* C. When VRFs are used, ARP protocol must be enabled in each VRF. This is incorrect. There is no separate requirement to manually enable ARP in each VRF for normal operation in this context.
* D. The ping command must be executed in the global routing table. This is incorrect because Cisco supports pinging within a specific VRF, and the exhibit already shows the use of ping vrf CUST-A .
ENCOR exam point:
With VRF-aware services, always remember:
* Routing table = per VRF
* ARP table = per VRF
* Verification commands often require the VRF keyword

質問: **61**
ネットワークの音声アプリケーションに推奨される最小 SNR はどれくらいですか?

A. 15
B. 20
C. 25
D. 10
正解: **C** (コメントを発表する)

質問: **62**
管理者がトラブルシューティングに使用する pcap ファイルを生成できる AP モードはどれですか?
A. Local
B. Monitor
C. Sniffer
D. H-REAP
正解: (正解を表示します)

質問: **63**
ある企業が最近、NETCONFの代わりにRESTCONFを使用することを決定しました。多くのNETCONFスクリプトには、<edit-config> (create)という操作が含まれています。これらのステートメントを置き換えるには、どのRESTCONF操作を使用する必要がありますか？
A. GET
B. CREATE
C. PUT
D. POST
正解: (正解を表示します)

質問: **64**
次世代ファイアウォールには搭載されているが、従来のファイアウォールには搭載されていないセキュリティメカニズムはどれですか？
A. 統合IPS
B. ステートフルファイアウォールポリシー
C. SSL VPN
D. NAT
正解: **A** (コメントを発表する)
The correct answer is A. integrated IPS.
A traditional firewall provides:
* Stateful inspection
* Basic ACL filtering
* NAT
* Sometimes VPN services

A Next-Generation Firewall (NGFW) adds advanced capabilities such as:
* Integrated Intrusion Prevention System (IPS)
* Application awareness and control
* Advanced malware protection
* Integrated IPS (Intrusion Prevention System) is a defining feature of NGFWs.
* It allows the firewall to:
* Detect and block known and unknown threats
* Perform deep packet inspection
* Stop attacks in real time
This capability is not part of traditional firewalls, which only inspect traffic based on state and basic rules.
* B. Stateful firewall policies This is a core feature of traditional firewalls, not unique to NGFWs.
* C. SSL VPN VPN functionality exists in both traditional and next-generation firewalls.
* D. NAT NAT is a basic firewall/network feature, not exclusive to NGFWs.
Remember the distinction:
* Traditional Firewall # Stateful filtering, NAT, VPN
* Next-Generation Firewall # Adds IPS + Application Awareness + Advanced Security NGFW = Traditional Firewall + Advanced Threat Protection

質問: **65**
vBond は Cisco SD-WAN ソリューションのどのレベルで動作しますか?
A. 管理プレーン
B. コントロールプレーン
C. データプレーン
D. オーケストレーションプレーン
正解: **(**正解を表示します**)**

質問: **66**
特定の距離における RF 信号振幅の低下を表す RF 値はどれですか?
A. 信号対雑音比
B. 自由空間パス損失
C. 受信信号強度インジケータ
D. 有効等方放射電力
正解: **B (**コメントを発表する**)**

質問: **67**
CAPWAPの検出および参加プロセス中に、複数のWLCがCISCO_CAPWAP-CONTROLLER.localdomainホスト名に応答すると、LAPは何を送信しますか？
A. すべてのWLCへの参加リクエスト
B. 各WLCへのユニキャスト検出要求
C. ドメイン名を解決する最初のWLSへのユニキャスト検出要求
D. ブロードキャスト検出リクエスト
正解: **C (**コメントを発表する**)**

質問: **68**
DNS を使用してワイヤレス LAN コントローラの IP アドレスを解決するには、アクセス ポイントにどの A レコード タイプを設定する必要がありますか?
A. CISCO-CAPWAP-CONTROLLER.localdomain
B. CISCO.CONTROLLER.localdomain
C. CISCO-CONTROLLER.localdomain
D. CISCO.CAPWARCONTROLLERJocaldomain
正解: **A** (コメントを発表する)

質問: **69**
統合ワイヤレス展開ではレイヤー 3 ローミングはどのように実現されますか?
A. 新しいコントローラは、新しいサブネットからクライアントに IP アドレスを割り当てます。
B. 元のコントローラー上のクライアント エントリが新しいコントローラー上のデータベースに渡されます。
C. 元のコントローラ上のクライアント データベースはアンカー エントリで更新され、新しいコントローラ データベースは外部エントリで更新されます。
D. クライアントとアンカー コントローラの間に EoIP トンネルが作成され、クライアントが新しい AP に関連付けられるとシームレスな接続が実現します。
正解: **C** (コメントを発表する)

質問: **70**
ルーターのWANインターフェースに適用されるアウトバウンドアクセスリストのうち、IPアドレス10.10.10.1を持つワークステーションからのHTTPトラフィックを除くすべてのトラフィックを許可するものはどれですか？
A. ip access-list extended 100
tcp host 10.10.10.1 any eq 80 を拒否します
ip any any を許可する
B. ip access-list extended 10
tcp host 10.10.10.1 any eq 80 を拒否します
ip any any を許可する
C. IPアクセスリスト拡張 NO_HTTP
tcp host 10.10.10.1 any eq 80 を拒否します
D. ip access-list extended 200
tcp host 10.10.10.1 eq 80 any を拒否します
ip any any を許可する
正解: **(**正解を表示します**)**
The correct answer is A.
* Block HTTP traffic (TCP port 80)
* Source: 10.10.10.1
* Destination: any
* Permit all other traffic
ip access-list extended 100
deny tcp host 10.10.10.1 any eq 80
permit ip any any
* deny tcp host 10.10.10.1 any eq 80 # Blocks HTTP traffic from 10.10.10.1 to any destination

* permit ip any any # Allows all other traffic
This perfectly matches the requirement.
* B. ip access-list extended 10 # Invalid - extended ACLs use ranges 100-199 or named ACLs, not 10
* C. ip access-list extended NO_HTTP # Missing permit ip any any # implicit deny all at the end blocks everything
* D. deny tcp host 10.10.10.1 eq 80 any # Incorrect syntax/order
* eq 80 is applied to destination port, not source
* This line is malformed and does not match HTTP filtering correctly
ACL evaluation rules:
* Top-down processing
* First match wins
* Implicit deny all at the end
Correct pattern for "block one thing, allow rest":
deny < specific traffic >
permit ip any any

質問: 71
OSPFとEIGRPの違いは何ですか？
A. OSPFはIPプロトコル番号88を使用します。EIGRPはIPプロトコル番号89を使用します。
B. OSPF はデフォルトのハロータイマーとして 5 秒を使用します。EIGRP はデフォルトのハロータイマーとして 10 秒を使用します。
C. OSPF は管理距離 115 を使用します。EIGRP は管理距離 160 を使用します。
D. OSPF はマルチキャストアドレス 224.0.0.5 と 224.0.0.6 を使用します。EIGRP はマルチキャストアドレス 224.0.0.10 を使用します。
正解: D (コメントを発表する)
The correct answer is D.
OSPF and EIGRP use different multicast addresses for exchanging routing information:
* OSPF uses:
* 224.0.0.5 # AllSPFRouters
* 224.0.0.6 # AllDRouters
* EIGRP uses:
* 224.0.0.10
This is a well-known operational difference between the two protocols and is commonly tested in Cisco ENCOR.
* A. OSPF uses IP protocol number 88. EIGRP uses IP protocol number 89. This is reversed.
* EIGRP = IP protocol 88
* OSPF = IP protocol 89
* B. OSPF uses a default hello timer of 5 seconds. EIGRP uses a default hello timer of 10 seconds. This is incorrect.
* On most broadcast and point-to-point networks, OSPF default hello = 10 seconds
* EIGRP default hello = 5 seconds on high-speed links
* C. OSPF uses an administrative distance of 115. EIGRP uses an administrative distance of 160. This is also incorrect.
* OSPF AD = 110
* EIGRP internal AD = 90
* EIGRP external AD = 170
Memorize these protocol identifiers:

* OSPF
* Protocol number: 89
* Multicast: 224.0.0.5 / 224.0.0.6
* EIGRP
* Protocol number: 88
* Multicast: 224.0.0.10

質問: **72**
YANG データ モデルで使用される 2 つのプロトコルはどれですか? (2 つ選択してください。)
A. HTTPS
B. SSH
C. TLS
D. RESTCONF
E. NETCONF
正解: **D,E (コメントを発表する)**

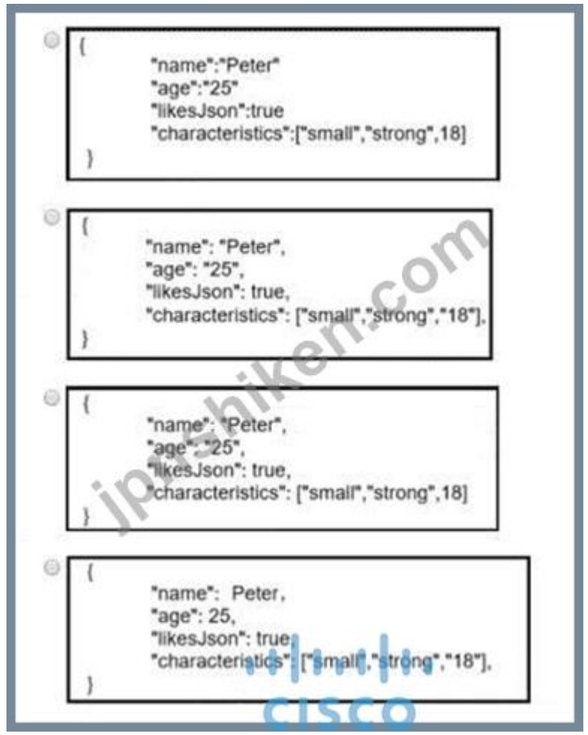
質問: **73**
Wi-Fi デバイスの総出力エネルギーを測定するために何が使用されますか?
A. dBm
B. EIRP
C. mW
D. dBi
正解: **(正解を表示します)**

質問: **74**
エンジニアが設定済みのチャネルをスキャンして不正なアクセスポイントを探すことができるAPモードはどれですか。
A. スニファ
B. ブリッジ
C. モニター
D. ローカル
正解: **C (コメントを発表する)**

質問: **75**
インターネット エッジで次世代ファイアウォールを使用することで導入される 2 つの新しいセキュリティ機能はどれですか?
（2つ選択してください。）
A. 統合侵入防止
B. NAT
C. アプリケーションレベルの検査
D. VPN
E. ステートフルパケットインスペクション

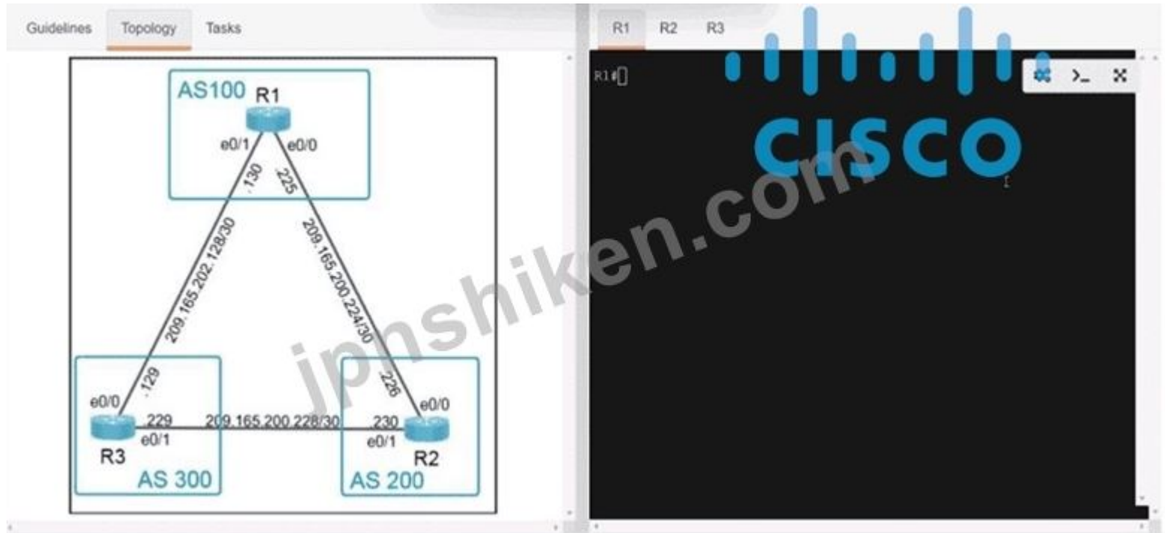
正解: (正解を表示します)

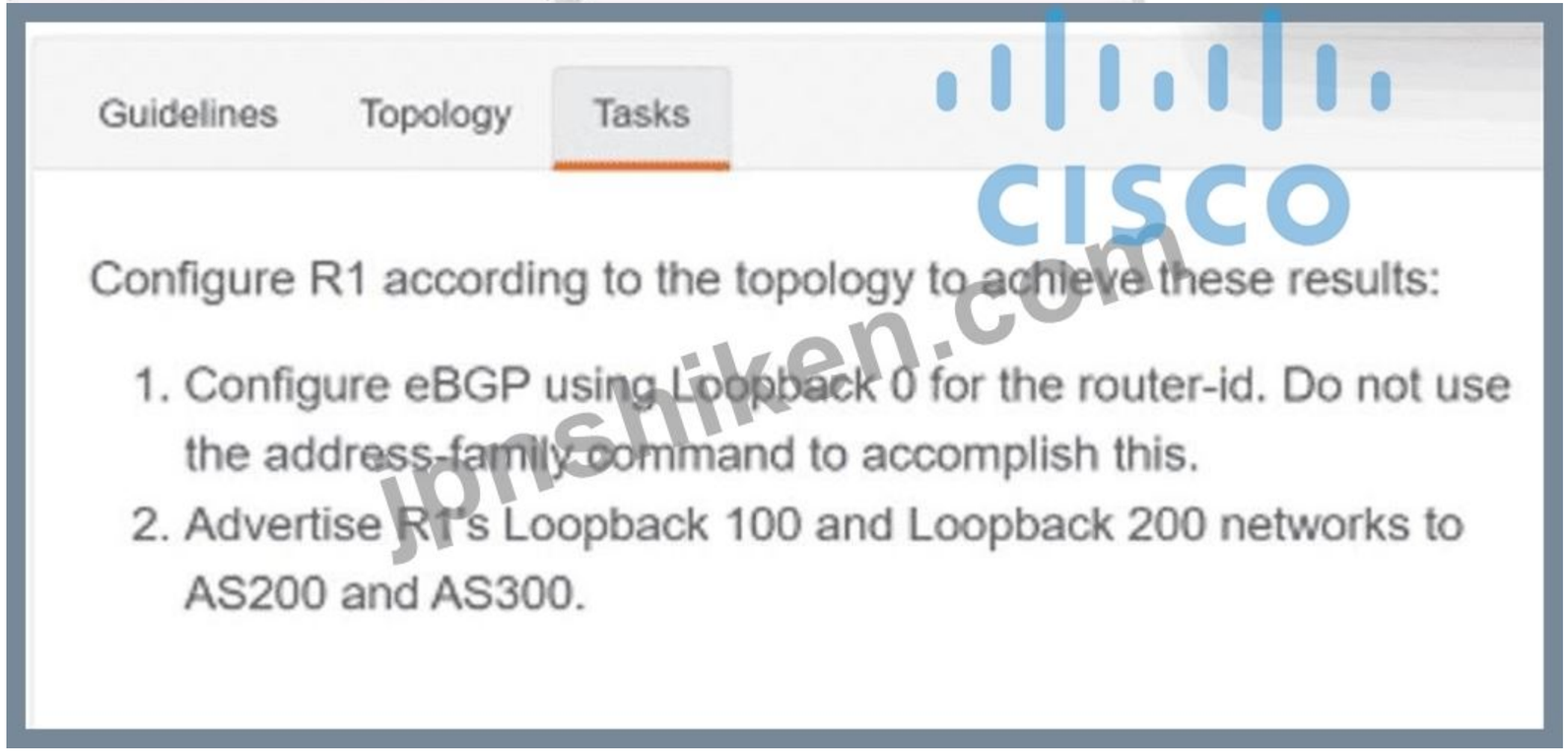
質問: **76**
どのデータが JSON で適切にフォーマットされていますか?



