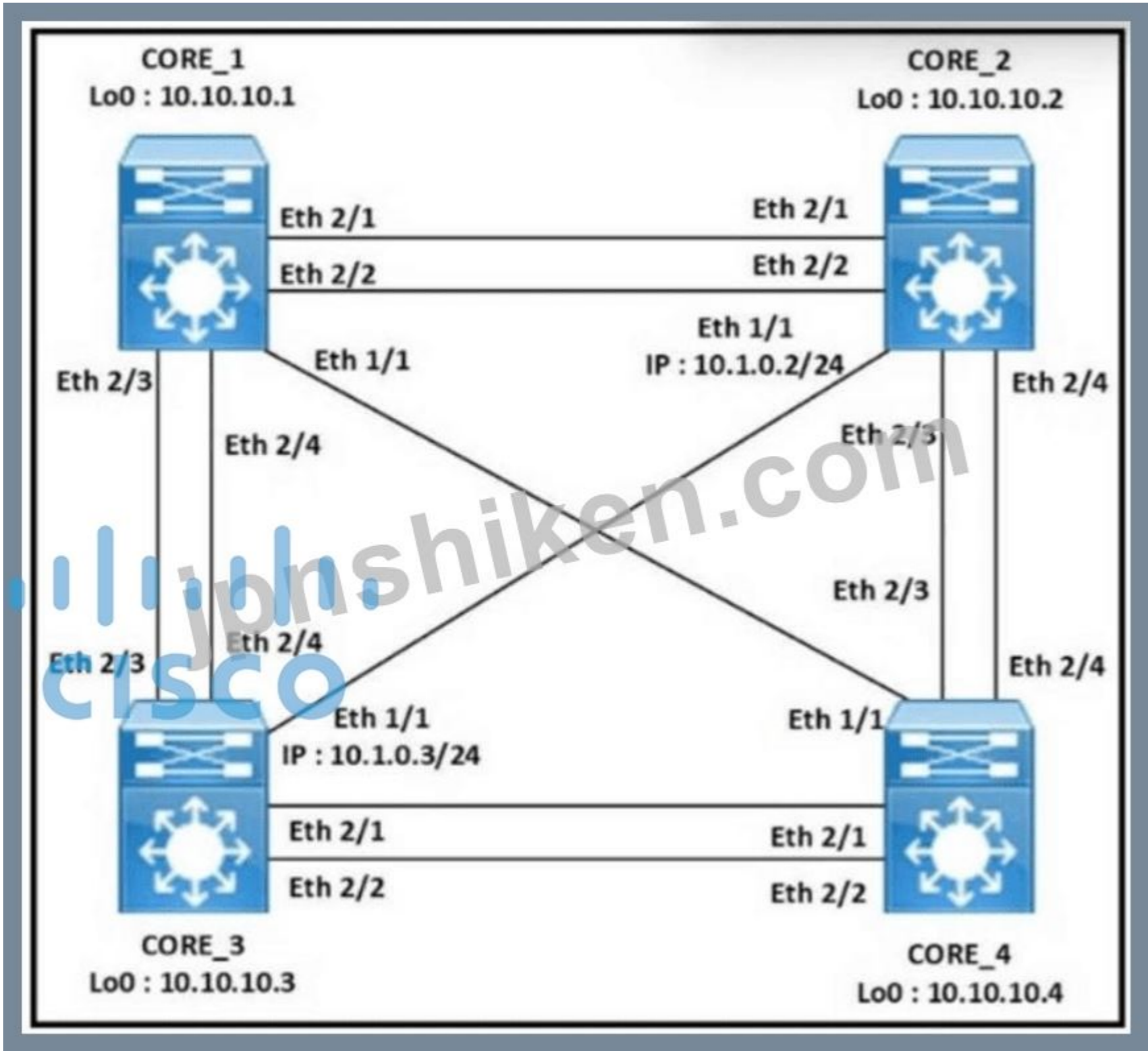


## Cisco.350-601.v2026-06-25.q301

試験コード : 350-601  
試験名称 : Implementing Cisco Data Center Core Technologies (350-601 DCCOR)  
認証ベンダー : Cisco  
無料問題の数 : 301  
バージョン : v2026-06-25  
ページの閲覧量 : 106  
問題集の閲覧量 : 3060

<https://www.jpnsiken.com/shiken/Cisco.350-601.v2026-06-25.q301.html>

質問: 1



```
feature vn-segment-vlan-based
feature nv overlay
```

```
vlan 100
 name APP
 vn-segment 10100
vlan 200
 name DB
 vn-segment 10200
```

```
Interface NVE1
 no shutdown
```

図を参照してください。ネットワークエンジニアは、CORE\_2とCORE\_3という2つのコアスイッチ間でVXLANを実装する必要があります。コアスイッチではマルチキャストを無効にする必要があります。さらに、APPと呼ばれるVLAN 100とDBと呼ばれるVLAN 200をコアスイッチ間で拡張する必要があります。CORE\_2での初期VXLAN設定は完了しています。どのネットワーク仮想インターフェイス設定でVXLAN設定が完了しますか？

```
source-interface nve1
 source loopback0
 member vni 10100
 ingress-replication protocol ospf
 peer-ip 10.1.0.3
 member vni 10200
 ingress-replication protocol ospf
 peer-ip 10.1.0.3
```

A.

```
source interface Loopback 0
 source nve1
 member vni 10100
 ingress-replication
 peer-ip 10.10.10.3
 member vni 10200
 ingress-replication
 peer-ip 10.10.10.3
```

B.

```
interface Loopback 0
  source interface nve1
  member vni 10100
  ingress-replication
  peer-ip 10.1.0.3
  member vni 10200
  ingress-replication
  peer-ip 10.1.0.3
```

C.

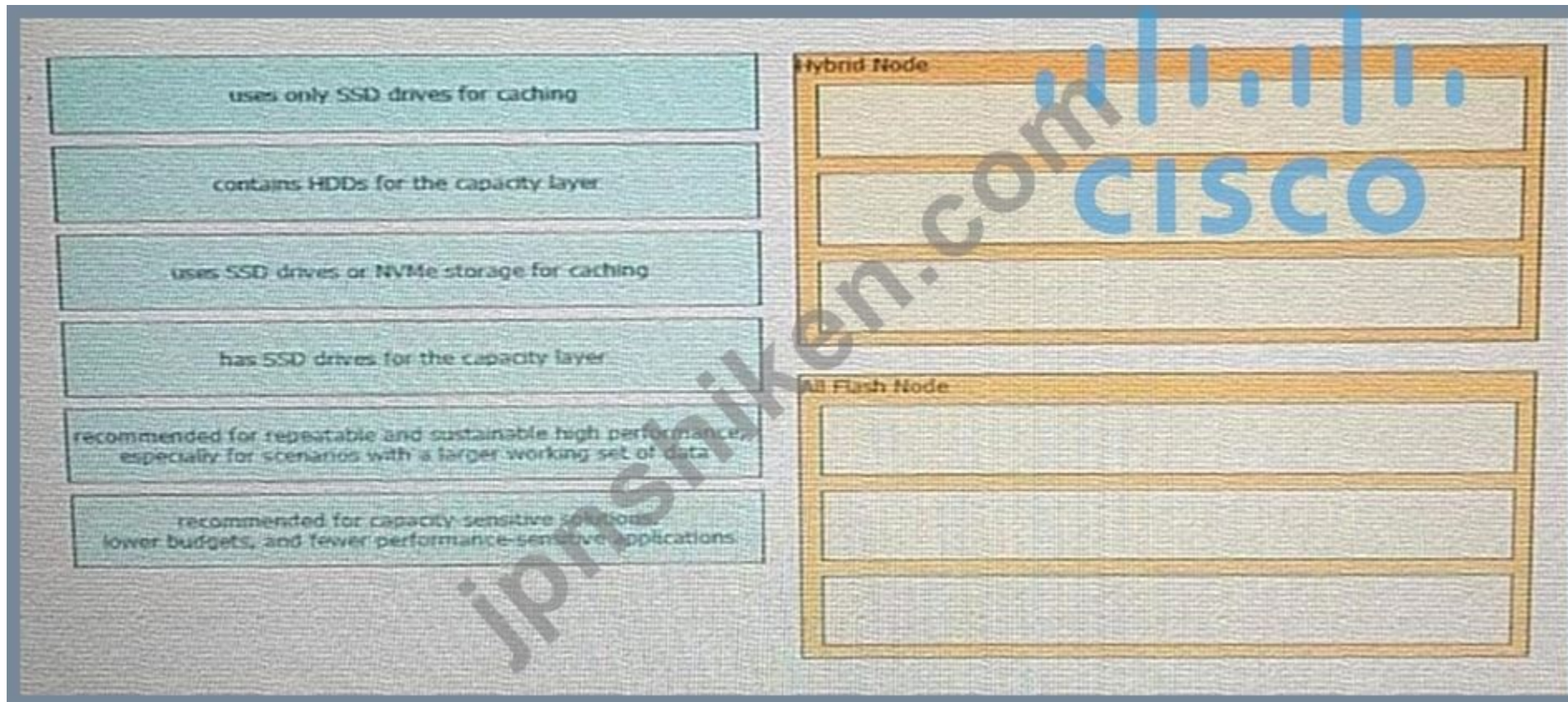
```
interface nve1
  source-interface loopback0
  member vni 10100
  ingress-replication protocol static
  peer-ip 10.10.10.3
  member vni 10200
  ingress-replication protocol static
  peer-ip 10.10.10.3
```

D.

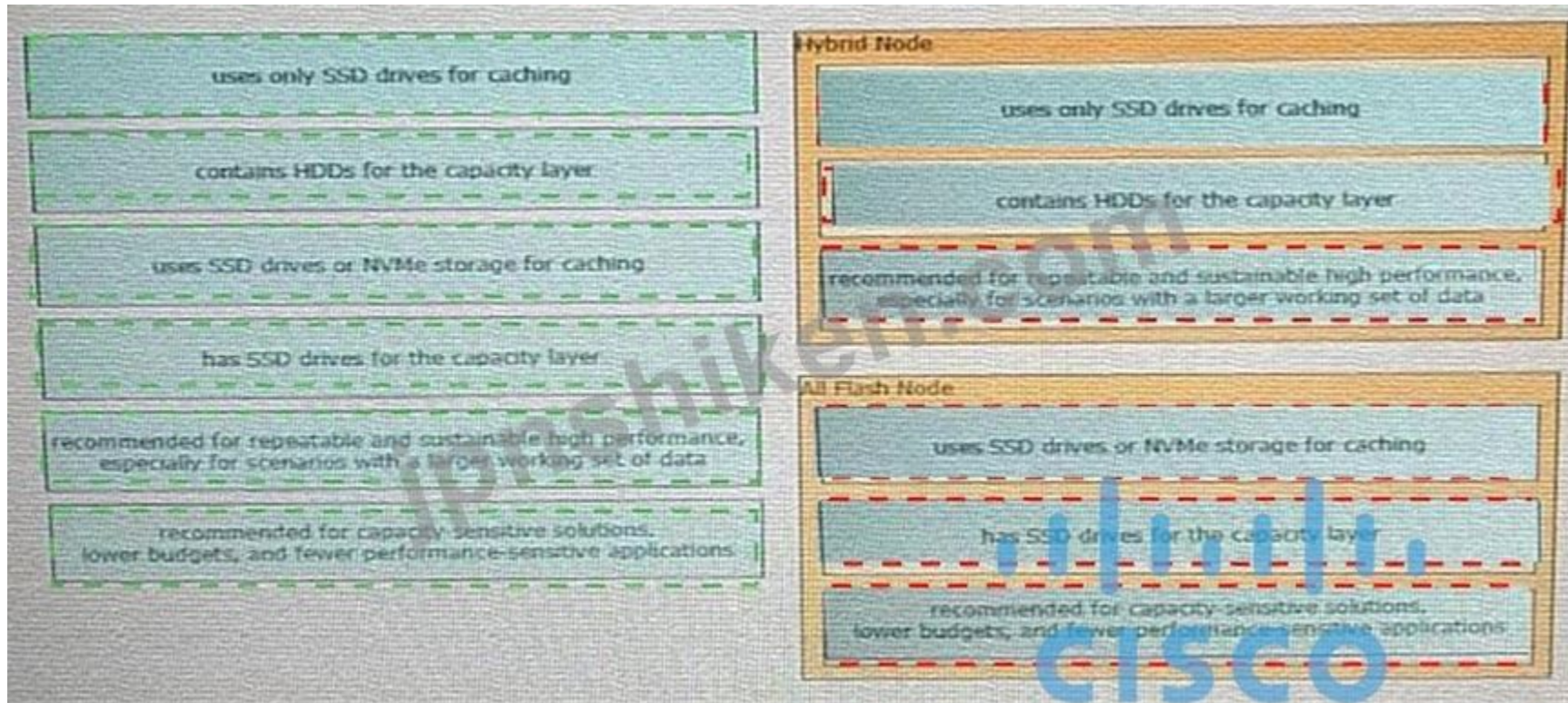
正解: ([正解を表示します](#))

質問: 2

左側のハイパーフレックス特性を、右側の適切なハイパーフレックスノードタイプにドラッグアンド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。



正解:





質問: 3

データセンターにCisco UCS Cシリーズサーバーが設置されています。このサーバーは、管理とデータトラフィックに1本のケーブルを使用し、Cisco UCS Managerによって管理される必要があります。物理接続が確立された後、どの構成を適用する必要がありますか？

```

UCS-A# scope chassis 1
UCS-A /chassis# scope cimc
UCS-A /chassis/cimc# set mgmt-conn-state enabled
UCS-A /chassis/cimc/mgmt-conn* # commit-buffer

UCS-A# scope server 1
UCS-A /server# scope cimc
UCS-A /server/cimc# scope mgmt-conn sideband
UCS-A /server/cimc/mgmt-conn # set mgmt-conn-state enabled
UCS-A /server/cimc/mgmt-conn* # commit-buffer

UCS-A# scope chassis 1
UCS-A /chassis# scope cimc
UCS-A /chassis/cimc# scope mgmt-conn sideband
UCS-A /chassis/cimc/mgmt-conn # mgmt-conn-state enabled
UCS-A /chassis/cimc/mgmt-conn* # commit-buffer

UCS-A# scope server 1
UCS-A /server# scope cimc
UCS-A /server/cimc# scope mgmt-conn sideband
UCS-A /server/cimc# mgmt-conn-state enabled
UCS-A /server/cimc/mgmt-conn* # commit-buffer

```

- A. オプションD
- B. オプションA
- C. オプションB
- D. オプションC

正解: C (コメントを发表する)

質問: 4



Name : **locale3**  
Organizations

Advanced Filter Export Print

Name	Org DN
Engineering	org-root/org-Engineering
Sales	org-root/org-Sales

Name : **locale4**  
Organizations

Advanced Filter Export Print

Name	Org DN
B2B	org-root/org-B2B
Sales	org-root/org-Sales

図を参照してください。エンジニアは、複数のサブ組織をホストする UCS ドメインで、user 1 という新しいユーザー名を設定する必要があります。セキュリティ ポリシーでは、admin ロールの使用が禁止されています。ユーザー名には、次の権限が必要です。

- user1 must have access to the Sales sub-organization.
- user1 must be allowed to acknowledge the chassis and IO Module.
- user1 must be allowed to configure beacons.
- user1 must have read access to the rest of the system.

ユーザー1がこれらの権限を持つためには、どの構成を使用する必要がありますか？

- A. 役割: server-profile ロケール: locale 1
- B. 役割: server-equipment ロケール: locale4
- C. 役割: server-compute ロケール: locale3
- D. 役割: server-security ロケール: locale2

正解: ([正解を表示します](#))

質問: 5

Cisco Intersightとの接続のためにCisco UCS Managerドメインを有効にする前に、どの2つの設定を構成する必要がありますか？ (2つ選択してください。)

- A. syslogリダイレクト
- B. DNSサーバー
- C. SMTPサーバー
- D. NTPサーバー
- E. SMTP返信先アドレス

正解: (正解を表示します)

Cisco Intersight との接続用に Cisco UCS Manager ドメインを有効にする前に、ドメインの DNS サーバーと NTP サーバーを設定する必要があります。DNS サーバーは Cisco Intersight サービス (svc.intersight.com) のホスト名を解決するために必要であり、NTP サーバーは Cisco UCS Manager と Cisco Intersight サービス間の時刻を同期するために必要です。これらの設定により、Cisco UCS Manager は Cisco Intersight サービスとの安全で信頼性の高い接続を確立し、ドメインを Cisco Intersight アカウントに登録できます。

参考資料 .Cisco Intersight接続用にCisco UCS Managerドメインを構成する方法の詳細については、以下の資料を参照してください。

\* Intersight Device Connector 用 Cisco UCS Manager 設定ガイド

\* Cisco Intersight 入門ガイド

質問: 6

展示資料を参照してください。

```
Nexus(config)# show checkpoint summary
User Checkpoint Summary
-----
1) BeforeL3:
Created by admin
Created at Mon, 15:25:08 31 Dec 2018
Size is 9,345 bytes
Description: None

System Checkpoint Summary
-----
2) system-fm-vrrp:
Created by admin
Created at Fri, 09:57:02 14 Jun 2019
Size is 20,865 bytes
Description: Created by Feature Manager.

3) system-fm-hsrp_engine:
Created by admin
Created at Fri, 09:57:28 14 Jun 2019
Size is 20,852 bytes
Description: Created by Feature Manager.
```

system-fm-vrrpチェックポイントが作成された理由は何ですか？

- A. VRRPサービスが再起動され、チェックポイントが自動的に作成されました。
- B. ネットワーク管理者が手動で作成しました。

- C. VRRPプロセスがクラッシュし、チェックポイントが自動的に作成されました。
- D. VRRP有効化機能が無効になっています。

正解: ([正解を表示します](#))

説明

質問: 7

DevOpsエンジニアは、Pythonを使用してCiscoデバイスを管理する必要があります。このデバイスは、高度なセキュリティが確保されたDMZ環境に設置されています。使用できるのは、信頼できるCisco製Pythonライブラリのみです。

どのソリューションが要件を満たしていますか？

- A. 信頼できるCiscoライブラリを使用するオンボックスPythonスクリプトを開発する。
- B. 主要なクラウドプロバイダーでサーバーレス技術を使用してアプリケーションを開発します。
- C. 信頼できるCiscoライブラリを使用する、外部Pythonスクリプトを開発する。
- D. シスコが提供する信頼できるライブラリを使用するコンテナ化アプリケーションを開発する。

正解: ([正解を表示します](#))

質問: 8

エンジニアは、Cisco Nexus 9000シリーズスイッチのEEM (エンタープライズ環境管理) 画面で、これらのコマンドを入力します。

イベントマネージャアプレット Backup-config

イベントタイマー ウォッチドッグ 時間 1800 名前 タイマー

イベント cli マッチ "copy running-config startup-config"

この設定を適用した結果はどうなりますか？

- A. 1800秒ごとに実行中の設定を保存します。
- B. アクションが指定されていないため、エラーが発生します。
- C. copy running-config startup-config コマンドを実行します。
- D. copy running-config startup-config コマンドをブロックします。

正解: ([正解を表示します](#))

説明

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/system-management/b-cisco-nexu>

## Prerequisites for EEM

EEM has the following prerequisites:

- You must have network-admin user privileges to configure EEM.

## Guidelines and Limitations for EEM

EEM has the following configuration guidelines and limitations:

- The maximum number of configurable EEM policies is 500.
- Action statements within your user policy or overriding policy should not negate each other or adversely affect the associated system policy.
- To allow a triggered event to process any default actions, you must configure the EEM policy to allow the default action. For example, if you match a CLI command in a match statement, you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute.
- When you configure an EEM policy action to collect **show tech** commands, make sure to allocate enough time for the **show tech** commands to complete before the same action is called again.

質問: 9

ブートフラッシュに動作イメージがない場合にファブリックインターコネクトを復旧するために、左側の手順を右側の手順を実行する順序にドラッグアンドドロップしてください。

Copy the main image files.	step 1
Configure the management interfaces.	step 2
Boot the kickstart image using TFTP.	step 3
Install the files.	step 4

正解:

Copy the main image files.	Boot the kickstart image using TFTP.
Configure the management interfaces.	Configure the management interfaces.
Boot the kickstart image using TFTP.	Copy the main image files.
Install the files.	Install the files.

Boot the kickstart image using TFTP.
Configure the management interfaces.
Copy the main image files.
Install the files.

**質問: 10**

エンジニアは、ブートフラッシュにバックアップされた以前のバージョンからCisco MDS 9000シリーズスイッチの設定を復元し、復元が成功したことを確認する必要があります。左側のコマンドを右側の正しい順序にドラッグ&ドロップしてください。

copy bootflash:<conrfiguration_file> runring-config	Step 1
copy running-config startup-config	Step 2
show startup-config	Step 3
write erase	Step 4
reload	Step 5

正解:

copy bootflash:<conrfiguration_file> runring-config	write erase
copy running-config startup-config	reload
show startup-config	copy bootflash:<conrfiguration_file> runring-config
write erase	copy running-config startup-config
reload	show startup-config

質問: 11

展示資料を参照してください。

```
CISCO-UCS-A# scope org /
CISCO-UCS-A /org* # create service-profile Cisco1 instance
CISCO-UCS-A /org/service-profile* # set bios-policy bios1
CISCO-UCS-A /org/service-profile* # set boot-policy boot1
CISCO-UCS-A /org/service-profile* # set ext-mgmt-ip-state none
CISCO-UCS-A /org/service-profile* # set host-fw-policy ipmi-user987
CISCO-UCS-A /org/service-profile* # set identity dynamic-uuid derived
CISCO-UCS-A /org/service-profile* # set ipmi-access-profile ipmi1
CISCO-UCS-A /org/service-profile* # set local-disk-policy local1
CISCO-UCS-A /org/service-profile* # set maint-policy maint1
CISCO-UCS-A /org/service-profile* # set mgmt-fw-policy mgmt1
CISCO-UCS-A /org/service-profile* # set power-control-policy power1
CISCO-UCS-A /org/service-profile* # set scrub-policy scrub1
CISCO-UCS-A /org/service-profile* # set sol-policy sol1
CISCO-UCS-A /org/service-profile* # set stats-policy stats1
CISCO-UCS-A /org/service-profile* # set user-label Cisco
CISCO-UCS-A /org/service-profile* # vcon-policy vconnpolicy
CISCO-UCS-A /org/service-profile* # commit-buffer
CISCO-UCS-A /org/service-profile #
```

提示されたサービスプロファイルにおけるUUIDの特徴は何ですか？

- A. ハードウェアに基づく
- B. ベンダー指定
- C. 独自のシステム生成
- D. UUIDプールから割り当てられました

正解: ([正解を表示します](#))

説明

質問: 12

図を参照してください。エンジニアは、Cisco NX-OSゲストシェルでPythonを使用して、インターフェースeth1/1上のEIGRP ASNの設定を取得します。エンジニアは次のスクリプトを作成しました。

```
>>> import json
```

```
>>> from cli import*
```

asn」キーの値を取得するには、どのコマンドセットを使用する必要がありますか？

```
{
  "TABLE_asn": {
    "ROW_asn": {
      "asn": "10",
      "TABLE_vrf": {
        "ROW_vrf": {
          "vrf": "default",
          "TABLE_peer": {
            "ROW_peer": {
              "peer_handle": "0",
              "peer_ipaddr": "10.13.0.2",
              "peer_ifname": "Eth1/1",
              "peer_holdtime": "13",
              "peer_srtd": "6",
              "peer_rto": "50",
              "peer_xmitq_count": "0",
              "peer_last_seqno": "4",
              "peer_uptime": "PT46M49S"
            }
          }
        }
      }
    }
  }
}
```

A. >>> output = json.loads(clid('show ip eigrp neighbors')) >>>

出力["TABLE\_asn"]["ROW\_asn"]["asn"]

B. >>> output = json.loads(clid('show ip eigrp neighbors')) >>> output['asn']

C. >>> output = json.dumps(clid('show ip eigrp neighbors')) >>>

出力["TABLE\_asn"]["ROW\_asn"]["asn"]

D. >>> output = json.dumps(clid('show ip eigrp neighbors')) >>> output['asn']

正解: [\(正解を表示します\)](#)

### 質問: 13

Cisco Nexusシリーズスイッチ上のCisco TACACS+は、デバイスへのアクセスを試みるすべてのユーザーを認証し、TACACS+サーバーが利用できなくなった場合はローカルアカウントにフェイルオーバーする必要があります。

これらの目的を達成するコマンドはどれですか？

A. aaa認証ログインデフォルトフォールバックエラーローカル

B. aaa認証ログインコンソールグループローカル

C. aaa認証ログインデフォルトローカル

D. aaa認証ログインデフォルトグループISEローカル

正解: [\(正解を表示します\)](#)

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5\\_x/nx-](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-)

[os/security/configuration/guide/b\\_Cisco\\_Nexus\\_7000\\_NX-](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/security/configuration/guide/b_Cisco_Nexus_7000_NX-)

[OS\\_Security\\_Configuration\\_Guide\\_\\_Release\\_5-x/b\\_Cisco\\_Nexus\\_7000\\_NX-](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/security/configuration/guide/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_5-x/b_Cisco_Nexus_7000_NX-)

質問: 14

エンジニアは、Cisco Nexus 9000 シリーズ スイッチの実行中の設定を削除し、スイッチを再起動せずにバックアップ ファイルに置き換える必要があります。バックアップ ファイルは、mgmt0 インターフェイス経由でアクセスできる SFTP サーバーに保存されます。

このタスクを実行するには、どのコマンドの組み合わせを使用しますか？

- copy sftp://admin@192.168.10.100/backup.cfg startup-config vrf mgmt0  
copy startup-config running-config
- configure replace sftp://admin@192.168.10.100/backup.cfg vrf mgmt0  
copy running-config bootflash://startup-config
- copy sftp://admin@192.168.10.100/backup.cfg bootflash:///backup.cfg vrf management  
configure replace bootflash:///backup.cfg
- copy sftp://admin@192.168.10.100/backup.cfg startup-config vrf management  
reload in 10

- A. オプションA
- B. オプションD
- C. オプションB
- D. オプションC

正解: [\(正解を表示します\)](#)

質問: 15

エンジニアが、ファブリックフェイルオーバーが有効になっているサーバーのvNICのトラフィック監視を実装しています。要件は、ファブリックインターコネクットのいずれかに障害が発生した場合でも、トラフィックをアナライザーに送信することです。アナライザーは、両方のファブリックインターコネクットの未設定のイーサネットポートに接続されています。このタスクを実現する構成はどれですか？

- A. ファブリックごとに異なる名前前のトラフィック監視セッションを 2 つ作成します。各 FI にアナライザーを接続し、FI にローカルな監視セッションの宛先とします。
- B. ファブリックごとに 1 つずつ、同じ名前前のトラフィック監視セッションを 2 つ作成します。各 FI 上のアナライザーを、その FI にローカルな監視セッションの宛先として接続します。
- C. ファブリックごとに異なる名前前のトラフィック監視セッションを 2 つ作成します。FI-B に接続されたアナライザーを両方の監視セッションの宛先として接続します。
- D. ファブリックごとに 1 つずつ、同じ名前前のトラフィック監視セッションを 2 つ作成します。FI-A に接続されているアナライザーを両方の監視セッションの宛先として接続します。

正解: [\(正解を表示します\)](#)

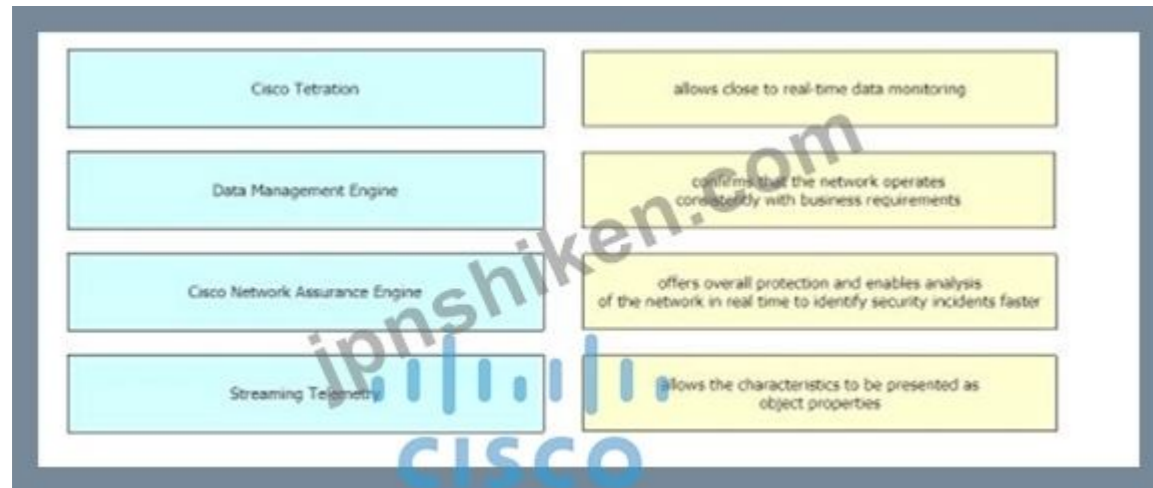
正解はBです。Cisco UCSのトラフィック監視はファブリックローカルであり、監視対象は1つのファブリック相互接続上の単一の物理ポートであるため、1つのセッションで両方のファブリックを同時に監視することはできません。

Ciscoのドキュメントによると、ファブリックフェイルオーバーが有効になっているvNICを、FI障害発生時に可視性を失うことなく監視するには、ファブリックごとに1つずつ、計2つの監視セッションを作成し、2台のアナライザーを接続し、両方のセッションでまったく同じセッション名を使用してvNICをトラフィックソースとして追加する必要があります。

この要件により、オプションCとDは除外されます。なぜなら、どちらも両方のセッションで1つのFI上のアナライザーのみを使用しようとするため、すべてのトラフィックソースと宛先ポートが同じローカルファブリック上に維持されなければならないというルールに違反するからです。オプションAも誤りです。Ciscoは、ファブリックフェイルオーバーを介したvNICトラフィックの中断のない監視を行う際には、両方のセッションに同じ名前を使用するようにと明記しているからです。したがって、通常動作時とファブリックフェイルオーバーイベント時の両方で監視を維持できる唯一の構成は、ファブリックごとに1つずつ、同じ名前前のセッションを2つ作成し、それぞれに独自のローカルアナライザー宛先を設定することです。

質問: 16

左側のネットワーク保証の概念を、右側の対応するメリットにドラッグ&ドロップしてください。



正解:



有効的な350-601問題集はJPNTTest.com提供され、350-601試験に合格することに役に立ちます！JPNTTest.comは今最新350-601試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで350-601問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> 384問、30%ディスカウント、特別な割引コード:

**JPNshiken**」

質問: 17

顧客は、CI/CDモデルを活用して業務を効率化し、コストを最適化するためのツールを必要としている。

顧客は、現在使用しているCisco製品 (Cisco ACIネットワークおよびCisco UCSサーバーを含む)とソリューションを統合したいと考えています。また、オンプレミスのKubernetesとAppDynamicsのパフォーマンス監視機能も提供する必要があります。セキュリティ要件のため、管理対象製品にローカルクライアントをインストールすることはできません。これらの要件を満たすオーケストレーションソリューションはどれでしょうか？

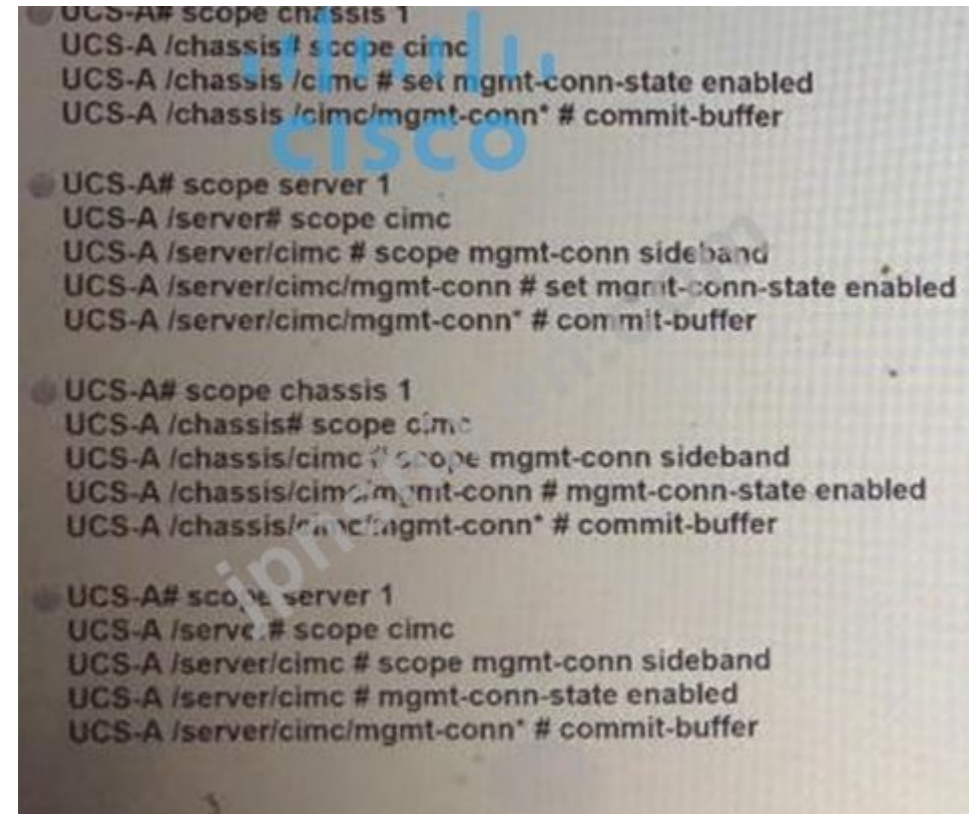
- A. シスコAPIC
- B. CISCO UCSディレクター
- C. Cisco DCNM
- D. Cisco CloudCenter

正解: ([正解を表示します](#))

Cisco CloudCenterは、お客様の要件に最適なオーケストレーションソリューションです。運用効率化とコスト最適化に不可欠なCI/CDモデルをサポートしています。Cisco CloudCenterは、Cisco ACIネットワークおよびCisco UCSサーバーと統合でき、統一された管理プラットフォームを提供します。また、管理対象製品にローカルクライアントをインストールする必要なく、オンプレミスのKubernetesサポートとAppDynamicsパフォーマンス監視を提供し、お客様のセキュリティ要件にも対応します。参考資料：  
Cisco CloudCenterのドキュメントおよびCiscoデータセンターコアテクノロジー学習ガイド。

質問: 18

データセンターにCisco UCS Cシリーズサーバーが設置されています。このサーバーは、管理とデータトラフィックに1本のケーブルを使用し、Cisco UCS Managerによって管理される必要があります。物理接続が確立された後、どの構成を適用する必要がありますか？



- A. オプションA
- B. オプションD
- C. オプションC
- D. オプションB

正解: [D \(コメントを发表する\)](#)

質問: 19

展示資料を参照してください。

```
; Router 1 configuration
interface loopback1
 ip address 10.10.32.121/30
 ip ospf network point-to-point
 ip router ospf 1 area 0.0.0.0
 ip pim sparse-mode

ip pim rp-address 10.10.32.122 group-list 225.0.0.0/8 bi-dir
```

Phantom RPをRP冗長化メカニズムとして使用する双方向PIMネットワークにおいて、2台のCisco NX-OSルータには以下の要件があります。

\* R1はアクティブなRPである必要があります。

\* R2は、R1にアクセスできない場合にのみ使用されるバックアップRPである必要があります。

ルーター2の設定を完了するには、設定手順をドラッグアンドドロップしてください。すべての設定手順を使用する必要はありません。

```
; Router 2 configuration
interface loopback1
 ip address 
 ip ospf network 
 ip router ospf 1 area 0.0.0.0
 ip pim 

ip pim rp-address  group-list 225.0.0.0/8 bi-dir
```

10.10.32.121/32

10.10.32.121

point-to-point

broadcast

10.10.32.121/29

10.10.32.122

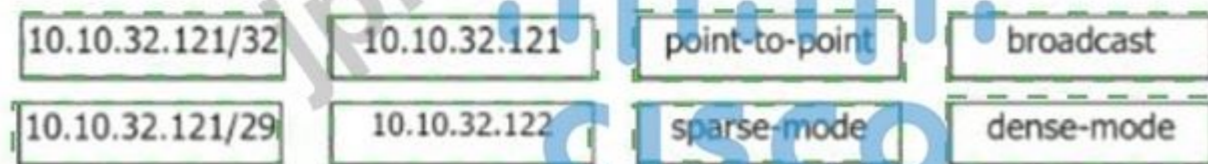
sparse-mode

dense-mode

正解:

```
; Router 2 configuration
interface loopback1
 ip address 10.10.32.121/29
 ip ospf network point-to-point
 ip router ospf 1 area 0.0.0.0
 ip pim sparse-mode

ip pim rp-address 10.10.32.122 group-list 225.0.0.0/8 bi-dir
```



Explanation:

グラフィカルユーザーインターフェース、テキスト、アプリケーションの説明は自動的に生成されます

```
Answer:
ip address 10.10.32.121/29
ip ospf network point-to-point
router ospf 1 area 0.0.0.0
ip pim sparse-mode

ip pim rp-address 10.10.32.122 group-list 225.0.0.0/8 bi-dir
```

質問: 20

展示資料を参照してください。

```
NEXUS# configure terminal
NEXUS# locator-led fex 100
NEXUS(config)# feature fex
NEXUS(config)# fex 100
NEXUS(config-fex)# type N2232TM
NEXUS(config-fex)# serial JAF1427BQLG
NEXUS(config)# interface ethernet 1/24-32
NEXUS(config-if)# switchport
NEXUS(config-if)# switchport mode fex-fabric
NEXUS(config-if)# fex associate 100
NEXUS(config-if)# no shutdown

NEXUS # show fex 100 detail
FEF: 100 Description: FEF0100 state: Online
FEF version: 5.0(2)N1(1) [Switch version: 5.0(2)N1(1)]
FEF Interim version: 5.0(2)N1(0.205)
Switch Interim version: 5.0(2)N1(0.205)
Extender Model: N2K-C2232TM, Extender Serial: JAF1427BQLG
Part No: 73-13373-01
Card Id: 132, Mac Addr: 68:ef:bd:62:2a:42, Num Macs: 64
Module Sw Gen: 21 [Switch Sw Gen: 21]
post level: complete
pinning-mode: static Max-links: 1
Fabric port for control traffic: Eth1/29
Fabric interface state:
Eth1/25 - Interface Up, State: Active
Eth1/26 - Interface Up, State: Active
Eth1/27 - Interface Up, State: Active
Eth1/28 - Interface Up, State: Active
Eth1/29 - Interface Up, State: Active
Eth1/30 - Interface Up, State: Active
Eth1/31 - Interface Up, State: Active
Eth1/32 - Interface Up, State: Active
```

エンジニアは、構成済みの8つのFEXアップリンクすべてを使用するように、すべてのホストポートを分配する必要があります。アップリンクが故障した場合の障害を最小限に抑えるソリューションが必要です。この目的を達成するには、どの操作を実行すればよいでしょうか？

- A. ピン留めの最大リンク数を8に設定します。
- B. 各ホストインターフェイスをファブリックアップリンクに静的に割り当てる
- C. サポート対象のFEXタイプを変更します
- D. ポートチャネルで8つのアップリンクを設定します

正解: [\(正解を表示します\)](#)

説明

アップリンク障害発生時には、トラフィックの中断を最小限に抑える必要があります。ピンニング方式を採用している場合、アップリンク障害が発生すると、障害が発生したリンクに関連するトラフィックは、再ルーティングされるまで中断されます。ポートチャネルを使用すれば、こうした中断を大幅に軽減できます。

質問: 21

Cisco HyperFlex Edgeの2ノード構成において、ウィットネスはどこに配置されますか？

- A. HyperFlex Edge 2ノードクラスタへ
- B. HyperFlex Edgeへのネットワークアクセスを持つ追加サーバーへ
- C. サードパーティのクラウドプロバイダーへ
- D. Cisco Intersightへ

正解: [\(正解を表示します\)](#)

説明

Cisco HyperFlex Edgeのインビジブルクラウド監視機能は、2ノード構成のHX Edge展開の場合にのみ必要です。

その通りです。共有されたドキュメントにあるように、これはクラウド上の目に見えない監視者であるため、Intersightに接続する必要があります。

Cisco HyperFlexEdgeのinvisiblecloud witnessは、2ノード構成のHX Edge展開でのみ必要です。このwitnessには、追加のインフラストラクチャ、セットアップ、構成、バックアップ、パッチ適用、または管理は一切必要ありません。この機能は、2ノード構成のHyperFlexEdgeのインストール時に自動的に構成されます。リモートサイトでは、Intersight (intersight.comまたはIntersight仮想アプライアンス)への接続のために、アウトバウンドアクセスが確立されている必要があります。この接続が確立されていないと、HyperFlexEdge 2ノードクラスタは動作しません。

[https://www.cisco.com/c/en/us/td/docs/hyperconverged\\_systems/HyperFlex\\_HX\\_DataPlatformSoftware/Edge\\_Deployment\\_Guide/b\\_HyperFlex\\_Edge\\_Deployment\\_Guide\\_4\\_0.pdf](https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/Edge_Deployment_Guide/b_HyperFlex_Edge_Deployment_Guide_4_0.pdf)

質問: 22

どの隣接サーバー構成であれば、同じサイトに設置された2台のOTVエッジデバイスがデュアルサイト隣接関係を確立できるでしょうか？

A)

```
Nexus-1:  
  
interface Ethernet1/2  
 ip address 20.1.1.1/24  
  
interface Overlay200  
 otv use-adjacency-server 20.1.1.2 unicast-only  
 otv join-interface Ethernet1/2  
  
Nexus-2:  
  
interface Ethernet1/2  
 ip address 20.1.1.2/24  
  
interface Overlay200  
 otv use-adjacency-server 20.1.1.1 unicast-only  
 otv join-interface Ethernet1/2
```

B)

NEXUS-1:

```
interface Ethernet1/2  
 ip address 20.1.1.1/24
```

```
interface Overlay200  
 otv adjacency-server unicast-only  
 otv join-interface Ethernet1/2
```

Nexus-2:

```
interface Ethernet1/2  
 ip address 20.1.1.2/24
```

```
interface Overlay200  
 otv join-interface Ethernet1/2  
 otv adjacency-server unicast-only  
 otv use-adjacency-server 20.1.1.1 unicast-only
```

C)

Nexus-1:

```
interface Ethernet1/2
 ip address 20.1.1.1/24
```

```
interface Overlay200
 otn adjacency-server unicast-only
 otn join-interface Ethernet1/2
```

Nexus-2:

```
interface Ethernet1/2
 ip address 20.1.1.2/24
```

```
intevrface Overlay200
 otn adjacency-server unicast-only
 otn join-interet1/2
```

D)

Nexus-1:

```
interface Ethernet1/2
 ip address 20.1.1.1/24
```

```
interface Overlay200
 otn adjacency-server unicast-only
 otn join-interface Ethernet1/2
```

Nexus-2:

```
interface Ethernet1/2
 ip address 20.1.1.2/24
```

```
intevrface Overlay200
 otn adjacency-server unicast-only
 otn join-interet1/2
```

A. オプションA

B. オプションC

C. オプションB

D. 選択肢D

正解: ([正解を表示します](#))

質問: 23

展示資料を参照してください。

```
FI-1# scope org /
FI-1 /org # create maint-policy maintenance
FI-1 /org/maint-policy* # set reboot-policy timer-automatic
FI-1 /org/maint-policy* # set soft-shutdown-timer never
```

保守ポリシーを締結する前に、どのような措置を講じる必要がありますか？

- A. スケジュールを選択してメンテナンス時間を指定します。
- B. サービスプロファイルを保守ポリシーに関連付けます。
- C. ソフトシャットダウンタイマーを特定の時間に設定します。
- D. 次回の再起動時に変更を適用するようポリシーを設定します。

正解: **A** ([コメントを发表する](#))

セクション: 計算

説明/参考資料:

質問: 24

Cisco MDS 9000 シリーズ スイッチがポート チャネルを使用する環境において、エンジニアは、特定のフローにおいて送信元と宛先間のフレームが同じリンクを経由するようにする必要があります。後続のフローでは、異なるリンクを使用することが許可されます。この目的を達成するには、どのロード バランシング方式を使用すべきでしょうか？

- A. 送信元ID/宛先ID
- B. src-dst-oui
- C. 送信元送信先ポート
- D. src-id/dst-id/oxid

正解: ([正解を表示します](#))

[https://www.cisco.com/en/US/docs/storage/san\\_switches/mds9000/sw/rel\\_1\\_x/1\\_3/san-os/configuration/guide/PortChnl.pdf](https://www.cisco.com/en/US/docs/storage/san_switches/mds9000/sw/rel_1_x/1_3/san-os/configuration/guide/PortChnl.pdf)

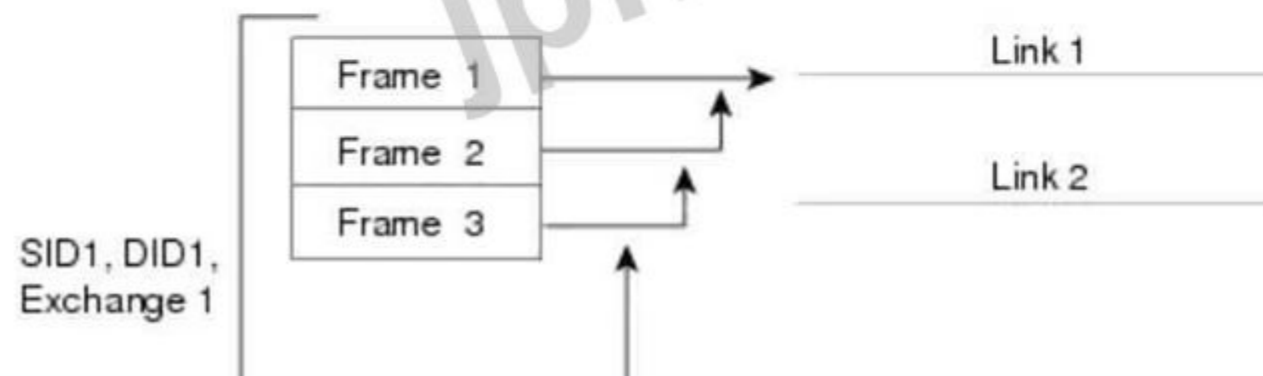
## About Load Balancing

Two mechanisms support the load balancing functionality:

- Flow based—All frames between source and destination follow the same links for a given flow. That is, whichever link is selected for the first exchange of the flow is used for all subsequent exchanges.
- Exchange based—The first frame in an exchange picks a link and subsequent frames in the exchange follow the same link. However, subsequent exchanges can use a different link. This provides more granular load balancing while preserving the order of frames for each exchange.

Figure 16-4 illustrates how source ID 1 (SID1) and destination ID 1 (DID1) based load balancing works. When the first frame in a flow is received on an interface for forwarding, link 1 is selected. Each subsequent frame in that flow is sent over the same link. No frame in SID1 and DID1 utilizes link 2.

Figure 16-4 SID1 and DID1 Based Load Balancing



### 質問: 25

Cisco MDS 9000シリーズスイッチでEPLDアップグレードを実行するプロセスに関する記述のうち、正しいものはどれですか？ 2つ選択してください。）

- A. アップグレードが中断された場合、接続が復旧するとアップグレードが再開されます。
- B. アップグレードはスタンバイ監視モジュールから実行できます。
- C. アクティブスーパーバイザはアップグレード可能です。
- D. モジュールをアップグレードするには、モジュールがオンラインである必要があります。
- E. アップグレード処理は、アップグレード対象のモジュールのみに影響を与えます。

正解: (正解を表示します)

説明

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8\\_x/release\\_notes/epld/epld\\_rn\\_8x.htm](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/release_notes/epld/epld_rn_8x.htm)

## Guidelines and Limitations

When you upgrade or downgrade the EPLDs, observe the following guidelines and limitations:

- You can upgrade each module only when it is online. The EPLD upgrade is only disruptive to the module being upgraded.
- If you interrupt an EPLD upgrade or downgrade, the module must be upgraded again.
- In Cisco MDS 9000 Director Switches, EPLD upgrade or downgrade can only be executed from the active supervisor module. To upgrade the supervisor EPLDs nondisruptively, upgrade the standby supervisor and then switchover. After the new standby supervisor is online its EPLDs can be upgraded.
- In Cisco MDS 9000 Series Fabric Switches, be sure to specify 1 as the module number. The switch must be power cycled for the EPLDs to start running the new code.

### 質問: 26

エンジニアは、Cisco MDS 9000シリーズスイッチをベースとしたSANファブリックのデバイスエイリアスを設定する必要があります。設定は以下の要件を満たす必要があります。

変更がデータベースに反映される前に、エンジニアに確認を求める必要があります。

保留中の変更は、コンソールに明示的に表示する必要があります。

このタスクを実行するコマンドはどれですか？

- A. デバイスエイリアス拡張
- B. デバイスエイリアスコミット
- C. device-alias confirm-commit
- D. device-alias distribute diffs-only

正解: C (コメントを发表する)

Cisco MDS 9000 シリーズ スイッチでは、デバイス エイリアスへの変更がデータベースにコミットされる前に確認されるように、device-alias confirm-commit コマンドが使用されます。このコマンドはユーザーに確認を求め、保留中の変更をコンソールに明示的に表示します。これは、質問で述べられている要件に合致しています。

参考資料 :より詳細な情報については、通常、Cisco Data Center Core Technologiesの学習ガイド、またはMDS 9000シリーズに関するCiscoの公式ドキュメントを参照してください。

### 質問: 27

エンジニアは、災害復旧シナリオにおいてシステムを再構築するために、Cisco UCSでバックアップとリストアを実行する必要があります。バックアップファイルは、パスワードが平文で保存されないように暗号化されている必要があります。これらの要件を満たすバックアップ構成はどれですか？

- A. すべての設定バックアップはSFTP経由で行われます。
- B. TFTPによるフルステートバックアップ
- C. SCPによる論理構成のバックアップ
- D. FTP経由でのシステム構成バックアップ

正解: A (コメントを发表する)

### 質問: 28

展示資料を参照してください。

```
OTV-Site1# show otv
OTV Overlay Information
Site Identifier 0000.0000.0111
Overlay interface Overlay200
VPN name: Overlay200
VPN state: UP
Extended vlans: 178 2500-2563 (Total:65)
Join interface(s): Eth1/2 (20.1.1.1)
Site vlan: 1999 (up)
AED-Capable: Yes
Capability: Unicast-Only
Is Adjacency Server: Yes
Adjacency Server(s): 20.1.1.1/20.2.1.1
```

ネットワークエンジニアがマルチホームOTVネットワークを構築しています。最初のサイトにはプライマリおよびセカンダリ隣接サーバーが設定されています。リモートOTV AEDサイトには、どの設定を追加する必要がありますか？

**A.** インターフェースOverlay200

```
otv join-interface Ethernet1/2
```

拡張VLAN 178、2500～2563を開く

```
otv use-adjacency-server 20.1.1.1 20.2.1.1 unicast-only
```

**B.** インターフェース Overlay200

```
otv join-interface Ethernet1/2
```

otv 拡張VLAN 178、2500-2563

otv 隣接サーバー ユニキャスト専用

**C.** インターフェースOverlay200

```
otv join-interface Ethernet1/2
```

拡張VLAN 178、2500～2563を開く

```
otv use-adjacency-server 20.1.1.1 unicast-only
```

**D.** インターフェース Overlay200

```
otv join-interface Ethernet1/2
```

拡張VLAN 178、2500～2563を開く

正解: ([正解を表示します](#))

質問: 29

PaaSモデルにおいて、ユーザーが管理するコンポーネントはどれですか？

**A.** サーバー

**B.** 仮想化

**C.** ネットワーキング

#### D. アプリケーション

正解: [\(正解を表示します\)](#)

PaaS (Platform as a Service) モデルでは、クラウドプロバイダーがサーバー、仮想化、ネットワーク、ストレージ、ランタイム環境など、基盤となるインフラストラクチャの大部分を管理します。ユーザーはアプリケーションとデータの管理を担当します。

ユーザーはアプリケーションの開発、デプロイ、管理を行い、クラウドプロバイダーはシステムの保守、スケーリング、アップデートを担当します。

- このモデルはインフラストラクチャの複雑さを抽象化することで、開発者がコーディングとアプリケーションロジックに集中できるようにします。

質問: 30

展示資料を参照してください。

```
Nexus# show vpc peer-keepalive | i Keepalive
--Keepalive interval : 1000 msec
--Keepalive timeout : 5 seconds
--Keepalive hold timeout : 3 seconds
--Keepalive vrf : management
--Keepalive udp port : 3200
--Keepalive tos : 192

Nexus# ethanalyzer local interface mgmt limit-captured-frames 1000

Capturing on mgmt0
2019-06-15 12:01:51.242597 192.168.254.11 -> 192.168.254.3 ICMP Echo (ping) request
2019-06-15 12:01:51.242860 192.168.254.3 -> 192.168.254.11 ICMP Echo (ping) reply
2019-06-15 11:50:15.975474 192.168.254.1 -> 192.168.254.3 TCP 47540 > bootps [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2019-06-15 11:50:15.975547 192.168.254.3 -> 192.168.254.1 TCP 29 > 47540 [RST, A CK] Seq=1 Ack=1 Win=0 Len=0
2019-06-15 11:50:15.975564 192.168.254.1 -> 192.168.254.3 TCP 47540 > 44 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2019-06-15 11:50:15.975924 192.168.254.1 -> 192.168.254.3 TCP 47540 > discard [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2019-06-15 11:50:15.976027 192.168.254.1 -> 192.168.254.3 TCP 47540 > 97 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2019-06-15 11:50:15.976381 192.168.254.1 -> 192.168.254.3 TCP 47540 > 35 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2019-06-15 11:50:16.661845 192.168.254.3 -> 192.168.254.4 UDP Source port: 3200 Destination port: 3200
2019-06-15 11:50:16.761147 00:8e:73:a2:41:13 -> 01:80:c2:00:00:00 STP Conf. Root = 8192/10/ec:e1:a9:df:6c:80 Cost = 22 Port = 0x8013
2019-06-15 11:50:16.853248 192.168.254.4 -> 192.168.254.3 UDP Source port: 3200 Destination port: 3200
2019-06-15 11:50:17.326253 192.168.254.1 -> 192.168.254.3 SSH Encrypted request packet len=52
2019-06-15 11:50:17.327313 192.168.254.3 -> 192.168.254.1 SSH Encrypted response packet len=1348
2019-06-15 11:50:17.377246 192.168.254.4 -> 239.255.70.83 UDP Source port: 7546 Destination port: 7546
2019-06-15 11:50:17.552215 192.168.254.1 -> 192.168.254.3 TCP 14139 > ssh [ACK] Seq=365 Ack=11277 Win=63546 Len=0
2019-06-15 11:50:17.661764 192.168.254.3 -> 192.168.254.4 UDP Source port: 3200 Destination port: 3200
2019-06-15 11:50:17.653242 192.168.254.4 -> 192.168.254.3 UDP Source port: 3200 Destination port: 3200
2019-06-15 11:50:17.872637 8c:60:4f:aa:c2:e1 -> 01:80:e7:00:00:0e LLDP Chassis : d = 8c:60:41:aa:c2:e1 Port Id = mgmt0 TTL = 120
2019-06-15 11:50:08.173056 192.168.256.3 -> 192.168.254.2 NTP NTP client
2019-06-15 11:50:08.173256 192.168.256.2 -> 192.168.254.3 NTP NTP server
```

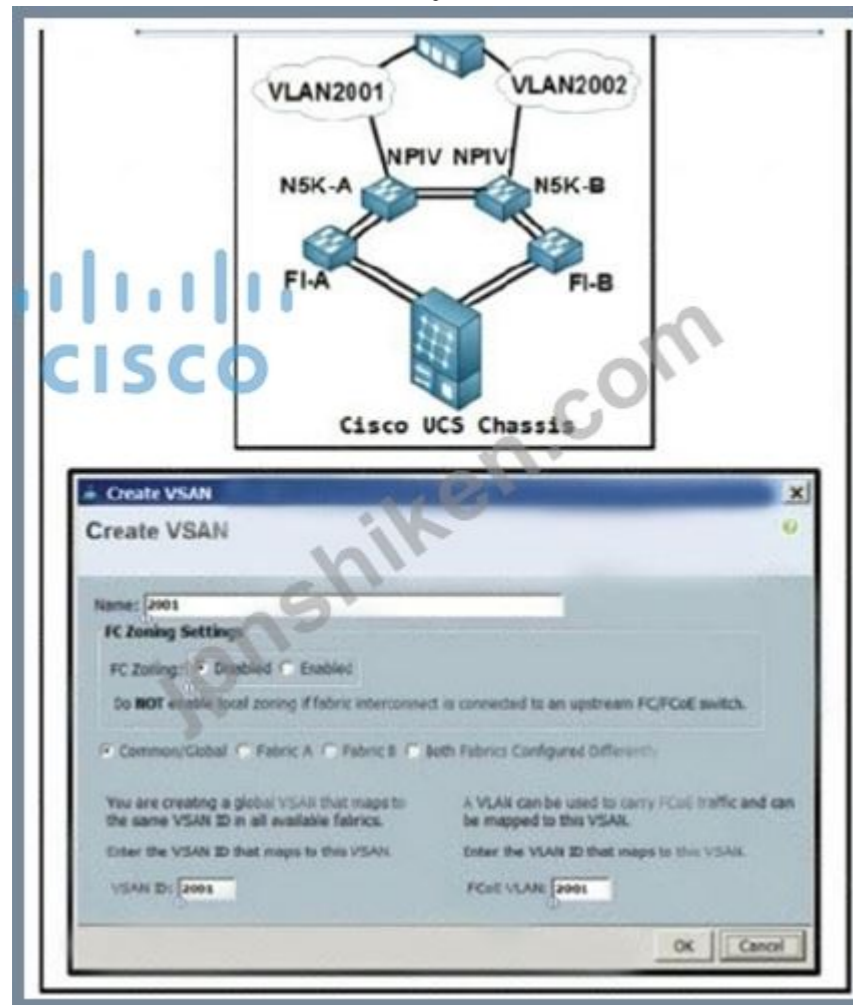
vPCキーブアライブリンクでリンクフラッピングの問題が報告されました。Cisco Nexusスイッチでパケットキャプチャが有効になっています。スイッチから送信されるvPCキーブアライブパケットの宛先IPアドレスは何ですか？

- A. 239.255.70.83
- B. 192.168.254.4
- C. 192.168.254.1
- D. 192.168.254.2

正解: [\(正解を表示します\)](#)

質問: 31

展示資料を参照してください。



エンジニアがネットワーク上でVSANを構成しています。VSANを作成するには、どのオプションを選択する必要がありますか？

- A. 共通／グローバル
- B. FCゾーニング有効
- C. 生地B
- D. 生地A

正解: D (コメントを发表する)

有効的な350-601問題集はJPNTTest.com提供され、350-601試験に合格することに役に立ちます！JPNTTest.comは今最新350-601試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで350-601問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> 384問、30%ディスカウント、特別な割引コード:

**JPNshiken**」

質問: 32

Cisco UCSブレードサーバー上に展開された仮想マシンで、サービス低下が報告されています。vNICからのトラフィックは、UCS-Aスロット2ポート12に接続されたパケットアナライザーまで双方向でSPANする必要があります。

設定を完了するために必要なコマンドはどれですか？ 2つ選択してください。)

- A. UCS-A/eth-1traffic-mon/fabric/eth-mon-session\* # create eth-mon-session/dest-interface 2 12

- B. UCS-A/eth-traffic-mon/fabric/eth-mon-session # アクティベート
- C. UCS-A/org/service-profile/vnic/mon-src\* # 方向を設定 rectiv# 送信
- D. UCS-A/eth-traffic-mon/fabric/eth-mon-session\* # 宛先インターフェースを作成 2 12
- E. UCS-A/org/service-profile/vnic/mon-src\* # 方向を両方設定

正解: ([正解を表示します](#))

#### 質問: 33

FCoE環境において、PAUSEメカニズムを実装するインターフェースは、どの2つのデータセットに対して常に十分なインGRESSバッファをプロビジョニングする必要があるか？ 2つ選択してください)

- A. 高額なクレジットで送られたフレーム
- B. PAUSEフレームが送信機から送信される前に送信機によって処理および送信されたフレーム
- C. リンクで送信されたが、まだ受信されていないフレーム。
- D. リンクで送信され、受信されたフレーム。
- E. PAUSEフレームが送信機から送信された後に、送信機によって処理および送信されたフレーム。

正解: **B,C** ([コメントを发表する](#))

FCoE環境では、PAUSEメカニズムを使用して、イーサネット上のファイバーチャネルトラフィックのロスレス動作を実現します。PAUSEメカニズムにより、受信側は入力バッファが満杯または満杯に近い場合にPAUSEフレームを送信側に送信し、送信側に指定された期間送信を停止するように指示できます。

これにより、受信側でのバッファオーバーフローによるパケット損失を防ぐことができます。しかし、PAUSEメカニズムはレイテンシとジッタも発生させ、FCoEアプリケーションのパフォーマンスに影響を与える可能性があります。そのため、受信側では、次の2つのデータセット12を収容できる十分な入力バッファを用意する必要があります。

\* PAUSEフレームが送信機から送信される前に、送信機によって処理および送信されたフレーム。

これらのフレームは既にネットワーク上に送信されており、PAUSEフレームによって停止させることはできません。受信側に到達し、受信バッファ領域を消費します。

\* リンク上で送信されたものの、まだ受信されていないフレーム。これらのフレームも回線内にあり、PAUSEフレームの後に受信側に到着します。また、受信バッファ領域を消費します。

必要なインGRESSバッファの容量は、リンク速度、リンク距離、およびPAUSE時間によって異なります。受信側は、インGRESSバッファが少なくともリンク距離の2倍のデータを保持でき、さらに安全マージンを確保する必要があります3。たとえば、リンク速度が10Gbps、リンク距離が10km、PAUSE時間が100マイクロ秒の場合、受信側はFCoE仮想レーンごとに少なくとも25MBのインGRESSバッファを用意する必要があります4。

参照:= 1: 長距離 FCoE マルチホップ向け Nexus 7000 F2/F2e インGRESS バッファの変更 - Cisco 2: Cisco Nexus 7000 シリーズ FCoE 設定ガイド 3: FCoE 環境では、PAUSE メカニズムを実装するインターフェースは、どの 2 つのデータセットに対して常に十分なインGRESS バッファをプロビジョニングする必要がありますか？

2つ選択)4 Fibre Channel over Ethernet (FCoE) - Cisco

#### 質問: 34

ファブリックインターコネクタがファイバーチャネルスイッチモードの場合、エンジニアは名前付きVSANを構成する必要があります。VSANは以下の要件を満たす必要があります。

\* 名前付きVSANは「VSAN 10」という名前であればなりません。

\* VSAN IDは10である必要があります。

\* FCoE IDは20である必要があります。

\* VSAN 10はスロット1のポート2に接続する必要があります。

ファブリックインターコネクタがファイバーチャネルスイッチモードの場合、どのコマンドセットでVSANが構成されますか？

```
● UCS-A# scope fc-storage
UCS-A/fc-storage# create vsan VSAN10 10 20
UCS-A /fc-storage/vsan # create member-port fcoe a 1 2
UCS-A /fc-storage/vsan/member-port* # commit-buffer

● UCS-A# scope fc-traffic-mon
UCS-A/fc-storage# create vsan VSAN10 20 10
UCS-A /fc-storage/vsan # create member-port fcoe a 2 1
UCS-A /fc-storage/vsan/member-port* # commit-buffer

● UCS-A# scope eth-storage
UCS-A/fc-storage# create vsan VSAN10 10 20
UCS-A /fc-storage/vsan # create member-port fcoe a 2 1
UCS-A /fc-storage/vsan/member-port* # commit-buffer

● UCS-A# scope fc-uplink
UCS-A/fc-storage# create vsan VSAN10 20 10
UCS-A /fc-storage/vsan # create member-port fcoe a 1 2
UCS-A /fc-storage/vsan/member-port* # commit-buffer
```

- A. オプションC
- B. オプションB
- C. オプションA
- D. オプションD

正解: [\(正解を表示します\)](#)

質問: 35

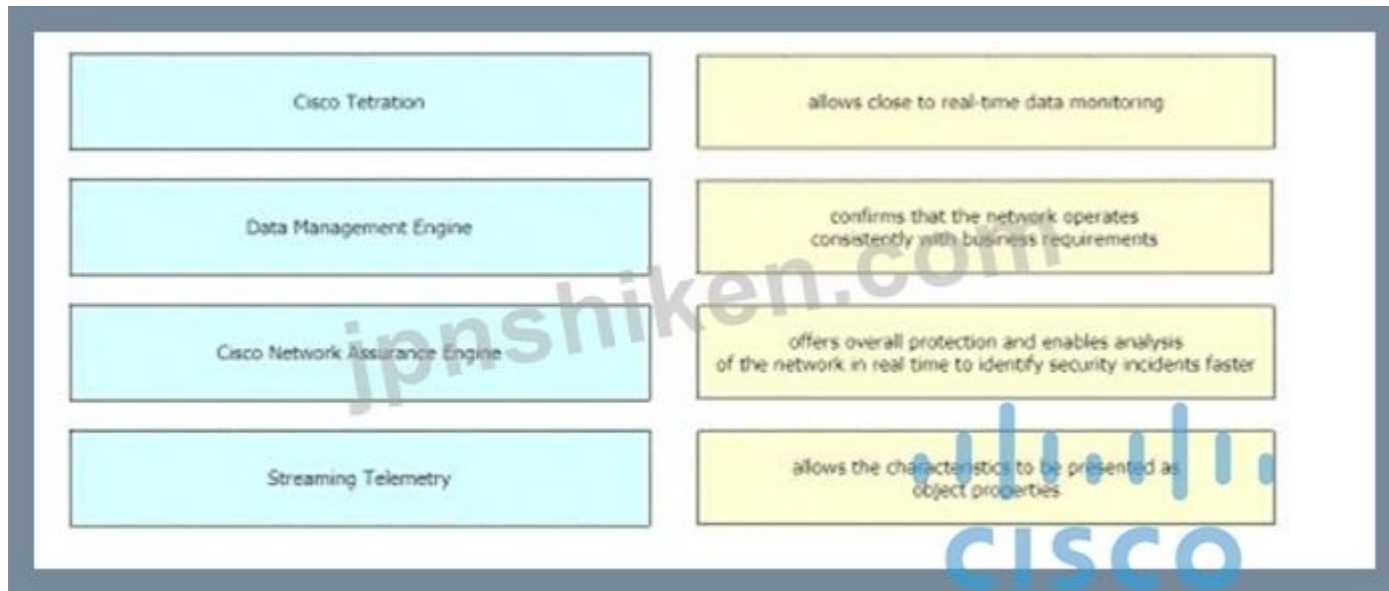
Cisco UCS Managerは、ファームウェアの自動インストールプロセス中にどのような動作を実行しますか？

