Cisco.350-401J.v2026-08-20.q190

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：	190
バージョン：	v2026-08-20
ページの閲覧量：	105
問題集の閲覧量：	2060

https://www.jpnshiken.com/shiken/Cisco.350-401J.v2026-08-20.q190.html

質問: **1**

展示を参照してください。このコードの出力は何ですか？

- ○ 1st_item######## : 6452987918
  2nd_item_that_m : jlugyydt##
- ○ 1st_item######## : 8791871446
  at_must_display : jlugyydt
- ○ 1st_item######## : 645298791871446
  2nd_item_that_must_display : jlugyydt##
- ○ 6452987918871446
  ##jlugyydt

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

質問: **2**
NETCONF および RESTCONF のデータの構造またはモデリングを定義する言語はどれですか?
A. YANG
B. JSON
C. YAML

D. XML
正解: **(**正解を表示します**)**

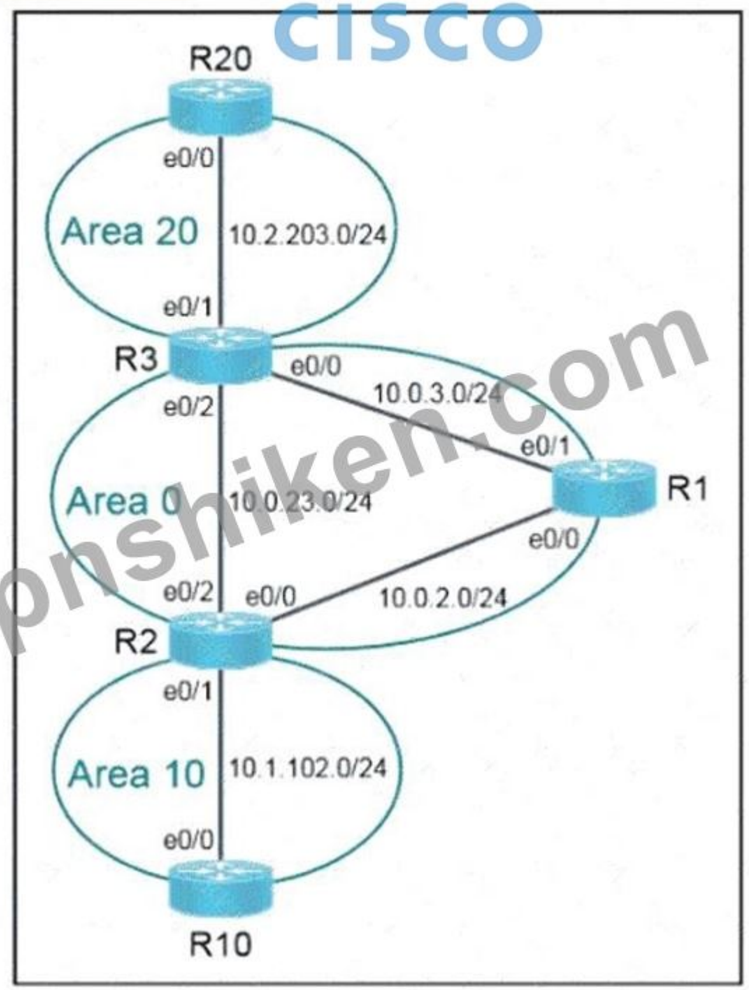
質問: **3**
従来のネットワーク要素とコントローラ層間の通信を提供する Cisco SD-Access コンポーネントはどれですか (2 つ選択してください)。
A. ファブリックオーバーレイ
B. ネットワークデータプラットフォーム
C. パートナーエコシステム
D. ネットワーク制御プラットフォーム
E. ネットワークアンダーレイ
正解: **(**正解を表示します**)**

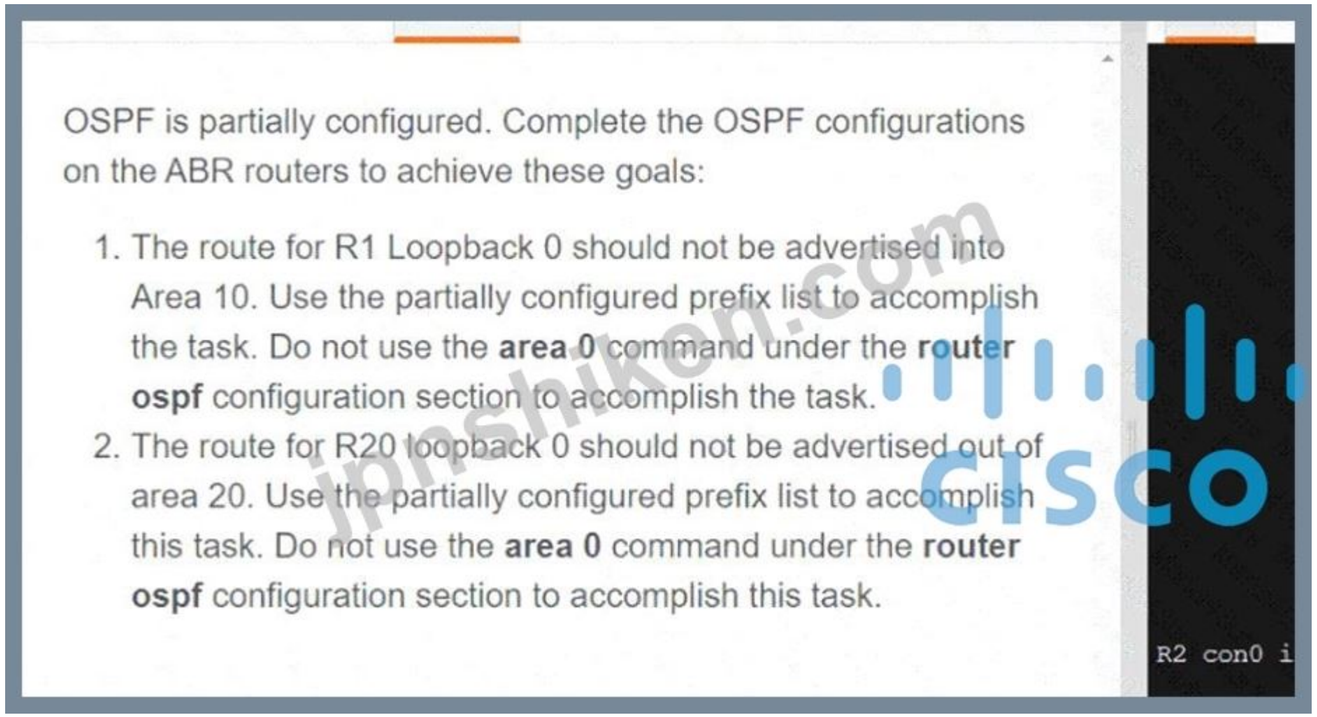
質問: **4**
Cisco ISE が 802.1X ベースの SSID 上のユーザーに VLAN を動的に割り当てることができるようにするには、Cisco Catalyst 9800 シリーズ WLC のどのラグ/プロファイルを変更する必要がありますか?
A. サイトタグ
B. ポリシープロファイル
C. インターフェースの遅延
D. WLAN プロファイル
正解: **(**正解を表示します**)**

質問: **5**
Cisco DNA Center ユーザ定義ネットワーク ワークフローはどのような機能を提供しますか?
A. IoTデバイスの自動セグメンテーション
B. AP設定用のインターフェース
C. APデバイスの自動プロビジョニング
D. 故障したデバイスの交換
正解: **(**正解を表示します**)**

質問: **6**

Guidelines | Topology | Tasks





正解:

See the solution below in Explanation:

Explanation:

Solution:

R2

R3

```
R3# sh run | s route|pref
router ospf 10
 router-id 10.0.1.3
 area 20 filter-list prefix deny_R20_Lo0 out
 network 10.0.1.0 0.0.0.255 area 0
 network 10.0.3.0 0.0.0.255 area 0
 network 10.0.23.0 0.0.0.255 area 0
 network 10.2.203.0 0.0.0.255 area 20
ip prefix-list deny_R20_Lo0 seq 5 deny 10.2.1.1/32
ip prefix-list deny_R20_Lo0 seq 10 permit 0.0.0.0/0 le 32
R3#
R3#
R3#
R3#
R3#
R3#
R3#wr
Building configuration...
```

質問: 7

Script

```
import ncclient

with ncclient.manager.connect(host='192.168.1.1', port=830, username='root', password='test123!',
    allow_agent=False) as m:
        print(m.get_config('running').data_xml)
```

Output

```
$ python get_config.py
Traceback (most recent call last):
  File "get_config.py", line 3, in <module>
    with ncclient.manager.connect(host='192.168.1.1', port=830, username='root',
AttributeError: 'module' object has no attribute 'manager'
```

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. ncclient からのインポート *

B. ncclient マネージャーのインポート

C. ncclientインポートマネージャーから

D. インポートマネージャー

正解: **C** (コメントを発表する)

質問: 8

ゼロトラスト セキュリティ モデルを可能にするアーキテクチャ コンポーネントはどれですか?

A. コントロールプレーン

B. プラグアンドプレイ

C. 管理プレーン

D. データプレーン

正解: (正解を表示します)

質問: **9**
Cisco SD-Access アンダーレイ ネットワークを設計する際の考慮事項は何ですか?
A. エンドユーザーのサブネットとエンドポイントは、アンダーレイ ネットワークの一部です。
B. 静的ルーティングが必須です。
C. アンダーレイ スイッチは、ユーザーにエンドポイントの物理接続を提供します。
D. IPv4 および IPv6 アンダーレイ ネットワークをサポートする必要があります。
正解: **C** (コメントを発表する)

質問: **10**
Cisco SD-Access にはどのような特性が適用されますか?
A. 制御プレーンにVXLANを使用する
B. PnPを使用して境界スイッチとアクセススイッチを検出し、プロビジョニングします。
C. ポリシープレーンにGREを使用します
D. 動的ルーティングを使用して境界スイッチとエッジスイッチを検出し、プロビジョニングします。
正解: (正解を表示します)

質問: **11**
ドラッグ＆ドロップ。図を参照してください。下部にあるコードスニペットをドラッグ＆ドロップして、Pythonスクリプトの空欄に貼り付け、PythonオブジェクトをJSON文字列に変換してください。すべてのオプションを使用するわけではありません。

```
import [                    ]

data = {
   "measurement": "freeMemory",
   "maxDataPoints": 30,
   "alert": True,
   "policy": "1.2.1",
   "devices": [{"model": "Cisco 2921 ISR", "ipv4": '10.10.10.1'}]
}
model = data["devices"][0]["model"]

json_string = [                    ](data)

print( [                    ])
```


model

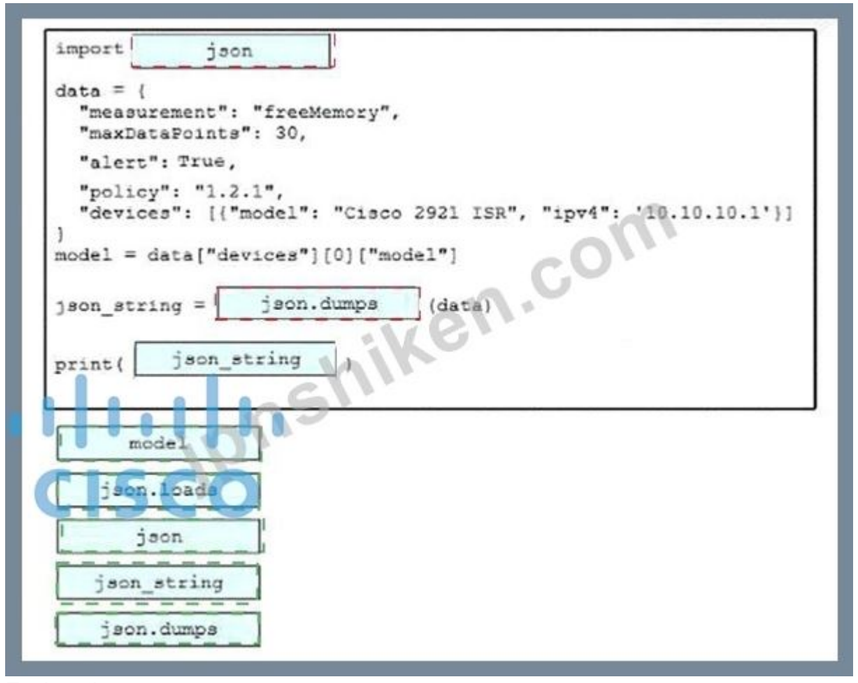
json.loads

json

json_string

json.dumps

正解:



Explanation:
Blank 1: C
Blank 2: E
Blank 3: D
The correct script must first import the JSON module, so the first blank is json, producing import json.
The Python object in the exhibit is a dictionary named data, containing fields such as measurement, policy, alert state, and device information. To convert a Python object into a JSON-formatted string, the correct function is json.dumps(). That makes the second blank json.dumps, producing json_string = json.dumps(data). The third blank must be json_string, because that is the variable containing the serialized JSON text that should be printed. json.loads() is the reverse operation; it parses a JSON- formatted string and converts it into a Python object, so it is not correct for object-to-string conversion.
model is merely a value extracted from the object and does not perform JSON serialization. The key distinction is dump/dumps versus load/loads: dumps returns a JSON string, while dump writes JSON to a file. References/topics: ENCOR Automation, Python data structures, JSON serialization, json.
dumps(), API payload handling, network programmability.

質問: 12
展示品を参照してください。

クライアントは、Web ベースの認証と外部 RADIUS サーバーを使用する新しい SSID を要求します。どのレイヤー 2 セキュリティ モードを選択する必要がありますか?

A. WPA2 + WPA3

B. WPA + WPA2

C. なし

D. 静的WEP

正解: **A** (コメントを発表する)

質問: **13**

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. スニファー

B. SEコネクト

C. 不正検出機能

D. モニター

正解: **B** (コメントを発表する)

質問: **14**

エンジニアは、REST APIを介してシステムをブルートフォースしようとする人々からの基本的なリプレイ攻撃をどのように防ぐことができますか？

A. APIヘッダーのリクエストにOAuthを追加します。

B. パスワードハッシュを使用する

C. UseHTTPS

D. APIヘッダーでリクエストにタイムスタンプを追加します。

正解: **D** (コメントを発表する)

質問: **15**

Cisco Threat Defense アーキテクチャのエンドポイント セキュリティの側面に当てはまる特性はどれですか。

A. 送信URL分析とデータ転送制御

B. ユーザーコンテキスト分析

C. メールの添付ファイル内のランサムウェアを検出してブロックする

D. クラウドベースの脅威分析
正解: **B** (コメントを発表する)

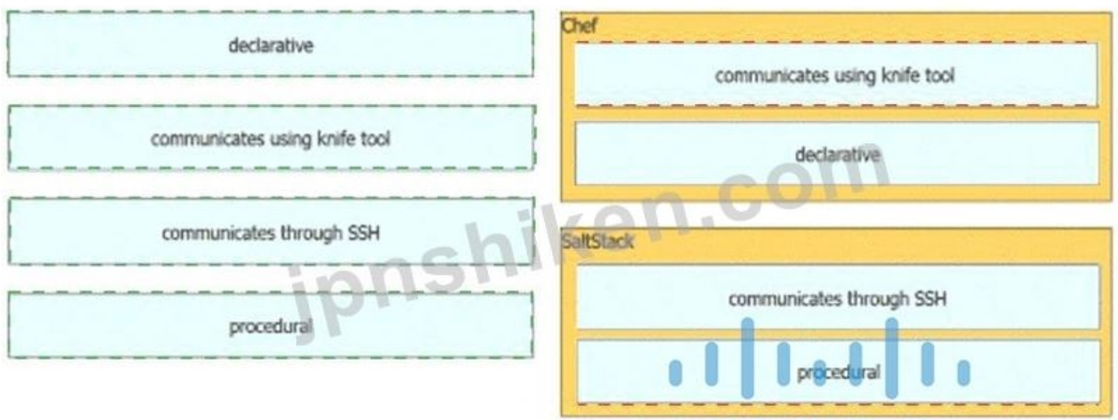
質問: **16**
SD-WANファブリックを介してサイト間のトラフィックを輸送するのはどの航空機ですか？
A. IPsec
B. マネジメント
C. データ
D. コントロール
正解: **C** (コメントを発表する)
The correct answer is C. Data.
Cisco SD-WAN architecture is divided into three main planes:
* Management Plane
* Handled by vManage
* Used for configuration and monitoring
* Control Plane
* 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: **17**
LISP マップ リゾルバはどのアクションを担当しますか?
A. EIDからRLOCへのマッピングを見つける

B. ITRからのマップ要求メッセージを受け入れる
C. ETRからの登録リクエストを受け付ける
D. ユーザーデータトラフィックの転送
正解: **D** (コメントを発表する)

質問: **18**
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。

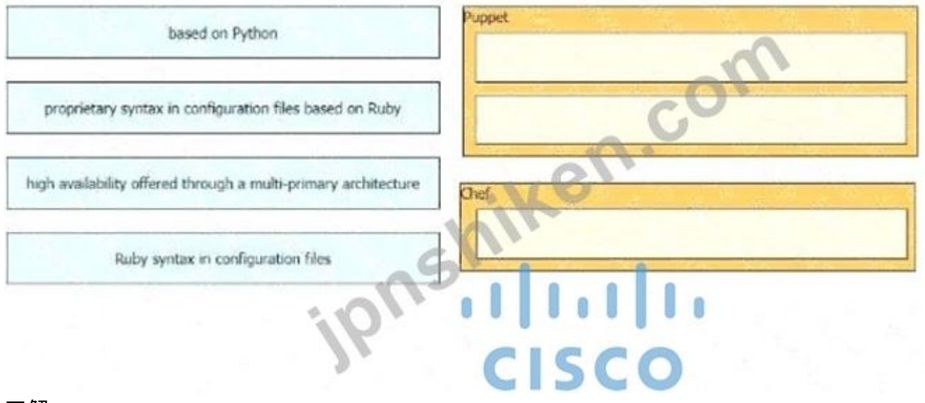
正解:



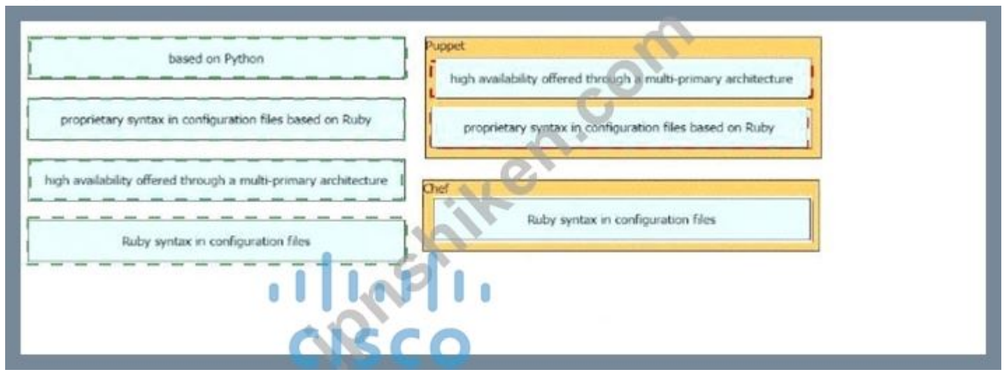
Explanation:

質問: **19**

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。

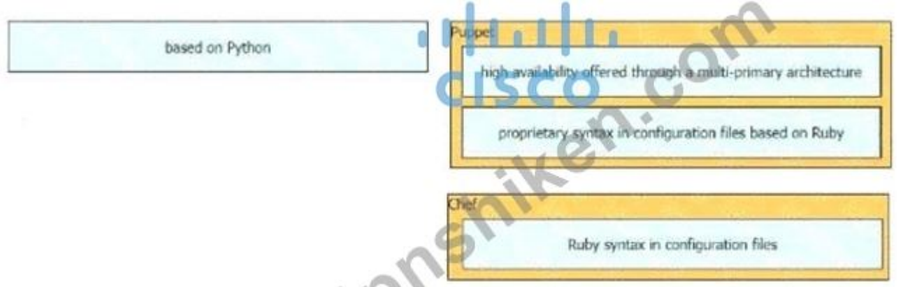


正解:

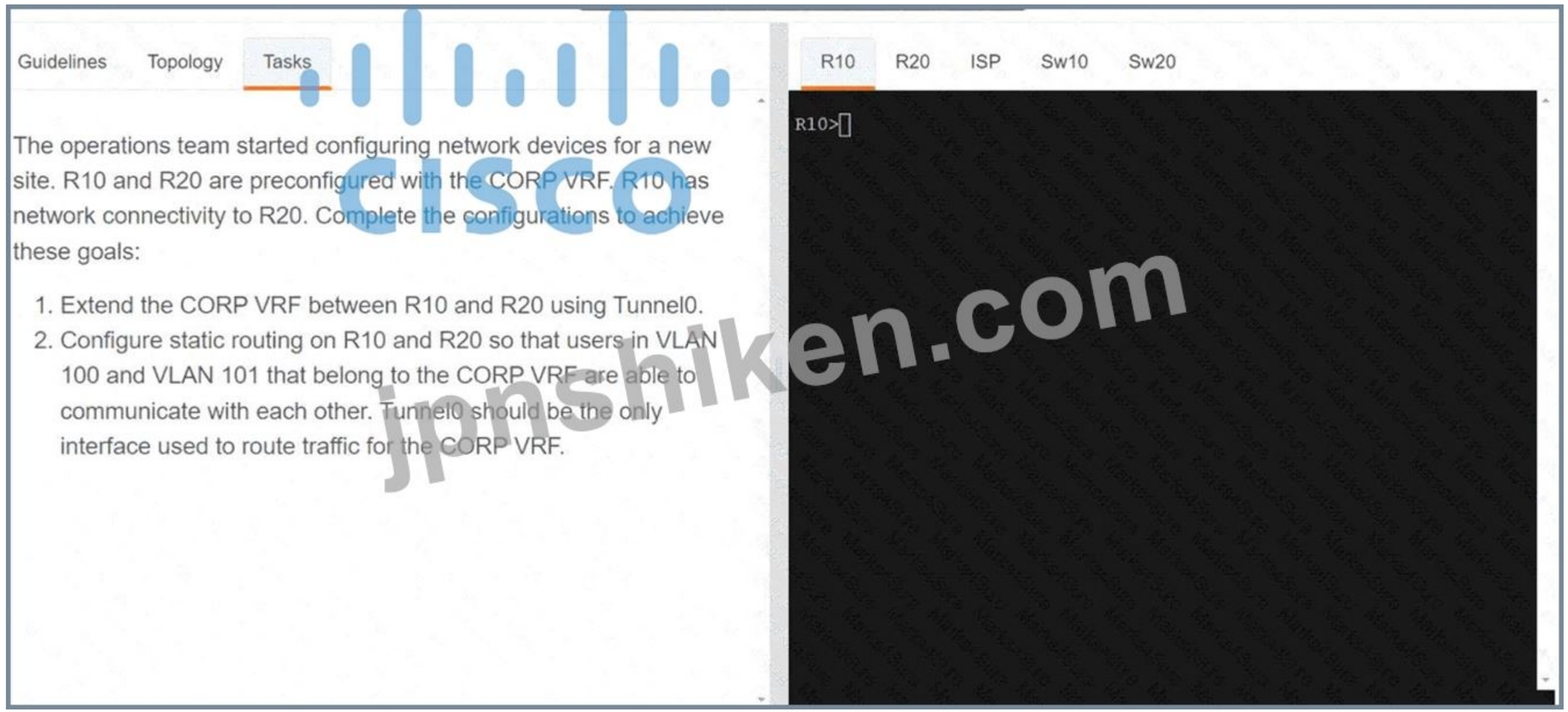


Explanation:

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



質問: 20



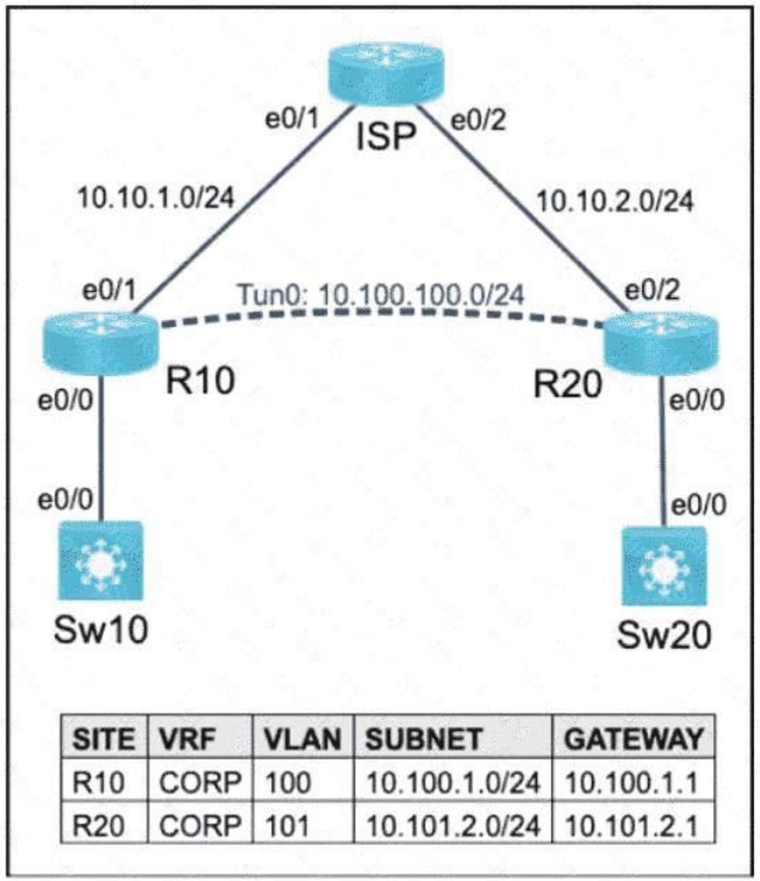
または

Guidelines Topology Tasks

The operations team started configuring network devices for a new site. R10 and R20 are preconfigured with the CORP VRF. R10 has network connectivity to R20. Complete the configurations to achieve these goals:

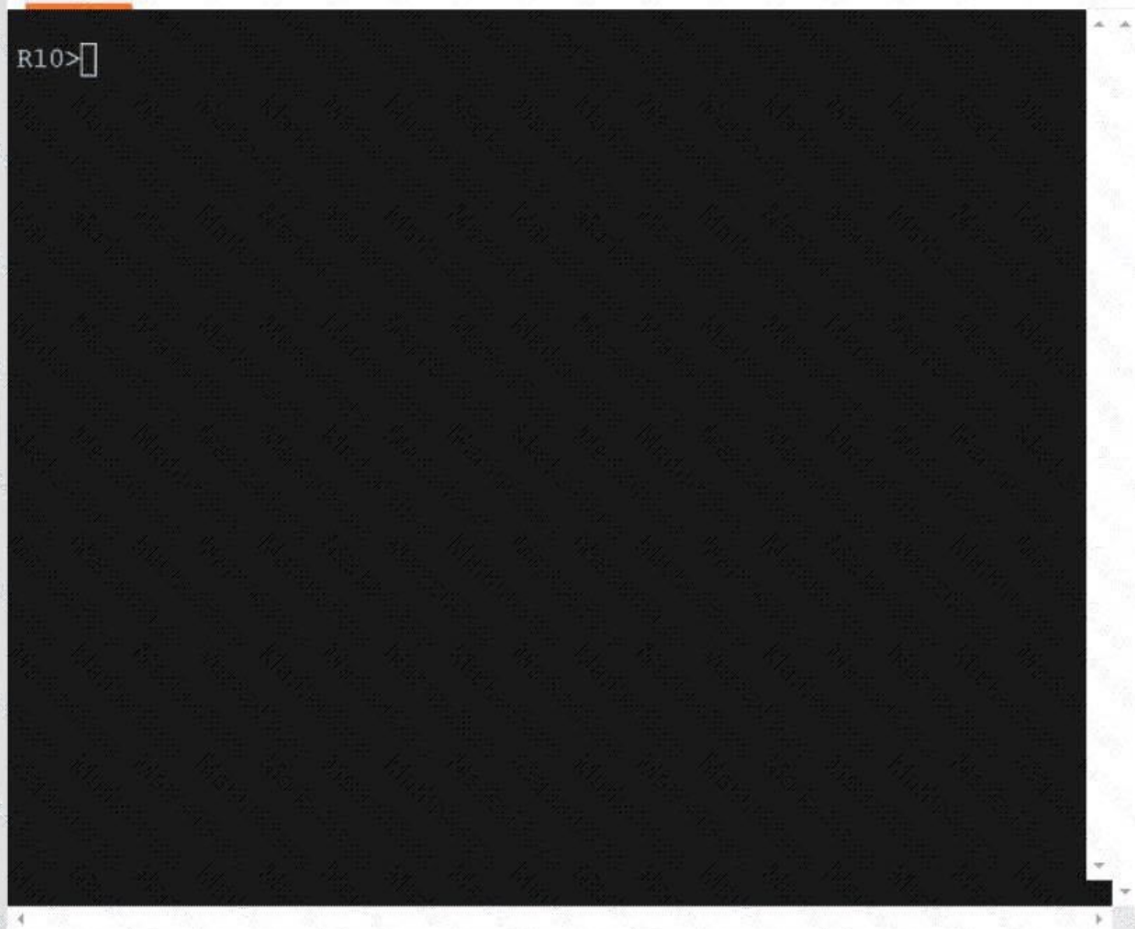
1. Extend the CORP VRF between R10 and R20 using Tunnel0.
2. Protect Tunnel0 using the preconfigured profile
3. Configure static routing on R10 and R20 so that users in VLANs100 and 101 that belong to the CORP VRF are able to communicate with each other. Tunnel0 should be the only interface used to route traffic for the CORP VRF

Guidelines | Topology | Tasks

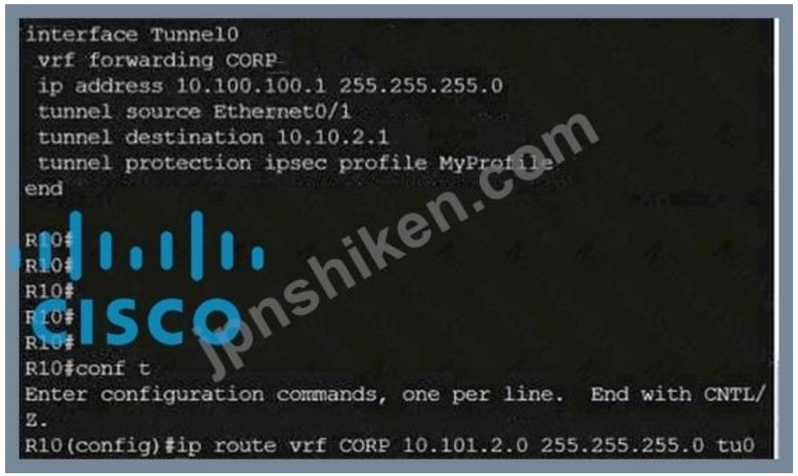


SITE	VRF	VLAN	SUBNET	GATEWAY
R10	CORP	100	10.100.1.0/24	10.100.1.1
R20	CORP	101	10.101.2.0/24	10.101.2.1

R10 | R20 | ISP | Sw10 | Sw20



正解:
See the solution below in Explanation:
Explanation:
Solution:
R10



Copy run start

R20

Copy run start

Verification:

質問: 21

環境内の新しいクライアントをサポートするには、エンジニアが企業の WLAN で Fast Transition を有効にする必要があります。

Cisco Catalyst 9800 シリーズ WLC に適用する必要があるコマンドはどれですか?

A. セキュリティ ft adaptive

B. セキュリティ wpa akm psk

C. セキュリティ wpa akm ft psk

D. セキュリティ wpa akm dotlx
正解: (正解を表示します)

質問: **22**
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. 10
B. 15
C. 20
D. 25
正解: (正解を表示します)

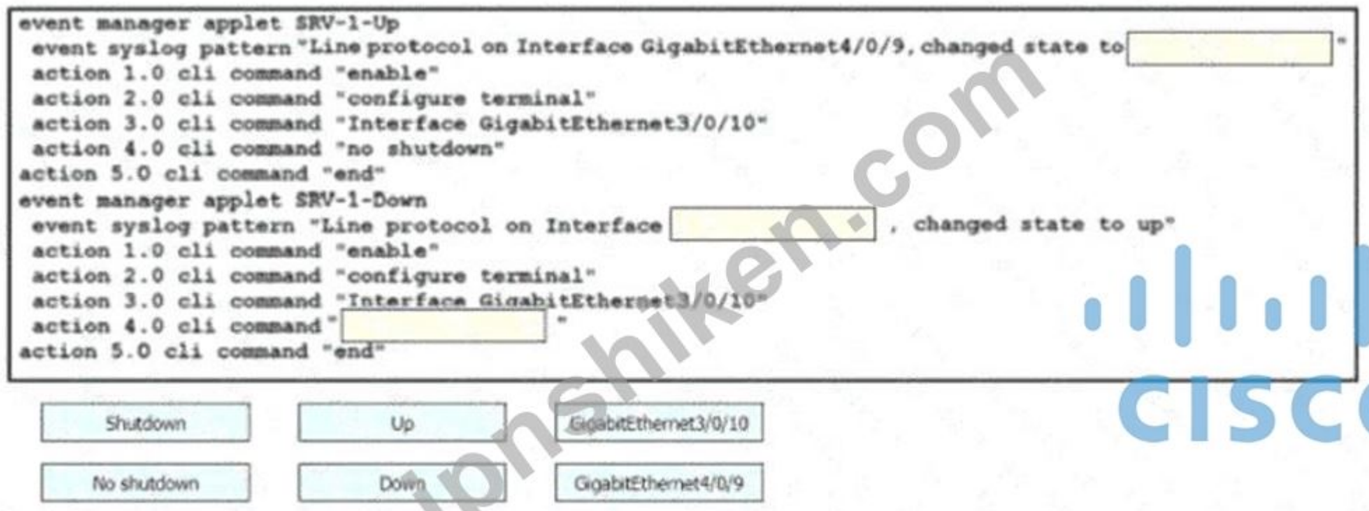
質問: **23**
従来のWANソリューションには当てはまるが、Cisco Catalyst SD-WANソリューションには当てはまらない特性はどれですか？
A. 集中管理されたアクセス性、セキュリティ、およびアプリケーションポリシー
B. 時間のかかる設定とメンテナンス
C. 低複雑度で全体的なソリューション規模が拡大
D. DTLS/TLS認証済みでセキュアなトンネル上で動作します
正解: (正解を表示します)
The correct answer is B. Time-consuming configuration and maintenance .
In a traditional WAN 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: **24**
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. データプレーン

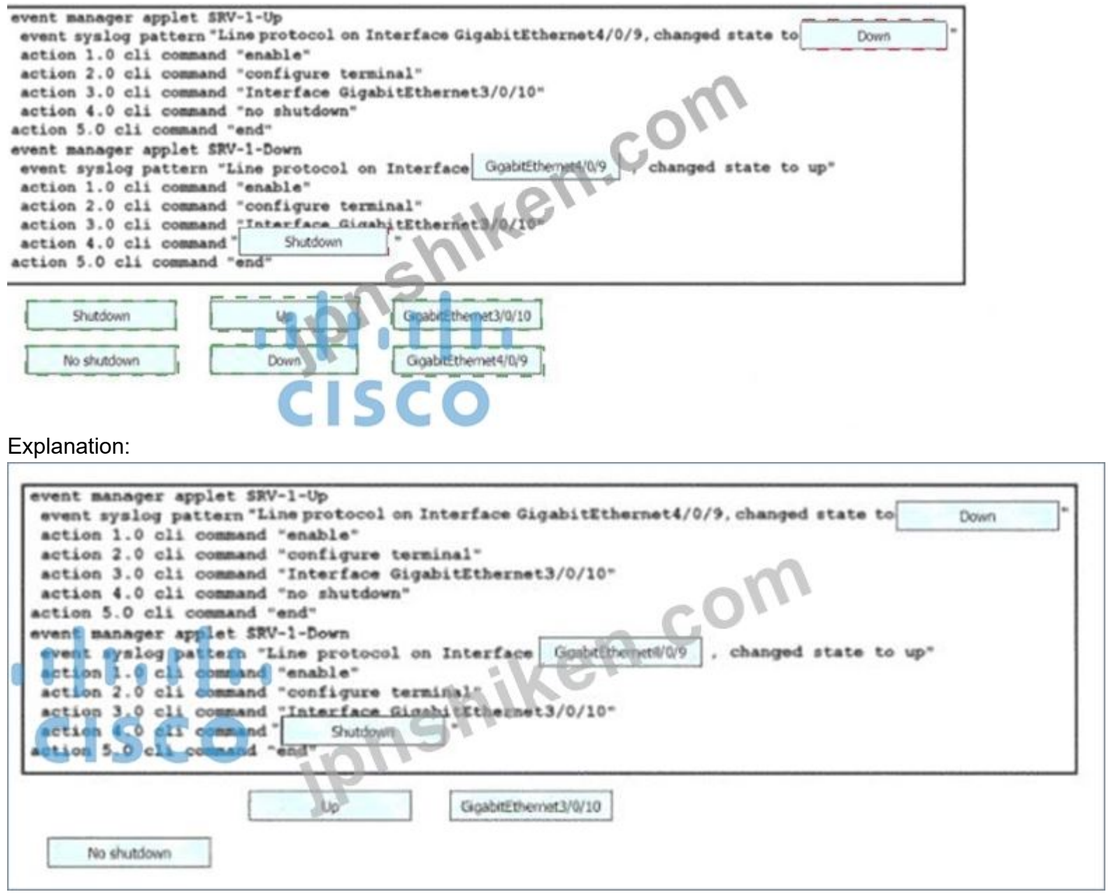
B. オーケストレーションプレーン
C. 管理プレーン
D. コントロールプレーン
正解: (正解を表示します)

質問: **25**
どのファースト ホップ冗長プロトコルがアップリンクの使用率を最大化し、必要な構成の量を最小限に抑えますか?
A. HSRP v2
B. HSRP v1
C. GLBP
D. VRRP
正解: (正解を表示します)

質問: **26**
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: **27**
クライアントの信頼性を検証するために使用され、HTTP リクエストで JSON オブジェクトとして送信されるものは何ですか?
A. TLS
B. HTTPS
C. SSH
D. JWT
正解: (正解を表示します)

質問: **28**
顧客は、異なるパスワードを使用して IoT デバイスを認証するために単一の SSID を使用したいと考えています。この要件を満たすには、Cisco ISE と組み合わせてどのレイヤー 2 セキュリティ タイプを設定する必要がありますか?
A. Cisco 集中キー管理
B. 中央Web認証
C. アイデンティティPSK

D. 高速遷移
正解: (正解を表示します)

質問: **29**
データ モデリング言語を採用することの利点は何ですか?
A. ステータスサブスクリプション用のSNMPなどの管理プロトコルの使用を強化する
B. 多数のデバイスを管理するためにマシンフレンドリーなコードを導入する
C. モデルに関するベンダー中心のアクションを使用して管理プロセスを拡張する
D. ベンダーおよびプラットフォーム固有の構成を、広く互換性のある構成にリファクタリングする
正解: (正解を表示します)

質問: **30**

添付資料を参照してください。POSTMAN は、Cisco Catalyst Center(旧 DNA Center)API からネットワークデバイス情報を取得しようとしていることを示しています。問題は何でしょうか？
A. JSONペイロードに不正なUUIDが含まれています
B. URI文字列が正しくありません
C. トークンの有効期限が切れました
D. 認証に失敗しました
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. ブリッジ
B. フレックスコネクト
C. ローカル
D. ファブリック
正解: **C** (コメントを発表する)

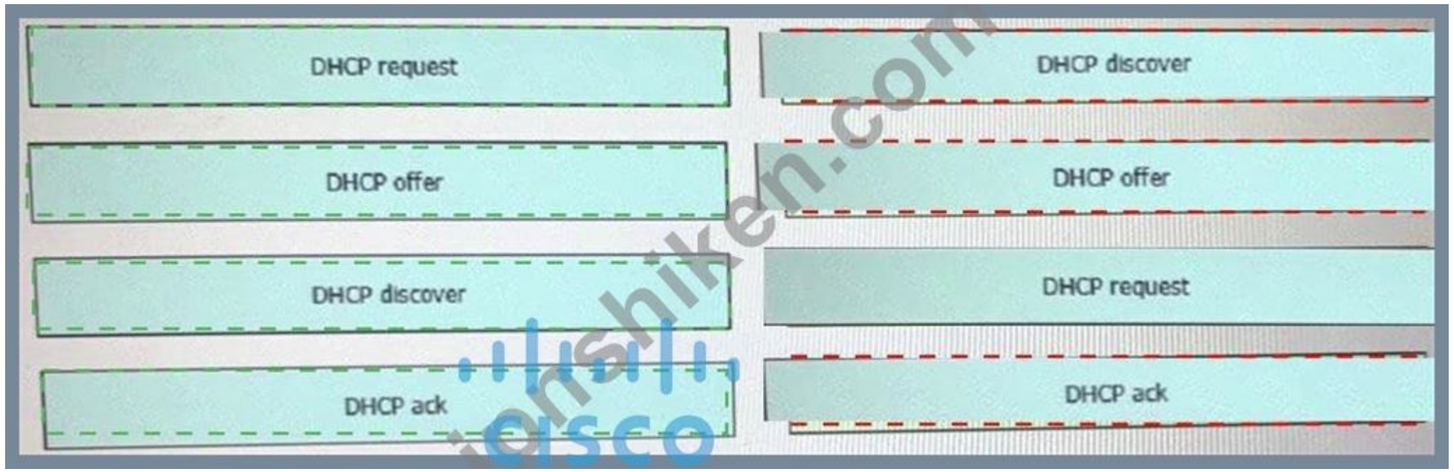
質問: **32**
タイプ 1 ハイパーバイザーとは何ですか?
A. 仮想サーバー上で実行され、既にインストールされているオペレーティングシステムに依存します。
B. 仮想サーバー上で実行され、独自のオペレーティングシステムが含まれています
C. 物理サーバー上で直接実行され、以前にインストールされたオペレーティングシステムに依存します。
D. 物理サーバー上で直接実行され、独自のオペレーティングシステムが含まれています
正解: **(**正解を表示します**)**

質問: **33**
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. ポリシータグ
B. APタグ
C. RFタグ
D. サイトタグ
正解: **(**正解を表示します**)**

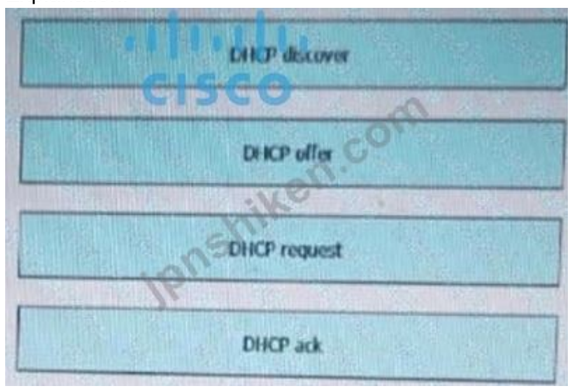
質問: **34**
VXLAN ヘッダーには何が含まれていますか?
A. 元のレイヤー2 VLAN ID
B. VXLANネットワーク識別子
C. エンドポイントID
D. 送信元と送信先のRLOC ID
正解: **B (**コメントを発表する**)**

質問: **35**
クライアントと AP 間で交換される DHCP メッセージを、右側の交換順序にドラッグ アンド ドロップします。

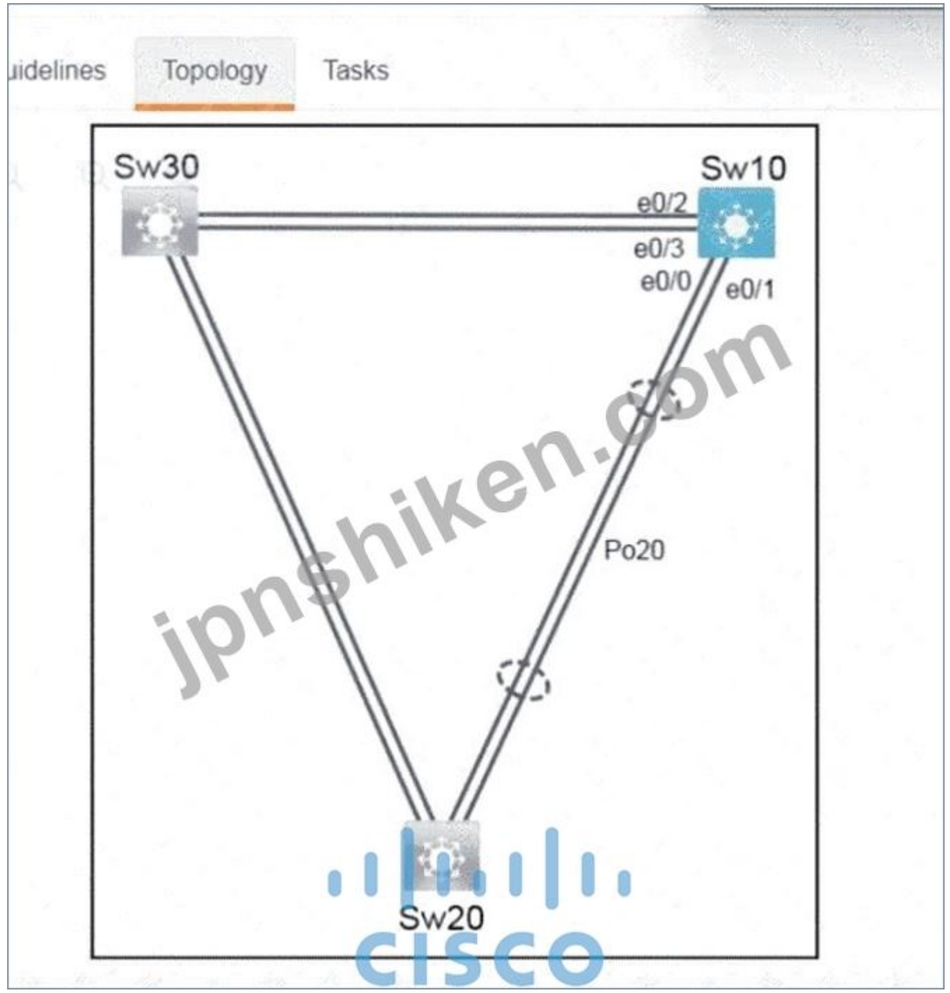

正解:



Explanation:



質問: 36


uidelines
Topology
Tasks
Sw30
Sw10
e0/2
e0/3
e0/0
e0/1
Po20
Sw20
jpnshiken.com
CISCO

Complete the tasks below by making changes to Sw10 only. No access is provided to Sw20 or Sw30.