A. オプションD
B. オプションA
C. オプションC
D. オプションB
正解: (正解を表示します)

質問: **77**





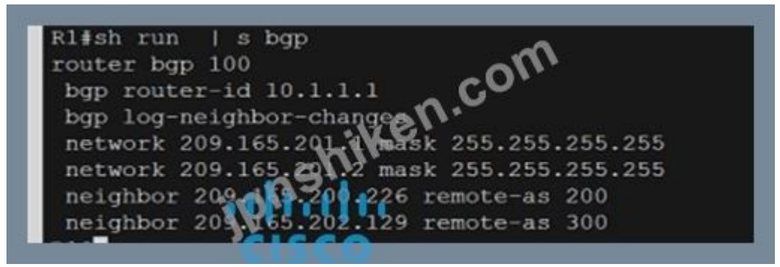
正解:

See the solution below in Explanation:

Explanation:

Solution:

Solution on R1:



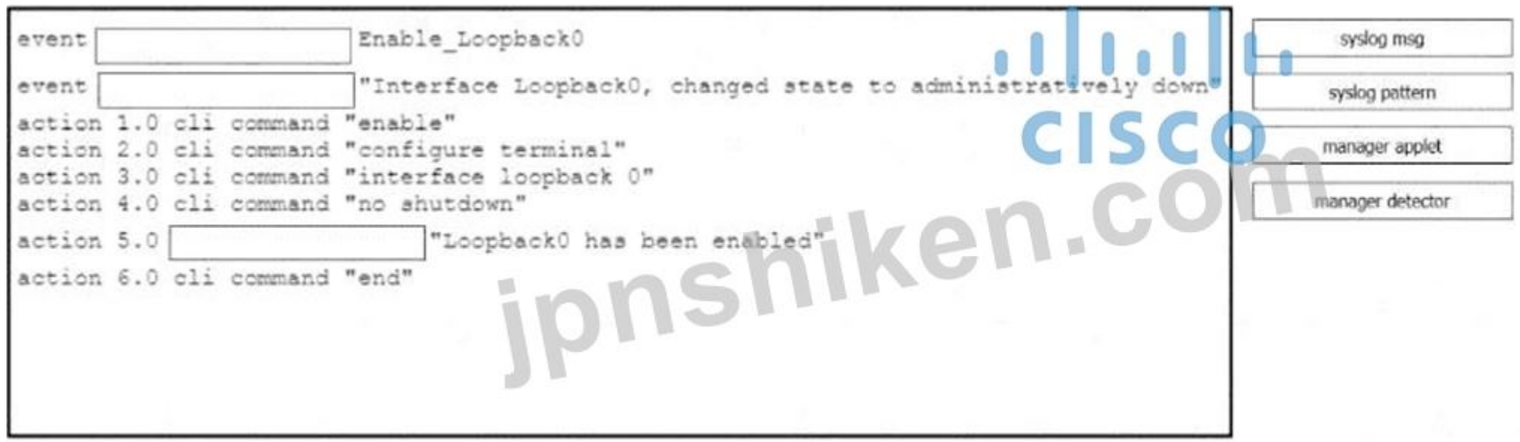
R1# copy run start

Verification:

OR

質問: **78**

右側のコマンド スニペットを設定内の空白部分にドラッグ アンド ドロップして、インターフェイス Loopback0 を有効にし、"Interface Loopback0. changed state to Administratively down"というログ メッセージを受信したときにメッセージをログに記録する EEM アプレットを作成します。すべてのコマンドが使用されるわけではありません。



正解:

Explanation:

質問: **79**
データモデリング言語はどのように使用されますか?
A. 変更できない有限かつ明確に定義されたネットワーク要素を表す
B. インフラストラクチャ内の非構造化データの流れをモデル化する
C. スクリプト言語に人間が読める形式を提供する
D. データを簡単に構造化、グループ化、検証、複製できるようにする
正解: **D** (コメントを発表する)

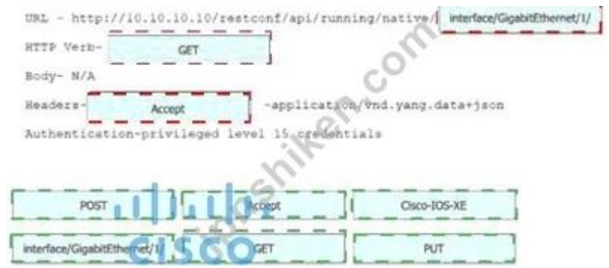
質問: **80**
SSOはHSRPとどのように連携して、ネットワークの中断を最小限に抑えますか。
A. HSRPが同じデバイス上のスタンバイRPにフェイルオーバーできるようにします。
B. HSRPがグループ内の別のスイッチをアクティブなHSRPスイッチとして選択できるようにします。
C. リンク障害が発生した場合の高速フェイルオーバーを保証します。
D. スイッチオーバー後の既知のルートに沿ったデータ転送を有効にします。ルーティングプロトコルが再収束します。
正解: (正解を表示します)

質問: **81**
Cisco SD-Access 拡張ノードはどのような機能を実行しますか?
A. 非ファブリック非管理ノードとのレイヤ3隣接関係を確立する役割を担う
B. ファブリックを拡張し、下流のファブリック非対応レイヤー2スイッチに接続するために使用されます。
C. リモート登録と構成を通じて非ファブリックデバイスにファブリック拡張を提供します。
D. ファブリックデバイスと非ファブリックデバイス間のトンネリングを実行し、未知のネットワークを介してトラフィックをルーティングします。
正解: (正解を表示します)

質問: **82**

添付資料を参照してください。スニペットをRESTCONFリクエストにドラッグ＆ドロップして、このレスポンスを返すリクエストを作成してください。すべてのオプションが使用されるわけではありません。

正解:



Explanation:

質問: **83**

```
Edge-3#show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf     Hold-time  Capability      Port ID
Core-SW.cisco.lab   Gi0/3          120        R               Gi0/3
Edge-2.cisco.lab    Gi0/2          120                        Gi0/2
Edge-1.cisco.lab    Gi0/1          120                        Gi0/1

Total entries displayed: 3
================================================================================
================================================================================
u2= []
client = paramiko.SSHClient()
client.load_system_host_keys()
client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
client.connect(192.168.1.1, port=22, username='cisco', password='cisco', allow_agent=False)
stdin, stdout, stderr = client.exec_command('show lld neighbors\n')
u = 0
for u in stdout:
    if 'Router' not in u and 'Capability' not in u and 'Repeater' not in u:
        if 'Device ID' not in u and 'displayed' not in u:
            u101 = u.split()
            if len(u101) != 0:
                u2.append(u101)
```

展示を参照してください。このコードは何を実現するのでしょうか？

A. LLDPネイバーとその機能のリストを生成します。

B. リピーター機能を持つルーターのリストを生成します。

C. LLDP ネイバーのカウントを生成します。

D. LLDP ネイバーのホスト名のみを含むリストを生成します。

正解: **D** (コメントを発表する)

質問: **84**

Cisco SD-Access ネットワーク アーキテクチャでは、どのアクセス レイヤーのケーブル配線設計がアンダーレイ ネットワークに最適ですか?

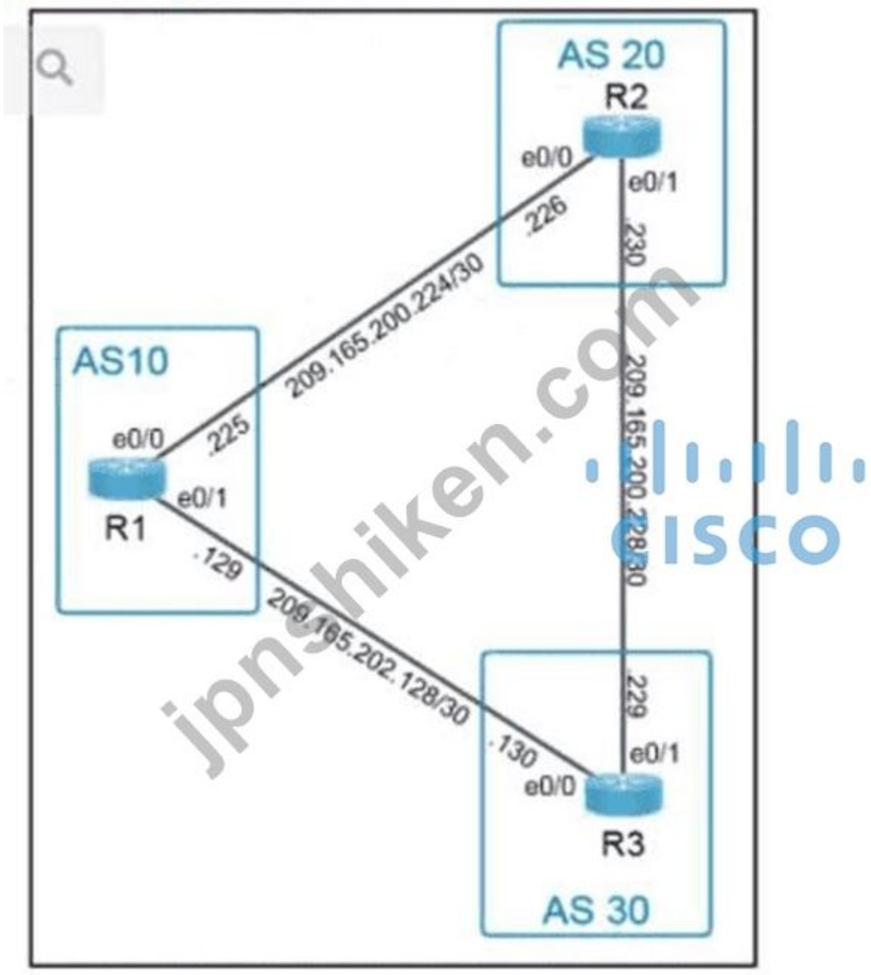
A. スイッチは各上流ディストリビューションおよびコアデバイスに接続されます。
B. スイッチは同じ層でクロスフィンされており、各上流配電装置に単一の接続があります。
C. スイッチは、同じレイヤーのデバイスと上流および下流のデバイスにクロスリンクされます。
D. スイッチは各上流配布デバイスに接続されます。
正解: **(**正解を表示します**)**

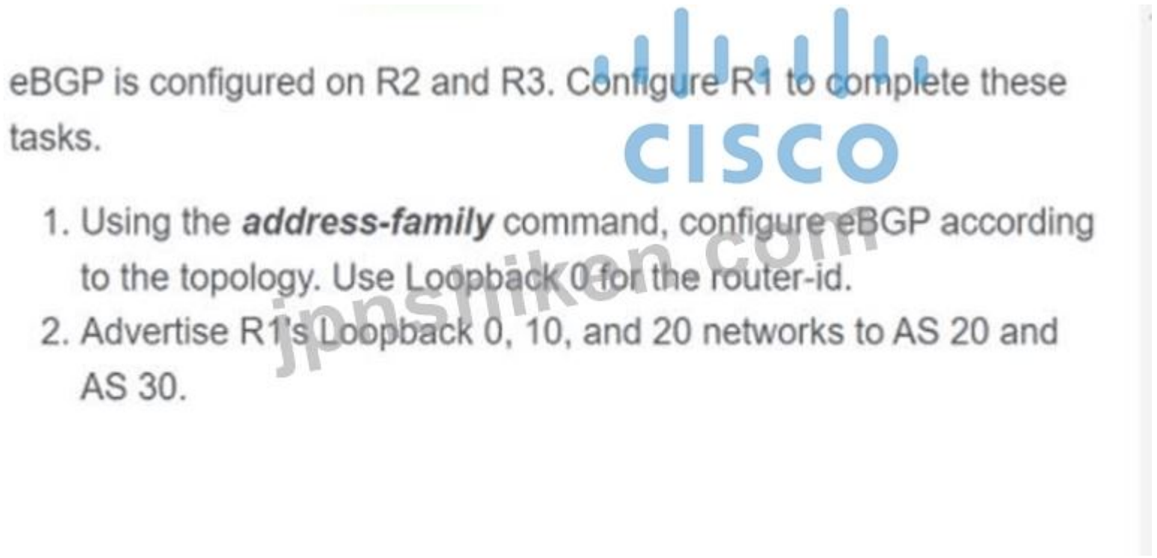
質問: **85**
Cisco SD-Accessアーキテクチャにおけるオーバーレイネットワークの特徴は何ですか？
A. アンダーレイネットワークでレイヤ2フラッディング機能を有効にするためにマルチキャストをサポートします。
B. ネットワークを維持するために使用される、物理的なルーターとスイッチのグループで構成されています。
C. 従来のルーティングアクセス設計を使用して、ネットワークのパフォーマンスと高可用性を提供します。
D. 仮想ネットワーク間の分離と物理ネットワークからの独立性を提供します。
正解: **(**正解を表示します**)**
The correct answer is D. It provides isolation among the virtual networks and independence from the physical network.
Cisco SD-Access is based on two main layers:
* Underlay network # Physical infrastructure (routers, switches, IP connectivity)
* Overlay network # Virtualized logical network built on top of the underlay According to Cisco ENCOR architecture principles, the overlay network:
* Uses technologies like LISP (control plane) and VXLAN (data plane)
* Creates virtual networks (VNs) for segmentation
* Provides end-to-end logical separation (macro-segmentation)
* Is independent of the physical topology
* Enables scalable and flexible network design
Thus, the overlay abstracts the complexity of the underlay and ensures isolation between different user groups, departments, or tenants.
* Directly describes virtual network segmentation
* Matches Cisco's definition of overlay abstraction and independence
* Core principle of SD-Access fabric design
* A. Multicast and Layer 2 flooding relate more to underlay or legacy designs, not overlay behavior.
* B. Describes the underlay network (physical devices), not overlay.
* C. Refers to traditional network design, which SD-Access replaces.
* Underlay = Physical IP network (reachability)
* Overlay = Virtual segmentation & policy (VXLAN + LISP)
Overlay = Abstraction + Segmentation + Independence

質問: **86**
従来のネットワーク要素とコントローラ層間の通信を提供する Cisco SD-Access コンポーネントはどれですか (2 つ選択してください)。
A. ファブリックオーバーレイ
B. パートナーエコシステム
C. ネットワーク制御プラットフォーム
D. ネットワークデータプラットフォーム
E. ネットワークアンダーレイ

正解: (正解を表示します)

質問: **87**





正解:
See the solution below in Explanation:
Explanation:
Solution:
router bgp 10
bgp router-id 10.1.1.111
no bgp defa ipv4-unicast
nei 209.165.200.226 remote-as 20
nei 209.165.202.130 remote-as 30
address-family ipv4
neigh 209.165.200.226 activate
neigh 209.165.202.130 activate
network 10.1.1.10 mask 255.255.255.255
network 209.165.201.10 mask 255.255.255.255
network 209.165.201.20 mask 255.255.255.255
wr

質問: **88**
Cisco Catalyst SD-WAN ネットワークのデータ プレーン セキュリティを提供する機能はどれですか?
A. IPsec
B. IPS
C. TLS/DTLS
D. SSH
正解: **(**正解を表示します**)**

質問: **89**
FlexConnect モードで動作する AP の特性は何ですか?
A. このモードでは、AP クライアントに対して Dot1x 認証はサポートされません。
B. クライアント認証は常に A P で実行されます。
C. FlexConnect グループは 802.11 r 高速ローミングをサポートする必要があります。
D. 設定はコントローラではなく AP 上で直接行われます。
正解: **D** (コメントを発表する)

質問: **90**
展示品を参照してください。

```
with manager.connect(host=192.168.0.1, port=22,
                     username='admin', password='password1', hostkey_verify=True,
                     device_params={'name':'nexus'}) as m:
```

コードスニペットは何を達成するのでしょうか?
A. Cisco Nexus デバイスへの一時的な接続を作成し、API 呼び出しに使用するトークンを取得します。
B. 保存されている SSH キーを使用して SSH 接続を作成し、パスワードは無視されます。
C. ホストキーが正しい場合、トンネルを開き、ログイン情報をカプセル化します。
D. Cisco Nexus デバイスへの ncclient 接続を開き、コンテキストの期間中それを維持します。
正解: **D** (コメントを発表する)

質問: **91**
Cisco StackWise プライマリ スイッチの役割が失われるのはいつですか?
A. スタックメンバーのプライオリティ値がより高い値に変更されたとき
B. スタックプライマリがリセットされたとき
C. より高い優先度のスイッチがスタックに追加された場合
D. スタックメンバーに障害が発生した場合
正解: (正解を表示します)

質問: **92**
Cisco SD-Accessソリューションにおいて、Anycast Gatewayサービスを提供するコンポーネントはどれですか？
A. ファブリック境界ノード
B. コントロールプレーンノード
C. 中間ノード
D. ファブリックエッジノード
正解: (正解を表示します)