- A. サードパーティ製ソフトウェアとの互換性を確認します。
- B. ファームウェアをアップグレードし、必要なコンポーネントを再起動します。
- C. 新しいファームウェアバージョンを自動的にダウンロードします。
- D. 管理者にメール通知を送信します。

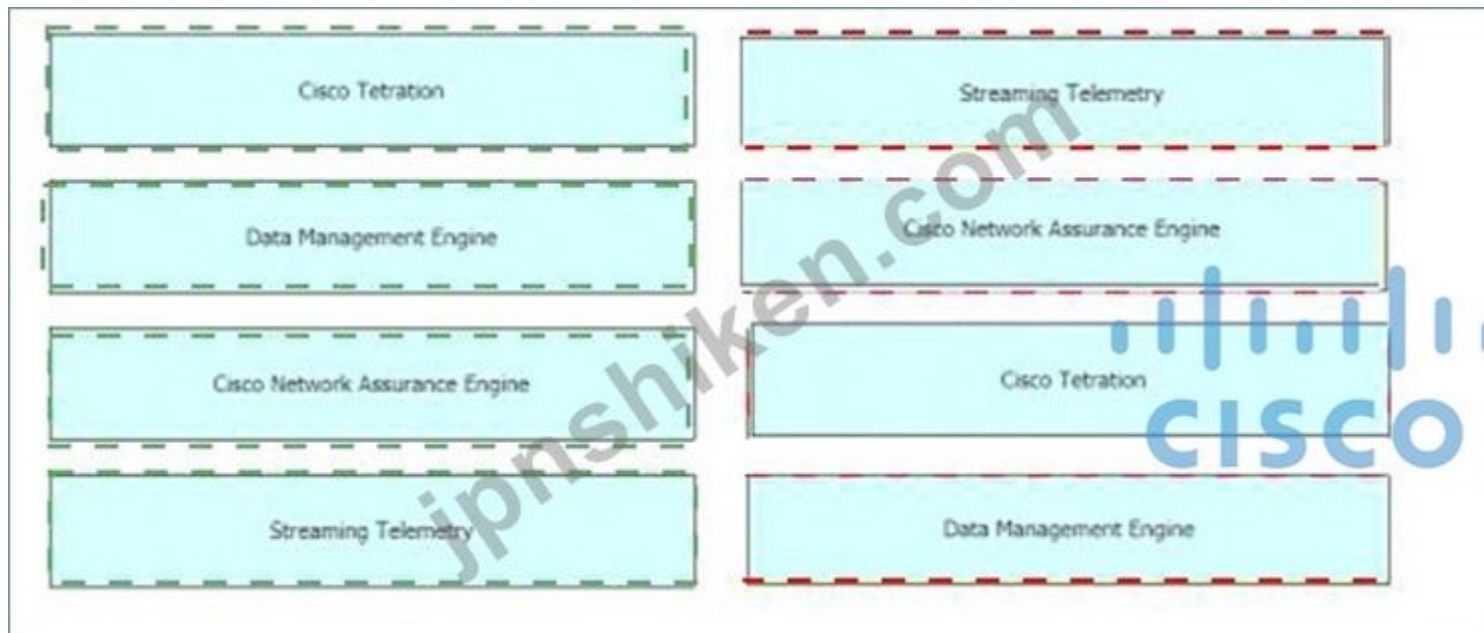
正解: B ([コメントを发表する](#))

質問: 36

左側のネットワーク保証の概念を、右側の対応するメリットにドラッグ&ドロップしてください。

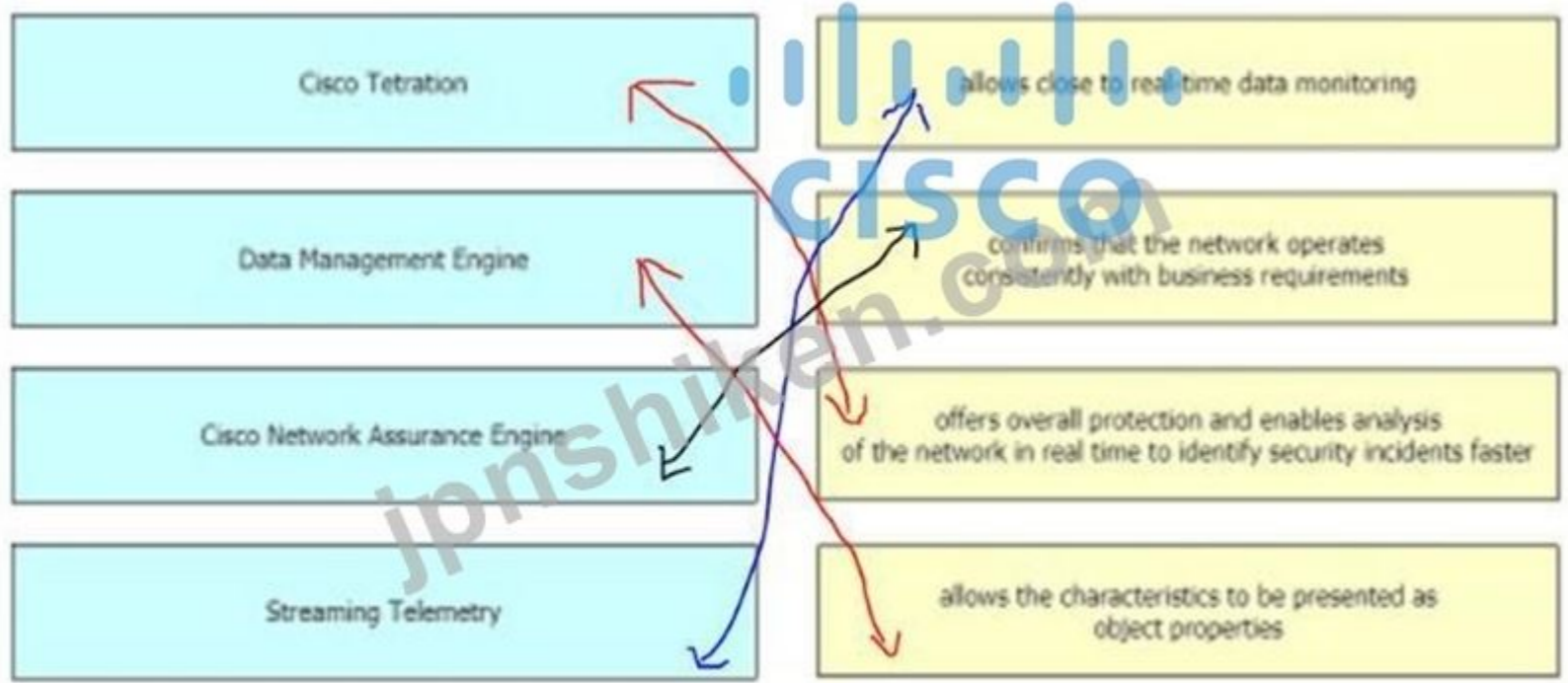


正解:



Explanation:

図の説明は自動的に生成されました



質問: 37

```
{
  "TABLE_asn": {
    "ROW_asn": {
      "asn": "10",
      "TABLE_vrf": {
        "ROW_vrf": {
          "vrf": "default",
          "TABLE_peer": {
            "ROW_peer": {
              "peer_handle": "0",
              "peer_ipaddr": "10.13.0.2",
              "peer_ifname": "Eth1/1",
              "peer_holdtime": "13",
              "peer_srtd": "6",
              "peer_rto": "50",
              "peer_xmitq_count": "0",
              "peer_last_seqno": "4",
              "peer_uptime": "PT46M49S"
            }
          }
        }
      }
    }
  }
}
```

図を参照してください。エンジニアは、Cisco NX-OSゲストシェルでPythonを使用して、インターフェースeth1/1上のEIGRP ASNの設定を取得します。エンジニアは次のスクリプトを作成しました。

```
>>> import json
>>> from cli import *
```

asn]キーの値を取得するには、どのコマンドセットを使用する必要がありますか？

- A. >>> output = json.dumps(cli('show ip eigrp neighbors'))
- >>> 出力['asn']
- B. >>> output = json.dumps(cli('show ip eigrp neighbors'))
- >>> output['TABLE\_asn']['ROW\_asn']['asn']
- C. >>> output = json.loads(cli('show ip eigrp neighbors'))
- >>> output['TABLE\_asn']['ROW\_asn']['asn']

D. >>> output = json.loads(cli('show ip eigrp neighbors'))

>>> 出力['asn']

正解: C (コメントを发表する)

質問: 38

ドラッグアンドドロップ問題

Cisco Nexus 9000シリーズスイッチへのすべてのログインは、IPアドレス192.168.10.10のTACACS+サーバーを経由する必要があります。設定は以下の要件を満たす必要があります。SSHおよびTelnetにはTACACS+サーバーを使用する必要があります。

- TACACS+サーバーキーはCisco123!である必要があります。

接続には管理用VRFを使用する必要があります。

- TACACS+が失敗した場合、デプロイメントはローカル認証情報にフェイルバックする必要があります。

サーバーが30秒以内に応答しません。

右側のコードスニペットを左側のコードの空欄にドラッグ&ドロップして、設定を完了してください。すべてのコードスニペットが使用されるわけではありません。

Answer Area

```
feature tacacs+
username admin password Cisco123!
tacacs-server host 10.10.10.10
aaa group tacacs+ TACACS
  server 192.168.10.10
aaa authentication login default
```

bind-interface vrf-

group tacacs+ local

use-vrf management

key Cisco123! timeout

正解:

Answer Area

```
feature tacacs+
username admin password Cisco123!
tacacs-server host 10.10.10.10
aaa group tacacs+ TACACS
  server 192.168.10.10
  use-vrf management
aaa authentication login default
```

bind-interface vrf-

key Cisco123! timeout

group tacacs+ local

質問: 39

エンジニアは、Cisco Fabric ServicesがCisco Unified Networkに属するVSANの範囲内のメンバーにのみNTP設定を配布することを要求しています。この要件を満たすには、どのスコープ配布を選択する必要がありますか？

A. 論理スコープ

B. 物理的範囲

C. 調整されていない範囲

D. 調整された範囲

正解: (正解を表示します)

Cisco Fabric Services (CFS) は、VSAN の範囲内で構成を配布できる論理スコープ配布モードを提供します。このモードは、構成データベースが VSAN 内でのみ適用される NTP などの機能に適しています。変更が特定の VSAN 内に限定されることで、ネットワーク内の他の VSAN への影響を防ぎます。

参考文献：

\* Ciscoの公式ドキュメント「VSANの構成と管理」1では、VSAN、その利点、およびCFSを使用してVSANを管理する方法について詳細に説明しています。

\* Cisco Fabric Services ガイド2では、論理スコープ配布モードやNTPなどの機能との関連性など、CFSの機能についてさらに詳しく説明しています。

\* NTP 設定に関するコミュニティの議論 3 は、これらの設定を実際のシナリオに適用するための実践的な洞察も提供します。

質問: 40

展示資料を参照してください。

```
1 configure terminal
2 scheduler job name BACKUP_JOB
3 cli copy running-config bootflash:/$ (NAME) .$ (TIMESTAMP) .cfg
4 exit
5 scheduler schedule name BACKUP_SCHEDULE
6 job name BACKUP_JOB
7
8 end
```

Cisco NX-OS スケジューラは毎日午前 3:00 に実行する必要があります。どのコードスニペットがスクリプトを完成させますか？

- A. 毎日午前3時開始
- B. 毎週7日 3:00開始
- C. 毎週7日 3:00
- D. 毎日午前3時

正解: (正解を表示します)

Cisco NX-OSスケジューラが毎日午前3時に実行されるようにするための正しいコードスニペットは `fime daily」`です。

3:00」。このコマンドは、指定されたジョブを毎日指定された時刻に実行するようにスケジューラを設定します。start」キーワードは不要です。これは、毎日繰り返されるタスクの構文では不要です。

参考資料 :この説明は、Cisco NX-OSのスケジューラ機能を使用してタスクをスケジュールする方法に関するガイドラインを提供するCisco NX-OSのドキュメントに基づいています。このドキュメントは、Ciscoデータセンターコアテクノロジーの学習教材の一部です。

質問: 41

エンジニアは、Cisco UCS Manager PowerShell モジュールを利用して Cisco UCS Manager に自動リクエストを送信する PowerShell スクリプトを作成する必要があります。エンジニアは、スイッチを VLAN から自動的に削除する必要があります。環境変数には、VLAN 名とスイッチ識別子を指定する必要があります。VLAN は、スイッチ ポートから削除された後も保持される必要があります。これらの目的を達成するために、エンジニアはスクリプトにどのコマンドを含める必要がありますか？

```
Get-UcsApplianceCloud | Get-UcsVlan -name $VLAN | Get-
UcsVlanMemberPort -SwitchId $SWID -SlotId $SLOT -
PortId $PORT | Remove-UcsVlanMemberPort -Force
```

A.

```
Get-UcsApplianceCloud | Get-UcsVlan -name $VLAN |
Remove-UcsVlanMemberPort -SwitchId B -SlotId 1 -
PortId 15
```

B.

```
Get-UcsApplianceCloud | Remove -UcsVlan -name $VLAN
```

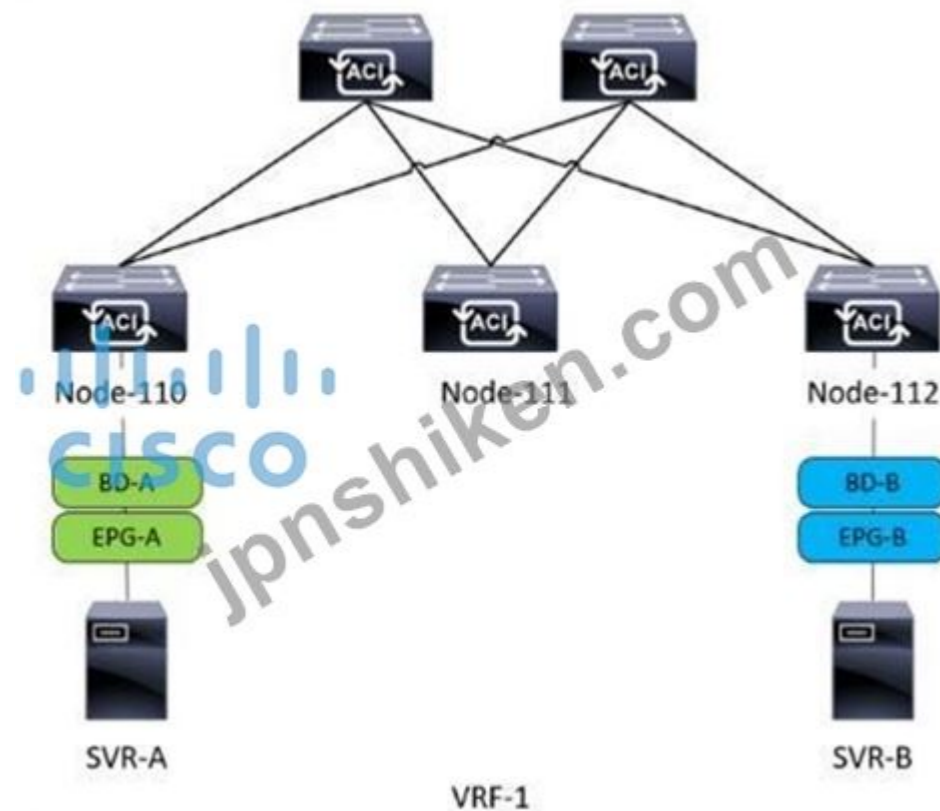
C.

```
Get-UcsApplianceCloud | Remove -UcsVlan -name $VLAN |  
Remove-UcsVlanMemberPort -SwitchId $SWID -SlotId  
$SLOT -PortId $PORT
```

D.

正解: ([正解を表示します](#))

質問: 42



図を参照してください。EPG-A/BD-A の SVR-A が EPG-B/BD-B の SVR-B に到達できません。2 つの EPG 間のトラフィックを分析するために確認すべき 2 つの条件はどれですか？ (2 つ選択してください。)

- A. EPG-AとEPG-Bの間には契約が存在し、トラフィックを許可します。
- B. SVR-Bは、ノード112からEPG-Bのエンドポイントとして学習されます。
- C. EPG-B のブリッジ ドメインが ARP パケットをフラッディングします。
- D. EPG-B のブリッジ ドメインでは、エンドポイント ラーニングの制限が無効になっています。
- E. EPG-AとEPG-Bは優先グループから除外されます。

正解: ([正解を表示します](#))

質問: 43

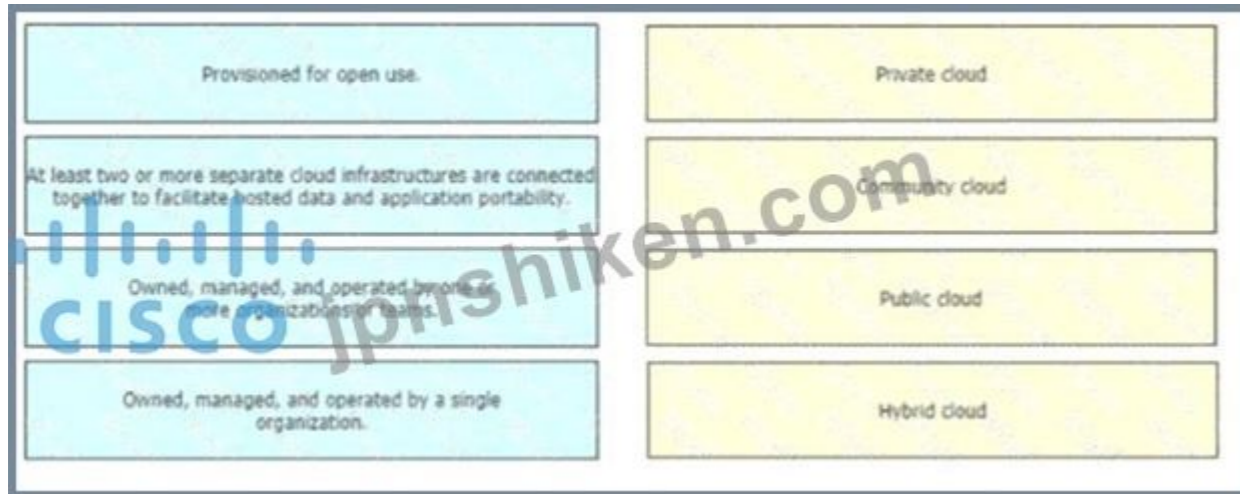
エンジニアは、Cisco UCS Manager からユーザーロールとロケールのバックアップを作成し、その設定を別のファブリックインターコネクに複製する必要があります。エンジニアは、ターゲットのファブリックインターコネクにインポートする前に、ファイルを確認したいと考えています。これらの要件を満たすには、どのバックアップタイプを選択する必要がありますか？

- A. 論理構成
- B. システム構成
- C. 全構成
- D. フルステート

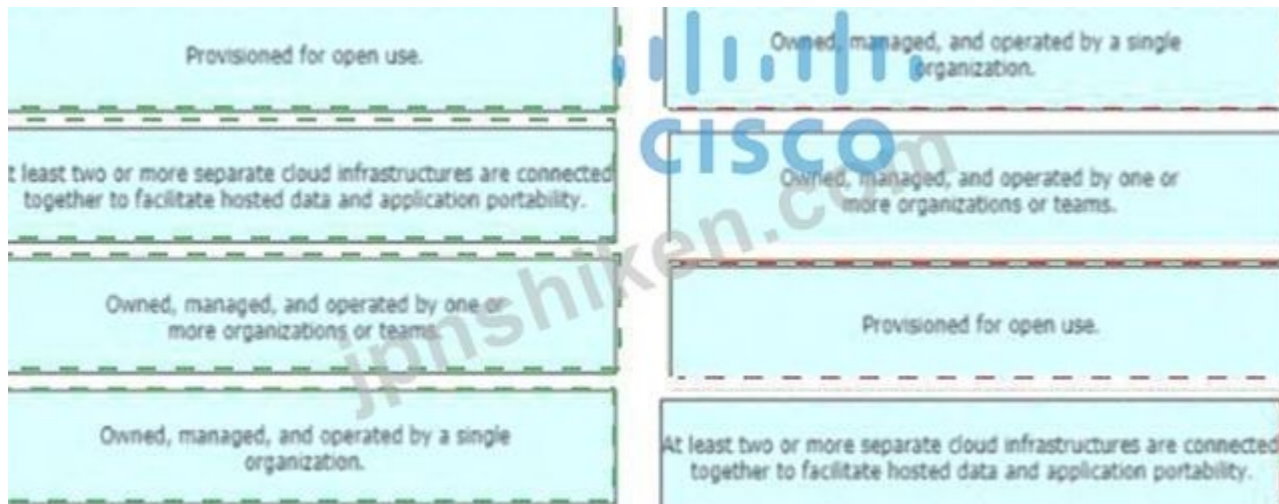
正解: [\(正解を表示します\)](#)

質問: 44

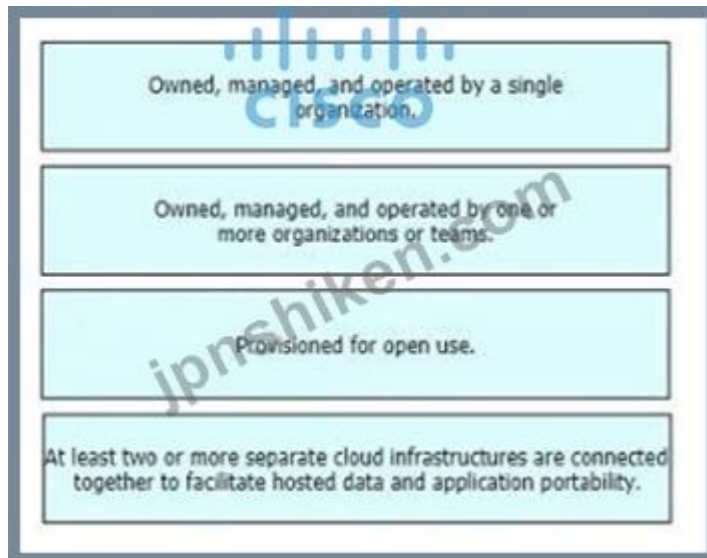
ネットワークエンジニアに、クラウドインフラストラクチャモデルを、その運用とリソースへのアクセスという観点から説明するよう依頼しました。左側の説明を適切な場所にドラッグアンドドロップしてください。



正解:



Explanation:



質問: 45

展示資料を参照してください。

```
Nexus(config)# show checkpoint summary
User Checkpoint Summary
-----
1) BeforeL3:
Created by admin
Created at Mon, 15:25:08 31 Dec 2018
Size is 9,345 bytes
Description: None

System Checkpoint Summary
-----
2) system-fm-vrrp:
Created by admin
Created at Fri, 09:57:02 14 Jun 2019
Size is 20,865 bytes
Description: Created by Feature Manager.

3) system-fm-hsrp_engine:
Created by admin
Created at Fri, 09:57:28 14 Jun 2019
Size is 20,852 bytes
Description: Created by Feature Manager.
```

system-fm-rrrpチェックポイントが作成された理由は何ですか？

- A. VRRPプロセスがクラッシュし、チェックポイントが自動的に作成されました。
- B. VRRP有効化機能が無効になっています。
- C. ネットワーク管理者が手動で作成しました。
- D. VRRPサービスが再起動され、チェックポイントが自動的に作成されました。

正解: ([正解を表示します](#))

質問: 46

NFSプロトコルを使用してファイルシステムへのアクセスを提供するには、どのストレージ機器を導入する必要がありますか？

- A. 光学ドライブストレージ
- B. 直接接続ストレージ
- C. ネットワーク領域ストレージ
- D. ネットワーク接続ストレージ

正解: D ([コメントを発表する](#))

ネットワーク接続ストレージ (NAS)は、NFS (ネットワークファイルシステム)やSMBなどのプロトコルを使用して、ネットワーク経由でファイルレベルのアクセスを提供するように特別に設計されています。これにより、複数のクライアントが共有ファイルに効率的にアクセスできます。

有効的な**350-601**問題集はJPNTTest.com提供され、**350-601**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-601**試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで**350-601**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> **384**問、**30%ディスカウント**、特別な割引コード:

**JPNshiken**」

質問: 47

ネットワークエンジニアは、統合ネットワークアダプタ (CNA)を設定し、仮想ファイバーチャネル7インターフェイスをVSAN 7に関連付ける必要があります。CNAはインターフェイスEth1/7に接続され、VLAN 700がVSNAにマッピングされます。

仮想ファイバーチャネルインターフェイスを作成し、それをイーサネット物理インターフェイスに関連付けるには、どの構成を適用する必要がありますか？

A. 

```
switch(config)# vsan database
switch(config-vsan)# vsan 7 interface vfc 7
```

B. 

```
switch(config)# vlan 700
switch(config-vlan)# fcoe vsan 7
```

C. 

```
switch(config)# interface ethernet 1/7
switch(config-if)# vfc 7 attach vlan 1,700
```

D. 

```
switch(config)# interface vfc 7
switch(config-if)# bind interface ethernet 1/7
```

正解: ([正解を表示します](#))

質問: 48

ネットワークエンジニアが顧客向けにクラウドサービスを導入します。顧客は、基盤となるオペレーティングシステム、データ、およびアプリケーションを完全に制御したいと考えています。この目標を達成するには、どのクラウドサービスモデルを使用する必要がありますか？

- A. サービスとしてのソフトウェア
- B. プラットフォーム・アズ・ア・サービス
- C. ストレージ・アズ・ア・サービス
- D. サービスとしてのインフラストラクチャ

正解: D ([コメントを发表する](#))

IaaS (Infrastructure as a Service)は、オペレーティングシステム、データ、ネットワーク、アプリケーションなど、基盤となるインフラストラクチャを顧客に完全に制御できるサービスです。IaaSを利用することで、顧客は独自のソフトウェアをインストールおよび管理したり、ストレージを構成したり、ネットワークコンポーネントを制御したりする柔軟性を得られます。

質問: 49

```
event manager applet ConfigMgmt
  event cli match "copy run start"
  action 1 syslog priority warnings msg Configuration Modified
```

図を参照してください。エンジニアは、設定が保存されたすべての事象をログに記録します。エンジニアは、イーサネットインターフェイスの設定変更が試みられた場合、追加のログメッセージを生成する必要があります。

1/1。

これらの要件を満たすには、どのコマンドセットを使用する必要がありますか？

- A. 

```
event manager applet ConfigMgmt
  event cli tag eth match "configure terminal ; interface Ethernet1/1"
  event cli tag copy match "copy run start"
  tag eth and copy happens 1 in 2
  action 1 syslog priority warnings msg Configuration Modified
```

- B. 

```
event manager applet ConfigMgmt
  event cli tag eth match "interface Ethernet1/1"
  event cli tag copy match "copy run start"
  event cli tag conf match "configure terminal"
  tag conf or eth or copy happens 2 in 3
  action 1 syslog priority warnings msg Configuration Modified
  action 2 event-default
```

- C. 

```
event manager applet ConfigMgmt
  event cli tag eth match "configure terminal ; interface Ethernet1/1"
  event cli tag copy match "copy run start"
  tag eth or copy happens 1 in 2
  action 1 syslog priority warnings msg Configuration Modified
  action 2 event-default
```

- D. 

```
event manager applet ConfigMgmt
  event cli tag eth match "interface Ethernet1/1"
  event cli tag copy match "copy run start"
  event cli tag conf match "configure terminal"
  tag conf and eth or copy happens 1 in 4294967295
  action 1 syslog priority warnings msg Configuration Modified
```

正解: C ([コメントを发表する](#))

質問: 50

ネットワークエンジニアが、Cisco Nexus 7000 シリーズスイッチのファンモジュールの EPLD アップデートを実行しています。y]を選択して続行した場合、どのような影響がありますか？

```
switch# install all epld bootflash:n7000-epld.6.2.10.img parallel fan-module 1
WARNING!!!: Executing the "install all epld" command
may result in multiple modules going offline and
affect redundant links.

It is strongly recommended to use one of the following
when EPLD upgrade is attempted on a system carrying
production traffic.or Module EPLDs".

1) "install module <mod#> epld"
2) "install all epld <uri> parallel module <mod#>"
where <mod#> is on a single module

For EPLD upgrade best practices, refer to the link-
http://www.cisco.com/.../switches/datacenter/.../guide/epld\_upgrade.html
Do you want to continue (y/n) ? [n] y
Copy complete, now saving to disk (please wait)...

EPLD image signature verification passed

Retrieving EPLD versions... Please wait.

Images will be upgraded according to following table:
Module Type EPLD Running-Version New-Version Upg-Required
-----
1 FAN Fan Controller (1) 0.002 0.006 Yes

1 FAN Fan Controller (1) 0.002 0.006 Yes
1 FAN Fan Controller (2) 0.002 0.006 Yes

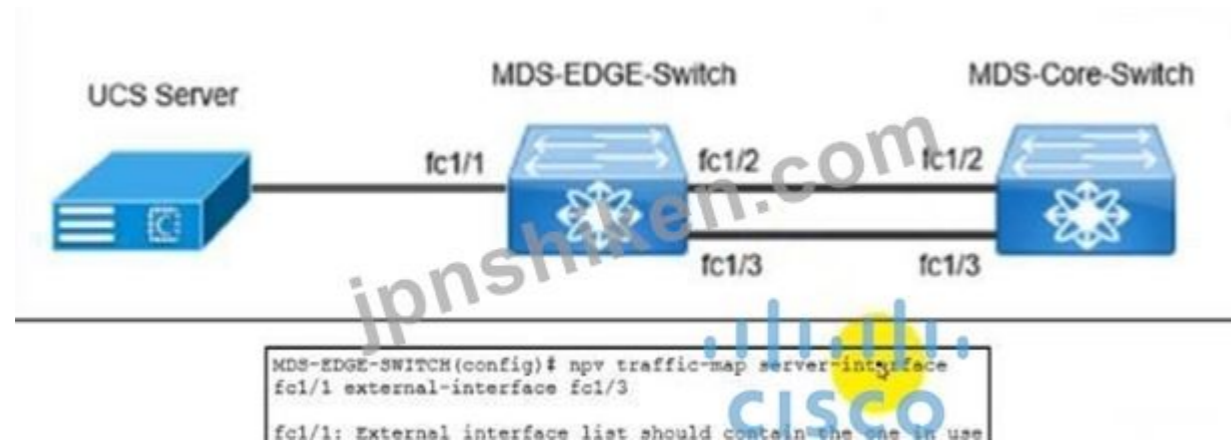
Programming Fan Module
Do you want to continue (y/n) ? [n] y
```

A. このアップデートは中断を伴わないため、完了しました。アップグレード後に電源の再投入は必要ありません。

- B. ファンモジュールがコードの実行を開始するためにスイッチの電源がオン/オフされ、自動的に再ロードされます。
- C. ファンモジュールが新しいコードとプロンプトの実行を開始するには、スイッチの電源を再投入してから、各モジュールが再ロードされます。
- D. アップデートが正常に完了しなかったため、スイッチの電源を入れ直す必要があります。

正解: **A** ([コメントを发表する](#))

質問: 51



図を参照してください。MDS-EDGE-SwitchとMDS-Core-SwitchはNPVおよびNPIV機能で構成されています。Cisco UCSからのFLOGIは、インターフェースfc1/2でMDS-Core-Switchによって受信されます。エンジニアは、MDS-EDGE-SwitchとMOS-Core-Switch間のすべてのトラフィックをインターフェースfc1/2からfc1/3に移動しようとしたが、失敗しました。どの操作で構成が完了しますか？

- Disable the NPV feature in the MDS-EDGE-Switch.  
Re-enable the NPV feature.  
Disable interface fc1/1.
- Disable the NPIV feature in the MDS-EDGE-Switch.  
Re-enable the NPIV feature.  
Disable interface fc1/3.
- Shut down fc1/1 in the MDS-EDGE-Switch.  
Re-apply the command.  
Enable interface fc1/1.
- Shutdown fc1/3 in the MDS-EDGE-Switch.  
Re-apply the command.  
Enable interface fc1/3.

- A. オプションB
- B. オプションA
- C. 選択肢D
- D. オプションC

正解: ([正解を表示します](#))

質問: 52

Cisco UCS のユーザー Employee1Jが、Cisco UCS Manager のルートレベルで、Cisco UCS サーバーのブート ポリシーを誤って変更してしまいました。この変更はすべてのサービス プロファイルに影響を与え、ストレージ接続が失われました。システム管理者は、今後この問題が再発しないようにしたいと考えています。新しいセキュリティ ポリシーでは、アクセスを組織レベルまで制限し、他のユーザーがルート ポリシーを変更できないようにすることが義務付けられています。これらの要件を満たすには、どのような対策を講じる必要がありますか？

- A. ユーザーに割り当てられた権限レベルを変更する
- B. カスタムユーザーロールを定義し、ユーザーに割り当てます。
- C. ユーザー Employee1Jにネットワークオペレーターの役割を割り当てます。
- D. ユーザーを特定のCisco UCSロケールに割り当てる

正解: ([正解を表示します](#))

# Locales

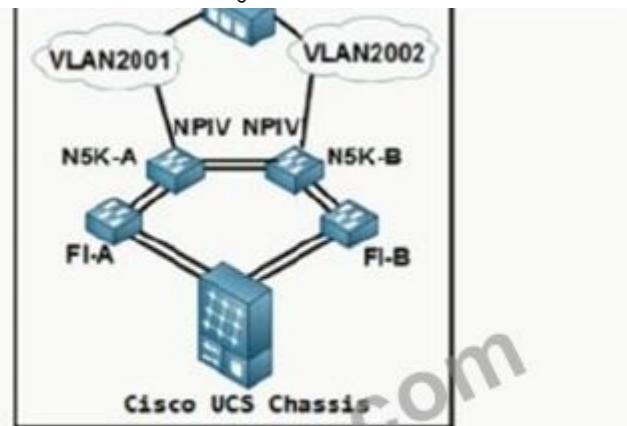
## User Locales

You can assign a user to one or more locales. Each locale defines one or more organizations (domains) to which a user can access. **Access is usually limited to the organizations specified in the locale.** An exception is a locale without any organizations. It provides unrestricted access to system resources in all organizations.

A Cisco UCS domain can contain up to 48 user locales. Any user locales configured after the first 48 are accepted, but are inactive with faults raised.

質問: 53

展示資料を参照してください。



エンジニアがネットワーク上でVSANを構成しています。VSANを作成するには、どのオプションを選択する必要がありますか？

A. 生地B

- B. FCゾーニング有効
- C. 共通/グローバル
- D. 生地A

正解: ([正解を表示します](#))

質問: 54

Cisco HyperFlexハードウェアアクセラレーションカードをHyperFlex環境に追加するメリットは何ですか？

- A. オフライン暗号化アクセラレーション
- B. ネットワークスループットの向上
- C. GPUアクセラレーション
- D. 圧縮効率の向上

正解: ([正解を表示します](#))

説明

• Additional information on HyperFlex Hardware Acceleration Cards

## Overview of HyperFlex Hardware Acceleration Cards

This chapter provides details for installation, post-installation, and troubleshooting of HyperFlex Hardware Acceleration Cards (PID: HX-PCIE-OFFLOAD-1) on HyperFlex nodes and for configuring your initial cluster. **These cards provide improved performance and compression efficiency for most storage workloads.**

**Note** An HXDP-P Enterprise license is required for installing and configuring HyperFlex Hardware Acceleration Cards.

[https://www.cisco.com/c/en/us/td/docs/hyperconverged\\_systems/HyperFlex\\_HX\\_DataPlatformSoftware/Installation\\_VMware\\_ESXi/3\\_5/b\\_HyperFlexSystems\\_Installation\\_Guide\\_for\\_VMware\\_ESXi\\_3\\_5/b\\_HyperFlexSystems\\_Installation\\_Guide\\_for\\_VMware\\_ESXi\\_3\\_5\\_chapter\\_01100.html#:~:text=Overview%](https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/Installation_VMware_ESXi/3_5/b_HyperFlexSystems_Installation_Guide_for_VMware_ESXi_3_5/b_HyperFlexSystems_Installation_Guide_for_VMware_ESXi_3_5_chapter_01100.html#:~:text=Overview%20枚のHyperFlexハードウェアアクセラレーションカード)

20枚のHyperFlexハードウェアアクセラレーションカード - この章では、これらのカードについて説明します。

20枚のカードは、ほとんどの用途でパフォーマンスと圧縮効率を向上させます。

ストレージワークロード。

質問: 55

エンジニアがCisco Bashシェル内でPythonスクリプトを実行する。このスクリプトにはこの辞書オブジェクトが含まれている。

```
switch_id_list = {  
    "N9K-Spine-1": "842534699747",  
    "N9K-Leaf-1": "126784690",  
    "N9K-Leaf-2": "56556473"  
}
```

要素をswitch\_idリストに追加するには、どのコマンドを使用する必要がありますか？

辞書？

```
switch_id_list=["N9K-Spine-2": "1498323434"]
switch_id_list.update({"N9K-Spine-2": "1498323434"})
switch_id_list.append({"N9K-Spine-2": "1498323434"})
switch_id_list += {"N9K-Spine-2": "1498323434"}
```

- A. オプションB
- B. 選択肢D
- C. オプションC
- D. オプションA

正解: [\(正解を表示します\)](#)

質問: 56

エンジニアは、バックアップ目的で Cisco UCS Manager の設定をエクスポートする必要があります。要件は、AAA および RBAC 設定を含む設定をエクスポートすることです。また、ファイルは人間が読みやすい形式で保存する必要があります。これらの要件を満たすには、どのようなバックアップタイプを選択する必要がありますか？

- A. 楽しい状態
- B. 全構成
- C. 論理構成
- D. システム構成

正解: [\(正解を表示します\)](#)

質問: 57

エンジニアは、UCS-A という名前のプライマリファブリックと、UCS-B という名前のセカンダリファブリックを持っています。kr2016 という名前のキーリングに対して、サブジェクト名が sjc2016 の証明書要求を作成する必要があります。クラスタの IP アドレスは 10.68.68.68 です。

この証明書要求を作成するコマンドセットは何ですか？

- A. UCS-A # スコープキーリング kr2016  
UCS-A /keyring # create certreq 10.68.68.68 sjc2016  
UCS-A /keyring\* # コミットバッファ
- B. UCS-B # スコープキーリング kr2016  
UCS-B /keyring # create certreq ip 10.68.68.68 subject-name sjc2016  
UCS-B /keyring\* # commit-both
- C. UCS-B#スコープセキュリティ  
UCS-B /セキュリティ # スコープキーリング kr2016  
UCS-B /security/keyring # set certreq 10.68.68.68 sjc2016  
UCS-B /security/keyring\* # commit-both
- D. UCS-A#スコープセキュリティ  
UCS-A /セキュリティ # スコープキーリング kr2016  
UCS-A /security/keyring # create certreq ip 10.68.68.68 subject-name sjc2016 UCS-A /security/keyring\* # commit-buffer

正解: [\(正解を表示します\)](#)

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/ucs-manager/CLI-User-Guides/Admin-Management/4-0/b\\_Cisco\\_UCS\\_Manager\\_CLI\\_Administration\\_Mgmt\\_Guide\\_4-0/b\\_Cisco\\_UCS\\_Manager\\_CLI\\_Administration\\_Mgmt\\_Guide\\_4-0\\_chapter\\_0110.html](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/CLI-User-Guides/Admin-Management/4-0/b_Cisco_UCS_Manager_CLI_Administration_Mgmt_Guide_4-0/b_Cisco_UCS_Manager_CLI_Administration_Mgmt_Guide_4-0_chapter_0110.html)

質問: 58

HSRPバージョン2グループ10のデフォルト仮想MACアドレスはどれですか？

- A. 0000.5E00.0110
- B. 0000.0C9F.F00A
- C. 3716.1350.1C0A
- D. 0000.0C9F.F010

正解: (正解を表示します)

HSRPバージョン2グループ10のデフォルトの仮想MACアドレスは0000.0C9F.F00Aです。HSRP (Hot Standby Router Protocol)は、複数のルータが仮想IPアドレスとMACアドレスを共有できるようにすることで、IPネットワークの冗長性と負荷分散を提供するプロトコルです。HSRPバージョン2は最大4096グループをサポートし、HSRPバージョン1とは異なるMACアドレス形式を使用します。HSRPバージョン2のMACアドレス形式は0000.0C9F.FXXXで、XXXはグループ番号の16進数値です。グループ10の場合、16進数値は0Aなので、MACアドレスは0000.0C9F.F00Aになります。参照:

\* Ciscoデータセンターコアテクノロジーの実装と運用 (DCCOR)v1.2、モジュール3 :データセンターLANネットワーク接続、レッスン3.6 :Cisco Nexus 5000シリーズスイッチ

\* Cisco Nexus 5000 シリーズ NX-OS ユニキャストルーティング設定ガイド、リリース 5.2(1)N1(1)、章:

HSRP の設定、セクション: HSRP バージョン 2 エッジ ブラウザ ユーザーは、メタデータが次の Microsoft Edge ブラウザ ウィンドウでページを開いています。



質問: 59

ネットワークアーキテクトは、ネットワークの初期サポートと将来のサーバーインフラストラクチャのサポートを両立させる自動化ソリューションを設計する必要があります。構成の一貫性を維持するため、ネットワークチームは、ネットワークの望ましい状態を強制し、手動による構成変更を元に戻すソリューションを必要としています。これらの目標を満たすソリューションはどれでしょうか？

- A. NX-API
- B. アンシブル
- C. テラフォーム
- D. 人形

正解: (正解を表示します)

Terraformは、インフラストラクチャ・アズ・コード (IaC) ツールであり、ユーザーはクラウドとオンプレミスの両方のリソースを、バージョン管理、再利用、共有が可能な人間が読みやすい構成ファイルで定義できます。Ciscoデータセンターコアテクノロジーのコンテキストでは、Terraformを使用して、必要に応じて構成を自動的に管理、更新、および元に戻すことで、ネットワークの望ましい状態を維持し、一貫性を保つことができます。幅広いCisco製品をサポートしており、将来的にはサーバーインフラストラクチャの管理にも拡張可能です。

参考文献 :Ciscoデータセンターコアテクノロジーの実装と運用 (DCCOR)コースでは、データセンターにおける自動化とセキュリティの基本について解説しており、望ましい状態構成を強制するためのTerraformなどのIaCツールの使用法についても説明しています1。さらに、Ciscoデータセンターソリューションの自動化の実装 (DCAUI)コースでは、CiscoデータセンターにおけるTerraformを含む自動化ソリューションの実装についてさらに詳しく解説しています2。

質問: 60

企業はCisco UCS Cシリーズサーバーのセキュリティを強化する必要があります。セキュリティポリシーでは、すべてのアウトオブバンド管理がこれらの要件を満たすことが求められています。

- \* すべての通信を暗号化する必要があります
- \* デフォルト以外のポートを使用する必要があります
- \* プライベートな管理セッションを提供する必要があります

どのCisco IMC構成が要件を満たしていますか？

```
data1# scope sol
data1 /sol # set enable @ yes
data1 /sol # set encrypted tls1.2
data1 /sol # set port 3389
data1 /sol # set session max 2
data1 /sol # set deny-local yes

data1# scope cimc
data1 /cimc # set enabled yes
data1 /cimc # set encrypted tls
data1 /cimc # set kvm-port 1972
data1 /cimc # set max-sessions 1
data1 /cimc # set local-session deny

data1# scope oob
data1 /oob # set enabled no
data1 /oob # set encrypted yes
data1 /oob # set kvm-port 2068
data1 /oob # set max-sessions 1
data1 /oob # set local-access no

data1# scope kvm
data1 /kvm # set enabled yes
data1 /kvm # set encrypted yes
data1 /kvm # set kvm-port 3168
data1 /kvm # set max-sessions 1
data1 /kvm # set local-video no
```

- A. オプションA
- B. オプションD
- C. オプションC
- D. オプションB

正解: B ([コメントを发表する](#))

質問: 61

展示資料を参照してください。

```
<?xml version="1.0" encoding="UTF-8"?><imdata totalCount="1"><error code="403" text="Token was invalid (Error: Token timeout)"/></imdata>
```

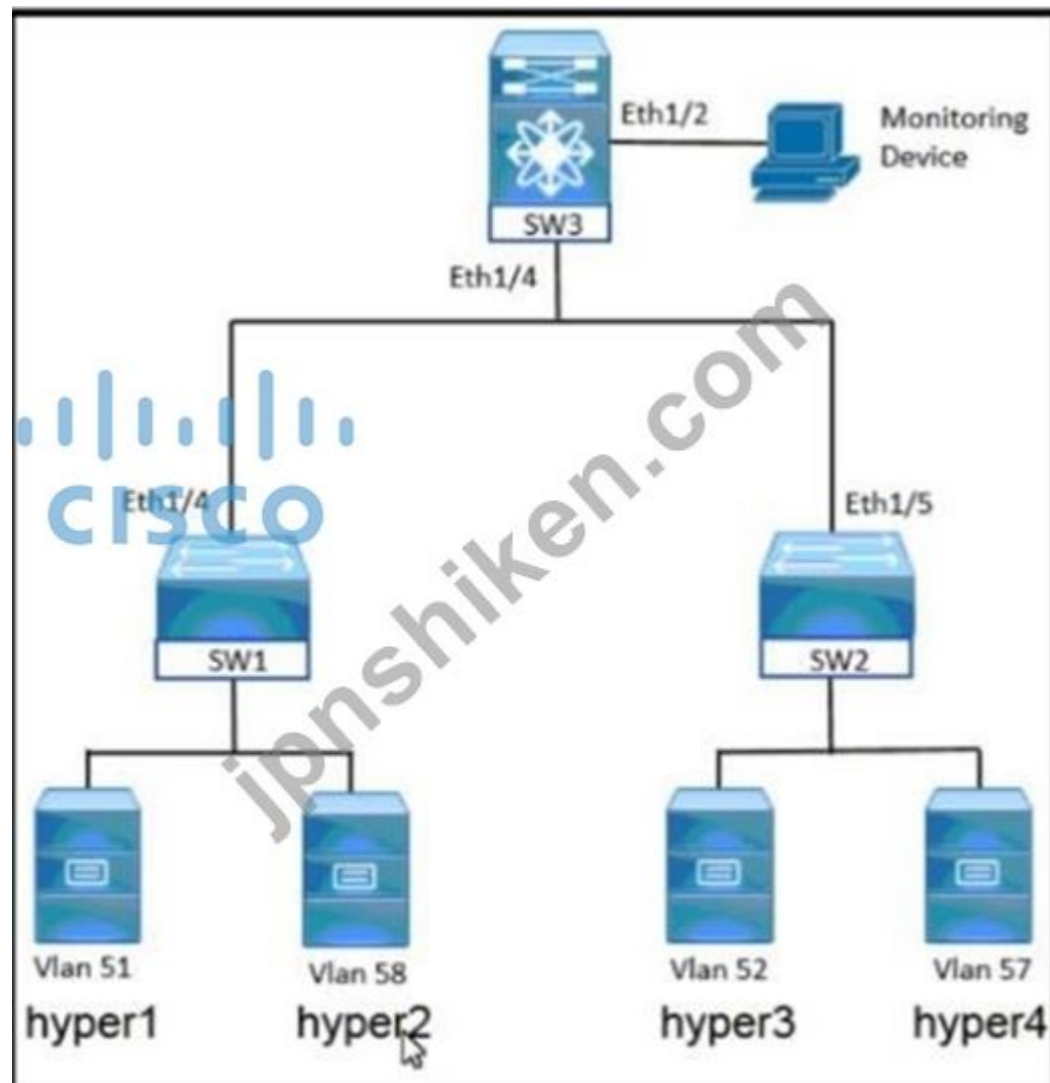
エンジニアがREST APIを使用して新しいアプリケーションプロファイルを構成した際に、このエラーメッセージを受け取りました。アプリケーションプロファイルを構成する前に使用できるメソッドはどれですか？

- A. aaaLogoutへPOST
- B. aaaRefresh に POST します
- C. aaaLoginにPOST
- D. aaaListDomainsへのGETリクエスト

正解: ([正解を表示します](#))

有効的な**350-601**問題集はJPNTTest.com提供され、**350-601**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-601**試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで**350-601**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> **384**問、**30%ディスカウント**、特別な割引コード：**JPNshiken**」

質問: 62



図を参照してください。エンジニアは、Hyper4 デバイスのイーサネットポートと対応する VLAN トラフィックを監視する必要があります。SW3 デバイスは Cisco Nexus 7000 シリーズ スイッチです。右側のコードスニペットを構成のボックスにドラッグアンドドロップして、これらの要件を満たしてください。

```
!SW3 configuration

interface ethernet 1/2
  switchport 

monitor session 2
  source interface 
  destination interface 
  source 
```

- 
- 
- 
- 
- 

正解:

```
!SW3 configuration

interface ethernet 1/2
  switchport 

monitor session 2
  source interface 
  destination interface 
  source 
```

- 
- 
- 
- 
- 

Explanation:

グラフィカルユーザーインターフェースの説明は自動生成されました

```
!SW3 configuration

interface ethernet 1/2
  switchport 

monitor session 2
  source interface 
  destination interface 
  source 
```

- 
- 
- 
- 
- 

質問: 63

どの隣接サーバー構成であれば、同じサイトに配置された2台のOTVエッジデバイスがデュアルサイト隣接関係を確立できるでしょうか？

```
interface Ethernet1/2
ip address 20.1.1.1/24

interface Overlay200
otv use-adjacency-server 20.1.1.2 unicast-only
otv join-interface Ethernet1/2
```

Nexus-2:

```
interface Ethernet1/2
ip address 20.1.1.2/24

interface Overlay200
otv use-adjacency-server 20.1.1.1 unicast-only
```

A. otv join-interface Ethernet1/2

Nexus-1:

```
interface Ethernet1/2  
ip address 20.1.1.1/24
```

```
interface Overlay200  
otv adjacency-server unicast-only  
otv join-interface Ethernet1/2
```

Nexus-2:

```
interface Ethernet1/2  
ip address 20.1.1.2/24
```

```
interface Overlay200  
otv join-interface Ethernet1/2  
otv adjacency-server unicast-only  
otv use-adjacency-server 20.1.1.1 unicast-only
```

B.

Nexus-1:

```
interface Ethernet1/2  
ip address 20.1.1.1/24
```

```
interface Overlay200  
otv adjacency-server unicast-only  
otv join-interface Ethernet1/2
```

Nexus-2:

```
interface Ethernet1/2  
ip address 20.1.1.2/24
```

```
interface Overlay200  
otv adjacency-server unicast-only  
otv join-interface Ethernet1/2
```

C.

```

Nexus-1:

interface Ethernet1/2
 ip address 20.1.1.1/24

interface Overlay200
 oty use-adjacency-server 20.1.1.1 unicast-only
 oty adjacency-server unicast-only
 oty join-interface Ethernet1/2

Nexus-2:

interface Ethernet1/2
 ip address 20.1.1.2/24

interface Overlay200
 oty use-adjacency-server 20.1.1.2 unicast-only
 oty adjacency-server unicast-only
 oty join-interface Ethernet1/2

```

D.

正解: **B** ([コメントを发表する](#))

セクション: ネットワーク

質問: 64

図を参照してください。エンジニアは、Cisco MDS 9000 シリーズ スイッチの sangroup ロールに割り当てられたユーザーが VSAN 15 ~ 20 に対してコマンドを発行できないように制限する必要があります。この目的を達成するために、エンジニアはどのコマンドを実行する必要がありますか？

```

1 Role: sangroup
2 Description: SAN management group
3 vsan policy: deny
4 Permitted vsans: 10-30
5
6 -----
7 Rule      Type  Command-type  Feature
8 -----
9 1. permit  config          *
10 2. deny   config          fspf
11 3. permit  debug          zone
12 4. permit  exec           fcping

```

A. 許可証 vsan 15-20

B. vsan ポリシー拒否なし

C. vsan ポリシー拒否 vsan 15-20

D. 許可なし vsan 15-20

正解: ([正解を表示します](#))

次の例では、vsan 15 からこのロールがコマンドを実行する権限を削除します。

20.

```
switch(config-role-vsan)# no permit vsan 15-20
```

質問: 65

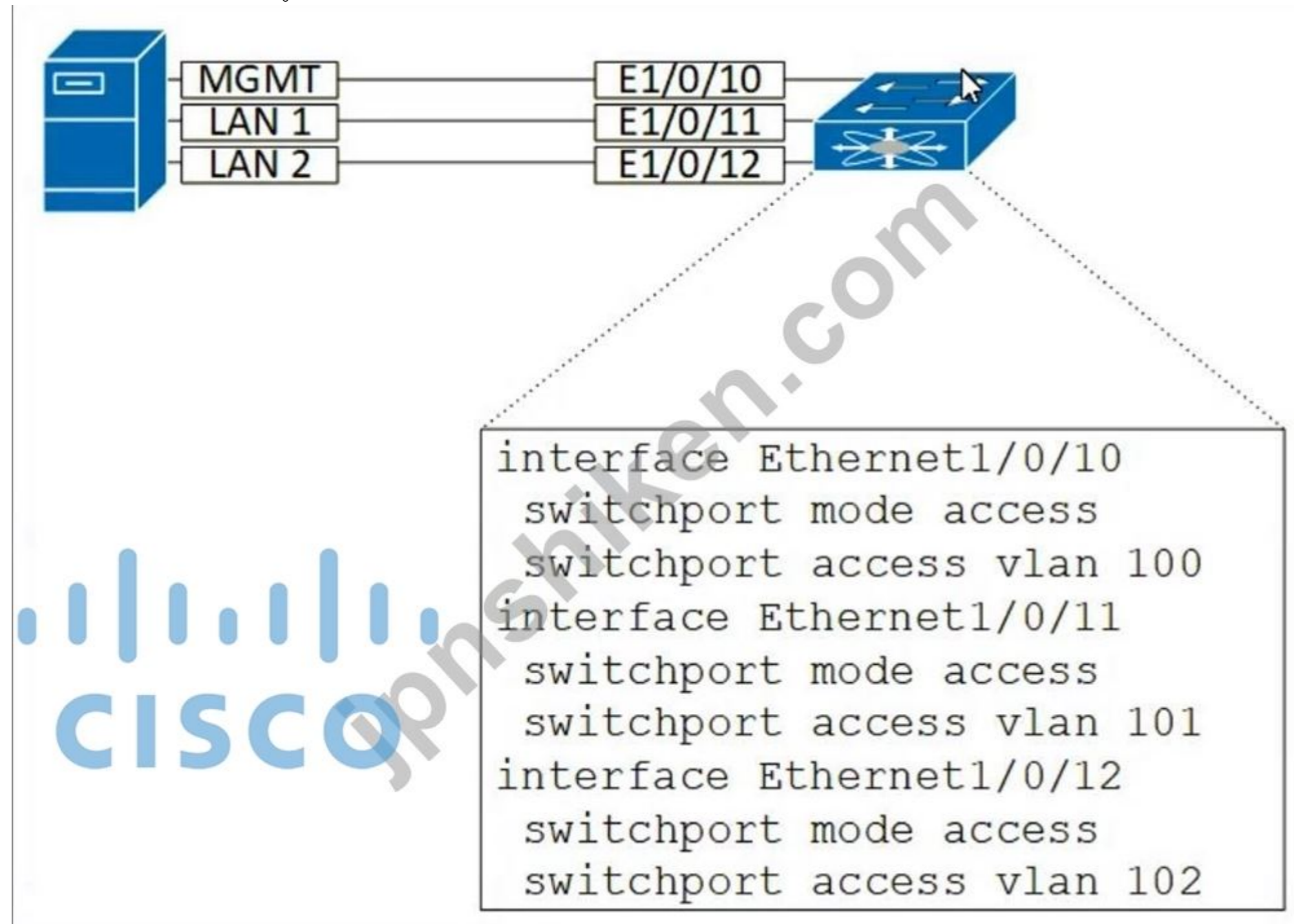
図を参照してください。生成された実行設定ファイルが fusion-config\_ という名前で、現在の日付を持つようにするには、file キーワードで始まる行にどのコマンドを追加する必要がありますか？

- A. ('fusion-config\_ + date')
- B. (\*fusion-config) + 日付
- C. str.(fusion-config) + date
- D. string(('fusion-config\_') + date)

正解: B ([コメントを发表する](#))

質問: 66

展示資料を参照してください。



エンジニアは、リモートの場所から Cisco UCS C-Series サーバーの KVM にアクセスする必要があります。エンジニアは、アウトオブバンドインターフェイスを使用して KYM にアクセスする必要があります。これらの要件を満たす構成セットはどれですか？

A. NICモード: 共有LOM -

VLAN ID: 100

B. NICモード: 専用 -

VLAN ID: 101

C. NICモード: 専用 -

VLANの状態: 無効

D. NICモード: 共有LOM -

VLANの状態: 無効

正解: **C** ([コメントを发表する](#))

専用回線 CIMCへの接続は、管理用イーサネットポートを介して可能です。

CIMCへのLOM-A共有接続は、LAN On Motherboard (LOM) イーサネットポート経由でのみ利用可能です。

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/c/sw/gui/config/guide/1-1-1/b\\_Cisco\\_UCS\\_C-Ser](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/1-1-1/b_Cisco_UCS_C-Ser)

質問: 67

展示資料を参照してください。

エンジニアは、Cisco Nexusシリーズスイッチのfc1/9ポートに接続されたデバイスに対して、TESTという名前のファイバーチャネルデバイスエイリアスを設定する必要があります。どのコマンドセットで設定が完了しますか？

A)

```
SITE-A-MDS-Fabric-A# configure terminal
SITE-A-MDS-Fabric-A (config)# device-alias database
SITE-A-MDS-Fabric-A (config-device-alias-db)# device-alias name TEST pwwn 50:00:14:42:d0:0c:f5:20
SITE-A-MDS-Fabric-A (config-device-alias-db)# device-alias commit
```

B)

```
SITE-A-MDS-Fabric-A# configure terminal
SITE-A-MDS-Fabric-A (config)# device-alias database
SITE-A-MDS-Fabric-A (config-device-alias-db)# device-alias name TEST pwwn 50:00:14:42:d0:0c:f5:20
SITE-A-MDS-Fabric-A (config-device-alias-db)# exit
```

C)

```
SITE-A-MDS-Fabric-A# configure terminal
SITE-A-MDS-Fabric-A (config)# device-alias database
SITE-A-MDS-Fabric-A (config-device-alias-db)# device-alias name TEST pwwn 50:00:14:40:47:b0:0c:f5
SITE-A-MDS-Fabric-A (config-device-alias-db)# exit
```

D)

```
SITE-A-MDS-Fabric-A# device-alias database
SITE-A-MDS-Fabric-A (device-alias-db)# device-alias name TEST pwwn 50:00:14:40:47:b0:0c:f5
SITE-A-MDS-Fabric-A (config-device-alias-db)# device-alias commit
```

A. オプション

B. オプション

C. オプション

#### D. オプション

正解: **A** ([コメントを发表する](#))

質問: **68**

デバイスMDS-9148S-2はどのFCモードで動作していますか？

```
MDS-9148S-2# show interface port-channel 2
port-channel 2 is up
  Hardware is Fibre Channel
  Port WWN is 24:02:8c:60:4f:2d:de:c0
  Admin port mode is NP, trunk mode is off
  snmp link state traps are enabled
  Port mode is NP
  Port vsan is 11
  Speed is 16 Gbps
  1 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
  1 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
  1160983754 frames input, 140497639680 bytes
  0 discards, 0 errors
  0 CRC, 0 unknown class
  0 too long, 0 too short
  90139726 frames output, 8743553423232 bytes
```

- A. FPMA
- B. NPIV
- C. NPV
- D. FDISC

正解: **C** ([コメントを发表する](#))

質問: **69**

図を参照してください。ネットワーク管理者は、ネットワークに関して次のような問題に直面しています。

\* PC1でビデオアプリケーションのバッファリング問題が発生しています。

\* SW2に接続されているサーバーは、インターネットに接続する際にパケット損失が発生しています。

エンジニアは、問題をさらに調査するために必要なトラフィックキャプチャを設定したいと考えています。トラフィックを監視するには、どの設定を実装する必要がありますか？

- A. N9K(config)# monitor session 5 txN9K(config-monitor)# description Span\_session\_5N9K(config-monitor)# source interface ethernet 1/1N9K(config-monitor)# source interface ethernet 1/2N9K(config-monitor)# destination interface ethernet 2/3
- B. N9K(config)# monitor session 5 rxN9K(config-monitor)# description Span\_session\_5N9K(config-monitor)# source interface ethernet 1/1N9K(config-monitor)# source interface ethernet 1/2N9K(config-monitor)# destination interface ethernet 2/3
- C. N9K(config)# monitor session 5 txN9K(config-monitor)# description Span\_session\_5N9K(config-monitor)# source vlan 10-15 rxN9K(config-monitor)# source interface ethernet 1/2N9K(config-monitor)# 宛先インターフェース イーサネット 2/3
- D. N9K(config)# monitor session 5 rxN9K(config-monitor)# description Span\_session\_5N9K(config-monitor)# source vlan 10 rxN9K(config-monitor)# source interface ethernet 1/2N9K(config-monitor)# destination interface ethernet 2/3

正解: **D** ([コメントを发表する](#))

正解はDです。SPANセッションでは、報告された2つの問題に関連するトラフィックのみをキャプチャする必要があります。図からPC1はVLAN 10に属しているため、source vlan 10 rxを使用することで、そのVLANで受信したトラフィックにキャプチャを集中させ、PC2に属するVLAN 15からの不要なトラフィックの収集を回避できます。そのため、VLAN 15のトラフィックもミラーリングしてアナライザー出力にノイズを追加するオプションCよりも、オプションDの方が精度が高くなります。

サーバーの問題に関しては、サーバーはSW2の背後にあり、SW2はイーサネット1/2でNexusに接続されています。そのため、エンジニアがこれらのサーバーに影響を与えているパケットドロップに関連するトラフィックを調査できるように、SW2へのアップリンクもソースとして含める必要があります。Cisco NX-OS SPANは、ターゲットを絞ったトラブルシューティングを目的とする場合、同じモニターセッションでVLANソースとインターフェイスソースを混在させることをサポートしています。

オプションAとBは、スイッチのアップリンクのみをミラーリングするため、PC1を個別に分離することはできません。オプションCはVLAN 10から15までをミラーリングするため、範囲が広すぎます。したがって、PC1のVLAN 10トラフィックと調査に必要なSW2アップリンクトラフィックをキャプチャできるDが最適な構成です。

質問: **70**

エンジニアは、UCS-A という名前のプライマリファブリックと、UCS-B という名前のセカンダリファブリックを持っています。kr2016 という名前のキーリングに対して、サブジェクト名が sjc2016 の証明書要求を作成する必要があります。

クラスタのIPアドレスは10.68.68.68です。この証明書要求を作成するコマンドセットはどれですか？

A)

```
UCS-A # scope keyring kr2016
UCS-A /keyring # create certreq 10.68.68.68 sjc2016
UCS-A /keyring* # commit-buffer
```

B)

```
UCS-A# scope security
UCS-A /security # scope keyring kr2016
UCS-A /security/keyring # create certreq ip 10.68.68.68 subject-name sjc2016
UCS-A /security/keyring* # commit-buffer
```

C)

```
UCS-A# scope security
UCS-A /security # scope keyring kr2016
UCS-A /security/keyring # create certreq ip 10.68.68.68 subject-name sjc2016
UCS-A /security/keyring* # commit-buffer
```

D)

```
UCS-B # scope keyring kr2016
UCS-B /keyring # create certreq ip 10.68.68.68 subject-name sjc2016
UCS-B /keyring* # commit-both
```

A. 選択肢D

B. オプションA

C. オプションC

D. オプションB

正解: **C** ([コメントを发表する](#))

質問: **71**

Cisco UCS のユーザー Employee1Jが、Cisco UCS Manager のルートレベルで、Cisco UCS サーバーのブート ポリシーを誤って変更してしまいました。この変更はすべてのサービス プロファイルに影響を与え、ストレージ接続が失われました。システム管理者は、今後この問題が再発しないようにしたいと考えています。新しいセキュリティ ポリシーでは、アクセスを組織レベルまで制限し、他のユーザーがルート ポリシーを変更できないようにすることが義務付けられています。これらの要件を満たすには、どのような対策を講じる必要がありますか？

- A. ユーザーに割り当てられた権限レベルを変更する
- B. カスタムユーザーロールを定義し、ユーザーに割り当てます。
- C. ユーザー Employee1Jにネットワークオペレーターの役割を割り当てます。
- D. ユーザーを特定のCisco UCSロケールに割り当てる

正解: ([正解を表示します](#))

説明

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Managem](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Managem)

## Locales

### User Locales

You can assign a user to one or more locales. Each locale defines one or more organizations (domains) to which a user can access. **Access is usually limited to the organizations specified in the locale.** An exception is a locale without any organizations. It provides unrestricted access to system resources in all organizations.