Task 1

Sw20 is actively attempting to negotiate an 802.1 trunking EtherChannel with Sw10 using LACP, but the channel is not functional. Resolve the issues on Sw10.

Task 2

Modify the spanning tree configuration to ensure that Sw10 is always the root for VLAN 20.

正解:

See the solution below in Explanation:

Explanation:

Solution:

Sw10

config t

no int po20

int et0/0

channel-group 20 mode active

no shut

spanning-tree vlan 20 pri 0

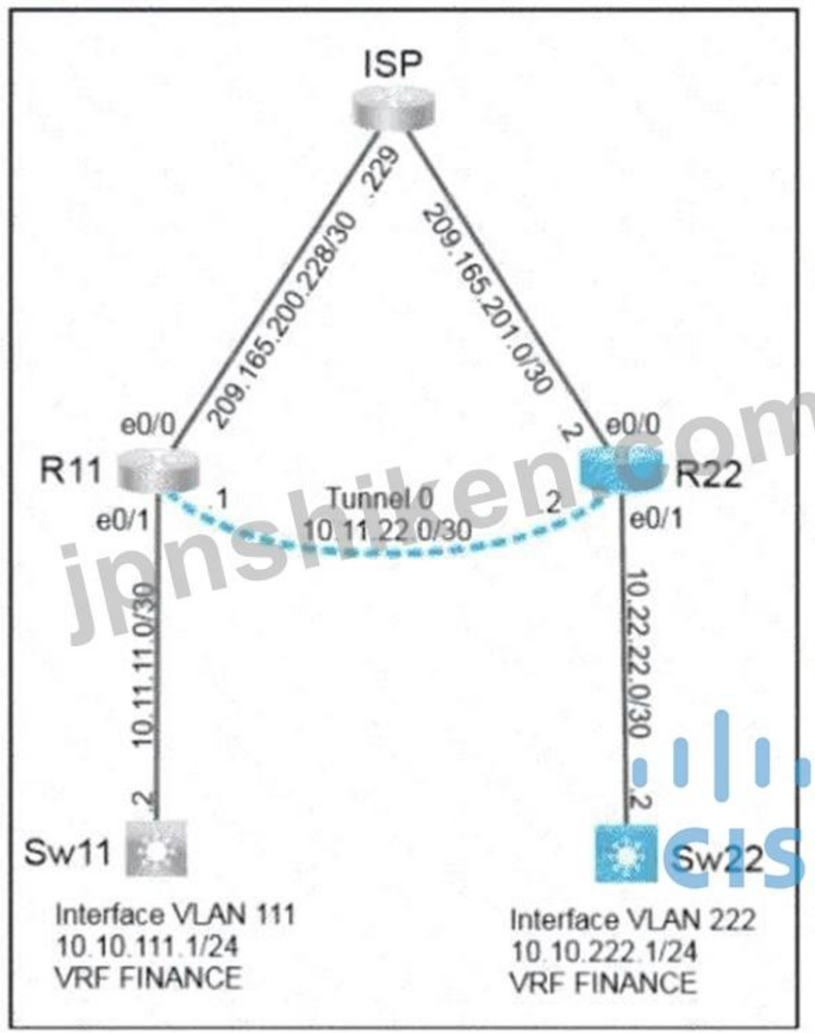
wr

Verification:-

```
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------
------------
20     Po20(SU)      LACP        Et0/0(P)
```


質問: 37


ISP
209.165.200.228/30
.229
209.165.201.0/30
.2
e0/0
e0/0
R11
R22
.1
Tunnel 0
10.11.22.0/30
.2
e0/1
e0/1
10.11.11.0/30
.2
10.22.22.0/30
.2
Sw11
Sw22
Interface VLAN 111
10.10.111.1/24
VRF FINANCE
Interface VLAN 222
10.10.222.1/24
VRF FINANCE

Guidelines Topology Tasks

A colleague started configuring a new network. All configurations on R11 are complete and communication between R11 and R22 is functional. Complete the configurations on R22 for the tasks below.

Task 1

Extend the Finance VRF between R11 and R22 using Tunnel 10.

Task 2

Complete the Finance VRF configuration on R22 and configure static routing so that traffic between VLAN 111 and VLAN 222 uses Tunnel 10 exclusively.

Note: Sw22 can be used to validate traffic flow.

正解:

See the solution below in Explanation:

Explanation:

Solution:

R22

config t

int tunn0

vrf forwarding FINANCE

ip add 10.11.22.2 255.255.255.0

tunn so e0/0

tunn dest 209.165.200.230

no shut

int et0/1

vrf forward FINANCE
ip add 10.22.22.1 255.255.255.252
no shut
ip route vrf FINANCE 10.10.111.0 255.255.255.0 tunn0
wr

質問: 38
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: 39
Cisco Catalyst Center(旧称 :DNA Center)において、類似のネットワーク設定を持つデバイスに適用可能な汎用構成を作成するために使用されるツールはどれですか？
A. 認証テンプレート
B. テンプレートエディター
C. アプリケーションポリシー
D. コマンドランナー
正解: (正解を表示します)

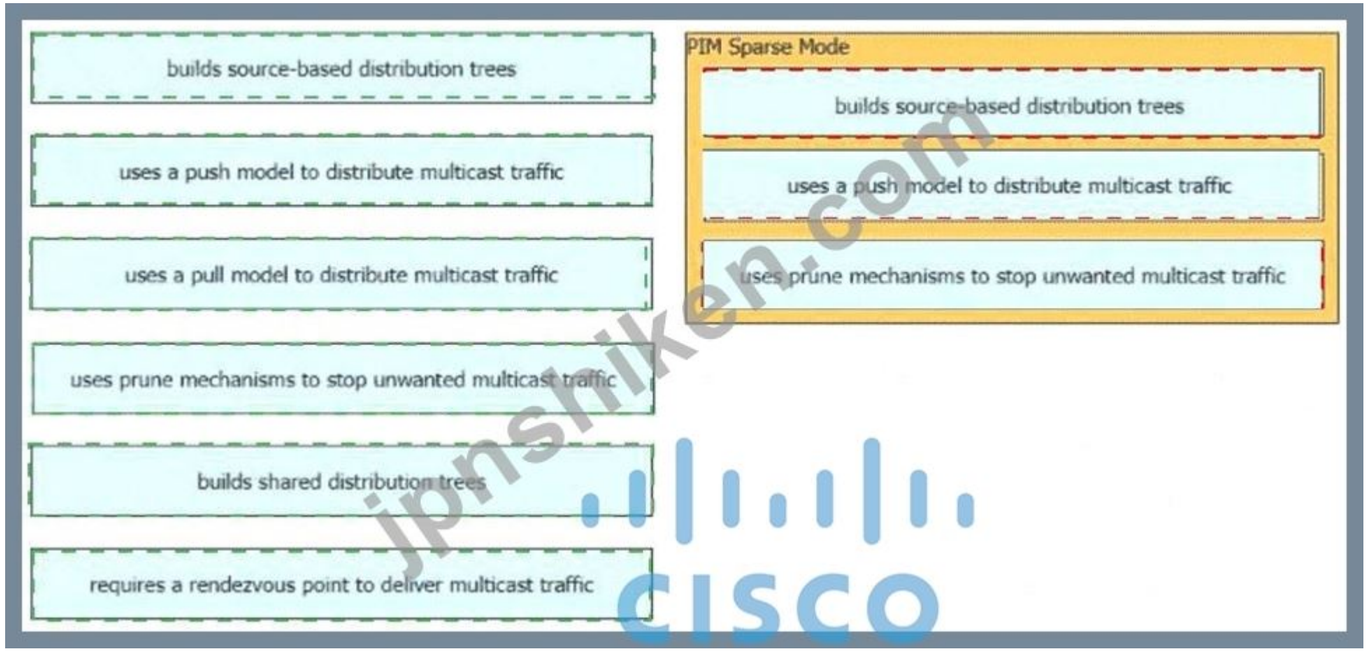
The correct answer is B. Template Editor.
Cisco Catalyst Center provides template-based automation to deploy configurations consistently across multiple devices.
* The Template Editor is specifically used to:
* Create reusable configuration templates
* Use variables and parameters for different devices
* Apply configurations to multiple devices with similar roles/settings
* It supports Jinja2-based templates, enabling dynamic and scalable deployments.
This directly matches the requirement:
"build generic configurations that are able to be applied on devices with similar network settings"
* A. Authentication Template This is not a primary Catalyst Center tool for building reusable configuration templates.
* C. Application Policies Used for QoS and traffic policies, not for general configuration templating.
* D. Command Runner Used to execute ad hoc CLI commands on devices, not to build reusable configurations.
* Template Editor = Build reusable configs
* Command Runner = Run one-time commands
* Application Policies = Define traffic/QoS behavior
Automation in Catalyst Center = Template-based deployment

質問: 40
ログイン方法は、ルータのVTY回線上で以下のパラメータを使用して設定されます。
* 認証の最初の方法はTACACS+で　す
* TACACSが利用できない場合、認証情報が提供されなくてもログインが許可されます。このタスクを実現する構成はどれですか？
A. aaa 新モデル
aaa認証ログインtelnetグループtacacs+なし
aaa セッション ID 共通
B. aaa 新モデル
aaa認証ログインデフォルトグループtacacs+
aaa セッション ID 共通
C. aaa 新モデル
aaa認証ログインデフォルトグループtacacs+なし
aaa セッション ID 共通
D. aaa 新モデル
aaa 認証ログイン VTY グループ tacacs+ なし
aaa セッション ID 共通
正解: **(**正解を表示します**)**
The correct answer is C. aaa authentication login default group tacacs+ none.
Cisco AAA authentication uses a method list, where methods are tried in order. The keyword none is critical here.
* group tacacs+ # First attempt authentication using TACACS+ servers
* none # If TACACS+ servers are unreachable, no authentication is required (access is granted) aaa authentication login default group tacacs+ none This configuration:
* Tries TACACS+ authentication first
* If TACACS+ is unavailable # falls back to no authentication, allowing login without credentials This exactly satisfies the requirement.
* A. aaa authentication login telnet group tacacs+ none # Uses a named method list (telnet) # Not applied to VTY lines unless explicitly configured (login authentication telnet)

* B. aaa authentication login default group tacacs+ # No fallback method # If TACACS fails # login is denied
* D. aaa authentication login VTY group tacacs+ none # Named method list (VTY) # Must be explicitly applied under VTY lines (login authentication VTY) AAA fallback keywords:
* local # fallback to local username/password
* none # no authentication required (open access)
Important Pattern:
aaa authentication login default group tacacs+ none
= TACACS first # allow access if server is unreachable

質問: 41
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: 42

Cisco DNA Center サウスバウンド API の機能は何ですか?

A. ServiceNow などの 10 個の ITSM サービスに接続します。

B. 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。
C. 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。
D. 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。
正解: **(**正解を表示します**)**

質問: **43**
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. ECMP
B. RSVP
C. HSRP
D. NSF
正解: **(**正解を表示します**)**

質問: **44**
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. vBond
C. vSmart
D. vEdge
正解: **(**正解を表示します**)**

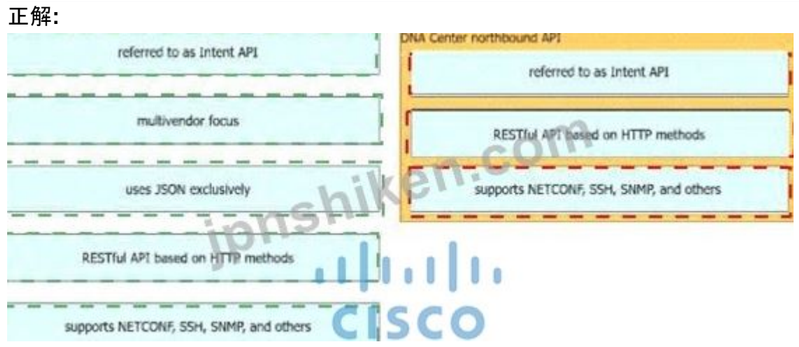
質問: **45**
キャンパスのレイヤー 3 インフラストラクチャを設計する際のベスト プラクティスを 2 つ挙げてください。(2 つ選択してください。)
A. 非トランジットリンクにパッシブインターフェースを設定します。
B. 集約レイヤーからコアレイヤーへのルートを要約します。
C. アクセス レイヤーから集約レイヤーに向かって要約します。
D. ECMP ルーティングの Cisco Express Forwarding ロード バランシング ハッシュを調整します。
E. コア部分にセキュリティ機能を実装します。
正解: **B,D (**コメントを発表する**)**

質問: **46**
Cisco SD-Access ファブリックの中間ノードの機能は何ですか?
A. ファブリックと外部リソース間の入口と出口を提供する
B. VXLANヘッダーでパケットをカプセル化およびカプセル化解除する
C. ヘッダー内のレイヤー3情報に基づいてファブリック内でパケットをルーティングする
D. 同じサブネット上のファブリッククライアントと非ファブリッククライアント間の到達可能性を提供する
正解: **(**正解を表示します**)**

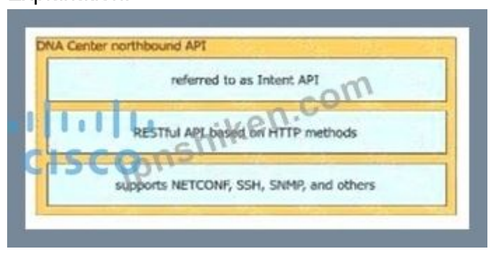
質問: 47

Cisco Catalyst Center（旧DNA Center）ノースバウンドAPI特性を左から右へドラッグ＆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:



質問: 48

Mobility Express モードで動作している AP の特徴は何ですか?

A. WLC 冗長性には少なくとも 3 つの AP が必要です。

B. AP が WLC として機能する必要があります。

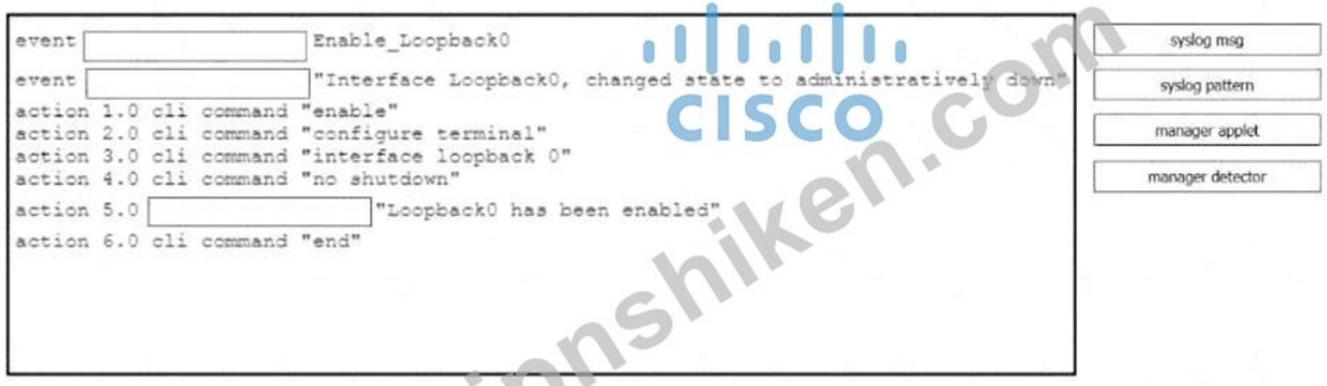
C. 大規模な展開に推奨されます。
D. 集中型 WLC が必要です。
正解: **(**正解を表示します**)**

質問: **49**
タイプ 2 ハイパーバイザーの特徴は何ですか?
A. 複雑な展開
B. クイック展開
C. データセンターに最適
D. ベアメタルと呼ばれる
正解: **(**正解を表示します**)**

質問: **50**
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)# netconf max-sessions 100
B. Device(config)# no netconf ssh acl 1
C. Device(config)# netconf max-message 1000
D. Device(config)# netconf lock-time 500
正解: **C (**コメントを発表する**)**

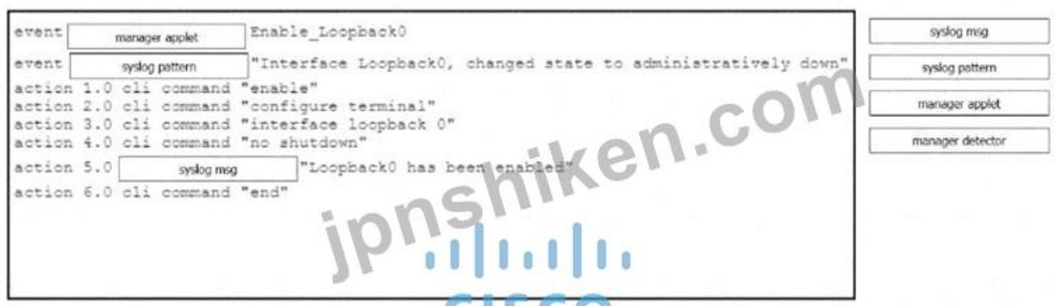
質問: **51**
Cisco Catalyst SD-WAN は、コントロール プレーン通信を保護するためにどのプロトコルを使用しますか?
A. IPsec
B. DTLS
C. STUN
D. OMP
正解: **B (**コメントを発表する**)**

質問: **52**
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: 53

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. 東行きのイベントと通知
C. サウスバウンド マルチベンダー サポート
D. 西行き統合
正解: **(**正解を表示します**)**

質問: **54**
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. Sniffer
B. Local
C. Monitor
D. H-REAP
正解: **(**正解を表示します**)**

質問: **55**
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. シグネチャベースのマルウェア
B. DMZ Web サーバーの脆弱性
C. DDoS
D. ゼロデイ攻撃
正解: **(**正解を表示します**)**

質問: **56**
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. DNS 保護
B. ネットフロー
C. トラストセック
D. 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: **57**
Cisco DNA Center および vManage ノースバウンド API の特徴は何ですか?
A. XML 形式のコンテンツを交換します。
B. NETCONF プロトコルを実装します。
C. 構成の変更をデバイスにプッシュします。
D. RESTCONF プロトコルを実装します。
正解: **D (**コメントを発表する**)**

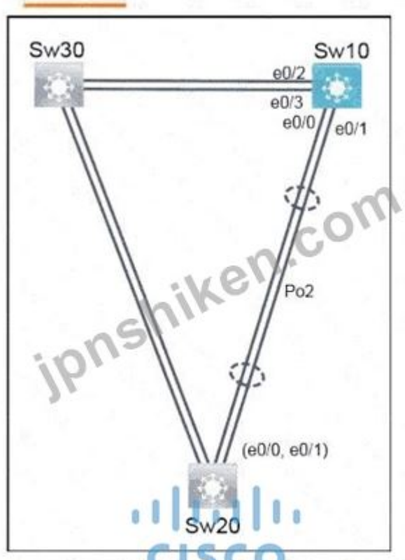
質問: **58**

Cisco SD-Access ファブリックのファブリック データ プレーンはどのプロトコルまたはテクノロジーに基づいていますか?
A. LISP
B. IS-IS
C. シスコ トラストセック
D. VXLAN
正解: **(**正解を表示します**)**

質問: **59**
データ モデリング言語を使用して API クライアント アプリケーションを開発する利点は何ですか?
A. 互換性の向上
B. リソース要件が低い
C. より強力なセキュリティ特性
D. 機能拡張が容易
正解: **(**正解を表示します**)**

質問: **60**
YANGデータモデルに含まれる項目はどれですか？(2つ選択してください。)
A. HTTPリターンコード
B. RPCステートメント
C. JSONスキーマ
D. XMLスキーマ
E. コンテナステートメント
正解: **B,E (**コメントを発表する**)**
The correct answers are B. rpc statements and E. container statements.
YANG is a data modeling language used to model configuration and operational data for protocols such as NETCONF and RESTCONF. In YANG, the model is built using defined language statements such as container, list, leaf, and rpc.
Cisco documentation explains that actions are defined in YANG models using RPC statements, and the YANG language definition identifies container as a standard statement used to define an interior data node in the schema tree.
Cisco documentation states that YANG models can define operational actions using RPC statements. These are used to trigger operations such as commands or actions on the device.
A container is one of the fundamental building blocks of a YANG model. It represents an interior node in the hierarchical data tree and is commonly used to group related configuration or state data.
* A. HTTP return codes These belong to HTTP-based protocol behavior, not to the YANG model language itself.
* C. JSON schema YANG is not a JSON schema language. Although YANG data may be encoded in JSON for some APIs, JSON schema is not a YANG model element. Cisco notes that protocols may use JSON formatting, but that does not make JSON schema part of YANG.
* D. XML schema YANG is its own modeling language. NETCONF commonly uses XML encoding, but XML schema itself is not one of the YANG language statements.
ENCOR exam point:
Know the difference between:
* YANG model elements # container, list, leaf, rpc
* Data encodings / transport formats # XML, JSON
* Protocol behaviors # HTTP status codes, NETCONF operations

質問: **61**



Complete the tasks below by making changes to Sw10 only. No access is provided to Sw20 or Sw30.

Task 1

Sw20 is actively attempting to negotiate an 802.1 trunking EtherChannel with Sw10 using LACP, but the channel is not functional. Resolve the issues on Sw10.

Task 2

Modify the spanning tree configuration to ensure that Sw10 is always the root for VLAN 10.