The correct answer is D. fabric edge node.
In Cisco SD-Access, the Anycast Gateway provides a consistent default gateway for endpoints across the fabric. This allows endpoints to keep the same gateway behavior regardless of where they attach within the fabric.
The fabric edge node provides the Anycast Gateway service for connected endpoints. It is the node where endpoints attach to the fabric, and it performs the first-hop gateway function using the distributed Anycast Gateway model.
This design provides:
* Consistent default gateway addressing
* Simplified endpoint mobility
* Optimal forwarding within the fabric
* Distributed first-hop gateway services
* A. fabric border node The border node connects the SD-Access fabric to external networks. It does not provide the endpoint Anycast Gateway service.
* B. control plane node The control plane node maintains host tracking and endpoint-to-location mappings using LISP. It is not the default gateway for endpoints.
* C. intermediate node An intermediate node only forwards traffic inside the fabric underlay/overlay path and does not provide gateway services to endpoints.
Remember these SD-Access roles:
* Fabric edge node = endpoint connectivity + Anycast Gateway
* Control plane node = endpoint mapping database
* Border node = external connectivity
* Intermediate node = transit forwarding
Anycast Gateway in SD-Access = Fabric Edge Node

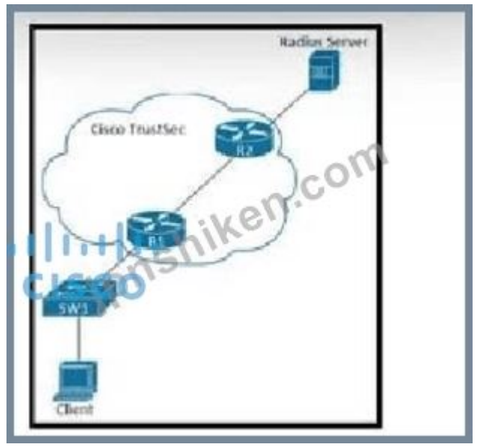
質問: 93

```
Status Code: 202
Body:
{
  "response": {
    "startTime": 1630851541471,
    "endTime": 1630851541523,
    "version": 1630851541514,
    "serviceType": "Discovery Service",
    "isError": false,
    "lastUpdate": 1630851541514,
    "progress": "1",
    "rootId": "2cbb8965-7562-7832-a4c7-88a97594411c",
    "instanceTenantId": "4cc6582496acb689cb4ca6be",
    "id": "2cbb8965-7562-7832-a4c7-88a97594411c "
  },
  "version": "1.0"
}
```


展示を参照してください。POST /discovery リクエストは非同期タスクを生成します。タスクに関する詳細情報をクエリした後、Cisco DNA Center プラットフォームは REST API レスポンスを返します。検出タスクのステータスはどうなっていますか？
A. 成功

B. 再起動しました
C. 失敗
D. 停止
正解: **A (**コメントを発表する**)**

質問: **94**
Cisco SD-Access ファブリックにおける 2 つのデバイス ロールは何ですか? (2 つ選択してください。)
A. エッジノード
B. 境界ノード
C. アクセススイッチ
D. vBondコントローラー
E. コアスイッチ
正解: **(**正解を表示します**)**

質問: **95**


図を参照してください。ネットワークデバイスアクセス制御を使用する場合、どのデバイスがサプリカントとみなされますか？
A. クライアント
B. SW1
C. RADIUSサーバー
D. R1
正解: **(**正解を表示します**)**
The correct answer is A. client.
In Cisco 802.1X / network admission control terminology, the supplicant is the endpoint device or client software requesting access to the network. Cisco documentation describes 802.1X as a client-server access control model in which the client must be authenticated before gaining ac cess, and the network device relays authentication messages between the supplicant and the authentication server.
* Client = Supplicant
* SW1 = Authenticator
* RADIUS server = Authentication server
* R1 = transit/network infrastructure device, not the supplicant

The supplicant is the device that is trying to join the network and provide credentials. In the diagram, that is the client. Cisco also defines the three 802.1X entities as supplicant system, authentication system, and authentication server system, with the supplicant being the endpoint such as a PC.
* B. SW1 SW1 functions as the authenticator, controlling access to the network port and relaying EAP messages.
* C. RADIUS server The RADIUS server is the authentication server, not the supplicant.
* D. R1 R1 is part of the network path in the figure, but it is not the device requesting admission to the network.
ENCOR exam point:
For 802.1X / NAC questions, remember this trio:
* Supplicant = endpoint/client
* Authenticator = switch or AP controlling access
* Authentication server = RADIUS / Cisco ISE

質問: 96
展示品を参照してください。

PSK を使用した WPA2-AES 用に WLAN を設定し、802.11r 対応クライアントのみが接続できるようにするには、どのアクションを実行する必要がありますか?
A. PSK と FT + PSK を有効にします。
B. Fast Transition を Adaptive Enabled に変更し、FT * PSK を有効にします。
C. 高速移行と PSK を有効にします。
D. 高速移行と FT + PSK を有効にします。
正解: **(**正解を表示します**)**

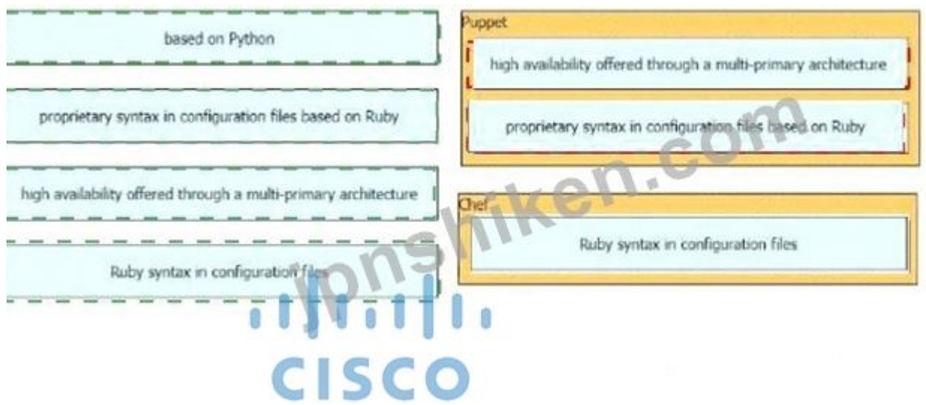
質問: 97
MAB はどのようなアクセス制御機能を提供しますか?

A. IP アドレスに基づくユーザー アクセス
Bは認証をバイパスするためにデバイスを遅くする
B. ユーザーとデバイスの同時認証
C. デバイスの物理アドレスに基づくネットワークアクセス
正解: **B** (コメントを発表する)

質問: **98**
ワイヤレスクライアントがローミングするかどうかを決定するデバイスはどれですか？
A. 無線LANコントローラー
B. ワイヤレスクライアント
C. WCSロケーションサーバー
D. アクセスポイント
正解: (正解を表示します)

質問: **99**
左側の自動化特性を右側の対応するツールにドラッグ＆ドロップします。すべてのオプションが使用されるわけではありません。

正解:



Explanation:
A screenshot of a computer AI-generated content may be incorrect.

質問: **100**
図を参照してください。requestsモジュールを使用してネットワークデバイスと通信するこのPythonスクリプトを実行すると、どのような結果が予想されますか？
A. このスクリプトは、デバイスの API エンドポイントに HTTP リクエストを送信することで、デバイス情報を取得します。
B. このスクリプトは、デバイスとの安全な接続を確立することにより、ネットワークデバイスの設定を構成します。
C. このスクリプトは、ネットワークデバイスとの SSH 接続を確立します。
D. このスクリプトは、ネットワークデバイスから受信した JSON データを解析し、表形式の構造に整形します。
正解: **(**正解を表示します**)**
The correct answer is A. The script retrieves device information by sending HTTP requests to the device ' s API endpoints.
The script uses the Python requests library:
response = requests . get(url)
* This sends an HTTP GET request to:
http:// < device_ip > /api/device/info
* This indicates communication with a REST API endpoint exposed by the network device.
* Builds a URL using the device IP
* Sends an HTTP GET request to the API
* Checks if the response status code is 200 (OK)
* If successful:
return response . json()
Converts the API response into a Python dictionary
* Prints the retrieved device information
* The script is clearly performing a read operation (GET)
* It interacts with a REST API
* It retrieves device information, not configuring anything
* B. Configures device settings via secure connection # No POST/PUT/PATCH methods are used # No HTTPS or authentication shown
* C. Establishes SSH connection # No SSH libraries (like Paramiko or Netmiko) are used
* D. Parses JSON into tabular structure # It only returns and prints JSON # No formatting (like pandas
/table conversion) is performed
* requests.get() # Retrieve data (READ)
* requests.post() / put() # Modify or create data

* .json() # Converts API response into Python dictionary
Key takeaway:
REST API + GET request = data retrieval from device

質問: **101**
エンジニアは、802.11r をサポートし、ユーザーにパスフレーズの入力を要求する新しい WLAN を構成する必要があります。
この要件をサポートするには何を構成する必要がありますか?
A. FT PSKと高速遷移
B. 802.1XおよびSUITEB-1X
C. FTPSKandSUITEB-1X
D. 802.1Xと高速移行
正解: **A** (コメントを発表する)

質問: **102**
インターネット エッジに加えてデータ センターに次世代ファイアウォールを導入することで、どのような新しいセキュリティ強化が導入されますか?
A. データセンターの東西トラフィックのファイアウォール保護
B. リモート アクセス用の仮想プライベート ネットワーク
C. データセンターの南北トラフィックのファイアウォール保護
D. DDoS 保護
正解: (正解を表示します)

質問: **103**
ステートフル スイッチオーバーを実装する利点は何ですか?
A. 柔軟性
D スケーラビリティ
B. 回復力
C. モジュール性
正解: (正解を表示します)

質問: **104**
タイプ 2 ハイパーバイザーの特徴は何ですか?
A. クイック展開
B. データセンターに最適
C. ベアメタルと呼ばれる
D. 複雑な展開
正解: **A** (コメントを発表する)

質問: **105**

展示を参照してください。デバイスのデータ構造をJSON形式で保存するPythonスニペットはどれですか？

A. テキスト AI 生成コンテンツのクローズアップが正しくない可能性があります。

B. テキスト AI 生成コンテンツのクローズアップが正しくない可能性があります。

C. 白の背景に黒のテキスト、AI 生成コンテンツが正しくない可能性があります。

D. ロゴのクローズアップ、AI 生成コンテンツが正しくない可能性があります。

正解: **B** (コメントを発表する)

質問: **106**

図を参照してください。「204 No Content」という応答は、REST APIリクエストに対してどのような意味を持ちますか？

A. インターフェース ループバック 100 が設定に見つかりません。

B. インターフェース ループバック 100 は設定から削除されていません。

C. DELETE メソッドはサポートされていません。

D. インターフェース ループバック 100 が設定から削除されました。

正解: (正解を表示します)

The correct answer is D. Interface loopback 100 is removed from the configuration.

In REST-based APIs, the HTTP status code 204 No Content means that the request was successfully processed, but the server does not return a message body in the response. For a DELETE operation, this indicates that the targeted resource was deleted successfully. Cisco RESTCONF examples use standard HTTP response behavior, where successful DELETE requests can return 204 No Content to confirm that the configuration item was removed.

The exhibit shows a DELETE request for interface Loopback100. A 204 No Content response means:

* the request was accepted,

* the operation succeeded,

* and there is no response payload to return.

Therefore, Loopback100 has been removed from the configuration.

* A. Interface loopback 100 is not found in the configuration. If the resource were not found, the server would typically return 404 Not Found, not 204.

* B. Interface loopback 100 is not removed from the configuration. This is the opposite of what a successful 204 DELETE response means.

* C. The DELETE method is not supported. If DELETE were not supported, the expected response would typically be 405 Method Not Allowed, not 204.

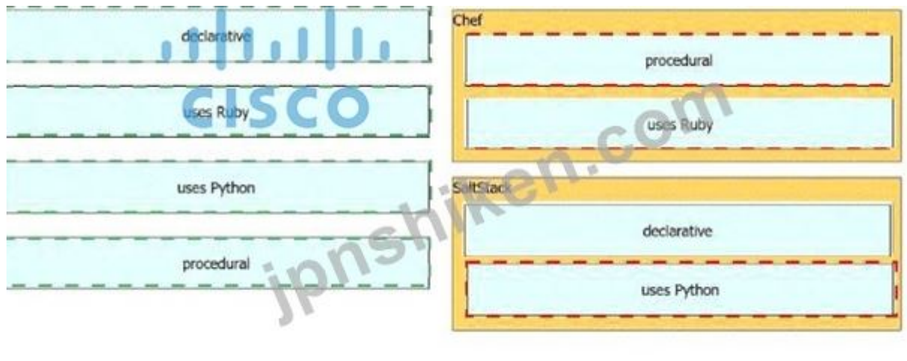
ENCOR exam point:
For Cisco automation and RESTCONF questions, remember these common HTTP meanings:
* 200 OK = successful request with content
* 201 Created = resource created
* 204 No Content = successful request with no response body, often seen with DELETE
* 404 Not Found = resource does not exist
* 405 Method Not Allowed = method not supported

質問: **107**
顧客は2台のCisco WLCを所有しており、それぞれが建物内の別々のAPを管理しています。各WLCは同じSSIDをアドバタイズしていますが、異なるインターフェースで終端しています。ユーザーから、ローミング時に接続が切断され、IPアドレスが変わるという報告を受けています。この問題を解決するには、どのような対策を講じればよいでしょうか？
A. モビリティ グループを構成します。
B. クライアント負荷分散を有効にする
C. 高可用性を構成します。
D. 高速ローミングを有効にします。
正解: (正解を表示します)

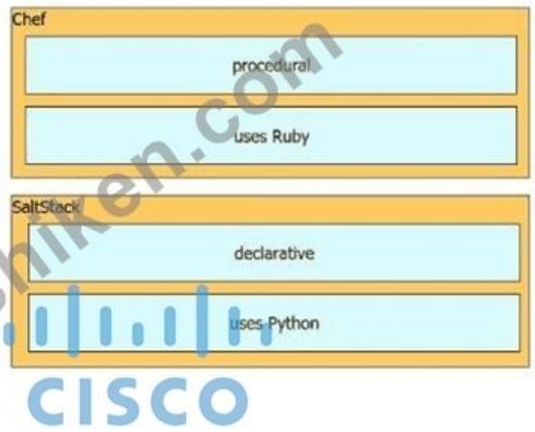
質問: **108**
SD-WAN サービスを提供するために、Cisco Catalyst SD-WAN ルータをサイトの境界にどのような形式で導入できますか?
A. ハードウェアと仮想化インスタンス
B. ハードウェア、ソフトウェア、クラウド、仮想化インスタンス
C. ハードウェア、仮想化、クラウドインスタンス
D. 仮想化されたインスタンス
正解: (正解を表示します)

質問: **109**
左側の特性を、右側で説明されているオーケストレーション ツールにドラッグ アンド ドロップします。

正解:



Explanation:



質問: **110**
主要な REST セキュリティ設計原則は何ですか?
A. パスワードハッシュ
B. フェイルセーフのデフォルト

C. OAuth
D. リクエストにタイムスタンプを追加する
正解: (正解を表示します)

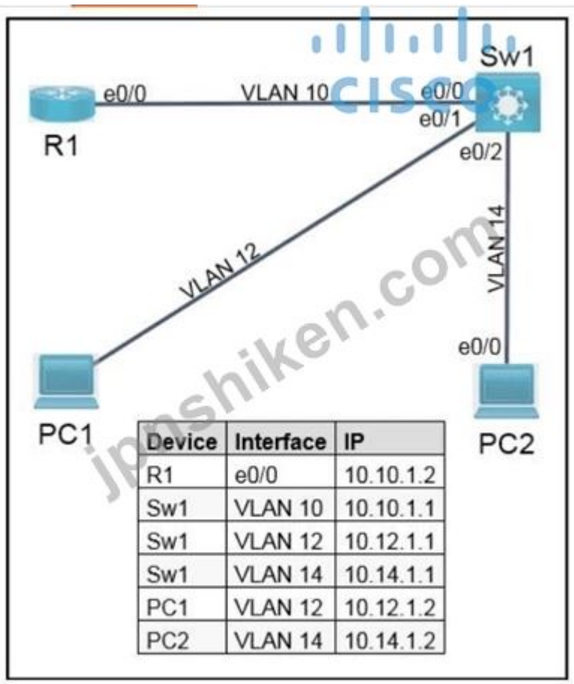
質問: **111**

図を参照してください。ユーザー認証では、まずRADIUSを使用し、RADIUSサーバーが利用できない場合はルーターのローカルデータベースにフォールバックする必要があります。この結果を得るには、どの2つの構成セットが必要ですか？
(2つ選択してください。)