A Cisco UCS domain can contain up to 48 user locales. Any user locales configured after the first 48 are accepted, but are inactive with faults raised.

質問: 72

このPythonコードを実行すると、どのようなデータ構造が生成されますか？

```
>>> import json
>>> f = open('fname.json', 'r')
>>> var1 = json.load(f)
>>> var1
{'u'bd': u'bd1', u'ap': {u'eggs': [{u'name': u'app'}, {u'name': u'web'}, {u'name': u'db'}], u'name': u'OnlineStore'}, u'name': u'39106329', u'pvn': u'pvn1'}
```

- A. セット
- B. タプル
- C. 辞書
- D. リスト

正解: ([正解を表示します](#))

提供されたPythonコードは、JSONファイルを読み込んでその内容を変数に格納しているようです。PythonではJSONファイルは通常辞書として表現されるため、結果として得られるデータ構造は辞書になります。

質問: 73

左側のハイパーフレックス特性を、右側の適切なハイパーフレックスノードタイプにドラッグアンド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。

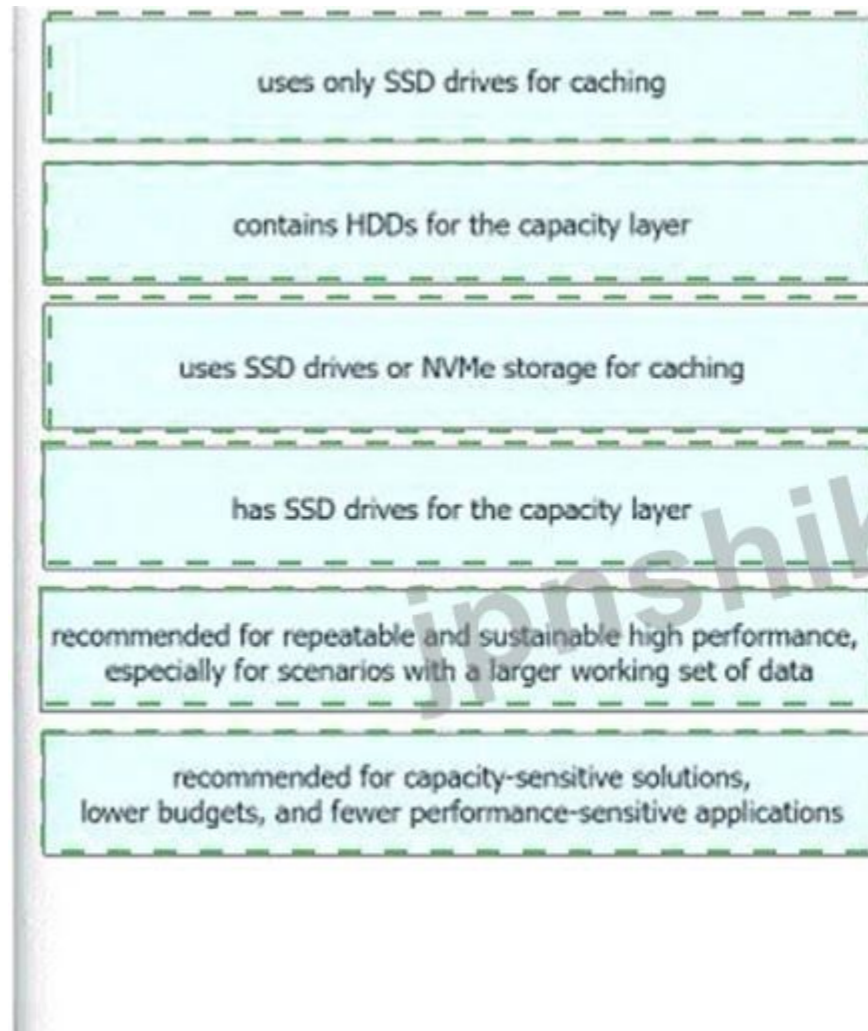
- uses only SSD drives for caching
- contains HDDs for the capacity layer
- uses SSD drives or NVMe storage for caching
- has SSD drives for the capacity layer
- recommended for repeatable and sustainable high performance, especially for scenarios with a larger working set of data
- recommended for capacity-sensitive solutions, lower budgets, and fewer performance-sensitive applications

Hybrid Node



All Flash Node

正解:



Explanation:

ハイブリッド:

キャッシュにはSSDドライブのみを使用する

容量層用のHDDが含まれています

容量重視のソリューション、低予算、およびパフォーマンス重視のアプリケーションが少ない場合に推奨されるオールフラッシュノード:

キャッシュにSSDドライブまたはNVMeストレージを使用する

容量層にはSSDドライブを採用している

再現性と持続的な高いパフォーマンスが期待でき、特に作業データセットが大きいシナリオに適しています。

質問: 74

The screenshot displays two sections of the Cisco UCS Manager interface. The top section is for 'locale3' and the bottom for 'locale4'. Both sections show a table of organizations with columns for 'Name' and 'Org DN'. In 'locale3', the organizations are 'Engineering' (Org DN: org-root/org-Engineering) and 'Sales' (Org DN: org-root/org-Sales). In 'locale4', the organizations are 'B2B' (Org DN: org-root/org-B2B) and 'Sales' (Org DN: org-root/org-Sales). The interface includes navigation options like 'Advanced Filter', 'Export', and 'Print'.

図を参照してください。エンジニアは、複数のサブ組織をホストする UCS ドメインで、user 1 という新しいユーザー名を設定する必要があります。セキュリティ ポリシーでは、admin ロールの使用が禁止されています。ユーザー名には、次の権限が必要です。

- user1 must have access to the Sales sub-organization.
- user1 must be allowed to acknowledge the chassis and IO Module.
- user1 must be allowed to configure beacons.
- user1 must have read access to the rest of the system.

ユーザー1がこれらの権限を持つためには、どの構成を使用する必要がありますか？

- A. 役割: server-compute ロケール: locale3
- B. 役割: server-security ロケール: locale2
- C. 役割: サーバー機器 ロケール: locale4
- D. 役割: server-profile ロケール locale 1

正解: [\(正解を表示します\)](#)

質問: 75

展示資料を参照してください。

```
switch# show install all impact epld n9000-epld.9.2.1.img
Compatibility check:
Module      Type      Upgradable      Impact      Reason
-----
1           SUP      YES             disruptive  Module Upgradable

Retrieving EPLD versions... Please wait.

Images will be upgraded according to following table:
Module      Type      EPLD      Running-Version      New-Version      Upg-Required
-----
1           SUP      MI FPGA      0x23                0x23            No
1           SUP      IO FPGA      0x06                0x06            No
1           SUP      MI FPGA2     0x23                0x23            No
```

ネットワークエンジニアがCisco Nexusスイッチの現在のソフトウェアイメージをアップグレードする予定です。EPLDアップグレードを開始すると、どのような影響がありますか？

- A. 新しいEPLDバージョンを有効にするには、スイッチを一度再起動する必要があります。
- B. 新しいEPLDバージョンを有効にするには、スイッチを複数回再起動する必要があります。
- C. スイッチは、スイッチの各EPLDデバイスに対してEPLDアップグレードをスキップします。
- D. スイッチはMIFPGAのEPLDアップグレードをスキップし、他のEPLDデバイスの処理に進みます。

正解: [\(正解を表示します\)](#)

Cisco NexusスイッチのEPLDをアップグレードするには、スイッチを複数回再起動する必要があるため、システムへの影響が大きくなります。スイッチ上の各EPLDデバイスは個別にアップグレードする必要があり、各デバイスの新しいEPLDバージョンを初期化するためにスイッチを再起動する必要があります。このプロセスにより、すべてのハードウェアコンポーネントが適切に更新され、新しいファームウェアで動作することが保証されますが、各モジュールが再起動するたびにネットワークトラフィックに一時的な中断が発生します。

参考資料 :より詳細な情報については、Cisco Nexus 9000シリーズ FPGA/EPLDアップグレードリリースノートを参照してください。このリリースノートでは、EPLDアップグレードの影響と、アップグレードプロセス中に複数回の再起動が必要となる理由について説明しています。1 また、Cisco Nexus 9000シリーズ NX-OSソフトウェアアップグレードおよびダウングレードガイドでは、EPLDアップグレードに伴うシステムへの影響を含め、アップグレードプロセスに関するガイドラインを提供しています。

質問: 76

エンジニアがCisco MDS 9000シリーズスイッチでポートセキュリティを有効にしようとしています。Cisco MDS 9000シリーズスイッチでポートセキュリティを有効にする際に考慮すべき機能はどれですか？

- A. ログインしているスイッチを常に学習します。
- B. Cisco Fabricサービスを使用して配布できます。
- C. 設定されたsWWNのみがファブリックに参加することを許可します。
- D. スイッチレベルで生地を結合します。

正解: [\(正解を表示します\)](#)

## Port Security Configuration Distribution

The port security feature uses the Cisco Fabric Services (CFS) infrastructure to enable efficient database management, provide a single point of configuration for the entire fabric in the VSAN, and enforce the port security policies throughout the fabric.

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6\\_2/configuration/guides/security/nx-os/sec\\_cli\\_6-x/psec.html#92130](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6_2/configuration/guides/security/nx-os/sec_cli_6-x/psec.html#92130)

有効的な**350-601**問題集はJPNTest.com提供され、**350-601**試験に合格することに役に立ちます！JPNTest.comは今最新**350-601**試験問題集を提供します。JPNTest.com 350-601試験問題集はもう更新されました。ここで**350-601**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> **384**問、**30%ディスカウント**、特別な割引コード：

**JPNshiken**」

質問: 77

図を参照してください。エンジニアは、以下の要件を満たすように、Cisco Nexus 5000シリーズスイッチでポートセキュリティを設定する必要があります。

ポートセキュリティはVSAN 10にのみ適用する必要があります。

- NWWN 20:10:10:10:10:10:10:10 SAN ポートチャネル 2 経由でログインします。

- インターフェース fc1/1、fc1/2 を介してログインできる WWN が必要です。

fc1/3。

自動学習機能は無効にする必要があります。

これらの条件を満たすコマンドセットはどれですか？

```
Nexus5K# configure terminal
Nexus5K(config)# port-security enable
Nexus5K(config)# port-security activate vsan 10 no-auto-learn
```

A. Nexus5K(config)# port-security database vsan 10

Nexus5K(config-port-security)# nwn 20:10:10:10:10:10:10:10 interface san-port-channel 2 Nexus5K(config-port-security)# any wwn interface fc1/1-3 Nexus5K(config-port-security)# port-security commit vsan 10

B. Nexus5K(config)# port-security activate vsan 10 no auto-learn

Nexus5K(config)# port-security database vsan 10

Nexus5K(config-port-security)# nwn 20:10:10:10:10:10:10:10 interface san-port-channel 2 Nexus5K(config-port-security)# any wwn interface fc1/1-3

C. Nexus5K(config)# port-security database vsan 10

Nexus5K(config-port-security)# nwn 20:01:01:01:01:01:01:01 interface san port-channel 5 Nexus5K(config-port-security)# any wwn interface fc1/1-3 Nexus5K(config)# port-security database diff active vsan 10

D. Nexus5K(config)# port-security database vsan 10

Nexus5K(config-port-security)# nwn 20:01:01:01:01:01:01:01 interface port-channel 5 Nexus5K(config-port-security)# any wwn interface fc1/1-3 Nexus5K(config)# port-security database diff active vsan 10

正解: [\(正解を表示します\)](#)

[https://www.cisco.com/en/US/docs/storage/san\\_switches/mds9000/sw/rel\\_3\\_x/configuration/guid es/cli\\_3\\_2/psec.html#wp1298070](https://www.cisco.com/en/US/docs/storage/san_switches/mds9000/sw/rel_3_x/configuration/guid es/cli_3_2/psec.html#wp1298070)

**質問: 78**

CPU使用率が60%を超えた場合にsyslogメッセージを生成する設定はどれですか？

**A.** イベントマネージャアプレット 高CPU負荷

イベント snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.6.1 get-type exact entry-op gt 60 poll-interval 5 action 1.0 syslog priority notifications msg "cpu high"

**B.** イベントマネージャアプレット HIGH-CPU

イベント snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.6.1 get-type exact entry-op lt 60 poll-interval 5 action 1.0 syslog priority notifications msg "cpu high"

**C.** イベントマネージャアプレット 高CPU負荷

イベント snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.6.1 get-type next entry-op gt 60 poll-interval 5 action 1.0 syslog priority notifications msg "cpu high"

**D.** イベントマネージャアプレット 高CPU負荷

イベント snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.6.1 get-type next entry-op lt 60 poll-interval 5 action 1.0 syslog priority notifications msg "cpu high"

正解: ([正解を表示します](#))

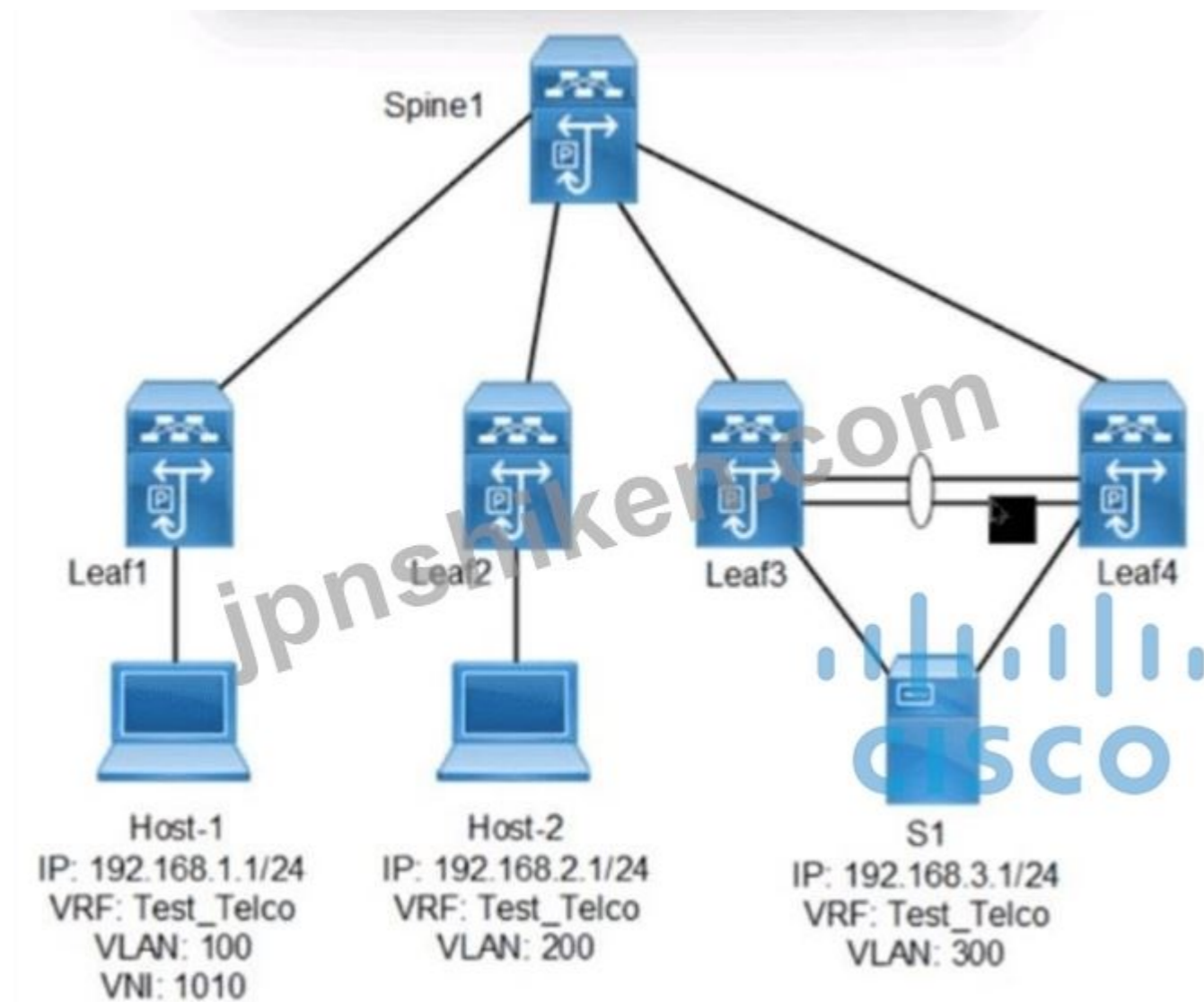
CPU使用率が60%を超えた場合にsyslogメッセージを生成するための正しい設定は、オプションAです。

この設定では、Cisco IOS のイベントマネージャアプレット機能を使用して、SNMP 経由で CPU 使用率を監視します。CPU 使用率が 60% を超えると、指定されたアクションがトリガーされます。この場合、優先度が notifications でメッセージ「cpu high」を含む syslog メッセージが送信されます。event snmp oid コマンドは監視対象の OID を指定し、entry-op gt 60 部分は、値が 60 より大きい場合にアクションをトリガーする条件を設定します。poll-interval 5 は、SNMP OID を 5 秒ごとにポーリングすることを指定します。

<https://www.cisco.com/c/en/us/support/docs/ip/internet-protocol-ip/200931-EEM-Subsystem-in-Order-to-Monitor-CPU-Tr.pdf>

<https://blog.ipSPACE.net/2008/06/generate-snmp-trap-on-high-cpu-load.html>

**質問: 79**



図を参照してください。VXLAN データセンターファブリックには、3 つのホストが 3 つの異なる VLAN にマッピングされています。インGRESS VTEP とエGRESS VTEP はレイヤ 2 とレイヤ 3 のルックアップを実行します。VLAN 100 はリード上の VNI 1010 にマッピングされています。ホスト 1 とホスト 2 間の通信を可能にする一連のアクションはどれですか。

- A. L3 VNIのインターフェイスvlanでプレフィックスベースルーティングを有効にします。Leaf2上のVLAN 200をレイヤ2 VNI 2020にMAPします。
- B. Leaf2 上で VLAN 200 をレイヤ 2 VNI 2020 に MAP します。Test\_Telco\_VRF をレイヤ 2 VNI 1010 にアタッチします。
- C. Test\_Telco\_VRF をレイヤ 3 VNI 1010 にアタッチします。インターフェイス NVE 下のレイヤ 3 VNI の ARP を抑制します。
- D. インターフェイス NVE 下のレイヤ 2 VNI の ARP を抑制します。L3 VNI のインターフェイス vlan でエニーキャスト ゲートウェイ機能を設定します。

正解: ([正解を表示します](#))

質問: 80

左側のネットワークからデータを収集するメカニズムを、右側のそれぞれの特性にドラッグアンドドロップしてください。

CLI-based scripts	Polling can take 5-10 minutes.
SNMP	Unstructured and susceptible to change and scripts failure.
syslog	It sends data from the device to a specific endpoint, for instance, JSON or by using Google protocol buffers.
telemetry	It pushes messages in the format "seq no:timestamp: %facility-severity MNEMONIC:description" and has limits in scale and efficiency.

正解:

CLI-based scripts	SNMP
SNMP	CLI-based scripts
syslog	telemetry
telemetry	syslog

Explanation:

表の説明は信頼度が低いため自動的に生成されました

SNMP  
CISCO

CLI-based scripts

telemetry

syslog

質問: 81

Cisco Hyperflexは、VMware vSphere環境内のノード間でデータを共有するために、どのプロトコルを使用しますか？

- A. CIFS
- B. NFS
- C. FCoE
- D. SMB

正解: [B \(コメントを发表する\)](#)

質問: 82

図を参照してください。Cisco NX-OS スケジューラは毎日午前 3:00 に実行する必要があります。どのコードスニペットがスクリプトを完成させますか？

```
1 configure terminal
2 scheduler job name BACKUP_JOB
3 cli copy running-config bootflash:/${NAME}.${TIMESTAMP}.cfg
4 exit
5 scheduler schedule name BACKUP_SCHEDULE
6 job name BACKUP_JOB
7 
8 end
```

- A. 毎日午前3時開始
- B. 毎週7日 3:00開始
- C. 毎日午前3時
- D. 毎週7日 3:00

正解: [\(正解を表示します\)](#)

質問: 83

展示資料を参照してください。

```
; Router 1 configuration
interface loopback1
  ip address 10.10.32.121/30
  ip ospf network point-to-point
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode

ip pim rp-address 10.10.32.122 group-list 225.0.0.0/8 bi-dir
```

Phantom RPをRP冗長化メカニズムとして使用する双方向PIMネットワークにおいて、2台のCisco NX-OSルータには以下の要件があります。

\* R1はアクティブなRPである必要があります。

\* R2は、R1にアクセスできない場合にのみ使用されるバックアップRPである必要があります。

ルーター2の設定を完了するには、設定手順をドラッグアンドドロップしてください。すべての設定手順を使用する必要はありません。

```
; Router 2 configuration
interface loopback1
  ip address 
  ip ospf network 
  ip router ospf 1 area 0.0.0.0
  ip pim 

ip pim rp-address  group-list 225.0.0.0/8 bi-dir
```

10.10.32.121/32

10.10.32.121

point-to-point

broadcast

10.10.32.121/29

10.10.32.122

sparse-mode

dense-mode

正解:

```
; Router 2 configuration
interface loopback1
 ip address 10.10.32.121/29
 ip ospf network point-to-point
 ip router ospf 1 area 0.0.0.0
 ip pim sparse-mode

ip pim rp-address 10.10.32.122 group-list 225.0.0.0/8 bi-dir
```

10.10.32.121/32	10.10.32.121	point-to-point	broadcast
10.10.32.121/29	10.10.32.122	sparse-mode	dense-mode

質問: 84

TCPプロトコルを使用し、サービス実行に必要なIPポートが1つだけのNFSバージョンはどれですか？

- A. NFSv1
- B. NFSv2
- C. NFSv3
- D. NFSv4

正解: [\(正解を表示します\)](#)

NFSv4の大きな利点の1つは、サービスを実行するためにUDPまたはTCPポート2049のみを使用するため、ファイアウォールを越えてプロトコルを簡単に利用できる点です。

質問: 85

Cisco UCS のユーザー Employee1」が、Cisco UCS Manager のルートレベルで、Cisco UCS サーバーのブート ポリシーを誤って変更してしまいました。この変更はすべてのサービス プロファイルに影響を与え、ストレージ接続が失われました。システム管理者は、今後この問題が再発しないようにしたいと考えています。新しいセキュリティ ポリシーでは、アクセスを組織レベルまで制限し、他のユーザーがルート ポリシーを変更できないようにすることが義務付けられています。これらの要件を満たすには、どのような対策を講じる必要がありますか？

- A. 特定の Cisco UCS ロケーションにユーザーを割り当てます。
- B. ユーザー 従業員1」にネットワークオペレーターの役割を割り当てます。
- C. ユーザーに割り当てられた権限レベルを変更します。
- D. カスタムユーザーロールを定義し、ユーザーに割り当てます。

正解: [\(正解を表示します\)](#)

質問: 86

エンジニアは、メンテナンス期間が始まる前に、Cisco UCSシステム全体のバックアップファイルを作成する必要があります。

バックアップファイルには、以下の属性を含める必要があります。

- \* サービスプロファイル、VLAN、VSANなどのすべての論理構成設定
- \* すべての Cisco UCS ユーザー名、ロール、およびロケール
- \* すべてのCisco UCSシステム設定

この目標を達成するには、どのバックアップタイプを選択する必要がありますか？

- A. システム構成
- B. フルステート
- C. 論理構成
- D. 全構成

正解: ([正解を表示します](#))

質問: 87

デュアルスーパーバイザモジュールと2つのI/Oモジュールを搭載したCisco Nexus 7000シリーズスイッチでISSUを完了するのにかかる時間を短縮するコマンドはどれですか？

- A. すべての Kickstart <イメージ>システム<イメージ>を並列インストールします
- B. すべての epld bootflash をインストールします:<イメージ>
- C. すべての epld bootflash をインストールします:<イメージ>
- D. すべてのキックスタート<イメージ>システム<イメージ>をインストールします

正解: A ([コメントを発表する](#))

**Parallel Upgrade**

**Parallel Upgrade with I/O Modules**

Starting with Cisco NX-OS Release 5.2(1), multiple linecards can be simultaneously upgraded, and the infrastructure support is available. This decreases the ISSU time when compared with an ISSU upgrade that is done serially (one card at a time).

To start a parallel upgrade, use the following command: `install all kickstart image system image parallel`

Up to three linecards can be upgraded in parallel with this command. During the upgrade process, the upgrade of the linecards is displayed in the output as follows:

```
Non-disruptive upgrading.
[#          ] 0%
Module 5 upgrade completed successfully.
.
Module 3 upgrade completed successfully.
```

The screenshot also features a large watermark 'ipnshiken.com' and the Cisco logo.

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/upgrade/guide/cisco\\_nexus7000\\_software\\_upgrade\\_and\\_downgrade\\_guide\\_8x.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/upgrade/guide/cisco_nexus7000_software_upgrade_and_downgrade_guide_8x.html)

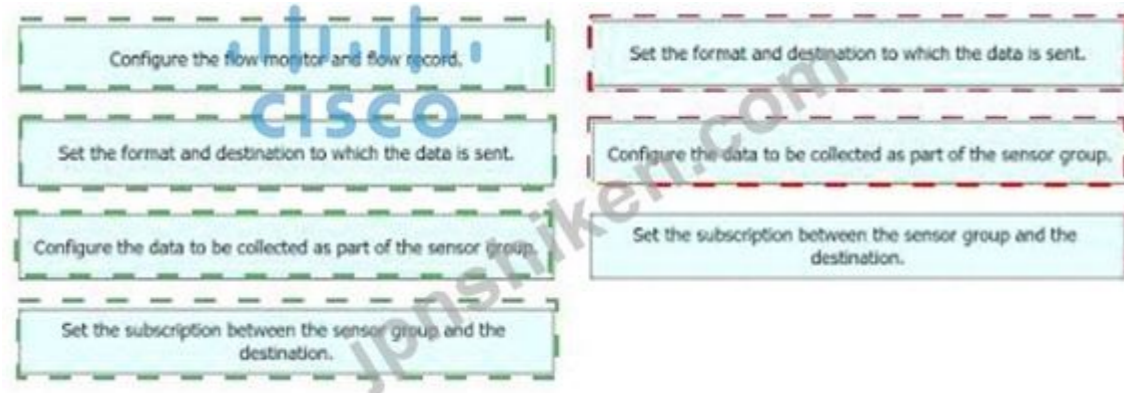
[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/7\\_x/nx-os/upgrade/guide/b\\_Cisco\\_Nexus\\_7000\\_Series\\_NX-OS\\_Software\\_Upgrade\\_and\\_Downgrade\\_Guide\\_Release\\_7-x.html#d54e307a1635](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/7_x/nx-os/upgrade/guide/b_Cisco_Nexus_7000_Series_NX-OS_Software_Upgrade_and_Downgrade_Guide_Release_7-x.html#d54e307a1635)

質問: 88

ネットワークエンジニアは、大規模ネットワークでリアルタイムの構造化データを収集するためのテレメトリソリューションを実装する必要があります。左側のアクションを右側の順序にドラッグアンドドロップして、ソリューションを実装してください。すべてのアクションを使用するわけではありません。



正解:



説明

1. データの送信形式と送信先を設定します。
2. センサーグループの一部として収集するデータを設定します。
3. センサーグループと宛先間のサブスクリプションを設定します。

質問: 89

モジュール式のCisco Nexus 9000シリーズスイッチにおいて、既知のハードウェアの問題を修正したり、機能を向上させたりするには、どのアップグレードタイプを使用する必要がありますか？

- A. EPLD
- B. 与える
- C. SMU
- D. ポップ

正解: A (コメントを发表する)

質問: 90

ブートフラッシュに動作イメージがない場合にファブリックインターコネクトを復旧するために、左側の手順を右側の手順を実行する順序にドラッグアンドドロップしてください。



正解:



#### 質問: 91

あるエンジニアが、組織向けにクラウドソリューションを設計している。セキュリティ要件により、クラウドはローカルデータセンターでホストする必要があるが、リモートバックアップにはリモートデータセンターを活用する必要がある。

さらに、データセンター内のワークロードは、将来的に実績のあるクラウドプロバイダーにスケールアウトされる必要がある。

これらの要件を満たすには、どのクラウド導入モデルを使用する必要がありますか？

- A. パブリッククラウド
- B. ハイブリッドクラウド
- C. プライベートクラウド
- D. エッジクラウド

正解: B (コメントを发表する)

ハイブリッドクラウドモデルは、上記シナリオに最も適しています。このモデルでは、ローカル (プライベート) クラウドインフラストラクチャとリモート (パブリック) クラウドサービスを組み合わせることができます。主要なワークロードをローカルデータセンターでホストし、バックアップにはリモートデータセンターを利用し、必要に応じてパブリッククラウドプロバイダーへスケールアウトできる柔軟性を提供します。ハイブリッドクラウドモデルは、セキュリティ、拡張性、柔軟性など、プライベートクラウドとパブリッククラウドの両方の利点を兼ね備えており、組織の要件に合致しています。

参考資料 :クラウド導入モデルとそのユースケースの詳細については、Cisco Data Center Core Technologies (DCCOR) の学習資料、またはクラウドソリューションに関するCiscoの公式ドキュメントを参照してください。

有効的な**350-601**問題集はJPNTTest.com提供され、**350-601**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-601**試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで**350-601**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> **884**問、**30%ディスカウント**、特別な割引コード:

**JPNshiken**」

**質問: 92**

ネットワークエンジニアは、すべてのAAAサーバーにアクセスできない場合に、コンソールアクセスにローカルユーザーデータベースを使用するようにCisco MDSスイッチを設定する必要があります。このタスクを完了するには、どの設定を適用する必要がありますか？

- A. aaa認証ログインコンソールフォールバックエラーローカル
- B. aaa認証ログインデフォルトローカル
- C. aaa認証ログインコンソールローカル
- D. aaa認証ログインデフォルトフォールバックエラーローカル

正解: ([正解を表示します](#))

**質問: 93**

エンジニアが災害復旧のためにCisco UCS Managerのバックアップを作成したいと考えています。Cisco UCS Managerデータベースの完全状態バックアップの2つの特徴は何ですか？ (2つ選択してください。)

- A. データベースの完全なバイナリダンプを.txzファイルとして実行します。
- B. すべての構成が含まれています
- C. データベースの完全なバイナリダンプをbinファイルとして実行します
- D. データベースの完全なバイナリダンプをSQLファイルとして実行します
- E. ランタイム状態とステータスはすべて含まれていますが、構成情報は含まれていません

正解: ([正解を表示します](#))

Cisco UCS Manager データベースの完全な状態バックアップは、データベースの完全なバイナリダンプを実行します。

.bin ファイルであり、.txz ファイルや .sql ファイルではありません。完全状態バックアップには、Cisco UCS ドメインのすべての構成とすべてのランタイム状態およびステータスが含まれますが、パスワードは含まれません。ハードウェア構成が同一であれば、完全状態バックアップを使用して Cisco UCS Manager データベースを同じファブリック相互接続または別のファブリック相互接続に復元できます。参照:= Implementing and Operating Cisco Data Center Core Technologies (DCCOR) - Cisco、第 5 章: Cisco Unified Computing System ラック サーバーの実装、セクション: Cisco UCS Manager データベースのバックアップと復元

**質問: 94**

ドラッグアンドドロップ問題

ネットワークエンジニアは、Cisco MDS 9000シリーズスイッチのインターフェイスでFCoEを設定する必要があります。これは、VLAN 600とVLAN 6間のマッピングに使用されます。一番下のコマンドをドラッグ&ドロップして、FCoE構成の実装順序に並べ替えてください。すべてのコマンドが使用されるわけではありません。

```
switch(config)# vlan 600
switch(config-vlan)# 
switch(config)# interface ethernet 1/2
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk 
switch(config-if)# spanning-tree port type edge trunk
switch(config)# interface vfc 6
switch(config-if)# bind interface ethernet 1/2
switch(config)# vsan database
switch(config-vsan)#
```

vsan 6 bind interface vfc 6

allowed vlan 1,600

allowed vlan 1

vsan 6 interface vfc 6

fcoe vsan 6

bind vsan 6

正解:

```
switch(config)# vlan 600
switch(config-vlan)# fcoe vsan 6
switch(config)# interface ethernet 1/2
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1,600
switch(config-if)# spanning-tree port type edge trunk
switch(config)# interface vfc 6
switch(config-if)# bind interface ethernet 1/2
switch(config)# vsan database
switch(config-vsan)# vsan 6 interface vfc 6
```

vsan 6 bind interface vfc 6

allowed vlan 1,600

allowed vlan 1

vsan 6 interface vfc 6

fcoe vsan 6

bind vsan 6

質問: 95

エンジニアがREST API呼び出しを使用してCisco APICを設定しています。ログイントークンを受け取るには、POSTメッセージ内でどのデータ構造を使用する必要がありますか？

A)

```
{aaaUser:{attributes:{name: apluser, pwd:cisco123}}}
```

B)

```
<aaaUser><name="apluser"/><pwd="cisco123"/></aaaUser>
```

C)

```
{"aaaUser":{"attributes":{"name":"apluser","pwd":"cisco123"}}
```

D)

```
<aaaUser><name>apluser</name><pwd>cisco123</pwd></aaaUser>
```

A. オプションA

B. オプションB

C. オプションC

D. 選択肢D

正解: C ([コメントを发表する](#))

説明

- **aaaListDomains** –Sent as a GET message, this method returns a list of valid AAA login domains. You can send this message without logging in.

You can call the authentication methods using this syntax, specifying either JSON or XML data structures:

```
{ http | https } :// host [:port] /api/ methodName . { json | xml }
```

This example shows a user login message that uses a JSON data structure:

```
POST https://apic-ip-address/api/aaaLogin.json
```

```
{  
  "aaaUser" : {  
    "attributes" : {  
      "name" : "georgewa",  
      "pwd" : "paSSword1"  
    }  
  }  
}
```



[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/rest\\_cfg/2\\_1\\_x/b\\_Cisco\\_APIC\\_REST\\_API\\_Configuration\\_Guide/b\\_Cisco\\_APIC\\_REST\\_API\\_Configuration\\_Guide\\_chapter\\_0](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/rest_cfg/2_1_x/b_Cisco_APIC_REST_API_Configuration_Guide/b_Cisco_APIC_REST_API_Configuration_Guide_chapter_0)

質問: 96

```
N7Switch# sh run | section callhome
callhome
email-contact admin@acme.com
phone-contact +1-800-123-4567
streetaddress 111 Somestreet St. Sometown, Somewhere
destination-profile full txt email-addr netadmin@acme.com
transport email smtp-server 192.168.1.25 port 25
transport email from N7Switch@acme.com
enable
alert-group Inventory user-def-cmd show logging last 100
N7Switch#
```

図を参照してください。ネットワークエンジニアがCisco NexusシリーズスイッチでSmart Call Home機能を設定しています。シャーシに新しいハードウェアが挿入されるたびに、ログの最後の100行を含むメールを生成する必要があります。メールを受信するために、設定にどのコマンドを追加する必要がありますか？

- A. 宛先プロファイル操作アラートグループ在庫
- B. alert-group Operations user-def-cmd show logging last 100
- C. alert-group Linecard-Hardware user-def-cmd show logging last 100
- D. 宛先プロファイル操作メッセージレベル2

正解: ([正解を表示します](#))

#### 質問: 97

Cisco MDSでNPVモードを実装する場合、エンジニアはファブリックの冗長性を確保する必要があります。

9000シリーズスイッチ。

どの操作によってファブリックの冗長性が可能になりますか？

- A. TEポートを使用して上流のスイッチに接続します。
- B. 上流スイッチにポートチャネルを追加します。
- C. NPV デバイスを外部 FLOGI データベースを使用するように設定します。
- D. NPVデバイスを複数の上流スイッチに接続します。

正解: ([正解を表示します](#))

ポートチャネルは、NPVスイッチとNPVスイッチ間のリンクレベルの冗長性を確保するのに役立つだけで、NPVモードを有効にした後にNPVスイッチを再起動する必要がある場合には役立ちません。ドキュメントによると、1台のNPVデバイスを複数のアップストリームスイッチに接続できますが、ダウンストリームホストが両方のファブリックに接続されていて、かつNPVスイッチのうち1台だけが一度に再起動される場合を除き、ダウンストリームホストには役立ちません。

[https://www.cisco.com/en/US/docs/storage/san\\_switches/mds9000/sw/rel\\_3\\_x/configuration/guides/fm\\_3\\_3\\_1/npv.html](https://www.cisco.com/en/US/docs/storage/san_switches/mds9000/sw/rel_3_x/configuration/guides/fm_3_3_1/npv.html)

#### 質問: 98

エンジニアは、Cisco UCSインフラストラクチャの災害復旧ポリシーを実装する必要があります。ソリューションは以下の基準を満たす必要があります。

回復目標時間は48時間でなければならない。

バックアップは暗号化された通信を使用する必要があります。

回復目標時間は4時間とする必要があります。

これらの要件を満たすには、スケジュールされたバックアップでどの構成セットを使用する必要がありますか？

- Protocol: SFTP  
Schedule: Weekly
- Protocol: FTP  
Schedule: Bi-Weekly
- Protocol: TFTP  
Schedule: Bi-Weekly
- Protocol: SCP  
Schedule: Daily

- A. オプションA
- B. オプションB
- C. オプションD
- D. オプションC

正解: [\(正解を表示します\)](#)

質問: 99

図を参照してください。ネットワークエンジニアがCisco Nexusスイッチの現在のソフトウェアイメージをアップグレードする予定です。EPLDアップグレードのスターリングによる影響は何ですか？

```
switch# show install all impact epld n9000-epld.9.2.1.img
Compatibility check:
Module      Type      Upgradable  Impact  Reason
-----
1           SUP      Yes         disruptive  Module Upgradable

Retrieving EPLD versions... Please wait.

Images will be upgraded according to following table:
Module  Type  EPLD      Running-Version  New-Version  Upg-Required
-----
1  SUP  MI FPGA  0x23            0x23         No
1  SUP  IO FPGA  0x06            0x06         No
1  SUP  MI FPGA2 0x23            0x23         No
```

- A. 新しいEPLDバージョンを有効にするには、スイッチを複数回再起動する必要があります。
- B. スイッチはMIFPGAのEPLDアップグレードをスキップし、他のEPLDデバイスの処理に進みます。
- C. スイッチは、スイッチの各EPLDデバイスのEPLDアップグレードをスキップします。
- D. 新しいEPLDバージョンを有効にするには、スイッチを一度再起動する必要があります。

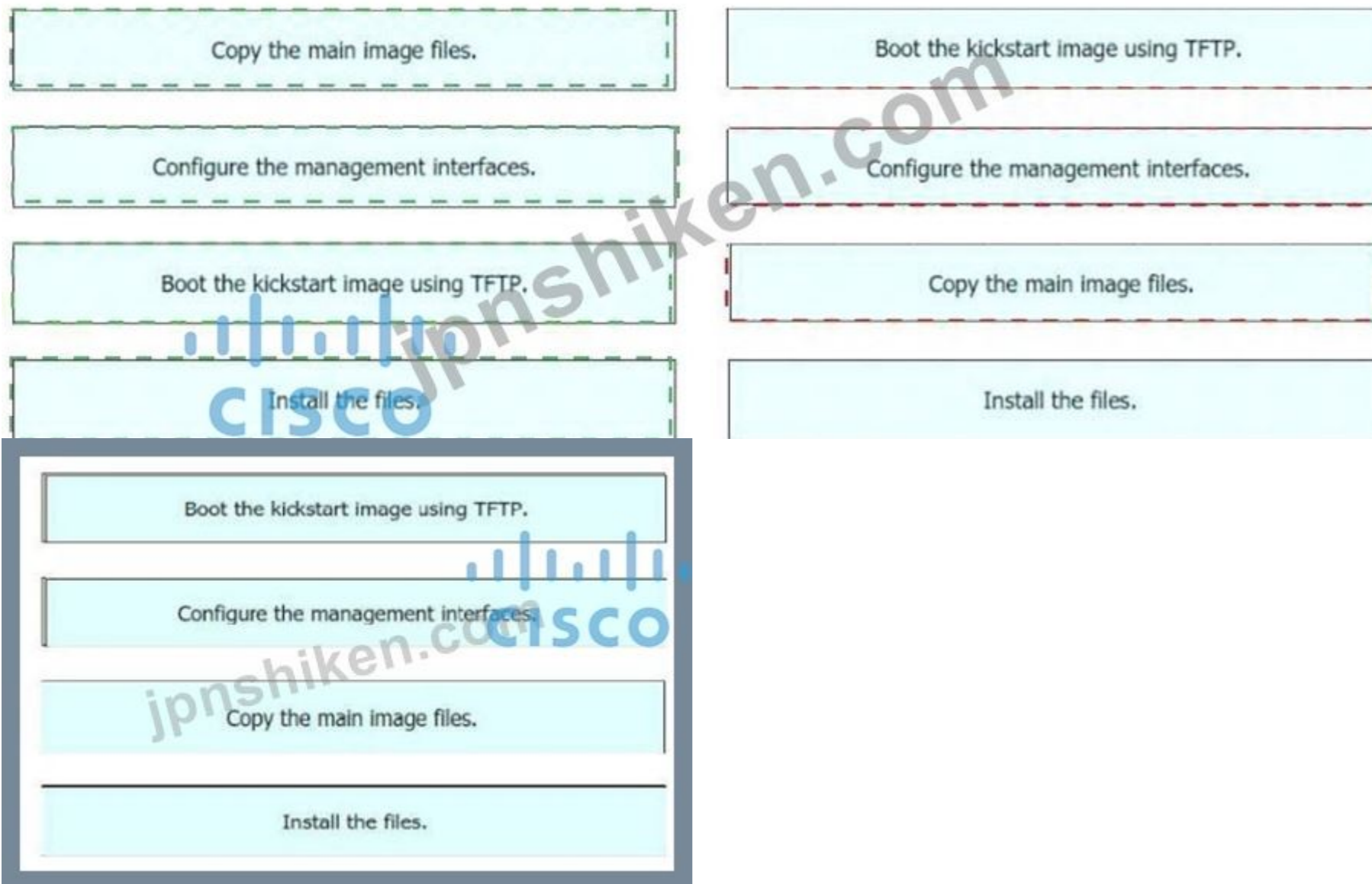
正解: [C \(コメントを发表する\)](#)

質問: 100

ブートフラッシュに動作イメージがない場合にファブリックインターコネクトを復旧するために、左側の手順を右側の手順を実行する順序にドラッグアンドドロップしてください。



正解:



質問: 101

展示資料を参照してください。

```
Enter the configuration method. (console/gui) ? console

Enter the setup mode; setup newly or restore from backup.
(setup/restore) ? restore

NOTE:
  To configure Fabric interconnect using a backup file on
  a remote server, you will need to setup management
  interface.
  The management interface will be re-configured (if
  necessary), based on information stored in the backup file.

Continue to restore this Fabric interconnect from a backup
file (yes/no) ? yes

Physical Switch Mgmt0 IPv4 address : 192.168.10.10
Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0
IPv4 address of the default gateway : 192.168.10.1
Enter the protocol to get backup file (scp/ftp/tftp/sftp)
? scp
Enter the IP address of backup server: 20.10.20.10
Enter fully qualified backup file name: Backup.bak
Enter user ID: user
Enter password:
  Retrieved backup configuration file.
Configuration file - Ok
```

Cisco UCSの設定を復元するには、どのタイプのバックアップが必要ですか？

- A. システム構成
- B. 全構成
- C. 論理構成
- D. 完全状態

正解: ([正解を表示します](#))

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/sw/cli/config/guide/1-0-2/b\\_CLI\\_Config\\_Guide\\_](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/cli/config/guide/1-0-2/b_CLI_Config_Guide_)

The following example restores a system configuration from the Backup.bak file, which was retrieved from the 20.10.20.10 backup server using FTP:

```
Enter the configuration method. (console/gui) ? console
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? restore
```

NOTE:

To configure Fabric interconnect using a backup file on a remote server, you will need to setup management interface.

The management interface will be re-configured (if necessary), based on information stored in the backup file.

```
Continue to restore this Fabric interconnect from a backup file (yes/no) ? yes
```

```
Physical Switch Mgmt0 IPv4 address : 192.168.10.10
```

```
Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0
```

```
IPv4 address of the default gateway : 192.168.10.1
```

```
Enter the protocol to get backup file (scp/ftp/tftp/sftp) ? scp
```

```
Enter the IP address of backup server: 20.10.20.10
```

```
Enter fully qualified backup file name: Backup.bak
```

```
Enter user ID: user
```

```
Enter password:
```

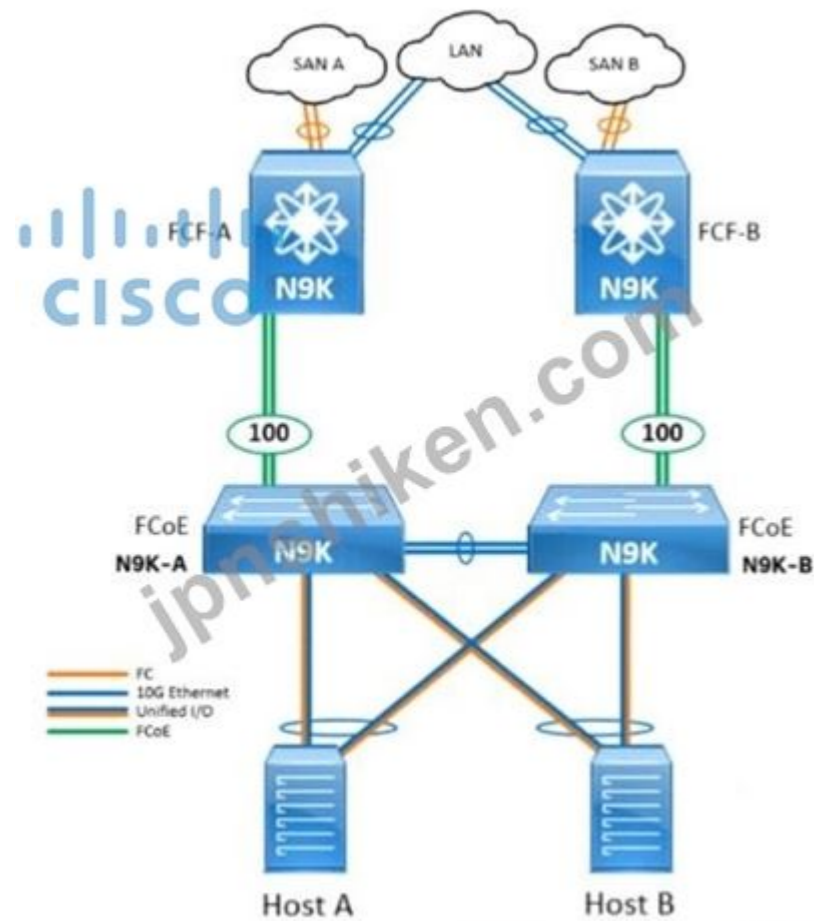
```
Retrieved backup configuration file.
```

```
Configuration file - Ok
```

```
Cisco UCS 6100 Series Fabric Interconnect
UCS-A login:
```

質問: 102

展示資料を参照してください。



図を参照してください。エンジニアは、N9K-AスイッチとFCF-A Nexus 9000コアスイッチ間でFCoEを構成する必要があります。この展開には以下の特徴があります。N9K-AおよびN9K-Bトップオブラック・スイッチは、コア・スイッチのドメインIDを共有します。ホストには統合型ネットワークアダプタが搭載されています。ポートチャネル100を通過することが許可されているVSANは、VSAN 20のみです。N9K-AデバイスでFCoE構成を完了するには、どの構成を使用しますか？

```

① N9K-A(config)# feature fcoe
N9K-A(config)# feature npv
N9K-A(config)# interface vfc 100
N9K-A(config-if)# bind interface port-channel 100
N9K-A(config-if)# switchport mode F
N9K-A(config-if)# switchport trunk allowed vsan 20

N9K-A(config)# feature fcoe
N9K-A(config)# feature npv
N9K-A(config)# interface vfc 100
N9K-A(config-if)# bind interface port-channel 100
N9K-A(config-if)# switchport mode N
N9K-A(config-if)# switchport trunk allowed vsan 1, 20

② N9K-A(config)# feature-set fcoe-npv
N9K-A(config)# interface vfc-port-channel 100
N9K-A(config-if)# switchport mode NP
N9K-A(config-if)# switchport trunk allowed vsan 20

③ N9K-A(config)# feature-set fcoe-npv
N9K-A(config)# interface vfc-port-channel 100
N9K-A(config-if)# switchport mode E
N9K-A(config-if)# switchport trunk allowed vsan 1, 20

```

A. 選択肢D

- B. オプションB
- C. オプションA
- D. オプションC

正解: [\(正解を表示します\)](#)

質問: 103

```
1 from cii import *
2 import json
3
4 interface_output = json.loads(cliid('show interface brief'))
5
6
7
8
9
10
11
12 print(json.dumps(active_interfaces, indent=4))
```

```
interface out = {
  "TABLE_interface": {
    "ROW_interface": [
      {
        "interface": "mgmt0",
        "speed": "1000",
        "state": "up",
        "ip_addr": "10.10.20.95",
        "mtu": "1500"
      },
      {
        "name": "Vlan101",
        "admin_status": "down",
        "line_protocol_status": "down",
        "lastmode": "D",
        "speed": "auto",
        "vlan": "30",
        "state": "down",
        "portmode": "access",
        "state_rsn_desc": "inactive",
        "interface": "Ethernet1/17",
        "type": "eth"
      },
      {
        "interface": "Vlan101",
        "svi_rsn_desc": "Administratively down",
        "svi_admin_state": "down"
      }
    ]
  }
}
```

図を参照してください。エンジニアが、Cisco Nexus 9000 シリーズ スイッチのネイティブ Python 環境で実行する Python スクリプトを作成します。スクリプトの標準出力には、スイッチ上のアクティブなインターフェイスの名前のリストが表示されます。interface\_output 変数の内容を解析して指定されたリストを作成するコード スニペットはどれですか？

○ 

```
active_interfaces = [
    interface['interface']
    for interface in
    interface_output["TABLE_interface"]["ROW_interface
"]
    if 'state' in interface.keys()
    if interface['state'] != 'down'
]
```

○ 

```
active_interfaces = [
    interface
    for interface in
    interface_output["TABLE_interface"]["ROW_interface
"]
    if 'state' in interface.keys()
]
```

○ 

```
active_interfaces = [
    interface['interface']
    for interface in interface_output
    if 'state' not in interface.keys()
]
```

○ 

```
active_interfaces = [
    interface['interface']
    for interface in interface_output
    if 'state' not in interface.keys()
    if interface['state'] != 'down'
]
```

- A. オプションD
- B. オプションB
- C. オプションC
- D. オプションA

正解: [\(正解を表示します\)](#)

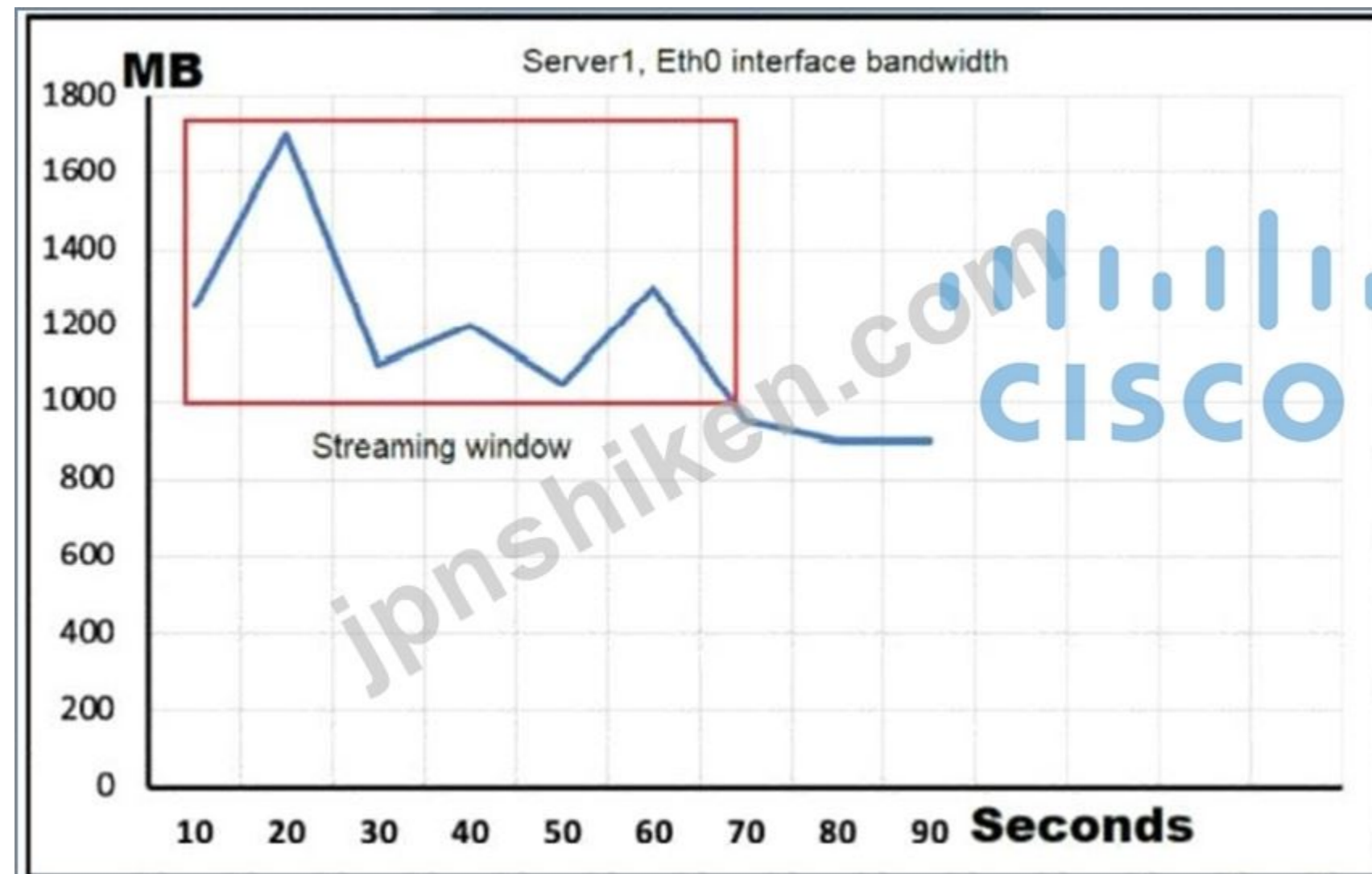
質問: 104

ある企業は、データセンターの一部として、Cisco Nexus 7706 シリーズ スイッチを 2 台運用しています。すべてのネットワーク エンジニアは、コア スイッチへの読み取り/書き込みアクセスが制限されています。ネットワーク エンジニアは、サービスから FCoE ストレージへのトラフィックを許可するために、新しい FCoE VLAN を作成する必要があります。これらの要件を満たすために、どのような一連のアクションを実行する必要がありますか？

- A. アクティブユーザーデータベースに変更をコミットします。
- B. 1. ユーザー定義ロールを作成し、必要な権限を追加します。  
2. ユーザーに役割を割り当てる。
- C. 1. ネットワークオペレーターの役割を変更し、必要な権限を追加します。  
2. ユーザーにVDCオペレーターの役割を割り当てます。
- D. 1. ユーザーにネットワーク管理者ロールを割り当てます。  
2. ロールをアクティブユーザーデータベースへの切り替えにコミットします
- E. 1. VDC-admin ロールに必要な権限を追加します。

正解: E ([コメントを发表する](#))

質問: 105



図を参照してください。Server1は、1Gbポートチャネルを介してCisco Nexus 9000シリーズスイッチに接続されています。Eth0デバイスには、ストーム制御が0%の値で適用されています。ストリーミングウィンドウ中にスイッチインターフェイスを通過するトラフィックがインターフェイスの帯域幅を超えた場合、スイッチはどのような処理を実行しますか？

- A. 交通量の半分を前方へ
- B. すべてのトラフィックを転送します
- C. すべてのトラフィックを抑制します
- D. 余分なトラフィックをすべて削除します

正解: [\(正解を表示します\)](#)

#### 質問: 106

エンジニアがCisco MDS 9000シリーズスイッチにおけるファイバーチャネルの導入に関するトラブルシューティングを行っている。

この出力はポートチャネル1について何を示していますか？

```
mds9509# show int po1
port-channel 1 is trunking
Hardware is Fibre Channel
Port WWN is 24:01:00:0d:ec:20:ba:00
Admin port mode is F, trunk mode is on
snmp link state traps are enabled
Port mode is TF
Port vsan is 1
Speed is 8 Gbps
Trunk vsans (admin allowed and active) (1,20)
Trunk vsans (up) (1,20)
Trunk vsans (isolated) ()
Trunk vsans (initializing) ()
5 minutes input rate 112 bits/sec, 14 bytes/sec, 0 frames/sec
5 minutes output rate 152 bits/sec, 19 bytes/sec, 0 frames/sec
25787798 frames input, 14409205722 bytes
0 discards, 0 errors
0 CRC, 0 unknown class
0 too long, 0 too short
23082 frames output, 1013152 bytes
0 discards, 0 errors
18 input OLS, 14 LRR, 29 NOS, 0 loop inits
17 output OLS, 0 LRR, 21 NOS, 0 loop inits
Member[1] : fc4/2
Member[2] : fc4/8
Interface last changed at Thu Mar 6 06:27:36 2020
```

- A. ポートチャネル1はNPVスイッチに接続するように設定されています。
- B. ポートチャネル1はNPVスイッチに接続するように設定されています。
- C. ポートチャネル1はISLとして構成されています。
- D. ポートチャネル1はホストバスアダプタに接続するように構成されています。

正解: B ([コメントを发表する](#))

有効的な**350-601**問題集はJPNTTest.com提供され、**350-601**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-601**試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで**350-601**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> **384**問、**30%ディスカウント**、特別な割引コード:

**JPNshiken**」

質問: 107

ホストファームウェアパッケージからデフォルトで除外されるコンポーネントはどれですか？

- A. ネットワークインターフェースコントローラ
- B. ボードコントローラ
- C. ストレージコントローラ
- D. ローカルディスク

正解: (正解を表示します)

Cisco UCS Managerは、ファームウェアのアップグレード中にデータ損失や破損が発生するのを防ぐため、デフォルトではホストファームウェアパッケージからローカルディスクを除外します。ホストファームウェアパッケージには、ネットワークインターフェースコントローラやストレージコントローラなどの他のコンポーネントのファームウェアが含まれていますが、機密データが含まれている可能性のあるローカルディスクは除外されます。

質問: 108



図を参照してください。エンジニアはVXLAN展開をプロビジョニングする必要があります。OSPFは既にアンダーレイプロトコルとして構成されています。すべてのBGP構成はテンプレート方式を使用して実行されます。展開はこれらの要件を満たす必要があります。

\* リーフスイッチのローカル更新ソースはループバック1である必要があります

ルーターIDはローカルループバックIPアドレスである必要があります。

\* 外部BGP接続ではテンプレート名を使用する必要があります

下部から設定スニペットをドラッグアンドドロップして設定を完了します。

```
router bgp 65000
  router-id [ ]
  template peer SPINE
  bfd
  remote-as [ ]
  update-source loopback1
  timers 3 9
  address-family [ ] [ ]
    send-community extended
  neighbor [ ]
    [ ] peer SPINE
```

10.255.255.1    inherit    65000  
10.255.255.10    12vpn    evpn

正解:

```
router bgp 65000
  router-id 10.255.255.10
  template peer SPINE
  bfd
  remote-as 65000
  update-source loopback1
  timers 3 9
  address-family 12vpn evpn
    send-community extended
  neighbor 10.255.255.1
    inherit peer SPINE
```

10.255.255.1    inherit    65000  
10.255.255.10    12vpn    evpn

```
router bgp 65000
  router-id 10.255.255.1
  template peer SPINE
  bfd
  remote-as 65000
  update-source loopback1
  timers 3 9
  address-family 12vpn evpn
    send-community extended
  neighbor 10.255.255.1
    inherit peer SPINE
```

**質問: 109**

ネットワークエンジニアは、ファブリック内のすべてのCisco MDSシリーズスイッチでポートセキュリティを有効にする必要があります。要件は、スイッチポートの大規模な手動設定を回避することです。これらの要件を満たすために、どのような対策を講じる必要がありますか？

- A. VSANごとに自動学習ポートセキュリティ機能を有効にします。
- B. VSANごとにCFS配布とファイル自動学習ポートセキュリティ機能を有効化します。
- C. ポートセキュリティの自動学習機能を有効にします。
- D. CFS配信と自動学習ポートセキュリティ機能を有効にします。

正解: ([正解を表示します](#))

**質問: 110**

展示資料を参照してください。

python code:

```
import requests
import json

url='http://lab-93180bdlf-sw1/ins'
switchuser='dazfre'
switchpassword='Clscorox0'

myheaders={'content-type' 'application/json'}
payload={
  "ins_api": {
    "version": "1.0",
    "type": "cli_show",
    "chunk": "0",
    "sid": "1",
    "input": "configure terminal : feature hsrp",
    "output_format": "json"
  }
}
response = requests post(url,data=json.dumps(payload),
headers=myheaders,auth=(switchuser,switchpassword))

print(response.text)
```

ERROR MESSAGE

```
{
  "ins_api" [
    "type": "cli_show"
    "version": "1.0",
    "sid": "eoc",
    "outputs" [
      "output" [
        [{"clierror" "% invalid command\n",
          "input" "configure terminal"
          "msg" "input CLI command error",
          "code" "400"}
        ],{
          "clierror" "% invalid command\n",
          "input" "feature hsrp",
          "msg" "input CLI command error",
          "code" "400"}
        ]
      ]
    }
  }
```

Cisco NX-API用のPythonコードがエラーメッセージを表示するのはなぜですか？

- A. NX-API では、リクエスト モジュールを介した機能の設定はできません。
- B. typeが間違っています。リクエストの本文であり、<code>cli\_conf</code>であるべきです。
- C. JSONはNX-APIでサポートされている形式ではありません。
- D. リクエストのヘッダーの typeが間違っており、<code>cli\_conf</code>であるべきです。

正解: [\(正解を表示します\)](#)

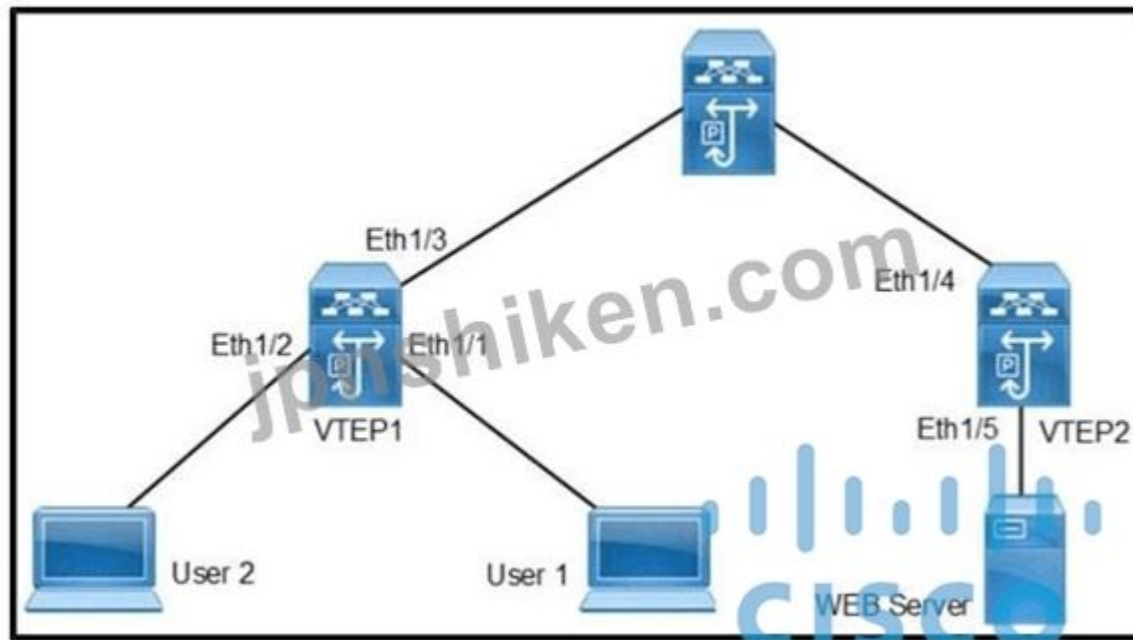
質問: 111

ネットワークエンジニアが、Cisco Intersight管理ポータルにCisco HyperFlexデータ プラットフォームを追加しています。IntersightがCisco HyperFlexデータ プラットフォームを認識するために必要なコンポーネントはどれですか？ 2つ選択してください。)

- A. デバイスクレームコード
- B. デバイスのパブリックIPアドレス
- C. デバイスのシリアル番号
- D. デバイスのFQDN
- E. デバイスID

正解: [\(正解を表示します\)](#)

質問: 112



図を参照してください。ユーザー1とユーザー2はVTEP1スイッチに接続されています。ユーザーはWebサーバーにアクセスできます。

監視ツールによると、ネットワークパフォーマンスが低下しており、User2からWEBサーバーへ過剰なトラフィックが送信されています。User2からのトラフィックを抑制し、User1からのすべてのトラフィックタイプを許可するには、どのストーム制御パーセンテージレベルを使用する必要がありますか？

- A. Eth1/2 のレベル 0、Eth1/1 のレベル 100
- B. Eth1/1でレベル100、Eth1/5でレベル100
- C. Eth1/1 のレベル 0、Eth1/2 のレベル 100
- D. Eth1/2 のレベル 0 と Eth1/5 のレベル 0

正解: [\(正解を表示します\)](#)

質問: 113

エンジニアは、既存のCisco UCS Manager環境の構成バックアップを実行する必要があります。バックアップファイルには、すべてのvNIC、vHBA、およびサービスプロファイルテンプレートの設定が含まれている必要があります。また、エンジニアはインポート前にバックアップを検証する必要があります。出力形式はXMLである必要があります。これらの要件を満たすには、どのバックアップタイプを使用する必要がありますか？