正解:

See the solution below in Explanation:

Explanation:

Solution:

Sw10

config t

no int po2

int et0/0

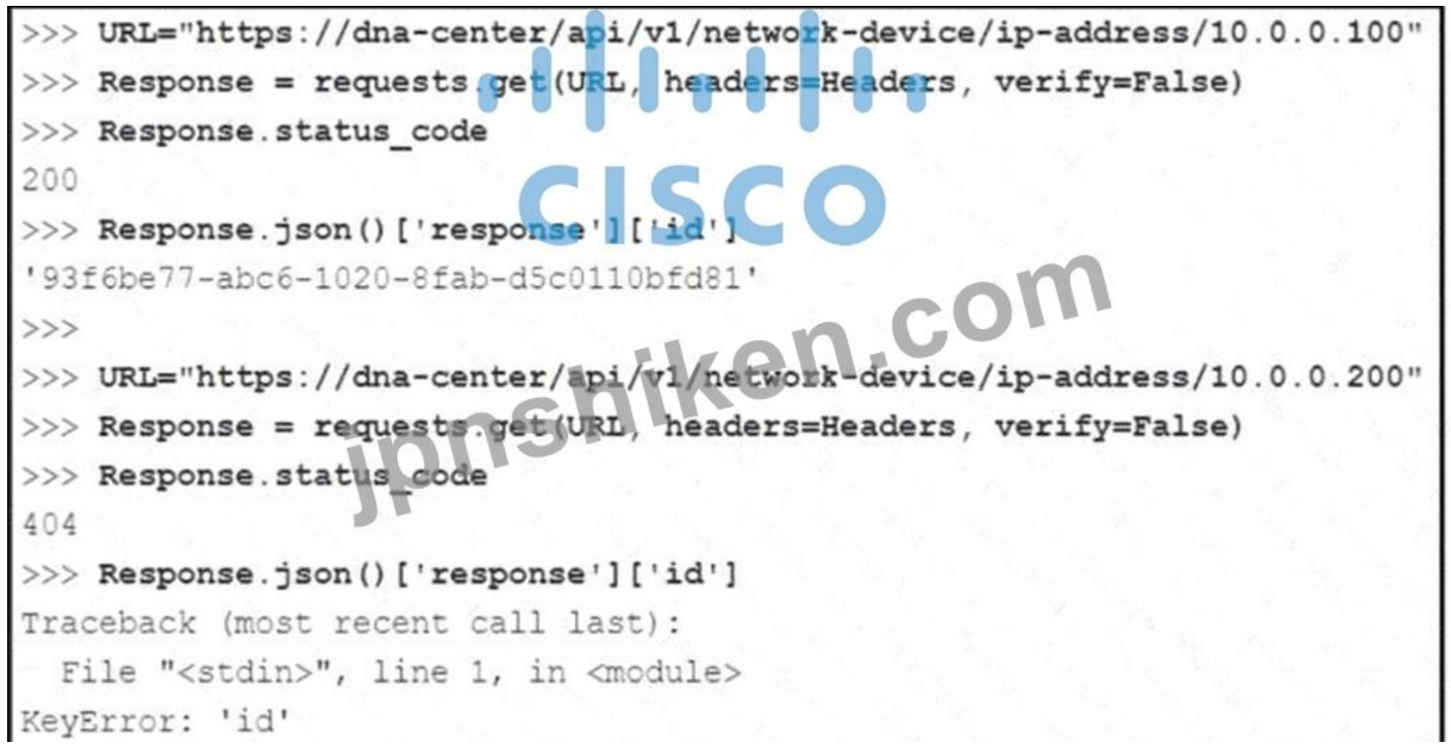
channel-group 2 mode active

no shut

spanning-tree vlan 10a pri 0

wr

質問: **62**



展示を参照してください。出力から何が分かりますか？

A. 10.0.0.100 は Cisco Catalyst Center (旧 DNA Center) によって管理されています。

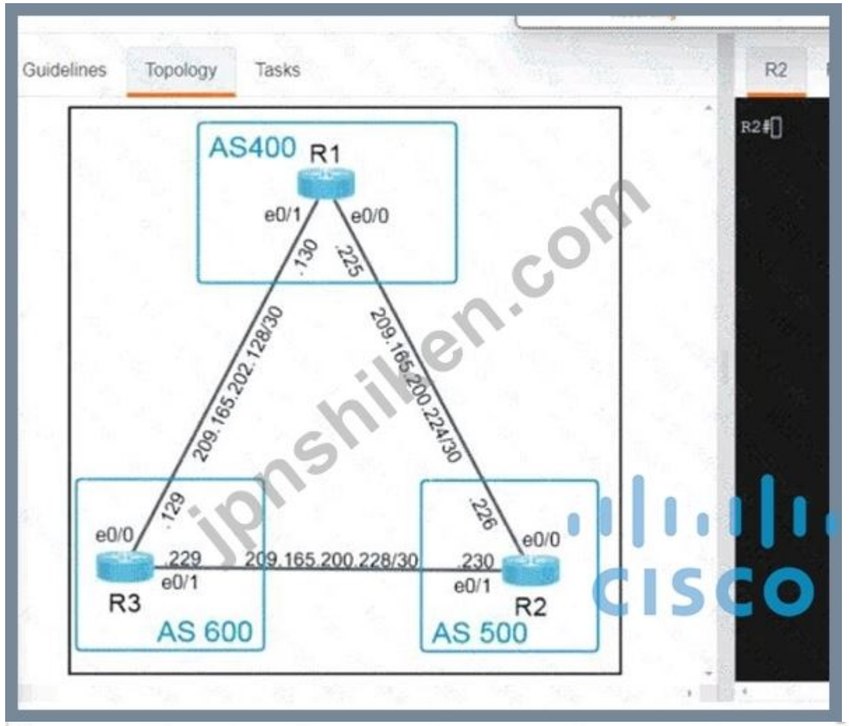
B. 2 番目のクエリの URL は構文的に正しくありません。

C. 10.0.0.200 は DNA Center に認識されていますが、その ID は空の文字列です。

D. 2 番目のクエリの認証は失敗します。

正解: **(**正解を表示します**)**

質問: **63**



Configure R2 according to the topology to achieve these results:

1. Configure eBGP using Loopback 0 for the router-id. Do not use the address-family command to accomplish this.
2. Advertise R2's Loopback 100 and Loopback 200 networks to AS400 and AS600.

正解:

See the solution below in Explanation:

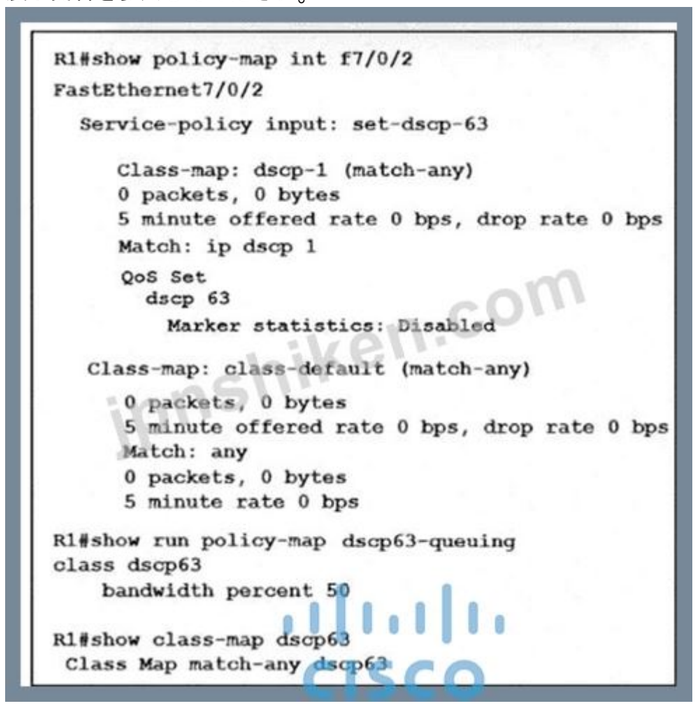
Explanation:

Solution:-

Copy run start

質問: 64

展示資料を参照してください。



ネットワークエンジニアが、ルーターR1でQoSを設定し、音声トラフィックとビデオトラフィックに異なるDSCP値を割り当てて優先順位を付けています。この設定による2つの結果は何ですか？(2つ選択してください。)

A. 帯域幅が50パーセントに達すると、送信時にスケジューリングが適用されます。

B. インターフェース Fa7/0/2 に入るパケットの DSCP1 マーキングは DSCP63 に変更されます。

C. 帯域幅が50パーセントに達すると、出力時にキューイングが適用されます。

D. インターフェース Fa7/0/2 に入るパケットの DSCP マーキングは変更されません。

E. 帯域幅が50パーセントに達したときに、DSCP63でマークされたトラフィックの分類が行われます。

正解: **(**正解を表示します**)**

The input service policy shown in the exhibit matches traffic with DSCP value 1 and applies a QoS set action to rewrite that marking to DSCP 63. Therefore, packets entering interface Fa7/0/2 with DSCP 1 are remarked to DSCP 63, making option B correct. The second part of the configuration defines a class map matching DSCP 63 and a policy map using bandwidth percent 50. That behavior belongs to class-based queuing/scheduling, where DSCP63-marked traffic is placed into a class that receives a bandwidth allocation. In the given option set, option C best represents this queuing behavior. Option D is wrong because the service policy explicitly changes the DSCP value. Option E is not accurate because classification is not triggered by reaching 50 percent bandwidth; classification occurs by matching packet fields such as DSCP. Option A is less precise than C because the shown policy behavior is class- based queuing with a bandwidth allocation. The important ENCOR concept is the separation between marking on ingress and queuing/scheduling on egress. References/topics: ENCOR Infrastructure, QoS, MQC, class maps, policy maps, DSCP marking, CBWFQ, bandwidth percent.

質問: **65**
スクリプトにステートメント white loop != 999 ' が含まれています。どの値がループを終了しますか?
A. 999 と等しくない値。
B. 999 以上の値。
C. 999 以下の値。
D. 999 に等しい値。
正解: **D (**コメントを発表する**)**

質問: **66**
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. セッションの二重認証を有効にします。
B. パスワードハッシュを使用します。
C. TACACS+認　証を使用します。
D. 帯域外認証を有効にします。
E. 暗号化に SSL を使用します。
正解: **(**正解を表示します**)**

質問: **67**
展示資料を参照してください。

PythonのNETCONFスクリプトを実行した結果はどうなりますか？

A. IPアドレスを持つデバイス上でshow running interface GigabitEthernet 1のXML出力を表示します。

192.168.1.10

B. GigabitEthernet 1 インターフェースに IP アドレス 192.168.1.10 を設定し、新しい XML 設定を出力します。

C. ルーター上でインターフェース設定モードを開き、ユーザーにさらなるXMLコマンドの入力を求めます。

D. IPアドレス192.168.1.0のデバイス上でshow runningのXML出力を表示します。

正解: **(**正解を表示します**)**

The script uses a NETCONF filter that targets the native Cisco IOS XE model and specifically filters the running configuration under interface - > GigabitEthernet - > name 1. The command shown in the script is m.get_config(' running ' , interface_filter), followed by print(result). get_config is a read operation; it retrieves configuration data from the selected datastore, in this case the running datastore.

It does not modify the device. Therefore, the result is printed XML output corresponding to the running configuration of GigabitEthernet 1 on the connected device. Option B is wrong because the script does not call edit_config, does not submit a configuration payload, and does not configure an IP address. Option C is wrong because NETCONF does not open an interactive CLI configuration mode.

Option D is too broad and uses the wrong IP/network wording; the filter narrows the request to GigabitEthernet 1 rather than retrieving the full running configuration. This is a model-driven programmability question. References/topics: ENCOR Automation, NETCONF, YANG, ncclient, get_config, XML filters, Cisco IOS XE native model.

質問**: 68**

タイプ 1 ハイパーバイザー上の仮想マシンの IP および MAC 割り当て要件を説明している記述はどれですか。

A. 各仮想マシンは固有のIPアドレスを必要としますが、MACアドレスは物理サーバーと共有します。

B. 各仮想マシンには一意の MAC アドレスが必要ですが、IP アドレスは物理サーバーと共有されます。

C. 各仮想マシンが他のノードに到達できるようにするには、一意の IP アドレスと MAC アドレスが必要です。

D. 各仮想マシンには一意の IP アドレスが必要ですが、MAC アドレスは物理サーバーのアドレスと共有されます。

正解: **(**正解を表示します**)**

質問: **69**
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. CNAMEレコード
B. SOAレコード
C. NSレコード
D. レコード
正解: **(**正解を表示します**)**

質問: **70**
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. TLS/DTLS
B. SSH
C. IPsec
D. IPS
正解: **C (**コメントを発表する**)**

質問: **71**

Guidelines Topology Tasks

The Operations team started configuring several monitoring activities. Complete the configurations for the tasks below.

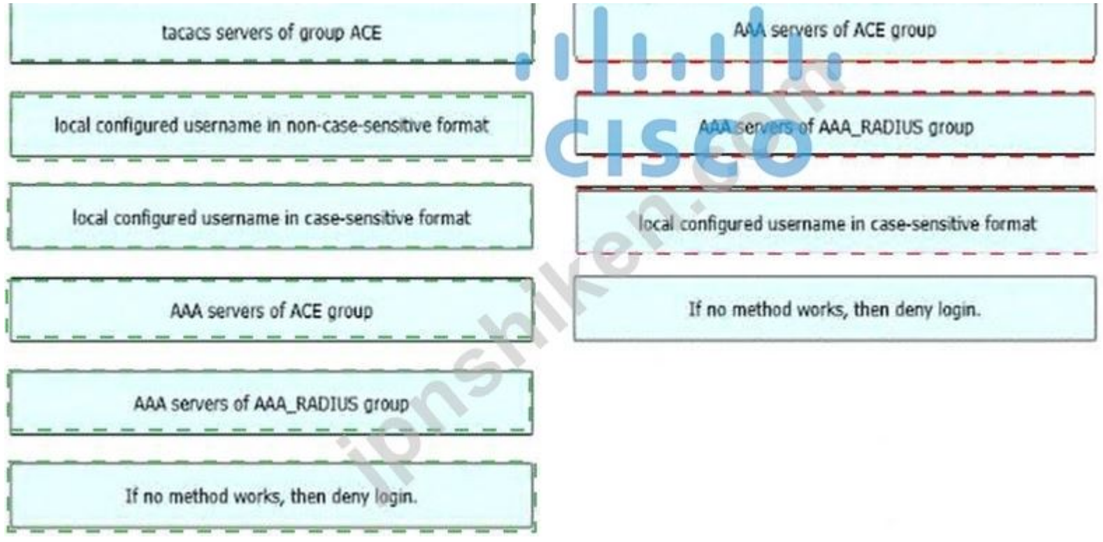
1. Complete the Flexible NetFlow Flow Exporter configuration on R1 to send data to the collector located at 10.10.1.10.
2. Configure the switch port analyzer on Sw1 and mirror all communication to and from PC1 and PC2 to interface E1/0 using session number 2.
3. Configure a basic IP SLA HTTP GET operation on R1 to monitor the server at 10.10.1.100 every 600 seconds.

正解:
See the solution below in Explanation:
Explanation:
Solution:
R1
config t
flow record NetFlow-Record
match ipv4 source address
match ipv4 destination address
collect country bytes
flow exporter NetFlow-Exporter
destination 10.10.1.10
transport udp 9996
flow monitor NetFlow-Monitor
record NetFlow-Record
exporter NetFlow-Exporter

exit
int et0/0
ip flow monitor NetFlow-Monitor input
ip sla 1
http
get http://10.10.1.100
frequency 600
exit
ip sla schedule 1 start-time now
wr
Sw1
config t
monitor session 2 source int e0/0
monitor session 2 source int et0/2
monitor session 2 destination interface e1/0
wr

質問: 72
ドラッグ＆ドロップ。エンジニアが以下の構成を作成します。左側の認証方法を右側の優先順位の高い順にドラッグ＆ドロップしてください。すべてのオプションが使用されるわけではありません。
R1#show run | include aaa
AAA新モデル
aaa認証ログインデフォルトグループACEグループAAA_RADIUSローカルケース
aaa セッション ID 共通

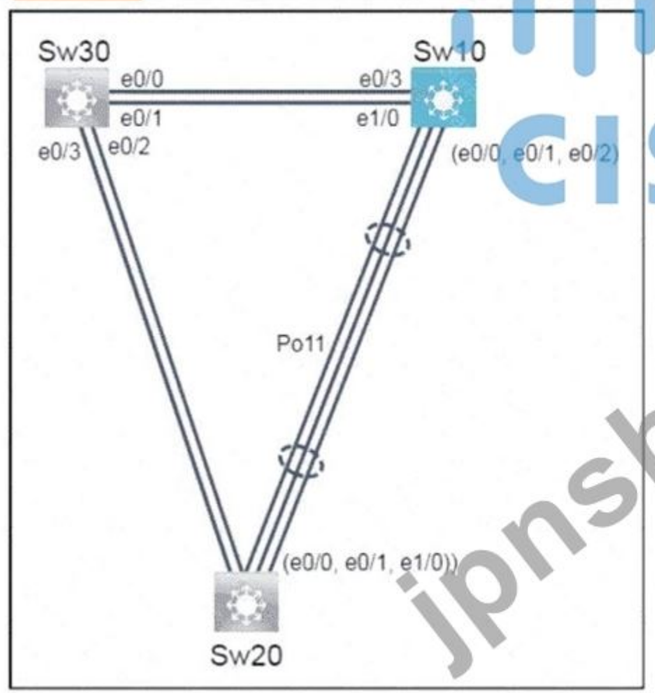
正解:



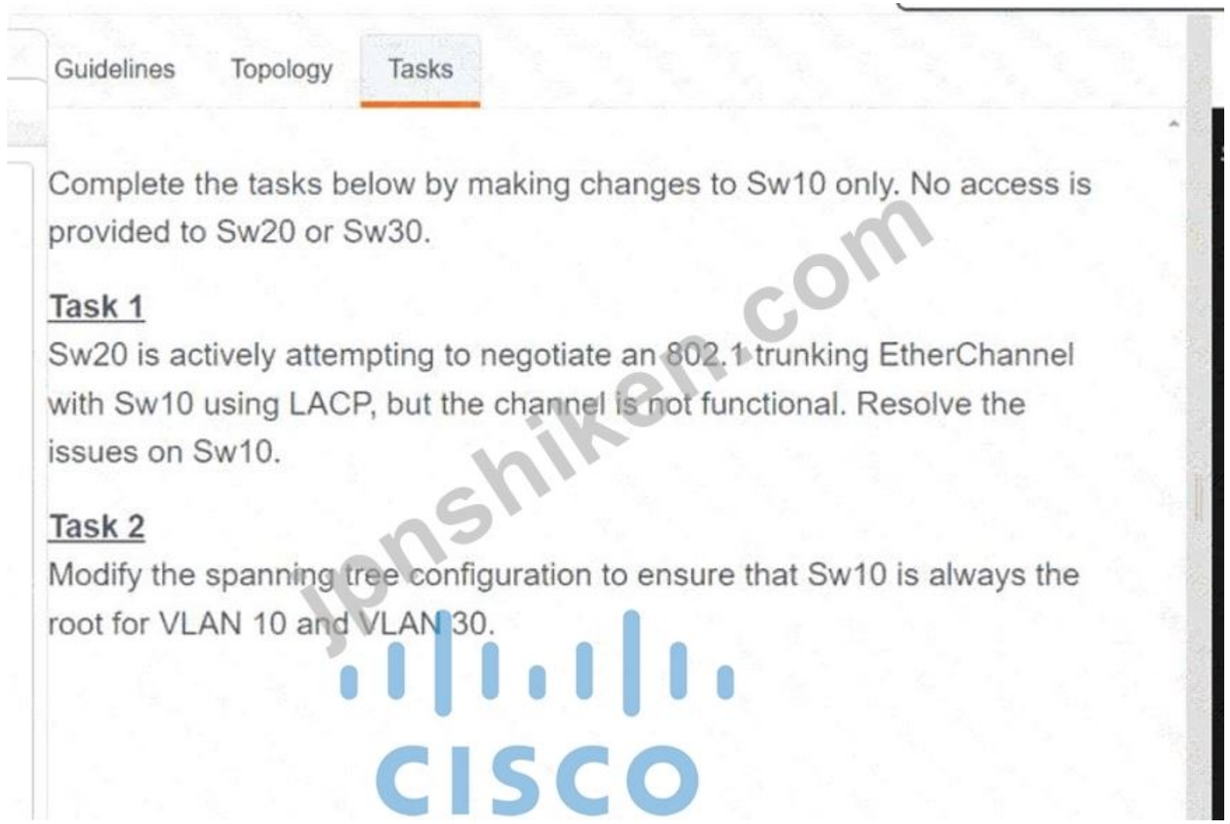
Explanation:
Priority 1: D
Priority 2: E
Priority 3: C
Priority 4: F
Cisco AAA method lists are processed from left to right. The command aaa authentication login default group ACE group AAA_RADIUS local-case defines the default login authentication sequence. The first method is the named AAA server group ACE, so the first priority is the AAA servers of the ACE group. If those servers do not respond or cannot authenticate the user, IOS tries the next method, which is the named AAA server group AAA_RADIUS. If that also fails, the router uses local-case, which checks the local username database with case-sensitive username matching. This is different from the normal local method, which does not enforce case-sensitive username comparison in the same way. If none of the configured methods succeeds, authentication fails and login is denied. The TACACS- specific option is not selected because the shown command uses a named AAA server group, not the literal group tacacs+ keyword. The non-case-sensitive local method is also not selected because the command explicitly uses local-case. References/topics: ENCOR Infrastructure Security, AAA method lists, login authentication, named server groups, local-case fallback behavior.