A. オプションB
B. オプションD

C. オプションA
D. オプションC
正解: **(**正解を表示します**)**

質問: **112**



正解:

See the solution below in Explanation:

Explanation:

Solution:

R1

Config t

Int et0/0

Ip flow monitor Monitor-R1Flow input

Ip flow monitor Monitor-R1Flow output

Exit

Ip sla 1

Icmp-echo 10.12.1.2

Freq 300

Ip sla schedule 1 life foreve start-time now

Sw1

Config t
Monitor session 12 source vlan 12
Monitor session 12 destination interface et1/3

質問: **113**
Cisco Advanced Malware Protection for Endpoints ソリューションではどのような機能が提供されますか?
A. ネットフロー
B. トラストセック
C. DNS 保護
D. ファイルサンドボックス
正解: **(**正解を表示します**)**

質問: **114**
TrustSec でセグメンテーションを使用する利点は何ですか?
A. セキュリティ グループ タグにより、ネットワークのセグメンテーションが可能になります。
B. LAN 上のエンドポイント間で送信されるパケットは、対称キー暗号化を使用して暗号化されます。
C. ビジネス レベルのプロファイルを使用することで、ファイアウォール ルールが合理化されます。
D. 整合性チェックにより、転送中にデータが変更されるのを防ぎます。
正解: **(**正解を表示します**)**

質問: **115**
ネットワーク管理者は、キャンパス全体に新しいソフトウェア定義ファブリックを展開する準備を進めています。全体的な設計を成功させるために必要なことは何でしょうか？
A. 完全にメッシュ化されたレイヤー2トポロジー
B. 完全にメッシュ化されたレイヤー3トポロジー
C. ジャンボフレームが有効になっているポイントツーポイントのレイヤ3アンダーレイネットワーク
D. デバイス間でLACPによる冗長性を備えたポイントツーポイントレイヤ2ネットワーク
正解: **(**正解を表示します**)**
The correct answer is C. A point-to-point Layer 3 underlay network with jumbo frames enabled .
In Cisco SD-Access , the fabric is built on top of an underlay network . Cisco documentation states that the SD-Access underlay uses a structured Layer 3 foundation and a Layer 3 routed access design , where the network elements establish IP connectivity through routing rather than relying on Layer 2 adjacency. Cisco Catalyst Center LAN automation documentation also describes the underlay links as point-to-point Layer 3 routed connections .
This makes Option C the best answer because it matches the recommended SD-Access design approach:
* Point-to-point Layer 3 links in the underlay
* Routed access instead of Layer 2 campus meshing
* Jumbo frames enabled to accommodate encapsulation overhead commonly associated with fabric technologies such as VXLAN in software-defined fabrics, which is a standard design consideration in Cisco fabric deployments.
Why the other options are incorrect:
* A. A fully meshed Layer 2 topology This is not the SD-Access design model. Cisco SD-Access is not based on a campus-wide Layer 2 mesh; instead, it uses a routed Layer 3 underlay.
* B. A fully meshed Layer 3 topology SD-Access does require Layer 3 underlay connectivity, but not a fully meshed Layer 3 topology . Cisco recommends a structured routed access design , not an every- device-to-every-device full mesh.

* D. A point-to-point Layer 2 network with LACP between devices for redundancy This contradicts the SD-Access underlay principle. The underlay should be Layer 3 point-to-point , not Layer 2 point- to-point.
ENCOR exam point:
For Cisco SD-Access, remember this core design rule:
Underlay = routed, point-to-point, Layer 3 foundation
Overlay = virtualized fabric services on top of that underlay

質問: **116**
Cisco Catalyst SD-WAN アーキテクチャにおいて vSmart によって実行される機能はどれですか?
A. NAT検出とトラバーサルの容易化
B. IPsecキーの配布
C. ローカライズされたポリシーの実行
D. OMPと他のルーティングプロトコル間の再配布
正解: (正解を表示します)

質問: **117**
スニペットをコード内の空白部分にドラッグ アンド ドロップして、プライマリ ポートがダウンした場合にフェイルオーバー イーサネット ポートを起動し、プライマリがサービスに復帰したときにフェイルオーバー ポートをシャットダウンするスクリプトを作成します。すべてのオプションが使用されるわけではありません。

正解:

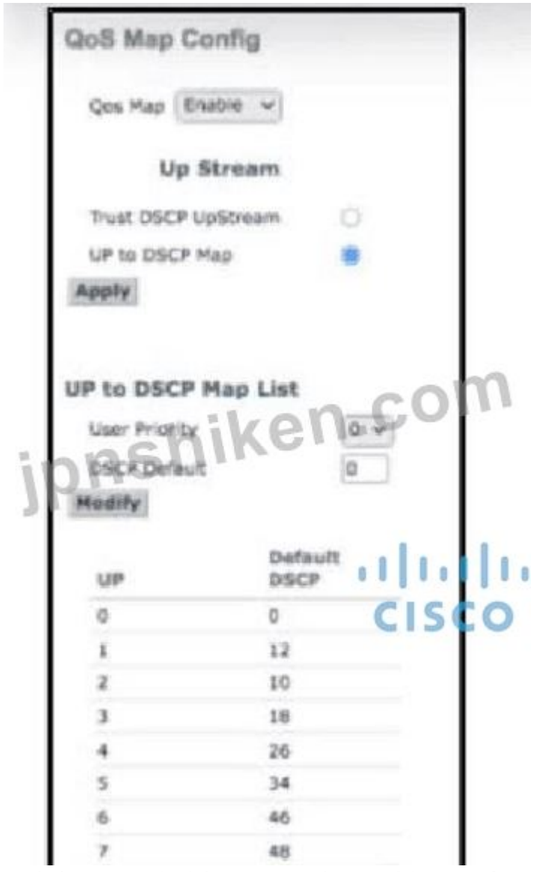
Explanation:

質問: **118**
REST API 認証の API キー オプションとは何ですか?
A. クライアントからサーバーに渡される事前に決定された文字列。
B. ローカルルータに保存されているユーザー名
C. ワンタイム暗号化トークン
D. 暗号化されずに送信される認証情報
正解: (正解を表示します)

質問: **119**
タイプ 1 ハイパーバイザーがタイプ 2 ハイパーバイザーよりも効率的なのはなぜですか?
A. タイプ 1 ハイパーバイザーは、CPU、メモリ、ストレージ、およびネットワーク リソースにアクセスするために、ホスト マシンの既存の OS に依存します。
B. タイプ 1 ハイパーバイザーは、基盤となる OS に依存せずに、ホスト マシンの物理ハードウェア上で直接実行されます。
C. タイプ 1 ハイパーバイザーでは、他のオペレーティング システムを実行できます。
D. タイプ 1 ハイパーバイザーは、ハードウェア アクセラレーション技術をサポートする唯一のハイパーバイザー タイプです。

正解: **B** (コメントを発表する)

質問: **120**



図を参照してください。エンジニアがキャンパス内の新しい建物に無線QoS設定を導入しました。すべてのネットワークデバイスは802.1p優先度タグをサポートしています。WLCの設定から何がわかりますか？

A. WLC の設定では、アクセス グループの割り当てに基づいてトラフィックの優先順位が付けられます。

B. WLC は、優先度に基づいてトラフィックを分類するために、プラチナ、ゴールド、シルバー、ブロンズのレベルを使用します。

C. WLC の設定は、アップストリーム AP から DSCP 値を継承します。

D. WLC の設定では、ユーザーデータの ToS レベルの優先度を IP 優先度レベルにマッピングします。

正解: **D** (コメントを発表する)

The correct answer is D. The WLC configuration maps user data ToS level priorities to IP precedence levels.

The exhibit shows the QoS Map feature enabled on the WLC and, under Up Stream, the option UP to DSCP Map is selected.

This means the controller is taking 802.1p User Priority (UP) values and mapping them to DSCP values for upstream traffic. Since 802.1p is a Layer 2 priority marking and DSCP/IP precedence are Layer 3 QoS markings in the IP header, the WLC is performing a priority-marking translation from user priority into IP QoS markings.

In ENCOR terms:

* 802.1p UP = Layer 2 Class of Service marking

* DSCP / IP precedence = Layer 3 QoS marking

* The WLC is configured to map UP values to DSCP values
* A. The WLC configuration prioritizes traffic based on access group assignment. This is unrelated to the exhibit. QoS mapping here is based on 802.1p UP values, not access group assignment.
* B. The WLC uses the Platinum, Gold, Silver, and Bronze levels for traffic classification based on priority. Those are older WLAN QoS profile names, but the exhibit is specifically showing UP-to- DSCP mapping, not profile-based classification.
* C. The WLC configuration inherits DSCP values from an upstream AP. This would align with Trust DSCP Upstream, but that option is not selected in the exhibit.
For wireless QoS questions, remember these mappings:
* 802.1p / CoS / UP = Layer 2 priority
* DSCP / IP precedence = Layer 3 priority
* If UP to DSCP Map is selected, the controller is converting Layer 2 priority markings into Layer 3 QoS markings.

質問: **121**
IPv4 を使用しているときに Cisco AP が WLC を検出できるようにするには、どの DNS レコード タイプが必要ですか?
A. NSレコード
B. CNAMEレコード
C. レコード
D. SOAレコード
正解: (正解を表示します)

質問: **122**
データセンターに導入される次世代ファイアウォールは何から保護するのでしょうか?
A. DMZ Web サーバーの脆弱性
B. DDoS
C. ゼロデイ攻撃
D. シグネチャベースのマルウェア
正解: (正解を表示します)

質問: **123**
エンジニアは、OSPFプロセスのトラブルによりネットワークに変化が発生した場合にSyslogメッセージを送信するEEMアプレットを作成する必要があります。エンジニアはどのようなアクションを実行すべきでしょうか？
イベントマネージャアプレット LogMessage
イベントルーティングネットワーク 172.30.197.0/24 タイプ all
A. アクション 1 syslog 送信 "OSPF ルーティング エラー」
B. アクション 1 syslog メッセージ "OSPF ルーティング エラー」
C. アクション 1 syslog 書き込み "OSPF ルーティング エラー"
D. アクション1 Syslogパターン "OSPFルーティングエラー」

正解: **(**正解を表示します**)**

質問: **124**
Cisco SD-Access ファブリックにおける 2 つのデバイス ロールは何ですか? (2 つ選択してください。)
A. 境界ノード
B. エッジノード
C. vBondコントローラー
D. アクセススイッチ
E. コアスイッチ
正解: **(**正解を表示します**)**

質問: **125**
VXLAN における VTEP の機能とはどのようなアクションですか?
A. ローカルVXLANイーサネットセグメント上で暗号化通信を許可する
B. VXLAN Ethernetフレームのカプセル化とカプセル化解除
C. IPv6からIPv4 VXLANへのトラフィックのトンネリング
D. IPv4からIPv6 VXLANへのトラフィックのトンネリング
正解: **(**正解を表示します**)**

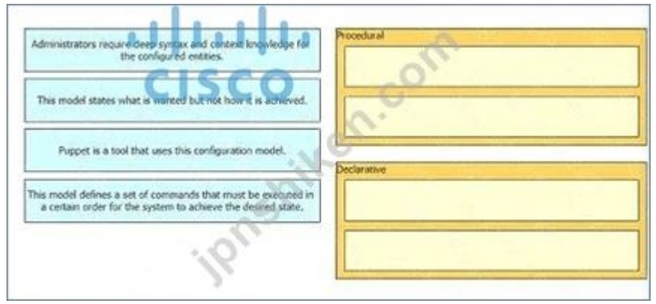
質問: **126**
REST APIセキュリティに関してJWTを説明している定義はどれですか？
A. 情報を安全に交換するために使用されるエンコードされたJSONトークン
B. 認証に使用されるエンコードされたJSONトークン
C. 認証に使用される暗号化されたJSONトークン
D. 承認に使用される暗号化されたJSONトークン
正解: **(**正解を表示します**)**

質問: **127**
管理者は次のXML文字列を使用してNETCONFを設定しています。管理者はリクエストの末尾に何を追加する必要がありますか？

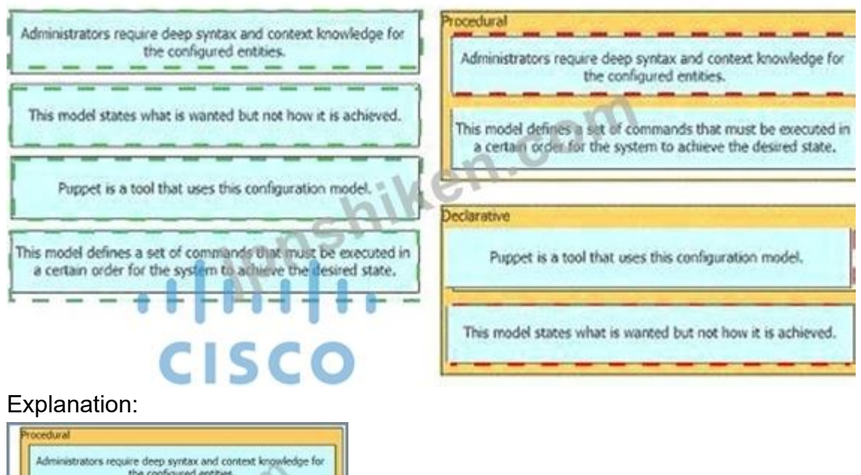
A. オプションB
B. オプションC
C. オプションD
D. オプションA
正解: **D (**コメントを発表する**)**

質問: **128**

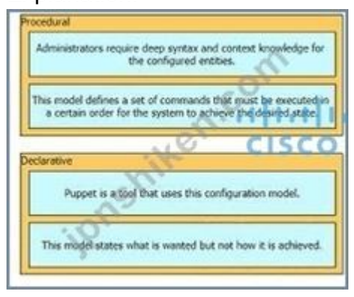
10 個の特性のうち右側の構成モデルにドラッグ アンド ドロップします。



正解:



Explanation:



質問: **129**
YANG モジュールの利点は何ですか?
A. 変更できない固定モジュールを持つことでエコシステムの断片化を回避する
B. メンテナンスとサポートを簡素化するための単一のプロトコルとモデルの結合
C. 共通モデルまたは業界モデルによって提供される、より容易なマルチベンダー相互運用性
D. パフォーマンスを向上させるためのエンコードを備えた密結合モデル
正解: (正解を表示します)

質問: **130**
Cisco Cyber Threat Defense ソリューションの Stealthwatch コンポーネントでは何が提供されますか?

A. マルウェア対策
B. コアネットワークとアクセスネットワークへのDDoS攻撃を阻止するリアルタイムの脅威管理
C. ウェブトラフィックの動的脅威制御
D. ネットワーク上のユーザー、デバイス、トラフィックのリアルタイム認識
正解: (正解を表示します)

質問: **131**
有効な JSON ファイルを表示する展示物はどれですか?

A.
```
{
    "hostname": "edge_router_1"
    "interfaces": [
        "GigabitEthernet1/1"
        "GigabitEthernet1/2"
        "GigabitEthernet1/3"
    ]
}
```

B.
```
{
    "hostname": "edge_router_1"
    "interfaces": {
        "GigabitEthernet1/1"
        "GigabitEthernet1/2"
        "GigabitEthernet1/3"
    }
}
```

C.
```
{
    "hostname": "edge_router_1",
    "interfaces": {
        "GigabitEthernet1/1",
        "GigabitEthernet1/2",
        "GigabitEthernet1/3",
    },
}
```

D. 