- A. 完全状態
- B. 全構成
- C. 論理構成
- D. システム構成

正解: C ([コメントを发表する](#))

Cisco UCS Manager の論理構成バックアップタイプには、サービスプロファイル、VLAN、VSAN、プール、ポリシーなどのすべての論理構成設定が含まれます。このバックアップタイプには、すべてのvNIC、vHBA、およびサービスプロファイルテンプレート設定が含まれているため、エンジニアの要件に適しています。さらに、論理構成バックアップはXML形式であるため、インポート前に検証を行うことができます。

参考文献：

\* Cisco のドキュメント「構成のバックアップと復元」には、さまざまなバックアップの種類とその内容に関する詳細情報が記載されています 1。

\* UCS Managerのバックアップ操作と種類に関する詳細については、Cisco UCS Manager管理ガイドを参照してください。

質問: 114

展示資料を参照してください。

```
import time
import cli

date= time.strftime('%Y%m%d')
file=
cli.execute ('copy running-config ftp://10.183.249.182/FusionSW/' + file)
exit()
```

file」キーワードを含むstarlingの行に、生成された実行設定ファイルの名前が fusion-config\_」で、日付が現在の日付になるようにするには、どのコマンドを追加する必要がありますか？

- A. ('fusion-config\_ + date')
- B. string(('fusion-config\_') + date)
- C. str.('fusion-config\_') + date
- D. ('fusion-config\_') + 日付

正解: C ([コメントを发表する](#))

質問: 115

FCoE実装において、FCoE初期化プロトコルがEノードで使用するために選択するMACアドレスに関する記述として正しいのはどれですか？

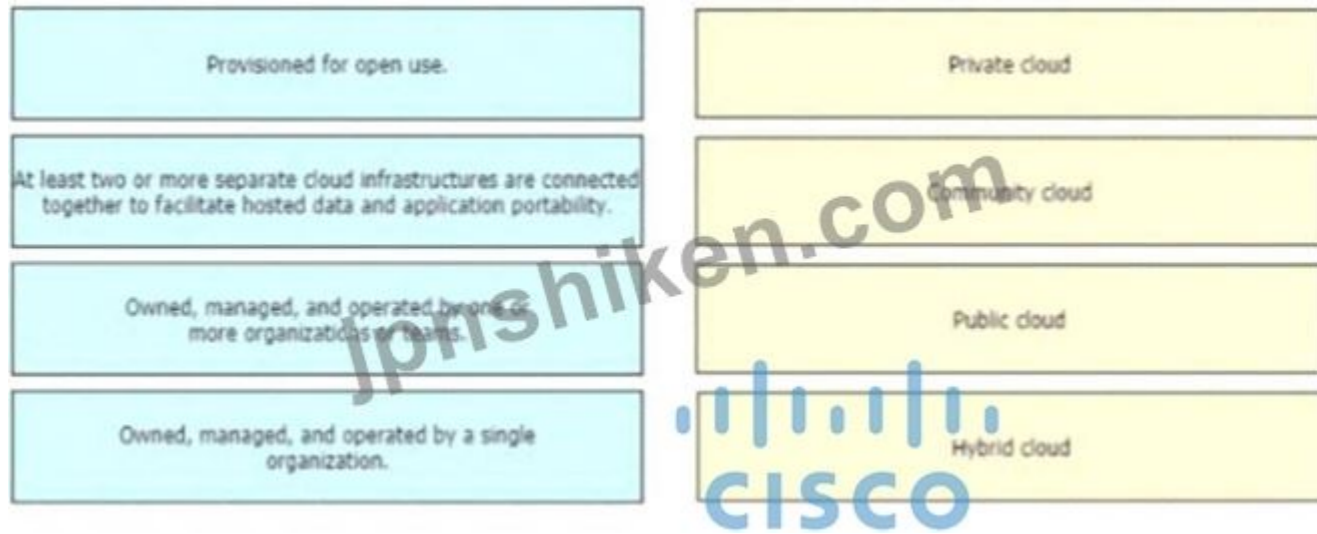
- A. FCoEはMACアドレスを使用しません。FCoE初期化プロトコルを使用してファイバーチャネルIDを取得し、そのアドレスはファイバーチャネルプロトコルと同様にすべてのFCoE通信に使用されます。
- B. FCoE初期化プロトコルは、MACアドレスの最初の24ビットとして01.00.0Cを使用し、24ビットのファイバーチャネルIDを追加して、完全な48ビットのFCoE MACアドレスを生成します。
- C. FCoE初期化プロトコルは24ビットのFC-MAPを使用し、24ビットのファイバーチャネルIDを連結して、ファイバー提供MACアドレスを作成します。
- D. FCoE初期化プロトコルは、すべてのFCoE操作に、統合ネットワークアダプタの焼き付けられたMACアドレスを使用します。

正解: C ([コメントを发表する](#))

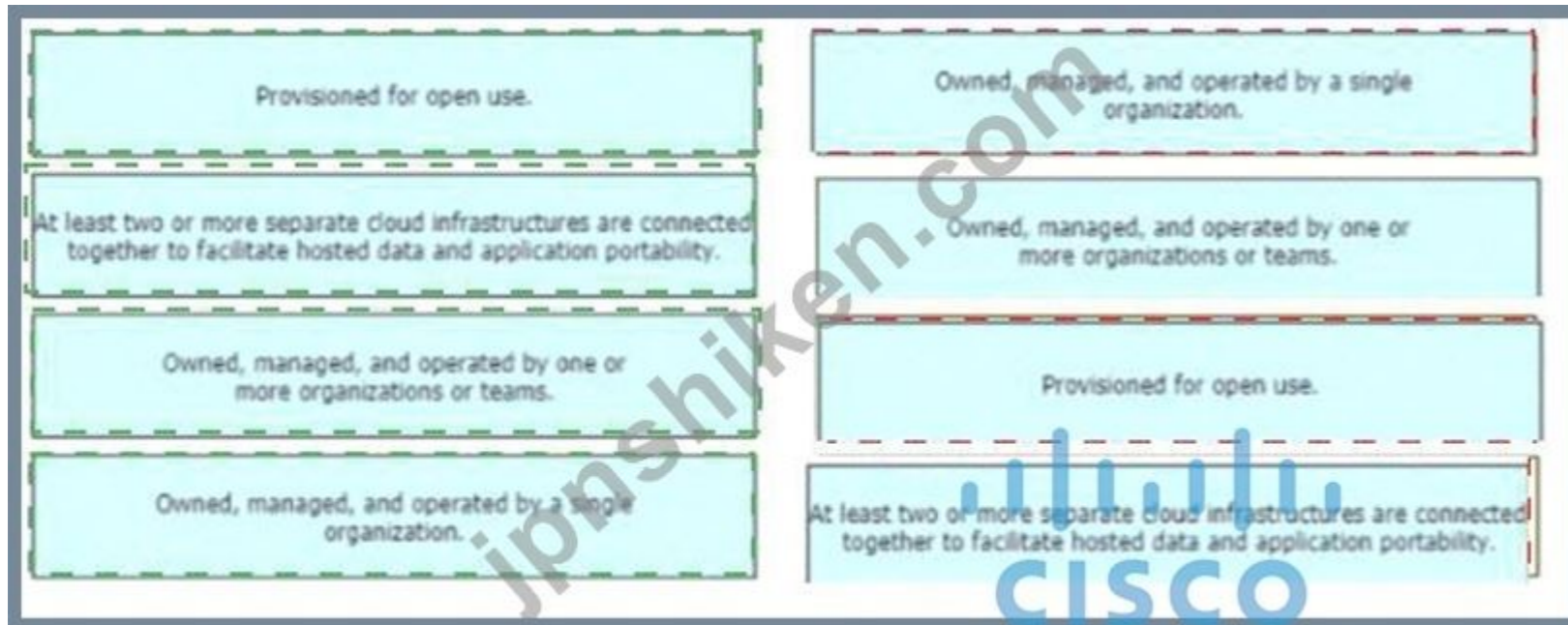
[https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data\\_Center/UF\\_FCoE\\_final.html#wp1154912](https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/UF_FCoE_final.html#wp1154912)

質問: 116

ネットワークエンジニアに、クラウドインフラストラクチャモデルを、その運用とリソースへのアクセスという観点から説明するよう依頼しました。左側の説明を適切な場所にドラッグアンドドロップしてください。



正解:



説明

プライベートクラウド : 単一の組織が所有、管理、運用するクラウド。

コミュニティクラウド : 1つまたは複数の組織やチームによって所有、管理、運営されるクラウド。

パブリッククラウド : 一般利用向けにプロビジョニングされています。

ハイブリッドクラウド : ホストされているデータとアプリケーションの移植性を容易にするために、少なくとも2つ以上の独立したクラウドインフラストラクチャが相互に接続されている。

質問: 117

エンジニアが、セキュリティ基準の高い顧客向けにストレージ環境を構成します。セキュアな環境はVSAN 50で構成されます。顧客は、構成とアクティブなデータベースを維持し、不正なスイッチがファブリックに参加するのを防ぎたいと考えています。さらに、スイッチは、初めて接続されたポートのWWPNを自動的に学習することで、不正なデバイスがポートに接続するのを防ぐ必要があります。これらの要件を満たすには、どの構成セットを使用する必要がありますか？ 2つ選択してください。)

A. fcspを有効にする

fcsp自動アクティブ

B. fcsp dhchap ハッシュ md5 sha1

C. 布地バインディングアクティベートvsan 50フォース

D. 透明布製バインディングアクティベートvsan 50

布地バインディングアクティベートvsan 50

E. ポートセキュリティを有効にする

port-security activate vsan 50

正解: C,E ([コメントを发表する](#))

シナリオで説明されている高度なセキュリティ要件を満たすには、次の2つの具体的な目標に取り組む必要があります。

不正なスイッチがファブリックに接続されるのを防ぐには、ファブリックバインディングが必要です。

WWPNを自動的に学習し、不正なデバイスの接続を防止します。これにはポートセキュリティが必要です。

布地バインディングvsan 50フォースを活性化

- VSAN 50 のファブリックバインディングを有効にします。

- 事前に定義されたスイッチのみがファブリックに参加できるようにし、不正なスイッチの参加を防止します。

- forceキーワードを使用すると、スイッチが既にファブリックの一部になっている場合でも、スイッチがアクティブになります。

ポートセキュリティを有効にする

port-security activate vsan 50

- ポートセキュリティを有効にします。これにより、スイッチは初回接続時にWWPNを動的に学習し、未知のデバイスがポートに接続するのを防ぎます。

質問: 118

エンジニアは、VLAN 100 で HSRP を使用するように Nexus 7000 シリーズ スイッチを設定する必要があります。完全に機能する場合、ルータはアクティブ マスターである必要があります。このシナリオを実装するには、どのコマンドセットを使用する必要がありますか？

feature hsrp  
interface vlan100  
ip address 10.1.1.2 255.255.255.0  
priority 120  
hsrp version 2  
hsrp 1000  
ip 10.1.1.1

feature hsrp  
interface vlan100  
ip address 10.1.1.2 255.255.255.0  
priority 100  
hsrp version 2  
hsrp 1000  
ip 10.1.1.1

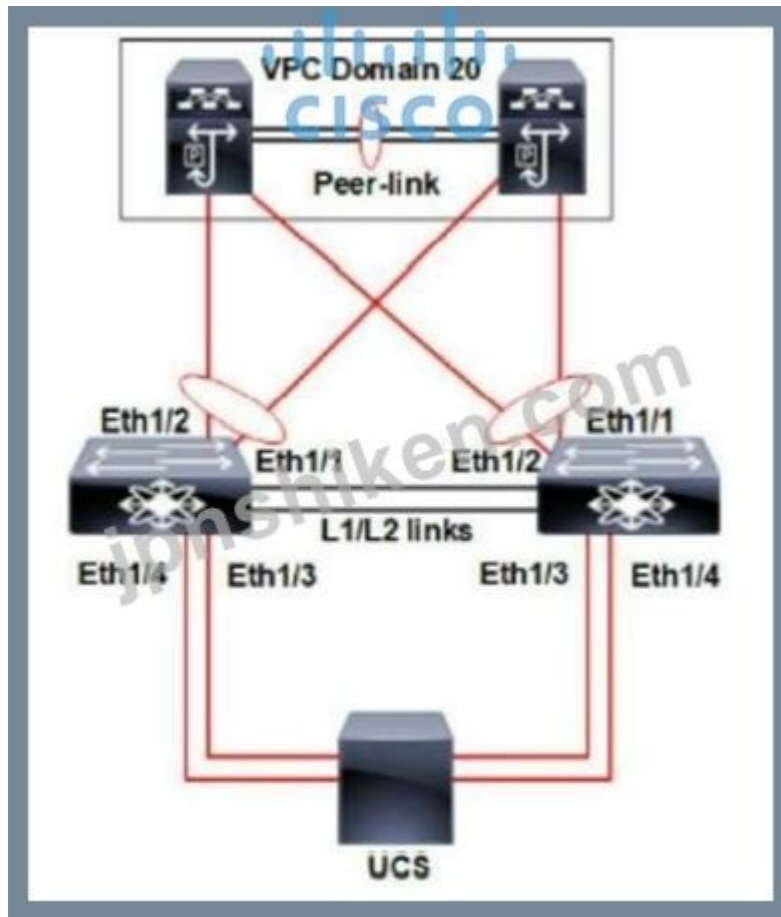
feature-set hsrp  
interface vlan100  
ip address 10.1.1.2 255.255.255.0  
priority 110  
hsrp version 2  
hsrp 1000  
ip 10.1.1.1

feature-set hsrp  
interface vlan100  
ip address 10.1.1.2 255.255.255.0  
priority 80  
hsrp version 2  
hsrp 1000  
ip 10.1.1.1

- A. オプションD
- B. オプションB
- C. オプションC
- D. オプションA

正解: D ([コメントを发表する](#))

質問: 119



図を参照してください。2台のCisco NexusスイッチがvPCを構成しています。既存のCisco UCSドメインに新しいシャーシが追加されます。新しいシャーシを検出し、シャーシからLANネットワークへのすべてのリンクを確立する必要があります。これらの要件を満たす一連のアクションはどれですか？

- Set the chassis discovery policy action to four links.  
Configure Eth1/3 and Eth1/4 as server ports.  
Acknowledge the chassis.
- Set the chassis discovery policy action to four links.  
Configure Eth1/1 and Eth1/2 as uplink Fibre Channel ports.  
Set the link group preference to None.
- Set the chassis discovery policy action to one link.  
Configure Eth1/1 and Eth1/2 as uplink Ethernet ports.  
Set the link group preference to Port Channel.
- Set the chassis discovery policy action to one link.  
Configure Eth1/3 and Eth1/4 as server ports.  
Acknowledge the chassis.



- A. オプションB
- B. オプションA
- C. オプションC
- D. 選択肢D

正解: **C** ([コメントを发表する](#))

質問: 120

エンジニアは、週末のメンテナンス期間中に Cisco UCS Manager のバックアップとリストアを設定する必要があります。設定は月曜日の朝に元の状態に復元されなければなりません。エンドユーザーはサービスプロファイルの設定のみを変更できます。これらの要件を満たすアクションはどれですか？

- A. 毎週週末の開始時にシステムバックアップを実行するようにスケジュールし、月曜日の朝にバックアップを手動でインポートします。
- B. 毎週週末の開始時に論理バックアップを実行するようにスケジュールし、月曜日の朝にバックアップのインポートを実行するようにスケジュールします。
- C. 毎週週末の開始時に論理バックアップを実行するようにスケジュールし、月曜日の朝にバックアップを手動でインポートします。
- D. 毎週週末の開始時にシステムバックアップを実行するようにスケジュールし、月曜日の朝にバックアップのインポートを実行するようにスケジュールしてください。

正解: [\(正解を表示します\)](#)

質問: 121

展示資料を参照してください。

```
ACI-Leaf1# show ip route vrf DATACENTER:DC
10.20.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
  *via 10.0.8.65%overlay-1, [1/0], 4w3d, static
172.16.100.0/24, ubest/mbest: 1/0
  *via 10.1.168.95%overlay-1, [200/5], 3wod, bgp-132, internal, tag 132 (mpls-vpn)
172.16.99.0/24, ubest/mbest: 1/0
  *via 10.0.1.14, [20/0], 3wod, bgp-132, external, tag 200
```

リーフスイッチのルーティングテーブルに関する記述のうち、正しいものはどれですか？ 2つ選択してください。

- A. ルート 10.20.1.0/24 のネクストホップ 10.0.8.65 は、ACI の境界リーフの TEP アドレスです。
- B. 10.20.1.0/24 は ACI の BD サブネットです。
- C. ルート 172.16.100.0/24 のネクストホップ 10.1.168.95 は、ACI の境界リーフの TEP アドレスです。
- D. ルート 172.16.99.0/24 のネクストホップ 10.0.1.14 は、ACI の境界リーフの TEP アドレスです。
- E. 172.16.100.0/24 は ACI の BD サブネットです。

正解: [\(正解を表示します\)](#)

有効的な350-601問題集はJPNTTest.com提供され、350-601試験に合格することに役に立ちます！JPNTTest.comは今最新350-601試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで350-601問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> 384問、30%ディスカウント、特別な割引コード:

**JPNshiken**

質問: 122

エンジニアが仮想化サーバーと Cisco Nexus 5500 シリーズスイッチ間の VNTag を設定しています。設定手順をドラッグ アンド ドロップして、右側の正しい順序に並べ替えてください。

Configure support for VNTag mode on the interface that connects to the server.	Step 1
Configure the vNICs of the server.	Step 2
Configure the server to support NIV mode.	Step 3
Enable the virtualization feature set.	Step 4
Configure the port profile.	Step 5
Install the virtualization feature set.	Step 6

正解:

Configure support for VNTag mode on the interface that connects to the server.	Install the virtualization feature set.
Configure the vNICs of the server.	Enable the virtualization feature set.
Configure the server to support NIV mode.	Configure the port profile.
Enable the virtualization feature set.	Configure support for VNTag mode on the interface that connects to the server.
Configure the port profile.	Configure the server to support NIV mode.
Install the virtualization feature set.	Configure the vNICs of the server.

Explanation:

仮想化機能セットをインストールします

仮想化機能セットを有効にする

ポートプロファイルを設定します

サーバーに接続するインターフェースで、VNTagモードのサポートを設定します。

NIVモードをサポートするようにサーバーを設定します。

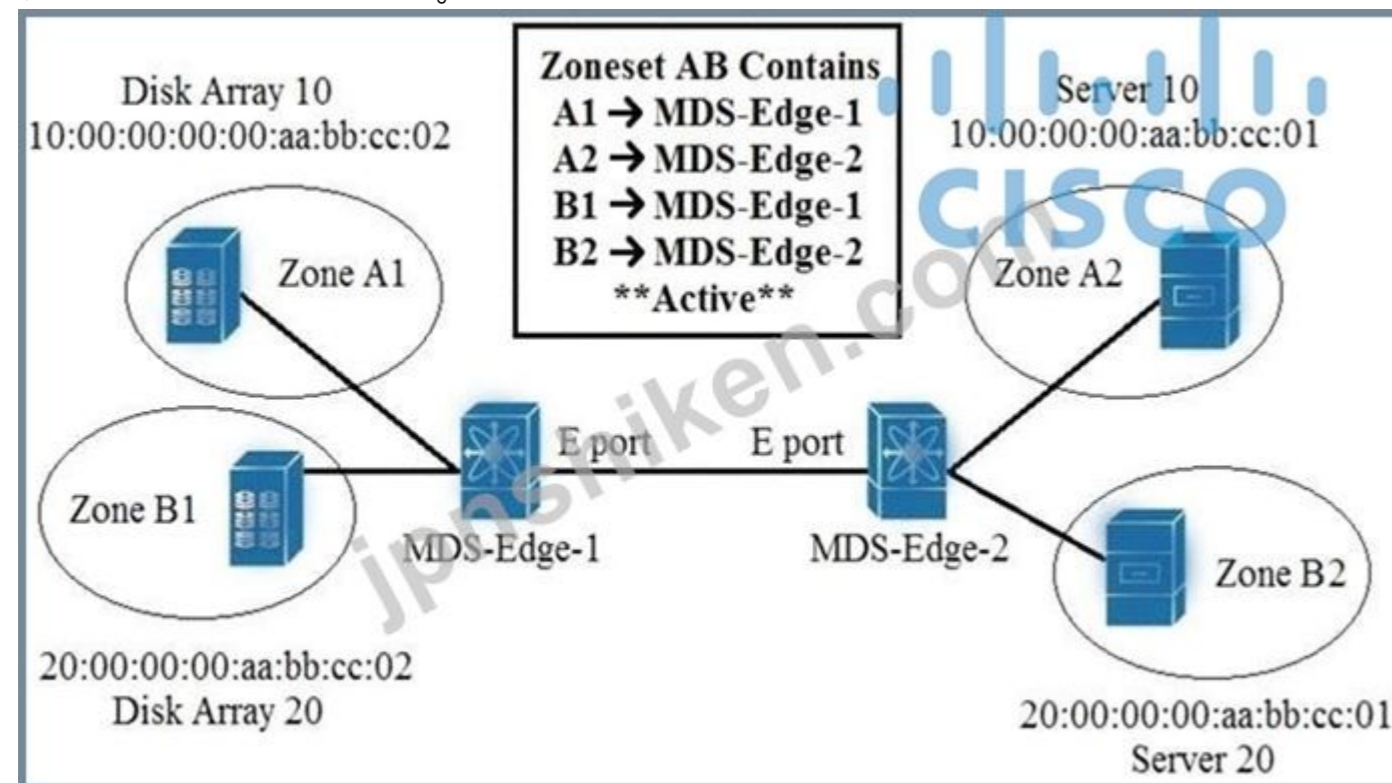
サーバーのvNICを設定する

<https://www.cisco.com/c/en/us/support/docs/switches/nexus-5000-series-switches/117691-config-5500switch-00.html>

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5500/sw/adaptor-fex/6x/b\\_5500\\_Adapter\\_FEX\\_Config\\_6x/b\\_5500\\_Adapter\\_FEX\\_Config\\_602N11\\_chapter\\_010.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5500/sw/adaptor-fex/6x/b_5500_Adapter_FEX_Config_6x/b_5500_Adapter_FEX_Config_602N11_chapter_010.html)

質問: 123

展示資料を参照してください。



エンジニアが2台のCisco MDSスイッチにゾーニングを実装しています。実装完了後、2台のCisco MDSスイッチを接続するEポートが分離されてしまいました。この実装の何が問題なのでしょう？

- A. ゾーニングを機能させるには、両方のMDSスイッチのEポートをFポートとして構成する必要があります。
- B. Eポートが機能するためには、両方のMDSスイッチでゾーン名が同じである必要があります。
- C. ゾーンはMDSスイッチにローカルであり、Eポート間の接続を有効にするには名前サービスを使用する必要があります。
- D. 両方のMDSスイッチで異なるゾーンセット名を設定する必要があります。

正解: [\(正解を表示します\)](#)

質問: 124

Cisco Nexus 7000 シリーズ スイッチのシャーシを交換した後、管理者は、vPC が有効になっているすべての LACP ポート チャンネルが再初期化されていることを発見しました。管理者は、次回シャーシを交換する際にこの問題を回避したいと考えています。隔離されたデバイスを再起動する前に、この要件を満たすために実行する必要がある 2 つのアクションは何ですか？

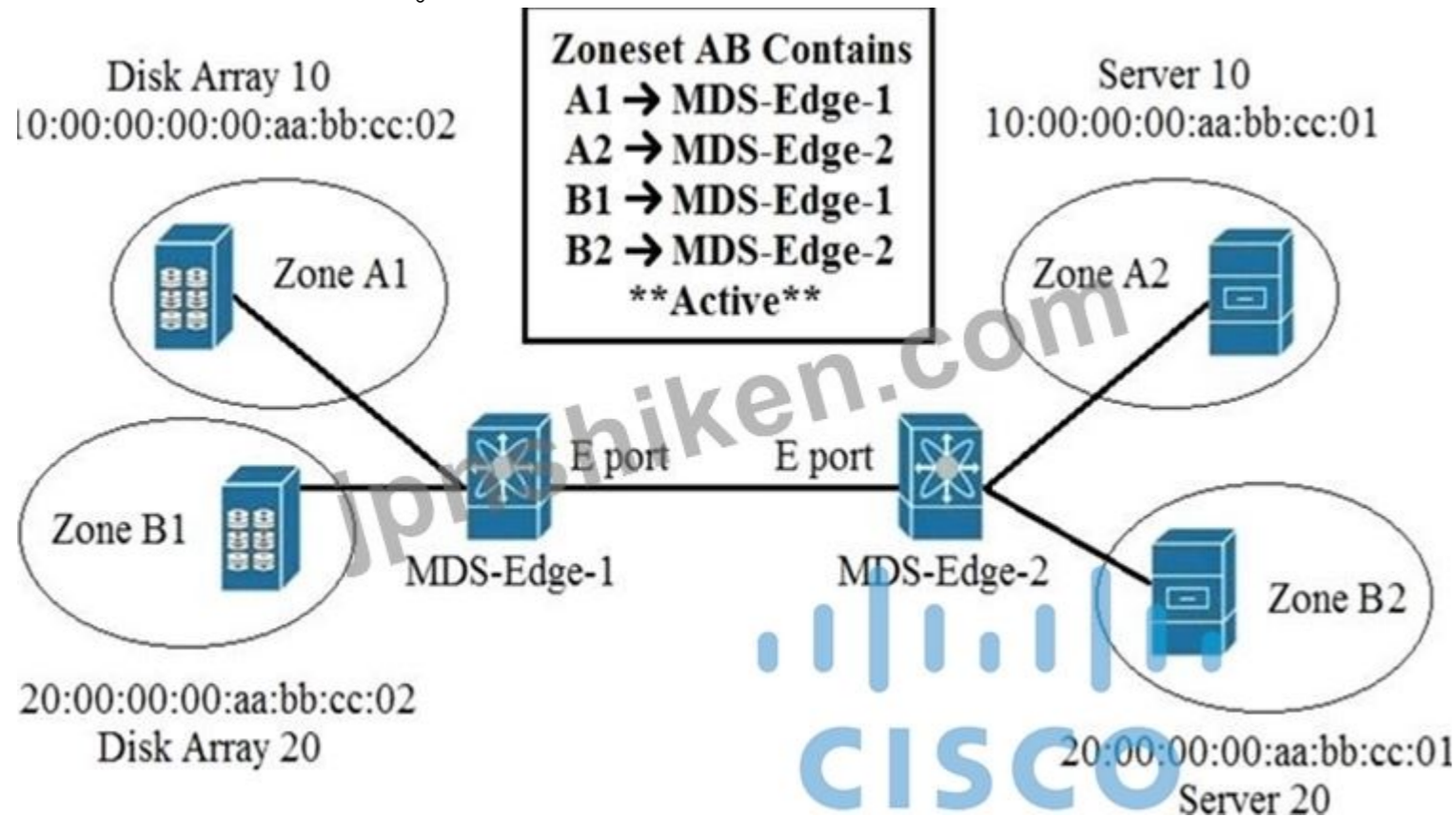
(2つ選択)

- A. 交換用シャーシのvPCシステム優先度をピアよりも高い値に変更します。
- B. vPC MACアドレスをピアよりもタワ一値に設定します
- C. 交換用シャーシのvPCシステム優先度をピアよりも低い値に変更します。
- D. vPC MACアドレスをピアよりも高い値に設定する
- E. 両方のピアで自動復旧を無効状態に設定する

正解: (正解を表示します)

質問: 125

展示資料を参照してください。



エンジニアが2台のCisco MDSスイッチにゾーニングを実装しています。実装完了後、2台のCisco MDSスイッチを接続するEポートが分離されてしまいました。この実装の何が問題なのでしょう？

- A. ゾーニングを機能させるには、両方のMDSスイッチのEポートをFポートとして構成する必要があります。
- B. 両方のMDSスイッチで異なるゾーンセット名を設定する必要があります。
- C. Eポートが機能するためには、両方のMDSスイッチでゾーン名が同じである必要があります。
- D. ゾーンはMDSスイッチにローカルであり、Eポート間の接続を有効にするには名前サービスを使用する必要があります。

正解: C (コメントを发表する)

ファブリック内の2つのスイッチがTEポートまたはEポートを使用して統合されている場合、2つのスイッチまたはファブリック間でアクティブゾーンセットデータベースが異なると、これらのTEポートとEポートが分離される可能性があります。

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6\\_2/configuration/guides/fabric/nxos/nx\\_os\\_fabric/zone.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6_2/configuration/guides/fabric/nxos/nx_os_fabric/zone.html)

質問: 126

サーバーに新しいCisco IMCソフトウェアをインストールするには、どのサーバーポリシーを使用しますか？

- A. ホストファームウェアポリシー
- B. ハイパーバイザーファームウェアポリシー

C. BIOSソフトウェアポリシー

D. Cisco IMCソフトウェアポリシー

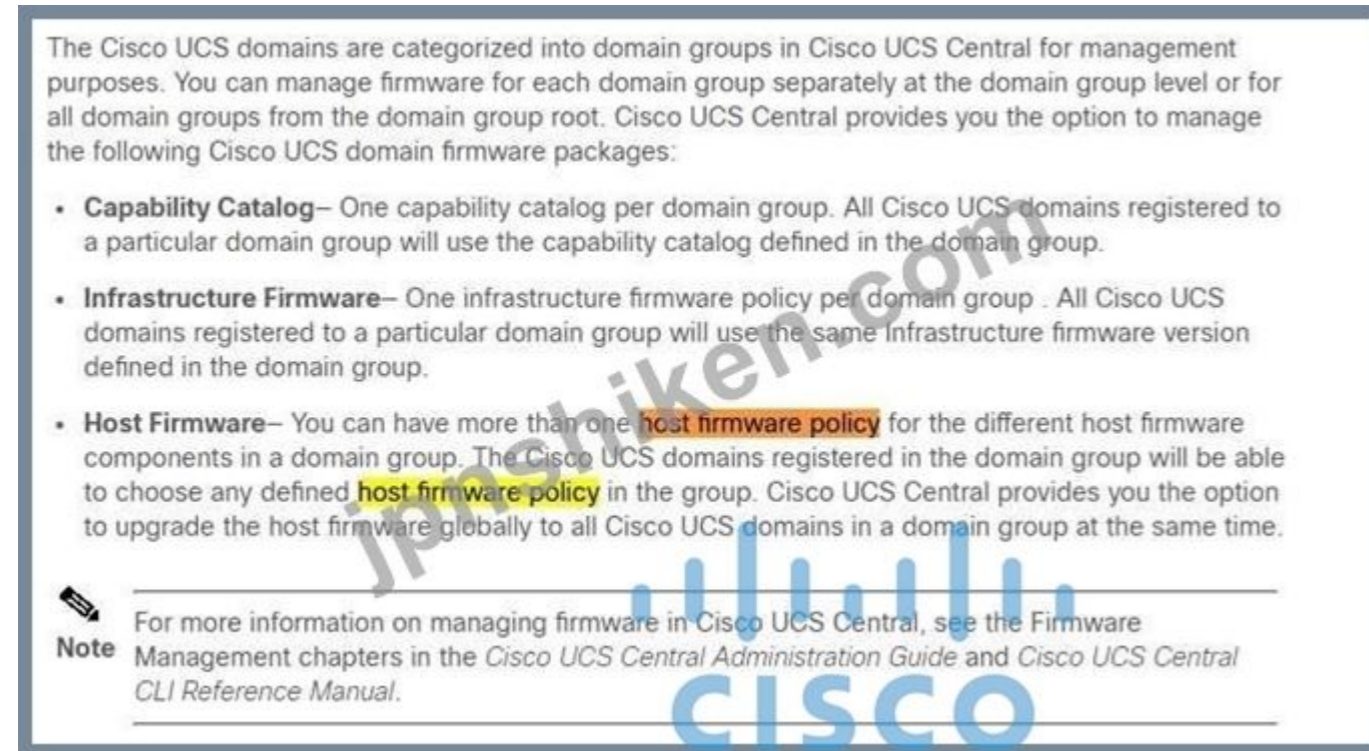
正解: **A** ([コメントを发表する](#))

説明

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/ucs-manager/CLI-User-Guides/Firmware-Mgmt/4-0/b\\_UCSM\\_CLI\\_Firmware\\_Management\\_Guide\\_4-0/](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/CLI-User-Guides/Firmware-Mgmt/4-0/b_UCSM_CLI_Firmware_Management_Guide_4-0/)

[b\\_UCSM\\_CLI\\_Firmware\\_Management\\_Guide\\_4-0\\_chapter\\_01.html#](#) ホストファームウェアパッケージを使用するには、更新テンプレートであるサービスプロファイルテンプレートの属性としてホストファームウェアポリシーを定義します。サービスプロファイルテンプレートに加えられた変更は、インスタンス化されたサービスプロファイルに自動的に反映されます。その後、サービスプロファイルに関連付けられたサーバーもファームウェアバージョンと並行してアップグレードされます。

グラフィカルユーザーインターフェース、テキスト、アプリケーションの説明は自動的に生成されます



The Cisco UCS domains are categorized into domain groups in Cisco UCS Central for management purposes. You can manage firmware for each domain group separately at the domain group level or for all domain groups from the domain group root. Cisco UCS Central provides you the option to manage the following Cisco UCS domain firmware packages:

- **Capability Catalog**— One capability catalog per domain group. All Cisco UCS domains registered to a particular domain group will use the capability catalog defined in the domain group.
- **Infrastructure Firmware**— One infrastructure firmware policy per domain group. All Cisco UCS domains registered to a particular domain group will use the same Infrastructure firmware version defined in the domain group.
- **Host Firmware**— You can have more than one **host firmware policy** for the different host firmware components in a domain group. The Cisco UCS domains registered in the domain group will be able to choose any defined **host firmware policy** in the group. Cisco UCS Central provides you the option to upgrade the host firmware globally to all Cisco UCS domains in a domain group at the same time.

**Note** For more information on managing firmware in Cisco UCS Central, see the Firmware Management chapters in the *Cisco UCS Central Administration Guide* and *Cisco UCS Central CLI Reference Manual*.

質問: 127

ネットワークエンジニアは、Cisco UCS Managerに構成バックアップポリシーを展開する必要があります。このバックアップから生成されるファイルには、災害復旧時にシステムを復元するために使用する、システム全体のスナップショットが含まれている必要があります。バックアップファイルは、TCPプロトコルを使用して安全でない方法で転送する必要があります。これらの要件を満たす構成バックアップ設定はどれですか？

A. タイプ :システム構成

プロトコル: TFTP

B. タイプ: 全構成

プロトコル: SCP

C. タイプ :フルステート

プロトコル: FTP

D. タイプ : 論理構成

プロトコル: SFTP

正解: ([正解を表示します](#))

質問: 128

展示資料を参照してください。

```
ACI-Leaf1# show ip route vrf DATACENTER:DC
10.20.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
  *via 10.0.8.65%overlay-1, [1/0], 4w3d, static
172.16.100.0/24, ubest/mbest: 1/0
  *via 10.1.168.95%overlay-1, [200/5], 3wod, bgp-132, internal, tag 132 (mpls-vpn)
172.16.99.0/24, ubest/mbest: 1/0
  *via 10.0.1.14, [20/0], 3wod, bgp-132, external, tag 200
```

リーフスイッチのルーティングテーブルに関する記述のうち、正しいものはどれですか？ (2つ選択してください。)

- A. ルート 172.16.99.0/24 のネクストホップ 10.0.1.14 は、ACI の境界リーフの TEP アドレスです。
- B. 10.20.1.0./24 は ACI の BD サブネットです。
- C. ルート 172.16.100.0/24 のネクストホップ 10.1.168.95 は、ACI の境界リーフの TEP アドレスです。
- D. 172.16.100.0/24 は ACI の BD サブネットです。
- E. ルート 10.20.1.0./24 のネクストホップ 10.0.8.65 は、ACI の境界リーフの TEP アドレスです。

正解: ([正解を表示します](#))

質問: 129

小規模なリモートオフィスがNSSA ASBR経由で地域ハブサイトに接続するように設定されています。リモートオフィスのOSPFエリアには、どのタイプのLSAが送信されますか？

- A. タイプ7 LSA
- B. タイプ3 LSA
- C. タイプ1 LSA
- D. タイプ5 LSA

正解: ([正解を表示します](#))

説明

質問: 130

ドラッグアンドドロップ問題

ネットワークエンジニアは、Cisco MDS 9000シリーズマルチレイヤースwitchにRBACを実装する必要があります。

左側のCisco MDS 9000シリーズの役割を、右側の適切なカテゴリにドラッグアンドドロップしてください。

san-operator	System Defined
global-admin	
server-admin	
storage-admin	
network-admin	User Defined
network-operator	

正解:

System Defined
network-admin
network-operator
server-admin

User Defined
san-operator
storage-admin
global-admin

Explanation:

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Management/3-1/b\\_Cisco\\_UCS\\_Admin\\_Mgmt\\_Guide\\_3\\_1/b\\_UCSM\\_Admin\\_Mgmt\\_Guide\\_chapter\\_01.html](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Management/3-1/b_Cisco_UCS_Admin_Mgmt_Guide_3_1/b_UCSM_Admin_Mgmt_Guide_chapter_01.html)

質問: 131

ネットワークエンジニアは、ユーザーがCisco Nexusスイッチに設定を保存した際に、実行中の設定のコピーをブートフラッシュに保存し、syslogにメッセージを書き込むEEMスクリプトを作成する必要があります。このタスクを完了するには、どの設定セットを適用すればよいでしょうか？

- event manager applet local- backup  
event cli match "copy running-config startup-config"  
action 1 cli copy running-config bootflash:/current\_config.txt  
action 2 syslog msg Configuration saved and copied to bootflash
- event manager applet local- backup  
event cli match "write memory"  
action 1 cli copy running-config bootflash:/current\_config.txt  
action 2 snmp-trap strdata "Configuration saved and copied to bootflash"
- event manager applet local- backup  
event cli match "copy running-config startup-config"  
action 1 cli copy running-config bootflash:/current\_config.txt  
action 2 syslog msg Configuration saved and copied to bootflash  
action 3 event-default
- event manager applet local- backup  
event cli match "write memory"  
action 1 cli copy running-config bootflash:/current\_config.txt  
action 2 syslog msg Configuration saved and copied to bootflash  
action 3 event-default

- A. オプションC
- B. オプションB
- C. オプションA
- D. 選択肢D

正解: ([正解を表示します](#))

NX-OSでは、write memoryコマンドは無効です。

「イベントデフォルト」

If you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the default action. For example, if you match a CLI command in a match statement, you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute.

#### 質問: 132

エンジニアは、仮想ポートチャネルを実行している2台のCisco Nexus 9000シリーズスイッチでHSRPプロトコルを設定する必要があります。さらに、HSRPの実装は以下の要件を満たす必要があります。

\* 500以上のグループを登録できる必要があります。

\* スイッチ1はプライマリスイッチとして動作する必要があります。

\* 両方のスイッチは、ユーザー定義のハードウェアアドレスを使用する必要があります。

右側のコマンドをドラッグ&ドロップして、左側のHSRP設定を完了してください。コマンドは複数回使用されます。すべてのコマンドが使用されるわけではありません。

```

! switch1
interface vlan300
ip 209.165.200.226/27
hserp 300
[ ]
[ ]
ip 209.165.200.225
[ ]

! switch2
interface vlan300
ip 209.165.200.227/27
hserp 300
[ ]
[ ]
ip 209.165.200.225
[ ]

```

mac-address 6000.6000.6000

hserp version 1

priority 255

hserp use-bia

priority 100

hserp version 2

正解:

```

! switch1
interface vlan300
ip 209.165.200.226/27
hserp 300
[ hserp version 2 ]
[ priority 100 ]
ip 209.165.200.225
[ mac-address 6000.6000.6000 ]

! switch2
interface vlan300
ip 209.165.200.227/27
hserp 300
[ hserp version 2 ]
[ priority 255 ]
ip 209.165.200.225
[ mac-address 6000.6000.6000 ]

```

mac-address 6000.6000.6000

hserp version 1

priority 255

hserp use-bia

priority 100

hserp version 2

Explanation:

スイッチ1 :

ボックス1 = HSRPバージョン2

ボックス2 = 優先度100

ボックス3 = MACアドレス 6000.6000.6000

スイッチ2 :

ボックス1 = HSRPバージョン2

ボックス2 = 優先度255

ボックス3 = MACアドレス 6000.6000.6000

**質問: 133**

展示資料を参照してください。

python Code:

```
import requests
import json

url='http://lab-93180bdlf-sw1/ins'
switchuser='dazfre'
switchpassword='Clscorox0'

myheaders={'content-type' 'application/json'})
payload={
  "ins_api": {
    "version": "1.0",
    "type": "cli_show",
    "chunk": "0",
    "sid": "1",
    "input": "configure terminal : feature hsrp",
    "output_format": "json"
  }
}
response = requests post(url,data=json.dumps(payload),
headers=myheaders,auth=(switchuser,switchpassword))

print(response.text)
```

ERROR MESSAGE

```
{
  "ins_api" [
    "type": "cli_show"
    "version": "1.0",
    "sid": "eoc",
    "outputs", [
      "output" [{
        "clierror" "% invalid command\n",
        "input" "configure terminal"
        "msg" "input CLI command error",
        "code" "400"
      }],{
        "clierror" "% invalid command\n",
        "input" "feature hsrp",
        "msg" "input CLI command error",
        "code" "400"
      }
    ]
  ]
}
```

Cisco NX-API用のPythonコードがエラーメッセージを表示するのはなぜですか？

- A. リクエストのヘッダーの type]が間違っており、cli\_conf]であるべきです。
- B. NX-API では、リクエスト モジュールを介した機能の設定はできません。
- C. type]が間違っています。リクエストの本文であり、cli\_conf]であるべきです。
- D. JSONはNX-APIでサポートされている形式ではありません。



正解: ([正解を表示します](#))

異なるメッセージタイプに属するコマンドを混在させてはいけません。例えば、showコマンドはcli\_showメッセージタイプであり、cli\_confモードではサポートされていません。」

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/programmability/guide/cisco\\_nexus7000\\_programmability\\_guide\\_8x/b-cisco-nexus7000-programmability-guide-8x\\_chapter\\_011.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/programmability/guide/cisco_nexus7000_programmability_guide_8x/b-cisco-nexus7000-programmability-guide-8x_chapter_011.html)

リクエスト本文中のペイロード「type」の値が間違っています。リクエストを正常に処理するには、「cli\_conf」に変更する必要があります。

例えば、更新されたペイロードを使用して同じリクエストを実行すると次のようになります。

```
{
  "ins_api": {
    "version": "1.0",
    "type": "cli_conf",
    "sid": "0",
    "input": "configure terminal ;feature hsrp",
    "output_format": "json"
  }
}
```

200番のレスポンスを受け取りました。

```
{
  "ins_api": {
    "sid": "eoc",
    "type": "cli_conf",
    "version": "1.0",
    "output": {
      "code": "200",
      "msg": "成功"
    }
  }
}
```

CLI検証:

```
nxos9kv# sh run | inc hsrp
```

## HSRP機能

### 質問: 134

ネットワーク管理者は、10.0.0.0/8サブネット内のすべてのIPアドレスに対してpingを実行するプロセスを自動化する必要があります。

サブネットは既にCisco NexusスイッチのARPテーブルに登録されています。目的の出力を生成するために、bashコマンドをドラッグアンドドロップしてください。すべてのコマンドを使用するわけではありません。

```
bash-4.3# | grep '^10\.' | | |
--- 10.1.0.2 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
--- 10.1.0.77 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
```

awk '{print "ping " \$1}' | egrep "statistics|loss" | grep -v "statistics|loss" | sed -e 's/ping /10./g'

show ip arp | vsh | vsh -c "show ip arp"

### 正解:

```
bash-4.3# | vsh | grep '^10\.' | vsh -c "show ip arp" | sed -e 's/ping /10./g' | awk '{print "ping " $1}'
--- 10.1.0.2 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
--- 10.1.0.77 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
```

awk '{print "ping " \$1}' | egrep "statistics|loss" | grep -v "statistics|loss" | sed -e 's/ping /10./g'

show ip arp | vsh | vsh -c "show ip arp"

### 説明

グラフィカルユーザーインターフェース、テキスト、アプリケーションの説明は自動的に生成されます

```
bash-4.3# | vsh | grep '^10\.' | vsh -c "show ip arp" | sed -e 's/ping /10./g' | awk '{print "ping " $1}'
--- 10.1.0.2 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
--- 10.1.0.77 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
```

egrep "statistics|loss" | grep -v "statistics|loss"

show ip arp

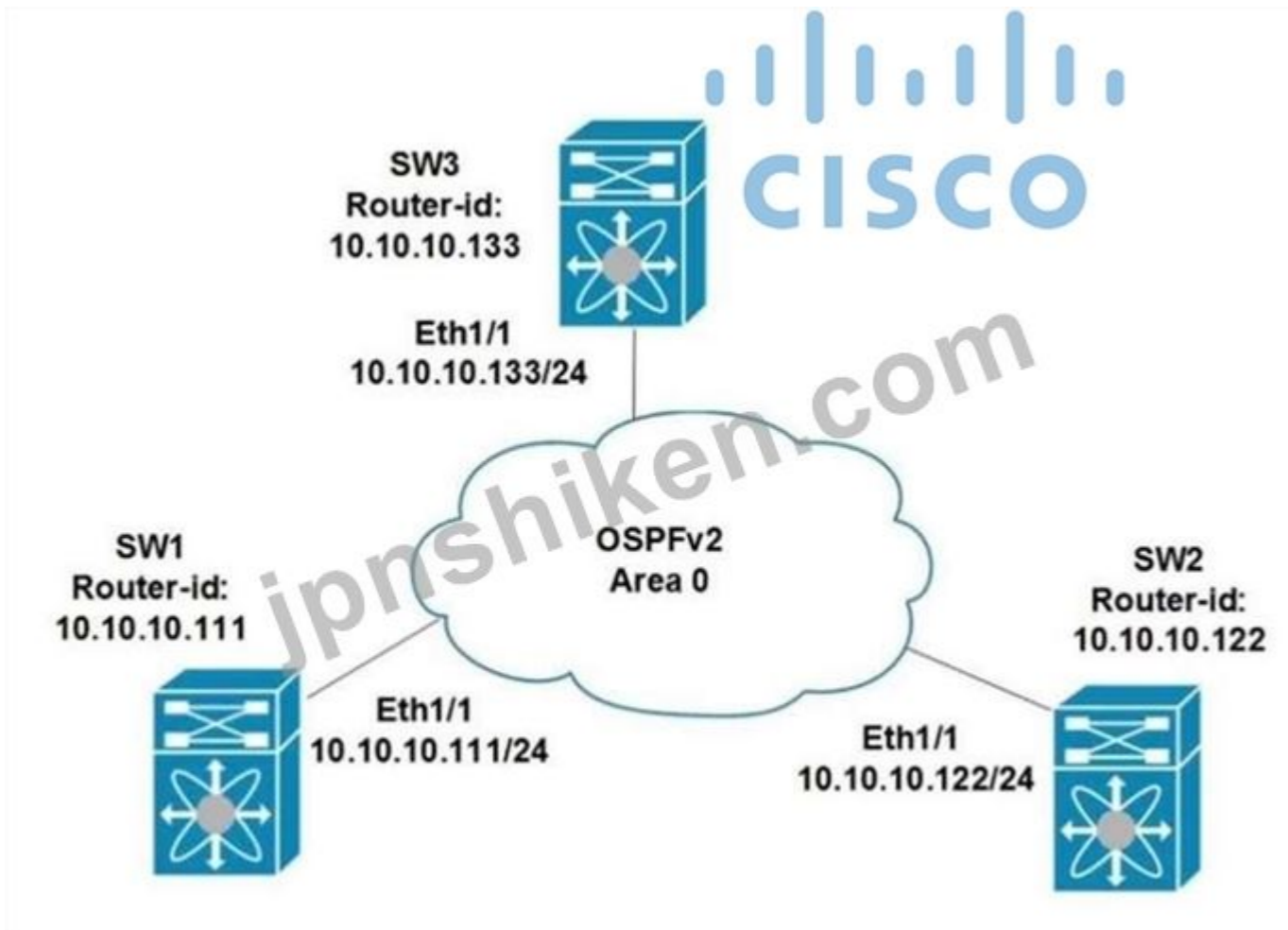
### 質問: 135

エンジニアがNexus 5000シリーズスイッチでSPAN設定を実装します。SPANセッション設定を完了するために必要なコマンドはどれですか？ (2つ選択してください)

```
N5K-Core# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
N5K-Core(config)# interface fo2/1
N5K-Core(config-if)# switchport speed 4000
N5K-Core(config-if)# no shutdown
N5K-Core(config)# interface fo2/2
N5K-Core(config-if)# no shutdown
N5K-Core(config)# monitor session 1
N5K-Core(config-monitor)# source interface fo2/1
N5K-Core(config-monitor)# destination interface fo2/2
N5K-Core(config-monitor)# no shutdown
```

- A. インターフェイスfc2/1の下でスイッチポートモードSDを設定します。
  - B. インターフェイスfc2/2でスイッチポートモードSDを設定します。
  - C. インターフェイスfc2/2の下でスイッチポート速度4000を設定します。
  - D. モニターセッション1の下でセッションタイプfcを設定します。
  - E. インターフェイスfc2/2でスイッチポートモニターを設定します。
- 正解: [\(正解を表示します\)](#)

質問: 136



図を参照してください。すべてのスイッチはデフォルトのOSPF優先度で設定されています。SW2 Cisco NexusスイッチがLSAフラッドを制御し、OSPFv2エリア内の残りのノードにネットワークをアドバタイズするには、どの設定を適用する必要がありますか？

- A. SW2# ターミナルを設定  
SW2 (config)# interface ethernet 1/1  
SW2 (config-if)# ip ospf priority 255

**B. SW2# ターミナルの設定**

```
SW2 (config)# interface ethernet 1/1
```

```
SW2 (config-if)# ip ospf priority 1
```

**C. SW2# ターミナルを設定**

```
SW2 (config)# router ospf 1
```

```
SW2 (config-router)# router-id 10.10.10.22
```

**D. SW2# ターミナルの設定**

```
SW2 (config)# interface ethernet 1/1
```

```
SW2 (config-if)# ip ospf priority 0
```

正解: [\(正解を表示します\)](#)

セクション: ネットワーク

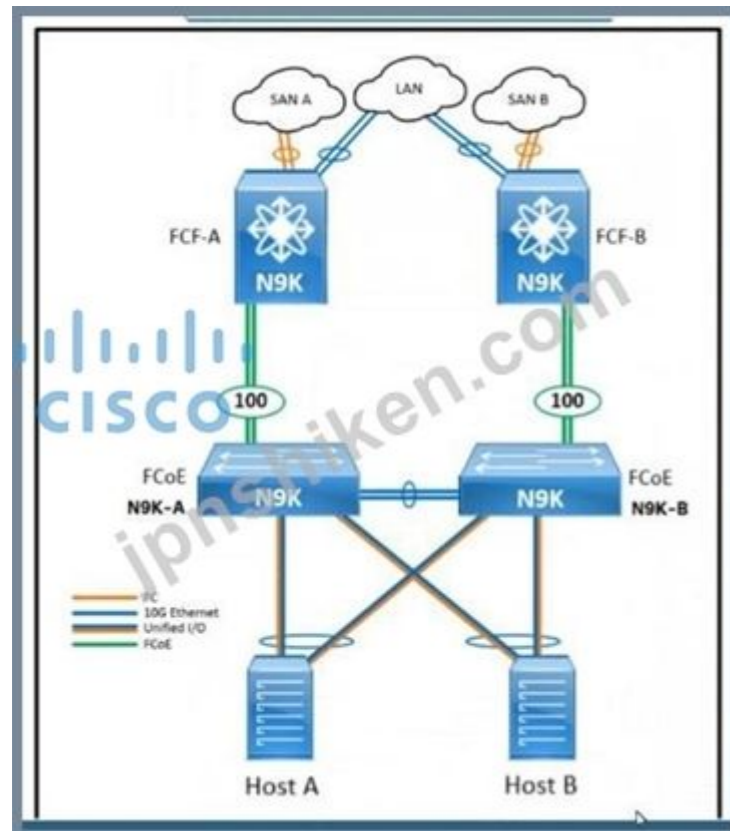
説明/参考資料:

[https://www.cisco.com/c/m/en\\_us/techdoc/dc/reference/cli/nxos/commands/ospf/ip-ospf-priority.html](https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/ospf/ip-ospf-priority.html)

有効的な**350-601**問題集はJPNTTest.com提供され、**350-601**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-601**試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで**350-601**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> **384**問、**30%ディスカウント**、特別な割引コード:

**JPNshiken**」

質問: 137



図を参照してください。エンジニアは、N9K-AスイッチとFCF-A Nexusの間でFCoEを設定する必要があります。

9000コアスイッチ。この導入事例には以下の特徴があります。

- \* N9K-AおよびN9K-Bトップオブラックスイッチは、コアスイッチのドメインIDを共有します。
  - \* ホストには統合型ネットワークアダプタが搭載されています。
  - \* ポートチャンネル100を通過することが許可されているVSANはVSAN 20のみです。
- N9K-AデバイスでFCoE構成を完了するには、どの構成を使用しますか？

- N9K-A(config)# feature fcoe  
N9K-A(config)# feature npv  
N9K-A(config)# interface vfc 100  
N9K-A(config-if)# bind interface port-channel 100  
N9K-A(config-if)# switchport mode F  
N9K-A(config-if)# switchport trunk allowed vsan 20
- N9K-A(config)# feature fcoe  
N9K-A(config)# feature npv  
N9K-A(config)# interface vfc 100  
N9K-A(config-if)# bind interface port-channel 100  
N9K-A(config-if)# switchport mode N  
N9K-A(config-if)# switchport trunk allowed vsan 1, 20
- N9K-A(config)# feature-set fcoe-npv  
N9K-A(config)# interface vfc-port-channel 100  
N9K-A(config-if)# switchport mode NP  
N9K-A(config-if)# switchport trunk allowed vsan 20
- N9K-A(config)# feature-set fcoe-npv  
N9K-A(config)# interface vfc-port-channel 100  
N9K-A(config-if)# switchport mode E  
N9K-A(config-if)# switchport trunk allowed vsan 1, 20

- A. オプションA
- B. オプションB
- C. オプションC
- D. 選択肢D

正解: [\(正解を表示します\)](#)

指定された特性を持つ N9K-A スイッチと FCF-A Nexus 9000 コアスイッチ間で FCoE を構成するには、FCoE NPV モードを有効にし、インターフェイスをポートチャンネルにバインドし、トランク上で VSAN 20 のみを許可する構成が正しいです。提供された CLI 構成に基づくと、スイッチを NPV モードに設定し、VSAN 20 のみを許可するオプション D が正解です。

質問: 138

展示資料を参照してください。

```
switch(config)# feature dhcp
switch(config)# ip dhcp snooping
switch(config)# service dhcp
switch(config)# ip dhcp snooping vlan 100,200,250-252
switch(config)# ip dhcp relay information option
```

リレーエージェントがDHCP BOOTREQUESTパケットをDHCPサーバーに転送することを確実にするために、どのような措置が取られますか？

- A. DHCPサーバーのインターフェイスを信頼されていないものとして設定します。
- B. DHCPサーバーのIPアドレスを設定します。
- C. DHCPリレーエージェントを有効にします。
- D. DHCPスヌーピングのバインディングを確認します。

正解: [\(正解を表示します\)](#)

スイッチでDHCPリレーエージェントを有効にすると、クライアントとDHCPサーバーが同じ物理サブネット上にない場合でも、クライアントからDHCP BOOTREQUESTパケットをDHCPサーバーに転送できるようになります。これは、クライアントがサブネット上に存在しないDHCPサーバーからIPアドレスやその他のネットワーク構成パラメータを取得するために不可欠です。

参考資料 :DHCPリレーエージェントに関する詳細情報は、Cisco Data Center Core Technologies (DCCOR)の学習ガイドまたは資料、特にネットワーク環境におけるDHCPの設定と管理について説明している章に記載されています。

質問: 139

FCoE環境において、PAUSEメカニズムを実装するインターフェースは、どの2つのデータセットに対して常に十分なイングレスバッファをプロビジョニングする必要があるか？ 2つ選択してください

- A. リンクで送信されたが、まだ受信されていないフレーム。
- B. PAUSEフレームが送信機から送信される前に送信機によって処理および送信されたフレーム
- C. リンクで送信され、受信されたフレーム。
- D. 高額なクレジットで送られたフレーム
- E. PAUSEフレームが送信機から送信された後に、送信機によって処理および送信されたフレーム。

正解: [\(正解を表示します\)](#)

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/fcoe/config/cisco\\_nexus7000\\_fcoe\\_config\\_guide\\_8x/configuring\\_fcoe.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/fcoe/config/cisco_nexus7000_fcoe_config_guide_8x/configuring_fcoe.html)

質問: 140

ネットワークエンジニアは、2台のホスト間の通信に影響を与える問題を特定するためにNetFlowを設定しました。ネットワークキャプチャは以下の基準を満たす必要があります。

\*送信元IPアドレス 10.0.0.17

宛先IPアドレス 10.0.200.150

\*10.100.1.15にエクスポートします。

右側のコードスニペットをコード内の空欄にドラッグアンドドロップして、NetFlowの設定を完了してください。

The screenshot shows a configuration window for a flow record named 'RECORD-A'. The code editor on the left contains the following configuration:

```
flow record RECORD-A
 match ipv4 [ ] [ ]
 match ipv4 destination address
 match ip [ ]
 match transport [ ]
 collect timestamp sys-uptime last
 collect transport tcp flags
 collect ip version
!
flow exporter EXPORT-A
 [ ] use-vrf management
 transport udp 3000
 source mgmt0
 version 9
```

On the right side, there is a list of fields to be selected for the flow record:

- destination-port
- address
- source
- destination
- 10.100.1.15
- protocol

正解:

```

flow record RECORD-A
 match ipv4  
 match ipv4 destination address
 match ip 
 match transport 
 collect timestamp sys-uptime last
 collect transport tcp flags
 collect ip version
!
flow exporter EXPORT-A
   use-vrf management
 transport udp 3000
 source mgmt0
 version 9

```

destination-port

address

source

destination

10.100.1.15

protocol

```

flow record RECORD-A
 match ipv4  
 match ipv4 destination address
 match ip 
 match transport 
 collect timestamp sys-uptime last
 collect transport tcp flags
 collect ip version
!
flow exporter EXPORT-A
   use-vrf management
 transport udp 3000
 source mgmt0
 version 9

```

destination-port

2 address

1 source

5 destination

3 10.100.1.15

4 protocol

質問: 141

Cisco Nexusスイッチの汎用オンライン診断ポリシーでは、PortLoopbackテストにおいて、ポートをエラー無効にするには10回連続で失敗する必要があります。お客様はこれを5回連続の失敗に変更したいと考えています。モジュール1のみに変更を適用する設定はどれですか？

```

● Nexus(config)# event manager applet custom-PortLoopback override __PortLoopback
Nexus(config-applet)# event gold mod all test PortLoopback testing-type bootup consecutive-failure 5
Nexus(config-applet)# action 1 publish-event

● Nexus(config)# event manager applet custom-PortLoopback override __PortLoopback
Nexus(config-applet)# event gold mod 1test PortLoopback testing-type bootup consecutive-failure 5
Nexus(config-applet)# action 1 publish-event

● Nexus(config)# event manager applet custom-PortLoopback override __PortLoopback
Nexus(config-applet)# event gold mod all test PortLoopback testing-type monitoring consecutive-failure 5
Nexus(config-applet)# action 1 policy-default

● Nexus(config)# event manager applet custom-PortLoopback override __PortLoopback
Nexus(config-applet)# event gold mod 1 test PortLoopback testing-type monitoring consecutive-failure 5
Nexus(config-applet)# action 1 policy-default

```

- A. オプションD
- B. オプションC
- C. オプションB
- D. オプションA

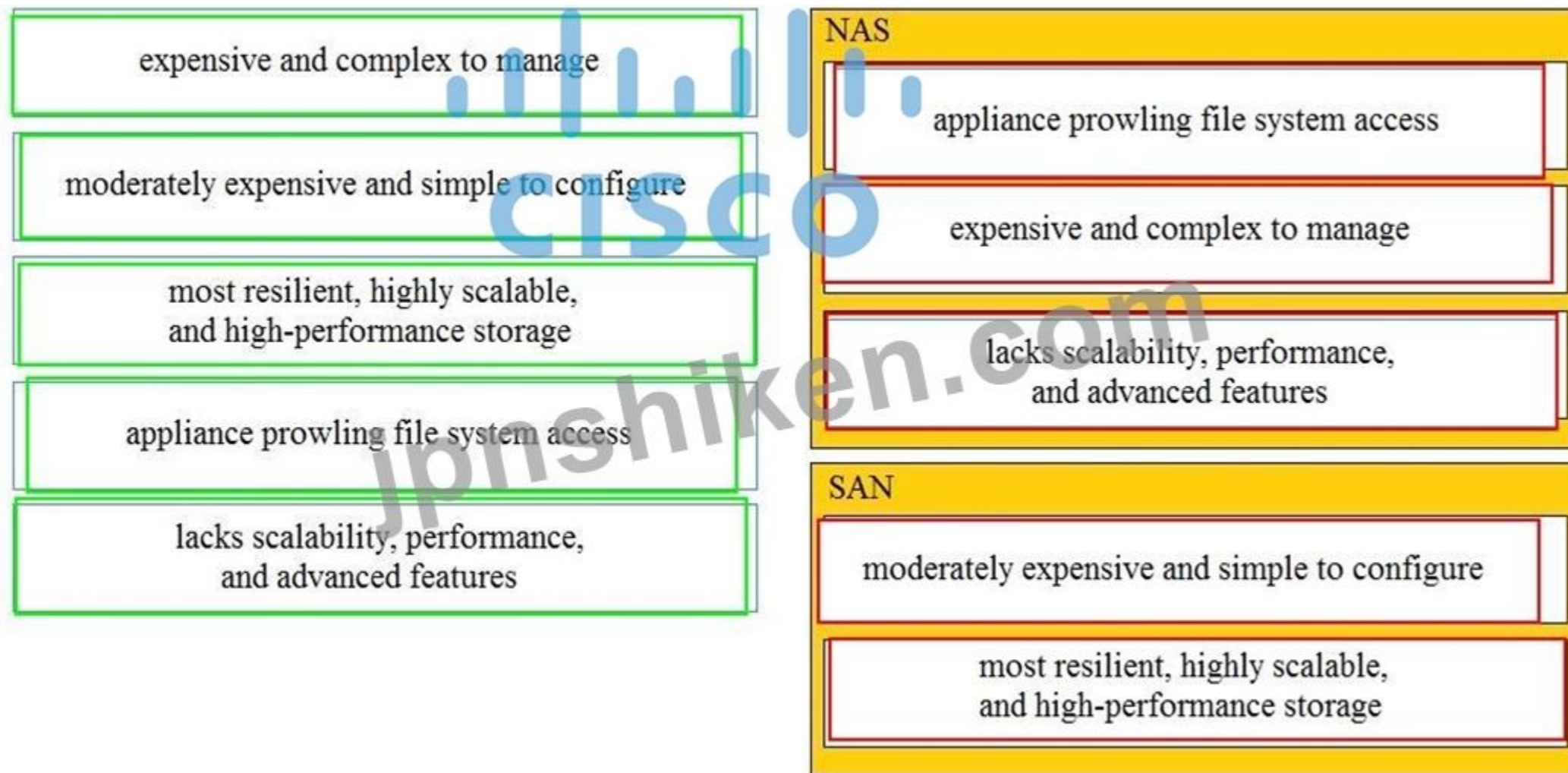
正解: B ([コメントを发表する](#))

質問: 142

左側の特性を、右側の適切なストレージシステムにドラッグ&ドロップしてください。

expensive and complex to manage	<div style="border: 1px solid black; background-color: #ffff00; padding: 5px; margin-bottom: 5px;">NAS</div> <div style="border: 1px solid black; height: 40px; margin-bottom: 5px;"></div> <div style="border: 1px solid black; height: 40px; margin-bottom: 5px;"></div> <div style="border: 1px solid black; height: 40px; margin-bottom: 5px;"></div> <div style="border: 1px solid black; height: 40px; margin-bottom: 5px;"></div> <div style="border: 1px solid black; background-color: #ffff00; padding: 5px; margin-bottom: 5px;">SAN</div> <div style="border: 1px solid black; height: 40px; margin-bottom: 5px;"></div> <div style="border: 1px solid black; height: 40px; margin-bottom: 5px;"></div>
moderately expensive and simple to configure	
most resilient, highly scalable, and high-performance storage	
appliance providing file system access	
lacks scalability, performance, and advanced features	

正解:



質問: 143

ネットワークエンジニアが、Catalystスイッチ上でwrite memoryコマンドを使用して設定を繰り返しNVRAMに保存しています。Nexusスイッチで同じ操作を実行するには、どのような手順を踏むべきでしょうか？

- A. メモリ書き込みコマンドを使用して設定を保存します。
- B. エイリアスコマンドを使用してメモリ書き込みコマンドを使用します。
- C. exitコマンドを使用して設定モードを終了し、設定を自動的に保存します。
- D. wri コマンドを使用して、copy running-config startup-config コマンドを使用します。

正解: [\(正解を表示します\)](#)

Nexusにはデフォルトでは実行中の設定ファイルや起動設定ファイルが存在しません。そのため、それに関連するエイリアスを作成する必要があります。

質問: 144

展示資料を参照してください。

```
N5K-1 (config)#interface fc2/3
N5K-1 (config-if) #switchport mode sd
N5K-1 (config-if) # no shutdown
```

この設定を実装した結果はどうなりますか？

- A. ファイバーチャネルインターフェースは同期配信用に構成されています。

- B. ファイバーチャネルインターフェースはFSPF用に構成されています。
- C. ファイバーチャネルインターフェースはSPAN用に構成されています。
- D. ファイバーチャネルインターフェースは、ソース分配のための構成です。

正解: [\(正解を表示します\)](#)

質問: 145

左側のストレージ技術を、右側の適切な説明にドラッグ&ドロップしてください。

NFSv2	uses client machine authentication
Kerberos	uses users authentication
NFSv4	authenticates clients and servers in NFSv4
RADIUS	authenticates clients to corporate directory systems

正解:

NFSv2	NFSv2
Kerberos	NFSv4
NFSv4	Kerberos
RADIUS	RADIUS

説明



アプリケーションの説明は自動的に生成されました

NFSv4のリリースは、NFSエクスポートにおける認証とセキュリティに革命をもたらしました。NFSv4では、RPCSEC\_GSSカーネルモジュール、Kerberosバージョン5 GSS-APIメカニズム、SPKM-3、およびLIPKEYの実装が必須となっています。NFSv4では、必須のセキュリティメカニズムは、NFSv2やNFSv3で使用されていたクライアントマシンではなく、個々のユーザーの認証に重点を置いています。

[https://web.mit.edu/rhel-doc/5/RHEL-5-manual/Deployment\\_Guide-en-US/s1-nfs-security.html](https://web.mit.edu/rhel-doc/5/RHEL-5-manual/Deployment_Guide-en-US/s1-nfs-security.html)

#### 質問: 146

エンジニアがマルチキャストをサポートするトランスポート上でOTVを実装しようとしています。このソリューションは以下の要件を満たす必要があります。

マルチキャストを使用して、リモートピアとの隣接関係を確立します。

\* VLAN 100 から他のサイトへの OTV アドバタイズメントを有効にします。

これらの要件を満たすために設定すべきコマンドはどれですか？ 2つ選択してください。)

- A. otvサイトVLAN 100
- B. otvデータグループ232.2.2.0/28
- C. otv use-adjacency-server 172.27.255.94
- D. 拡張VLAN 100を開く
- E. otv コントロールグループ 232.1.1.1

正解: ([正解を表示します](#))

説明

[https://www.cisco.com/c/dam/en/us/products/collateral/switches/nexus-7000-series-switches/guide\\_c07-728315](https://www.cisco.com/c/dam/en/us/products/collateral/switches/nexus-7000-series-switches/guide_c07-728315).