質問: 73

es Topology Tasks



Sw10



正解:
See the solution below in Explanation:
Explanation:
Solution:-
Default int range et0/0-1
Int range e0/0 - 1
Sw trunk encap dot1
Switch mode trunk
Channel-group 2 mode passive
No shut
Spanning-tree vlan 10 priority 0
Spanning-tree vlan 30 priority 0

質問: 74
Cisco 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. ピン

B. 指定されたIPアドレスの範囲
C. NETCONF
D. CDP
E. SNMP
F. LLDP
正解: **B,D,F** (コメントを発表する)

質問: **75**

正解:

See the solution below in Explanation:

Explanation:

Solution:

R30

show ip access-list

config t

ip access-list extended 120

5 permit eigrp any any

wr

R20

config t

ip access-list extended 100

permit tcp 192.168.25.0 0.0.0.255 any eq 23

class-map match-any TELNET

match access-group 100

policy-map CoPP

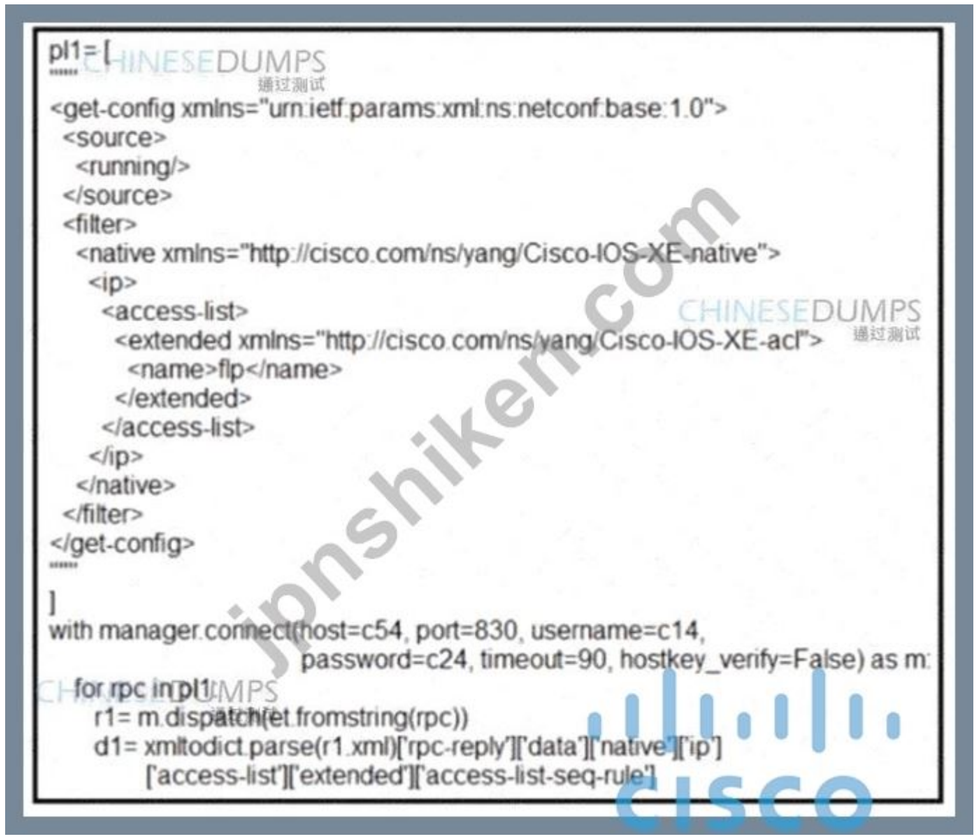
class TELNET

police 10000 conform-action transmit exceed-action drop

control-plane

service-policy input CoPP
wr

質問: 76



展示を参照してください。このPythonスクリプトによって何が達成されるのでしょうか？

A. アクセスリストのステートメントを辞書リストに読み込みます

B. アクセス リスト ステートメントを端末画面に表示します。

C. アクセスリストステートメントを設定します

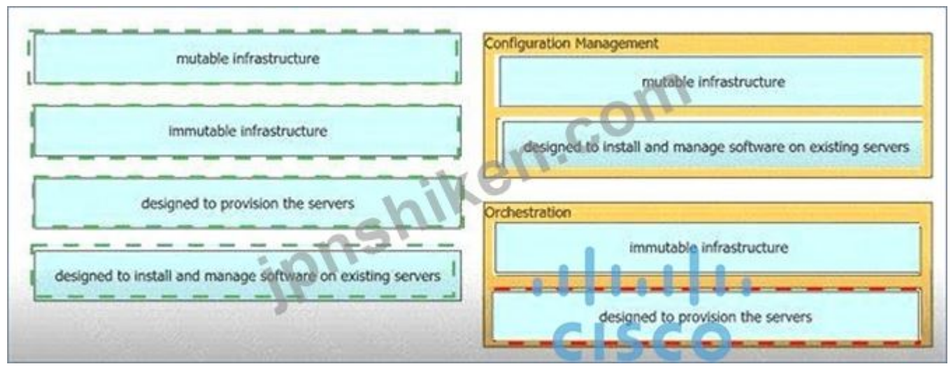
D. アクセス リスト ステートメントを人間が読める形式に変換します。

正解: **(**正解を表示します**)**

質問: 77
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: 78
左側の特性を右側のオーケストレーション ツールの分類にドラッグ アンド ドロップします。


正解:

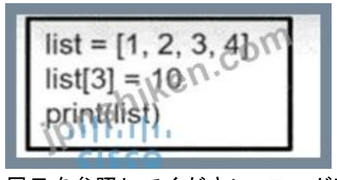


Explanation:

質問: **79**
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.freeze(target-running')
B. m.freeze(config-running')
C. m.lock(target-running')
D. m.lock(config='running')
正解: **(**正解を表示します**)**

質問: **80**
Cisco Catalyst Center (旧 DNA Center) テンプレート エディタ機能の特徴は何ですか?
A. すべてのネットワーク デバイスの健全性に関する概要を提供します。
B. パラメータ化された要素または変数を通じて事前定義された構成を使用します。
C. ネットワーク デバイスの脆弱性評価を容易にします。
D. ネットワーク デバイスのソフトウェア アップグレードを中央から容易に実行できます。
正解: **B (**コメントを発表する**)**

質問: **81**



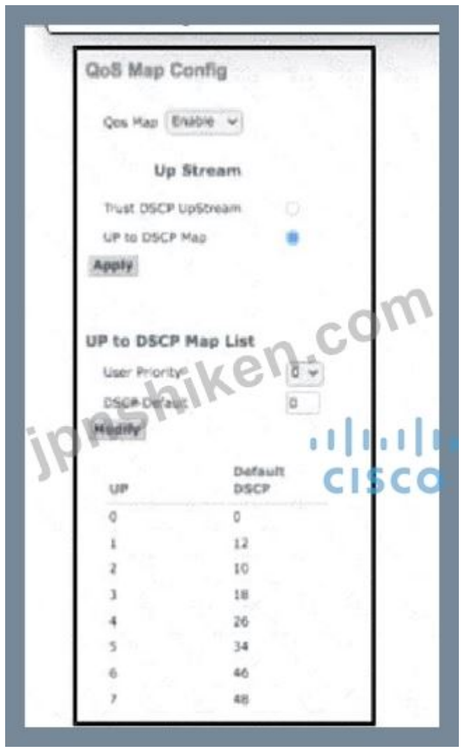
展示を参照してください。コード実行後の変数リストの値は何ですか？
A. [1, 2, 10, 4]
B. [1, 2, 10]
C. [1, 2, 3, 10]
D. [1, 10, 10, 10]
正解: **(**正解を表示します**)**

質問: **82**
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. インターフェースグループ
D. AAAオーバーライド
正解: **(**正解を表示します**)**

質問: **83**
Wi-Fi チャンネルの特徴は何ですか?
A. 同じ Wi-Fi チャネルに接続するデバイスは、同じ衝突ドメインに存在します。
B. 2つの4GHz帯balWMS§24の重複しないチャネル
C. Wi-Fi チャネルの間隔は 30 MHz です。
D. 5GHz帯はWi-Fiクライアントに11の異なるチャネルを提供します
正解: **A (**コメントを発表する**)**

質問: **84**
データモデリング言語の目的は何ですか?
A. ネットワーク内のデータフローパターンを記述するためのフレームワークを提供する
B. 任意のデータエンコード形式に変換可能なデータスキーマを記述する
C. 異なるCPUアーキテクチャ間の相互運用性のためにエンコードされたデータを変換する
D. バイナリエンコードされたプロトコルデータユニットをデコードするために必要なアルゴリズムを指定する
正解: **(**正解を表示します**)**

質問: **85**



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: **(**正解を表示します**)**

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: 86
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: **87**
VRRPの特徴は何ですか？
A. 冗長性を実現するために仮想IPアドレスと仮想MACアドレスを使用します
B. Cisco 独自のプロトコルです。
C. 本質的に、利用可能なゲートウェイ間で負荷を分散します。
D. アップストリームとダウンストリームの対称的なトラフィック フローを保証します。
正解: **(**正解を表示します**)**

質問: **88**
展示品を参照してください。

このデータからどの JSON 構文が派生されますか?

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

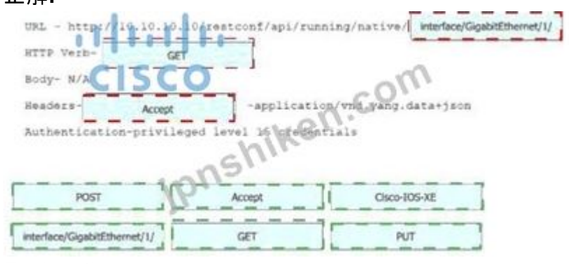
質問: **89**
高密度 AP 環境では、RF セル サイズを縮小し、特定のしきい値を超える無線パケットを復調しないようにするためにどの機能を使用できますか?
A. RRM

B. 80211k
C. RX-SOP
D. フランス
正解: (正解を表示します)

質問: **90**

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: **91**
Cisco SD-Access ネットワークの特徴は何ですか?
A. スケーラブル グループ タグは、マクロ セグメント アトロンに使用されます。
B. デバイスは、VLAN メンバーシップに基づいて仮想ネットワークに割り当てられます。
C. 仮想ネットワークはマイクロセグメンテーションに使用されます。
D. ファブリック内のすべてのトラフィックはレイヤー 3 です。
正解: **A** (コメントを発表する)

質問: **92**
下部にあるコードスニペットをPythonスクリプトの空白部分にドラッグアンドドロップして、プログラムがIPアドレスを変更し、それを新しいJSONファイルとしてディスクに保存するようにします。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:

```
import json

with open("json ios xe.json", "r") as json file:
    json_file_content = json_file.read()

decoded_json = json.loads(json_file_content)

decoded json['Cisco-IOS-XE-native:interface']['GigabitEthernet'][0]['ip']
            ['address']['primary']['address'] = \ "192.168.1.2"

encoded_json_compact = json.dumps(decoded_json)
encoded json indented = json.dumps(decoded json, indent = 4)

with open("jso                    compact.json", "w") as json file:
    json_file.write(encoded_json_compact)

with open("json ios xe indented.json", "w") as json file:
    json file.write(encoded json indented)
```


質問: 93

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?

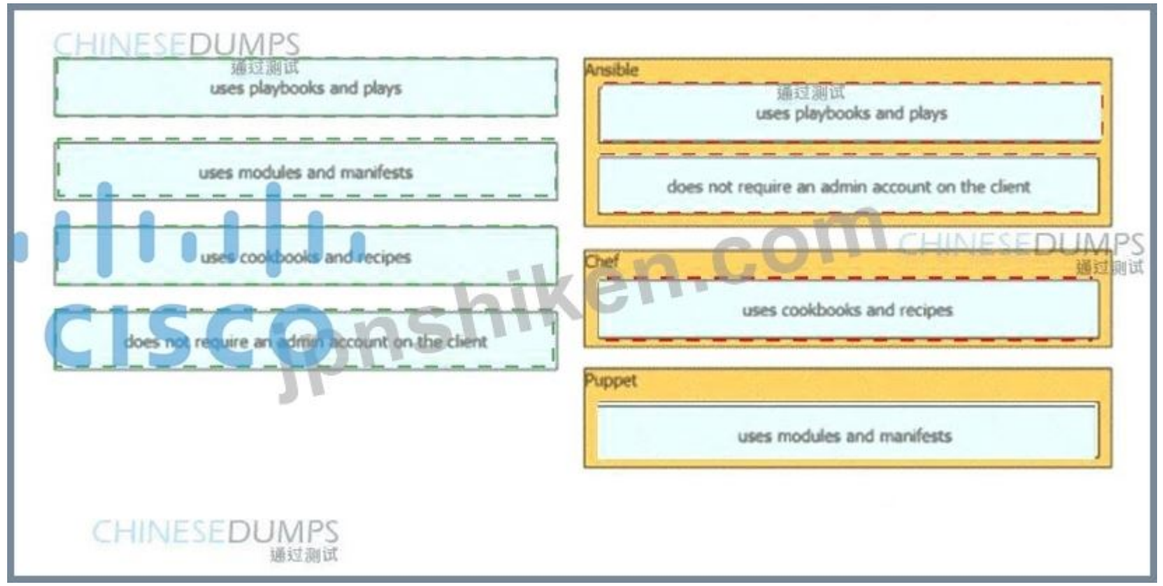
A. IP ヘルパー アドレス
B. プライマリ/セカンダリ - ターシャリ/バックアップ
C. DNS
D. 保存されたWLC情報

正解: **(**正解を表示します**)**

質問: 94

自動化特性を左側から右側の対応するツールにドラッグ アンド ドロップします。

正解:



Explanation:

質問: **95**
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 40 MHz に減らします。
B. 必須の最小データ レートを下げます。
C. 無線チャネル幅を 160 MHz に増やします。

D. 必須の最小データ レートを増やします。
正解: **D** (コメントを発表する)

質問: **96**
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. SSH
B. 802.1X
C. TLS
D. IPsec
正解: **C** (コメントを発表する)

質問: **97**
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: **98**

この WLAN セキュリティ設定の構成に基づいて、クライアントがネットワークへの認証に使用できる方法はどれですか?

A. テキスト文字列

B. ユーザー名とパスワード

C. RADIUSトークン

D. 証明書

正解: **(**正解を表示します**)**

質問: **99**

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. device_ip.items() 内のデバイスの場合: print(device)

C. デバイスの場合、deviceip: 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: **100**

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: 101
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. マップリゾルバ
B. マップサーバー
C. 出力トンネルルータ
D. 入力トンネルルータ
正解: **C** (コメントを発表する)

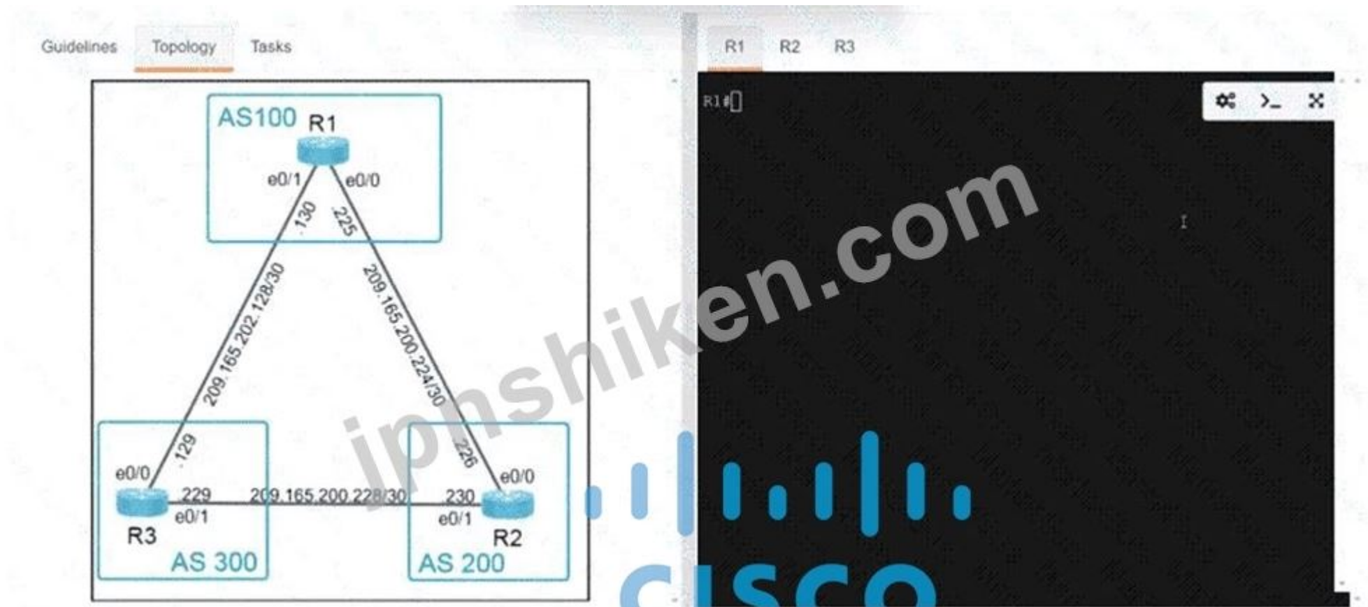
質問: 102
Cisco SD-Accessソリューションに当てはまる特性はどれですか？
A. 動的ルーティングは、境界スイッチとエッジスイッチを検出およびプロビジョニングするために使用されます。
B. コントロールプレーンはVXLANに基づいています。
C. データプレーンはVXLANに基づいています。
D. GRE がポリシープレーンとして使用されます。
正解: **C** (コメントを発表する)
The correct answer is C. The data plane is based on VXLAN.
In Cisco SD-Access, the fabric uses:
* 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: **103**
ネットワーク設計マットが小さく繰り返し可能なセクションを使用することで得られる 2 つの利点は何ですか? (2 つ選択してください。)
A. 迅速な障害分離
B. 低レイテンシー
C. スループットの向上
D. スケーラビリティ
E. 監視要件の低減
正解: **(**正解を表示します**)**

質問: **104**
クライアントが複数のモビリティ グループ間をローミングする場合、どのタイプのローミング イベントが発生しますか?
A. レイヤー1
B. レイヤー3
C. レイヤー 7
D. レイヤー2
正解: **(**正解を表示します**)**

質問: **105**



Guidelines Topology Tasks

Configure R1 according to the topology to achieve these results:

1. Configure eBGP using Loopback 0 for the router-id. Do not use the address-family command to accomplish this.
2. Advertise R1's Loopback 100 and Loopback 200 networks to AS200 and AS300.

正解:

See the solution below in Explanation:
Explanation:
Solution:
Solution on R1:

```
R1#sh run  | s bgp
router bgp 100
 bgp router-id 10.1.1.1
 bgp log-neighbor-changes
 network 209.165.201.1 mask 255.255.255.255
 network 209.165.201.2 mask 255.255.255.255
 neighbor 209.165.200.226 remote-as 200
 neighbor 209.165.202.129 remote-as 300
```

R1# copy run start
Verification:

```
R1#sh ip bgp su
BGP router identifier 10.1.1.1, local AS number 100
BGP table version is 3, main routing table version 3
2 network entries using 288 bytes of memory
2 path entries using 168 bytes of memory
1/1 BGP path/bestpath attribute entries using 160 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 616 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
209.165.200.226 4   200       8       6        3    0    0
00:00:51        0
209.165.202.129 4   300       6       6        3    0    0
00:01:23        0
R1#
```

OR

質問: **106**
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. 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。
C. クライアント認証は常に A P で実行されます。
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: **(**正解を表示します**)**

質問: **107**
Cisco EDR は脅威の検出と対応による保護を提供するためにどの機能を使用しますか?
A. 封じ込め、脅威インテリジェンス、機械学習
B. コンテナベースのエージェント
C. クラウドアナリストとエンドポイントファイアウォール制御
D. ファイアウォールと侵入防止
正解: **(**正解を表示します**)**

質問: **108**
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: **109**
PIMネットワークにおいて、Auto-RPはどのような役割を果たしますか？
A. スパースモードおよびデンスモードのPIMネットワーク間でIGMPトラフィックを分散します。

B. グループとRPのマッピングの配布を自動化します
C. リーフルーターの設定を自動化します
D. 待ち合わせ場所の選択を実行する
正解: **(**正解を表示します**)**
Auto-RP is used in Protocol Independent Multicast sparse-mode environments to distribute rendezvous point information automatically. In PIM sparse mode, multicast routers must know which RP is responsible for specific multicast group ranges. Without a dynamic RP-discovery mechanism, administrators would have to configure RP information manually across routers. Auto-RP solves that by allowing candidate RPs to announce themselves and mapping agents to advertise group-to-RP mappings throughout the multicast domain. Therefore, option B is correct. Option A is incorrect because Auto-RP does not distribute IGMP traffic; IGMP operates between hosts and local multicast routers to manage group membership. Option C is wrong because Auto-RP does not automate leaf- router configuration generally; it specifically distributes RP mapping information. Option D is also inaccurate because Auto-RP does not perform an election in the same way as BSR. It advertises candidate RP and mapping-agent information so routers can learn RP mappings. The key ENCOR concept is multicast control-plane discovery for PIM sparse-mode RP selection. References/topics: ENCOR multicast, PIM sparse mode, Auto-RP, rendezvous point discovery, multicast group-to-RP mapping.

質問: **110**
ワイヤレス管理者は、ISE を外部 RADIUS サーバとして使用する新しい Web 認証企業 SSID を作成する必要があります。認証が完了したら、ゲスト VLAN を指定する必要があります。
ISE サーバーがゲスト VLAN を指定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. ネットワーク アクセス制御状態を有効にします。
B. RADIUS プロファイリングを設定します。
C. AAA オーバーライドを有効にします。
D. AAA ポリシー名を設定します。
正解: **(**正解を表示します**)**

質問: **111**

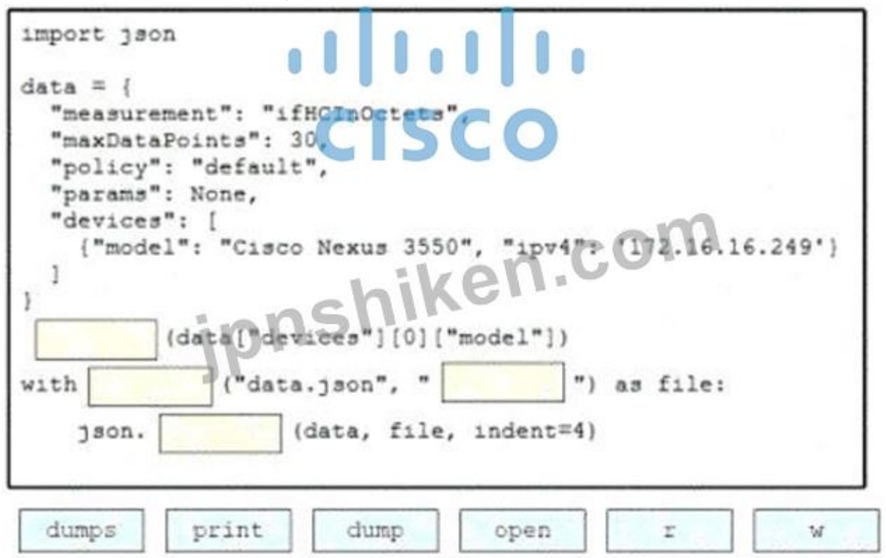
R1	R2
key chain cisco123 key 1 key-string Cisco123!	key chain cisco123 key 1 key-string cisco123!
Ethernet0/0 - Group 10 State is Active 8 state changes, last state change 00:02:49 Virtual IP address is 192.168.0.1 Active virtual MAC address is 0000.0c07.ac0a	Ethernet0/0 - Group 10 State is Active 17 state changes, last state change 00:02:17 Virtual IP address is 192.168.0.1 Active virtual MAC address is 0000.0c07.ac0a

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. HSRPv2
C. VRRP
D. GLBP
正解: **A (**コメントを発表する**)**

質問: **112**
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> ¢reate）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. POST

C. CREATE
D. PUT
正解: **(**正解を表示します**)**

質問: **113**
下部のコードスニペットをPythonスクリプトの空白部分にドラッグアンドドロップすると、デバイスモデルが画面に表示され、JSONデータがファイルに書き込まれます。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: **114**
アーキテクトが OSPF 仮想リンクを使用するのはなぜでしょうか?
A. 非バックボーンエリアを別の非バックボーンエリアを介してエリア0に接続する
B. 重複するプライベートIPアドレス空間を持つ2つのネットワークを接続する
C. 非バックボーンを介して2つの既存のエリア0をマージする
D. スタブエリアが別のスタブエリアを通過できるようにする
正解: **A** (コメントを発表する)

質問: **115**

Comment

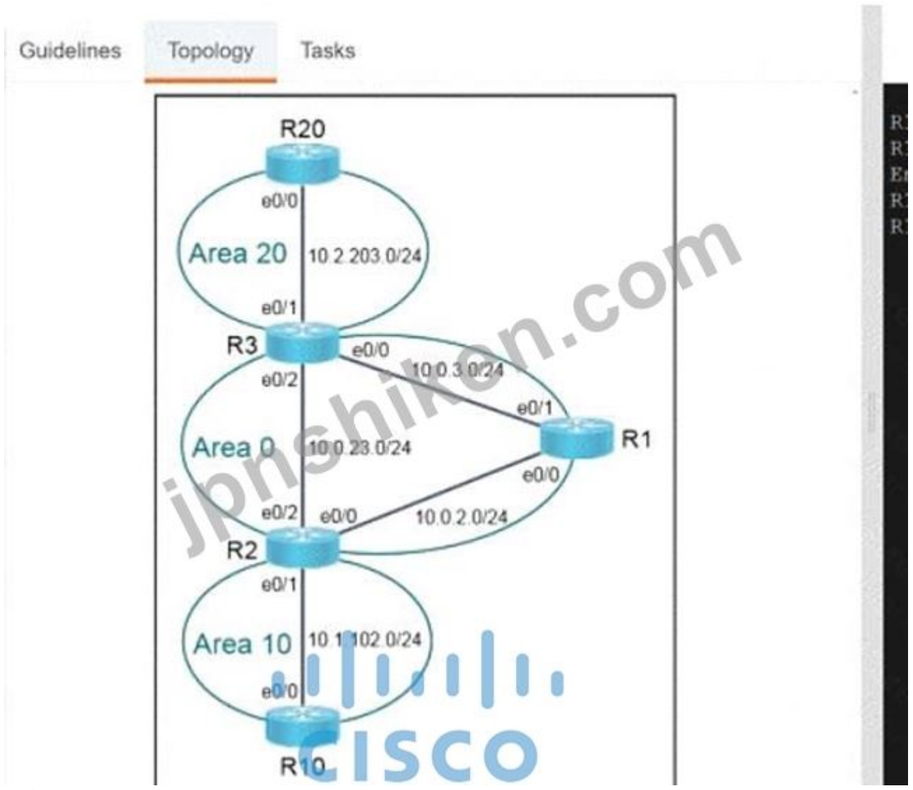
Guidelines | Topology | Tasks

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

1. Configure R3 to always be the DR in Area 20. Do not change the router ID.
2. Configure R2 and R10 so they do not participate in a DR/BDR election process in Area 10.