正解: **(**正解を表示します**)**

質問: **132**

```
event manager applet config-alert
event cli pattern "conf t.*" sync yes
```

図を参照してください。ユーザーが設定モードに切り替えたときに、ネットワークエンジニアに通知する必要があります。SNMPトラップと重大レベルのログメッセージを受信するには、どのスクリプトを適用すればよいですか？

- action 1.0 snmp-trap strdata "Configuration change alarm"
  action 2.0 syslog msg "Configuration change alarm"
- action 1.0 snmp-trap strdata "Configuration change critical alarm"
- action 1.0 snmp-trap strdata "Configuration change alarm"
  action 1.0 syslog priority critical msg "Configuration change alarm"
- action 1.0 snmp-trap strdata "Configuration change alarm"
  action 1.1 syslog priority critical msg "Configuration change alarm"

A. オプションB
B. オプションD
C. オプションC
D. オプションA
正解: **B (**コメントを発表する**)**

質問: **133**
RESTCONF に有効な操作はどれですか? (2 つ選択してください)
A. プル
B. 追加
C. プッシュ
D. ヘッド
E. 取得
F. 削除
正解: **D,E (**コメントを発表する**)**

質問: **134**
Cisco SD-Accessソリューションに当てはまる特性はどれですか？
A. 動的ルーティングは、境界スイッチとエッジスイッチを検出およびプロビジョニングするために使用されます。

B. コントロールプレーンはVXLANに基づいています。
C. データプレーンはVXLANに基づいています。
D. GRE がポリシープレーンとして使用されます。
正解: **(**正解を表示します**)**
The correct answer is C. The data plane is based on VXLAN.
In Cisco SD-Access, the fabric uses:
* LISP for the control plane
* VXLAN for the data plane
* Cisco TrustSec / SGT-based policy for the policy plane
Cisco documentation explicitly states that SD-Access uses a LISP-based control plane and a VXLAN-based data plane.
VXLAN is the encapsulation technology used to transport user traffic across the SD-Access fabric overlay.
This is why the data plane in Cisco SD-Access is based on VXLAN.
* A. Dynamic routing is used to discover and provision border and edge switches. Dynamic routing may exist in the underlay, but it is not what "discovers and provisions" border and edge nodes in SD-Access.
Provisioning is handled through Cisco DNA Center / Cisco Catalyst Center, not by dynamic routing itself.
* B. The control plane is based on VXLAN. This is incorrect because the control plane in SD-Access is based on LISP, not VXLAN.
* D. GRE is used as the policy plane. This is incorrect because the policy plane in SD-Access is based on TrustSec/SGT-based policy, not GRE.
ENCOR exam point:
Memorize this SD-Access mapping:
* Control plane = LISP
* Data plane = VXLAN
* Policy plane = Cisco TrustSec / SGT

質問: **135**
Cisco Unified Wireless ソリューションを導入する場合、分散 WLC 導入モデルを使用する設計上の正当性は何ですか?
A. MAC ARPとND処理を複数のスイッチに均等に分散し、スケーラビリティを向上させます。
B. 無線クライアントの数が少なく、物理的なキャンパスの規模が小さい
C. WLCを共通の場所に配置することで、ネットワーク管理者がサポートしなければならないWLCの数を減らすことができます。
D. キャンパスコアネットワークを通過するLWAPPおよびCAPWAPトンネルには遅延の懸念はありません。
正解: **(**正解を表示します**)**

質問: **136**
REST API を保護するためのセキュリティのベストプラクティスとして推奨される 2 つのアクションはどれですか? (2 つ選択してください。)
A. TACACS+認　証を使用します。
B. 帯域外認証を有効にします。
C. パスワードハッシュを使用します。
D. セッションの二重認証を有効にします。
E. 暗号化に SSL を使用します。
正解: **D,E (**コメントを発表する**)**

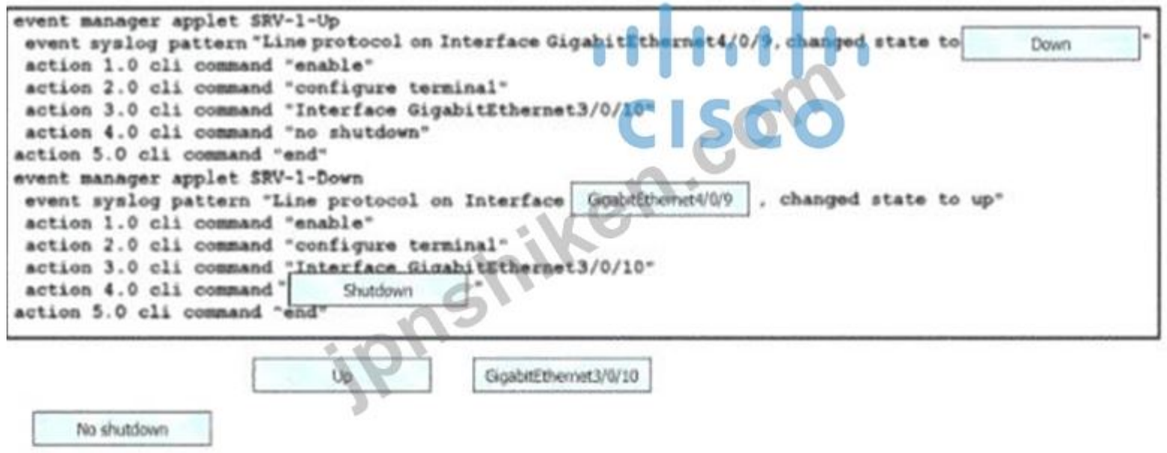
質問: **137**
複数のデバイス間でより効率的なデフォルト帯域幅の使用に関する設計要件を満たすには、どのファースト ホップ冗長プロトコルを使用する必要がありますか?
A. HSRP
B. LCAP
C. VRRP
D. GLBP
正解: (正解を表示します)

質問: **138**
ワイヤレス インフラストラクチャでレイヤー 2 ローミングを使用するクライアントが利用できる機能はどれですか?
A. 同じサブネットを捕捉し、同じIPアドレスを維持する別のワイヤレスコントローラにローミングします。
B. 異なるサブネット上にある別のワイヤレス コントローラに接続し、同じ IP アドレスを維持します。
C. 別のワイヤレス コントローラ上の新しいアクセス ポイントに関連付け、接続を中断せずに IP アドレスを変更します。
D. 同じワイヤレス コントローラ上の新しいアクセス ポイントに関連付け、接続を中断せずに IP アドレスを変更します。
正解: (正解を表示します)

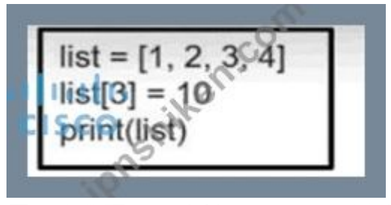
質問: **139**
スニペットをコード内の空白部分にドラッグ アンド ドロップして、プライマリ ポートがダウンした場合にフェイルオーバー イーサネット ポートを起動し、プライマリがサービスに復帰したときにフェイルオーバー ポートをシャットダウンするスクリプトを作成します。すべてのオプションが使用されるわけではありません。

正解:

Explanation:



質問: **140**



展示を参照してください。コード実行後の変数リストの値は何ですか？

A. [1, 2, 10]

B. [1, 10, 10, 10]

C. [1, 2, 10, 4]

D. [1, 2, 3, 10]

正解: **D** (コメントを発表する)

質問: **141**
Cisco SD-Access 展開では、どのノードに VXLAN カプセル化のサポートが必要ですか?
A. コアノード
B. 集約ノード
C. 配布ノード
D. 境界ノード
正解: **(**正解を表示します**)**

質問: **142**
エンジニアが高速移行を有効にして WLAN を構成します。一部のレガシー クライアントはこの WLAN に接続できません。どの機能を使用すると、レガシー クライアントが接続しながら、他のクライアントが OLTI に基づいて高速移行を使用できるようになりますか?
A. 802.11k
B. adaptive R
C. over the DS
D. 802.11V
正解: **B (**コメントを発表する**)**

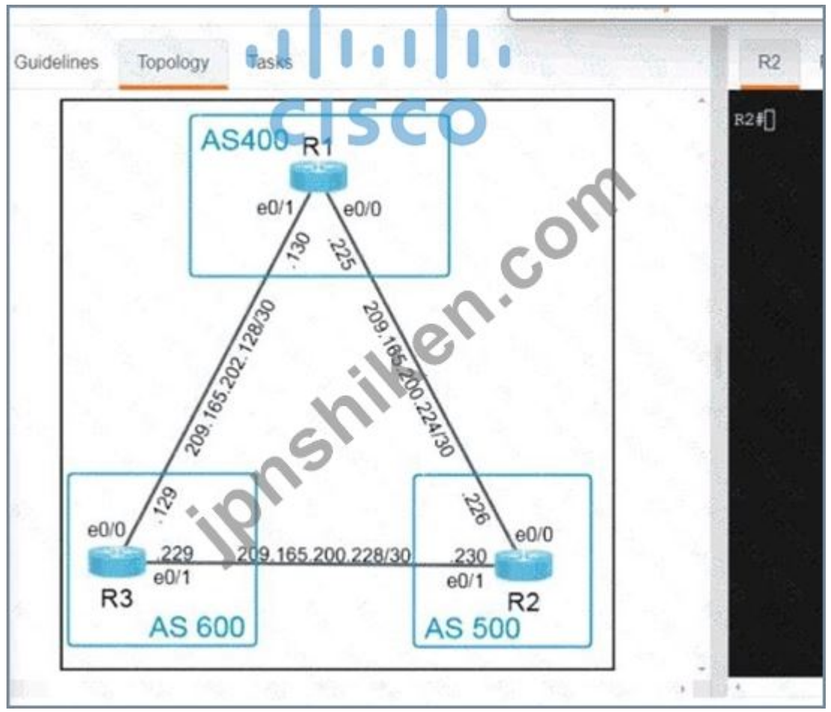
質問: **143**
アクセス ポイントのセルのエッジを示すために、ワイヤレス後の調査から使用される測定値はどれですか。
A. Noise
B. CCI
C. SNR
D. RSSI
正解: **C (**コメントを発表する**)**

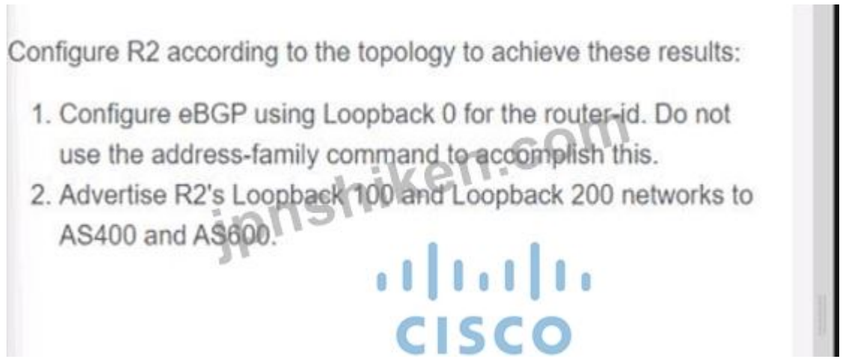
質問: **144**
Cisco Catalyst Center (旧 DNA Center) が、結果を達成するために必要な個々のステップではなく、結果に重点を置くことを可能にするのは、どのタイプの API ですか?
A. 北向きの意図
B. 西行き統合
C. サウスバウンド マルチベンダー サポート
D. 東行きのイベントと通知
正解: **A (**コメントを発表する**)**

質問: **145**
データ プレーン トラフィック ポリシーの配布を担当する Cisco Catalyst SD-WAN コンポーネントはどれですか?
A. vSmart
B. vBond
C. WAN edge
D. vManage
正解: **(**正解を表示します**)**

質問: **146**
複数の部門に対して個別のセキュリティ サービスをサポートする次世代ファイアウォール機能はどれですか?
A. 各コンテキスト内で特定の論理または物理インターフェイスを割り当て、セキュリティゾーンにグループ化したマルチコンテキストモード
B. ファイアウォールに入るフローのトラフィック検査機能を提供し、ポリシー設定に基づいてパケットをドロップする仮想スイッチモード
C. フェールオーバーリンクを使用してユーザーデータセッションとレプリケーションを隣接ファイアウォールに渡す状態共有モード
D. リソース追跡機能とノードとセキュリティゾーン間の自動構成同期を備えたレイヤー3モード
正解: **(**正解を表示します**)**

質問: **147**
REST API を介して交換される機密情報の機密性を保護するために使用されるメカニズムはどれですか?
A. IPsec
B. 802.1X
C. TLS
D. SSH
正解: **(**正解を表示します**)**

質問: **148**




正解:

See the solution below in Explanation:

Explanation:

Solution:-

Copy run start

質問: **149**

高密度 RF 環境でスティッキー クライアントを削減するアクションはどれですか?

A. 無線チャネル幅を 160 MHz に増やします。

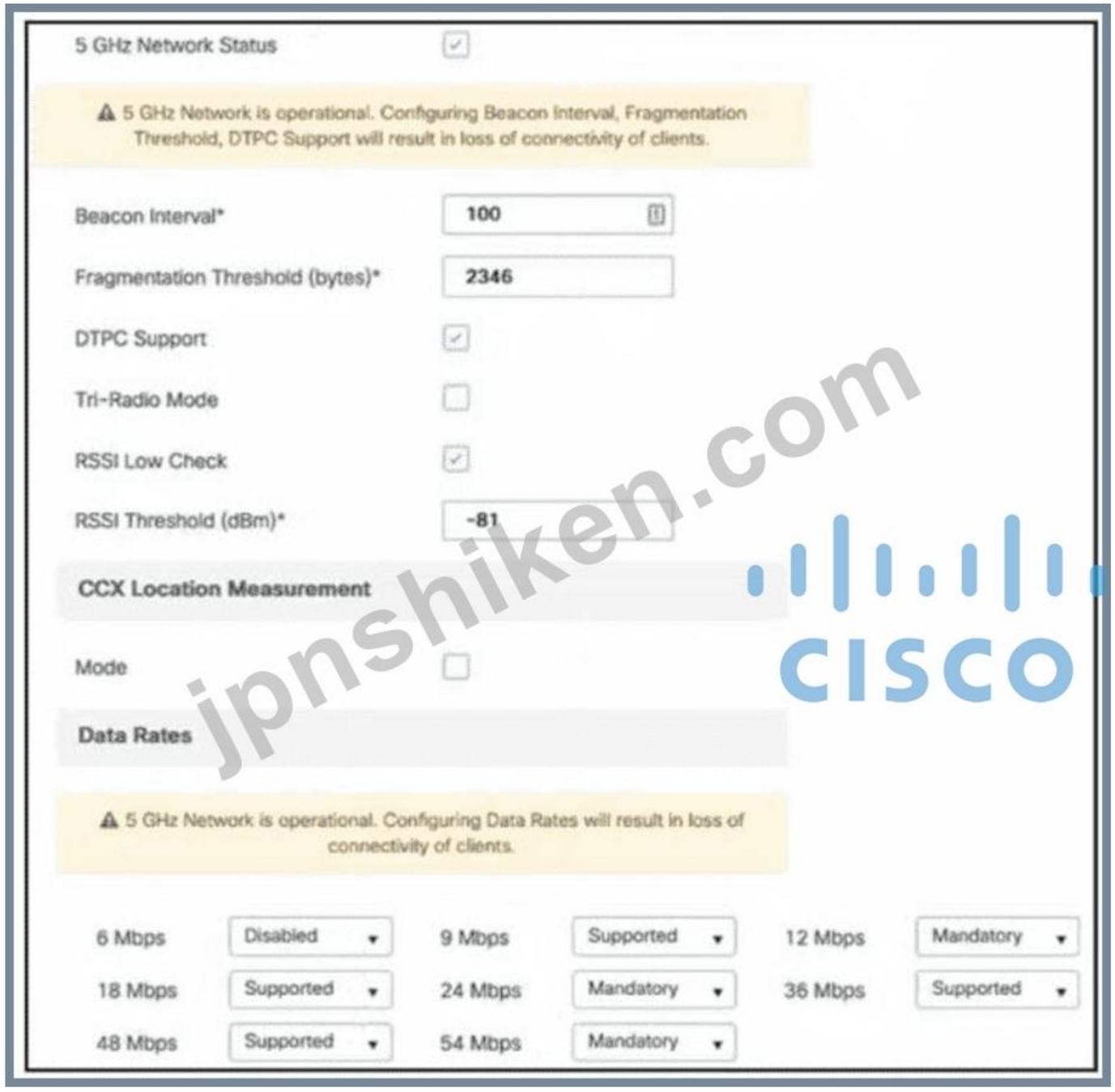
B. 必須の最小データ レートを増やします。

C. 必須の最小データ レートを下げます。

D. 無線チャネル幅を 40 MHz に減らします。

正解: (正解を表示します)

質問: **150**



展示を参照してください。多くのワイヤレスクライアントがマルチキャストオーディオを確実に受信できないという報告が顧客から寄せられています。
この問題を解決するには、どのようなアクションを実行すればよいですか?