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/OTV/config\\_guide/b\\_Cisco\\_Nexus\\_7000\\_S](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/OTV/config_guide/b_Cisco_Nexus_7000_S)

#### 質問: 147

エンジニアは、OTVをサポートするために、同じデータセンター内の2台のCisco Nexus 7000シリーズスイッチを設定する必要があります。どのコマンドセットを使用すると、ジョインインターフェイスの設定が完了しますか？

```
feature otv
otv site-identifier 256
interface overlay 1
otv control-group 239.1.1.1
otv data-group 239.1.1.0/29
otv join-interface ethernet 2/1
otv extend-vlan 5-10
no shutdown
```

A. Edge Device 1  
interface ethernet 2/1  
ip address 192.0.2.1/24  
ip igmp version 3

Edge Device 2  
interface ethernet 2/1  
ip address 192.0.2.16/24  
ip igmp version 3

B. Edge Device 1  
interface ethernet 2/1  
ip address 192.0.2.1/24  
ip igmp version 3  
ip pim sparse-mode

Edge Device 2  
interface ethernet 2/1  
ip address 192.0.2.16/24  
ip igmp version 3  
ip pim sparse-mode

C. Edge Device 1  
interface ethernet 2/1  
ip address 192.0.2.1/24

Edge Device 2  
interface ethernet 2/1  
ip address 192.0.2.16/24

D. Edge Device 1  
interface ethernet 2/1  
ip address 192.0.2.1/24  
ip igmp version 3

Edge Device 2  
interface ethernet 2/1  
ip address 192.0.2.1/24  
ip igmp version 3

A. オプションB

B. オプションA

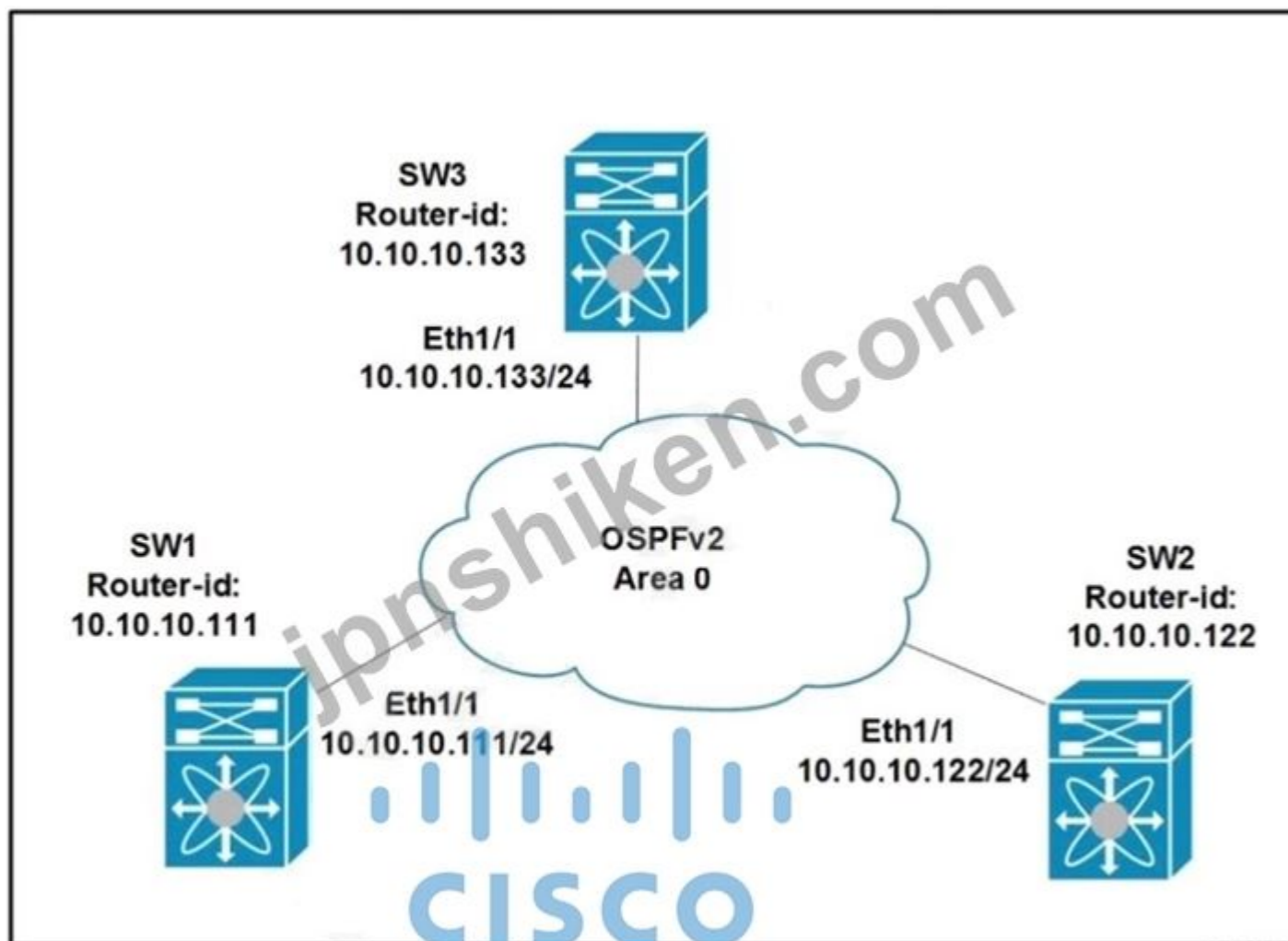
C. 選択肢D

D. オプションC

正解: ([正解を表示します](#))

質問: 148

展示資料を参照してください。



すべてのスイッチは、デフォルトのOSPF優先度で設定されています。SW2 Cisco NexusスイッチがLSAフラッドを制御し、OSPFv2エリア内の残りのノードにネットワークをアドバタイズするには、どの設定を適用する必要がありますか？

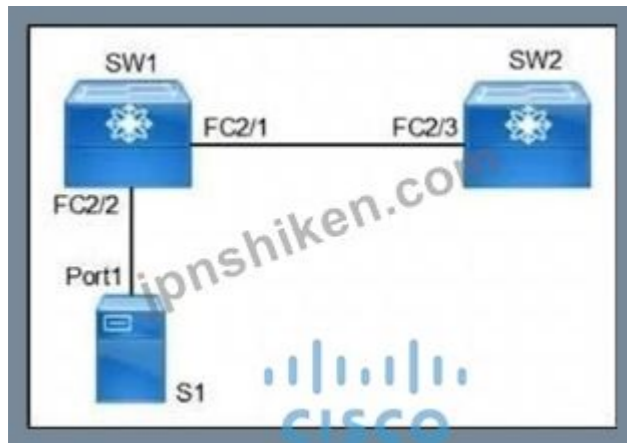
- A. SW2# configure terminal SW2 (config)# interface ethernet 1/1 SW2 (config-if)# ip ospf priority 0
- B. SW2# configure terminal SW2 (config)# interface ethernet 1/1 SW2 (config-if)# ip ospf priority 1
- C. SW2# configure terminal SW2 (config)# router ospf 1 SW2 (config-router)# router-id 10.10.10.22
- D. SW2# configure terminal SW2 (config)# interface ethernet 1/1 SW2 (config-if)# ip ospf priority 255

正解: ([正解を表示します](#))

OSPFにおける優先度は、主にネットワークの指定ルーター (DR) またはバックアップ指定ルーター (BDR) を決定するために使用されます。デフォルトでは、すべてのルーターの優先度は1です。優先度の高いルーターは、DR/BDR選出プロセスで常に勝利します。

質問: 149

図を参照してください。データセンターに2台のCisco MDS 9000シリーズスイッチが設置されています。サーバーS1がSW1にFLOGIリクエストを送信します。SW2からFLOGIレスポンスを受信するには、どの設定を使用する必要がありますか？



- A. SW1をNPIVとして使用  
SW2をNPVとして
- B. SW1をNPVとして  
SW2をNPIVとして使用
- C. SW1をNPIVとして使用  
SW2をNPIVとして使用
- D. SW1をNPVとして  
SW2をNPVとして

正解: (正解を表示します)

NPIV (N\_Port ID仮想化)を使用すると、単一の物理ファイバーチャネルポートで、ファブリックに複数のワールドワイドポート名 (WWPN)を登録できます。これは通常、フル機能のファイバーチャネルスイッチまたはディレクターで有効になります。

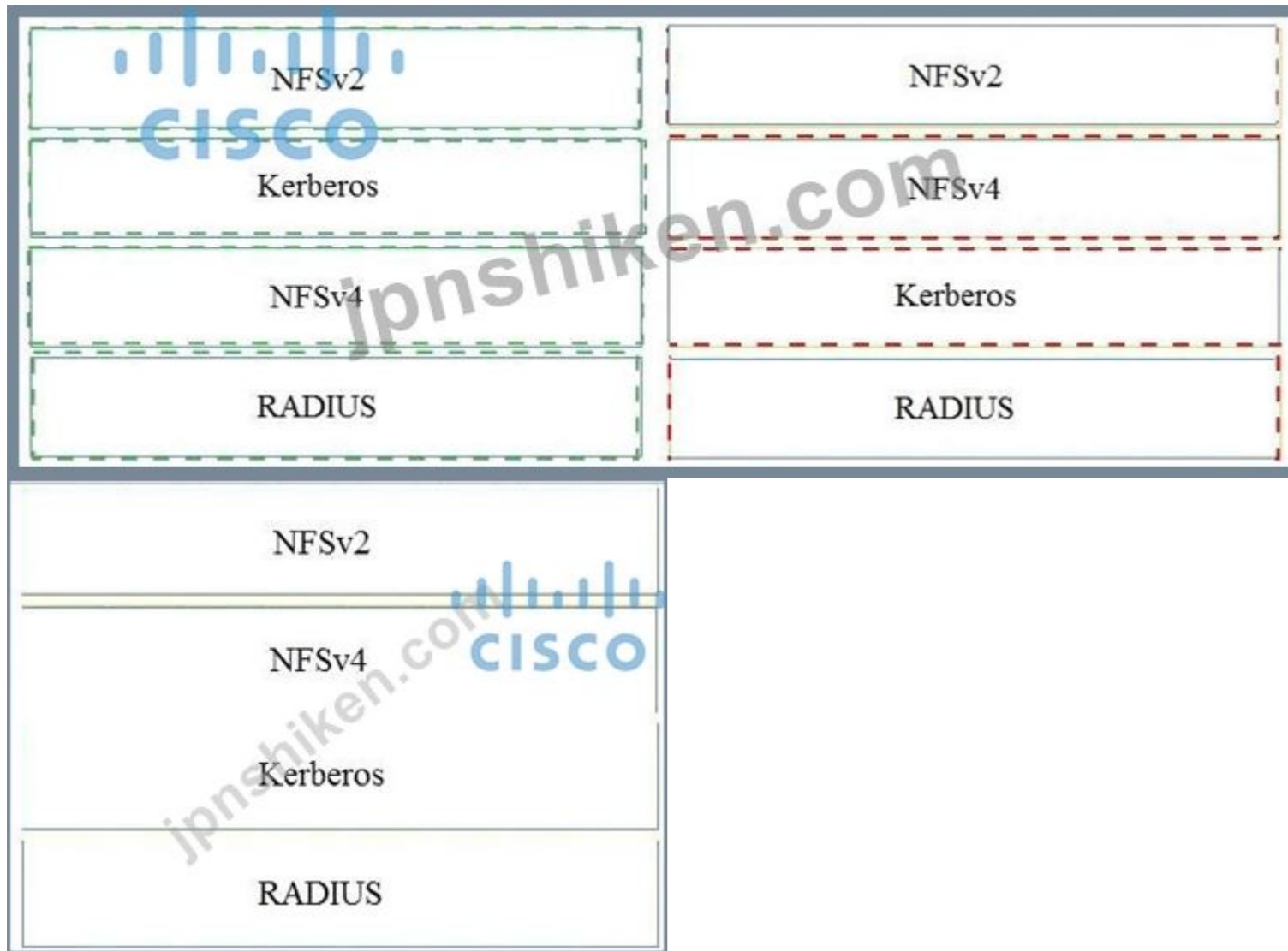
NPV (N\_Port Virtualization)は、FLOGIリクエストを上流のNPIV対応スイッチに転送することでトポロジーを簡素化します。NPVはゾーニングやネームサービスなどのファブリックサービスには参加せず、パススルーのように動作します。

質問: 150

左側のストレージ技術を、右側の適切な説明にドラッグ&ドロップしてください。

NFSv2	uses client machine authentication
Kerberos	uses users authentication
NFSv4	authenticates clients and servers in NFSv4
RADIUS	authenticates clients to corporate directory systems

正解:



質問: 151

顧客は、ストリーミングビデオをネットワーククライアントに配信するためにメディアサーバーを導入します。要件は、ビデオフィードが要求元のクライアントにのみ届くようにすることです。共有ツリーから要求されたクライアントがない場合、そのツリーはビデオフィードを伝播してはなりません。設定の手間を減らすため、ソリューションはRPセット情報の自動検出と通知をサポートする必要があります。ネットワーク内の各ルーターはRPを選択する責任を負います。これらの要件を満たす構成セットはどれですか？

A. 

```
router(config-if)# ip pim dense-mode
router(config)# ip pim rp-address 1.1.1.1
router(config)# ip pim rp listener
```

B. 

```
router(config-if)# ip pim sparse mode
router(config)# ip pim bsr-candidate Lo0
router(config)# ip pim rp-candidate Lo0
```

C. 

```
router(config-if)# ip pim sparse-sense mode
router(config)# ip pim auto-rp
router(config)# ip pim send-rp-announce
```

```
router(config-if)# ip pim bidir-enable
router(config)# ip pim ssm default
router(config)# ip igmp version 3
```

D.

正解: ([正解を表示します](#))

有効的な350-601問題集はJPNTTest.com提供され、350-601試験に合格することに役に立ちます！JPNTTest.comは今最新350-601試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで350-601問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> 384問、30%ディスカウント、特別な割引コード:

**JPNshiken**」

質問: 152

POAPが有効になっているCisco NexusスイッチがPOAPモードに移行しない場合、どの2つの条件を確認する必要がありますか？  
(2つ選択してください。)

- A. ブートフラッシュにCisco NX-OSイメージが存在しません。
- B. スwitchにライセンスファイルがありません。
- C. Bootflashには、poap.pyファイルを含むPOAPという名前の特別なディレクトリが含まれている必要があります。
- D. 起動設定は利用できません。
- E. スwitchは起動処理中です。

正解: B,C ([コメントを发表する](#))

質問: 153

ストレージエンジニアは、Cisco MDS 9000 シリーズスイッチでゾーニングを設定する必要があります。左側のアクションを右側の順序にドラッグアンドドロップしてください。

```
zone name Zone1 vsan 4
```

Step 1

```
member pwwn 10:00:00:23:45:67:89:ac
```

Step 2

```
zoneset activate name Zoneset1 vsan 4
```

Step 3

```
member Zone1
```

Step 4

```
copy running-config startup-config
```

Step 5

```
zoneset name Zoneset1 vsan 4
```

Step 6

正解:

```
zone name Zone1 vsan 4
```

```
member pwwn 10:00:00:23:45:67:89:ac
```

```
zoneset activate name Zoneset1 vsan 4
```

```
member Zone1
```

```
copy running-config startup-config
```

```
zoneset name Zoneset1 vsan 4
```

```
zone name Zone1 vsan 4
```

```
member pwwn 10:00:00:23:45:67:89:ac
```

```
zoneset name Zoneset1 vsan 4
```

```
member Zone1
```

```
zoneset activate name Zoneset1 vsan 4
```

```
copy running-config startup-config
```

Explanation:

グラフィカルユーザーインターフェース、表の説明は中程度の信頼度で自動生成されます

zone name Zone1 vsan 4

member pwn 10:00:00:23:45:67:89:ac

zoneset name Zoneset1 vsan 4

member Zone1

zoneset activate name Zoneset1 vsan 4

copy running-config startup-config

```
Switch1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch1#(config)# vsan database
Switch1#(config-vsan-db)# vsan 100
Switch1#(config-vsan-db)# exit

Switch1#(config)# zone name zone1 vsan 100
Switch1#(config-zone)# member pwn 11:11:11:11:11:11:11:1a
Switch1#(config-zone)# member pwn 11:11:11:11:11:11:11:1b
Switch1#(config-zone)# exit

Switch1#(config)# zoneset name setA vsan 100
Switch1#(config-zoneset)# member zone1
Switch1#(config-zoneset)# exit

Switch1#(config)# zoneset activate name setA vsan 100
Zoneset activation initiated. check zone status
Switch1#(config)# exit

Switch1# sh zoneset active vsan 100
zoneset name setA vsan 100
zone name zone1 vsan 100
pwn 11:11:11:11:11:11:11:1a
pwn 11:11:11:11:11:11:11:1b
Switch1#
```

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6\\_2/configuration/guides/fabric/nx-os/nx\\_os\\_fabric/zone.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6_2/configuration/guides/fabric/nx-os/nx_os_fabric/zone.html)

顧客は、ストリーミングビデオをネットワーククライアントに配信するためにメディアサーバーを導入します。要件は、ビデオフィードが要求元のクライアントにのみ届くようにすることです。共有ツリーから要求されたクライアントがない場合、そのツリーはビデオフィードを伝播してはなりません。設定の手間を減らすため、ソリューションはRPセット情報の自動検出と通知をサポートする必要があります。ネットワーク内の各ルーターは、RPを選択する責任を負います。

これらの要件を満たす構成セットはどれですか？

- ```
router(config-if)# ip pim sparse-mode
router(config)# ip pim auto-rp
router(config)# ip pim send-rp-announce
```
- A.
- ```
router(config-if)# ip pim dense-mode
router(config)# ip pim rp-address 1.1.1.1
router(config)# ip pim rp listener
```
- B.
- ```
router(config-if)# ip pim bidir-enable
router(config)# ip pim ssm default
router(config)# ip igmp version 3
```
- C.
- ```
router(config-if)# ip pim sparse-mode
router(config)# ip pim bsr-candidate Lo0
router(config)# ip pim rp-candidate Lo0
```
- D.

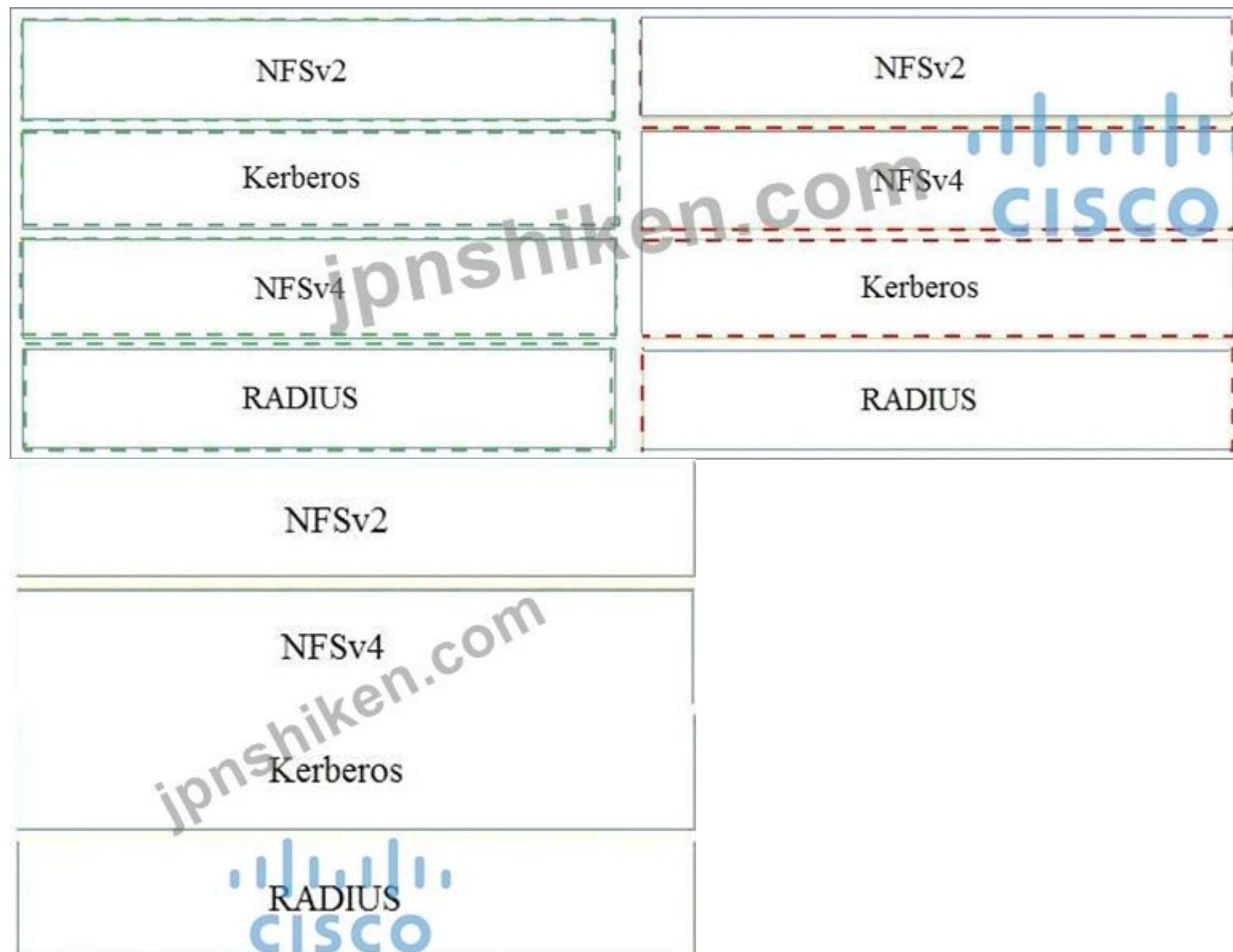
正解: [A \(コメントを发表する\)](#)

質問: 155

左側のストレージ技術を、右側の適切な説明にドラッグ&ドロップしてください。

NFSv2	uses client machine authentication
Kerberos	uses users authentication
NFSv4	authenticates clients and servers in NFSv4
RADIUS	authenticates clients to corporate directory systems

正解:



質問: 156

ネットワークエンジニアは、Cisco Nexus 9000シリーズスイッチの実行中の設定を、stable1という名前の既存のスナップショットに復元する必要があります。復元手順は、エラーが発生しない場合にのみ実行されるべきです。この目的を達成するには、どの設定を使用すべきでしょうか？

- A. ロールバックチェックポイント stable1 ベストエフォート実行 -config ベストエフォート
- B. ロールバック実行設定チェックポイント stable1 アトミック
- C. 実行中の設定チェックポイント stable1 をロールバックしてベストエフォート
- D. ロールバック チェックポイント stable1 ベストエフォート 実行設定 アトミック

正解: [\(正解を表示します\)](#)

質問: 157

```
MDS-B# show role
Role: network-admin
Description: Predefined Network Admin group. This role cannot be modified.
Vsan policy: permit (default)
-----
Rule   Type   Command-type   Feature
-----
1      permit clear      *
2      permit config    *
3      permit debug     *
4      permit exec      *
5      permit show      *

Role: default-role
Description: This is a system defined role and applies to all users.
Vsan policy: permit (default)
-----
Rule   Type   Command-type   Feature
-----
1      permit show      system
2      permit show      snap
3      permit show      module
4      permit show      hardware
5      permit show      environment

Role: san-users
Description: SAN users
Vsan policy: permit (default)
-----
```

図を参照してください。ネットワークエンジニアがSANユーザーに割り当てる新しい役割を作成しました。要件は、ユーザーが以下の特性を持つことです。

\* システム、SNMP、モジュール、およびハードウェアへのアクセスを表示することが許可されています

\* 情報

デバッグゾーンの実行とfcpingコマンドの実行が許可されています

show feature environment コマンドへのアクセスが制限されています。

構成セットはこれらの要件を満たしていますか？

- A. 選択肢D
- B. オプションA
- C. オプションC
- D. オプションB

正解: [\(正解を表示します\)](#)

質問: 158

Host1はデータセンター1にあるVLAN100に属し、Host2はデータセンター2にあるVLAN200に属しています。

どのOTV VLANマッピング構成であれば、これら2つのホスト間でレイヤ2接続が可能になりますか？

```
DC1:
interface Overlay1
  otn extend-vlan 100
  otn vlan mapping 100 to 200
```

```
DC2:
interface Overlay1
  otn extend-vlan 100
  otn vlan mapping 100 to 200
```

A.

```
DC1:
interface Overlay1
  otn extend-vlan 100
  otn vlan mapping 100 to 200
```

```
DC2:
interface Overlay1
  otn extend-vlan 200
```

B.

```
DC1:
interface Overlay1
  otn extend-vlan 100

DC2:
interface Overlay2
  otn extend-vlan 200
```

C.

```
DC1:
interface Overlay1
  otn extend-vlan 100

DC2:
interface Overlay1
  otn extend-vlan 200
```

D.

正解: ([正解を表示します](#))

ローカルサイトのVLANを、リモートサイトの異なるVLAN IDを持つVLANにマッピングできます。

異なる VLAN ID を持つ 2 つの VLAN をサイト間でマッピングすると、それらはトランスポート VLAN と呼ばれる共通の VLAN にマッピングされます。たとえば、サイト A の VLAN 1 をサイト B の VLAN 2 にマッピングすると、両方の VLAN がトランスポート VLAN にマッピングされます。サイト A の VLAN 1 から発信されるすべてのトラフィックは、トランスポート VLAN から発信されるものとして扱われます。トランスポート VLAN からサイト B に到着するすべてのトラフィックは、VLAN 2 に転送されます。

参照：

<https://www.cisco.com/c/en/us/support/docs/switches/nexus-7000-series-switches/200998-Nexus-7000-OTV-VLAN-Mapping-on-Overlay.html? dtid=ossdc000283>

質問: 159

ホストファームウェアパッケージからデフォルトで除外されるコンポーネントはどれですか？

- A. ストレージコントローラ
- B. ローカルディスク
- C. ボードコントローラ
- D. ネットワークインターフェースコントローラ

正解: ([正解を表示します](#))

質問: 160

この出力のフォーマットは何ですか？



```
{
  "ins_api": {
    "type": "cli_show",
    "version": "1.0",
    "sid": "eoc",
    "outputs": {
      "output": {
        "input": "show hostname",
        "msg": "Success",
        "code": "200",
        "body": "hostname: sbx-437device34691kv"
      }
    }
  }
}
```

- A. XML
- B. 石鹼
- C. JSCN
- D. YAML

正解: ([正解を表示します](#))

質問: 161

展示資料を参照してください。

```
monitor fabric session mySession
description "This is my fabric ERSPAN session"
destination tenant t1 application appl epg epg1 destination-ip 192.0.20.123 source-ip-prefix 10.0.20.1

erspan-id 100
ip dscp 42
ip ttl 16
mtu 9216
exit

source interface eth 1/1 switch 101

direction tx

filter tenant t1 bd bdl
filter tenant t1 vrf vrfl

no shut
```

エンジニアは、以下の要件を満たす監視セッションを実装する必要があります。

\* Cisco ACIネットワーク上のリーフスイッチ間のトラフィックを監視します。

\* ブリッジドメインまたはVRFからのトラフィックのフィルタリングをサポート

これらの要件を満たすには、どの設定を追加する必要がありますか？

- A. アプリケーション epg epg1 app1
- B. アプリケーション app1 epg epg1
- C. インターフェース eth 1/2 スイッチ 101
- D. インターフェース eth 1/2 リーフ 101

正解: [\(正解を表示します\)](#)

#### 質問: 162

エンジニアが、ファブリックフェイルオーバーが有効になっているサーバーのvNICのトラフィック監視を実装しています。要件は、ファブリックインターコネクットのいずれかに障害が発生した場合でも、トラフィックをアナライザーに送信することです。アナライザーは、両方のファブリックインターコネクットの未設定のイーサネットポートに接続されています。このタスクを実現する構成はどれですか？

A. ファブリックごとに異なる名前のトラフィック監視セッションを2つ作成します。

FI-Bに接続されたアナライザーを、両方のモニタリングセッションの送信先として接続してください。

B. ファブリックごとに1つずつ、同じ名前のトラフィック監視セッションを2つ作成します。

各FIにアナライザーを接続し、そのFIにローカルなモニタリングセッションの宛先とします。

C. ファブリックごとに1つずつ、同じ名前のトラフィック監視セッションを2つ作成します。

FI-Aに接続されたアナライザーを、両方のモニタリングセッションの送信先として接続してください。

D. ファブリックごとに異なる名前のトラフィック監視セッションを2つ作成します。  
各FIにアナライザを接続し、FIローカルのモニタリングセッションの宛先とする。

正解: ([正解を表示します](#))

トラフィック監視の宛先は単一の物理ポートであるため、トラフィック監視セッションでは単一のファブリックしか監視できません。ファブリックフェイルオーバーを介したvNICトラフィックの途切れのない監視を行うには、ファブリックごとに1つずつ、合計2つのセッションを作成し、2台のアナライザを接続してください。

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/ucs-manager/CLI-User-Guides/System-Monitoring/3-1/b\\_UCSM\\_CLI\\_System\\_Monitoring\\_Guide\\_3\\_1/b\\_UCSM\\_CLI\\_System\\_Monitoring\\_Guide\\_3\\_1\\_chapter\\_01101.html](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/CLI-User-Guides/System-Monitoring/3-1/b_UCSM_CLI_System_Monitoring_Guide_3_1/b_UCSM_CLI_System_Monitoring_Guide_3_1_chapter_01101.html)

質問: 163

エンジニアは、新しいCisco MDS 9000シリーズスイッチを導入し、業界標準のセキュアなプロトコルを使用して送信されたLinkUp/LinkDown通知を受信できるようにする必要があります。この目標を達成するには、どのテクノロジーを使用する必要がありますか？

- A. PMON
- B. RMON
- C. SNMP
- D. スパン

正解: C ([コメントを发表する](#))

質問: 164

エンジニアは、詳細なパケット分析のために、これらのアプリケーションからのトラフィックをキャプチャするために、Cisco Nexus 5000シリーズスイッチでSPANを設定する必要があります。考慮すべき2つの特性はどれですか？ (2つ選択してください。)

- A. 宛先SPANポートとして使用できるのは、イーサネット、FC、vFC、ポートチャネルのポートタイプのみです。
- B. Ethernet、FC、vFC、ポートチャネル、SANポートチャネルはSPANソースポートとして使用できます。
- C. SPANソースポートは複数のSPANセッションで監視できます。
- D. VLANまたはVSAN SPANセッションでは、rx/txオプションが利用可能です。
- E. SPANの送信元ポートは、宛先SPANポートにはなれません。

正解: ([正解を表示します](#))

質問: 165

エンジニアは、Cisco UCS Directorとの統合のために、Cisco Nexus 9000シリーズスイッチを設定する必要があります。設定では、スイッチがオンラインになった際に自動的にオンボーディングされるようにする必要があります。セキュリティ上の理由から、スイッチには必要最低限の接続方法のみを有効にする必要があります。接続プロトコルは、認証情報による認証を許可する必要があります。自動オンボーディングを可能にするには、スイッチ上でどのプロトコルを設定する必要がありますか？

- A. SNMP
- B. Telnet
- C. SSH
- D. HTTPS

正解: ([正解を表示します](#))

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/ucs-director/network-devices-mgmt-guide/6-5/cisco-ucs-director-network-devices-mgmt-65/cisco-ucs-director-network-devices-mgmt-65\\_chapter\\_010.html#id\\_33557:~:text=Protocol%20drop%2Ddown%20list](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-director/network-devices-mgmt-guide/6-5/cisco-ucs-director-network-devices-mgmt-65/cisco-ucs-director-network-devices-mgmt-65_chapter_010.html#id_33557:~:text=Protocol%20drop%2Ddown%20list)

[https://community.cisco.com/kxiwq67737/attachments/kxiwq67737/5668j-docs-dc-ucs-director/299/11/UCSD\\_Tech\\_Module\\_Nexus\\_Ethernet\\_v1.0.pdf](https://community.cisco.com/kxiwq67737/attachments/kxiwq67737/5668j-docs-dc-ucs-director/299/11/UCSD_Tech_Module_Nexus_Ethernet_v1.0.pdf)

質問: 166

エンジニアは、OTVをサポートするために、同じデータセンター内の2台のCisco Nexus 7000シリーズスイッチを設定する必要があります。どのコマンドセットを使用すると、ジョインインターフェイスの設定が完了しますか？

An engineer must configure two Cisco Nexus 7000 Series switches in the same data center to support OTV. Which command set completes the join interface configuration?

```
feature otv
otv site-identifier 256
interface overlay 1
otv control-group 239.1.1.1
otv data-group 239.1.1.0/29
otv join-interface ethernet 2/1
otv extend-vlan 5-10
no shutdown
```

Edge Device 1  
interface ethernet 2/1  
ip address 192.0.2.1/24  
ip igmp version 3

Edge Device 2  
interface ethernet 2/1  
ip address 192.0.2.16/24  
ip igmp version 3

Edge Device 1  
interface ethernet 2/1  
ip address 192.0.2.1/24  
ip igmp version 3  
ip pim sparse-mode

Edge Device 2  
interface ethernet 2/1  
ip address 192.0.2.16/24  
ip igmp version 3  
ip pim sparse-mode

Edge Device 1  
interface ethernet 2/1  
ip address 192.0.2.1/24

Edge Device 2  
interface ethernet 2/1  
ip address 192.0.2.16/24

Edge Device 1  
interface ethernet 2/1  
ip address 192.0.2.1/24  
ip igmp version 3

Edge Device 2  
interface ethernet 2/1  
ip address 192.0.2.1/24  
ip igmp version 3

A. オプションA

B. オプションC

C. 選択肢D

D. オプションB

正解: [\(正解を表示します\)](#)

有効的な350-601問題集はJPNTest.com提供され、350-601試験に合格することに役に立ちます！JPNTest.comは今最新350-601試験問題集を提供します。JPNTest.com 350-601試験問題集はもう更新されました。ここで350-601問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> 384問、30%ディスカウント、特別な割引コード：**JPNshiken**」

質問: 167

左側の特性を右側のNASプロトコルにドラッグアンドドロップしてください。一部の特性は複数回使用されます。

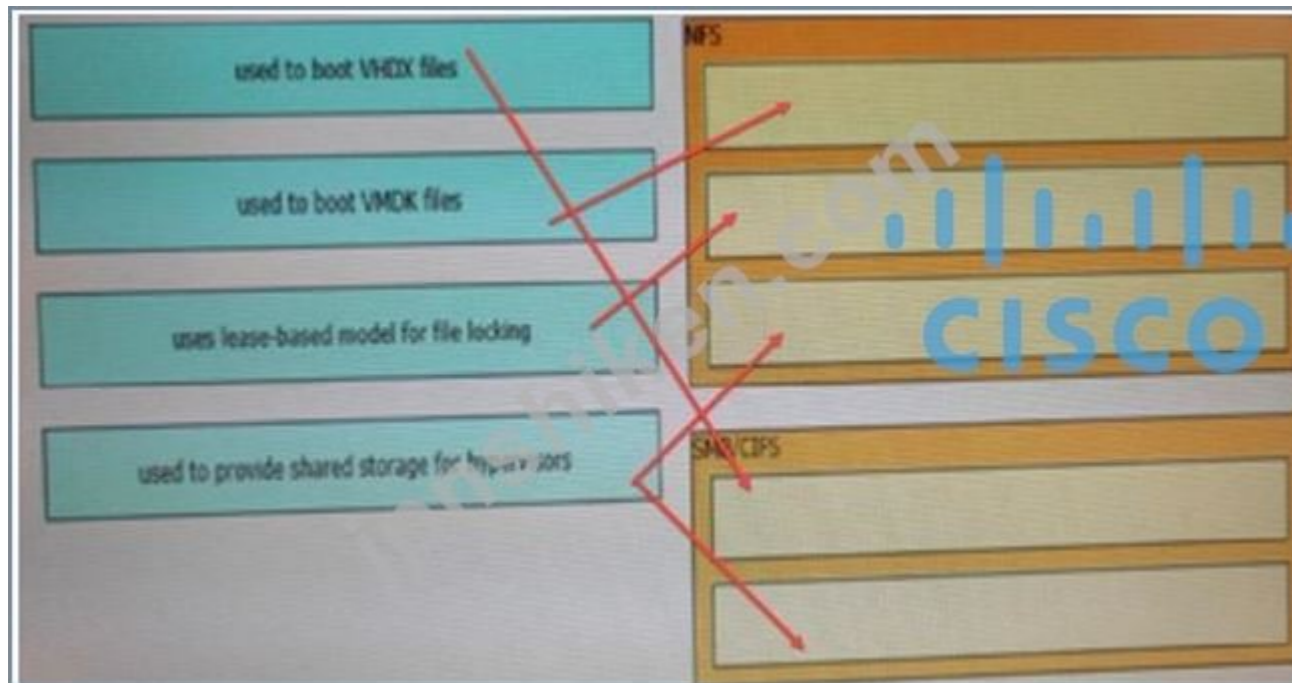


正解:



説明

図の説明は自動的に生成されました



NFS:

VMDKファイルの起動に使用されます

ファイルロックにはリースベースのモデルを使用します

ハイパーバイザーに共有ストレージを提供するために使用されます。

SMB/CIFS:

-VHDXファイルの起動に使用されます

ハイパーバイザーに共有ストレージを提供するために使用されます。

質問: 168

```
show incompatibility-all system bootflash:n7000-s1-dk9.4.2.4.bin
```

図を参照してください。Cisco Nexus 7000 シリーズ スイッチでソフトウェアのダウングレードが必要です。このコマンドを実行すると、何が表示されますか？

- A. 設定から自動的に削除される機能とコマンド
- B. システムブートフラッシュファイル内のソフトウェアの互換性
- C. ダウングレード後に自動的に有効になる機能
- D. ISSUにおけるソフトウェアアップグレードとシャーシ再ロードの影響

正解: [\(正解を表示します\)](#)

質問: 169

展示資料を参照してください。

```
Step 20 Enter no (no is the default) if you are satisfied with the configuration.

The following configuration will be applied:

switchname CiscoMDS
 interface mgmt0
  ip address 192.168.10.10
  subnetmask 255.255.255.0
  no shutdown
 ip default-gateway 192.168.10.1
 telnet server enable
 no ssh server enable
 no system default switchport shutdown
 system default switchport trunk mode on
 no zone default-zone permit vsan 1-4093
 zoneset distribute full vsan 1-4093
Would you like to edit the configuration? (yes/no) [n]: no

Step 21 Enter yes (yes is default) to use and save this configuration.

Use this configuration and save it? (yes/no) [y]: yes
```



エンジニアがCisco MDS 9000シリーズスイッチを初めて設定しています。初期設定プロセス後、IPアドレス192.168.10.11のネームサーバーが設定から欠落しています。設定を完了するには、どの操作を実行すればよいでしょうか？

- A. 手順21で 「no」と入力し、インストーラーを再初期化します。Escキーを押してROMMONモードにアクセスします。
- B. ステップ21で 「いいえ」と入力し、スイッチを再起動します。高度なIPオプションを設定します。
- C. ステップ21で 「はい」と入力して設定を編集します。dns-server 192.168.10.11という行を追加します。
- D. ステップ21で 「はい」と入力してログインします。起動設定のDNSを変更します。

正解: [\(正解を表示します\)](#)

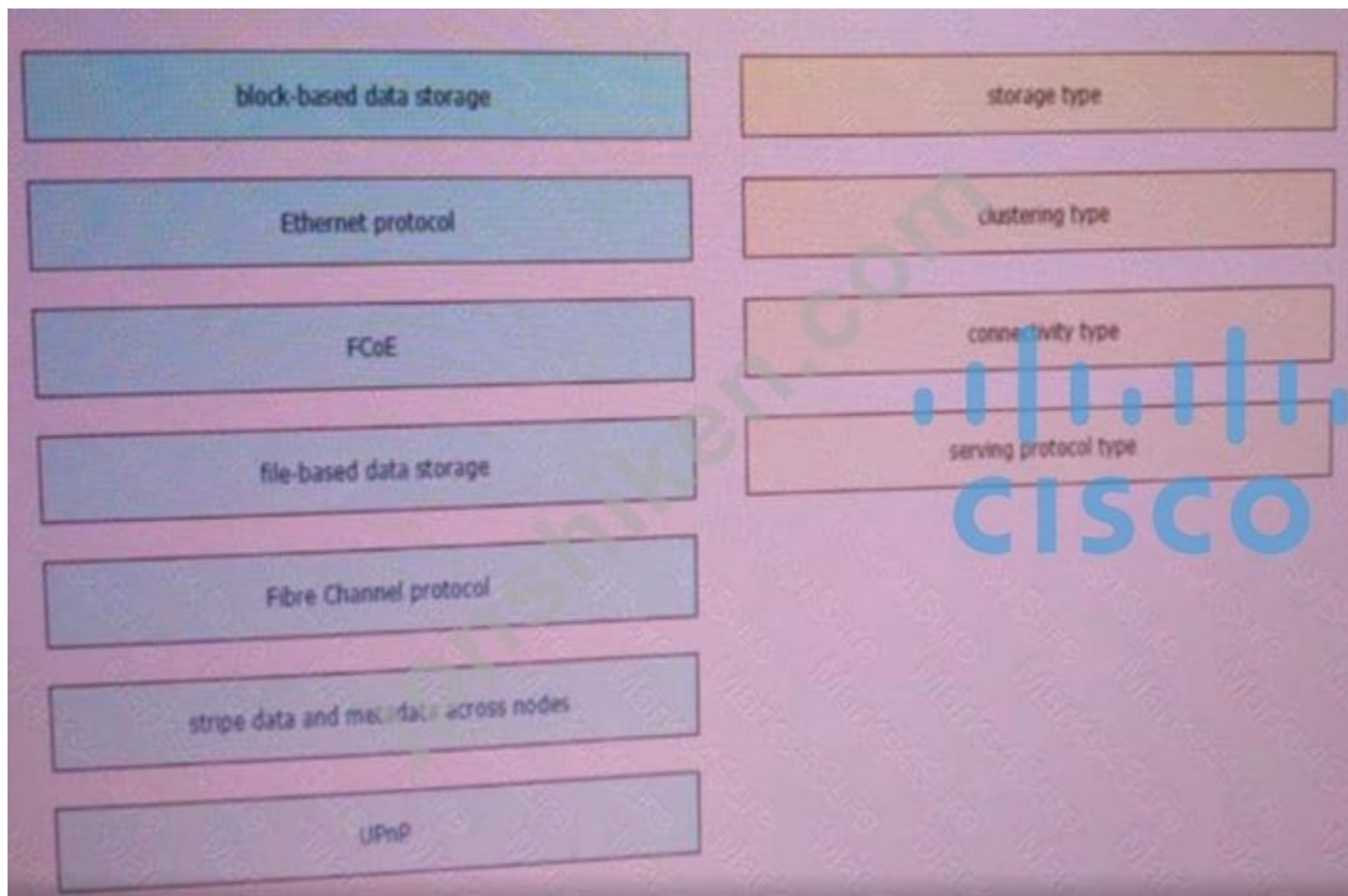
この質問は、エンジニアがCisco MDS 9000シリーズスイッチを設定している際に、IPアドレス192.168.10.11のネームサーバーが設定に含まれていないことに気づいたというものです。設定を完了するための正しい操作はオプションC、「ステップ21でyesを入力して設定を編集します。dns-serverという行を追加します」です。

192.168.10.11。この手順により、エンジニアは初期設定プロセスの結果を変更し、保存する前に不足しているDNSサーバー情報を直接設定に追加することができます。

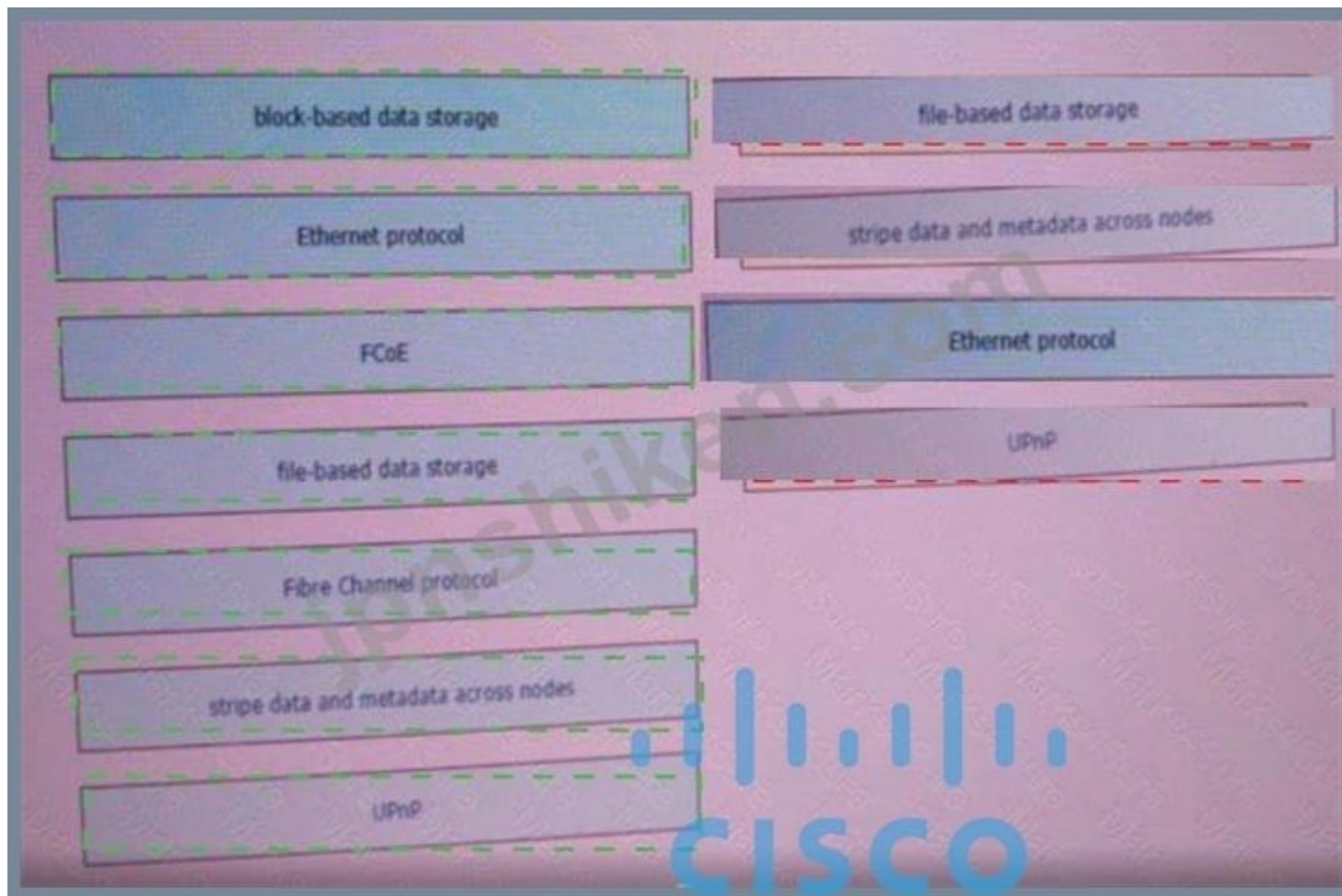
参考資料：詳細については、Ciscoラーニングネットワークストアで入手可能なCiscoデータセンターコアテクノロジーのソースドキュメントまたは学習ガイド、およびデータセンター仮想化に関するCiscoのソリューション一覧を参照してください。

質問: 170

左側のNAS機能を右側のNASの説明にドラッグ&ドロップしてください。すべての機能を使用するわけではありません。

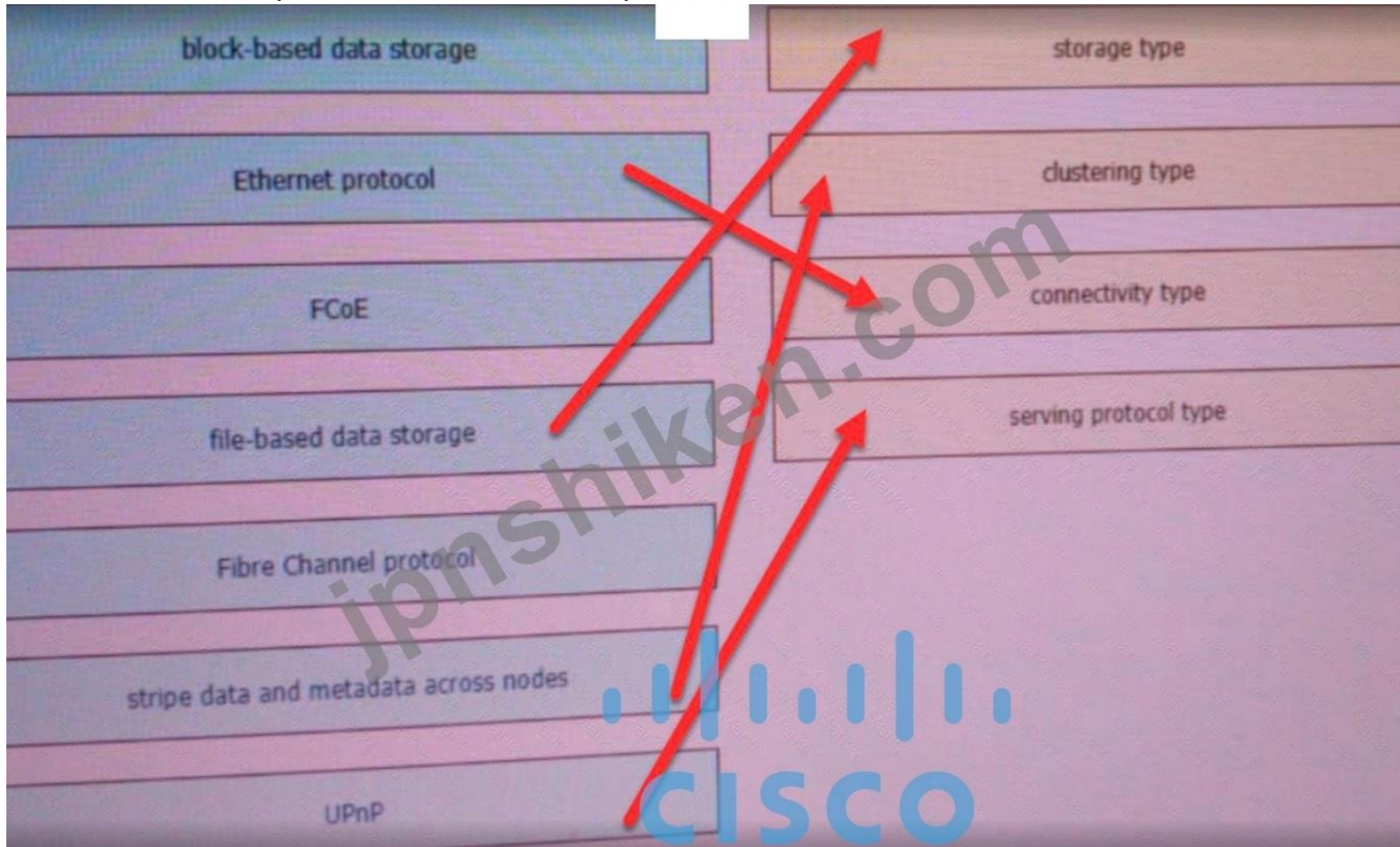


正解:



Explanation:

コンピュータのスクリーンショット。説明は中程度の信頼度で自動生成されました。



[https://en.wikipedia.org/wiki/Network-attached\\_storage](https://en.wikipedia.org/wiki/Network-attached_storage)

質問: 171

CPU使用率が60%を超えた場合にsyslogメッセージを生成する設定はどれですか？

A. イベントマネージャアプレット 高CPU負荷

イベント snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.6.1 get-type exact entry-op gt 60 poll-interval 5 action 1.0 syslog priority notifications msg "cpu high"

B. イベントマネージャアプレット HIGH-CPU

イベント snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.6.1 get-type exact entry-op lt 60 poll-interval 5 action 1.0 syslog priority notifications msg "cpu high"

C. イベントマネージャアプレット 高CPU負荷

イベント snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.6.1 get-type next entry-op gt 60 poll-interval 5 action 1.0 syslog priority notifications msg "cpu high"

D. イベントマネージャアプレット 高CPU負荷

イベント snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.6.1 get-type next entry-op lt 60 poll-interval 5 action 1.0 syslog priority notifications msg "cpu high"

正解: A (コメントを发表する)

説明

<https://www.cisco.com/c/en/us/support/docs/ip/internet-protocol-ip/200931-EEM-Subsystem-in-Order-to-Monitor-CPU-Tr.pdf>

<https://blog.ipospace.net/2008/06/generate-snmp-trap-on-high-cpu-load.html>

質問: 172

ストレージエンジニアは、Cisco MDS 9000 シリーズスイッチでゾーニングを設定する必要があります。左側のアクションを右側の順序にドラッグアンドドロップしてください。

zone name Zone1 vsan 4	Step 1
member pwwn 10:00:00:23:45:67:89:ac	Step 2
zoneset activate name Zoneset1 vsan 4	Step 3
member Zone1	Step 4
copy running-config startup-config	Step 5
zoneset name Zoneset1 vsan 4	Step 6

正解:



説明

A、B、F、D、C、E

質問: 173

エンジニアがACIファブリックを実装する際に、ネットワークベースの属性を使用して、同一IPサブネット内のエンドポイントのマイクロセグメンテーションを実装する必要があります。属性マッピングはIPサブネットの独立性を確保する必要があります。どの属性を選択すべきでしょうか？

- A. MACアドレス
- B. IP
- C. カスタム
- D. 日

正解: B ([コメントを发表する](#))

質問: 174

展示資料を参照してください。

```
Start time: Mon Apr 15 09:23:01 2019
Last election time: Mon Apr 15 09:24:24 2019
A: UP, PRIMARY
B: UP, SUBORDINATE
A: memb state UP, lead state PRIMARY, mgmt services state: UP
B: memb state UP, lead state SUBORDINATE, mgmt services state: UP
heartbeat state PRIMARY_OK
INTERNAL NETWORK INTERFACES:
eth1, UP
eth2, UP
HA NOT READY
No device connected to this Fabric Interconnect
```

HA NOT READY状態を解除するには、何を接続すればよいですか？

- A. レイヤー1～レイヤー2ポート
- B. サーバーシャーシ
- C. ネットワークアップリンク
- D. 管理ポート

正解: ([正解を表示します](#))

質問: 175

デュアルスーパーバイザモジュールと2つのI/Oモジュールを搭載したCisco Nexus 7000シリーズスイッチでISSUを完了するのにかかる時間を短縮するコマンドはどれですか？

- A. すべてのキックスタート<イメージ>システム<イメージ>を並列インストールします
- B. すべての epld bootflash をインストールします:<画像>
- C. すべての epld bootflash をインストールします:<イメージ> 並列
- D. すべてのキックスタート<イメージ>システム<イメージ>をインストールします

正解: ([正解を表示します](#))

質問: 176

デュアルスーパーバイザモジュールと2つのI/Oモジュールを搭載したCisco Nexus 7000シリーズスイッチでISSUを完了するのにかかる時間を短縮するコマンドはどれですか？

- A. すべての epld bootflash をインストールします:<イメージ> 並列
- B. すべてのキックスタート<イメージ>システム<イメージ>を並列インストールします
- C. すべてのキックスタート<イメージ>システム<イメージ>をインストールします
- D. すべての epld bootflash をインストールします:<画像>

正解: ([正解を表示します](#))

セクション: 計算

質問: 177

データセンターにCisco UCS Cシリーズサーバーが設置されています。このサーバーは、管理とデータトラフィックに1本のケーブルを使用し、Cisco UCS Managerによって管理される必要があります。物理接続が確立された後、どの構成を適用する必要がありますか？

- A. UCS-A# スコープサーバー 1

```
UCSA /server# scope cimc
UCSA /server/cimc # scope mgmt-conn sideband
UCS-A /server/cimc/mgmt-conn #set mgmt-conn-state enabled
UCS-A /server/cimc/mgmt-conn* # コミットバッファ
```

**B. UCS-A#スコープシャーシ1**

```
UCS-A /シャーシ# スコープ cimc
UCS-A /chassis/cimc # scope mgmt-conn sideband
UCS-A /chassis/cimc/mgmt-conn # mgmt-conn-state 有効
UCS-A /chassis/cimc/mgmt-conn* # コミットバッファ
```

**C. UCS-A#スコープサーバー1**

```
UCSA /server# scope cimc
UCSA /server/cimc # scope mgmt-conn sideband
UCS-A /server/cimc # mgmt-conn-state 有効
UCS-A /server/cimc/mgmt-conn* # コミットバッファ
```

**D. UCS-A#スコープシャーシ1**

```
UCS-A /シャーシ# スコープ cimc
UCS-A /chassis /cimc # mgmt-conn-state を有効に設定
UCS-A /chassis /cimc/mgmt-conn* # コミットバッファ
```

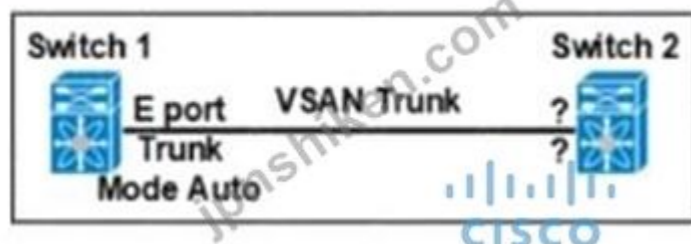
正解: ([正解を表示します](#))

例

```
UCS-A# スコープサーバー 1
UCSA /server # scope cimc
UCS-A /server/cimc # スコープ mgm
UCS-A /server/cimc # スコープ mgmt-conn
UCSA /server/cimc # scope mgmt-conn sideband
UCS-A /server/cimc/mgmt-conn # mgmt-conn-state を有効に設定
UCS-A /server/cimc/mgmt-conn* # コミットバッファ
UCS-A /server/cimc/mgmt-conn
```

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/c-series\\_integration/ucsm3-1/b\\_C-Series-Integration\\_UCSM3-1/b\\_C-Series-Integration\\_UCSM3-1\\_chapter\\_010.html](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c-series_integration/ucsm3-1/b_C-Series-Integration_UCSM3-1/b_C-Series-Integration_UCSM3-1_chapter_010.html)

質問: 178



図を参照してください。スイッチ1とスイッチ2の間でVSANトランクを確立するために、スイッチ2で設定する必要がある機能セットはどれですか？



- A. オプションC
- B. オプションA
- C. オプションB
- D. オプションD

正解: [\(正解を表示します\)](#)

質問: 179

エンジニアは、2 台の Cisco Nexus 9000 シリーズ スイッチ間で HSRP プロトコルを設定する必要があります。この設定は Nexus A に存在します。

```
! Nexus A
key chain NHRP-KEYS
key 1010
  key-string 7 072a43795c1d0c4050883003163b3e2121a720361a021e11
  accept-lifetime 00:00:00 Jan 01 2021 23:59:59 Aug 31 2021
  send-lifetime 00:00:00 Jan 01 2021 23:59:59 Jul 31 2021
key 1020
  key-string 7 036f43cd5c150c1702630203163b3e2221a520261a011a12
  accept-lifetime 00:00:00 Jul 01 2021 23:59:59 Dec 31 2021
  send-lifetime 00:00:00 Jul 01 2021 23:59:59 Dec 31 2021
interface ethernet 1/1
ip 209.165.200.226/27
hsrp 200
  priority 201
  ip 209.165.200.225
-- missing output --
no shutdown
```

最終的なHSRP構成は、これらの要件を満たす必要があります。

HSRP通信は両方のスイッチで保護されなければならない。

両方のスイッチは300以上のグループをサポートする必要があります。

これらの要件を満たすために、Nexus AのHSRP設定に追加する必要があるコマンドはどれですか？ 2つ選択してください)

- A. NHRP-KEYSのMD5キーチェーンを認証する
- B. 認証テキスト 1020
- C. 認証テキスト 1010
- D. HSRPバージョン1
- E. HSRPバージョン2

正解: [\(正解を表示します\)](#)

質問: 180

エンジニアは、Cisco UCS Manager PowerShell モジュールを利用して Cisco UCS Manager に自動リクエストを送信する PowerShell スクリプトを作成する必要があります。エンジニアは、VLAN からスイッチを削除するプロセスを自動化する必要があります。環境変数には、VLAN 名とスイッチ識別子を指定する必要があります。スイッチ ポートから削除された後も VLAN は保持される必要があります。これらの目的を達成するために、エンジニアはスクリプトにどのコマンドを含める必要がありますか？

- ```
Get-UcsApplianceCloud | Remove -UcsVlan -name $VLAN
```
- ```
Get-UcsApplianceCloud | Remove -UcsVlan -name $VLAN |  
Remove-UcsVlanMemberPort -SwitchId $$SWID -SlotId  
$SLOT -PortId $PORT
```
- ```
Get-UcsApplianceCloud | Get-UcsVlan -name $VLAN |  
Remove-UcsVlanMemberPort -SwitchId B -SlotId 1 -  
PortId 15
```
- ```
Get-UcsApplianceCloud | Get-UcsVlan -name $VLAN | Get-  
UcsVlanMemberPort -SwitchId $$SWID -SlotId $$SLOT -  
PortId $PORT | Remove-UcsVlanMemberPort -Force
```

- A. オプションA
- B. オプションB
- C. 選択肢D
- D. オプションC

正解: [\(正解を表示します\)](#)

質問: 181



図を参照してください。エンジニアはVXLAN展開をプロビジョニングする必要があります。OSPFは既にアンダーレイプロトコルとして構成されています。すべてのBGP構成はテンプレート方式を使用して実行されます。展開はこれらの要件を満たす必要があります。

\* リーフスイッチのローカル更新ソースはループバック1である必要があります

ルーターIDはローカルループバックIPアドレスである必要があります。

\* 外部BGP接続ではテンプレート名を使用する必要があります

下部から設定スニペットをドラッグアンドドロップして設定を完了します。

```
router bgp 65000
  router-id 
  template peer SPINE
  bfd
  remote-as 
  update-source loopback1
  timers 3 9
  address-family  
    send-community extended
  neighbor 
     peer SPINE
```

10.255.255.1	inherit	65000
10.255.255.10	12vpn	evpn

正解:

```
router bgp 65000
  router-id 10.255.255.10
  template peer SPINE
  bfd
  remote-as 65000
  update-source loopback1
  timers 3 9
  address-family 12vpn evpn
    send-community extended
  neighbor 10.255.255.1
    inherit peer SPINE
```

```
10.255.255.1 inherit 65000
10.255.255.10 12vpn evpn
```

Explanation:

```
router bgp 65000
  router-id 10.255.255.10
  template peer SPINE
  bfd
  remote-as 65000
  update-source loopback1
  timers 3 9
  address-family 12vpn evpn
    send-community extended
  neighbor 10.255.255.1
    inherit peer SPINE
```

有効的な350-601問題集はJPNTTest.com提供され、350-601試験に合格することに役に立ちます！JPNTTest.comは今最新350-601試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで350-601問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> 884問、30%ディスカウント、特別な割引コード:

**JPNshiken**」

エンジニアが、スタンドアロンの Cisco C シリーズ サーバー用に、Cisco UCS (Cisco 統合管理コントローラ) ネットワーク アダプタのプロパティを設定します。vNIC のフォールバック タイムアウトは 600 に設定されています。障害が発生した場合、セカンダリ インターフェイスが使用され、プライマリ インターフェイスが再び使用可能になったときにフォールバックする必要があります。これらの要件を満たすために、どのような措置を講じるべきでしょうか？