R2 | R3 | R1 | R10 | R20

```
R10>en
R10#conf t
Enter configuration commands, one per line.  End with CNTL/Z
R10(config)#interface g0/0
R10(config-if)#ip ospf priority
```



正解:

See the solution below in Explanation:

Explanation:

Solution:

R3

Int e0/1

Ip ospf priority 255

End

Copy run start

R2

Int e0/1

Ip ospf network point-to-point

End

Copy run start

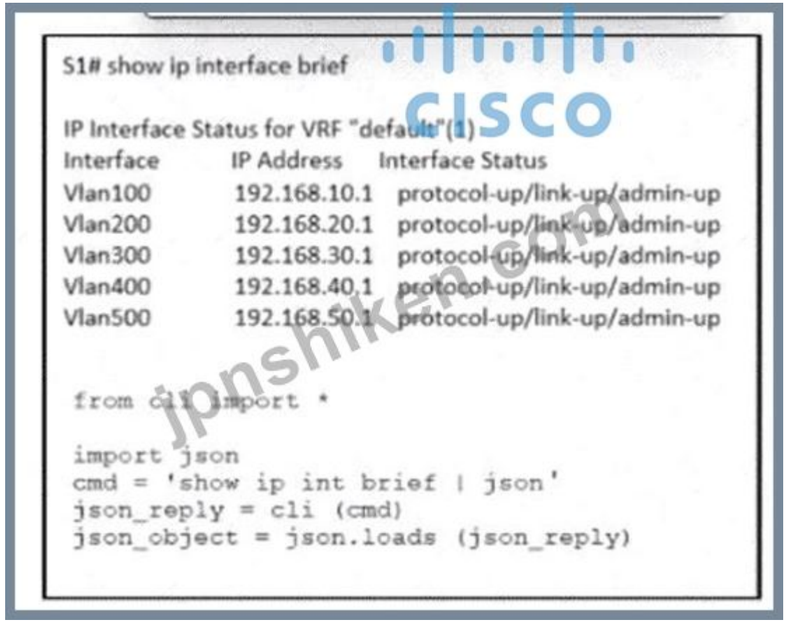
R10

Int e0/0

lp ospf network point-to-point
End
Copy run start

質問: **116**
無線 RF SNR を測定するために使用される測定単位は何ですか?
A. mw
B. dBi
C. dbm
D. db
正解: (正解を表示します)

質問: **117**



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: 118
展示資料を参照してください。

```
router#sh run | b line con
line con 0
 password cisco
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
!
end

router#sh run | i username|aaa
no aaa new-model
username user password 0 user
router#
```

どの設定で、コンソール回線上でパスワードのみを使用してパスワードチェックが有効になりますか？

A. router(config)# line con 0
router(config-line)# exec-timeout 0 0

B. router(config)# line con 0
router(config-line)# login

C. router(config)# line con 0
router(config-line)# login local

D. router(config)# line vty 0 4
router(config-line)# login

正解: **(**正解を表示します**)**

The correct command is login under line con 0. In classic Cisco IOS line authentication, setting a line password alone is not enough; the login command tells IOS to prompt for and validate the configured line password. The exhibit shows console line configuration with a password configured, and AAA is not enabled. Therefore, line con 0 followed by login enables console password checking using only the line password. Option A only disables console session timeout by setting the exec timeout to zero; it does not enable authentication. Option C, login local, tells IOS to authenticate against the local username database, which requires a username and password, not only the line password. Option D applies the setting to VTY lines, which control remote Telnet/SSH access, not the physical console line. This is a fundamental device-hardening and management-plane access-control concept. For ENCOR, candidates must distinguish line passwords, local username authentication, AAA authentication, console lines, and VTY lines. References/topics: ENCOR Infrastructure Security, console access, line password, login, login local, local authentication, device administration.

質問**: 119**

レイヤー 2 のコントローラ間ローミング中に何が起こりますか?

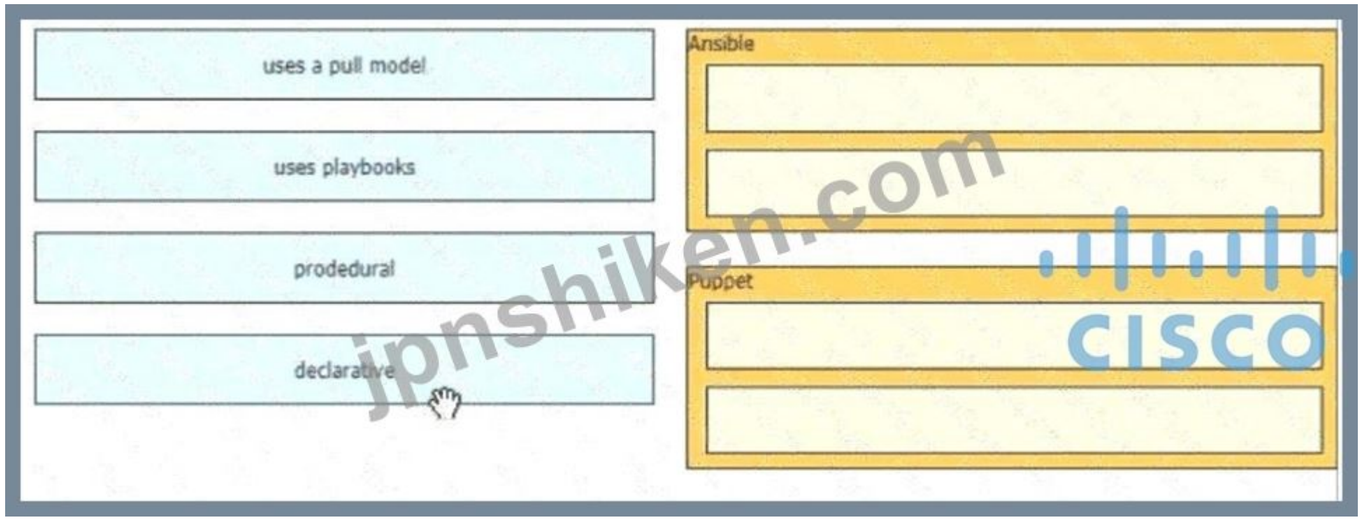
A. クライアントが関連付けられている各コントローラに新しいセキュリティ コンテキストが適用されますが、IP アドレスは同じままです。

B. クライアントは同じ IP アドレスとセキュリティ コンテキストを保持します。
C. クライアントは、接続される各新しいコントローラーのデータベースで外部としてマークされます。
D. クライアントは、新しい IP アドレスとセキュリティ コンテキストが適用される新しいコントローラに関連付ける必要があります。
正解: **(**正解を表示します**)**

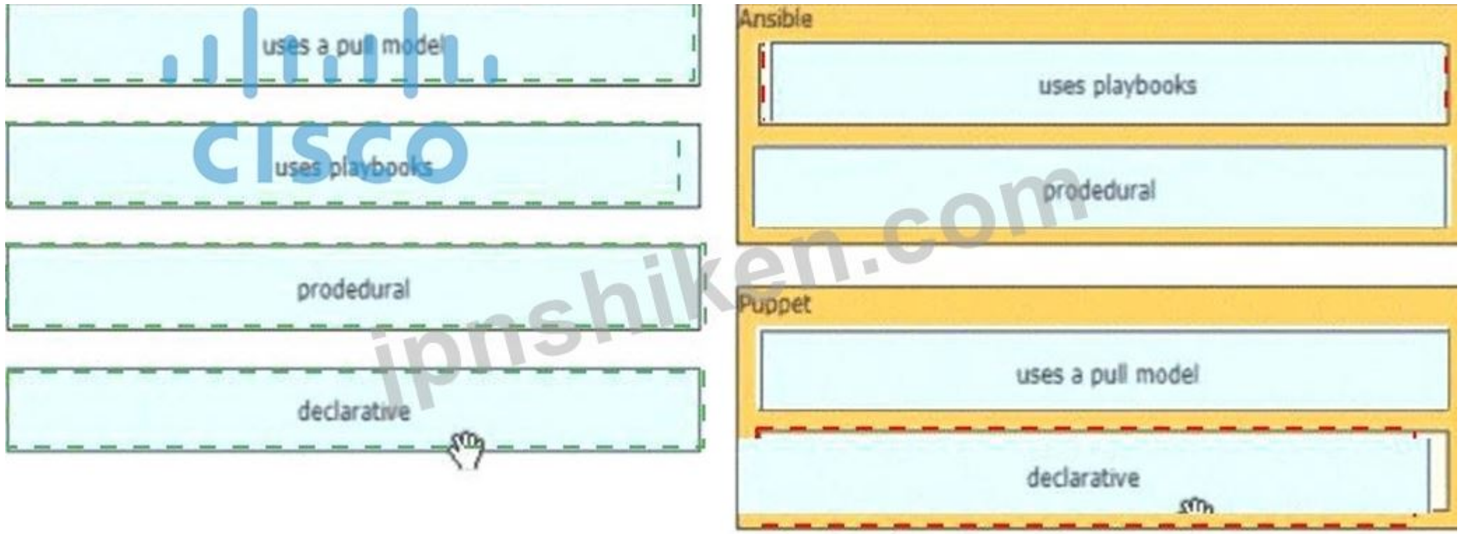
質問: **120**
Cisco Catalyst Center (旧 DNA Center) のインテント API とは何ですか?
A. ITSM、IPAM、レポート情報などのデータの交換を可能にする西向きのインターフェース
B. コントローラとネットワークデバイス間のインターフェース。ネットワーク検出と構成管理を可能にします。
C. サウスバウンドの消費者向けRESTful API。ネットワーク検出と構成管理を可能にします。
D. ネットワーク検出と構成管理を可能にする北向きの消費者向けRESTful API
正解: **(**正解を表示します**)**

質問: **121**
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. フレックスコネクト
B. スニファー
C. 不正検出機能
D. モニター
E. ローカル
正解: **(**正解を表示します**)**

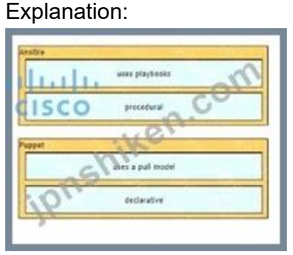
質問: **122**
左側の特性を、右側で説明されているオーケストレーション ツールにドラッグ アンド ドロップします。



正解:



Explanation:



質問: **123**
YANG モジュールの利点は何ですか?
A. 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
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. 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
D. 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
正解: **(**正解を表示します**)**

質問: **124**
どのソリューションが、2つのサイト間でエンドツーエンドの回線速度暗号化をサポートしていますか？
A. TrustSec
B. IPsec
C. GRE
D. MACsec
正解: **B (**コメントを発表する**)**

質問: **125**
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. TLS
B. HTTPS
C. NETCONF
D. RESTCONF
E. SSH
正解: **(**正解を表示します**)**

質問: **126**
全方向性アンテナの特徴は何ですか？
A. 最も集中した狭いビーム幅を提供します。
B. ゲインが高いです。
C. ダイポールアンテナが含まれます。
D. 皿アンテナが含まれます。
正解: **(**正解を表示します**)**

質問: **127**
サードパーティ認証に使用されるフレームワークはどれですか?
A. カスタムトークン
B. OAuth
C. ソープ
D. API キー

正解: **(**正解を表示します**)**

質問: **128**
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 エンタープライズ
B. WPA3 エンタープライズ
C. WPA3 パーソナル
D. WPA2 パーソナル
正解: **(**正解を表示します**)**

質問: **129**
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. データセンターの南北トラフィックのファイアウォール保護
B. DDoS 保護
C. 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
D. リモート アクセス用の仮想プライベート ネットワーク
正解: **(**正解を表示します**)**

質問: **130**
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. 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
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. VXLANトンネルエンドポイント識別子
正解: **B (**コメントを発表する**)**

質問: **131**
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. ブロードキャスト検出リクエスト
B. 各WLCへのユニキャスト検出要求
C. すべてのWLCへの参加リクエスト
D. 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
正解: **(**正解を表示します**)**

質問: **132**
クライアントの認証が必要で、暗号化なしでも機能する方法はどれですか?
A. PSK
B. WebAuth
C. open

D. WEP
正解: **(**正解を表示します**)**

質問: **133**
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、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。
B. 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。
C. 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。
D. 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。
正解: **(**正解を表示します**)**

質問: **134**
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. SNR
B. RSSI
C. Noise
D. CCI
正解: **(**正解を表示します**)**

質問: **135**

図を参照してください。サブネット 10.10.10.0/24 の管理者のみがルーターにアクセスできます。ルーターへのリモートアクセスと管理には、平文プロトコルではなく、セキュアなプロトコルを使用する必要があります。この目的を達成する構成はどれですか？
A. アクセスリスト 23 許可 10.10.10.0 0.0.0.255
回線 vty 0 15
アクセスクラス23アウト

輸送入力すべて
B. アクセスリスト 23 許可 10.10.10.0 255.255.255.0
回線 vty 0 15
アクセスクラス23
トランスポート入力ssh
C. アクセスリスト 23 許可 10.10.10.0 0.0.0.255
回線 vty 0 4
アクセスクラス23
トランスポート入力ssh
D. アクセスリスト 23 許可 10.10.10.0 0.0.0.255
回線 vty 0 15
アクセスクラス23
トランスポート入力ssh
正解: (正解を表示します)
The correct answer is D.
To meet the requirement, the configuration must do two things:
* Permit only the 10.10.10.0/24 subnet to access the VTY lines
* Allow only a secure remote access protocol, which is SSH
The correct Cisco IOS configuration is:
access-list 23 permit 10.10.10.0 0.0.0.255
line vty 0 15
access-class 23 in
transport input ssh
* access-list 23 permit 10.10.10.0 0.0.0.255 This correctly matches the subnet 10.10.10.0/24 using the proper wildcard mask 0.0.0.255.
* line vty 0 15 This applies the restriction to all VTY lines, not only a subset.
* access-class 23 in This filters incoming remote access connections to the router.
* transport input ssh This allows only SSH, which is encrypted and secure, and prevents Telnet or other clear-text remote access protocols.
* A is incorrect because:
* access-class 23 out filters outbound connections from the VTY lines, not inbound management access.
* transport input all allows insecure protocols such as Telnet.
* B is incorrect because:
* 255.255.255.0 is a subnet mask, not a wildcard mask, so the ACL syntax is wrong for a standard ACL entry.
* C is incorrect because:
* It applies only to VTY 0 4, while the router also has VTY 5 15 configured.
* This leaves other VTY lines unrestricted, which does not fully meet the requirement.
For secure remote management on Cisco devices:
* Use transport input ssh to disable Telnet
* Use access-class < ACL > in on VTY lines to restrict who can connect
* Use the correct wildcard mask for the subnet
For 10.10.10.0/24, the wildcard mask is:
0.0.0.255

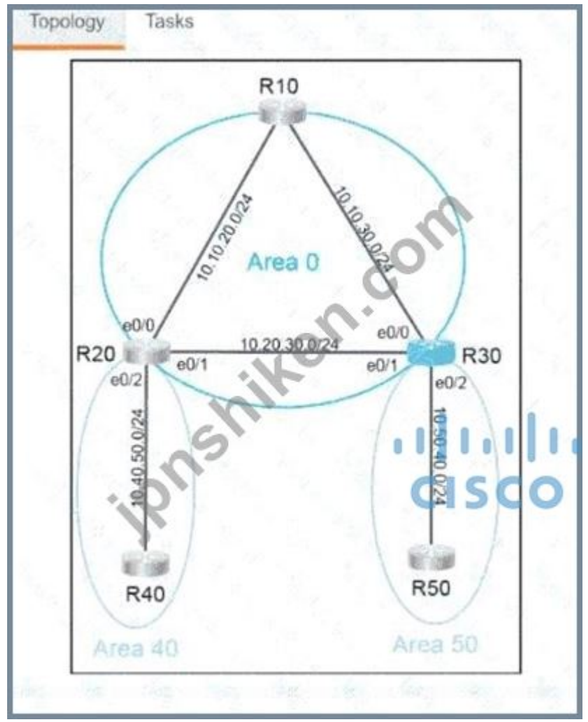
So the complete secure solution is:
restrict inbound VTY access + allow only SSH + apply to all VTY lines

質問: **136**
認証に 802.1x を実行しているクライアントは何と呼ばれますか?
A. NAC device
B. supplicant
C. policy enforcement point
D. authenticate
正解: **B** (コメントを発表する)

質問: **137**
主要な REST セキュリティ設計原則は何ですか?
A. リクエストにタイムスタンプを追加する
B. OAuth
C. パスワードハッシュ
D. フェイルセーフのデフォルト
正解: (正解を表示します)

質問: **138**
IP ベースのアクセス制御ポリシーを展開するときに、Cisco DNA Center はどのデバイスを設定しますか?
A. 選択された個々のデバイス
B. 選択したサイト内のすべてのデバイス
C. すべての有線デバイス
D. ISEと統合するすべてのデバイス
正解: (正解を表示します)

質問: **139**



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.

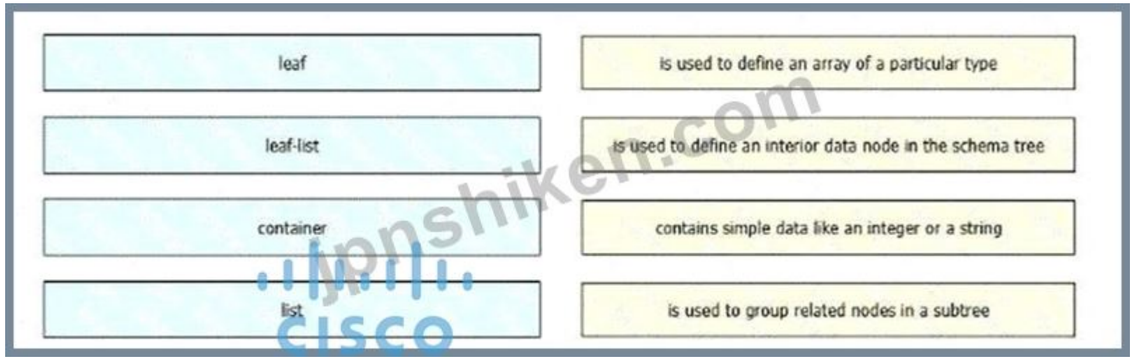
Task 2:

Configure a /18 summary route for Area 50.

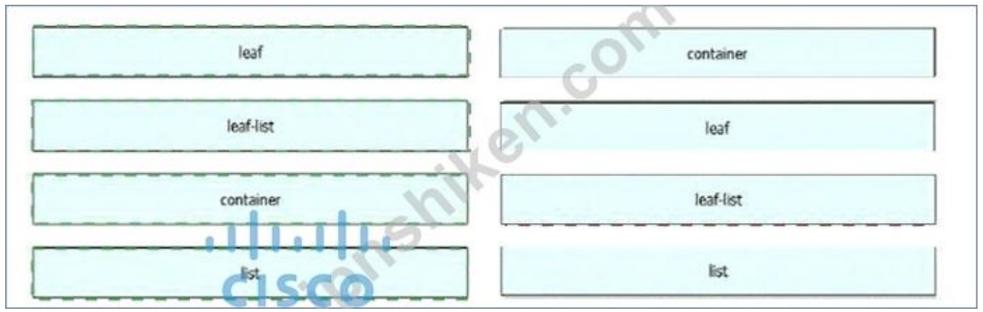
正解:
See the solution below in Explanation:
Explanation:
Solution:
R30
Config t
router ospf 100
router-id 10.0.1.30
int ran lo0 , e0/0-1
ip ospf 100 a 0
exit
int et0/2
ip ospf 100 a 50
exit
router ospf 30
area 50 range 10.10.0.0 255.255.192.0
area 50 range 10.50.0.0 255.255.192.0
end
wr

質問: **140**

ドラッグ＆ドロップ。左側のYANGノードを、右側の対応する定義にドラッグ＆ドロップしてください。



正解:



Explanation:

A # 3

B # 1

C # 2

D # 4

YANG models describe configuration and operational state data in a structured tree. A leaf represents a single simple value, such as a string, integer, boolean, or enumeration, so it maps to "contains simple data like an integer or a string." A leaf-list represents a sequence of leaf values of the same type, so it maps to the array-style definition. A container is an interior node in the YANG schema tree. It does not itself hold a scalar value; instead, it contains child nodes and organizes related data. A list represents a set of repeated entries and is used to group related child nodes into list entries, commonly identified by a key. The important distinction is that a leaf has no child nodes, while containers and lists organize structured data below them. In ENCOR automation, YANG is critical because protocols such as NETCONF and RESTCONF use YANG models to define valid configuration and operational data paths. References/topics: ENCOR Automation, YANG data models, NETCONF, RESTCONF, leaf, leaf- list, container, list, model-driven programmability.

質問: **141**

Cisco TrustSecテクノロジーを使用する場合、トラフィックはどのように分類されますか？

A. VLANを使用

B. セキュリティグループタグ付き

C. MACアドレス付き

D. IPアドレス付き

正解: (正解を表示します)
Cisco TrustSec classifies traffic using Security Group Tags, commonly called SGTs. An SGT represents the security group identity assigned to a user, device, or endpoint session. Instead of relying only on VLANs, IP subnets, or ACLs tied to topology, TrustSec allows policy to follow the identity of the endpoint. That makes option B correct. VLAN-based classification is less flexible because VLANs are tied to Layer 2 segmentation and network placement. MAC addresses can identify devices but are not the TrustSec policy classification mechanism. IP addresses are commonly used in traditional ACLs, but TrustSec's purpose is to reduce dependence on IP-based segmentation by using group-based policy.
Once traffic is tagged with an SGT, network devices can enforce Security Group ACLs, also called SGACLs, based on source and destination security groups. This supports scalable segmentation across campus and enterprise networks.
The ENCOR concept is identity-based segmentation and policy abstraction. References/topics: ENCOR Security, Cisco TrustSec, Security Group Tag, SGACL, identity-based access control, scalable group-based segmentation.