A. RSSI Low チェックを無効にします。

B. RSSIしきい値を-67dBm に設定します。
C. 断片化しきい値を1250バイトに設定する
D. 24 Mbps および 54 Mbps のデータ レートを [サポート] に設定します。
正解: **(**正解を表示します**)**

質問: **151**
顧客は、ワイヤレス データ トラフィックをアクセス ポイントのスイッチ ポートから出力することを必要としています。どのアクセス ポイント モードがこれをサポートしていますか?
A. スニファー
B. モニター
C. フレックスコネクト
D. ブリッジ
正解: **(**正解を表示します**)**

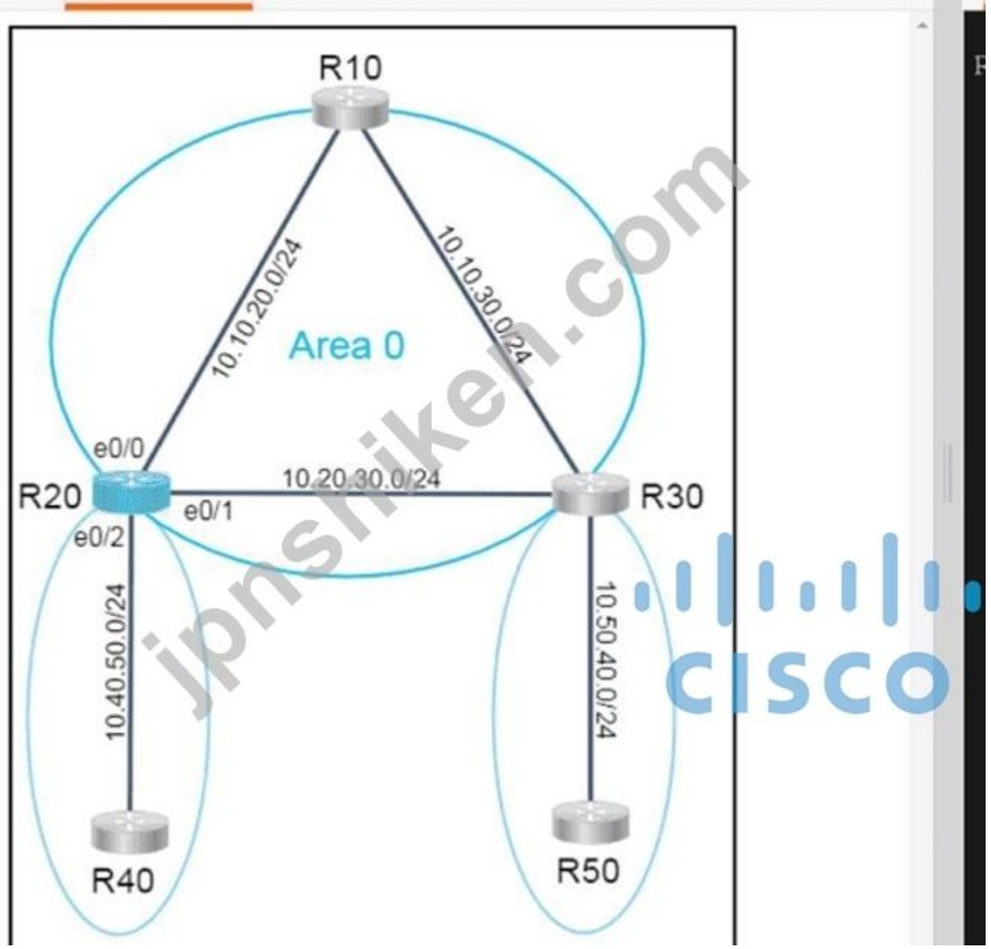
質問: **152**
REST API セッションに誤ったパスワードが適用されたリクエストに対する正しい応答はどの HTTP ステータス コードですか?
A. HTTPステータスコード 302
B. HTTPステータスコード 200
C. HTTPステータスコード401
D. HTTP ステータス コード: 504
正解: **C (**コメントを発表する**)**

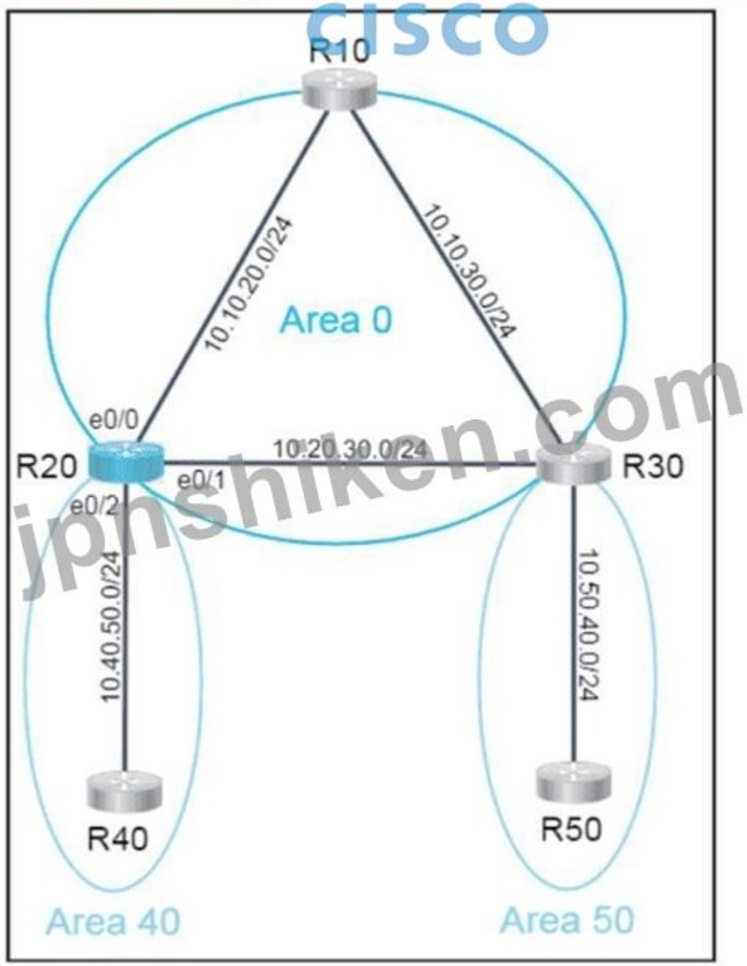
質問: **153**
図を参照してください。エンジニアは、ルータ A がアクティブ ルータになるように設定を調整する必要があります。
ルータ A に適用する必要があるコマンドはどれですか? (2 つ選択してください)

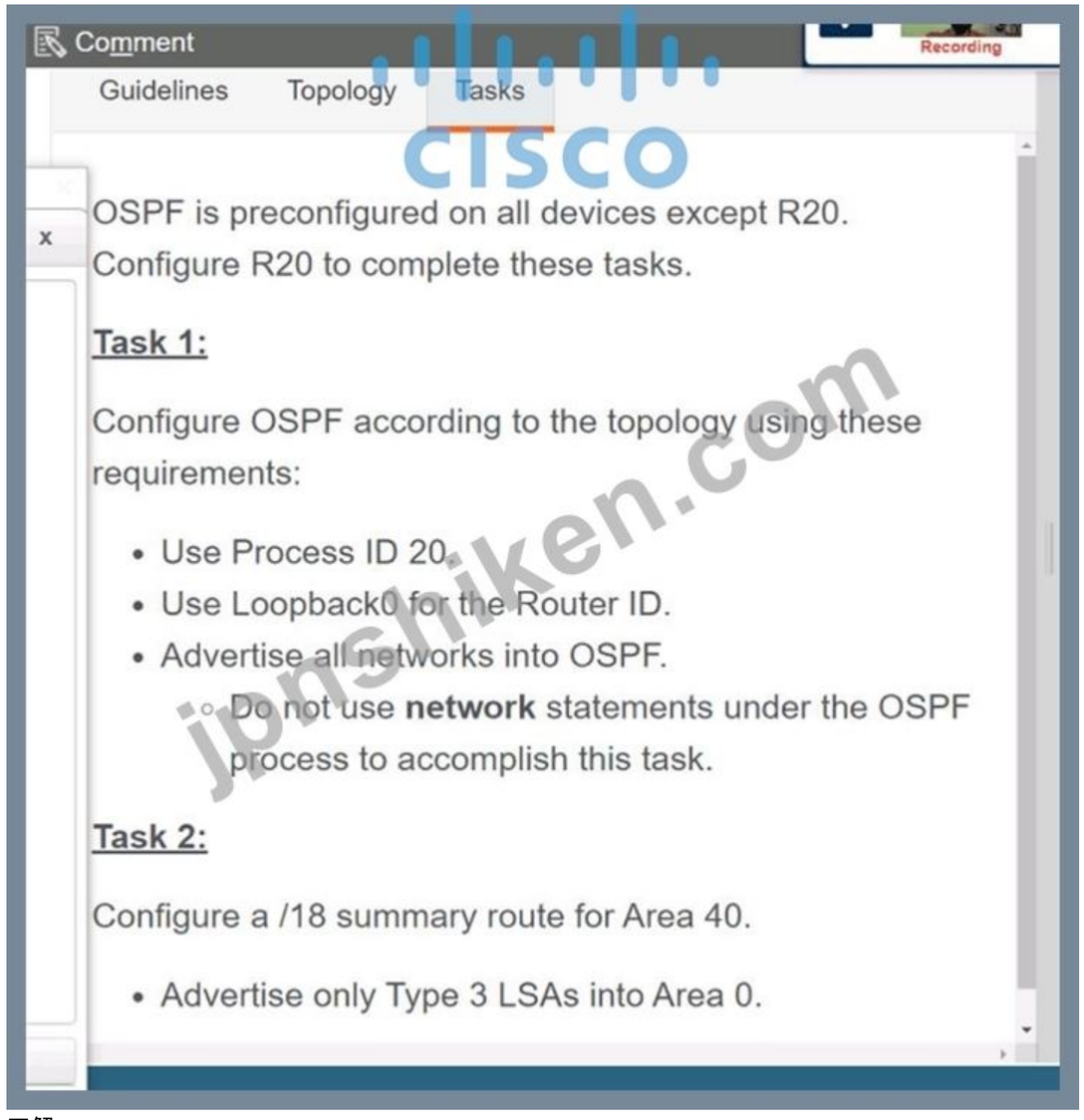
A. VRRP リップ 10.1.0.11
B. VRRP 1 優先度 120
C. IPアドレス 10.1.0.11 255.0.0.0
D. VRRP 1 優先度 90
E. vrrp 1 タイマーが 1 をアドバタイズします
正解: **(**正解を表示します**)**

質問: **154**

uidelines | Topology | Tasks







正解:
See the solution below in Explanation:
Explanation:
Solution:
R30
Config t
router ospf 100
router-id 10.0.1.30
int ran lo0 , e0/0-1
ip ospf 100 a 0

exit
int et0/2
ip ospf 100 a 50
exit
router ospf 30
area 50 range 10.10.0.0 255.255.192.0
area 50 range 10.50.0.0 255.255.192.0
end
wr

質問: **155**
LISP ネットワーク アーキテクチャとプロトコルはどの 2 つの名前空間を使用しますか? (2 つ選択してください。)
A. DNS
B. RLOC
C. VTEP
D. EID
E. TLOC
正解: **(**正解を表示します**)**

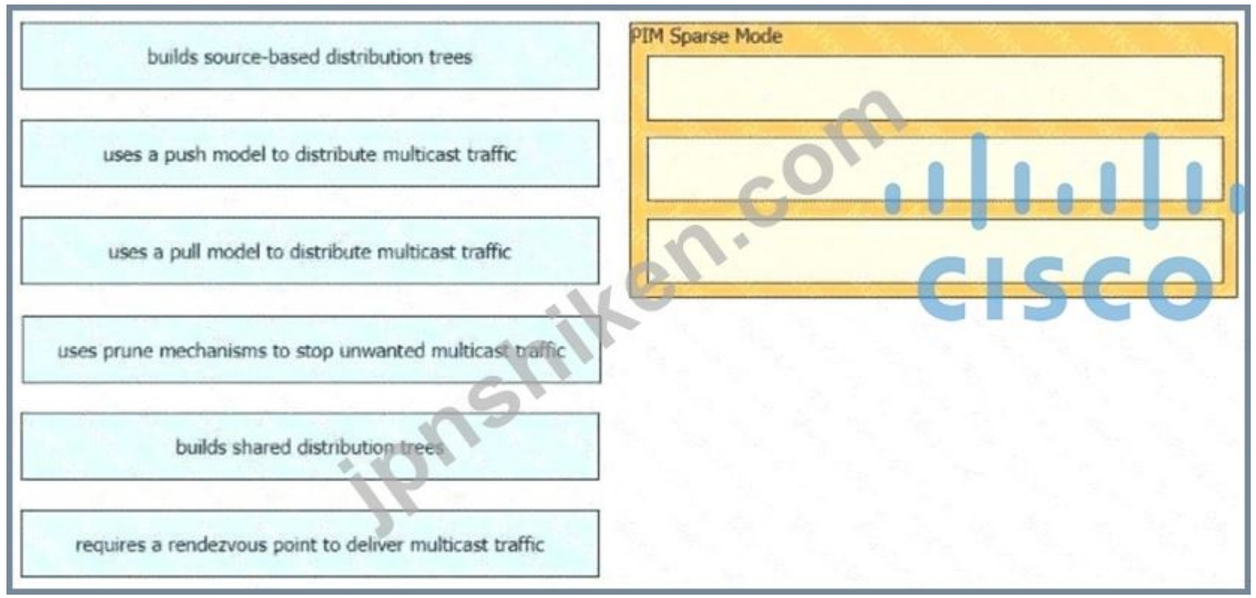
質問: **156**
エンジニアはランサムウェア攻撃から会社を守る必要があります。エンジニアが実行段階をブロックし、ファイルの暗号化を防ぐことができるソリューションはどれですか?
A. Cisco Firepower を使用して、TOR ネットワークへのトラフィックをブロックします。
B. 侵入ポリシーと SMB の悪用をブロックする Snort ルールを備えた Cisco Firepower を使用します。
C. エクスプロイト防止エンジンを有効にした Cisco AMP 展開を使用します。
D. 悪意のあるアクティビティ保護エンジンを有効にした Cisco AMP 展開を使用します。
正解: **(**正解を表示します**)**

質問: **157**
Cisco Catalyst SD-WAN の 2 つの特徴は何ですか? (2 つ選択してください。)
A. 分散制御プレーン
B. コントロールプレーンは、DTLS/TLS 認証およびセキュリティ保護されたトンネルを介して動作します。
C. 統合データプレーンとコントロールプレーン
D. 時間のかかる設定とメンテナンス
E. 集中化された到達可能性、セキュリティ、およびアプリケーション ポリシー
正解: **(**正解を表示します**)**

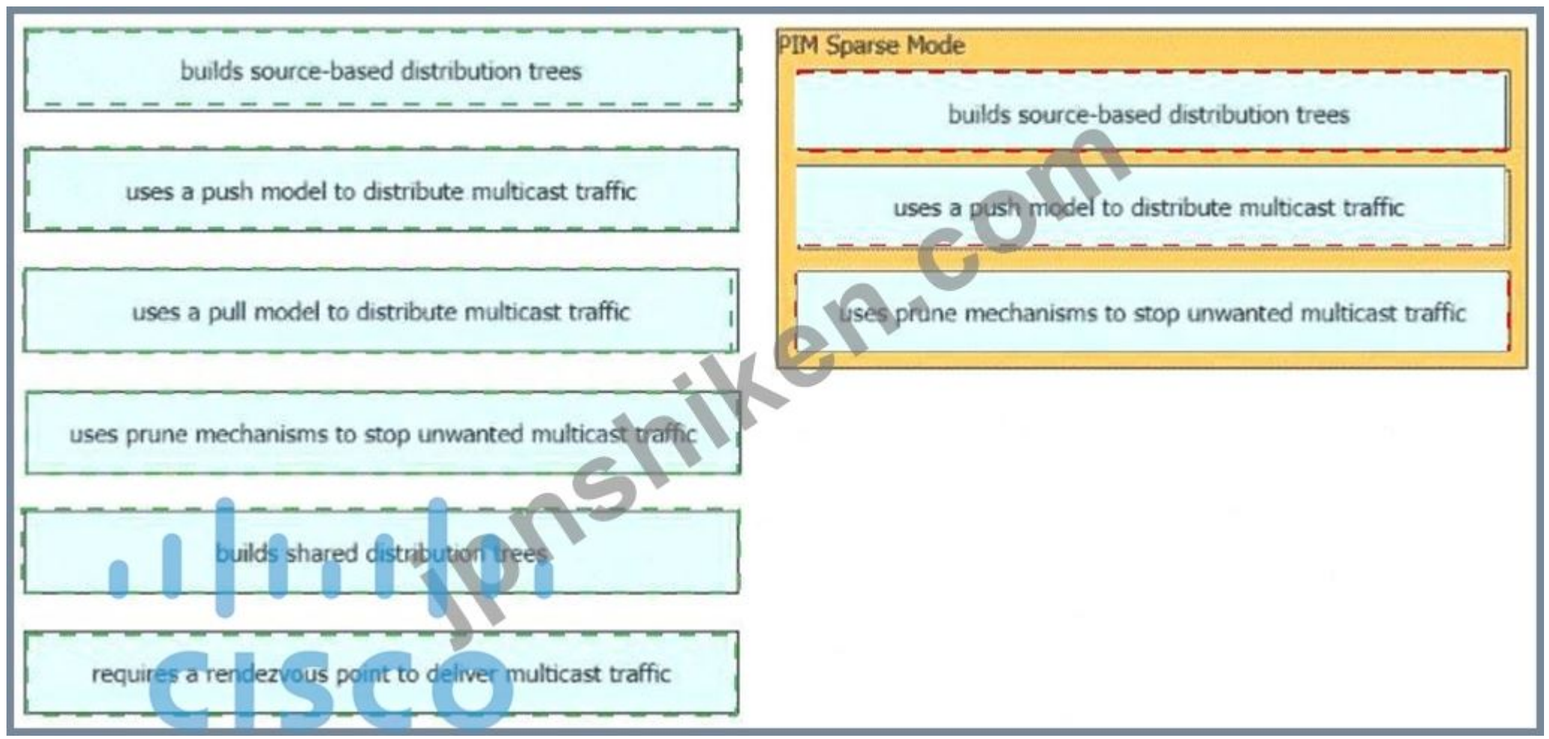
質問: **158**
エンジニアが顧客サイトで Wi-Fi カバレッジを測定します。RSSI 値は次のように記録されます。
*場所A -72dBm
* 場所B:-75 dBm