- A. アダプタにデフォルトのVLANを設定します。
- B. Cosを6に増やします。
- C. VNTAGモードを無効にします。
- D. アップリンクのフェイルオーバーを有効にする。

正解: [\(正解を表示します\)](#)

セカンダリ インターフェイスを使用し、プライマリ インターフェイスが再び使用可能になったときにプライマリ インターフェイスにフォールバックするという要件を満たすには、エンジニアはスタンドアロンの Cisco C-Series サーバー用の Cisco UCS Cisco Integrated Management Controller (CIMC) ネットワーク アダプタの vNIC プロパティで、アップリンク フェイルオーバー オプションを有効にする必要があります。アップリンク フェイルオーバー オプションを使用すると、プライマリ インターフェイスに障害が発生した場合に vNIC がセカンダリ インターフェイスに切り替わり、プライマリ インターフェイスが復旧したときにプライマリ インターフェイスに切り替わります。また、アップリンク フェイルオーバー オプションでは、vNIC がプライマリ インターフェイスに切り替わるまでの待機時間を決定するフォールバック タイムアウト値を設定することもできます。この場合、フォールバック タイムアウト値は 600 秒に設定されているため、vNIC はプライマリ インターフェイスにフォールバックするまでに 10 分間待機します。

参考文献:

\* Ciscoデータセンターコアテクノロジーの実装と運用 (DCCOR)v1.2、モジュール5 :Cisco Unified Computing System、レッスン5.3 :Cisco UCS Cシリーズサーバー

\* Cisco UCS Cシリーズサーバー統合管理コントローラGUI構成ガイド、リリース4.0、章 :ネットワーク関連の設定と機能の構成、セクション :vNICの構成

#### 質問: 183

DevOps エンジニアは、Cisco Nexus シリーズ スイッチをベースとしたデータセンターのネットワーク インフラストラクチャをプロビジョニング、監視、トラブルシューティングするための Cisco Unified Fabric ソリューションを設計する必要があります。このソリューションは、統合データセンターの可視性と制御機能を提供する必要があります。これらの要件を満たすソリューションはどれですか？

- A. Cisco AppDynamics
- B. シスコDNAセンター
- C. Nexus Dashboard Fabric Controller
- D. Cisco CloudCenter Suite

正解: [\(正解を表示します\)](#)

Nexus Dashboard Fabric Controller (旧称Cisco DCNM)は、データセンター環境におけるCisco Nexusスイッチの管理に特化して設計されています。ネットワークインフラストラクチャのプロビジョニング、監視、トラブルシューティングのための包括的なツールに加え、統合ファブリック全体の可視化と制御機能を提供します。特に、データセンターにおけるCisco Nexus環境の管理に最適です。

#### 質問: 184

この出力に表示されているCisco Nexusコンソールラインインターフェイスはどれですか？

```
switch# dir bootflash:
```

```
25863680 2020年9月23日 12:02:16 m9250-sSek9-kickstart-mz.8.2.1.bin
25864704 2021年9月5日 12:21:26 m9250-s5ek9-kickstart-mz.8.2.1.bin
29869312 2021年4月1日 12:29:34 m9250-sSek9-kickstart-mz.8.2.2.bin
25869312 2021年4月12日 01:55:22 m9250-s5ek9-kickstart-mz.8.2.2.bin
25947136 2021年11月9日 13:41:43 m9250-s5ek9-kickstart-mz.8.3.1.bin
29970176 2021年1月17日 14:10:47 m9250-sSek9-kickstart-mz.8.3.2.bin
26126848 2021年5月7日 11:51:20 m9250-s5ek9-kickstart-mz.8.4.1.bin
```

[出力省略]

bootflash://sup-local の使用方法  
1050153904658バイト使用  
638636406560バイトの空き容量

- A. ゲストシェル
- B. NX-OS キックスタート CLI
- C. NX-OS CLI
- D. Bashシェル

正解: ([正解を表示します](#))

#### 質問: 185

Cisco HyperFlex Edgeの2ノード構成において、ウィットネスはどこに配置されますか？

- A. HyperFlex Edge 2ノードクラスターへ
- B. HyperFlex Edgeへのネットワークアクセスを持つ追加サーバーへ
- C. サードパーティのクラウドプロバイダーへ
- D. Cisco Intersightへ

正解: ([正解を表示します](#))

2ノード構成のCisco HyperFlex Edge展開では、監視対象はCisco Intersightに展開されます。このクラウドベースの管理プラットフォームは、ビジネスの成長に合わせて拡張可能なインテリジェントなインサイトと自動化機能を提供します。単一のクラウドベースのインターフェースから、グローバルなすべてのHyperFlex Edge展開を管理できます。参考文献：

\* Cisco HyperFlex Edge データシート - Cisco、Cisco HyperFlex Edge データシート、Cisco HyperFlex Edge 導入オプション

\* Cisco HyperFlex Edge インストール ガイド、リリース 4.0 - HyperFlex Edge クラスターの展開 [Cisco HyperFlex HX Data Platform]、HyperFlex Edge クラスターの展開、2 ノード HyperFlex Edge クラスターの展開

#### 質問: 186

```
1 - name: Use Ansible to resolve the switch connectivity issue.
2   cisco.nxos.nxos_12_interfaces:
3     config:
4       - name: GigabitEthernet0/1
5         trunk:
6           native_vlan: 10
7           allowed_vlans: 10, 20
8       - name: GigabitEthernet0/2
9         trunk:
10          native_vlan: 20
11          allowed_vlans: 10, 20
12     state: merged
```

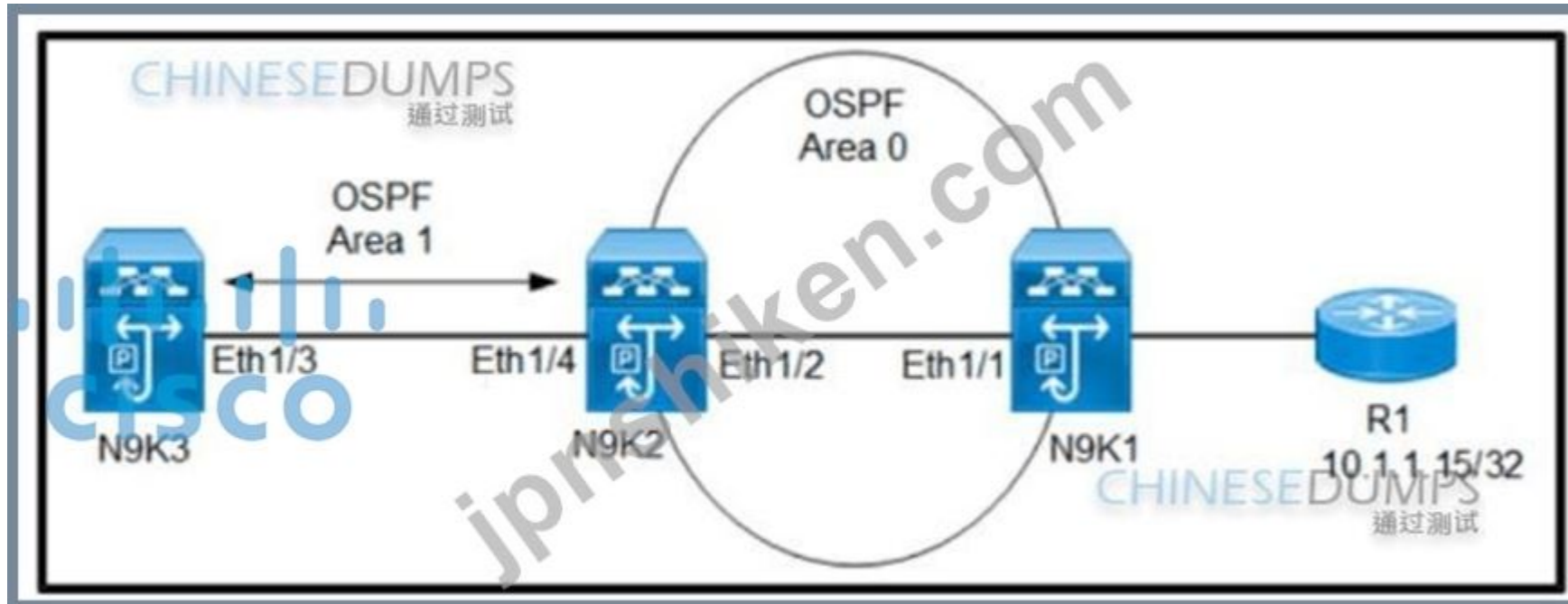
図を参照してください。エンジニアは、Ansibleを使用して構成された Cisco 9000 Series スイッチの接続問題を解決する必要があります。スイッチは、次の要件を満たすように構成する必要があります。\* インターフェイス G\*gabetethernet0/1 は、アクセスモードで VLAN 10 のメンバーである必要があります。\* インターフェイス G\*gabetethernet0/2 は、ネイティブ VLAN 20 を使用して、トランクモードで VLAN 10 と 20 を許可する必要があります。これらの基準を満たすには、どの一連のアクションを実行する必要がありますか。

- A. インターフェイスGigabitethernet0/2をトランクモードに設定し、インターフェイスGigabitethernet0/1をVLAN 10に割り当てます。
- B. インターフェイスGigabitethernetQ/2をアクセスモードに設定し、インターフェイスGigabitethernet0/2をVLAN 20に割り当てます。
- C. インターフェイスGigabitethernet0/1をアクセスモードに設定し、インターフェイスGigabitethernet0/1をVLAN 10に割り当てます。

D. インターフェース GigabitethernetO/1 をトランクモードに設定し、インターフェース GigabitethernetO/2 を VLAN 20 に割り当てます。

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 10.1.1.15/32 は N9K1 にアドバタイズされています。N9K2 と N9K3 はエリア 1 の OSPF ネイバーです。どの設定がネットワーク 10.1.1.15/32 を LSA タイプ 7 として N9K3 にアドバタイズしますか？

- A. N9K2(config-router)# area 1 nssa  
N9K3(config-router)# area 1 nssa
- B. N9K1(config-router)# area 0 nssa  
N9K2(config-router)# area 0 nssa
- C. N9K1(config-router)# area 0 stub no-summary  
N9K2(config-router)# area 0 stub
- D. N9K2(config-router)# area 1 stub no-summary  
N9K3(config-router)# エリア1スタブ

正解: ([正解を表示します](#))

質問: 188

エンジニアは、Cisco MDS 9000 シリーズ スイッチで VSAN 110 のみにファブリック バインディングを実装する必要があります。両方の WWN はドメイン 110 の一部である必要があります。展開が完了したら、アクティブな VSAN の設定をアクティブな設定と比較する必要があります。設定を完了するには、下部のコード スニペットを上部のコードの空白にドラッグ アンド ドロップします。すべてのコード スニペットが使用されるわけではありません。

```
CISCO MDS# configure terminal
CISCO MDS(config)# feature [redacted]
CISCO MDS(config)# fabric-binding [redacted]
CISCO MDS(config-fabric-binding)# swwn 20:10:10:10:10:10:10:10 domain 110
CISCO MDS(config-fabric-binding)# nwn 20:30:30:30:30:30:30:30 domain 110
CISCO MDS(config-fabric-binding)# exit
CISCO MDS(config)# exit
CISCO MDS# fabric-binding database [redacted]
CISCO MDS# copy run start
```



database vsan 110	fabric-binding
diff active vsan 110	database enable

正解:

```
CISCO MDS# configure terminal
CISCO MDS(config)# feature fabric-binding
CISCO MDS(config)# fabric-binding database vsan 110
CISCO MDS(config-fabric-binding)# swwn 20:10:10:10:10:10:10:10 domain 110
CISCO MDS(config-fabric-binding)# nwn 20:30:30:30:30:30:30:30 domain 110
CISCO MDS(config-fabric-binding)# exit
CISCO MDS(config)# exit
CISCO MDS# fabric-binding database diff active vsan 110
CISCO MDS# copy run start
```

database vsan 110	fabric-binding
diff active vsan 110	database enable

```
CISCO MDS# configure terminal
CISCO MDS(config)# feature 
CISCO MDS(config)# fabric-binding 
CISCO MDS(config-fabric-binding)# nwwn 20:10:10:10:10:10:10:10 domain 110
CISCO MDS(config-fabric-binding)# nwwn 20:30:30:30:30:30:30:30 domain 110
CISCO MDS(config-fabric-binding)# exit
CISCO MDS(config)# exit
CISCO MDS# fabric-binding database 
CISCO MDS# copy run start
```

database vsan 110      fabric-binding  
diff active vsan 110      database nabl

質問: 189

エンジニアは、信頼できないDHCPサーバーがネットワークを侵害するのを防ぐソリューションを実装する必要があります。この機能はCisco Nexus 7000シリーズスイッチで設定し、VLAN 10に適用する必要があります。正規のDHCPサーバーはインターフェイスEthernet 2/4に接続されています。これらの要件を満たすには、どの設定セットを使用する必要がありますか？

```
n7k-1(config)# ip dhcp snooping vlan 10
n7k-1(config)# interface Ethernet2/4
n7k-1(config-if)# ip dhcp snooping trust

n7k-1(config)# ip dhcp snooping vlan 10
n7k-1(config)# interface Ethernet2/4
n7k-1(config-if)# ip dhcp snooping verify vlan 10

n7k-1(config)# ip dhcp snooping verify
n7k-1(config)# interface Ethernet2/4
n7k-1(config-if)# ip dhcp snooping verify vlan 10

n7k-1(config)# ip dhcp snooping verify
n7k-1(config)# vlan configuration 10
n7k-1(config-vlan)# ip dhcp snooping trust
```

- A. オプションA
- B. オプションB
- C. オプションC
- D. 選択肢D

正解: A (コメントを发表する)

DHCPスヌーピング機能は、信頼できないホストと信頼できるDHCPサーバー間のファイアウォールとして機能します。信頼できない送信元から受信したDHCPメッセージを検証し、無効なメッセージをフィルタリングします。Cisco Nexus 7000シリーズスイッチでVLAN 10に対してこの機能を実装するには、そのVLANでDHCPスヌーピングを有効にし、正当なDHCPサーバーに接続されている特定のインターフェイスを信頼するように設定する必要があります。これにより、正当なサーバーからのDHCP応答は許可され、それ以外のサーバーからの応答はブロックされます。

参考文献 :

\* Cisco Nexus 7000シリーズ NX-OSセキュリティ設定ガイド1

\* DHCP Snooping2の設定

質問: 190

展示資料を参照してください。

```
switch(config)# feature dhcp
switch(config)# ip dhcp snooping
switch(config)# service dhcp
switch(config)# ip dhcp snooping vlan 100,200,250-252
switch(config)# ip dhcp relay information option
```

リレーエージェントがDHCP BOOTREQUESTパケットをDHCPサーバーに転送することを確実にするために、どのような措置が取られますか？

- A. DHCPサーバーのインターフェースを信頼されていないものとして設定します。
- B. DHCPサーバーのIPアドレスを設定します。
- C. DHCPリレーエージェントを有効にします。
- D. DHCPスヌーピングのバインディングを確認します。

正解: [\(正解を表示します\)](#)

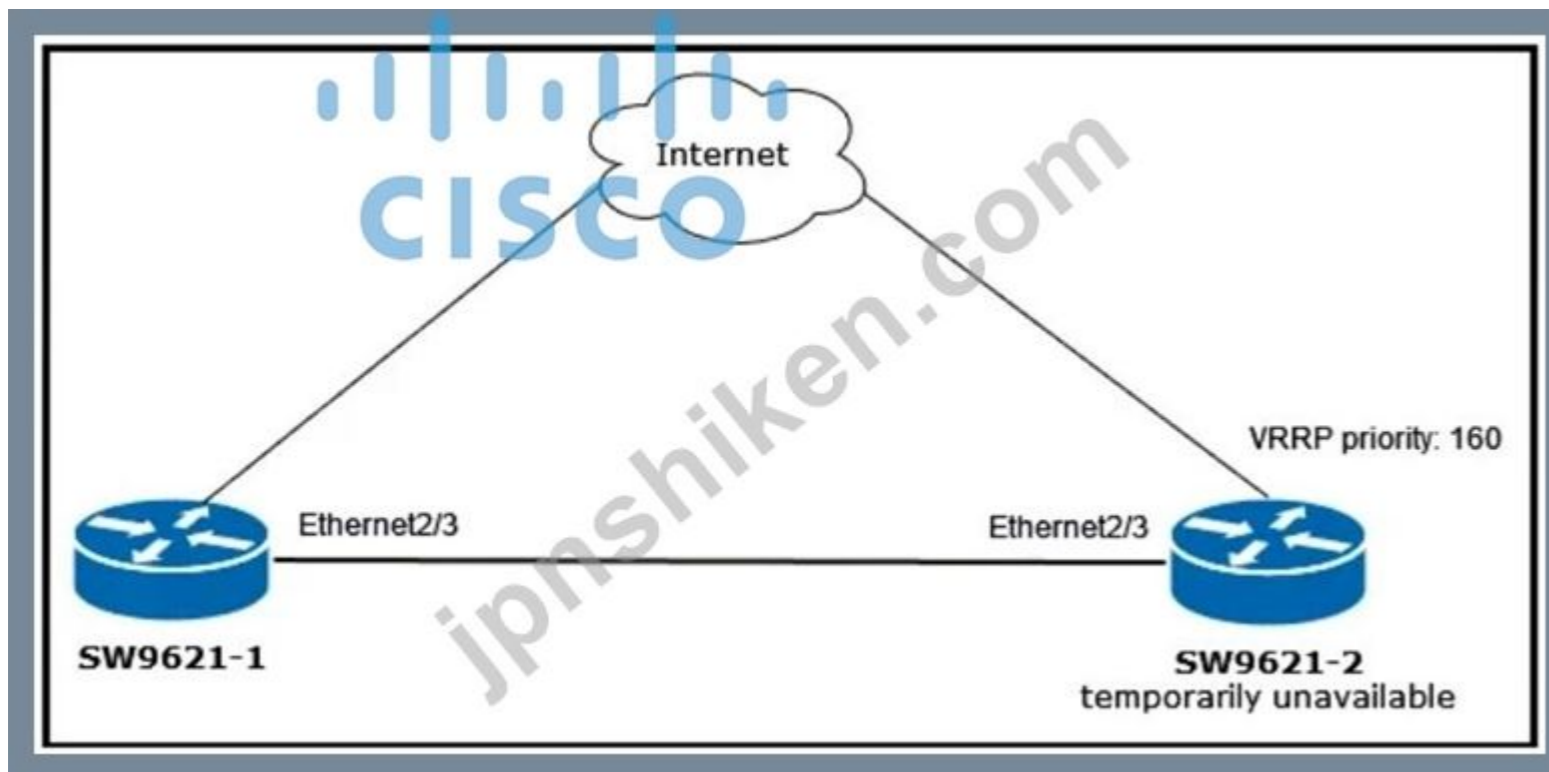
[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4\\_0/dcnm/security/configuration/guide/sec\\_dcnm](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_0/dcnm/security/configuration/guide/sec_dcnm) テキスト説明は自動生成されました

## Configuring a DHCP Server Address on a VLAN Interface

You can configure a DHCP server IP address on a VLAN interface (sometimes referred to as a switched virtual interface or SVI). When an inbound DHCP BOOTREQUEST packet arrives on the VLAN interface, the relay agent forwards the packet to the IP address specified.

質問: 191

図を参照してください。ルーターSW9621-2が稼働状態になると、VRRPの設定はどうなりますか？



```

SW9621-1# show vrrp detail
Ethernet2/3 - Group 100 (IPV4)
State is Master
Virtual IP address is 192.168.30.100
Priority 100, Configured 100
Forwarding threshold(for VPC), lower: 1 upper: 100
Advertisement interval 3
Preemption enabled
Authentication text "D458F7B032E4632090EF06EE5A"
Virtual MAC address is 0000.5e00.0164
Master router is Local

```

- A. SW9621-2ルーターが新しいアクティブマスターになります。
- B. SW9621-1ルーターは3秒後に新しいアクティブマスターになります。
- C. SW9621-1ルーターはアクティブなマスターのままです。
- D. SW9621-2ルーターは3秒後にアクティブマスターになります。

正解: **A** ([コメントを发表する](#))

[https://www.cisco.com/assets/sol/sb/Switches\\_Emulators\\_v2\\_3\\_5\\_xx/help/350\\_550/index.html#page/tesla\\_350\\_550\\_olh/ts\\_vrrp\\_18\\_09.html](https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_3_5_xx/help/350_550/index.html#page/tesla_350_550_olh/ts_vrrp_18_09.html)

2番目のスイッチは優先度160で、電源投入後にアクティブになります。プリエンプションは有効です。

広告間隔は、検出に失敗したノードを意味し、ダウンを検出するための重要なメトリックであるタイムアウト間隔があります。これは広告間隔の3倍です。プリエンプション遅延はプリエンプションに関連しています。

質問: **192**

デュアルスーパーバイザを備えたCisco MDSストレージスイッチのファームウェアをアップグレードする場合、正しい記述はどれですか？

- A. 両方のスーパーバイザーが新しいファームウェアをロードし、その後アクティブなスーパーバイザーが再起動します。

- B. スーパーバイザーは個別にアップグレードして新しいファームウェアをテストできます。
- C. 新しいファームウェアは、まずスタンバイスーパーバイザーにロードされます。
- D. ファームウェアのアップグレードを開始する前に、スタンバイスーパーバイザーがオフラインになっている必要があります。

正解: (正解を表示します)

[https://www.cisco.com/c/en/us/support/docs/storage-networking/mds-9000-nx-os-san-os-software/118952-technote-mds9k-00.html#:~:text=On%20a%2095xx%20or%2097xx,becomes%20the%20new%20standby%](https://www.cisco.com/c/en/us/support/docs/storage-networking/mds-9000-nx-os-san-os-software/118952-technote-mds9k-00.html#:~:text=On%20a%2095xx%20or%2097xx,becomes%20the%20new%20standby%20)

20人の監督者。

質問: 193

図を参照してください。エンジニアがCisco MDS 9000シリーズスイッチを初めて設定しているところです。

初期設定後、IPアドレス192.168.10.11のネームサーバーが設定から欠落しています。設定を完了するには、どのような操作を行う必要がありますか？

```
Step 20 Enter no (no is the default) if you are satisfied with the configuration.

The following configuration will be applied:

switchname CiscoMDS
 interface mgmt0
   ip address 192.168.10.10
   subnetmask 255.255.255.0
   no shutdown
 ip default-gateway 192.168.10.1
 telnet server enable
 no ssh server enable
 no system default switchport shutdown
 system default switchport trunk mode on
 no zone default-zone permit vsan 1-4093
 zoneset distribute full vsan 1-4093
Would you like to edit the configuration? (yes/no) [n]: no

Step 21 Enter yes (yes is default) to use and save this configuration.

Use this configuration and save it? (yes/no) [y]: yes
```

- A. ステップ21で「いいえ」と入力し、スイッチを再起動します。高度なIPオプションを設定します。
- B. ステップ21で「はい」と入力してログインします。起動設定のDNSを変更します。
- C. 手順21で「no」と入力し、インストーラーを再初期化します。Escキーを押してROMMONモードにアクセスします。
- D. ステップ21で「はい」と入力して設定を編集します。dns-server 192.168.10.11という行を追加します。

正解: ([正解を表示します](#))

質問: 194

```
NEXUS(config)# radius-server timeout 15
NEXUS(config)# ip radius source-interface Vlan100
NEXUS(config)# radius-server host 10.1.50.31 key 7 "Fewhg1234"
authentication accounting
NEXUS(config)# aaa group server radius RADIUS
NEXUS(config-radius)# server 10.1.50.31
NEXUS(config-radius)# deadtime 10
NEXUS(config-radius)# use-vrf management
NEXUS(config-radius)# source-interface mgmt 0
NEXUS(config)# aaa authentication login default group RADIUS
```

図を参照してください。この構成を実装した結果はどうなりますか？

- A. RADIUSサーバーのタイムアウト値は15ミリ秒です。
- B. RADIUSトラフィックはVLAN 200インターフェースから発信されます。
- C. ユーザーはログイン時にRADIUSサーバーを指定します。
- D. 認証にはRADIUSサーバーのみが使用されます。

正解: ([正解を表示します](#))

セクション :セキュリティ

質問: 195

エンジニアは、UCS-A という名前のプライマリファブリックと、UCS-B という名前のセカンダリファブリックを持っています。kr2016 という名前のキーリングに対して、サブジェクト名が sjc2016 の証明書要求を作成する必要があります。

クラスターのIPアドレスは10.68.68.68です。この証明書要求を作成するコマンドセットはどれですか？

A)

```
UCS-A # scope keyring kr2016
UCS-A /keyring # create certreq 10.68.68.68 sjc2016
UCS-A /keyring* # commit-buffer
```

B)

```
UCS-A# scope security
UCS-A /security # scope keyring kr2016
UCS-A /security/keyring # create certreq ip 10.68.68.68 subject-name sjc2016
UCS-A /security/keyring* # commit-buffer
```

C)

```
UCS-A# scope security
UCS-A /security # scope keyring kr2016
UCS-A /security/keyring # create certreq ip 10.68.68.68 subject-name sjc2016
UCS-A /security/keyring* # commit-buffer
```

D)

```
UCS-B # scope keyring kr2016
UCS-B /keyring # create certreq ip 10.68.68.68 subject-name sjc2016
UCS-B /keyring* # commit-both
```

- A. 選択肢D
- B. オプションB
- C. オプションA
- D. オプションC

正解: D ([コメントを发表する](#))

質問: 196

展示資料を参照してください。

```
Nexus(config)# show checkpoint summary
User Checkpoint Summary
-----
1) BeforeL3:
Created by admin
Created at Mon, 15:25:08 31 Dec 2018
Size is 9,345 bytes
Description: None

System Checkpoint Summary
-----
2) system-fm-vrrp:
Created by admin
Created at Fri, 09:57:02 14 Jun 2019
Size is 20,865 bytes
Description: Created by Feature Manager.

3) system-fm-hsrp_engine:
Created by admin
Created at Fri, 09:57:28 14 Jun 2019
Size is 20,852 bytes
Description: Created by Feature Manager.
```

system-fm-vrrpチェックポイントが作成された理由は何ですか？

- A. VRRPサービスが再起動され、チェックポイントが自動的に作成されました。
- B. ネットワーク管理者が手動で作成しました。
- C. VRRPプロセスがクラッシュし、チェックポイントが自動的に作成されました。

D. VRRP有効化機能が無効になっています。

正解: D ([コメントを发表する](#))

説明

VRRP機能が無効になっている場合にNexusによって自動的に作成されます。

有効的な**350-601**問題集はJPNTTest.com提供され、**350-601**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-601**試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで**350-601**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> **384**問、**30%ディスカウント**、特別な割引コード:

**JPNshiken**」

質問: **197**

どの構成で静的インGRESレプリケーションが実装されますか？

A. インターフェース nve 1

メンバー番号 vni 2100980

インGRESレプリケーションプロトコル静的

ピアIP 10.0.0.4

B. インターフェース nve 1

メンバー番号 vni 384233213

ピアvtep 10.0.0.41

C. インターフェース nve 1

メンバー vni 127772151

インGRESレプリケーションプロトコルbgp

D. インターフェース nve 1

メンバー番号 vni 3126980

peervtep 10.0.0.4

インGRESレプリケーションプロトコル静的

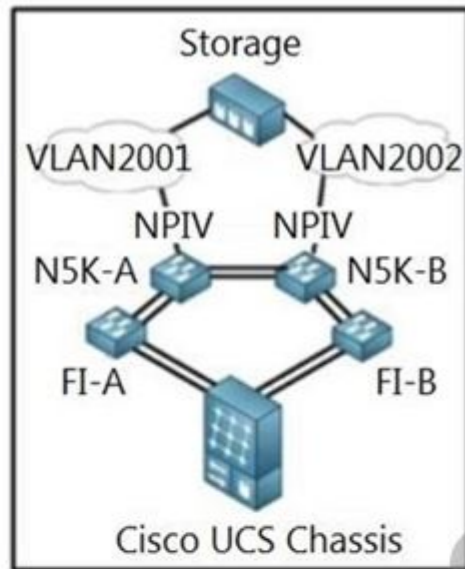
ピアIP 10.0.0.4

正解: ([正解を表示します](#))

質問: **198**

図を参照してください。エンジニアがネットワーク上でVSANを構成しています。

VSANを作成するには、どのオプションを選択する必要がありますか？



**Create VSAN**

Name:

**FC Zoning Settings**

FC Zoning:  Disabled  Enabled

Do **NOT** enable local zoning if fabric interconnect is connected to an upstream FC/FCoE switch.

Common/Global  Fabric A  Fabric B  Both Fabrics Configured Differently

You are creating a global VSAN that maps to the same VSAN ID in all available fabrics. A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.

Enter the VSAN ID that maps to this VSAN. Enter the VLAN ID that maps to this VSAN.

VSAN ID:  FCoE VLAN:

- A. 生地B
- B. FCゾーニング有効
- C. 生地A
- D. 共通/グローバル

正解: (正解を表示します)

VSANは、ドメイングループのルートまたは特定のドメインに作成できます。また、VSANをファブリックAまたはファブリックB、あるいはファブリックAとBの両方に割り当てることもできます。VSANを両方のファブリックに割り当てる場合は、両方のファブリックに異なるVSAN IDとFCoE VLAN IDを設定する必要があります。

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/ucs-central/GUI-User-Guides/Storage-](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-central/GUI-User-Guides/Storage-Mgmt/1-5/b_CiscoUCSCentral_Storage_Management_Guide_1-5/b_CiscoUCSCentral_Storage_Management_Guide_1-5_chapter_011.pdf)

[Mgmt/1-5/b\\_CiscoUCSCentral\\_Storage\\_Management\\_Guide\\_1-5/b\\_CiscoUCSCentral\\_Storage\\_Management\\_Guide\\_1-5\\_chapter\\_011.pdf](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-central/GUI-User-Guides/Storage-Mgmt/1-5/b_CiscoUCSCentral_Storage_Management_Guide_1-5/b_CiscoUCSCentral_Storage_Management_Guide_1-5_chapter_011.pdf)

#### 質問: 199

エンジニアは、Cisco Nexus 9000シリーズスイッチのEEM (エンタープライズ環境管理) 画面で、これらのコマンドを入力します。

イベントマネージャーアプレット Backup-config

イベントタイマー ウォッチドッグ 時間 1800 名前 タイマー

イベント cli マッチ "copy running-config startup-config"

この設定を適用した結果はどうなりますか？

- A. copy running-config startup-config コマンドをブロックします。
- B. copy running-config startup-config コマンドを実行します。
- C. アクションが指定されていないため、エラーが発生します。
- D. 1800秒ごとに実行中の設定を保存します。

正解: [\(正解を表示します\)](#)

#### 質問: 200

エンジニアは、Cisco Intersight SaaSプラットフォームによる監視および管理のために、Cisco UCSドメインを構成する必要があります。セットアップが完了したら、管理者はCisco UCS ManagerとIntersightを介してデバイスを構成するための完全な制御権限を持つ必要があります。このタスクを実行するには、どの操作を実行すればよいでしょうか？

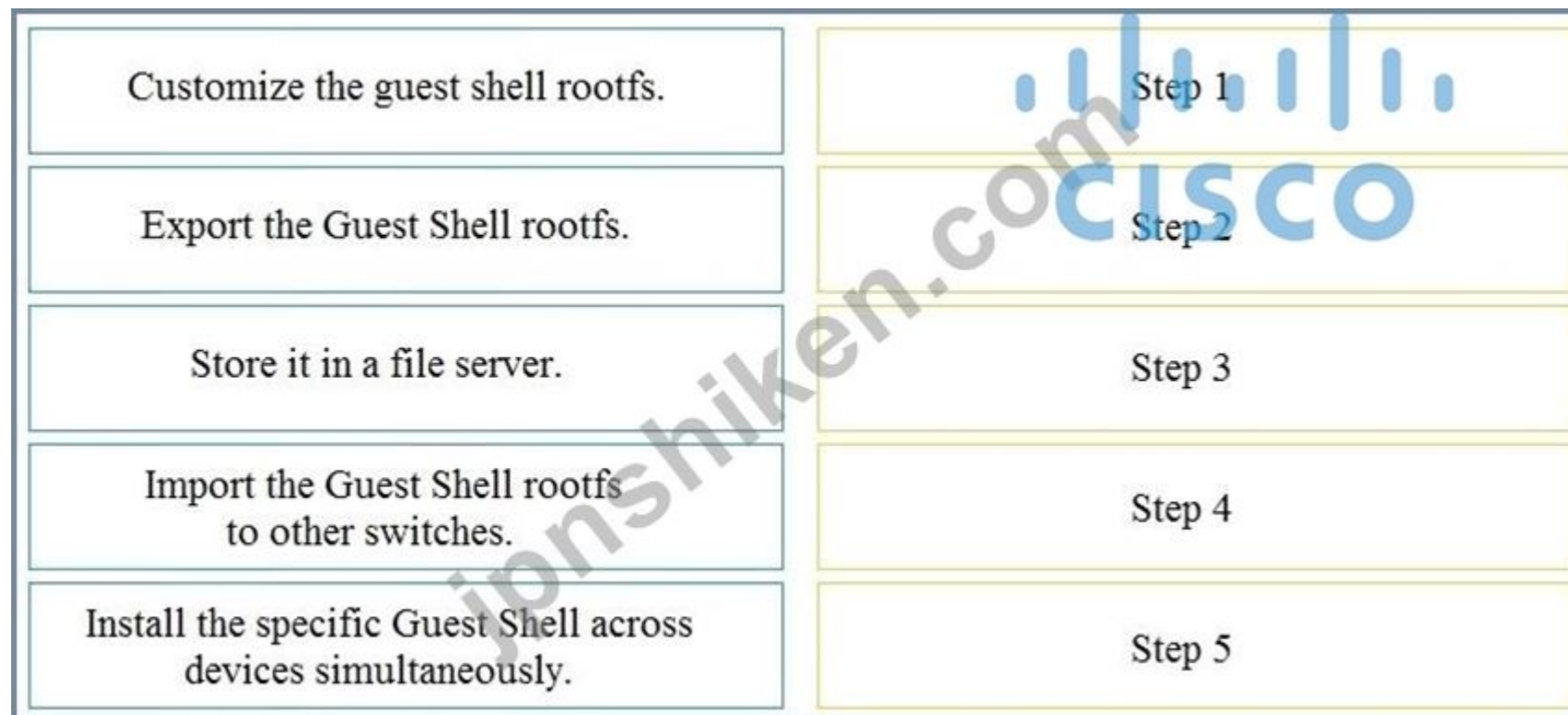


- A. オプションC
- B. オプションD
- C. オプションB
- D. オプションA

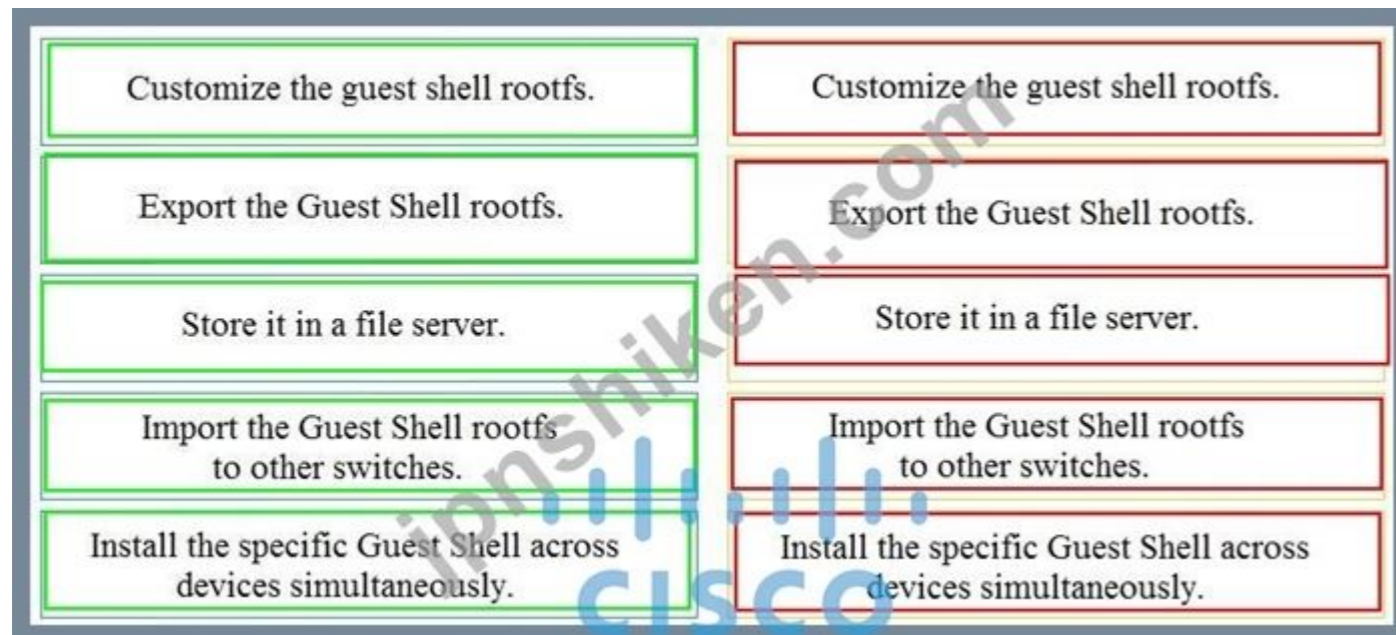
正解: [A \(コメントを发表する\)](#)

#### 質問: 201

エンジニアがNexus 9000シリーズスイッチにカスタムゲストシェルルートファイルシステムをデプロイします。左側の手順をドラッグアンドドロップして、右側のソリューションをデプロイするために必要な順序に並べ替えてください。すべてのオプションを使用するわけではありません。



正解:



質問: 202

エンジニアがマルチキャストをサポートするトランスポート上でOTVを実装しようとしています。このソリューションは以下の要件を満たす必要があります。

マルチキャストを使用して、リモートピアとの隣接関係を確立します。

\* VLAN 100 から他のサイトへの OTV アドバタイズメントを有効にします。

これらの要件を満たすために設定すべきコマンドはどれですか？ 2つ選択してください。)

- A. otvサイトVLAN 100
- B. otvデータグループ232.2.2.0/28
- C. otv use-adjacency-server 172.27.255.94
- D. 拡張VLAN 100を開く

E. otv コントロールグループ 232.1.1.1

正解: ([正解を表示します](#))

[https://www.cisco.com/c/dam/en/us/products/collateral/switches/nexus-7000-series-switches/guide\\_c07-728315](https://www.cisco.com/c/dam/en/us/products/collateral/switches/nexus-7000-series-switches/guide_c07-728315).

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/OTV/config\\_guide/b\\_Cisco\\_Nexus\\_7000\\_S](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/OTV/config_guide/b_Cisco_Nexus_7000_S)

質問: 203

どの構成で静的イングレスレプリケーションが実装されますか？

**interface nve 1**  
**member vni 3716135**  
**ingress-replication protocol bgp**

**interface nve 1**  
**member vni 3716135**  
**peer vtep 10.0.0.4**

**interface nve 1**  
**member vni 3716135**  
**peer vtep 10.0.0.4**  
**ingress-replication protocol static**  
**peer-ip 10.0.0.4**

**interface nve 1**  
**member vni 3716135**  
**ingress-replication protocol static**  
**peer-ip 10.0.0.4**

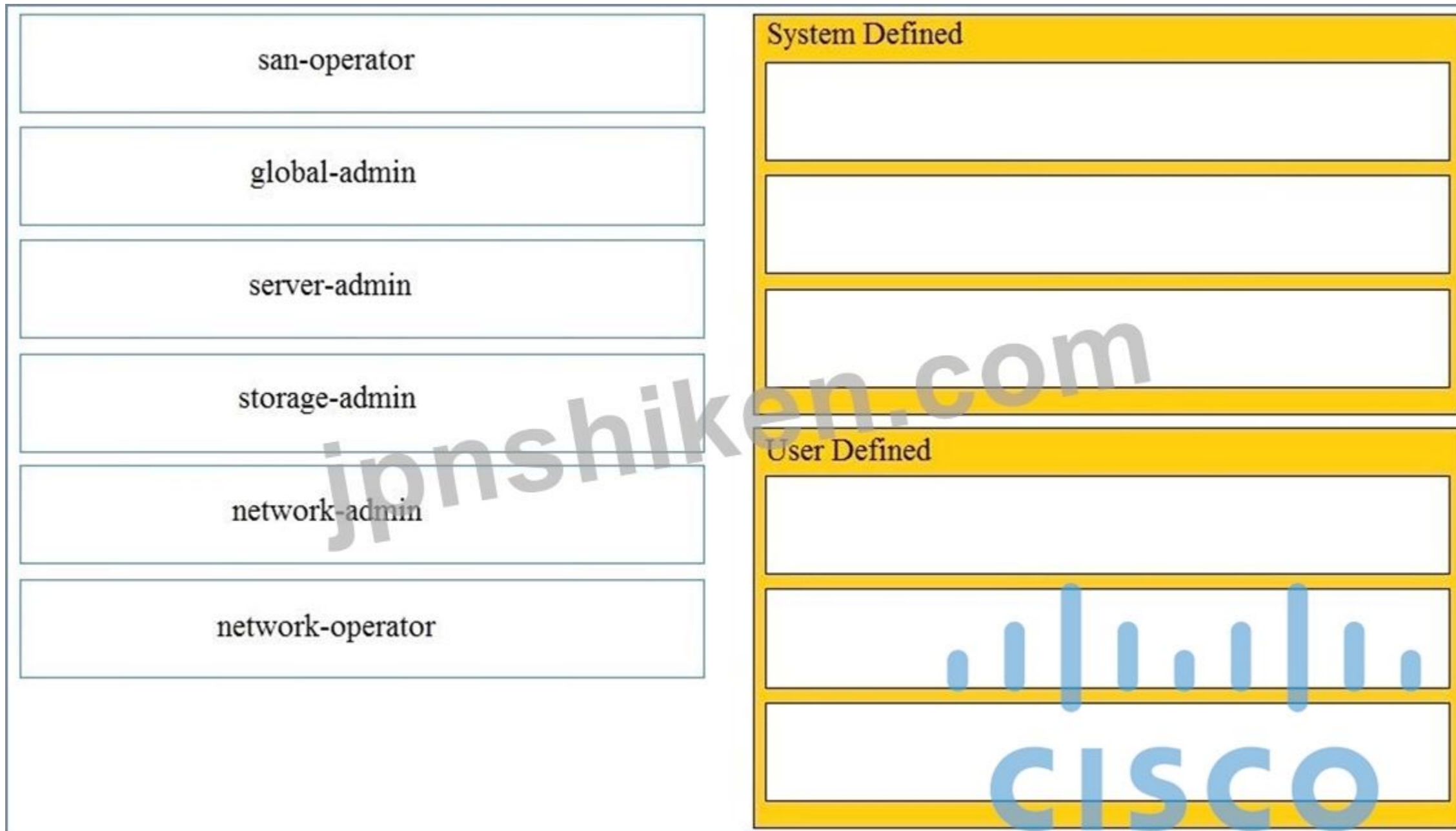
正解: ([正解を表示します](#))

セクション: ネットワーク

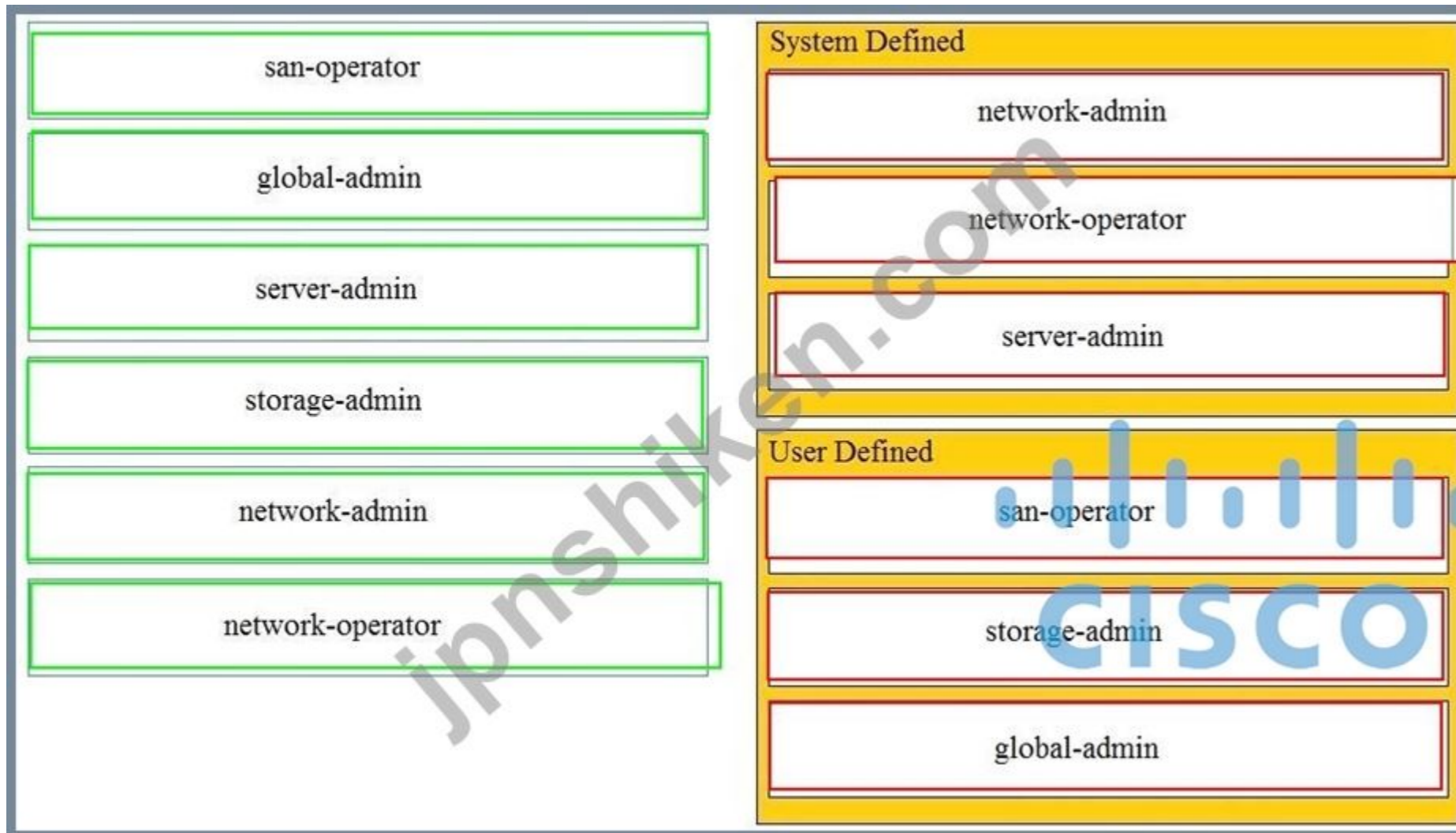
質問: 204

ネットワークエンジニアは、Cisco MDS 9000シリーズマルチレイヤースイッチにRBACを実装する必要があります。

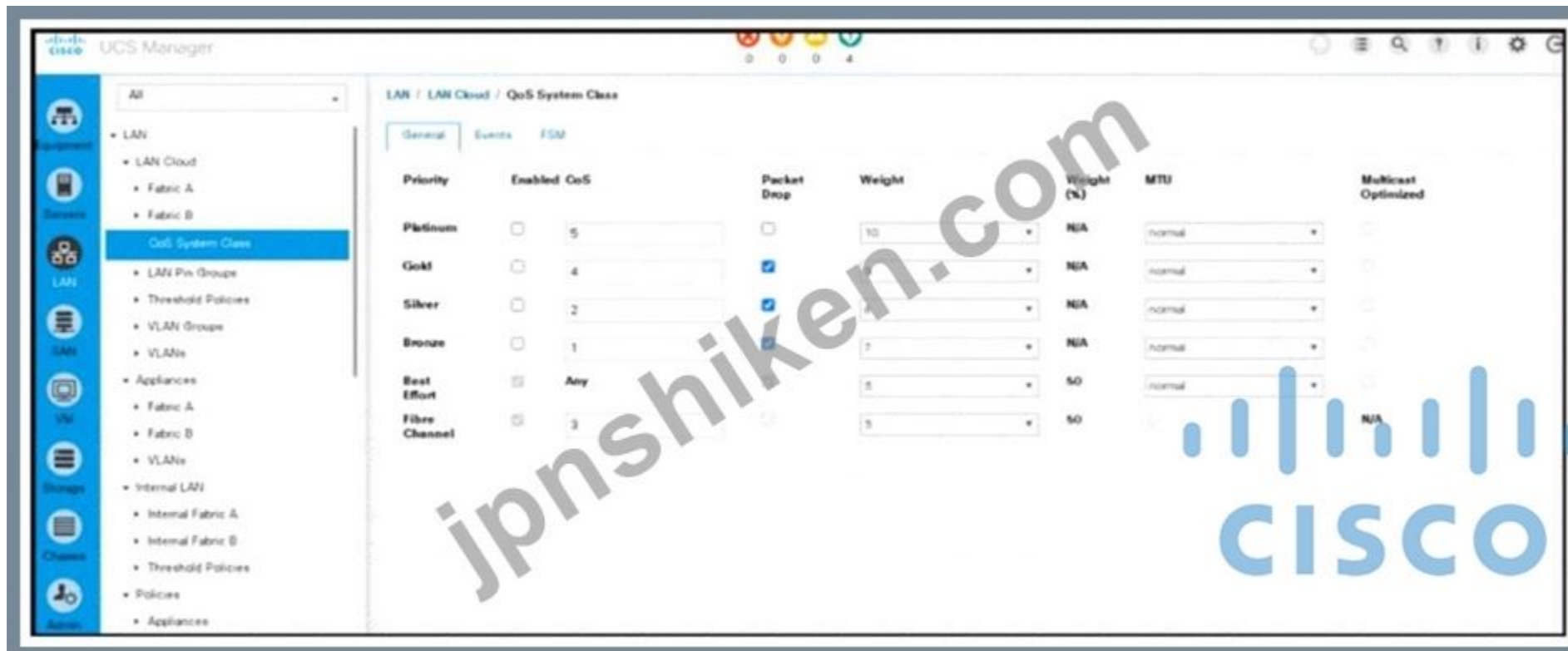
左側のCisco MDS 9000シリーズの役割を、右側の適切なカテゴリにドラッグアンドドロップしてください。



正解:



質問: 205





図を参照してください。エンジニアがクライアントPCとDHCPサーバー間の断続的な接続問題のトラブルシューティングを行っています。Cisco Nexus 2000シリーズスイッチから最後にキャプチャされたパケットは何を示していますか？

- A. クライアントはユニキャストメッセージを送信して、DHCPサーバーからIPアドレスを受信します。
- B. DHCPサーバーはクライアントからIPアドレスを解放します。
- C. クライアントはDHCPサーバーからIPアドレスを取得します。
- D. DHCPサーバーはブロードキャストメッセージを介してIPアドレスを送信します。

正解: [\(正解を表示します\)](#)

#### 質問: 208

Cisco MDS 9000シリーズストレージスイッチが予期せず再起動しました。

エンジニアは最新のコアダンプファイルをどこで探すのでしょうか？

- A. /mnt/recovery
- B. /mnt/core
- C. /mnt/logs
- D. /mnt/pss

正解: [\(正解を表示します\)](#)

最後のコアをブートフラッシュに保存

この最後のコアダンプは、切り替えまたは再起動が行われる前に、/mnt/pss/パーティション内のbootflashに自動的に保存されます。

スーパーバイザモジュールが再起動してから3分後、保存された最後のコアがフラッシュパーティション /mnt/pss)から元のRAMの位置に復元されます。

この復元処理はバックグラウンドで行われるため、ユーザーには表示されません。

復元された最後のコアファイルのタイムスタンプは、最後のコアが実際にダンプされた時刻ではなく、スーパーバイザが起動した時刻を示しています。

最後のコアダンプが発生した正確な時刻を知るには、同じPIDを持つ対応するログファイルを確認してください。

最新のコア情報を表示するには、EXECモードでshow coresコマンドを入力します。

実際の最後のコアダンプが発生した時刻を確認するには、EXECモードでshow process logコマンドを入力してください。

参照 :

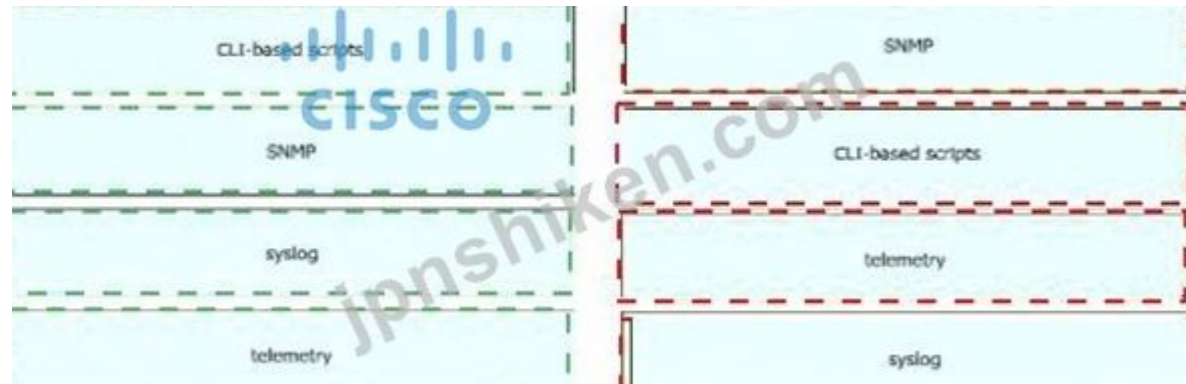
[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6\\_2/configuration/guides/system\\_management/nx-os/sysmgmt\\_cli\\_6-x/sys.html#64619](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6_2/configuration/guides/system_management/nx-os/sysmgmt_cli_6-x/sys.html#64619)

#### 質問: 209

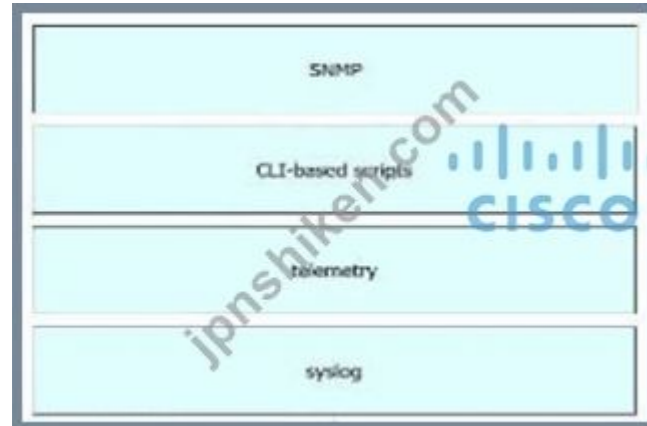
左側のネットワークからデータを収集する仕組みを、右側のそれぞれの特性の上にドラッグ&ドロップしてください。



正解:



Explanation:



質問: 210

展示資料を参照してください。

```

Start time: Mon Apr 15 09:23:01 2019
Last election time: Mon Apr 15 09:24:24 2019
A: UP, PRIMARY
B: UP, SUBORDINATE
A: memb state UP, lead state PRIMARY, mgmt services state: UP
B: memb state UP, lead state SUBORDINATE, mgmt services state: UP
heartbeat state PRIMARY_OK
INTERNAL NETWORK INTERFACES:
eth1, UP
eth2, UP
HA NOT READY
No device connected to this Fabric Interconnect

```

HA NOT READY状態を解除するには、何を接続すればよいですか？

- A. サーバーシャーシ
- B. ネットワークアップリンク
- C. レイヤ1-レイヤ2ポート
- D. 管理ポート

正解: A (コメントを发表する)

質問: 211

展示資料を参照してください。

```
switch(config-dest)# sensor-group 100
switch(conf-tm-sensor)# path show_stats_fc3/1
switch(conf-tm-sensor)# subscription 100
switch(conf-tm-sub)# 
switch(conf-tm-sub)# dst-grp 100
```

図を参照してください。エンジニアは、Cisco MDS 9000 シリーズ スイッチでストリーミング テレメトリを実装する必要があります。要件は、show コマンドのデータを 30 秒ごとに収集し、受信側に送信することです。この要件を満たすには、どのコマンドを構成に追加する必要がありますか？

- A. センサーグループ200、サンプル周期30000
- B. Snsr-grp 200 サンプル間隔 30
- C. センサーグループ200、サンプル周期30
- D. Snsr-grp 200 サンプル間隔 30000

正解: **D** ([コメントを发表する](#))

snsr-grp <id> sample-interval <interval> 現在、センサーグループIDは数値ID値のみをサポートしています。ストリーミングサンプル間隔値を指定します。値はミリ秒単位で指定する必要があります。サポートされている最小ストリーミングサンプル間隔は30000ミリ秒です。 [https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8\\_x/config/san\\_analytics/cisco-mds9000-san-analytics-telemetry-streaming-config-guide-8x/configuring-san-telemetry-streaming.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/san_analytics/cisco-mds9000-san-analytics-telemetry-streaming-config-guide-8x/configuring-san-telemetry-streaming.html)

有効的な**350-601**問題集はJPNTTest.com提供され、**350-601**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-601**試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで**350-601**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> **384**問、**30%ディスカウント**、特別な割引コード:

**JPNshiken**」

質問: **212**

エンジニアは、Cisco Nexus 9000シリーズスイッチ上でファイバーチャネルポートチャネルを設定する必要があります。設定は以下の要件を満たす必要があります。

- \* ピアポートとの間でポートチャネルプロトコルのネゴシエーションが実行されます。
- \* トランクモードは、インターフェースごとに明示的に設定する必要があります。
- \* 10~20個のVSANを許可する必要があります。

要件を満たすようにデバイスを設定するコマンドセットはどれですか？

interface san-port-channel 10  
channel mode on  
switchport trunk mode on  
switchport trunk allowed vsan 10, 20

interface san-port-channel 10  
channel mode active  
switchport trunk mode on  
switchport trunk allowed vsan 10-20

interface port-channel 10  
channel mode on  
switchport trunk mode active  
switchport trunk allowed vsan 10, 20

interface port-channel 10  
channel mode auto  
switchport trunk mode on  
switchport trunk allowed vsan 10-20

通过测试

A. オプションA

B. 選択肢D

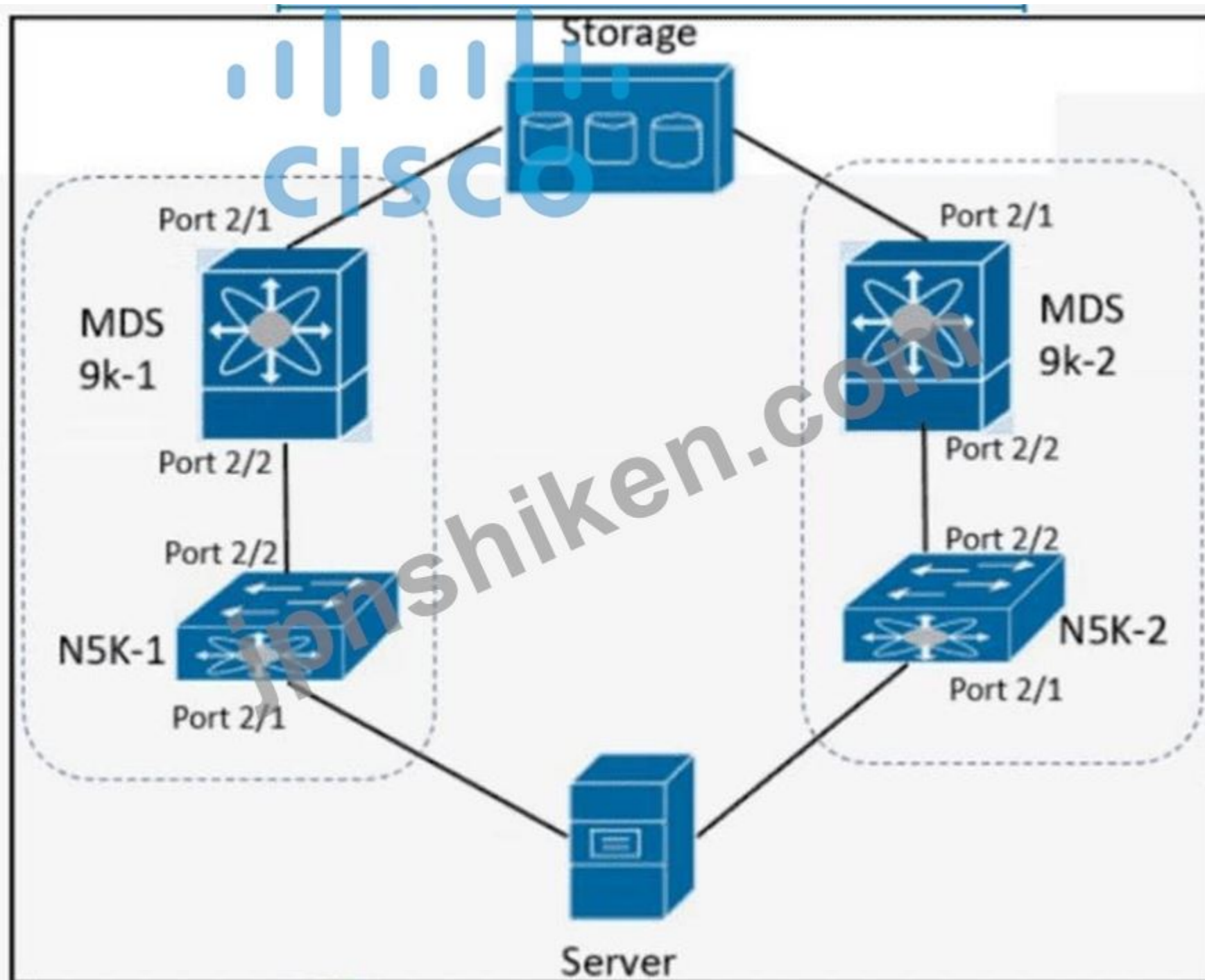
C. オプションC

D. オプションB

正解: ([正解を表示します](#))

質問: 213

展示資料を参照してください。



サーバーはファイバーチャネルプロトコルを使用してストレージサーバーにトラフィックを送信しています。要件は、N5K-1がトラフィックをMDS9k-1に転送することです。右側の設定手順をドラッグアンドドロップして、左側のN5K-1の設定を完了してください。すべての設定手順を使用するわけではありません。

N5K-1# configuration terminal	interface fc 2/1
N5K-1#(config)#	interface port 2/1
N5K-1#(config)# interface fc 2/2	interface port 2/2
N5K-1#(config-if)#	npv enable
N5K-1#(config-if)# no shutdown	switchport mode F
N5K-1#(config)#	switchport mode NP
N5K-1#(config-if)#	
N5K-1#(config-if)# no shutdown	

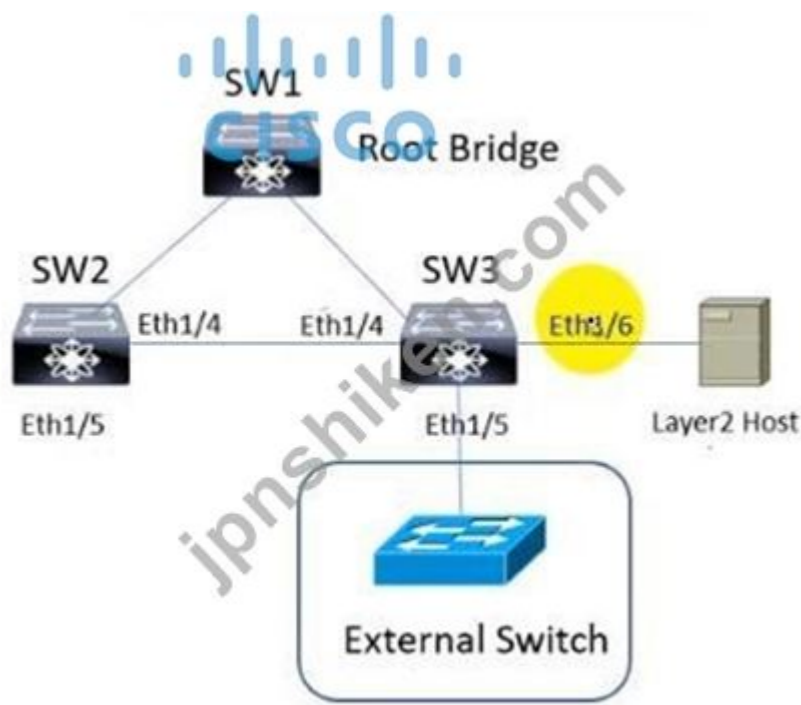
正解:

N5K-1# configuration terminal	interface fc 2/1
N5K-1#(config)# npv enable	interface port 2/1
N5K-1#(config)# interface fc 2/2	interface port 2/2
N5K-1#(config-if)# switchport mode F	npv enable
N5K-1#(config-if)# no shutdown	switchport mode F
N5K-1#(config)# interface fc 2/1	switchport mode NP
N5K-1#(config-if)# switchport mode NP	
N5K-1#(config-if)# no shutdown	

Explanation:

npv 有効化、スイッチポートモード F、インターフェース fc2/1、スイッチポートモード NP

質問: 214



図を参照してください。Cisco NexusシリーズスイッチSW1、SW2、およびSW3は、レイヤ2銅線インターフェイスを介して接続されています。エンジニアは、ネットワークの変更または障害からの迅速な復旧を実現するために、各VLANにループ防止規格IEEE 802.1wを実装します。この実装には、以下の要件があります。

- \* レイヤ2ホストに接続されているインターフェイスは、STP BPDUを受信してはなりません。
- \* 実装では、一方向トラフィックのツイストペアリンクによる単方向リンクを検出する必要があります。
- \* SW2とSW3の間でブリッジアシュアランスを有効にする必要があります。
- \* レイヤ2ドメインは、外部スイッチから到着する上位BPDUから保護されなければならない。

右側のコードスニペットを左側のコードの空欄にドラッグ&ドロップして、SW3の設定を完了してください。すべてのコードスニペットを使用するわけではありません。

```

! SW3 configuration
interface ethernet 1/4
  spanning-tree port type
  udid
interface ethernet 1/5
  spanning-tree guard
interface ethernet 1/6
  spanning-tree port type
  
```

edge  
aggressive  
normal  
network  
root  
bpdu

正解:

```

! SW3 configuration
interface ethernet 1/4
  spanning-tree port type network
  udid aggressive
interface ethernet 1/5
  spanning-tree guard bpdu
interface ethernet 1/6
  spanning-tree port type edge
  
```

Explanation:

ネットワーク  
攻撃的  
BPDU

角

質問: 215

ネットワーク管理者が、Linuxサーバー上で動作するカスタムDjangoセルフサービスポータルを作成し、Cisco UCS Managerで新しいVLANの作成を自動化しようとしています。サーバーにインストールおよび構成する必要がある機能はどれですか？

- A. Cisco DNA Center API
- B. Cisco AppDynamics
- C. Cisco UCS PowerTool Suite
- D. Cisco UCS Python SDK

正解: [\(正解を表示します\)](#)

質問: 216

OTVをサポートするためには、エンジニアが同じデータセンター内に設置した2台のCisco Nexus 7000シリーズスイッチを設定する必要があります。

どのコマンドセットで参加インターフェースの設定が完了しますか？

An engineer must configure two Cisco Nexus 7000 Series switches in the same data center to support OTV. Which command set completes the join interface configuration?

```
feature otv
otv site-identifier 256
interface overlay 1
otv control-group 239.1.1.1
otv data-group 239.1.1.0/29
otv join-interface ethernet 2/1
otv extend-vlan 5-10
...
```

- Edge Device 1
  - interface ethernet 2/1
  - ip address 192.0.2.1/24
  - ip igmp version 3
- Edge Device 2
  - interface ethernet 2/1
  - ip address 192.0.2.16/24
  - ip igmp version 3

A.

jpnshiken.com



```
Edge Device 1
interface ethernet 2/1
ip address 192.0.2.1/24
ip igmp version 3
ip pim sparse-mode

Edge Device 2
interface ethernet 2/1
ip address 192.0.2.16/24
ip igmp version 3
ip pim sparse-mode
```

B.

```
Edge Device 1
interface ethernet 2/1
ip address 192.0.2.1/24

Edge Device 2
interface ethernet 2/1
ip address 192.0.2.16/24
```

C.

```
Edge Device 1
interface ethernet 2/1
ip address 192.0.2.1/24
ip igmp version 3

Edge Device 2
interface ethernet 2/1
ip address 192.0.2.1/24
ip igmp version 3
```

D.