質問: **142**
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. GLBP
C. VRRP
D. LCAP
正解: **B** (コメントを発表する)

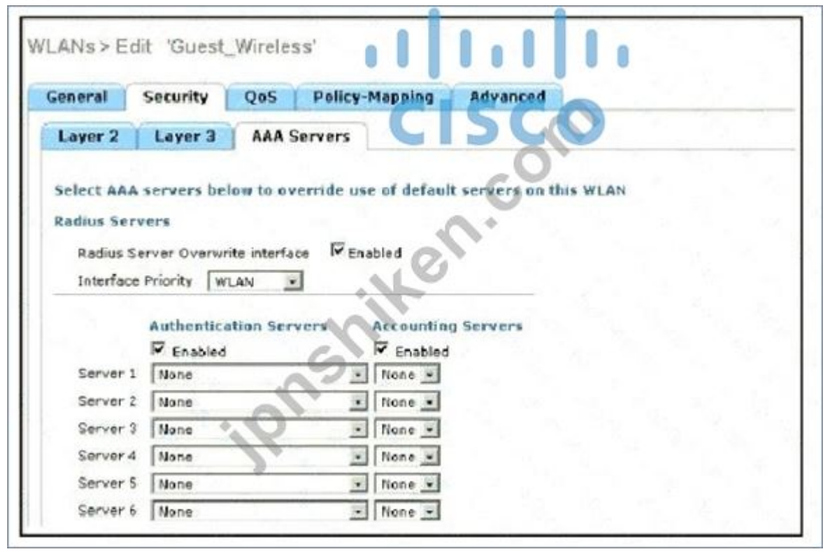
質問: **143**
レイヤ 3 ローミング後、新しいコントローラのクライアント テーブルでクライアントに割り当てられるモビリティ ロールはどれですか。
A. 外国人
B. 透明
C. アンカー
D. 機動性
正解: (正解を表示します)

質問: **144**
企業ポリシーでは、ワイヤレス インフラストラクチャに証明書ベースの認証システムを実装することが義務付けられています。すべての企業クライアントには、クライアントが企業 Wi-Fi に接続できるようになる前に、ISE およびユーザー資格情報と組み合わせて認証を実行するために使用される証明書が含まれます。
この認証を確実に行うには、どの認証キー オプションを選択する必要がありますか?
A. PSK
B. CCKM
C. なし
D. 802.1x
正解: (正解を表示します)

質問: **145**
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: 146



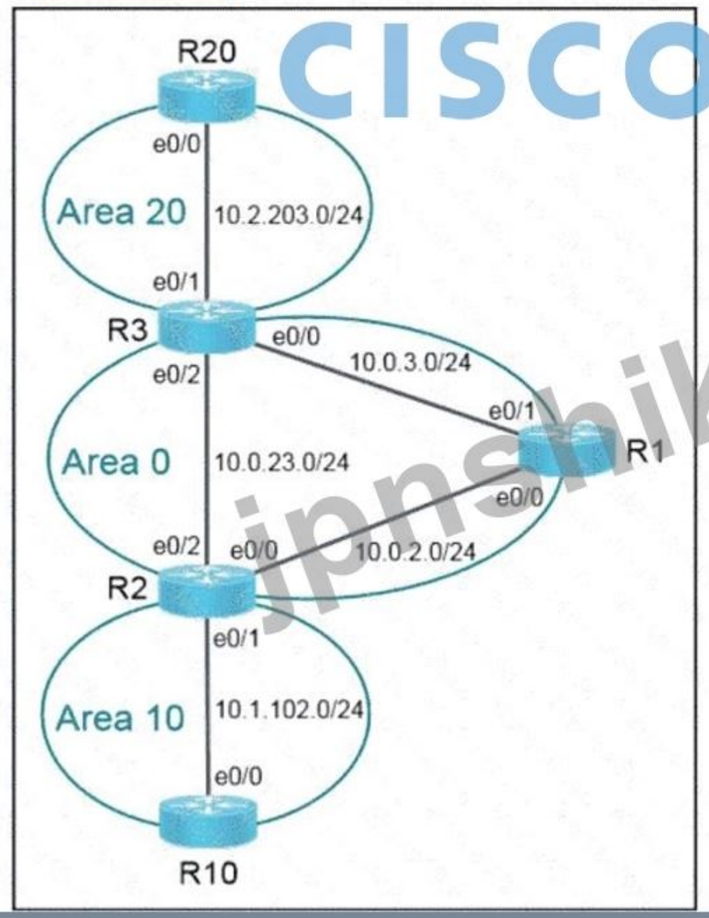
WLC のインターフェイスが RADIUS サーバと同じサブネットにない場合、WLC はすべての RADIUS 関連トラフィックのソースとしてどのインターフェイスを使用しますか?
A. コントローラの仮想インターフェース
B. WLCに設定されている任意のインターフェース
C. コントローラ管理インターフェース
D. WLAN設定で指定されたインターフェース
正解: **D** (コメントを発表する)

質問: **147**
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. 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
B. 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
C. 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
D. 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
正解: **(**正解を表示します**)**

質問: **148**

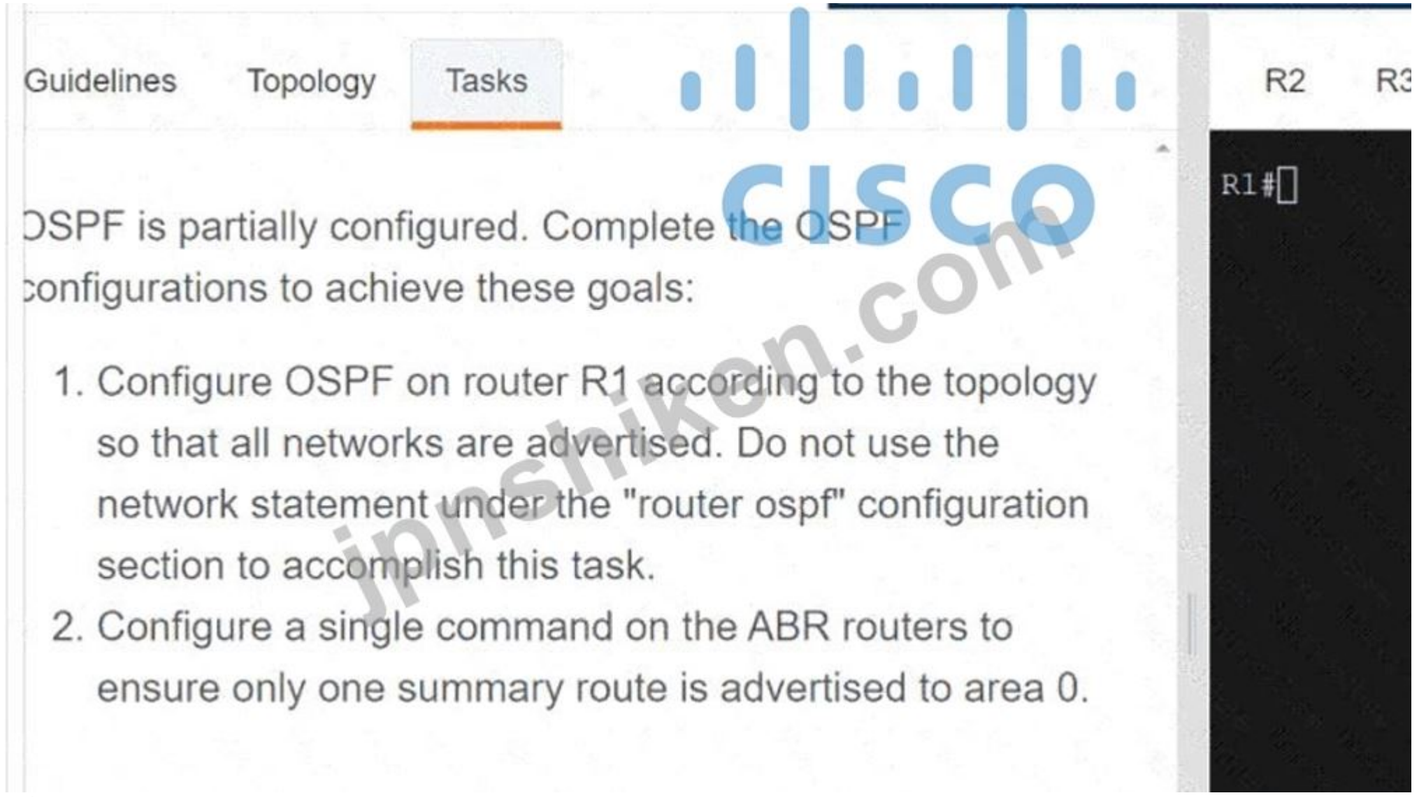
Recording

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

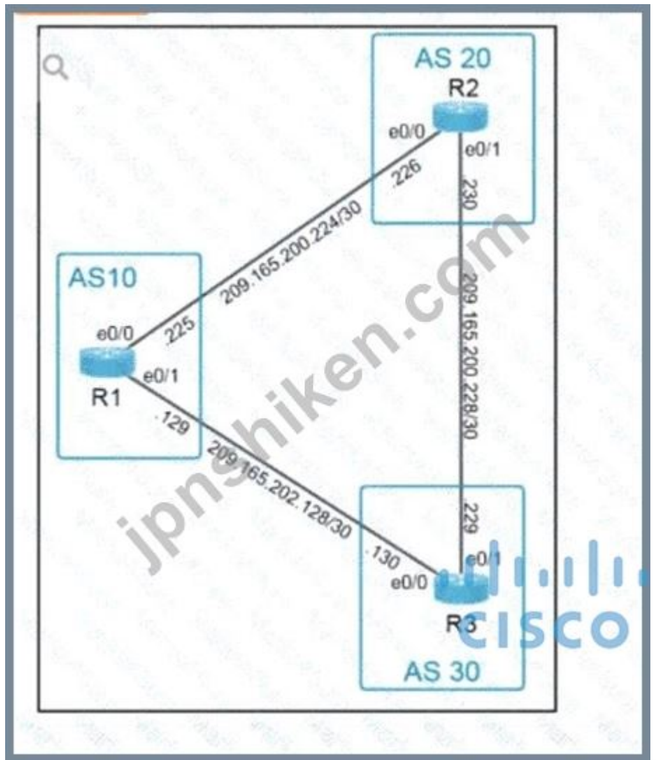
wr
R3
Router ospf 10
Area 10 range 10.2.0.0 255.255.0.0
Exit
Wr
OR

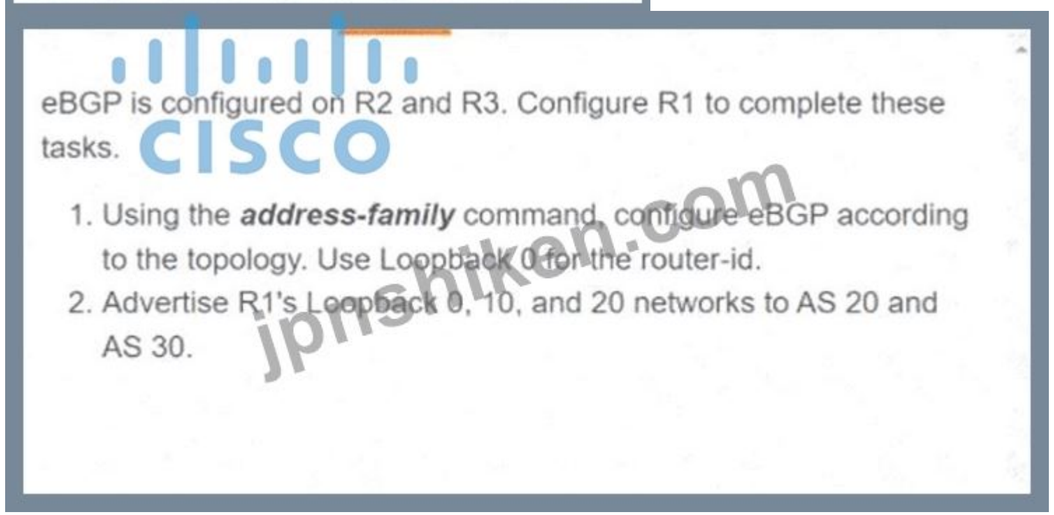
質問: **149**
特定の距離における RF 信号振幅の低下を表す RF 値はどれですか?
A. 有効等方放射電力
B. 自由空間パス損失
C. 受信信号強度インジケータ
D. 信号対雑音比
正解: **(**正解を表示します**)**

質問: **150**
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. 配布ノード
B. 境界ノード
C. 集約ノード
D. コアノード
正解: **(**正解を表示します**)**

質問: **151**
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. YANG
B. JSON
C. XML
D. XDR
正解: **(**正解を表示します**)**

質問: **152**





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: **153**
どの NGFW モードがファイアウォールを通過するフローをブロックしますか?
A. タップ
B. インラインタップ
C. インライン
D. パッシブ
正解: **C** (コメントを発表する)

質問: **154**
2 層の Cisco SD-Access 設計で、集約されたコアを構成する 2 つのノードはどれですか? (2 つ選択してください。)
A. 拡張ノード
B. 境界ノード
C. エッジノード
D. コアノード
E. 配布ノード
正解: **D,E** (コメントを発表する)

質問: **155**

```
R2(config)#ntp authenticate
R2(config)#ntp authentication-key 1 md5 NTP-p455w0rd
```

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.

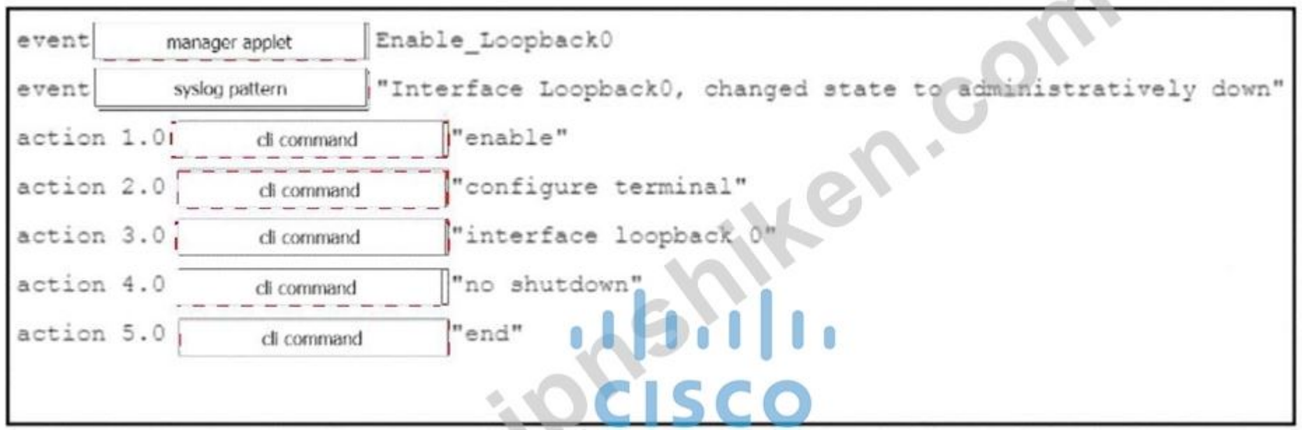
質問**: 156**
コントローラ間ローミングを有効にするには、2 つの WLC 間にどのタイプのトンネルが必要ですか?
A. CAPWAP
B. LWAPP
C. IPsec
D. 機動性
正解: **(**正解を表示します**)**

質問**: 157**
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. GRE
B. TrustSec
C. IPsec
D. MACsec
正解: **(**正解を表示します**)**

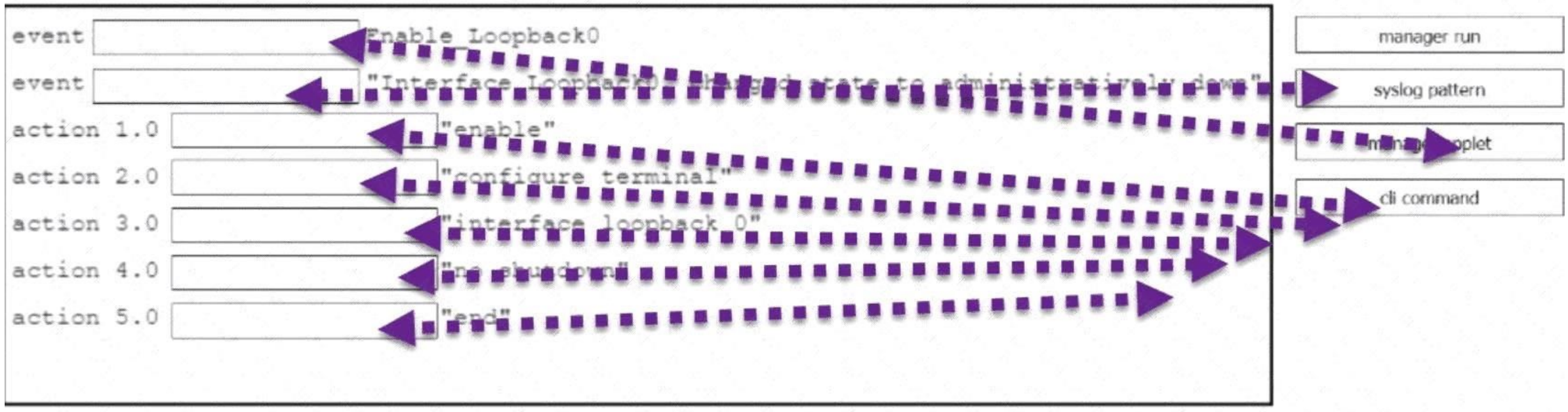
質問**: 158**

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: 159
必要な認証データを含まないGET REST API呼び出しをサーバーに送信すると、どのような結果になりますか？
A. サーバーはクライアントのIPアドレスを使用してクライアントを認証し、それに応じて呼び出しを実行します。
B. サーバーはセッションを開いたままにして、クライアントが認証データを提供するのを待ち、その後、それに応じて呼び出しを実行します。
C. サーバーはゲスト権限で呼び出しを実行します。
D. サーバーは呼び出しを実行せずに4xx応答コードを返します。
正解: **D** (コメントを発表する)
A REST API request that lacks required authentication information is rejected by the server before the requested operation is executed. REST APIs commonly use HTTP status codes to communicate request success or failure. When authentication credentials, API tokens, session cookies, or authorization headers are missing or invalid, the server normally returns a client-error response in the 4xx range.
Common examples include 401 Unauthorized, meaning authentication is required or failed, and 403 Forbidden, meaning the server understood the request but refuses access because the requester lacks permission. The server does not authenticate based only on source IP unless a separate IP-based access- control mechanism has been deliberately configured, so option A is not generally correct. The server also does not normally keep the HTTP transaction open indefinitely waiting for credentials, so option B is wrong. Option C is dangerous and wrong: APIs should not downgrade unauthenticated requests into guest execution unless an endpoint is intentionally public. In ENCOR automation, REST API security requires explicit authentication and authorization, usually over HTTPS/TLS. References/topics:
ENCOR Automation, REST APIs, HTTP status codes, API authentication, tokens, Cisco Catalyst Center API behavior.

質問: 160
無線クライアントが2つの異なる無線コントローラ間をローミングすると、一定時間ネットワーク接続が途切れます。この問題の原因となる設定上の問題は何でしょうか？
A. モビリティ グループ内のすべてのコントローラが同じ仮想インターフェイス IP アドレスを使用しているわけではありません。
B. モビリティ グループ内のすべてのコントローラが同じモビリティ グループ名を使用しています
C. モビリティ グループ内のすべてのコントローラが同じモビリティ グループ名を使用しているわけではありません。

D. モビリティ グループ内のすべてのコントローラは同じ仮想インターフェイス IP アドレスを使用しています。
正解: **A** (コメントを発表する)

質問: **161**
スクリプトにステートメント white loop != 999 ' が含まれています。どの値がループを終了しますか?
A. 999 以下の値。
B. 999 以上の値。
C. 999 に等しい値。
D. 999 と等しくない値。
正解: (正解を表示します)

質問: **162**

```
ip sla 10
icmp-echo 192.168.10.20
timeout 500
frequency 3
ip sla schedule 10 life forever start-time now
track 10 ip sla 10 reachability
```


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 sla 10 状態ダウン
C. 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
D. イベントマネージャアプレット EEM_IP_SLAevent トラック 10 状態到達不能
正解: (正解を表示します)

質問: **163**
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、ソフトウェア、クラウド、仮想化インスタンス
B. ハードウェア、仮想化、クラウドインスタンス
C. ハードウェアと仮想化インスタンス
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: **164**
REST API セキュリティを実現する 1 つの方法は何ですか?
A. Webサービスセキュリティと呼ばれる組み込みプロトコルを使用する
B. MD5ハッシュを使用して整合性を検証する

C. XML暗号化とXML署名の組み合わせを使用する
D. HTTPSおよびTLS暗号化を使用
正解: **D** (コメントを発表する)

質問: **165**
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. モビリティグループ
C. RFグループ化
D. N+1の高可用性
正解: (正解を表示します)

質問: **166**
データモデリング言語の目的は何ですか?
A. 送受信データの解析時に実行される手順を標準化する
B. テキストとバイナリデータのエンコード間のトランスコードのルールを指定する
C. オブジェクト指向プログラミングアプローチを使用してデータを処理するためのフレームワークを確立する
D. 交換されるデータの構造と意味を記述する
正解: (正解を表示します)

質問: **167**
タイプ 1 ハイパーバイザーの特徴は何ですか?
A. 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。
B. ホスト オペレーティング システム上で実行されます。
C. 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。
D. ベアメタル サーバー上で実行されます。
正解: (正解を表示します)

質問: **168**
FHRP と SSO の違いは何ですか?
A. 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。
B. 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。
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。
正解: (正解を表示します)

質問: **169**

```
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)
```

1 video

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: **170**
YANG モデルは何を提供しますか?
A. 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
B. 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
C. 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
D. トランスポートプロトコルの作成とOSとの相互作用
正解: (正解を表示します)

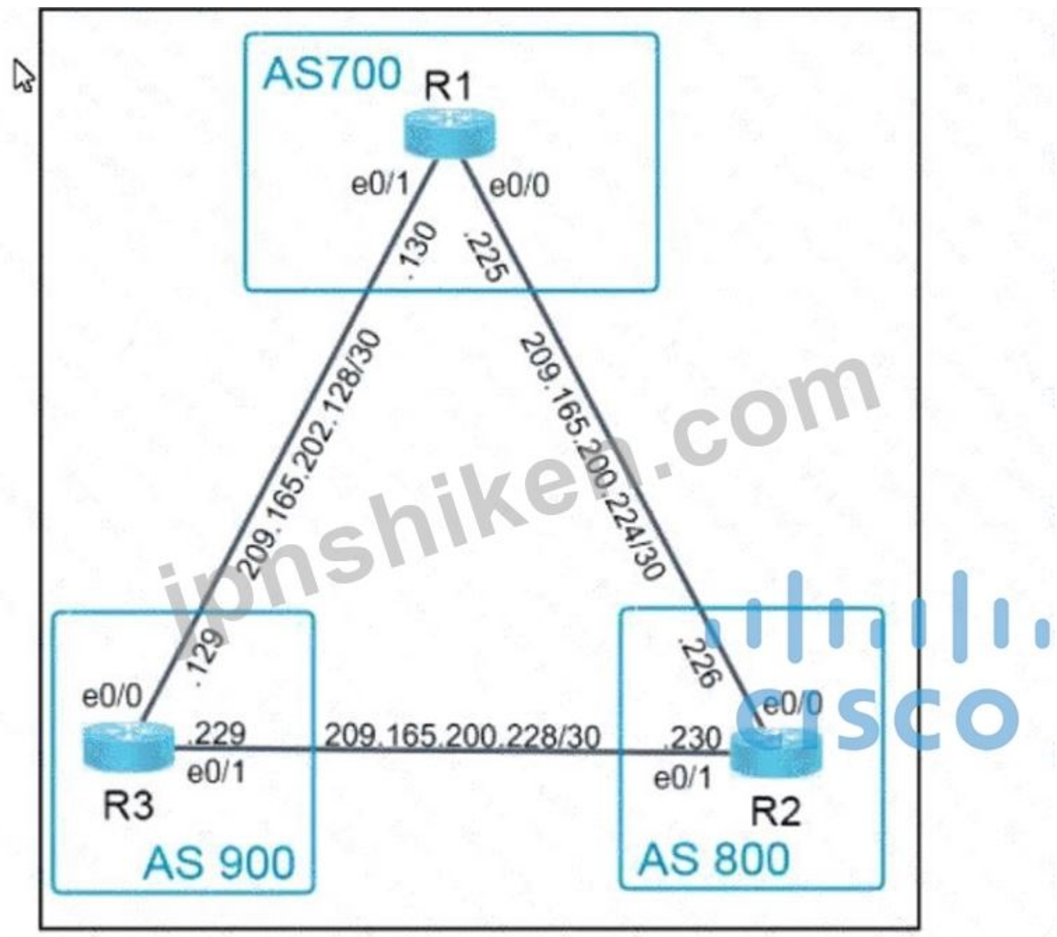
質問: **171**

どのタグが AP 展開のローミング ドメインとプロパティを定義しますか?
A. サイトタグ
B. ポリシータグ
C. APタグ
D. RFタグ
正解: **(**正解を表示します**)**

質問: **172**
API リクエストに使用できるデータ形式はどれですか?
A. パイソン
B. HTML
C. パール
D. JSON
正解: **D (**コメントを発表する**)**

質問: **173**
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 D の RF 信号強度が最も強くなります。
B. 場所CのRF信号強度は場所Bの10倍強い
C. 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
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 B の RF 信号強度は場所 A よりも 50% 弱くなります。
正解: **B,C (**コメントを発表する**)**

質問: **174**



Guidelines Topology Tasks

Configure R3 according to the topology to achieve these results:

1. Configure eBGP using Loopback 0 for the router-id. Do not use the address-family command to accomplish this.
2. Advertise R3's Loopback 100 and Loopback 200 networks to AS800 and AS900.