* 場所 C; -65 dBm
* 場所D -80 dBm
エンジニアはこれらの値を顧客に説明するためにどの 2 つのステートメントを使用しますか? (2 つ選択してください。)
A. 場所CのRF信号強度は場所Bの10倍強い
B. 場所 B の RF 信号強度は場所 A よりも 50% 弱くなります。
C. 場所 D の RF 信号強度が最も強くなります。
D. 場所 B の信号強度は場所 C よりも 10 dB 優れています。
E. 場所Cの信号強度が弱すぎて、Webサーフィンができません
正解: **(**正解を表示します**)**

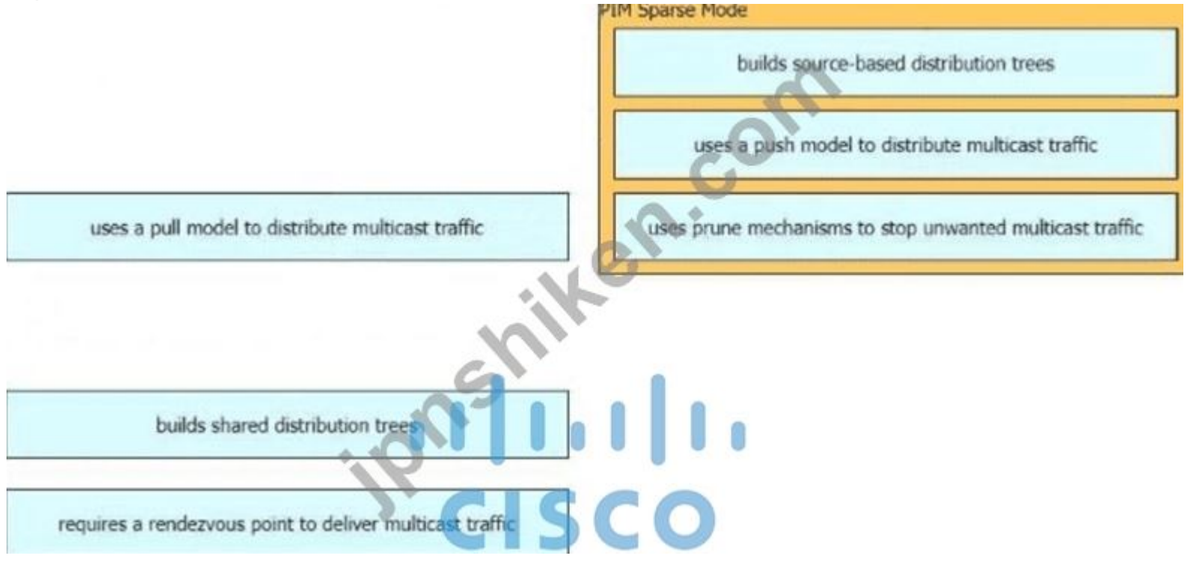
質問: **159**
PIM スパース モードの特性を左から右にドラッグ アンド ドロップします。すべてのオプションが使用されるわけではありません。



正解:



Explanation:



質問: **160**

EEM に登録され、オンデマンドまたは手動で実行される EEM アプレット ポリシーを作成する方法はどれですか。

A. イベント マネージャ アプレット ondemand アクション 1.0 syslog 優先度 クリティカル メッセージ 'これは ondemand からのメッセージです'

B. イベント マネージャ アプレット オンデマンド イベント 手動アクション 1.0 Syslog 優先度 クリティカル メッセージ 'これはオンデマンドからのメッセージです'
C. イベント マネージャ アプレット ondemand イベント レジスタ アクション 1.0 syslog 優先度 クリティカル メッセージ 'これは ondemand からのメッセージです'
D. イベント マネージャ アプレット ondemand イベント なし アクション 1.0 syslog 優先度 クリティカル メッセージ 'これは ondemand からのメッセージです'
正解**: (**正解を表示します**)**

質問**: 161**
Cisco Catalyst SD-WANノード間で安全な制御プレーン隣接関係を確立するために実装されるプロトコルはどれですか？
A. IPsec
B. TLS
C. IKE
D. ESP
正解**: B (**コメントを発表する**)**
The correct answer is B. TLS.
In Cisco Catalyst SD-WAN, the architecture separates:
* Control Plane # Secure communication between controllers and edge devices
* Data Plane # Encrypted tunnels carrying user traffic
* The control plane (between vSmart, vBond, vManage, and WAN Edge routers) uses:
* TLS (Transport Layer Security)
* In some cases also DTLS, depending on configuration
* These protocols provide:
* Authentication
* Encryption
* Integrity protection
Thus, TLS is used to establish secure control plane adjacencies.
* A. IPsec Used for data plane encryption (IPsec tunnels), not control plane.
* C. IKE Used for key exchange in IPsec, not for SD-WAN control plane adjacencies.
* D. ESP Part of IPsec (data plane encryption), not control plane.
Memorize this SD-WAN separation:
* Control Plane # TLS / DTLS
* Data Plane # IPsec (ESP encapsulation)
This distinction is frequently tested in ENCOR exams.

質問**: 162**
仮想環境における VMDK ファイルとは何ですか?
A. 仮想マシンのディスク ドライブを含むファイル。
B. ゲスト OS などの仮想マシンの設定が含まれる構成ファイル。
C. 仮想マシン構成ファイルと仮想ディスクを接続する zip ファイル。
D. 仮想マシンのスナップショットに関する情報を含むファイル。
正解**: D (**コメントを発表する**)**

質問: **163**
エンジニアは、Cisco 9800 ワイヤレス LAN コントローラに新しい SSID を作成する必要があります。クライアントは認証に事前共有キーを使用するように要求しています。この要件を満たすには、エンジニアはどのプロファイルを編集する必要がありますか?
A. RF
B. フレックス
C. ポリシー
D. 無線LAN
正解: **D** (コメントを発表する)

質問: **164**
Cisco Catalyst SD-WANソリューションにおいて、データプレーントンネルの状態はどのように監視されますか？
A. IP SLA付き
B. OMP付き
C. BFD を使用する
D. ARPプロービング
正解: (正解を表示します)
The correct answer is C. using BFD.
In Cisco Catalyst SD-WAN, the health of data plane tunnels is monitored using Bidirectional Forwarding Detection (BFD). Cisco documentation states that BFD runs over all data plane tunnels between Cisco IOS XE Catalyst SD-WAN devices and is used to monitor the liveness and path characteristics of those tunnels, including loss, jitter, and latency.
BFD is the protocol specifically used in Cisco SD-WAN to detect tunnel failures quickly and measure tunnel quality. These measurements are also used by SD-WAN features such as application-aware routing to make path-selection decisions.
* A. with IP SLA IP SLA is a Cisco feature for measuring network performance in many environments, but Cisco SD-WAN data plane tunnel health is monitored with BFD, not IP SLA.
* B. with OMP OMP (Overlay Management Protocol) is the control-plane routing protocol in Cisco SD- WAN. It distributes routes, TLOCs, and service information, but it does not monitor data plane tunnel health.
* D. ARP probing ARP is used for Layer 2/neighbor resolution on local segments and is not the tunnel- health monitoring mechanism for SD-WAN data plane tunnels.
ENCOR exam point:
In Cisco Catalyst SD-WAN:
* OMP = control-plane route exchange
* BFD = data-plane tunnel liveliness and performance monitoring

質問: **165**
タイプ 1 ハイパーバイザーの特徴は何ですか?
A. 非本番環境のワークロードをサポートする場合に適しています。
B. ベアメタル サーバー上で実行されます。
C. タイプ 2 ハイパーバイザーよりもレイテンシが大きくなります。
D. ホスト オペレーティング システム上で実行されます。
正解: (正解を表示します)

質問: **166**
どの設定により、Cisco ルータは、特権レベル 15 に関連付けられた個々の EXEC コマンドの情報を TACACS+ サーバに送信できるようになりますか?
A. Router(config)# aaa accounting exec default start-stop group tacacs+

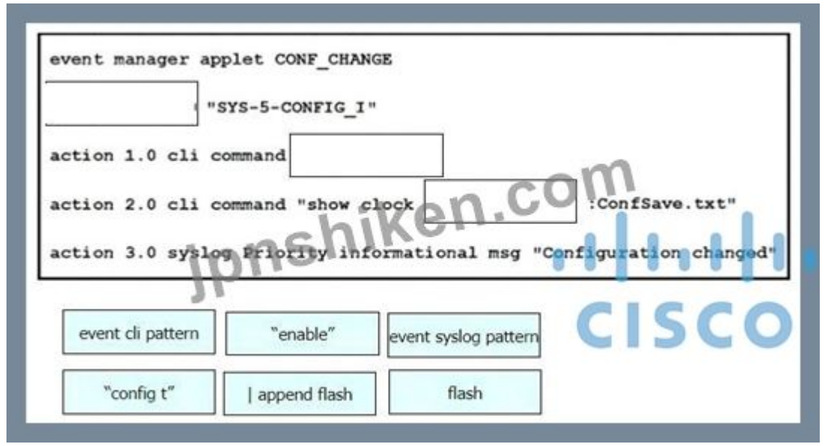
B. Router(config)# aaa authorization commands 15 default group tacacs+
C. Router(config)# aaa authorization exec default group tacacs+
D. Router(config)# aaa accounting commands 15 default start-stop group tacacs+
正解: **(**正解を表示します**)**

質問: **167**
YANG モデルは何を提供しますか?
A. トランスポートプロトコルに依存しない標準化されたデータ構造
B. トランスポートプロトコルの作成とOSとの相互作用
C. NETCONFまたはRESTCONFトランスポートプロトコルでのみ使用できる標準化されたデータ構造
D. デバイスの CLI と直接対話してネットワーク構成を受信または変更するためのユーザー アクセス
正解: **A (**コメントを発表する**)**

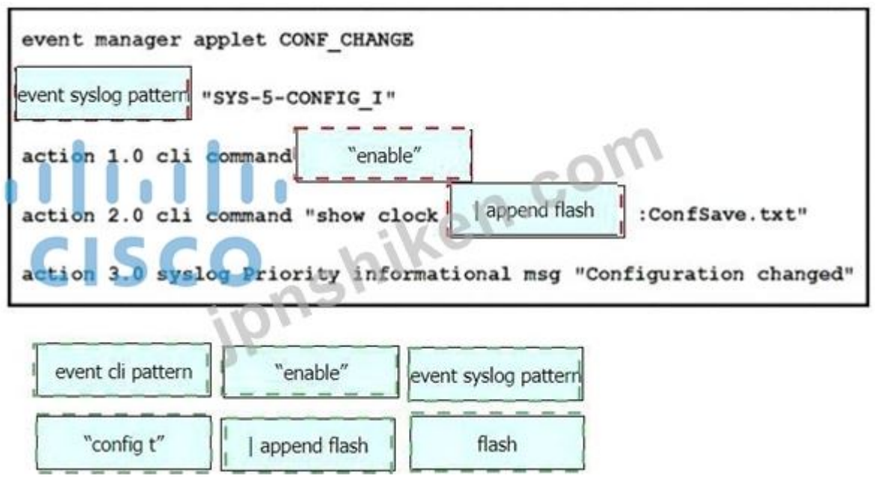
質問: **168**
Cisco SD-Access ファブリックを設計するときに必要な 2 つのコンポーネントはどれですか? (2 つ選択してください。)
A. Cisco Catalyst Center (旧 DNA Center) アプリケーション
B. シスコ プライム インフラストラクチャ
C. 火力脅威防御
D. シスコ データセンター ネットワーク マネージャ
E. アイデンティティサービスエンジン
正解: **A,E (**コメントを発表する**)**

質問: **169**
ネットワーク管理者は、ネットワーク上の Cisco IOS XE ベースのデバイスを設定するための Python スクリプトを準備しています。管理者は、スクリプトの実行中に同僚がデバイスに変更を加えることを心配しています。NC クライアント マネージャーのどの操作によって、スクリプトの実行中に同僚がデバイスに変更を加えるのを防ぐことができますか。
A. m.lock(target-running')
B. m.freeze(config-running')
C. m.freeze(target-running')
D. m.lock(config='running')
正解: **(**正解を表示します**)**

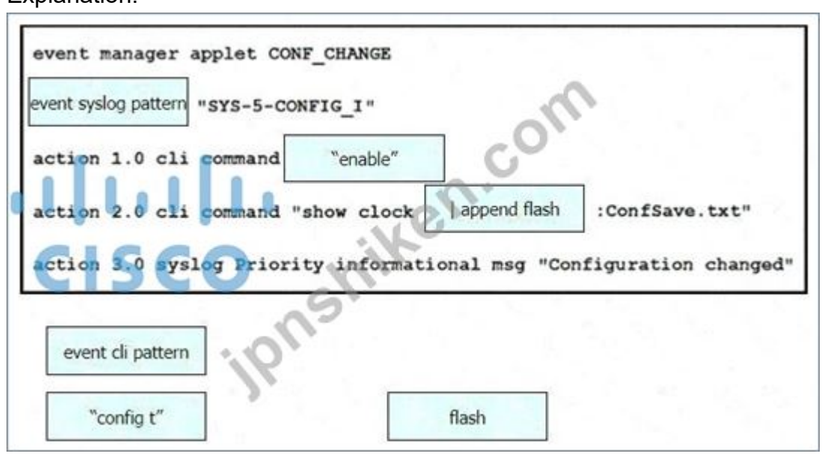
質問: **170**
スニペットをコード内の空白部分にドラッグ アンド ドロップして、構成の変更が行われたときにタイムスタンプ付きのエントリをローカルに保存されたテキスト ファイルに追加する EEM スクリプトを作成します。すべてのオプションが使用されるわけではありません。



正解:



Explanation:



質問: **171**
2 つのサイト間のエンドツーエンドのラインレート暗号化をサポートするソリューションはどれですか?
A. トラストセック
B. IPsec
C. MACsec
D. GRE
正解: **(**正解を表示します**)**