正解: [B \(コメントを发表する\)](#)

Cisco Nexus 7000シリーズスイッチ2台をOTV対応に設定する場合、オプションAが正解です。この設定では、エッジデバイスに特定のインターフェイスイーサネットとIPアドレスを設定します。オプションAで指定されているコマンドは、Cisco Nexus 7000シリーズスイッチでOTV参加インターフェイスを設定するための要件と一致しています。これらのコマンドにより、エッジデバイスがOTV経由で通信できるように適切に設定されます。

質問: 217

どのMACアドレスがHSRPバージョン2ですか？

A. 0100.5E7F.FFFF

B. 3799.9943.3000

C. 0000.0C9F.F0C8

D. 0000.0C07.AC1H

正解: [\(正解を表示します\)](#)

HSRPバージョン2では、グループ番号の範囲が0～4095に拡張され、その結果、新しいMACアドレス範囲0000.0C9F.F000～0000.0C9F.FFFFが使用されます。

グループ数の範囲が拡大されたからといって、インターフェイスがその数のHSRPグループをサポートできる、あるいはサポートすべきであるという意味ではありません。

拡張されたグループ番号の範囲が変更され、サブインターフェイス上のグループ番号がVLAN番号と一致するようになりました。

参照：

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp\\_fhrp/configuration/xs-3s/fhp-xe-3s-book/fhp-hsrp-v2.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/xs-3s/fhp-xe-3s-book/fhp-hsrp-v2.html)

質問: 218

展示資料を参照してください。

```
import time
import os

date= time.strftime('%Y%m%d')
file= ('fusion-config_') + date
os.execute ('copy running-config ftp://10.183.249.182/fusionSW/' + file)
exit()
```

図を参照してください。このPythonコードを実行すると、どのような結果になりますか？

- A. Ciscoデバイスのバックアップをリモートの宛先に送信します。
- B. スイッチの設定をCisco TACに送信します。
- C. EEMを使用してCiscoスイッチのバックアップをスケジュールします。
- D. CiscoスイッチをCisco Primeインフラストラクチャにバックアップします。

正解: ([正解を表示します](#))

質問: 219

ネットワークアーキテクトが、企業向けにCisco HyperFlexの設計ソリューションを検討しています。提案されているソリューションは、パフォーマンスを重視しない仮想環境向けですが、大容量のストレージと低コストが求められます。どのCisco HyperFlexストレージ構成を使用すべきでしょうか？

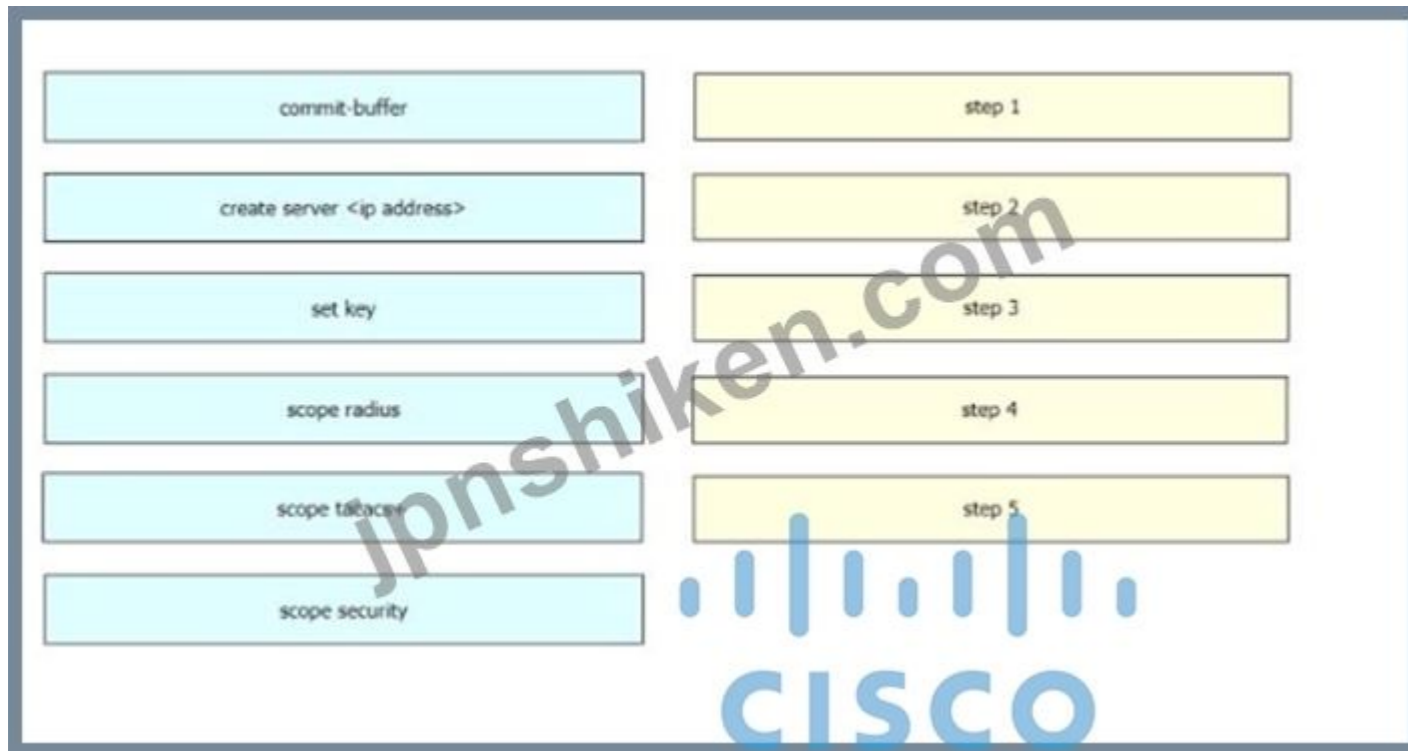
- A. オールSAN
- B. ハイブリッド
- C. オールフラッシュ
- D. オールNVMe

正解: ([正解を表示します](#))

<https://www.cisco.com/c/en/us/products/collateral/hyperconverged-infrastructure/hyperflex-hx-series/white-paper-c11-744026.html> ハイブリッドには容量のためにHDDが含まれています。

質問: 220

エンジニアは、Cisco UCS システムでリモート認証を設定する必要があります。ユーザーパスワードは、認証サーバーに送信する前に暗号化する必要があります。会社のセキュリティポリシーでは、サーバーはオープンスタンダードに基づいている必要があります。左側の UCS CLI AAA 設定コマンドを、右側の必須の順序にドラッグアンドドロップしてください。すべてのコマンドを使用するわけではありません。



正解:



質問: 221

エンジニアがCisco Nexus 9000シリーズスイッチのbashをアップグレードしている。

```

guestshell:~$ sudo [MISSING_COMMAND] /bootflash/bash-4.2_8642092948678a-r8x86_64.rpm.rpm
Preparing...
##### [100%]
1:bash ##### [100%]
update-alternatives: Linking //bin/sh to /bin/bash
  
```

タスクを完了するには、どのコマンドを使用する必要がありますか？

- A. rpm -qa
- B. rpm -Uhv
- C. アップグレード -U
- D. update -vh

正解: ([正解を表示します](#))

質問: 222

電子プログラマブルロジックデバイス (EPLD)のソフトウェアアップグレードの特徴は何ですか？

- A. EPLDソフトウェアは、Cisco TACの指示があった場合にのみアップグレードしてください。
- B. Cisco MDS NX-OSをアップグレードするには、EPLDソフトウェアもアップグレードする必要があります。
- C. ELPDモジュールのアップグレードは中断を伴いません
- D. ELPDのアップグレードは、ファブリックモジュールと電源モジュールで利用可能です。

正解: B ([コメントを発表する](#))

質問: 223

ファイバーチャネルと比較した場合、NFSの利点は何ですか？

- A. NFSはLUNのシンプロビジョニングを有効にします。
- B. NFSはストレージ容量の動的な割り当てを提供します。
- C. NFSはIPオーバーヘッドの影響を排除します。
- D. NFSは基盤となるストレージハードウェアへの直接アクセスを提供します。

正解: ([正解を表示します](#))

<https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2018/pdf/BRKINI-1011.pdf>

質問: 224

Cisco MDS 9000 シリーズ スイッチがポート チャネルを使用する環境において、エンジニアは、特定のフローにおいて送信元と宛先間のフレームが同じリンクを経由するようにする必要があります。後続のフローでは、異なるリンクを使用することが許可されます。この目的を達成するには、どのロード バランシング方式を使用すべきでしょうか？

- A. 送信元ID/宛先ID
- B. src-dst-oui
- C. 送信元送信先ポート
- D. src-id/dst-id/oxid

正解: ([正解を表示します](#))

Exchange ベース - Exchange 内の最初のフレームがリンクを選択し、Exchange 内の後続のフレームは同じリンクに従います。ただし、後続の Exchange では別のリンクを使用できます。これにより、各 Exchange のフレームの順序を維持しながら、よりきめ細かな負荷分散が可能になります。出典:

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/5\\_0/configuration/guides/int/nxos/cli\\_interfaces/pc.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/5_0/configuration/guides/int/nxos/cli_interfaces/pc.html) 負荷分散属性は、負荷分散パスの選択にソース宛先 ID (src-dst-id) または発信元 Exchange OX ID (src-dst-ox-id、デフォルト) を使用することを示します。出典: [https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6\\_2/configuration/guides/fabric/nx-os/nx\\_os\\_fabric/vsan.html?bookSearch=true](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6_2/configuration/guides/fabric/nx-os/nx_os_fabric/vsan.html?bookSearch=true)

質問: 225

エンジニアはCisco UCS Managerを外部ストレージレイに接続する必要があります。予算の制約により、エンジニアはCisco UCS ManagerをFCストレージポートに直接接続しなければなりません。この接続を完了するために実行する必要がある2つの操作はどれですか？ 2つ選択してください)

- A. ファブリックインターコネクトmエンドホストモードを設定します
- B. ストレージ接続ポリシーを作成する
- C. ファブリックインターコネクトをFCスイッチモードに設定する
- D. SANクラウドで必要なVSANを作成します

E. VSAN作成時にFCゾーニングを無効にする

正解: C,E (コメントを发表する)

質問: 226

エンジニアがNX-OS APIを使用してCisco Nexus 9000シリーズスイッチの自動化を行っています。どのコードスニペットが、有効期限が11月22日の「tacuser」という名前のローカルユーザーを作成しますか？

```
PUT http://10.91.14.12/api/policymgr/mo/uni/
{
  "aaaUser": {
    "email": "tacuser@cisco.com",
    "name": "tacuser",
    "createdAt": "2020-09-11T00:00:00.090210Z",
    "authorizations": {
      "authorizedZone": "VDC1",
      "expiresAt": "2021-11-22T00:00:00.000+00:00",
      "authorizedByName": "OPS",
      "authorizedByEmail": "ops@company.com"
    }
  }
}
```

A.

○ GET http://10.12.14.91/api/mo/sys/userext/user-tacuser.json

```
{
  {
    "aaaUserEp": {
      "attributes": {
        "childAction": "add",
        "dn": "sys/userext",
        "lcOwn": "local",
        "modTs": "2021-11-22T00:00:00.000+00:00",
        "pwdSecureMode": "yes",
        "pwdStrengthCheck": "no",
        "status": "",
        "uid": "0"
      }
    }
  }
}
```



B.

○ HEAD http://10.14.91.12/api/policymgr/mo/uni/userext.json

```
{
  "aaaUser": {
    "name": "tacuser",
    "phone": "",
    "pwd": "H97NW894SDASgQL",
    "expire": "yes",
    "aaaUserDomain": {
      "description": "",
      "name": "all",
      "rn": "userdomain-all"
    }
  }
}
```



C.

```
○ POST http://10.91.12.14/api/mo/sys/userext.json
{
  "aaaUserEp": {
    "children": [
      {
        "aaaUser": {
          "attributes": {
            "allowExpired": "no",
            "expiration": "2021-11-22T00:00:00.000+00:00",
            "expires": "yes",
            "name": "tacuser",
            "pwd": "AKw47PS3:g4M410:F501",
            "pwdEncryptType": "clear"
          }
        }
      }
    ]
  }
}
```

D.

正解: (正解を表示します)

有効的な350-601問題集はJPNTTest.com提供され、350-601試験に合格することに役に立ちます！JPNTTest.comは今最新350-601試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで350-601問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> 384問、30%ディスカウント、特別な割引コード:

**JPNshiken**

質問: 227

ネットワークエンジニアは、MDSスイッチのシステムログを設定する必要があります。メッセージは「警告」以上の重要度レベルで表示する必要があります。セキュリティ上の理由から、ユーザーは5分間操作がないとコンソールからログアウトする必要があります。これらの要件を満たすには、どの設定を適用する必要がありますか？

▶ MDS-A(config)# logging console 5  
MDS-A(config-console)# exec-timeout 300

▶ MDS-A(config)# line console  
MDS-A(config-console)# speed 38400  
MDS-A(config-console)# exec-timeout 5  
MDS-A(config)# logging console 4

▶ MDS-A(config)# console  
MDS-A(config-console)# speed 38400  
MDS-A(config-console)# session-limit 5  
MDS-A(config)# logging console 5

▶ MDS-A(config)# logging line 4  
MDS-A(config-console)# session-limit 300

- A. オプションA
- B. オプションB
- C. オプションC
- D. 選択肢D

正解: (正解を表示します)

DETAILED STEPS		
	Command or Action	Purpose
Step 1	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	<b>line console</b> <b>Example:</b> switch# line console switch(config-console)#	Enters console configuration mode.
Step 3	<b>databits bits</b> <b>Example:</b> switch(config-console)# databits 7	Configures the number of data bits per byte. The range is from 5 to 8. The default is 8.
Step 4	<b>exec-timeout minutes</b> <b>Example:</b> switch(config-console)# exec-timeout 30	Configures the timeout for an inactive session. The range is from 0 to 525600 minutes (8760 hours). A value of 0 minutes disables the session timeout. The default is 30 minutes.
Step 5		

質問: 228

エンジニアは Cisco UCS システムを復旧する必要があります。完全なバックアップはバックアップ SCP サーバーで利用可能です。Cisco UCS Manager の構成を復旧するには、どの操作を行う必要がありますか？



- A. オプションC
- B. オプションB
- C. オプションA
- D. 選択肢D

正解: (正解を表示します)

質問: 229

この出力に基づくと、どのストレージプロトコルが使用されていますか？

```
N9K# show interface vfc 1011
vfc1011 is trunking
Bound interface is Ethernet100/1/1
Hardware is Ethernet
Port WWN is 20:48:8c:96060:6f:0d:6e:99
Admin port mode is F, trunk mode is on
snmp link state traps are enabled
Port mode is TF
Port vsan is 11
Trunk vsans (admin allowed and active) (11)
Trunk vsans (up) (11)
Trunk vsans (isolated) ()
Trunk vsans (initializing) ()
<... output omitted ...>
```

- A. FCoE
- B. iSCSI
- C. SMB
- D. NFSv4

正解: [\(正解を表示します\)](#)

質問: 230

エンジニアがCisco MDS 9000シリーズスイッチでISSUアップグレードを実施しています。このアップグレードはスイッチのコントロールプレーンにどのような影響を与えますか？

- A. 次の再起動までダウンしたままです。
- B. アップデート中もずっと表示されます。
- C. 80秒以上140秒未満ダウン状態が続く。
- D. 80秒未満で停止します。

正解: [\(正解を表示します\)](#)

これらのファブリックスイッチにおける無停止アップグレードは、制御プレーンへの影響を80秒以内に抑えます。ただし、アップグレードが正常な停止範囲を超えて進行した場合、または障害が発生した場合は、ソフトウェアアップグレードが障害を引き起こす可能性があります。

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6\\_2/upgrade/guides/nx-os/upgrade.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6_2/upgrade/guides/nx-os/upgrade.html)

質問: 231

ネットワーク管理者は、10.0.0.0/8サブネット内のすべてのIPアドレスに対してpingを実行するプロセスを自動化する必要があります。

サブネットは既にCisco NexusスイッチのARPテーブルに登録されています。目的の出力を生成するために、bashコマンドをドラッグアンドドロップしてください。すべてのコマンドを使用するわけではありません。

```

bash-4.3$ | grep --10\.- |
--- 10.1.0.2 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
--- 10.1.0.77 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss

```

awk '{print "ping" \$1}'     egrep "statistics|loss"     grep -v "statistics|loss"     sed -e 's/ping /10./g'  
 show ip arp     vsh     vsh -c "show ip arp"

正解:

```

bash-4.3$ | grep --10\.- |
--- 10.1.0.2 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
--- 10.1.0.77 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss

```

awk '{print "ping" \$1}'     egrep "statistics|loss"     grep -v "statistics|loss"     sed -e 's/ping /10./g'  
 show ip arp     vsh     vsh -c "show ip arp"

Explanation:

vsh -c "show ip arp", awk'{print "ping" \$1}', vsh, egrep "statistics|loss"

質問: 232

ネットワークエンジニアは、サードパーティ製のロードバランサーに接続された2台のCisco Nexusスイッチ上でvPCを構成する必要があります。接続は以下の要件を満たす必要があります。

- \* ポートチャネルは、オープンスタンダードプロトコルを介してロードバランサーとネゴシエートする必要があります。
  - \* 他のピアスイッチの物理MACアドレスに直接送信されるトラフィックは、受信側のスイッチによってローカルに転送される必要があります。
- これらの目標を達成できるコマンドセットはどれですか？

- A. vpe ドメイン10ピアゲートウェイインターフェースEth1/1チャンネルグループ1モードオン
- B. vpc domain 10peer-gateway interface Eth1/1 channel-group 1 mode active
- C. vpe ドメイン10ピアスイッチインターフェースEth1/1チャンネルグループ1モードアクティブ
- D. vpe ドメイン10ピアスイッチインターフェースEth1/1チャンネルグループ1モードオン

正解: B (コメントを发表する)

質問: 233

マルチパスiSCSIトラフィックのためのトポロジーにおいて、推奨される設計上の選択肢は何ですか？

- A. 単一のイニシエーターから2つのターゲットへ
- B. イニシエーターとターゲットが別々のサブネットにある
- C. 結合界面を有する単一ターゲットへのデュアルイニシエーター
- D. イニシエーター上で2つのNICが一緒に曲がっている

正解: (正解を表示します)

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/sw/4\\_2\\_1\\_s\\_v\\_1\\_5\\_1/system\\_management/configuration/guide/n1000v\\_system/n1000v\\_system\\_13iscsi.html#wp1052813](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_5_1/system_management/configuration/guide/n1000v_system/n1000v_system_13iscsi.html#wp1052813)

質問: 234

展示資料を参照してください。

```
ACI-Leaf1# show ip route vrf DATACENTER:DC
10.20.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
  *via 10.0.8.65%overlay-1, [1/0], 4w3d, static
172.16.100.0/24, ubest/mbest: 1/0
  *via 10.1.168.95%overlay-1, [200/5], 3wod, bgp-132, internal, tag 132 (mpls-vpn)
172.16.99.0/24, ubest/mbest: 1/0
  *via 10.0.1.14, [20/0], 3wod, bgp-132, external, tag 200
```

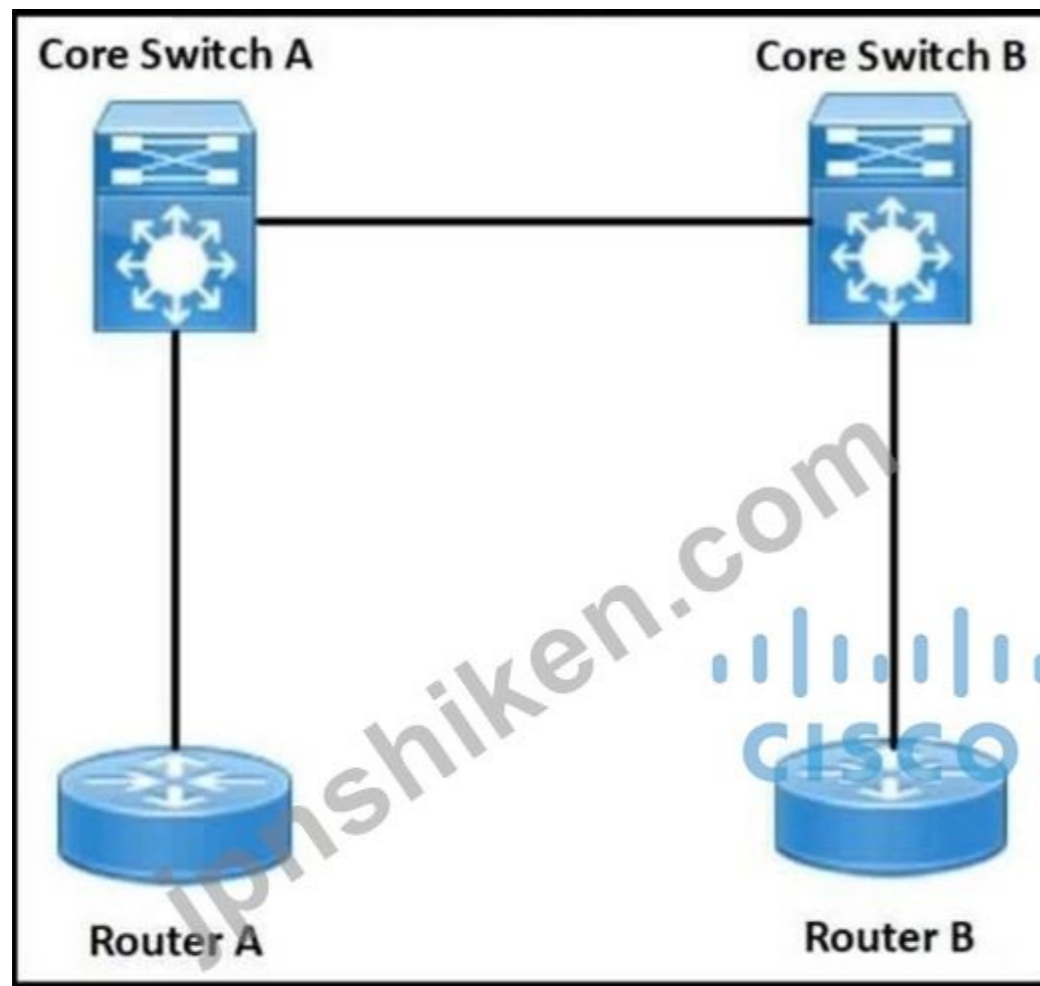
リーフスイッチのルーティングテーブルに関する記述のうち、正しいものはどれですか？ 2つ選択してください。)

- A. 10.20.1.0/24 は ACI の BD サブネットです。
- B. ルート 172.16.99.0/24 のネクストホップ 10.0.1.14 は、ACI の境界リーフの TEP アドレスです。
- C. 172.16.100.0/24 は ACI の BD サブネットです。
- D. ルート 172.16.100.0/24 のネクストホップ 10.1.168.95 は、ACI の境界リーフの TEP アドレスです。
- E. ルート 10.20.1.0/24 のネクストホップ 10.0.8.65 は、ACI の境界リーフの TEP アドレスです。

正解: ([正解を表示します](#))

#### 質問: 235

図を参照してください。ネットワークエンジニアがデータセンター内のルーター間でVXLANを設定しています。VLAN 10はルーターAとルーターB間で拡張する必要があります。初期VXLAN設定はルーターAで完了します。どの設定を行うと、ルーターAのVXLAN設定が完了しますか？



```

feature vn-segment-vlan-based
feature nv overlay

vlan 10
  vn-segment 10010

Interface Loopback0
  ip address 10.10.0.1/32
  ip pim sparse mode
  
```

```

/rf context tenant1
vni 10010

interface nve1
source-interface lo0
no shutdown
member vni 10010 interface 10.10.0.1
  
```

A.

```

Interface nve1
no shutdown
source-interface lo0
member vni 10010 mcast-group 231.1.1.1
  
```

B.

```

Interface nve1
no shutdown
source-interface lo0
vni 10100 I2
rd auto
  
```

C.

```
system bridge-domain 10
member vni 10010
interface nve1
no shutdown
D. source-interface lo0
```

正解: [\(正解を表示します\)](#)

#### 質問: 236

Cisco UCS Manager のデフォルトのホストファームウェアポリシーが変更された場合、どのサービスプロファイルが影響を受けますか？

- A. ホストファームウェアポリシーが定義されていないサービスプロファイル
- B. ユーザーが作成したホストファームウェアポリシーを使用するサービスプロファイル
- C. ルートサブ組織に含まれていないサービスプロファイル
- D. グローバルデフォルトのホストファームウェアポリシーを使用するサービスプロファイル

正解: [D \(コメントを发表する\)](#)

Cisco UCS Manager でデフォルトのホストファームウェアポリシーを変更すると、グローバルデフォルトのホストファームウェアポリシーを使用するすべてのサービスプロファイルに影響します。これは、グローバルデフォルトのホストファームウェアポリシーが、特定のホストファームウェアポリシーが定義されていないサービスプロファイルのテンプレートとして機能するためです。デフォルトポリシーに変更を加えると、そのポリシーを参照するすべてのサービスプロファイルに反映され、複数のサーバーのファームウェアバージョンと設定に影響を与える可能性があります。

参考文献: 350-601 DCCOR 試験トピック2。

#### 質問: 237

エンジニアは、IPアドレスが指定されたCisco Nexus 9000シリーズスイッチで制御プレーンポリシーを設定する必要があります。

192.168.20.1 これらの要件を無効にする

- \* サブネット 192.168.10.0/24 からは HTTP、RDP、ICMP トラフィックのみが許可されます。
- \* 約束された情報レートは54000ppsでなければなりません。
- \* バーストサイズは128パケットでなければなりません。
- \* その他のトラフィックはすべて遮断する必要があります。

下部のコードスニペットを上部のコードの空欄にドラッグアンドドロップして、設定を完了してください。すべてのコードスニペットが使用されるわけではありません。



正解:

```
ip access-list permithosts
 permit tcp 192.168.10.0/24 host 192.168.20.1 eq 443
 permit tcp 192.168.10.0/24 host 192.168.20.1 eq 3389
 permit icmp 192.168.10.0/24 host 192.168.20.1

class-map type control-plane match-any hostsmap
 match access-group name permithosts

policy-map type control-plane hostsmap
 class hostsmap
 police cir 54000 pps bc 128 packets conform transmit violate drop
```

説明

テキスト説明は自動的に生成されました

```
ip access-list permithosts
 permit tcp 192.168.10.0/24 host 192.168.20.1 eq 443
 permit tcp 192.168.10.0/24 host 192.168.20.1 eq 3389
 permit icmp 192.168.10.0/24 host 192.168.20.1

class-map type control-plane match-any hostsmap
 match access-group name permithosts

policy-map type control-plane hostsmap
 class hostsmap
 police cir 54000 pps bc 128 packets conform transmit violate drop
```

```
host 192.168.20.1 eq 443
access-group name permithosts
class hostsmap
conform transmit violate drop
class permithosts
```

質問: 238

ネットワークエンジニアは、Cisco UCS Cシリーズラックサーバーの冷却要件を決定する必要があります。PCIeカードを搭載したサーバーには、ファン構成ポリシーが設定されています。サーバーのファンポリシーには、どの構成を使用すべきでしょうか？

```
server # scope chassis
server /chassis # scope fan-policy
server /chassis/fan-policy # set fan-policy high-power
server /chassis/fan-policy* # commit

server # scope chassis
server /chassis # scope fan-policy
server /chassis/fan-policy # set fan-policy balanced
server /chassis/fan-policy* # commit

server # scope server
server /server # scope fan-policy
server /server /fan-policy # set fan-policy acoustic
server /server /fan-policy* # commit

server # scope server
server /server # scope fan-policy
server /server /fan-policy # set fan-policy low-power
server /server /fan-policy* # commit
```

- A. 選択肢D
- B. オプションB
- C. オプションC
- D. オプションA

正解: [\(正解を表示します\)](#)

#### 質問: 239

HTTPSアクセス用の有効なCA署名付きキーリングが作成された後、エンジニアはCisco UCS ManagerのIDを確認する必要があります。どの操作を行うと設定が完了しますか？

- A. SSLv3を実装する
- B. TLSv1.2を有効にする
- C. 暗号スイートモードの設定
- D. 信頼できるポイントを作成する

正解: [D \(コメントを发表する\)](#)

#### 質問: 240

エンジニアは、大規模なデータセンターを管理し、Cisco NX-OSデータ管理エンジンモデルを使用して複数のCisco NX-OSデバイスから情報を収集するよう依頼されました。この目標を達成するには、どのテクノロジーを使用すべきでしょうか？

- A. NX-API REST
- B. NETCONF
- C. JSON-RPC
- D. NX Yang

正解: [\(正解を表示します\)](#)

説明

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/programmability/guide/b\\_Cisco\\_Nexus\\_9000\\_Series\\_NX-OS\\_Programmability\\_Guide\\_7x/b\\_Cisco\\_Nexus\\_9000\\_Series\\_NXOS\\_Programmability\\_Guide\\_7x\\_chapter\\_010001.pdf](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/programmability/guide/b_Cisco_Nexus_9000_Series_NX-OS_Programmability_Guide_7x/b_Cisco_Nexus_9000_Series_NXOS_Programmability_Guide_7x_chapter_010001.pdf)

質問: 241

Cisco Nexus 9000シリーズスイッチがPOAPを使用して起動に失敗した場合、どの2つのコンポーネントを確認すべきですか？  
(2つ選択してください。)

- A. スクリプトファイル内のスイッチブートフラッシュに対するイメージ
- B. DHCPサーバーがIP情報をブートストラップします
- C. POAP機能ライセンス
- D. セキュリティキーで署名されたスクリプト
- E. 設定スクリプトを含むTFTPサーバー

正解: B,E ([コメントを發表する](#))

有効的な**350-601**問題集はJPNTTest.com提供され、**350-601**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-601**試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで**350-601**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> **384**問、**30%ディスカウント**、特別な割引コード:

**JPNshiken**」

質問: 242

EPG Client のホストが EPG Web の Web サーバーと通信したい場合、EPG Client と EPG Web の間にデフォルト設定の契約が定義され、クライアントが TCP 宛先ポート 80 を使用して Web サーバーに対して TCP 通信を開始することが許可されます。

この状況を最もよく表しているのは、次のうちどれですか？

- A. EPG Web を優先グループメンバーに設定すると、EPG Client のホストが EPG Web のウェブサーバーにアクセスするために、EPG Client と EPG Web 間の契約は不要になります。
- B. vzAny が「すべて拒否」契約を消費および提供するように構成されている場合、EPG Client と EPG Web 間のトラフィックは許可されなくなります。
- C. EPGクライアントのホストは、EPG WebのウェブサーバーのTCP宛先ポート80に接続できます。  
ウェブサーバーは、TCPソースポートを持つホストポートへの個別のTCP接続を開始することはできません。

80.

- D. EPGクライアントのホストは、EPG WebのウェブサーバーのTCP宛先ポート80に接続できます。  
ウェブサーバーは、TCP送信元ポート80を使用して、ホストポートへの個別のTCP接続を開始することが許可されています。

正解: ([正解を表示します](#))

セクション :セキュリティ

質問: 243

Cisco Nexusスイッチの汎用オンライン診断ポリシーでは、PortLoopbackテストにおいて、ポートをエラー無効にするには10回連続で失敗する必要があります。お客様はこれを5回連続の失敗に変更したいと考えています。モジュール1のみに変更を適用する設定はどれですか？

```

① Nexus(config)# event manager applet custom-PortLoopback override __PortLoopback
Nexus(config-applet)# event gold mod all test PortLoopback testing-type bootup consecutive-failure 5
Nexus(config-applet)# action 1 publish-event

② Nexus(config)# event manager applet custom-PortLoopback override __PortLoopback
Nexus(config-applet)# event gold mod 1test PortLoopback testing-type bootup consecutive-failure 5
Nexus(config-applet)# action 1 publish-event

③ Nexus(config)# event manager applet custom-PortLoopback override __PortLoopback
Nexus(config-applet)# event gold mod all test PortLoopback testing-type monitoring consecutive-failure 5
Nexus(config-applet)# action 1 policy-default

④ Nexus(config)# event manager applet custom-PortLoopback override __PortLoopback
Nexus(config-applet)# event gold mod 1 test PortLoopback testing-type monitoring consecutive-failure 5
Nexus(config-applet)# action 1 policy-default

```

- A. オプションA
- B. オプションB
- C. オプションC
- D. 選択肢D

正解: [D \(コメントを发表する\)](#)

「mod all」は誤りです。「mod 1test」は誤りです。「publish event」は誤りです。

「mod 1 test」は正しいです。「policy-default」の場合です。

質問: 244

エンジニアは、2台のCisco Nexus 7000シリーズスイッチでLACPポートチャネルを設定する必要があります。インターフェイスe1/2は、他のポートとのネゴシエーションを開始するホットスタンバイリンクである必要があります。右側のコマンドを左側の設定の空白にドラッグアンドドロップしてください。すべてのコマンドが使用されるわけではありません。

```

configure terminal
feature 
interface Ethernet 1/2
switchport
channel-group 2 
interface Ethernet 1/3
switchport
channel-group 2 mode active
lacp port 

```

mode active

lacp

priority 1

mode passive

priority 65534

mode on

正解:

```
configure terminal
feature lACP
interface Ethernet 1/2
switchport
channel-group 2 mode active
interface Ethernet 1/3
switchport
channel-group 2 mode active
lACP port priority 1
```

mode active  
lACP  
priority 1  
mode passive  
priority 65534  
mode on

質問: 245

エンジニアがCisco MDS 9000シリーズスイッチのポートセキュリティを設定します。MDSスイッチの設定は、以下の要件を満たす必要があります。

\*スイッチは、競合が発生した場合でも、VSAN Aポートのセキュリティデータベースを初期化する必要があります。

\*新しいデバイスは、meスイッチに静的に追加する必要があります。

\*VSAN 4 の構成変更は、ファブリック上のすべてのロックを解除した上で、ファブリック全体に適用する必要があります。

これらの要件を満たす構成セットはどれですか？

A. port-security activate vsan 4

no port-security auto-learn vsan 4 port-security allocate port-security commit vsan 4

B. port-security activate vsan 4 force port-security auto-learn vsan 4 port-security distribute port-security commit

C. port-security activate vsan 4 force no port-security auto-learn vsan 4 port-security distribute port-security commit vsan 4

D. port-security activate vsan 4 port-security manual-learn vsan 4 port-security allocate port-security commit

正解: [\(正解を表示します\)](#)

質問: 246

```
switch1#show run interface Vlan 10
interface Vlan10
description Service Datacenter-Rack-A
ip address 209.165.200.225 255.255.255.224
end
switch1#
```

図を参照してください。エンジニアはスイッチ上でトラフィックをミラーリングする必要があります。エンジニアはスイッチ1上で監視が必要なサーバーポートを特定しますが、パケットスニファはスイッチ2上にあります。エンジニアはスイッチ1上で送信元IPアドレスを設定する必要があります。この目的を達成するには、どのようなコマンドが必要ですか？

A. モニター erspon 発信元 IP アドレス 209.165.200.225

B. モニターセッション 10 タイプ erspan-source

C. ソースインターフェース vbn512

D. 送信元IPアドレス 209.165.200.225

正解: [\(正解を表示します\)](#)

質問: 247

ネットワークエンジニアがサーバーのCANインターフェースをスイッチに接続します。スイッチは、FCoEが有効になっていないインターフェース上のすべてのVLANを停止する必要がありますが、FCoEが有効になっているVLANはSANトラフィックを中断することなく継続する必要があります。この目的を達成するには、スイッチにどの設定を適用する必要がありますか？



- A. オプションA
- B. オプションC
- C. 選択肢D
- D. オプションB

正解: C ([コメントを发表する](#))

質問: 248

あるエンジニアは、UCS CシリーズラックマウントサーバーのBIOS設定を構成しながら、オンデマンドCPUの最適なパフォーマンスを追求している。どのような環境であれば、この目標を達成できるでしょうか？

- A. C0/C1状態
- B. C6保持
- C. C2状態
- D. C6 非保持

正解: ([正解を表示します](#))

参照 :

[https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/whitepaper\\_c11-740098.pdf](https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/whitepaper_c11-740098.pdf) パッケージCステートの値が高いほど、そのアイドル状態のパッケージの消費電力は低くなります。デフォルト設定のパッケージC6（非保持は、プロセッサがサポートする最も低消費電力のアイドル状態のパッケージです。

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/c/sw/gui/config/guide/4\\_0/b\\_Cisco\\_UCS\\_C-Series\\_GUI\\_Configuration\\_Guide\\_for\\_S3260\\_Servers\\_40/b\\_Cisco\\_UCS\\_C-Series\\_GUI\\_Configuration\\_Guide\\_for\\_S3260\\_Servers\\_40\\_appendix\\_010011.html](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/4_0/b_Cisco_UCS_C-Series_GUI_Configuration_Guide_for_S3260_Servers_40/b_Cisco_UCS_C-Series_GUI_Configuration_Guide_for_S3260_Servers_40_appendix_010011.html)

BIOSがC6レポートをオペレーティングシステムに送信するかどうか。OSがレポートを受信すると、プロセッサをより低いC6電力状態に移行させ、最適なプロセッサ性能を維持しながらエネルギー消費を削減できます。」

質問: 249

HSRPバージョン2グループ10のデフォルト仮想MACアドレスはどれですか？

- A. 0000.0C9F.F010

- B. 3719.0351.1C0A
- C. 0000.0C9F.F00A
- D. 0000.5E00.0110

正解: **C** ([コメントを发表する](#))

**質問: 250**

エンジニアはCisco UCSの設定をバックアップする必要があります。バックアップジョブは以下の要件を満たす必要があります。

\* TCPプロトコルを使用する必要があります。

\* データ送信前にクライアントの本人確認を行う必要があります。

バックアップには、すべてのシステム設定と論理構成設定が含まれている必要があります。

運用チームは、バックアップファイルが人間が読みやすい形式であることを要求しています。

エンジニアはどの構成セットを使用しなければならないか？

- A. タイプ: システム構成プロトコル: SFTP
- B. タイプ: 論理構成プロトコル: TFTP
- C. タイプ: すべての構成 プロトコル: SCP
- D. タイプ: フルステートプロトコル: SFTP

正解: ([正解を表示します](#))

正解はCです。なぜなら、Cは4つの条件すべてを同時に満たす唯一の選択肢だからです。

Cisco UCS Managerのドキュメントによると、全構成バックアップは、すべてのシステム構成設定と論理構成設定を含むXMLファイルです。XML形式であるため、人間が読みやすく、運用チームの要件を満たしています。一方、完全状態バックアップはバイナリスナップショットであるため、人間が読みやすくなく、システム構成または論理構成のみでは、両方の設定セットが含まれません。

トランスポート要件に関しては、Cisco UCSはFTP、TFTP、SCP、またはSFTPによるバックアップ転送をサポートしており、SCPはSSH/TCP上で動作するため、実際のデータコピーが行われる前に認証済みの安全なファイル転送が提供されることから、SCPが正解です。TFTPはUDPを使用し、安全なID検証を提供しないため、ここでは無効です。SFTPもSSH/TCPを使用しますが、オプションDは「完全な状態」がバイナリであるため不合格となり、オプションAは「システム構成」にすべての論理設定が含まれていないため不合格となります。したがって、完全に正しい組み合わせは「すべての構成 + SCP」のみです。

**質問: 251**

エンジニアはデータセンターでOSPFを設定する必要があります。外部ルートは既にOSPFによって再配布されています。ネットワークは以下の条件を満たす必要があります。

\* データセンターのサーバーは、クラウド上のサービスと、再分配された経路の背後にあるサービスにアクセスできる必要があります。

\* インターネットへの出口ポイントは、上流ルーターから動的に学習されたデフォルトルートが存在する場合にのみ伝播されるべきである。

どの機能が必要ですか？

- A. 完全に短いエリア
- B. 短いエリア
- C. デフォルト情報は常に
- D. デフォルト情報の発生源

正解: ([正解を表示します](#))

**質問: 252**

Cisco MDS 9000 シリーズ スイッチがポート チャネルを使用する環境において、エンジニアは、特定のフローにおいて送信元と宛先間のフレームが同じリンクを経由するようにする必要があります。後続のフローでは、異なるリンクを使用することが許可されます。この目的を達成するには、どのロード バランシング方式を使用すべきでしょうか？

- A. 送信元ID/宛先ID
- B. src-dst-oui

C. 送信元送信先ポート

D. src-id/dst-id/oxid

正解: [\(正解を表示します\)](#)

Exchange ベース - Exchange 内の最初のフレームがリンクを選択し、Exchange 内の後続のフレームは同じリンクに従います。ただし、後続の Exchange では別のリンクを使用できます。これにより、各 Exchange のフレームの順序を維持しながら、よりきめ細かな負荷分散が可能になります。出典:

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/5\\_0/configuration/guides/int/nxos/cli\\_interfaces/pc.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/5_0/configuration/guides/int/nxos/cli_interfaces/pc.html) 負荷分散属性は、負荷分散パスの選択にソース宛先 ID (src-dst-id) または発信元 Exchange OX ID (src-dst-ox-id、デフォルト) を使用することを示します。出典: [https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6\\_2/configuration/guides/fabric/nx-os/nx\\_os\\_fabric/vsan.html?bookSearch=true](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6_2/configuration/guides/fabric/nx-os/nx_os_fabric/vsan.html?bookSearch=true)

[https://www.cisco.com/en/US/docs/storage/san\\_switches/mds9000/sw/rel\\_1\\_x/1\\_3/san-os/configuration/guide/PortChnl.pdf](https://www.cisco.com/en/US/docs/storage/san_switches/mds9000/sw/rel_1_x/1_3/san-os/configuration/guide/PortChnl.pdf)

質問: 253

展示資料を参照してください。

```
UCS-A# scope adapter 1/1/1
UCS-A# /chassis/server/adapter # show image
Name                               Type          Version      State
-----
ucs-m81kr-vic.2.2.1b.bin           Adapter       2.2(1b)      Active

UCS-A# /chassis/server/adapter # update firmware 2.2(1b)
UCS-A# /chassis/server/adapter* # activate firmware 2.2(1b)
set-startup-only
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter #
```

一連のコマンドを実行すると、どのような結果になりますか？

- A. サーバーを即座に再起動します。
- B. サーバー上のファームウェアアップデートを確認します。
- C. アダプター1/1/1のファームウェアを即座に更新します。
- D. 次回のアダプタ起動時にファームウェアを有効化します。

正解: D ([コメントを发表する](#))

質問: 254

エンジニアは、Cisco Nexus 9000シリーズスイッチのEEM (エンタープライズ環境管理) 画面で、これらのコマンドを入力します。

イベントマネージャーアプレット Backup-config

イベントタイマー ウォッチドッグ 時間 1800 名前 タイマー

イベント cli マッチ "copy running-config startup-config"

この設定を適用した結果はどうなりますか？

- A. アクションが指定されていないため、エラーが発生します。

- B. 1800秒ごとに実行中の設定を保存します。
- C. copy running-config startup-config コマンドをブロックします。
- D. copy running-config startup-config コマンドを実行します。

正解: (正解を表示します)

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/system-management/b-cisco-nexus-9000-series-nx-os-system-management-configuration-guide-93x/b-cisco-nexus-9000-series-nx-os-system-management-configuration-guide-93x\\_chapter\\_0100010.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/system-management/b-cisco-nexus-9000-series-nx-os-system-management-configuration-guide-93x/b-cisco-nexus-9000-series-nx-os-system-management-configuration-guide-93x_chapter_0100010.html)

## Prerequisites for EEM

EEM has the following prerequisites:

- You must have network-admin user privileges to configure EEM.

## Guidelines and Limitations for EEM

EEM has the following configuration guidelines and limitations:

- The maximum number of configurable EEM policies is 500.
- Action statements within your user policy or overriding policy should not negate each other or adversely affect the associated system policy.
- To allow a triggered event to process any default actions, you must configure the EEM policy to allow the default action. For example, if you match a CLI command in a match statement, you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute.
- When you configure an EEM policy action to collect **show tech** commands, make sure to allocate enough time for the **show tech** commands to complete before the same action is called again.

質問: 255

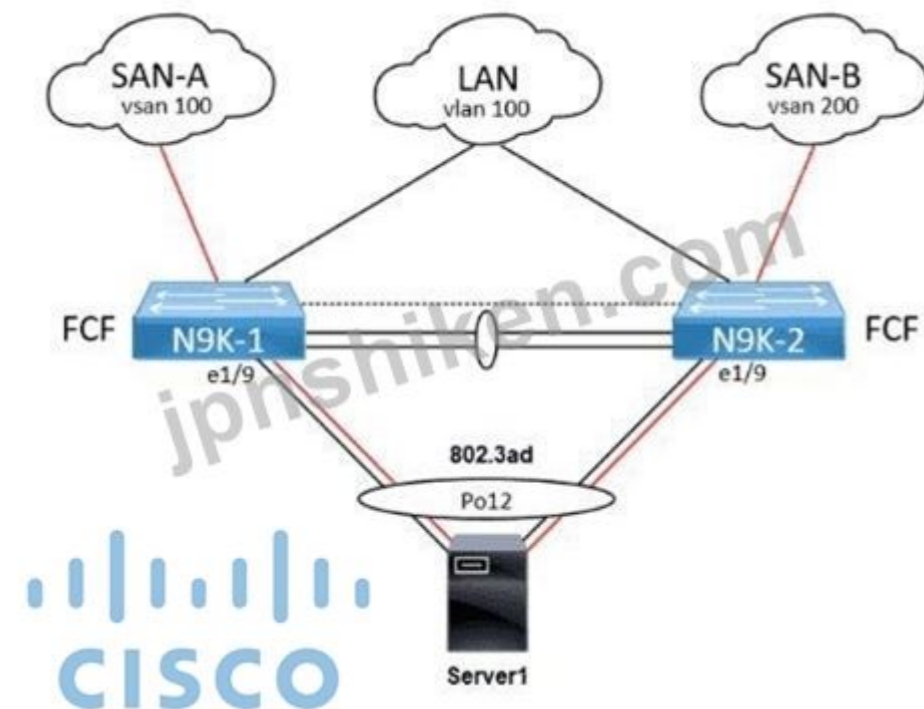
Cisco UCS ファームウェアの自動同期サーバーポリシーで使用できる設定項目はどれですか？ (2つ選択可能)

- A. ユーザー承認
- B. 遅延作用
- C. 即時対応
- D. ユーザー通知
- E. 何もしない

正解: A,E (コメントを發表する)

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/sw/firmware-mgmt/gui/2-2/b\\_GUI\\_Firmware\\_Management\\_22/b\\_GUI\\_Firmware\\_Management\\_22\\_chapter\\_01111.pdf](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/firmware-mgmt/gui/2-2/b_GUI_Firmware_Management_22/b_GUI_Firmware_Management_22_chapter_01111.pdf) ファームウェア自動同期サーバー ポリシーの値は次のとおりです。\* ユーザー承認 - 管理者が保留中のアクティビティ ダイアログボックスでアップグレードを承認するまで、サーバー上のファームウェアは同期されません。\* アクションなし - サーバーでファームウェアのアップグレードは開始されません。

質問: 256



図を参照してください。管理者は、Server1 と 2 台の Cisco Nexus 9000 シリーズ スイッチ間の統合ファブリック構成を完了する必要があります。右側のコード スニペットを左側のコードの空白にドラッグアンドドロップして、N9K-1 の構成を完了します。スニペットは複数回使用されます。

```
service-policy type qos input default-fcoe-in-policy
int [ ]
switchport trunk allowed [ ] 1, 100
int [ ]
band interface [ ]
no shut
```

vlan  
vfc 1  
pol2

正解:

```
service-policy type qos input default-fcoe-in-policy
int pol2
switchport trunk allowed vlan 1, 100
int vfc 1
band interface pol2
no shut
```

vlan  
vfc 1  
pol2

Explanation:

- ポ12
- VLAN
- VFC1
- ポ12

有効的な350-601問題集はJPNTTest.com提供され、350-601試験に合格することに役に立ちます！JPNTTest.comは今最新350-601試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで350-601問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> 884問、30%ディスカウント、特別な割引コード:

**JPNshiken**」

質問: 257

エンジニアは Cisco UCS システムを復旧する必要があります。完全なバックアップはバックアップ SCP サーバーで利用可能です。Cisco UCS Manager の構成を復旧するには、どの操作を行う必要がありますか？



A. オプションA

B. オプションB

C. オプションC

D. 選択肢D

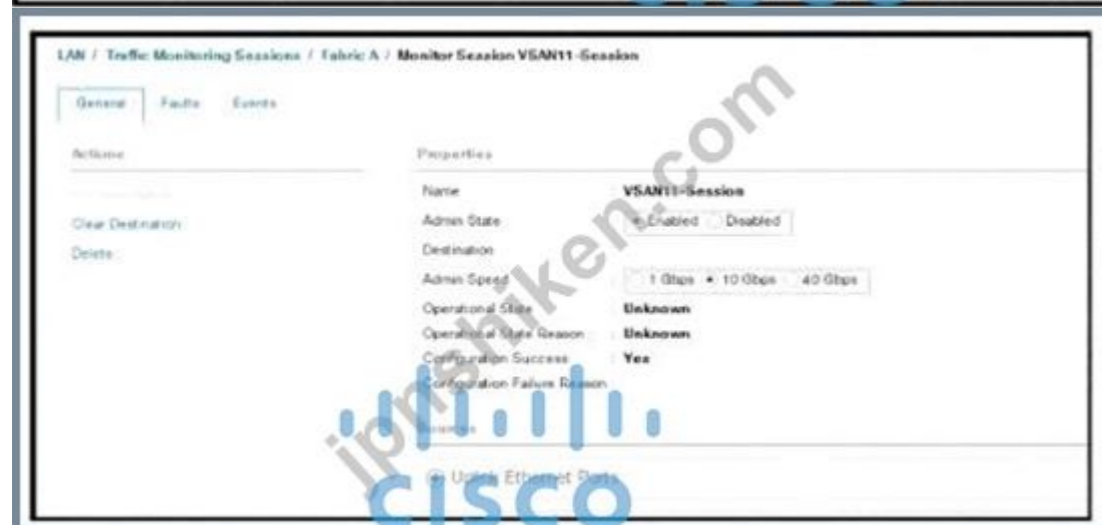
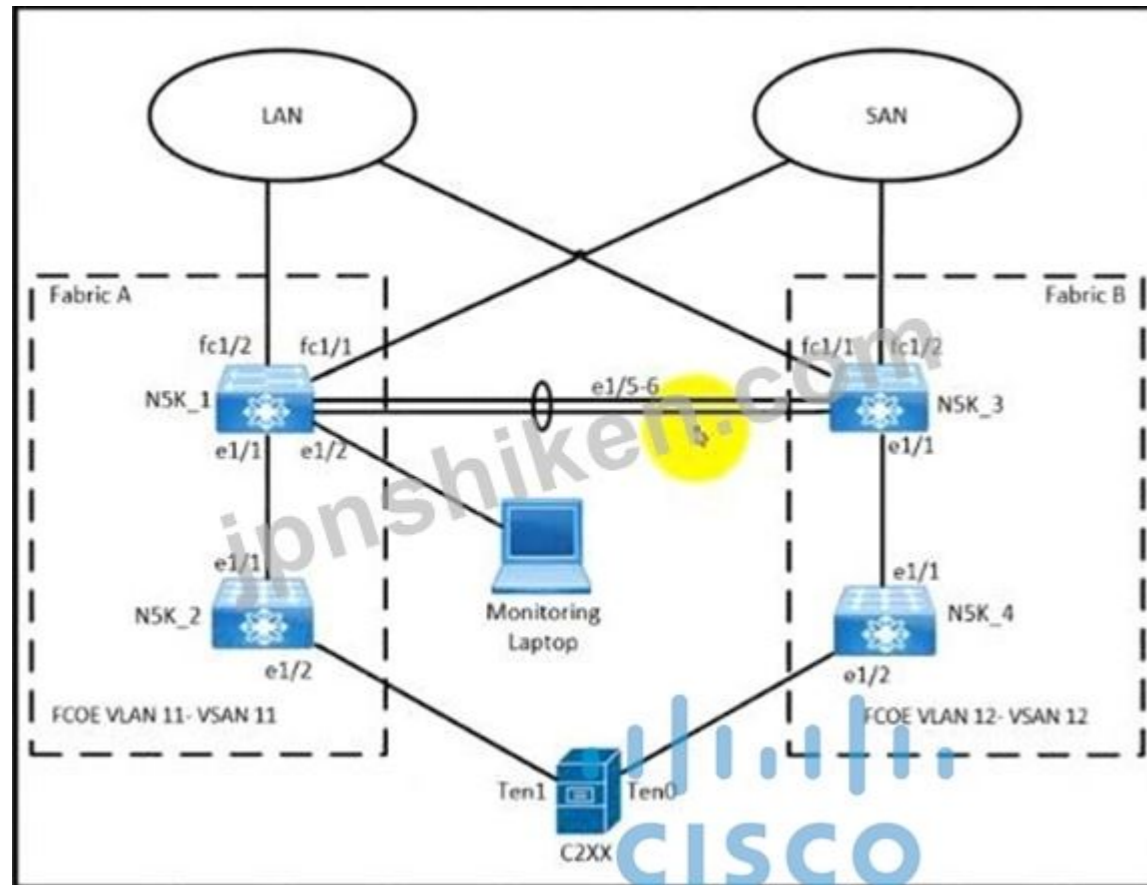
正解: (正解を表示します)

バックアップ SCP サーバー上のフルバックアップから Cisco UCS Manager の設定を復元するには、オプション A の手順に従う必要があります。これらの手順には通常、Cisco UCS Manager インターフェイスにアクセスし、バックアップおよび復元設定に移動して、SCP プロトコルを使用して復元操作を開始し、SCP サーバーからバックアップ ファイルを取得することが含まれます。

参考資料：詳細な手順とベストプラクティスについては、Ciscoの公式ドキュメントを参照してください。

Cisco UCS Manager ガイドの「構成のバックアップと復元」を参照してください。

質問: 258



図を参照してください。エンジニアが、NSK\_1 上の Fabric-A VSAN 11 トラフィックのコピーを監視用ラップトップに送信する SPAN セッションを作成しています。提示されているコンフィギュレータは、既に Cisco UCS Manager に適用されています。どの操作を行うと、構成が完了しますか？

- A. VLAN 11をトラフィックの宛先として設定します。
- B. トラフィックの送信元としてVSAN 11を選択します。
- C. SANトラフィック監視セッションを作成する
- D. NetFlow監視セッションをアクティブ化する

正解: (正解を表示します)

質問: 259

Cisco MUS 9000シリーズスイッチのEPLDをアップグレードするプロセスを説明しているのは、次のうちどれですか？ (2つの記述)

(2つ選択)

- A. アップグレード検証では、各EPLDアップグレードの影響を特定します。
- B. EPLDはハードウェアを交換することなくアップグレード可能です
- C. EPLDは最新のFHにのみアップグレード可能です。Dイメージ
- D. EPLDのアップグレードは、アップグレード中にモジュールの電源を切ることなく完了できます。
- E. スイッチ上のすべてのモジュールのCPLDは同時にアップグレードする必要があります

正解: [\(正解を表示します\)](#)

質問: 260



図を参照してください。エンジニアはVXLAN展開をプロビジョニングする必要があります。OSPFは既にアンダーレイプロトコルとして構成されています。すべてのBGP構成はテンプレート方式を使用して実行されます。展開はこれらの要件を満たす必要があります。

- \* リーフスイッチのローカル更新ソースはループバック1である必要があります
  - ルーターIDはローカルループバックIPアドレスである必要があります。
  - \* 外部BGP接続ではテンプレート名を使用する必要があります
- 下部から設定スニペットをドラッグアンドドロップして設定を完了します。

```

router bgp 65000
  router-id 
  template peer SPINE
  bfd
  remote-as 
  update-source loopback1
  timers 3 9
  address-family  
    send-community extended
  neighbor 
     peer SPINE

```

10.255.255.1	inherit	65000
10.255.255.10	12vpn	evpn

正解:

```
router bgp 65000
  router-id 10.255.255.10
  template peer SPINE
  bfd
  remote-as 65000
  update-source loopback1
  timers 3 9
  address-family 12vpn evpn
    send-community extended
  neighbor 10.255.255.1
    inherit peer SPINE
```

10.255.255.1 inherit 65000  
10.255.255.10 12vpn evpn



Explanation:

```
router bgp 65000
  router-id 10.255.255.10
  template peer SPINE
  bfd
  remote-as 65000
  update-source loopback1
  timers 3 9
  address-family 12vpn evpn
    send-community extended
  neighbor 10.255.255.1
    inherit peer SPINE
```

質問: 261

エンジニアが、ネイティブファイバーチャネルを備えたCisco MDS 9000シリーズスイッチ上でVSANを実装しています。この展開は、以下の要件を満たす必要があります。

- \* ポートfc1/1のホストはVSAN 10に割り当てられている必要があります。
- \* ポートチャネル10 ISLは、VSAN 10を含む複数のVSANを通過する必要があります。

これらの要件を満たす構成セットはどれですか？

A. vFCインターフェースでVSAN 10を有効化します。

VSAN 10 をインターフェース vfc 1/1 に関連付けます。

ISL上でvsan F-port-channel-trunkを有効にします。

スイッチポートにカプセル化プロトコルEISLを設定します。

**B.** VSANデータベースにVSAN 10を作成します。

VSANデータベースで、VSAN 10をインターフェースfc1/1にバインドします。

ISL上でVSANトランキングを有効にする。

ISL上でVSAN 10を許可する。

**C.** インターフェース設定でVSAN 10を設定します。

VSAN 10をVSANデータベースに接続します。

fc1/1でVSANトランキングを有効にします。

ISL上のすべてのVSANをフィルタリングします。

**D.** VSANデータベースでVSAN 1を無効にします。

VSAN 10をISLに割り当てます。

ポートチャネルメンバーでVSANトランキングを有効にします。

FLOGIデータベースでVSAN 10を許可します。

正解: ([正解を表示します](#))

Cisco MDS 9000 シリーズ スイッチで VSAN を実装するための展開要件を満たすには、VSAN データベースに VSAN 10 を作成し、インターフェイス fc1/1 にバインドする必要があります。これにより、ポート fc1/1 のホストが VSAN 10 に割り当てられます。さらに、スイッチ間リンク (ISL) で VSAN トランキングを有効にし、ISL で VSAN 10 を許可することで、ポート チャネル 10 が複数の VSAN (VSAN 10 を含む) を通過できるようになります。

10. この構成により、トラフィックの分離が可能になり、共有物理インフラストラクチャを介した通信を許可しながら、異なる VSAN の分離が維持されます。12.

参考文献：

\* Cisco のドキュメント 「VSAN とインターフェイスの設定」には、VSAN の作成と管理に関する詳細な手順が記載されています。

\* 「Cisco MDS 9000シリーズファブリック構成ガイド」では、VSANとその関連インターフェイスの管理についてさらに詳しく説明しています。

質問: **262**

展示資料を参照してください。

```
MDSSWITCH# config terminal
MDSSWITCH(config)# fcip profile 1
MDSSWITCH(config-profile)# ip address 192.0.1.10
MDSSWITCH(config-profile)# port 5000
MDSSWITCH(config-profile)# tcp max-bandwidth-mbps 5000
min-available-bandwidth-mbps 4000 round-trip-time-ms 1
MDSSWITCH(config-profile)# exit
MDSSWITCH(config)# interface fcip 1
MDSSWITCH(config-if)# use-profile 1
MDSSWITCH(config-if)# peer-info ipaddr 192.0.1.11
MDSSWITCH(config-if)# tcp-connections 1
MDSSWITCH(config-if)# ip-compression mode2
MDSSWITCH(config-if)# no shutdown
MDSSWITCH(config-if)# exit
MDSSWITCH(config)# interface ipStorage 1/1
MDSSWITCH(config-if)# ip address 192.0.1.10 255.255.255.0
MDSSWITCH(config-if)# switchport mtu 2500
MDSSWITCH(config-if)# no shutdown
MDSSWITCH(config-if)# end
```

エンジニアがCisco MDS 9000シリーズスイッチでFCIPを設定します。この設定を実行すると、どのような結果になりますか？

- A. スイッチは2つのTCP接続を確立しようとします
- B. 圧縮はハードウェアを使用して行われます
- C. モード2はデフォルトで有効になっています。
- D. 圧縮はソフトウェアを使用して行われます。

正解: [\(正解を表示します\)](#)

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8\\_x/config/ip\\_services/ipsvc/cfcip.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/ip_services/ipsvc/cfcip.html)

質問: 263

展示資料を参照してください。

```
<?xml version="1.0" encoding="UTF-8"?><imdata totalCount="1"><error
code="403" text="Token was invalid (Error: Token timeout)"/></imdata>
```

エンジニアがREST APIを使用して新しいアプリケーションプロファイルを構成した際に、このエラーメッセージを受け取りました。アプリケーションプロファイルを構成する前に使用できるメソッドはどれですか？

- A. aaaLoginにPOST
- B. aaaRefreshにPOSTします
- C. aaaLogoutへPOST
- D. aaaListDomainsへのGETリクエスト

正解: [\(正解を表示します\)](#)

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/rest\\_cfg/2\\_1\\_x/b\\_Cisco\\_APIC\\_REST\\_API\\_Configuration\\_Guide/b\\_Cisco\\_APIC\\_REST\\_API\\_Configuration\\_Guide\\_chapter\\_01.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/rest_cfg/2_1_x/b_Cisco_APIC_REST_API_Configuration_Guide/b_Cisco_APIC_REST_API_Configuration_Guide_chapter_01.html)

## Authentication

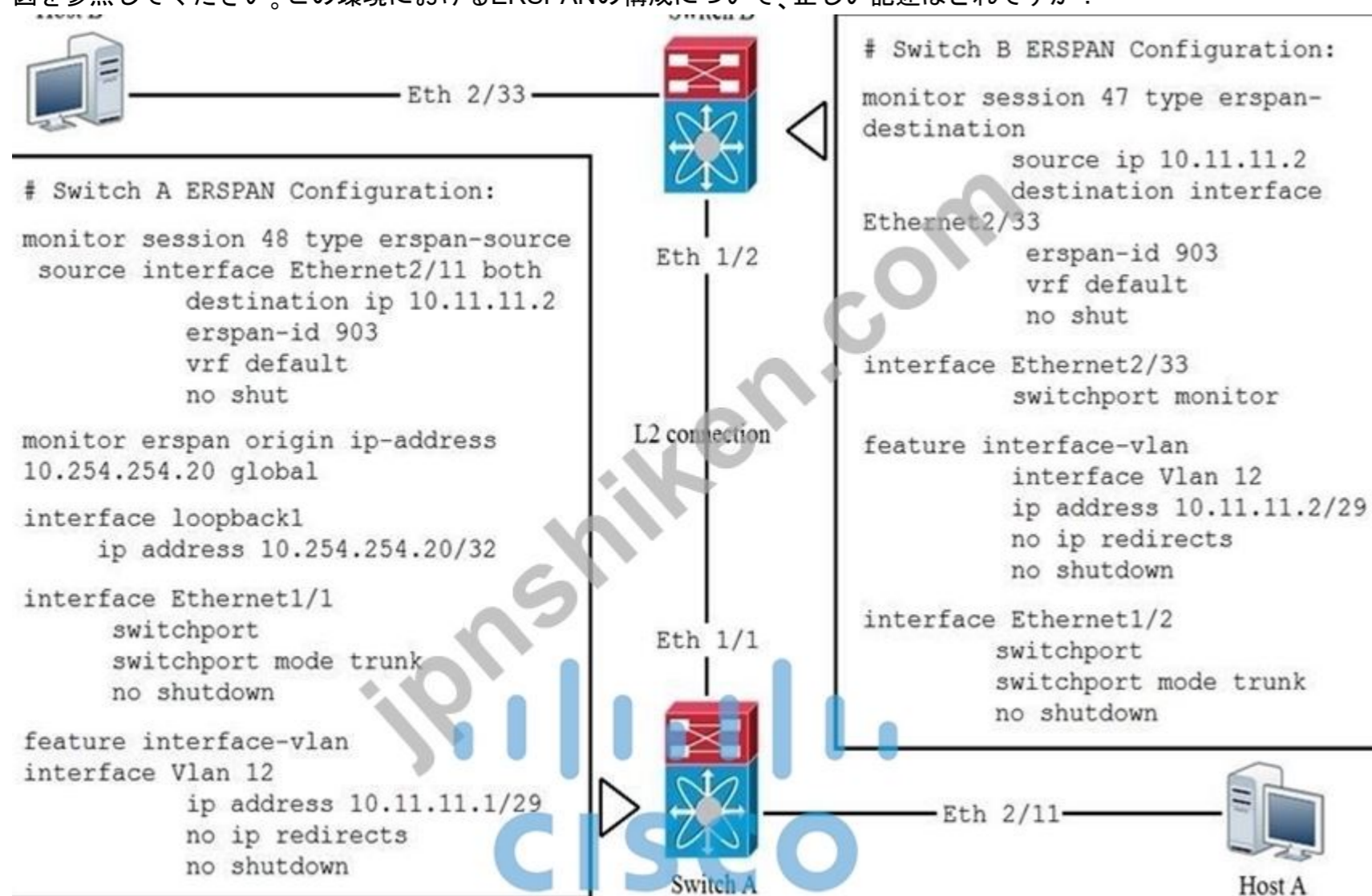
REST API username- and password-based authentication uses a special subset of request Universal Resource Identifiers (URIs), including `aaaLogin`, `aaaLogout`, and `aaaRefresh` as the DN targets of a POST operation. Their payloads contain a simple XML or JSON payload containing the MO representation of an `aaaUser` object with the attribute `name` and `pwd` defining the username and password: for example, `<aaaUser name='admin' pwd='password'/>`. The response to the POST operation will contain an authentication token as both a Set-Cookie header and an attribute to the `aaaLogin` object in the response named `token`, for which the XPath is `/imdata/aaaLogin/@token` if the encoding is XML. Subsequent operations on the REST API can use this token value as a cookie named `APIC-cookie` to authenticate future requests.