正解:

See the solution below in Explanation:

Explanation:

Solution:

```
R3#sh run | s bgp
router bgp 900
 bgp router-id 10.3.3.3
 bgp log-neighbor-changes
 network 209.165.201.4 mask 255.255.255.255
 network 209.165.201.5 mask 255.255.255.255
 neighbor 209.165.200.230 remote-as 800
 neighbor 209.165.202.130 remote-as 700
R3#
```

Copy run start

Verification:

```
R3#sh ip bgp su
BGP router identifier 10.3.3.3, local AS number 900
BGP table version is 3, main routing table version 3
2 network entries using 288 bytes of memory
2 path entries using 168 bytes of memory
1/1 BGP path/bestpath attribute entries using 160 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 616 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ U
p/Down  State/PfxRcd
209.165.200.230 4          800      10      10        3    0    0 0
0:03:00        0
209.165.202.130 4          700       8       8        3    0    0 0
0:03:18        0
R3#
```

OR

質問: **175**

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. TLOC

B. DNS

C. RLOC

D. EID

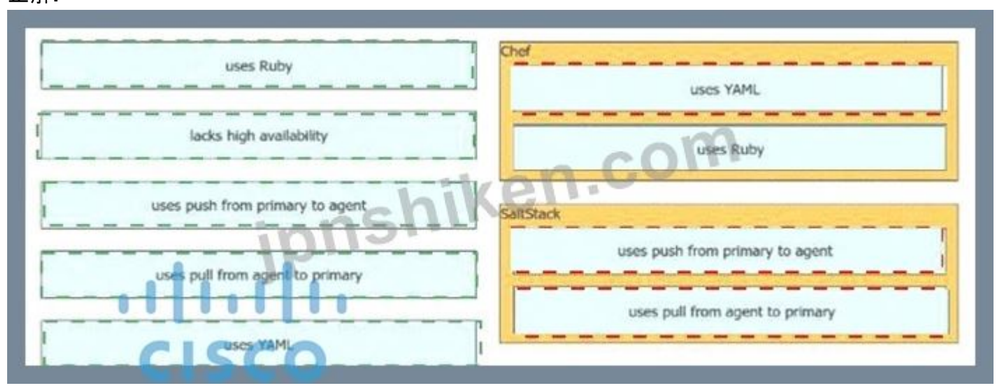
E. VTEP

正解: **C,D** (コメントを発表する)

質問: **176**

左側の自動化特性を右側の適切なツールにドラッグ 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:

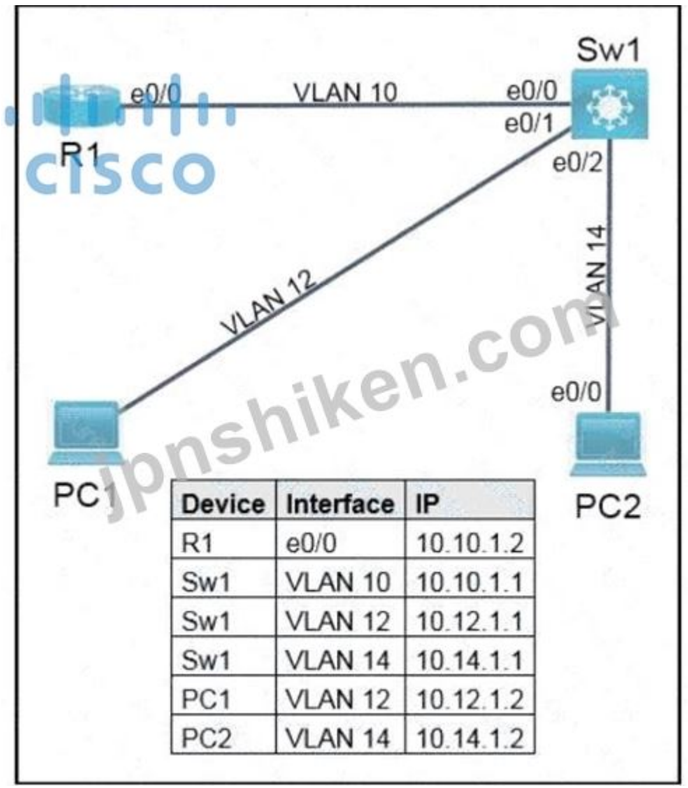


Explanation:

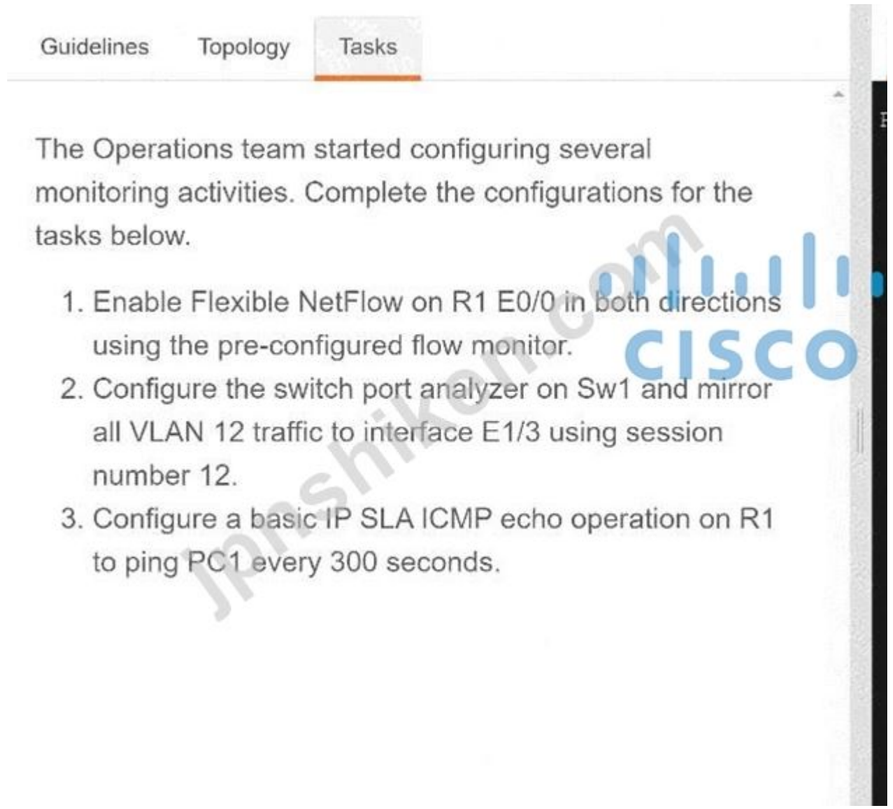
質問: **177**
ワイヤレスクライアントがローミングするかどうかを決定するデバイスはどれですか？
A. ワイヤレスクライアント
B. WCSロケーションサーバー
C. 無線LANコントローラー
D. アクセスポイント
正解: **A (**コメントを発表する**)**

質問: **178**
サイト間ワイヤレス接続にはどのタイプのアンテナを使用すればよいですか?
A. 双極子
B. パッチ
C. 全方向
D. 八木
正解: **(**正解を表示します**)**

質問: **179**



Device	Interface	IP
R1	e0/0	10.10.1.2
Sw1	VLAN 10	10.10.1.1
Sw1	VLAN 12	10.12.1.1
Sw1	VLAN 14	10.14.1.1
PC1	VLAN 12	10.12.1.2
PC2	VLAN 14	10.14.1.2



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: **180**
REST API 認証の API キー オプションとは何ですか?
A. ワンタイム暗号化トークン
B. ローカルルータに保存されているユーザー名
C. 暗号化されずに送信される認証情報
D. 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。
正解: **D** (コメントを発表する)

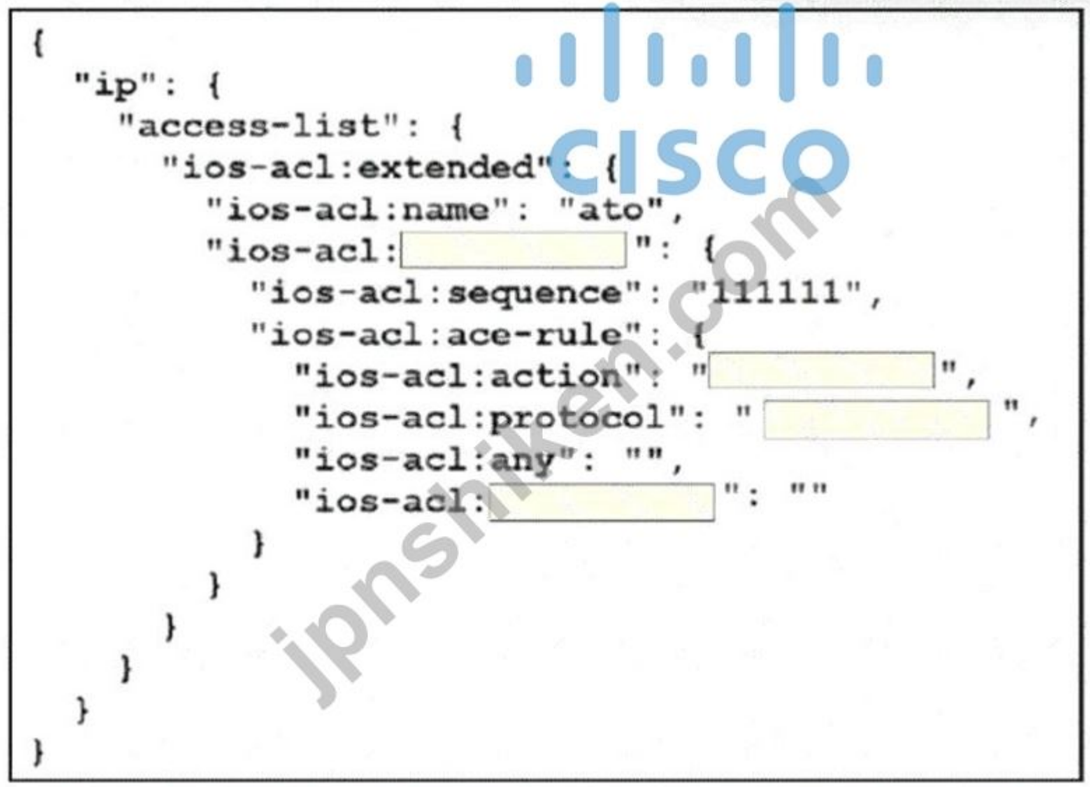
質問: **181**
エンジニアは、Cisco Catalyst 9800シリーズWLC用のアクセスリストを作成し、ワイヤレスゲストユーザーをCisco ISEサーバー上でホストされているスプラッシュページにリダイレクトする必要があります。
Cisco ISEサーバーは、10.9.11.141と10.1.11.141でホストされています。
どのアクセスリストが要件を満たしていますか？
A. ip access-list extended REDIRECT
udp 任意の eq ドメインを許可する
任意のIPアドレスからのアクセスをホスト10.9.11.141に許可する
任意のIPアドレスからのアクセスをホスト10.1.11.141に許可する
TCP 任意のポート 80 と等しいポートを拒否します
TCP 任意の 443 と等しい通信を拒否します
B. ip access-list extended REDIRECT
UDP の任意のドメインを拒否します
10.9.11.141 の IP アドレスを任意のホストから拒否します
10.1.11.141 の IP アドレスを任意のホストから拒否します
TCP 任意のポート 80 と等しいポートを拒否します
TCP 任意の 443 と等しい通信を拒否します
C. ip access-list extended REDIRECT
UDP の任意のドメインを拒否します
10.9.11.141 の IP アドレスを任意のホストから拒否します
10.1.11.141 の IP アドレスを任意のホストから拒否します
TCP 任意のポート 80 を許可する
TCP 任意の 任意の 443 を許可する
D. ip access-list extended REDIRECT
udp 任意の eq ドメインを許可する
10.9.11.141 の IP アドレスを任意のホストから拒否します
10.1.11.141 の IP アドレスを任意のホストから拒否します
TCP 任意のポート 80 を許可する
TCP 任意の 任意の 443 を許可する
正解: (正解を表示します)

質問: **182**
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. 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。
B. 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。
C. 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。
D. 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。
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: **183**
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.CAPWARCONTROLLERJocaldomain
D. CISCO.CONTROLLER.localdomain
正解: **A (**コメントを発表する**)**

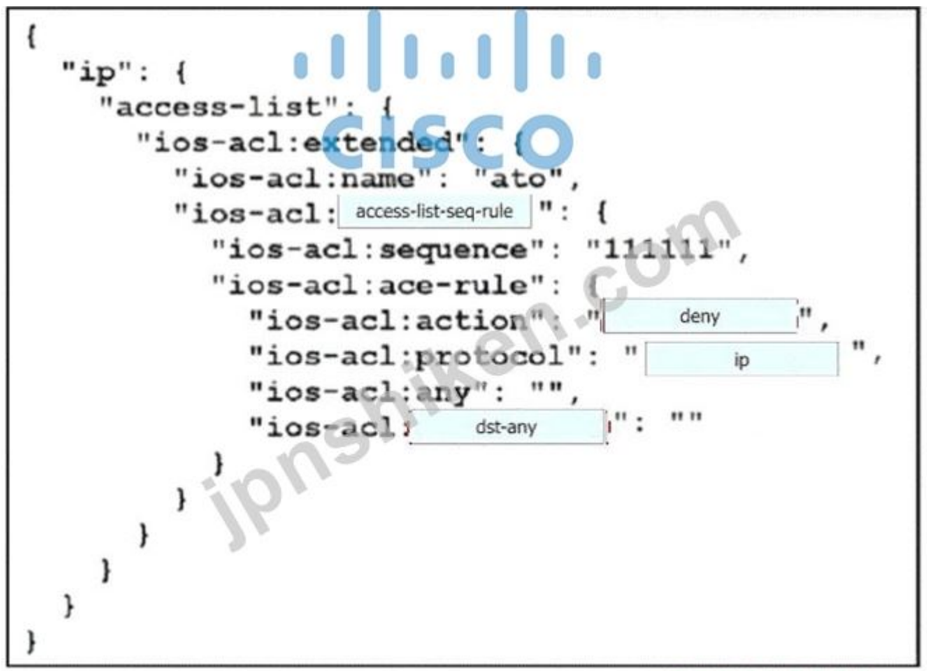
質問: **184**
Cisco Cyber Threat Defense は何に対して可視性を提供しますか?
A. 侵害されたホストと攻撃者間の通信チャネル上のコマンドおよび制御トラフィック
B. ネットワーク内の継続的なスキャンプローブによるネットワークソフトウェアの脆弱性
C. ログメッセージとテレメトリ情報に基づくセキュリティ脅威
D. ユーザーが保存したデータと、ユーザーが実行しているプログラムの内部依存関係
正解: **(**正解を表示します**)**

質問: **185**
下部のコード 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、アクセス リストに拒否ルールを構成する要求を作成します。



deny | access-list-seq-rule | dst-any | ip

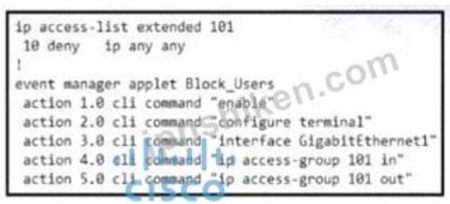
正解:



deny | access-list-seq-rule | dst-any | ip

Explanation:
access-list-sec-rule, deny, ip, dst-any

質問: **186**



展示を参照してください。エンジニアがアクセスリストを適用するためのEEMスクリプトを作成します。スクリプトを完成させるには、どのステートメントを追加する必要がありますか？

A. action 2.1 cli command "ip access-list extended 101"
B. action 3.1 cli command "ip access-list extended 101"
C. イベントなし
D. action 6.0 cli command "ip access-list extended 101"
正解: **(**正解を表示します**)**

質問: **187**

図を参照してください。ネットワーク管理者は、すべてのRADIUSサーバーにアクセスできない場合でも、構成変更を実行できる必要があります。ユーザーが正常に認証された場合に、すべてのコマンドを承認できる構成はどれですか？

A. aaa authorization exec default group radius if-authenticated

B. aaa authorization exec default group radius none

C. aaa authorization exec default group radius

D. aaa 認証ログインデフォルトグループradiusローカルなし

正解: **A** (コメントを発表する)

The correct answer is A. aaa authorization exec default group radius if-authenticated.

The key part of this question is the phrase "when all the RADIUS servers are unreachable" and "if the user has successfully authenticated." In Cisco AAA, the if-authenticated keyword means that if the authorization server cannot be reached, the device grants authorization as long as the user has already been authenticated successfully. Cisco documentation explicitly states that with:

aaa authorization exec default group radius if-authenticated

the device contacts the RADIUS server for EXEC authorization, and if an error occurs contacting the server, the fallback is to permit the CLI to start, provided the user has been properly authenticated.

* The current config already has:

aaa authentication login default group radius local

So, if RADIUS is down, login can fall back to the local user database.

* Adding:

aaa authorization exec default group radius if-authenticated

ensures that once the user is authenticated, authorization is permitted even if RADIUS is unreachable. This is the Cisco-supported fallback behavior for AAA authorization.

* B. aaa authorization exec default group radius none The none method means no authorization is performed if the previous method fails, but this is not the Cisco ENCOR-recommended method for allowing access after successful authentication. The question specifically targets the if-authenticated authorization fallback behavior.

* C. aaa authorization exec default group radius This attempts authorization through RADIUS only. If the RADIUS servers are unreachable, authorization fails and the administrator may not be able to proceed.

* D. aaa authentication login default group radius local none This is an authentication command, not an authorization command, so it does not solve the requirement to authorize commands after login.

ENCOR exam point:

Remember the difference:

* Authentication = verifies identity

* Authorization = determines what the user is allowed to do

For Cisco AAA fallback behavior:

* local is commonly used for authentication fallback

* if-authenticated is the key keyword for authorization fallback when the AAA server is unreachable

質問: **188**

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. 必要なユーザーVLANのみを集約層全体に拡張する

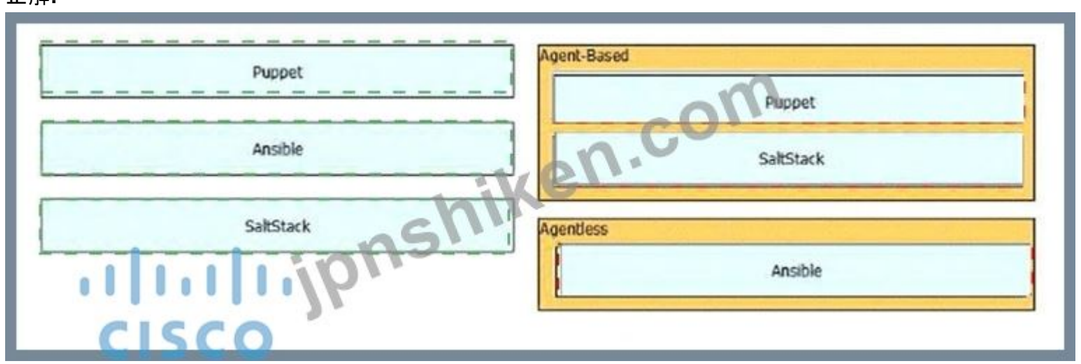
C. アクセス層全体に必要なユーザーVLANのみを拡張する

D. すべてのユーザーVLANをアクセス層全体に拡張します
正解: **(**正解を表示します**)**

質問: **189**
ユニキャスト ルーティング テーブルを変更せずにマルチキャスト RPF チェックに合格することを保証する 2 つの方法は何ですか? (2 つ選択してください。)
A. OSPFルーティングプロトコルの実装
B. ルータのマルチキャストソースへのインターフェースを無効にする
C. MBGPの実装
D. BGPルーティングプロトコルを無効にする
E. 静的 mroute の実装
正解: **(**正解を表示します**)**

質問: **190**
ドラッグ＆ドロップ。左側のツールを右側のエージェントタイプにドラッグ＆ドロップしてください。

正解:



Explanation:
Agent-Based: A, C
Agentless: B
Puppet and SaltStack are generally categorized as agent-based automation tools because they normally rely on managed nodes running a local agent or minion process. Puppet uses agents on managed systems to receive catalogs from the Puppet master/server and enforce the desired state. SaltStack commonly uses a Salt master and Salt minions, where the minion runs on the managed node and receives commands or state instructions. Ansible is agentless because it

does not require a resident agent on managed devices or servers. Instead, Ansible connects using standard remote access mechanisms such as SSH for Linux/Unix systems, WinRM for Windows, and network-specific connection plugins for network devices. In ENCOR automation topics, this distinction matters because agentless tools reduce endpoint installation overhead, while agent-based systems can provide persistent state enforcement and event-driven control. For Cisco network automation, Ansible is frequently tested as an agentless automation tool using playbooks and modules. References/topics: ENCOR Automation, orchestration tools, Ansible, Puppet, SaltStack, agent-based versus agentless automation.