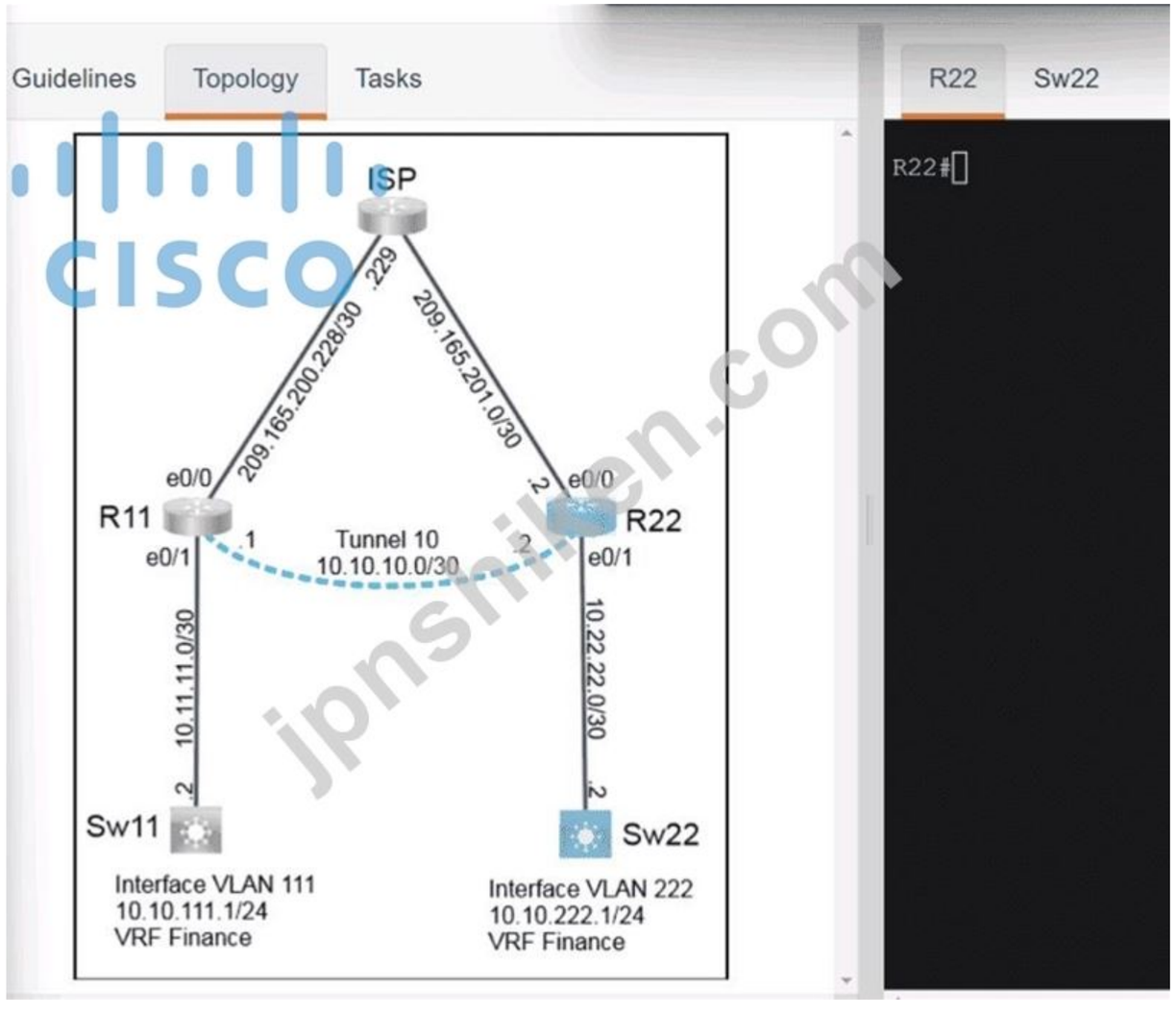
質問: **172**
従来のWANソリューションには当てはまるが、Cisco Catalyst SD-WANソリューションには当てはまらない特性はどれですか？
A. 集中管理されたアクセス性、セキュリティ、およびアプリケーションポリシー
B. 時間のかかる設定とメンテナンス
C. 低複雑度で全体的なソリューション規模が拡大
D. DTLS/TLS認証済みでセキュアなトンネル上で動作します
正解: **(**正解を表示します**)**
The correct answer is B. Time-consuming configuration and maintenance .
In a traditional WAN architecture , configurations are typically performed manually on each device (router-by-router basis) . This leads to:
* Increased operational overhead
* Slower deployment times
* Higher chances of configuration inconsistency
* Difficult scalability
According to Cisco ENCOR (350-401) architecture principles, traditional WANs lack centralized orchestration, making configuration and maintenance time-consuming and complex .
In contrast, Cisco Catalyst SD-WAN introduces:
* Centralized management and control (via vManage, vSmart, vBond)
* Policy-based automation
* Zero-touch provisioning (ZTP)
* Simplified operations and faster deployment
Now, why the other options are incorrect:
* A. Centralized reachability, security, and application policies # This is a defining feature of Cisco SD-WAN , not traditional WAN.
* C. Low complexity and increased overall solution scale # SD-WAN is specifically designed to reduce complexity and improve scalability .
* D. Operates over DTLS/TLS-authenticated and secured tunnels # Cisco SD-WAN uses secure control connections (DTLS/TLS) , which is not a characteristic of traditional WAN .
Final Concept (ENCOR Exam Focus):
Traditional WAN = Manual, complex, time-consuming
Cisco SD-WAN = Centralized, automated, scalable, secure

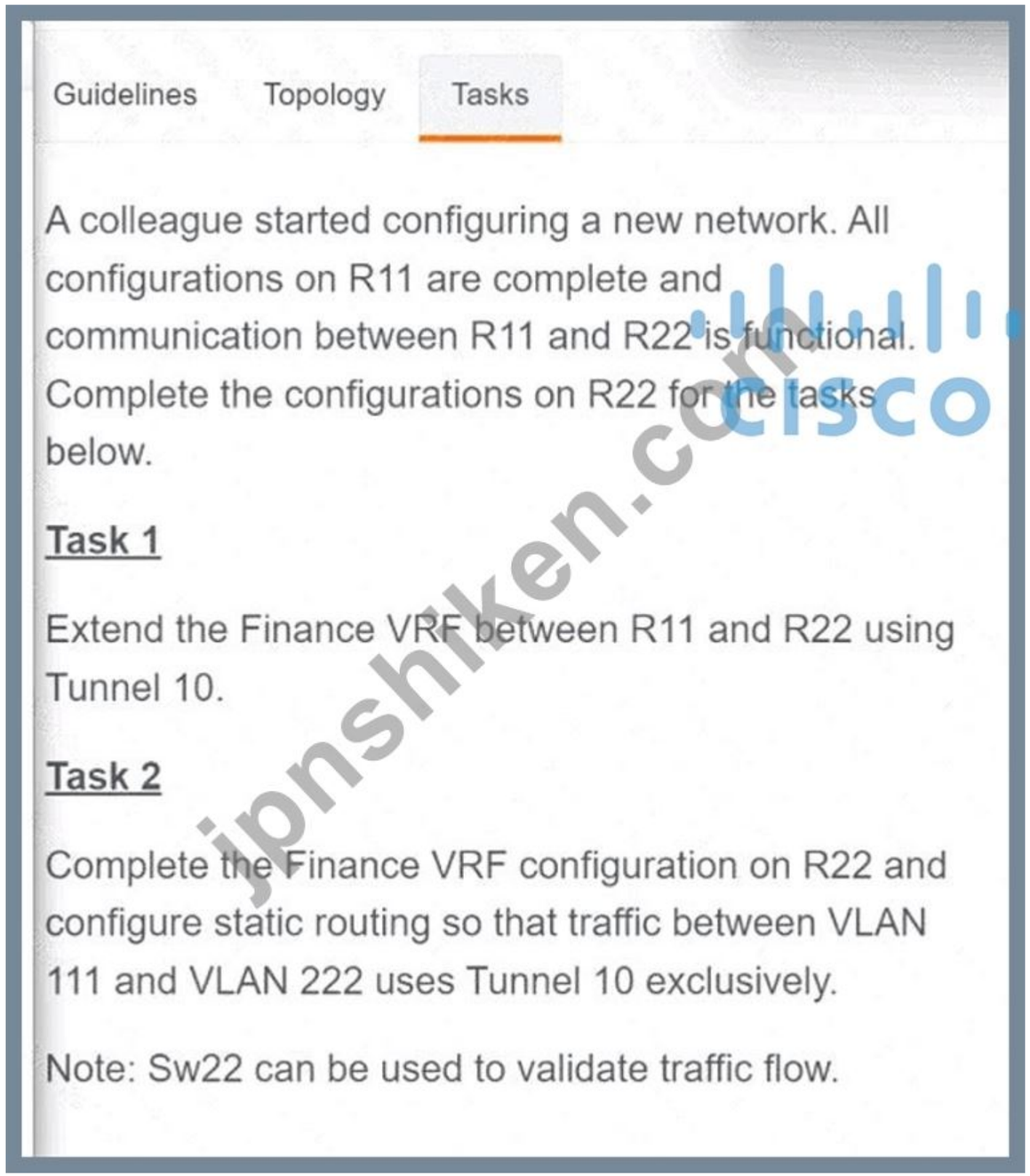
質問: **173**
Cisco SD-WAN の単一管理プレーンとなるコントローラはどれですか?
A. vManage
B. vSmart
C. vEdge
D. vBond

正解: (正解を表示します)

質問: **174**
AP が HA コントローラに参加するために使用され、NVRAM で設定される方法はどれですか?
A. DNS
B. 保存されたWLC情報
C. プライマリ/セカンダリ - ターシャリ/バックアップ
D. IP ヘルパー アドレス
正解: (正解を表示します)

質問: **175**





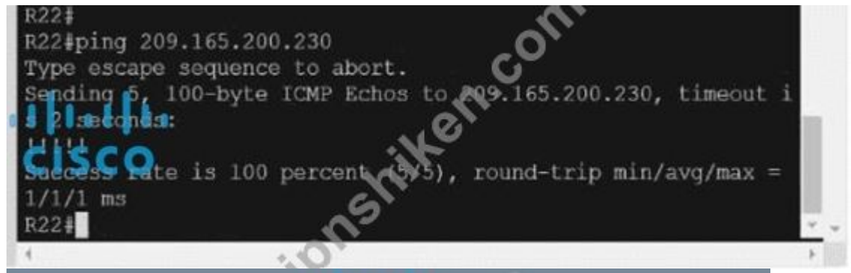
正解:

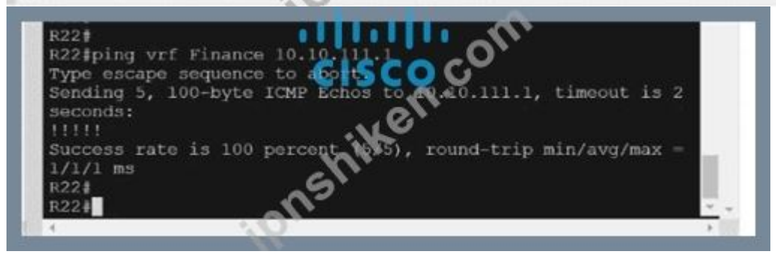
See the solution below in Explanation:

Explanation:

Solution:

R22
int tun0
vrf forwarding FINANCE
ip add 10.10.10.2 255.255.255.0
tunn source e0/0
tunnel dest 209.165.200.230
no shut
ip route vrf FINANCE 10.10.111.0 255.255.255.0 tunn0
int et0/1
vrf forwarding FINANCE
ip address 10.22.22.1 255.255.255.252
wr
Verification:-





質問: **176**
ステートメント print(format(0.8, \0%')) は何を表示しますか?
A. 0.08%
B. 80%
C. 8.8%
D. 8%
正解: **(**正解を表示します**)**

質問: **177**
企業ネットワークにおいて、集約層とレイヤ2アクセス層間の収束時間を短縮できるネットワーク設計はどれか？
A. 従来のループ設計で、共通のVLANが別々のアクセススイッチ間で拡張されている。
B. 集約中間ノードとアクセスレイヤ間のCisco SD-Access構成

C. 集約ノードとアクセスレイヤーエッジノード間のCisco SD-Access構成
D. 個別のアクセススイッチ間で独自の VLAN が拡張された、従来型の非ループ設計
正解**:** (正解を表示します)
The correct answer is D.
Cisco campus design guidance explains that a nonlooped topology with unique VLANs per access switch improves stability and convergence compared with looped Layer 2 designs. Cisco states that in a multilayer campus design, each access switch should have unique VLANs, with no Layer 2 loops and no blocked links, which improves convergence behavior. Cisco also notes that VLANs spanning multiple access switches increase flooding impact, while a nonlooped topology with localized VLANs reduces that impact.
A traditional nonlooped design reduces reliance on spanning-tree reconvergence across shared Layer 2 domains. With unique/local VLANs, failures affect a smaller fault domain and convergence is faster than in a looped design with common VLANs stretched across switches. Cisco's campus design material specifically recommends no Layer 2 loops and unique VLANs per access switch for better operational behavior.
* A. Traditional looped design that has common VLANs extended between separate access switches This increases Layer 2 complexity and spanning-tree dependency, which slows convergence compared to a nonlooped design. Cisco documents that VLANs spanning multiple access switches increase flooding impact.
* B. Cisco SD-Access configuration between aggregation intermediate nodes and access layers This is not the standard way the question is framed for classic aggregation-to-Layer 2 access convergence in a traditional enterprise campus design. The question is targeting the design principle of looped vs nonlooped Layer 2 access.
* C. Cisco SD-Access configuration between aggregation and access-layer edge nodes SD-Access is a different fabric architecture. The question is about reducing convergence time between aggregation and a Layer 2 access layer, which maps to the traditional campus design choice rather than SD-Access node roles.
For enterprise campus design, remember:
* Looped Layer 2 + stretched/common VLANs = slower convergence and larger fault domains
* Nonlooped Layer 2 + unique/local VLANs per access switch = faster convergence and better stability

質問**: 178**
Cisco Catalyst Center (旧 DNA Center) がデバイスを検出するために使用する 3 つの方法はどれですか? (3 つ選択してください。)
A. NETCONF
B. 指定されたIPアドレスの範囲
C. SNMP
D. ping
E. CDP
F. LLDP
正解**: B,E,F (**コメントを発表する**)**

質問**: 179**
SD-WANファブリックを介してサイト間のトラフィックを輸送するのはどの航空機ですか？
A. IPsec
B. マネジメント
C. データ
D. コントロール
正解**: (**正解を表示します**)**
The correct answer is C. Data.
Cisco SD-WAN architecture is divided into three main planes:
* Management Plane
* Handled by vManage
* Used for configuration and monitoring

* Control Plane
* Handled by vSmart (OMP protocol)
* Responsible for routing information exchange and policy distribution
* Data Plane
* Built using IPsec tunnels between WAN Edge devices
* Responsible for forwarding actual user/application traffic between sites The data plane is the plane that:
* Carries user traffic
* Transports data between SD-WAN sites
* Uses secure tunnels (IPsec) for communication
* A. IPsec IPsec is a technology used within the data plane, not a plane itself.
* B. Management Used for configuration and orchestration, not traffic forwarding.
* D. Control Used for routing and policy decisions, not actual traffic transport.
Memorize SD-WAN planes:
* Management Plane # vManage (configuration)
* Control Plane # vSmart (routing/policy via OMP)
* Data Plane # IPsec tunnels (user traffic transport)
User traffic = Data Plane

質問: **180**
VXLAN トンネル エンドポイントを動作させるには何が必要ですか?
A. VXLANトンネルエンドポイント識別子
B. VXLANネットワーク識別子
C. 少なくとも 1 つのレイヤー 2 インターフェースと 1 つのレイヤー 3 インターフェース
D. トランジットネットワーク用の少なくとも 1 つの IP とエンドポイント接続用の 1 つの IP
正解: **B** (コメントを発表する)

質問: **181**
AP が 1 つ以上の無線チャネルをスキャンして不正なアクセス ポイントを検出し、同時にクライアントに無線サービスを提供できるようにする 2 つの動作モードはどれですか (2 つ選択してください)。
A. スニファー
B. 不正検出機能
C. モニター
D. フレックスコネクト
E. ローカル
正解: (正解を表示します)

質問: **182**

Cisco Catalyst Center（旧DNA Center）SDK は、ネットワーク内のシスコ以外のデバイスのトポロジを検出するためにどのプロトコルを使用しますか?
A. LLDP
B. Telnet
C. CDP
D. SSH
正解: **(**正解を表示します**)**

質問: **183**
エンジニアは、6 GHz 無線でブロードキャストする必要がある新しい SSID を Cisco Catalyst 9800 シリーズ WLC に実装しています。ユーザーは認証に EAP-TLS を使用する必要があります。必要なワイヤレス レイヤー 2 セキュリティ メソッドはどれですか。
A. WPA3 パーソナル
B. WPA3 エンタープライズ
C. WPA2 パーソナル
D. WPA3 エンタープライズ
正解: **(**正解を表示します**)**

質問: **184**
データ センター環境で VM を使用してサーバーを仮想化する 2 つの利点は何ですか? (2 つ選択してください。)
A. IPアドレスとMACアドレスの要件が削減されました
B. 迅速な展開
C. より小さなレイヤー2ドメイン
D. ラックスペース、電力、冷却要件の削減
E. セキュリティ強化
正解: **(**正解を表示します**)**