## Subscription

The REST API supports the subscription to one or more MOs during your active API session. When any MO is created, changed, or deleted because of a user- or system-initiated action, an event is generated. If the event changes the data on any of the active subscribed queries, the APIC will send out a notification to the API client that created the subscription.

### 質問: 264

図を参照してください。この環境におけるERSPANの構成について、正しい記述はどれですか？



- A. トラフィックアナライザがトラフィックを受信するためには、ERSPAN スパン トラフィックの送信元のセッション番号のセッション ID が 47 である必要があります。
- B. ホストBはERSPANのスパントラフィックの発信元であり、ホストAはトラフィックアナライザです。
- C. トラフィックアナライザがトラフィックを受信するためには、ERSPAN スパン トラフィックの送信元のセッション番号のセッション ID が 48 である必要があります。
- D. ホストAはERSPANのスパンされたトラフィックの発信元であり、ホストBはトラフィックアナライザです。

正解: (正解を表示します)

ERSPANをローカルSPANとして使用する場合、以下の要素が適用されます。

両方のセッションは同じERSPAN IDを持っています。

両方のセッションは同じIPアドレスを使用します。このIPアドレスはルーター自身のIPアドレス、つまりループバックIPアドレス、または任意のポートに設定されているIPアドレスです。

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/lanswitch/configuration/x-16/lanswitch-xe-16-book/lsw-conf-erspan.html>

質問: 265

展示資料を参照してください。

```
1.130599 192.168.254.1 -> 192.168.254.13 TCP 60 29652 > ssh [ACK] Seq=1 Ack=53
Win=32449 Len=0
1.136261 00:8e:73:a2:41:0e -> Spanning-tree-(for-bridges)_00 STP 60 Conf. Root =
8192/10/ec:e1:a9:df:6c:80 Cost = 22 Port = 0x800e
1.373417 192.168.254.13 -> 192.168.254.1 SSH 106 Encrypted response packet len=52
1.570377 192.168.254.1 -> 192.168.254.13 TCP 60 29652 > ssh [ACK] Seq=1 Ack=105
Win=32786 Len=0
1.815558 192.168.254.13 -> 192.168.254.1 SSH 106 Encrypted response packet len=52
2.021840 192.168.254.1 -> 192.168.254.13 TCP 60 29652 > ssh [ACK] Seq=1 Ack=157
Win=32773 Len=0
2.525173 192.168.254.13 -> 192.168.254.1 SSH 106 Encrypted response packet len=52
2.731382 192.168.254.1 -> 192.168.254.13 TCP 60 29652 > ssh [ACK] Seq=1 Ack=209
Win=32760 Len=0
2.947365 192.168.254.13 -> 192.168.254.1 NTP 90 NTP Version 2, client
2.947623 192.168.254.1 -> 192.168.254.13 NTP 90 NTP Version 2, server
3.138157 00:8e:73:a2:41:0e -> Spanning-tree-(for-bridges)_00 STP 60 Conf. Root =
8192/10/ec:e1:a9:df:6c:80 Cost = 22 Port = 0x800e
3.139400 192.168.254.13 -> 192.168.254.1 SSH 106 Encrypted response packet len=52
3.270728 192.168.254.1 -> 239.255.70.63 UDP 166 Source port: cfs Destination port:
cfs
3.341123 192.168.254.1 -> 192.168.254.13 TCP 60 29652 > ssh [ACK] Seq=1 Ack=261
Win=32747 Len=0
3.835409 192.168.254.13 -> 192.168.254.1 SSH 106 Encrypted response packet len=52
4.041411 192.168.254.1 -> 192.168.254.13 TCP 60 29652 > ssh [ACK] Seq=1 Ack=313
Win=32734 Len=0
4.535284 192.168.254.13 -> 192.168.254.1 SSH 106 Encrypted response packet len=52
4.741072 192.168.254.1 -> 192.168.254.13 TCP 60 29652 > ssh [ACK] Seq=1 Ack=365
Win=32721 Len=0
4.947308 192.168.254.13 -> 192.168.254.1 NTP 90 NTP Version 2, client
4.947519 192.168.254.1 -> 192.168.254.13 NTP 90 NTP Version 2, server
5.139627 00:8e:73:a2:41:0e -> Spanning-tree-(for-bridges)_00 STP 60 Conf. Root =
8192/10/ec:e1:a9:df:6c:80 Cost = 22 Port = 0x800e
5.140867 192.168.254.13 -> 192.168.254.1 SSH 106 Encrypted response packet len=52
```

Cisco Fabric Servicesがネットワークで有効になっています。Cisco Fabric Services プロトコルでは、どのような種類のIPアドレスが使用されますか？

- A. IPv4ユニキャストアドレス
- B. IPv4マルチキャストアドレス
- C. IPv4ゲートウェイアドレス
- D. IPv4エニーキャストアドレス

正解: (正解を表示します)

Cisco Fabric Services (CFS) は、IPv4 マルチキャスト アドレスを使用して、ネットワーク デバイス間で構成情報を配信します。これにより、ネットワーク内のすべてのデバイスが一貫性のある同期された構成データを持つことが保証され、ネットワークの整合性と安定性を維持する上で非常に重要となります。

参考資料：詳細については、Cisco Data Center Core Technologies (DCCOR) の学習資料、特にネットワークインフラストラクチャ内での CFS とその動作メカニズムについて説明しているセクションを参照してください。

質問: 266

左側のファームウェアパッケージを、右側の対応するソフトウェアバンドルにドラッグアンドドロップしてください。

The diagram shows two software bundles on the right side, each with three empty slots for components. The top bundle is labeled "Cisco UCS Infrastructure Software Bundle" and the bottom bundle is labeled "Cisco UCS B-Series Blade Server Software Bundle". On the left side, there are six light blue boxes representing firmware packages: "Board controller firmware", "BIOS firmware", "Kernel and system firmware for Fabric Interconnects", "CIMC firmware", "I/O module firmware", and "Cisco UCS Manager software".

正解:

The diagram shows the same two software bundles as in the previous image, but now they contain the correct components. The "Cisco UCS Infrastructure Software Bundle" contains "Kernel and system firmware for Fabric Interconnects", "I/O module firmware", and "Cisco UCS Manager software". The "Cisco UCS B-Series Blade Server Software Bundle" contains "Board controller firmware", "CIMC firmware", and "BIOS firmware". The left side still shows the six original firmware packages, but they are no longer being dragged.

質問: 267

POAP対応のCisco Nexusスイッチは、POAPモードに移行しません。

検証すべき条件はどれですか？ (2つ選択してください。)

- A. スイッチは起動処理中です。
- B. 起動設定は利用できません。
- C. ブートフラッシュにCisco NX-OSイメージが存在しません。
- D. Bootflashには、poap.pyファイルを含むPOAPという名前の特別なディレクトリが含まれている必要があります。
- E. スイッチにライセンスファイルがありません。

正解: A,B ([コメントを发表する](#))

質問: 268

ネットワークエンジニアは、Cisco UCS Cシリーズラックサーバーに電源冗長ポリシーを設定する必要があります。この電源冗長は、サーバーへの給電に2つの電源が使用される場合に対応できるものでなければなりません。この要件を満たすには、どの構成を適用すべきでしょうか？

```
server# scope org /
server /org # scope psu-policy
server /org/psu-policy # set redundancy N+1
server /org/psu-policy* # commit-buffer

server# scope org /
server /org # scope psu-policy
server /org/psu-policy # set psu-redundancy-policy grid
server /org/psu-redundancy-policy* # commit-buffer

server# scope org /
server /org # scope psu-policy
server /org/psu-policy # set psu-redundancy-policy N+1
server /org/psu-redundancy-policy* # commit-buffer

server# scope org /
server /org # scope psu-policy
server /org/psu-policy # set redundancy grid
server /org/psu-policy* # commit-buffer
```

- A. 選択肢D
- B. オプションB
- C. オプションA
- D. オプションC

正解: ([正解を表示します](#))

質問: 269

展示資料を参照してください。

LAN / Traffic Monitoring Sessions / Fabric A / Monitor Session test-span

General Faults Events

Actions	Properties
Set Destination	Name : test-span
Clear Destination	Admin State : <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Delete	Destination : sys/switch-A/slot-1/switch-ether/port-17
	Admin Speed : <input type="radio"/> 1 Gbps <input checked="" type="radio"/> 10 Gbps <input type="radio"/> 40 Gbps
	Operational State : Down
	Operational State Reason : No Sources Configured
	Configuration Success : Yes
	Configuration Failure Reason :

Sources

エンジニアは、ブレードサーバーからファブリックA上のすべてのLANトラフィックを監視する必要があります。このタスクを完了するには、テストスパンモニターセッションでどのソースを設定すればよいでしょうか？

- A. このサーバーに対応するサービスプロファイル内のすべてのvHBA
- B. すべてのアップリンクFCoEポート
- C. すべてのアップリンクイーサネットポート
- D. このサーバーに対応するサービスプロファイル内のすべてのvNIC

正解: ([正解を表示します](#))

[https://www.cisco.com/en/US/docs/unified\\_computing/ucs/sw/gui/config/guide/141/UCSM\\_GUI\\_Configuration\\_Guide\\_141\\_chapter45.html](https://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/141/UCSM_GUI_Configuration_Guide_141_chapter45.html)

## Guidelines and Recommendations for Traffic Monitoring

When configuring or activating traffic monitoring, consider the following guidelines:

- You can create and store up to 16 traffic monitoring sessions, but only two can be active at the same time.
- A traffic monitoring session is disabled by default when created. To begin monitoring traffic, you must activate the session.
- To monitor traffic from a server, add all vNICs from the service profile corresponding to the server.
- To monitor traffic from a VM, you must first determine the identity of the dynamic vNIC assigned to the VM. Follow the procedure in to find the vNIC and view its identity properties, then add the vNIC as a source for the monitoring session. If you later move the VM using VMotion, a new dynamic vNIC is assigned and you must reconfigure the monitoring source.

### Viewing Dynamic vNIC Properties in a VM

- You can monitor Fibre Channel traffic using either a Fibre Channel traffic analyzer or an Ethernet traffic analyzer. When Fibre Channel traffic is monitored using an Ethernet traffic monitoring session, with an Ethernet destination port, the destination traffic will be FCoE.
- Because a traffic monitoring destination is a single physical port, a traffic monitoring session can monitor only a single fabric. To monitor uninterrupted vNIC traffic across a fabric failover, you must create two sessions—one per fabric—and connect two analyzers. Add the vNIC as the traffic source for both sessions.
- All traffic sources must be located within the same switch as the destination port.
- A port configured as a destination port cannot also be configured as a source port.
- A member port of a port channel cannot be configured individually as a source. If the port channel is configured as a source, all member ports are source ports.

### 質問: 270

ネットワークエンジニアは、Cisco Nexusシリーズスイッチの初期導入を簡素化するソリューションを必要としています。このソリューションは、以下の要件を満たす必要があります。

- ゼロタッチプロビジョニング
- DHCPオプションによる設定
- 中央TFTPサーバーからの初期設定
- 初回インストール後の手動設定管理は不要

これらの目標を支援する技術はどれですか？

- A. シスコインターサイト
- B. アンシブル
- C. シェフ
- D. ポップ

正解: D ([コメントを发表する](#))

### 質問: 271

あるエンジニアがFCoEを導入している。

Cisco NexusスイッチにおけるDCBXPのどの側面が、この実装に影響を与えますか？

- A. FCoEインターフェースでLLDP送信とLLDP受信が有効になっている必要があります。
- B. Cisco Fabric Servicesプロトコルを使用して、2つのピアリンク間でパラメータを交換します。
- C. Cisco Nexusスイッチ上のピアの認証を提供します。
- D. 10/100Mbpsネイティブイーサネットポートでは常に有効になっています。

正解: ([正解を表示します](#))

データセンターブリッジング交換プロトコル (DCBXP)は、LLDPの拡張機能です。これは、ピア間でノードパラメータを通知、交換、およびネゴシエートするために使用されます。DCBXPパラメータは、特定のDCBXP TLVにパッケージ化されます。このTLVは、受信したLLDPパケットに対する確認応答を提供するように設計されています。

LLDPが有効になっている場合、DCBXPはデフォルトで有効になります。LLDPの送受信が無効になっているポートでは、DCBXPは無効になります。

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503\\_n2\\_1/b\\_Cisco\\_n5k\\_layer2\\_config\\_gd\\_rel\\_503\\_N2\\_1/b\\_Cisco\\_n5k\\_layer2\\_config\\_gd\\_rel\\_503\\_N2\\_1\\_chapter\\_01110.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503_n2_1/b_Cisco_n5k_layer2_config_gd_rel_503_N2_1/b_Cisco_n5k_layer2_config_gd_rel_503_N2_1_chapter_01110.html)

有効的な**350-601**問題集はJPNTTest.com提供され、**350-601**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-601**試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで**350-601**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> **884**問、**30%ディスカウント**、特別な割引コード:

**JPNshiken**」

質問: **272**

展示資料を参照してください。

```
; Router 1 configuration
interface loopback1
 ip address 10.10.32.121/30
 ip ospf network point-to-point
 ip router ospf 1 area 0.0.0.0
 ip pim sparse-mode

ip pim rp-address 10.10.32.122 group-list 225.0.0.0/8 bi-dir
```

Phantom RPをRP冗長化メカニズムとして使用する双方向PIMネットワークにおいて、2台のCisco NX-OSルータには以下の要件があります。

\* R1はアクティブなRPである必要があります。

\* R2は、R1にアクセスできない場合にのみ使用されるバックアップRPである必要があります。

ルーター2の設定を完了するには、設定手順をドラッグアンドドロップしてください。すべての設定手順を使用する必要はありません。

```
; Router 2 configuration
interface loopback1
  ip address [ ]
  ip ospf network [ ]
  ip router ospf 1 area 0.0.0.0
  ip pim [ ]

ip pim rp-address [ ] group-list 225.0.0.0/8 bi-dir
```

- 10.10.32.121/32
- 10.10.32.121
- point-to-point
- broadcast
- 10.10.32.121/29
- 10.10.32.122
- sparse-mode
- dense-mode

正解:

```
; Router 2 configuration
interface loopback1
  ip address 10.10.32.121/29
  ip ospf network point-to-point
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode

ip pim rp-address 10.10.32.122 group-list 225.0.0.0/8 bi-dir
```

- 10.10.32.121/32
- 10.10.32.121
- point-to-point
- broadcast
- 10.10.32.121/29
- 10.10.32.122
- sparse-mode
- dense-mode

質問: 273  
 ネットワークエンジニアが、Cisco Intersight管理ポータルにCisco HyperFlexデータプラットフォームを追加しています。IntersightがCisco HyperFlexデータプラットフォームを認識するために必要なコンポーネントはどれですか？ 2つ選択してください。)

- A. デバイスのFQDN
- B. デバイスのパブリックIPアドレス
- C. デバイスクレームコード
- D. デバイスID
- E. デバイスのシリアル番号

正解: C,D (コメントを发表する)

**Step 1** In the Cisco Intersight, left navigation pane, select **ADMIN > Targets**.

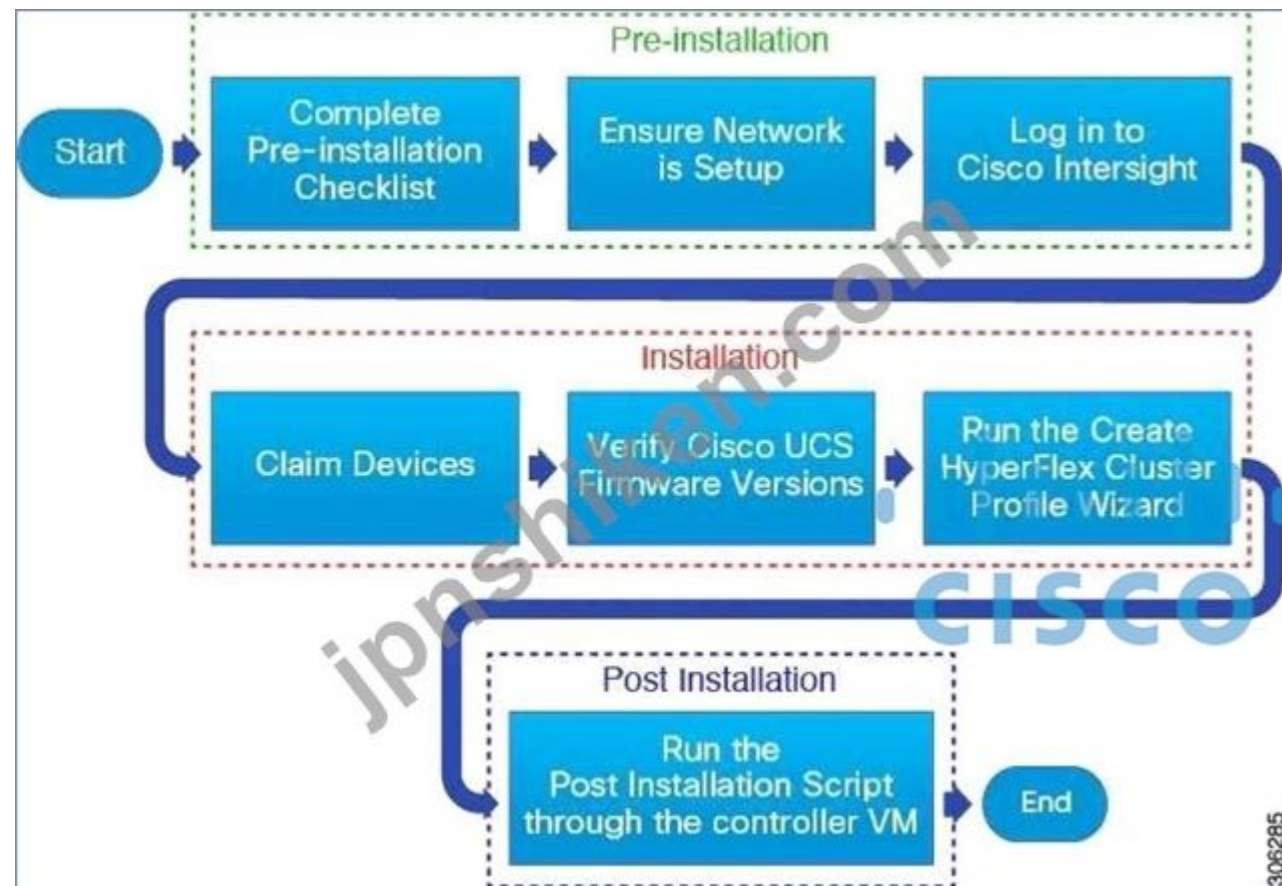
**Step 2** In the **Targets** details page, click **Claim a New Target**.

**Step 3** In the **Claim a New Target** wizard, select **Hyperconverged > Cisco HyperFlex Cluster** and complete the following fields:

**Note** You can locate the **Device ID** and the **Claim Code** information in:

- a. Cisco UCS Manager and Cisco IMC by navigating to **Admin > Device Connector**.
- b. Cisco HyperFlex by navigating to **HyperFlex Connect UI > Settings > Device Connector**.
- c. Cisco UCS Director by navigating to **Administration > Device Connector**.

UI Element	Essential Information
<b>Device ID</b>	Enter the applicable Device ID. <ul style="list-style-type: none"> <li>• For a UCS Domain, use the serial number of the primary and subordinate FIs, in this format: (Serial number of FI-A &amp; Serial number of FI-B). Example: [SAL1924GKV6&amp;SAL1913CJ7V]</li> <li>• For a standalone server, use serial number. Example: NGTR12345</li> <li>• For HyperFlex, use Cluster UUID. Example: xxxxxxxx-xxxx-xxxx-xxxx-</li> </ul>



[https://www.cisco.com/c/en/us/td/docs/hyperconverged\\_systems/HyperFlex\\_HX\\_DataPlatformSoftware/HyperFlex\\_Installation\\_Guide\\_for\\_Intersight/b\\_HyperFlex\\_Installation\\_Guide\\_for\\_Intersight\\_chapter\\_011.html](https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/HyperFlex_Installation_Guide_for_Intersight/b_HyperFlex_Installation_Guide_for_Intersight/b_HyperFlex_Installation_Guide_for_Intersight_chapter_011.html)

<https://www.cisco.com/c/en/us/support/docs/hyperconverged-infrastructure/hyperflex-hx-dataplatform/214268-cisco-intersight-hyperflex-installatio.html>

**質問: 274**

FC/FCoEの過剰加入率にはどのような種類がありますか？ (2つ選択してください。)

- A. サーバーストレージからエンドノードへのカウント
- B. ポート帯域幅からアップリンク帯域幅へ
- C. エッジISL帯域幅からコアISL帯域幅へ
- D. ホスト帯域幅からストレージ帯域幅へ
- E. 処理能力をエンドノードの処理能力に切り替える

正解: C,D (コメントを发表する)

<https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2017/pdf/BRKDCN-1121.pdf>

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/operations/n5k\\_fcoe\\_ops.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/operations/n5k_fcoe_ops.html)

**質問: 275**

エンジニアがREST API呼び出しを使用してCisco APICを設定しています。ログイントークンを受け取るには、POSTメッセージ内でどのデータ構造を使用する必要がありますか？

```
{aaaUser:{attributes:{name: apluser, pwd:cisco123}}}
```

A.

- B. `<aaaUser><name="apiuser"/><pwd="cisco123"/></aaaUser>`
- C. `{"aaaUser":{"attributes":{"name":"apiuser","pwd":"cisco123"}}`
- D. `<aaaUser><name>apiuser</name><pwd>cisco123</pwd></aaaUser>`

正解: **A** ([コメントを发表する](#))

REST API呼び出しを介してCisco APICを設定する際に、ログイントークンを受け取るためのPOSTメッセージ内で使用する正しいデータ構造は、ユーザー名とパスワード用の<name>タグと<pwd>タグがネストされた<aaaUser>タグを含むXMLペイロードです。この構造はオプションAに示されており、これはCisco APICへの認証リクエストの標準フォーマットです。

参考資料 :より詳細な情報については、Cisco APIC REST API構成ガイドを参照してください。このガイドには、認証やトークン取得プロセスを含む、システム構成にREST APIを使用するための包括的な手順が記載されています。

#### 質問: 276

Cisco MDS 9000シリーズスイッチでは、ポートセキュリティが有効になっています。

次の記述のうち、正しいものはどれですか？

- A. ポートセキュリティはグローバルにのみ有効にでき、すべてのVSANに影響します。
- B. 現在ログインしているデバイスはすべて、デバイスデータベースに手動で追加する必要があります。
- C. ポートセキュリティが有効になっている場合、自動学習は常に自動的に有効になります。
- D. ポートセキュリティを有効にする前に、Cisco Fabric Servicesを無効にする必要があります。

正解: **C** ([コメントを发表する](#))

セクション :セキュリティ

#### 質問: 277

展示資料を参照してください。

```
Start time: Mon Apr 15 09:23:01 2019
Last election time: Mon Apr 15 09:24:24 2019
A: UP, PRIMARY
B: UP, SUBORDINATE
A: memb state UP, lead state PRIMARY, mgmt services state: UP
B: memb state UP, lead state SUBORDINATE, mgmt services state: UP
heartbeat state PRIMARY_OK
INTERNAL NETWORK INTERFACES:
eth1, UP
eth2, UP
HA NOT READY
No device connected to this Fabric Interconnect
```

HA NOT READY状態を解除するには、何を接続すればよいですか？

- A. 管理ポート

- B. レイヤー1～レイヤー2ポート
- C. サーバーシャーシ
- D. ネットワークアップリンク

正解: [\(正解を表示します\)](#)

質問: 278

管理者は、MDSスイッチで特定のしきい値を超えた場合にリンクをシャットダウンする自動ポリシーを設定する必要があります。どの機能を使う必要がありますか？

- A. RMON
- B. EEM
- C. 自宅へ電話する
- D. スケジューラ

正解: [\(正解を表示します\)](#)

EEMは主に3つの構成要素から成り立っています。

イベントステートメント - 他の Cisco NX-OS コンポーネントから監視するイベントで、  
■ 何らかの対応、回避策、または通知。

アクションステートメント - EEM が実行できるアクション。たとえば、電子メールの送信や、  
■ インターフェースを使用して、イベントから復旧します。

ポリシー - イベントステートメントとアクションステートメントの組み合わせ。指定された  
■ イベントが発生すると、設定されたアクションが実行されます。

質問: 279

展示資料を参照してください。

```
Enter the configuration method. (console/gui) ? console
Enter the setup mode; setup newly or restore from backup.
(setup/restore) ? restore

NOTE:
To configure Fabric interconnect using a backup file on
a remote server, you will need to setup management
interface.
The management interface will be re-configured (if
necessary), based on information stored in the backup file.

Continue to restore this Fabric interconnect from a backup
file (yes/no) ? yes

Physical Switch Mgmt0 IPv4 address : 192.168.10.10
Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0
IPv4 address of the default gateway : 192.168.10.1
Enter the protocol to get backup file (scp/ftp/tftp/sftp)
? scp
Enter the IP address of backup server: 20.10.20.10
Enter fully qualified backup file name: Backup.bak
Enter user ID: user
Enter password:
Retrieved backup configuration file.
Configuration file - Ok
```

Cisco UCSの設定を復元するには、どのタイプのバックアップが必要ですか？

- A. 全構成

- B. 完全状態
- C. 論理構成
- D. システム構成

正解: ([正解を表示します](#))

質問: 280

エンジニアは、VLAN 100でHSRPを使用するようにNexus 7000シリーズスイッチを設定する必要があります。

完全に機能する場合、ルーターはアクティブマスターである必要があります。

このシナリオを実行するには、どのコマンドセットを使用する必要がありますか？

- feature hsrp  
interface vlan100  
ip address 10.1.1.2 255.255.255.0  
priority 120  
hsrp version 2  
hsrp 1000  
ip 10.1.1.1
- feature hsrp  
interface vlan100  
ip address 10.1.1.2 255.255.255.0  
priority 100  
hsrp version 2  
hsrp 1000  
ip 10.1.1.1
- feature-set hsrp  
interface vlan100  
ip address 10.1.1.2 255.255.255.0  
priority 110  
hsrp version 2  
hsrp 1000  
ip 10.1.1.1
- feature-set hsrp  
interface vlan100  
ip address 10.1.1.2 255.255.255.0  
priority 80  
hsrp version 2  
hsrp 1000  
ip 10.1.1.1

- A. オプションA
- B. 選択肢D
- C. オプションC
- D. オプションB

正解: ([正解を表示します](#))

質問: 281

展示資料を参照してください。

```
switch(config)# feature dhcp
switch(config)# ip dhcp snooping
switch(config)# service dhcp
switch(config)# ip dhcp snooping vlan 100,200,250-252
switch(config)# ip dhcp relay information option
```

リレーエージェントがDHCP BOOTREQUESTパケットをDHCPサーバーに転送することを確実にするために、どのような措置が取られますか？

- A. DHCPサーバーのインターフェースを信頼されていないものとして設定します。
- B. DHCPスヌーピングのバインディングを確認します。
- C. DHCPサーバーのIPアドレスを設定します。
- D. DHCPリレーエージェントを有効にします。

正解: D ([コメントを发表する](#))

質問: 282

ドラッグアンドドロップ問題

エンジニアは、2台のCisco Nexusシリーズスイッチを使用して冗長性を実装するためにHSRPプロトコルを設定する必要があります。さらに、HSRPは以下の要件を満たす必要があります。

- \* switch2がオフラインになった場合、switch1はプライマリロールを維持する必要があります。
- \* スイッチ1は、通常の状態に戻るまでプライマリロールを維持する必要があります。
- \* switch1とswitch2は、アクティブな役割を担う前に、ルーティングテーブルが収束していることを確認する必要があります。
- \* デフォルトゲートウェイに到達できない場合、switch2はプライマリの役割を維持する必要があります。

要件を満たすように、設定コマンドを右側から左側へドラッグアンドドロップしてください。

コマンドは複数回使用されます。ただし、すべてのコマンドが使用されるわけではありません。

```
! switch1
track 100 ip route 0.0.0.0/0 reachability
```

```
interface ethernet 1/1
ip 209.165.200.226/27
```

```
hsrp 200
ip 209.165.200.225
priority 210
```

```
no shutdown
```

```
! switch2
track 100 ip route 0.0.0.0/0 reachability
```

```
interface ethernet 1/1
ip 209.165.200.227/27
```

```
hsrp 200
ip 209.165.200.225
```

```
no shutdown
```

```
preempt delay minimum 30
```

```
track 100 decrement 200
```

```
track 200 decrement200
```

```
preempt sync 30
```

正解:

```

! switch1
track 100 ip route 0.0.0.0/0 reachability

interface ethernet 1/1
ip 209.165.200.226/27

hsrp 200
ip 209.165.200.225
priority 210
track 100 decrement 200
preempt delay minimum 30
no shutdown

! switch2
track 100 ip route 0.0.0.0/0 reachability

interface ethernet 1/1
ip 209.165.200.227/27

hsrp 200
ip 209.165.200.225
track 100 decrement 200
preempt delay minimum 30
no shutdown

```

```

preempt delay minimum 30
track 100 decrement 200
track 200 decrement 200
preempt sync 30

```

質問: 283

厳格なCoPPポリシーが実装されている場合、パケットが破棄される事象を説明しているのは次のうちどれですか？

- A. 15個のSSHセッションがスイッチに接続されたままです。
- B. デフォルトのVRFを使用して、大きなシステムイメージをスイッチにコピーします。
- C. スwitchを介して接続されたネットワークに対してピングスキャンを実行します。
- D. スwitchに接続されているウェブサーバーがDDoS攻撃の影響を受けています。

正解: C ([コメントを发表する](#))

厳格なCoPP（制御プレーンポリシング）ポリシーは、制御プレーンパケットのトラフィックフローを管理し、ルータやスイッチの制御プレーンが不要なトラフィックや悪意のあるトラフィックによって過負荷になるのを防ぐように設計されています。ネットワーク上の稼働中のデバイスを識別するために複数のホストにICMPエコー要求を送信するピングスイープが、厳格なCoPPポリシーが設定されたスイッチ

を介して接続されたネットワークで実行される場合、過剰なICMPパケットは破棄され、過剰なリソース消費を防ぐことができます。参考資料 :Ciscoデータセンターコアテクノロジーのソースドキュメントまたは学習ガイド

質問: 284

ブートフラッシュに動作イメージがない場合にファブリックインターコネクトを復旧するために、左側の手順を右側の手順を実行する順序にドラッグアンドドロップしてください。

Copy the main image files.	step 1
Configure the management interfaces.	step 2
Boot the kickstart image using TFTP.	step 3
Install the files.	step 4

正解:

Copy the main image files.	Boot the kickstart image using TFTP.
Configure the management interfaces.	Configure the management interfaces.
Boot the kickstart image using TFTP.	Copy the main image files.
Install the files.	Install the files.

Boot the kickstart image using TFTP.

Configure the management interfaces.

Copy the main image files.

Install the files.

質問: 285

ストレージエンジニアは、Cisco MDS 9000 シリーズスイッチでゾーニングを設定する必要があります。左側のアクションを右側の順序にドラッグアンドドロップしてください。

zone name Zone1 vsan 4	Step 1
member pwnn 10:00:00:23:45:67:89:ac	Step 2
zoneset activate name Zoneset1 vsan 4	Step 3
member Zone1	Step 4
copy running-config startup-config	Step 5
zoneset name Zoneset1 vsan 4	Step 6

正解:



説明

グラフィカルユーザーインターフェース、表の説明は中程度の信頼度で自動生成されます



```
Switch1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch1#(config)# vsan database
Switch1#(config-vsan-db)# vsan 100
Switch1#(config-vsan-db)# exit
```

```
Switch1#(config)# zone name zone1 vsan 100
Switch1#(config-zone)# member pwwn 11:11:11:11:11:11:1a
Switch1#(config-zone)# member pwwn 11:11:11:11:11:11:1b
Switch1#(config-zone)# exit
```

```
Switch1#(config)# zoneset name setA vsan 100
Switch1#(config-zoneset)# member zone1
Switch1#(config-zoneset)# exit
```

```
Switch1#(config)# zoneset activate name setA vsan 100
Zoneset activation initiated. check zone status
Switch1#(config)# exit
```

```
Switch1# sh zoneset active vsan 100
zoneset name setA vsan 100
zone name zone1 vsan 100
pwwn 11:11:11:11:11:11:1a
pwwn 11:11:11:11:11:11:1b
Switch1#
```

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6\\_2/configuration/guides/fabric/nx-os/nx\\_os\\_fabric/zone.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6_2/configuration/guides/fabric/nx-os/nx_os_fabric/zone.html)

質問: 286

展示資料を参照してください。

```
; Router 1 configuration
interface loopback1
 ip address 10.10.32.121/30
 ip ospf network point-to-point
 ip router ospf 1 area 0.0.0.0
 ip pim sparse-mode

ip pim rp-address 10.10.32.122 group-list 225.0.0.0/8 bi-dir
```

Phantom RPをRP冗長化メカニズムとして使用する双方向PIMネットワークにおいて、2台のCisco NX-OSルータには以下の要件があります。

\* R1はアクティブなRPである必要があります。

\* R2は、R1にアクセスできない場合にのみ使用されるバックアップRPである必要があります。

ルーター2の設定を完了するには、設定手順をドラッグアンドドロップしてください。すべての設定手順を使用する必要はありません。

```
; Router 2 configuration
interface loopback1
  ip address [ ]
  ip ospf network [ ]
  ip router ospf 1 area 0.0.0.0
  ip pim [ ]

ip pim rp-address [ ] group-list 225.0.0.0/8 bi-dir
```

10.10.32.121/32	10.10.32.121	point-to-point	broadcast
10.10.32.121/29	10.10.32.122	sparse-mode	dense-mode

正解:

```
; Router 2 configuration
interface loopback1
ip address 10.10.32.121/29
ip ospf network point-to-point
ip router ospf 1 area 0.0.0.0
ip pim sparse-mode

ip pim rp-address 10.10.32.122 group-list 225.0.0.0/8 bi-dir
```

10.10.32.121/32    10.10.32.121    point-to-point    broadcast

10.10.32.121/29    10.10.32.122    sparse-mode    dense-mode

#### 説明

グラフィカルユーザーインターフェース、テキスト、アプリケーションの説明は自動的に生成されます

```
Answer :
ip address 10.10.32.121/29
ip ospf network point-to-point
router ospf 1 area 0.0.0.0
ip pim sparse-mode

ip pim rp-address 10.10.32.122 group-list 225.0.0.0/8 bi-dir
```

有効的な**350-601**問題集はJPNTTest.com提供され、**350-601**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-601**試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで**350-601**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> **384**問、**30%ディスカウント**、特別な割引コード:

**JPNshiken**」

#### 質問: 287

双方向PIMがサイトに導入されると、どのmroute状態が作成されますか？

- A. \*.G
- B. MVPN タイプ6
- C. MVPN タイプ7
- D. SG

正解: ([正解を表示します](#))

双方向PIMは、多数の送信元と受信元が相互に通信するネットワーク向けに開発されました。PIMスパースモードRPは\*,GとS,Gの2つのエントリを作成しますが、双方向PIMモードを使用すると、RPはS,Gエントリを作成せず、\*,Gエントリのみを許可します。

PIM双方向モードを使用する場合、RPは(S,G)エントリを作成せず、共有ツリーに対して(\*,G)エントリのみを許可します。PIMルーターは、送信元への最短経路ツリー(SPT)を作成しません。

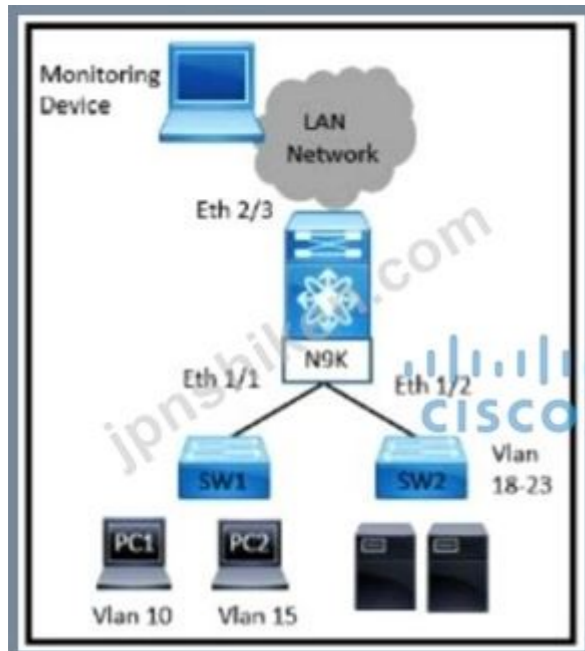
参照：

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti\\_pim/configuration/xr-16-5/imc-pim-xr-16-5-book/imc-tech-overview.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xr-16-5/imc-pim-xr-16-5-book/imc-tech-overview.html)

<https://networklessons.com/multicast/multicast-bidirectional-pim>

質問: 288

展示資料を参照してください。



図を参照してください。ネットワーク管理者は、ネットワークに関して次のような問題に直面しています。

PC1でビデオアプリケーションのバッファリング問題が発生しています

SW2に接続されているサーバーがインターネットに接続する際にパケット損失が発生しています。エンジニアは、この問題をさらに調査するために必要なトラフィックキャプチャを設定したいと考えています。トラフィックを監視するには、どの設定を実装する必要がありますか？

- N9K(config)# monitor session 5 rx  
N9K(config)# monitor session 5 tx  
N9K(config-monitor)# description Span\_session\_5  
N9K(config-monitor)# source interface ethernet 1/1  
N9K(config-monitor)# source interface ethernet 1/2  
N9K(config-monitor)# destination interface ethernet 2/3
- N9K(config)# monitor session 5 tx  
N9K(config-monitor)# description Span\_session\_5  
N9K(config-monitor)# source interface ethernet 1/1  
N9K(config-monitor)# source interface ethernet 1/2  
N9K(config-monitor)# destination interface ethernet 2/3
- N9K(config)# monitor session 5 tx  
N9K(config-monitor)# description Span\_session\_5  
N9K(config-monitor)# source vlan 10-15 rx  
N9K(config-monitor)# source interface ethernet 1/2  
N9K(config-monitor)# destination interface ethernet 2/3
- N9K(config)# monitor session 5 rx  
N9K(config-monitor)# description Span\_session\_5  
N9K(config-monitor)# source vlan 10 rx  
N9K(config-monitor)# source interface ethernet 1/2  
N9K(config-monitor)# destination interface ethernet 2/3

- A. オプションA
- B. オプションB
- C. オプションC
- D. 選択肢D

正解: [\(正解を表示します\)](#)

質問: 289

エンジニアがカスタムゲストシェルルートファイルシステムを複数のスイッチに展開します。左側の手順を右側の正しい順序にドラッグアンドドロップしてください。

Customize the guest shell rootfs.	Step 1
Export the Guest Shell rootfs.	Step 2
Store it in a file server.	Step 3
Import the Guest Shell rootfs to other switches.	Step 4
Install the specific Guest Shell across devices simultaneously.	Step 5

正解:

Customize the guest shell rootfs.	Export the Guest Shell rootfs.
Export the Guest Shell rootfs.	Store it in a file server.
Store it in a file server.	Customize the guest shell rootfs.
Import the Guest Shell rootfs to other switches.	Import the Guest Shell rootfs to other switches.
Install the specific Guest Shell across devices simultaneously.	Install the specific Guest Shell across devices simultaneously.

説明

ゲストシェルのルートファイルシステムをエクスポートする手順1

ファイルサーバーに保存する手順2

ゲストシェルルートファイルシステムのカスタマイズ手順3

ゲストシェルのルートファイルシステムを他のスイッチにインポートする手順4

特定のゲストシェルを複数のデバイスに同時にインストールする手順5

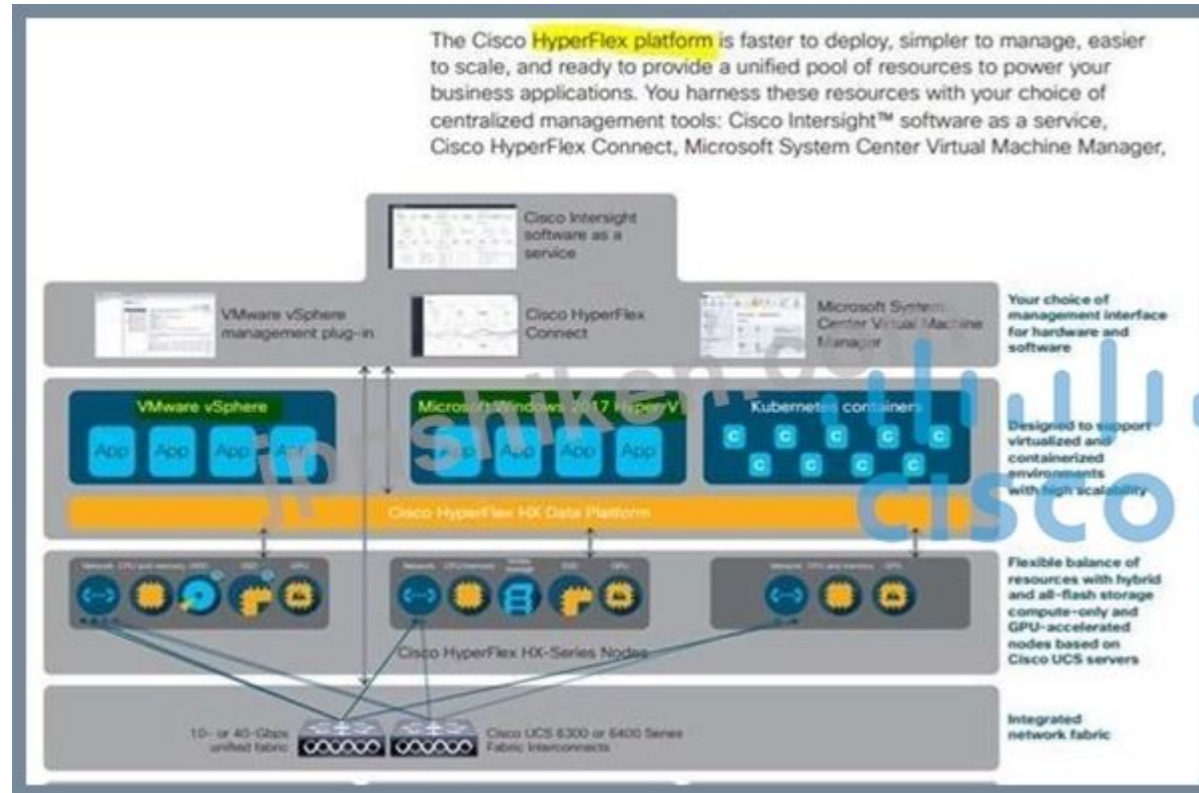
質問: 290

Cisco HyperFlexは、どの2つのハイパーバイザーをサポートしていますか？ (2つ選択してください。)

- A. VMware vSphere
- B. Microsoft Hyper-V
- C. OpenStack
- D. Citrix XenServer
- E. RedHat KVM

正解: (正解を表示します)

説明



<https://www.cisco.com/c/dam/en/us/products/collateral/hyperconverged-infrastructure/hyperflex-hx-series/solution-overview-c22-736815.pdf>

質問: 291

図を参照してください。Cisco MDS 9700シリーズスイッチモジュールのEPLDのうち、アップグレードされたのはどれですか？

- A. PSU
- B. 生地
- C. 待機監督者
- D. ファン

正解: (正解を表示します)

正解はC. 待機監督者です。

展示資料から、コマンド出力は明確に以下を示している。

モジュール6 SUP はい、破壊的モジュール アップグレード可能で、後日確認します:

モジュール6のEPLDアップグレードとSUP6のアップグレードは成功しました。

これは、EPLDのアップグレードがスーパーバイザ (SUP) モジュール、具体的にはモジュール6で実行されたことを示しています。Cisco MDS 9700アーキテクチャでは、スーパーバイザモジュールは冗長構成 (アクティブとスタンバイ) で動作します。EPLDのアップグレードを実行する際、Ciscoのベストプラクティスおよびシステム動作では、通常、スタンバイ側のスーパーバイザを先にアップグレードします。これは、システムが制御プレーンの継続性を維持し、障害を最小限に抑えることができるためです。

出力には電源ユニット、ファン、ファブリックモジュールに関する記述がないため、オプションA、B、Dは除外されます。SUPへの明示的な言及から、アップグレードはスーパーバイザーモジュールに適用されることが確認できます。

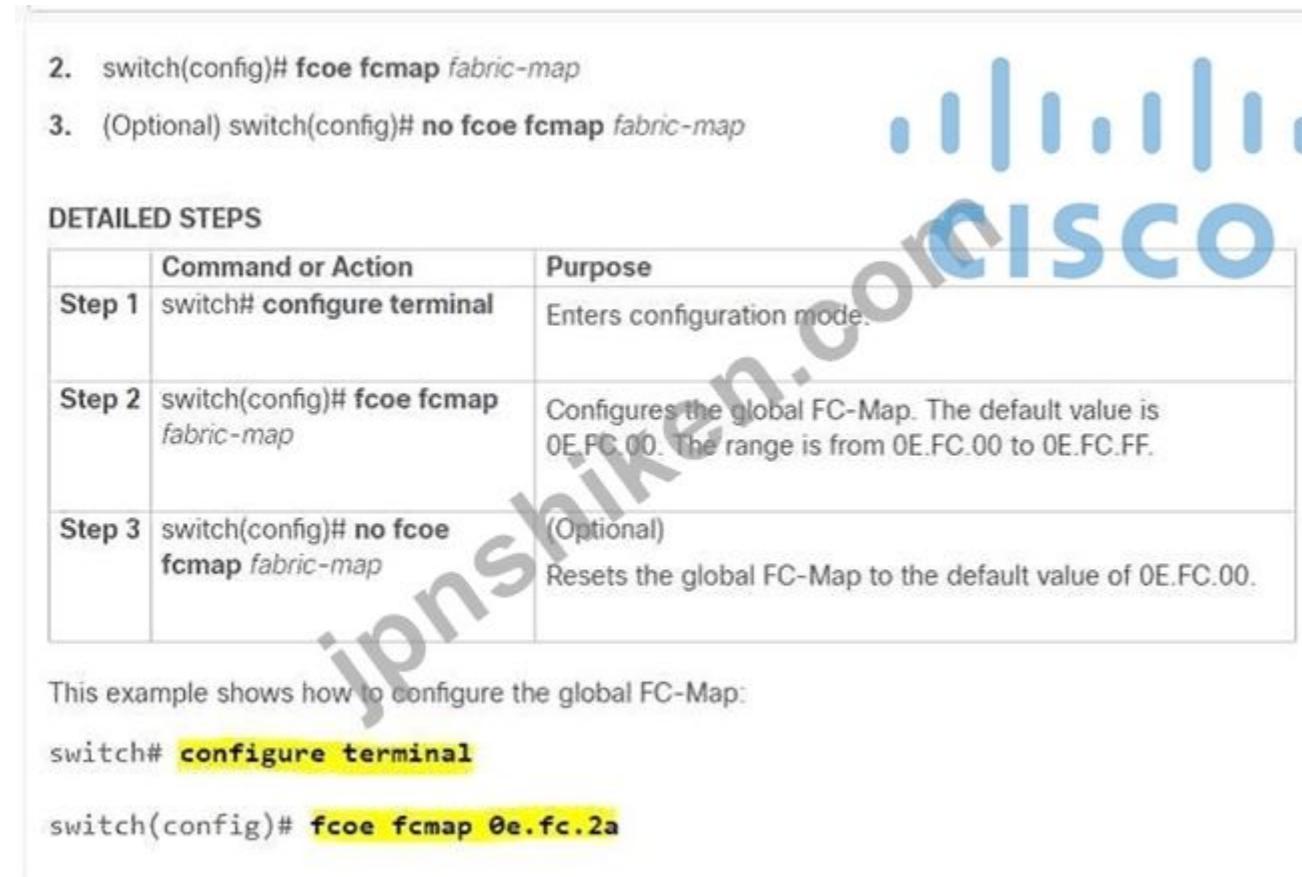
したがって、出力に表示されているモジュールタイプと標準的なCiscoのアップグレード動作に基づくと、EPLDのアップグレードはスタンバイスーパーバイザに適用されるため、Cが正解となります。

質問: 292

ネットワークエンジニアは、FCoE環境におけるファブリック間通信によるデータ破損を防止する必要があります。この目的を達成するには、Cisco Nexus Unified Switchにどのような設定を適用する必要がありますか？

- A. Switch(config)#fcoe fcmmap 0e,fc,2a
- B. Switch(config-if)# no fcoe fcf-priority 0
- C. Switch(config-if) # shutdown lan
- D. Switch(config) # no fcoe fcf-priority

正解: (正解を表示します)



2. switch(config)# fcoe fcmmap fabric-map

3. (Optional) switch(config)# no fcoe fcmmap fabric-map

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# fcoe fcmmap fabric-map	Configures the global FC-Map. The default value is 0E.FC.00. The range is from 0E.FC.00 to 0E.FC.FF.
Step 3	switch(config)# no fcoe fcmmap fabric-map	(Optional) Resets the global FC-Map to the default value of 0E.FC.00.

This example shows how to configure the global FC-Map:

```
switch# configure terminal
switch(config)# fcoe fcmmap 0e.fc.2a
```

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/fcoe/b\\_Cisco\\_Nexus\\_5000\\_Series\\_NX-OS\\_Fibre\\_Channel\\_over\\_Ethernet\\_Configuration\\_Guide\\_/Cisco\\_Nexus\\_5000\\_Series\\_NX-OS\\_Fibre\\_Channel\\_over\\_Ethernet\\_Configuration\\_Guide\\_\\_chapter3.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/fcoe/b_Cisco_Nexus_5000_Series_NX-OS_Fibre_Channel_over_Ethernet_Configuration_Guide_/Cisco_Nexus_5000_Series_NX-OS_Fibre_Channel_over_Ethernet_Configuration_Guide__chapter3.html)

質問: 293

エンジニアは、Cisco Nexusシリーズスイッチの設定を中央の場所にバックアップするための自動化ソリューションを実装する必要があります。このソリューションは以下の要件を満たす必要があります。

- \* フレームワークがサポートする必要があるRPMパッケージを使用してパッケージ化された、チームが開発したカスタム監視スクリプトをサポートする。
- \* 基盤となるCisco Nexusオペレーティングシステムをベースに開発される。
- リソース競合が発生した場合でも、基盤となるスイッチのオペレーティングシステムには影響を与えません。
- \* Pythonを使用して、既存の自動化フレームワークを拡張します。

これらの要件を満たすソリューションはどれですか？

- A. ゲストシェル
- B. バッシュシェル
- C. TCLシェル
- D. ベガスシェル

正解: ([正解を表示します](#))

Cisco Nexusシリーズスイッチの設定を中央の場所にバックアップするための自動化ソリューションの実装要件を満たすソリューションは、ゲストシェルです。ゲストシェルは、Cisco Nexusオペレーティングシステム上で動作するLinuxベースのコンテナであり、Pythonスクリプトやカスタムアプリケーションを実行するための安全な環境を提供します。ゲストシェルはRPMパッケージ形式をサポートしているため、チームが開発したカスタム監視スクリプトを簡単にインストールおよび管理できます。ゲストシェルは基盤となるCisco Nexusオペレーティングシステムから分離されているため、リソース競合が発生してもオペレーティングシステムに影響を与えません。また、ゲストシェルを使用すると、既存の自動化フレームワークを拡張するためにPythonを使用できます。たとえば、NX-APIやCisco Nexus Python SDKを使用してスイッチの設定や状態とやり取りできます。参照:

\* Cisco Data Center Core Technologies (DCCOR) v1.2 の実装と運用、モジュール 8: データセンターの自動化とオーケストレーション、レッスン 8.2: Cisco NX-OS プログラマビリティ

\* Cisco Nexus 9000シリーズ NX-OS プログラマビリティガイド、リリース9.3(x)、章 :ゲストシェルの使用

#### 質問: 294

顧客サイトでドメイン名が変更されたため、Cisco UCSクラスタの名前を変更する必要があります。エンジニアは、Cisco UCS ManagerがHTTPS経由で利用可能であることを保証するための解決策を提案する必要があります。この目的を達成するには、どの操作を実行すればよいでしょうか？

- A. クラスタを再インストールして、デフォルトのキーリング証明書を生成します。
- B. Cisco UCS Managerから新しいデフォルトキーリング証明書を生成する
- C. Cisco UCS ManagerのSSOコンポーネントを再起動します。
- D. デフォルトのキーリング証明書を手動で再生成する

正解: ([正解を表示します](#))

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Managem](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Managem)

The default key ring certificate must be manually regenerated if the cluster name changes or the certificate expires.

#### 質問: 295

エンジニアがセキュアな環境にCisco Intersightを導入しようとしています。この環境ではLDAPディレクトリサービスを使用し、情報の完全性と機密性を確保する必要があります。このソリューションを導入するために実行すべき2つの手順はどれですか？ (2つ選択してください。)

- A. LDAPの暗号化を有効にする
- B. Cisco Intersightに自己署名LDAP証明書を追加します。
- C. Cisco Intersightで証明書署名要求を有効にする。
- D. Cisco Intersightに信頼できるルートLDAP証明書を追加する
- E. 信頼できるOAuthトークンをCisco Intersightに追加する

正解: A,D ([コメントを发表する](#))

Find Matches in This Book

**Step 3** On the **Configure LDAP** page, add the corresponding details in the fields that are listed below, and click **Save**.

- **Name**—Enter a name to easily identify the LDAP domain that you are configuring.
- **Base DN**—Enter a Base Distinguished Name (DN) for the server. For example, DC=Intersight, DC=com.
- **Bind DN**—Enter a DN used to authenticate against LDAP server and the password for the user.
- **Group Attribute**—Enter the Group member attribute to which an LDAP entry belongs. Cisco Intersight Virtual Appliance uses this Group attribute to map/assign Intersight roles to the user. The default value is **member** and you can change it from **Edit LDAP** settings.
- **Password**—Enter a DN password for the user.
- **Enable Encryption**—You must enable Encryption to secure the communication over the LDAP server. If encryption is enabled, a trusted root certificate has to be added. For more information, see *Adding Certificates*.
- **In Server**—Add an LDAP Server IP address or hostname. Cisco Intersight Virtual Appliance supports only one LDAP provider and port.

**Attention**

- LDAPS is supported on Port 636 and Port 3269. All other ports support LDAP on TLS.
- Cisco Intersight Virtual Appliance uses the email ID or username to log in an LDAP user. If you want to use email ID to log in to the appliance, configure the mail attribute in the LDAP server. If you want to use the username, use the sAMAccountName configured for that user in the LDAP server.
- After you add the required details to configure LDAP settings, wait for the DeployApplianceLDAP workflow to complete before you add User or Group to assign appropriate roles to LDAP users. You can

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/Intersight/b\\_Cisco\\_Intersight\\_Appliance\\_Getting\\_Started\\_Guide/b\\_Cisco\\_Intersight\\_Appliance\\_Install\\_and\\_Upgrade\\_Guide\\_chapter\\_0110.html](https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Cisco_Intersight_Appliance_Getting_Started_Guide/b_Cisco_Intersight_Appliance_Install_and_Upgrade_Guide_chapter_0110.html)

#### 質問: 296

エンジニアは、仮想ポートチャネルを実行している2台のCisco Nexus 9000シリーズスイッチでHSRPプロトコルを設定する必要があります。さらに、HSRPの実装は以下の要件を満たす必要があります。

- It must allow more than 500 groups.
- switch1 must act as the primary switch.
- Both switches must use a user-defined hardware address.

右側のコマンドをドラッグアンドドロップして、左側のHSRPの設定を完了してください。コマンドは複数回使用されます。すべてのコマンドが使用されるわけではありません。

```
! switch1
interface vlan300
ip 209.165.200.226/27
harp 300
```

```
ip 209.165.200.225
```

```
! switch2
```

```
interface vlan300
ip 209.165.200.227/27
harp 300
```

```
ip 209.165.200.225
```



```
mac-address 6000.6000.6000
```

```
harp version 1
```

```
priority 255
```

```
harp use-bia
```

```
priority 100
```

```
harp version 2
```

正解:

```
! switch1
interface vlan300
ip 209.165.200.226/27
harp 300
```

```
mac-address 6000.6000.6000
```

```
harp version 2
```

```
ip 209.165.200.225
```

```
priority 255
```

```
! switch2
```

```
interface vlan300
ip 209.165.200.227/27
harp 300
```

```
mac-address 6000.6000.6000
```

```
harp version 2
```

```
ip 209.165.200.225
```

```
priority 100
```



```
mac-address 6000.6000.6000
```

```
harp version 1
```

```
priority 255
```

```
harp use-bia
```

```
priority 100
```

```
harp version 2
```

```

! switch1
interface vlan300
ip 209.145.200.224/24
harp 300
mac-address 6000.6000.6000
harp version 2
priority 255

! switch2
interface vlan300
ip 209.145.200.224/24
harp 300
mac-address 6000.6000.6000
harp version 2
priority 100

```

質問: 297

ネットワークエンジニアは、ユーザーがCisco Nexusスイッチに設定を保存した際に、実行中の設定のコピーをブートフラッシュに保存し、syslogにメッセージを書き込むEEMスクリプトを作成する必要があります。このタスクを完了するには、どの設定セットを適用すればよいでしょうか？

```

event manager applet local- backup
event cli match "copy running-config startup-config"
action 1 cli copy running-config bootflash:/current_config.txt
action 2 syslog msg Configuration saved and copied to bootflash

event manager applet local- backup
event cli match "write memory"
action 1 cli copy running-config bootflash:/current_config.txt
action 2 snmp-trap strdata "Configuration saved and copied to bootflash"

event manager applet local- backup
event cli match "copy running-config startup-config"
action 1 cli copy running-config bootflash:/current_config.txt
action 2 syslog msg Configuration saved and copied to bootflash
action 3 event-default

event manager applet local- backup
event cli match "write memory"
action 1 cli copy running-config bootflash:/current_config.txt
action 2 syslog msg Configuration saved and copied to bootflash
action 3 event-default

```

- A. オプションA
- B. オプションB
- C. オプションC
- D. 選択肢D

正解: [\(正解を表示します\)](#)

NX-OSでは、write memoryコマンドは無効です。

「イベントデフォルト」

If you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the default action. For example, if you match a CLI command in a match statement, you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute.

質問: 298

エンジニアはデータセンターでOSPFを設定する必要があります。外部ルートは既にOSPFによって再配布されています。ネットワークは以下の条件を満たす必要があります。

\* データセンターのサーバーは、クラウド上のサービスと、再分配された経路の背後にあるサービスにアクセスできる必要があります。

\* インターネットへの出口ポイントは、上流ルーターから動的に学習されたデフォルトルートが存在する場合にのみ伝播されるべきである。

どの機能が必要ですか？

- A. 完全に短いエリア
- B. 短いエリア
- C. デフォルト情報の発生源
- D. デフォルト情報は常に

正解: [\(正解を表示します\)](#)

<https://learningnetwork.cisco.com/s/question/0D53i00000Kt544/defaultinformationoriginate-always>

質問: 299

展示資料を参照してください。

```
NEXUS (config)# feature tacacs+
NEXUS (config)# tacacs-server timeout 5
NEXUS (config)# tacacs-server directed-request
NEXUS (config)# tacacs-server deadtime 0
NEXUS (config)# tacacs server host 10.1.50.20 port 49
NEXUS (config)# tacacs-server host 10.1.50.20 key 7 "Flwhg123" timeout 1
NEXUS (config)# aaa group server tacacs+ ISE
NEXUS (config-tacacs+)# server 10.1.50.20
NEXUS (config-tacacs+)# deadtime 10
NEXUS (config-tacacs+)# use vrf management
NEXUS (config-tacacs+)# source-interface mgmt 0
NEXUS (config)# aaa authentication login default group ISE
```

この設定を実装した結果はどうなりますか？

- A. スイッチは暗号化されたテキストPAPログインを使用してTACACS+サーバーに問い合わせます。
- B. TACACS+サーバーのタイムアウト値は10秒です。
- C. TACACS+サーバーはタイプ6暗号化フォーマットを使用します。
- D. スイッチは平文のPAPログインを使用してTACACS+サーバーに問い合わせます。

正解: [D \(コメントを发表する\)](#)

質問: 300

ネットワークエンジニアは、ファブリック内のすべてのCisco MDSシリーズスイッチでポートセキュリティを有効にする必要があります。要件は、スイッチポートの大規模な手動設定を回避することです。

これらの要件を満たすために、どのような対策を講じる必要がありますか？

- A. CFS配信と自動学習ポートセキュリティ機能を有効にします。
- B. VSANごとにCFS配布とファイル自動学習ポートセキュリティ機能を有効化します。
- C. VSANごとに自動学習ポートセキュリティ機能を有効にします。
- D. ポートセキュリティの自動学習機能を有効にします。

正解: [\(正解を表示します\)](#)

スイッチに、指定した期間にわたってポートセキュリティ設定を自動的に学習（自動学習するように指示できます。この機能により、Cisco MDS 9000 ファミリーのスイッチは、接続されているデバイスやスイッチを自動的に学習できます。ポートセキュリティ機能を初めて有効化する際には、この機能を使用すると、各ポートの面倒な手動設定を省くことができます。自動学習は、VSAN ごとに設定する必要があります。https://www.cisco.com/en/US/docs/storage/san\_switches/mds9000/sw/rel\_3\_x/configuration/guides/fm\_3\_3\_1/psec.html#wp1170020

#### 質問: 301

Cisco Nexusシリーズスイッチ上のCisco TACACS+は、デバイスへのアクセスを試みるすべてのユーザーを認証し、TACACS+サーバーが利用できなくなった場合はローカルアカウントにフェイルオーバーする必要があります。

これらの目的を達成するコマンドはどれですか？

- A. aaa認証ログインデフォルトフォールバックエラーローカル
- B. aaa認証ログインコンソールグループローカル
- C. aaa認証ログインデフォルトローカル
- D. aaa認証ログインデフォルトグループISEローカル

正解: D (コメントを发表する)

コマンド「aaa authentication login default group ISE local」は、Cisco Nexus Series SwitchをデフォルトでTACACS+認証を使用するように設定し、TACACS+サーバーが利用できなくなった場合にローカル認証にフォールバックするように指定します。これにより、TACACS+サーバーが利用可能な場合はユーザーが認証されることが保証されますが、サーバーに接続できない場合はローカルスイッチの認証情報を使用できるため、ローカルアカウント1へのフェイルオーバー要件を満たします。

参考文献:

Cisco NexusシリーズスイッチのTACACS+設定に関するCiscoのドキュメントには、認証の設定とローカルアカウントへのフェイルオーバーの確保に関する詳細な手順と説明が記載されています。

有効的な**350-601**問題集はJPNTTest.com提供され、**350-601**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-601**試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで**350-601**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> **384**問、**30%ディスカウント**、特別な割引コード:

**JPNshiken**」

有効的な**350-601**問題集はJPNTTest.com提供され、**350-601**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-601**試験問題集を提供します。JPNTTest.com 350-601試験問題集はもう更新されました。ここで**350-601**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-601-mondaishu> **384**問、**30%ディスカウント**、特別な割引コード:

**JPNshiken**」