GETCERTKEY

GETCERTKEY
100% guarantee you pass IT cert exam!

http://www.getcertkey.com

No help, Full refund!

Exam : **350-601J**

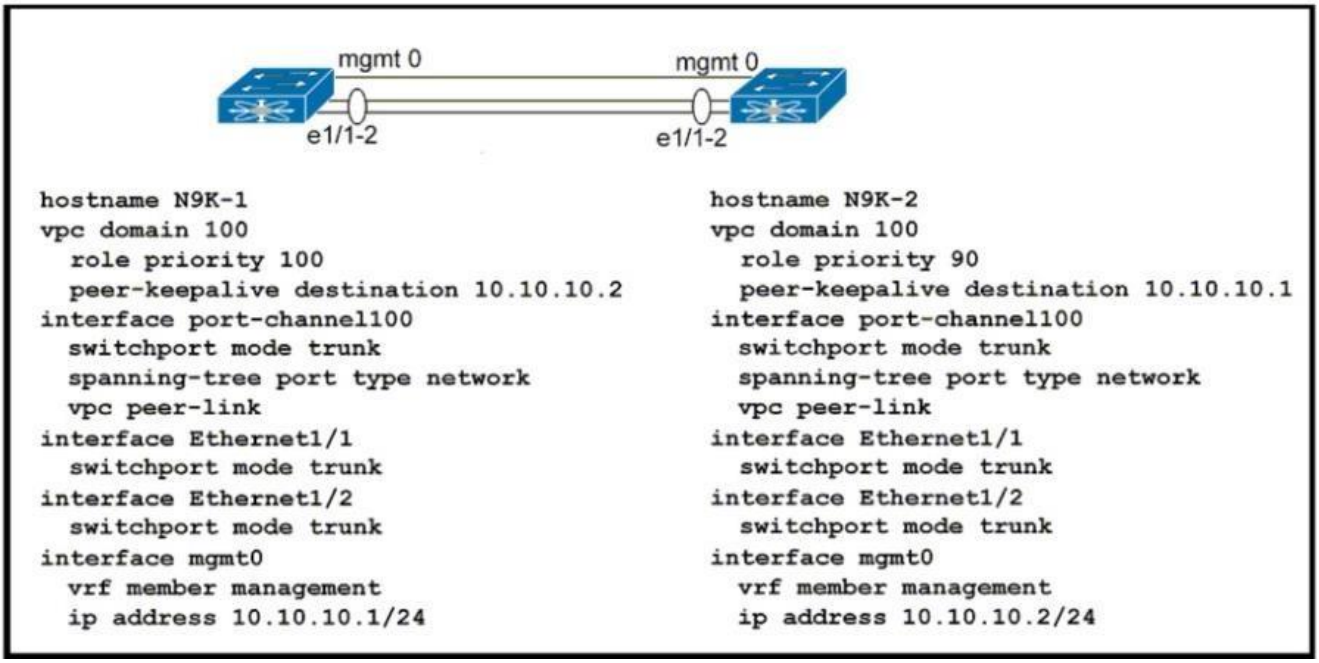
Title : Implementing and Operating Cisco Data Center Core Technologies (350-601日本語版)

Vendor : Cisco

Version : DEMO

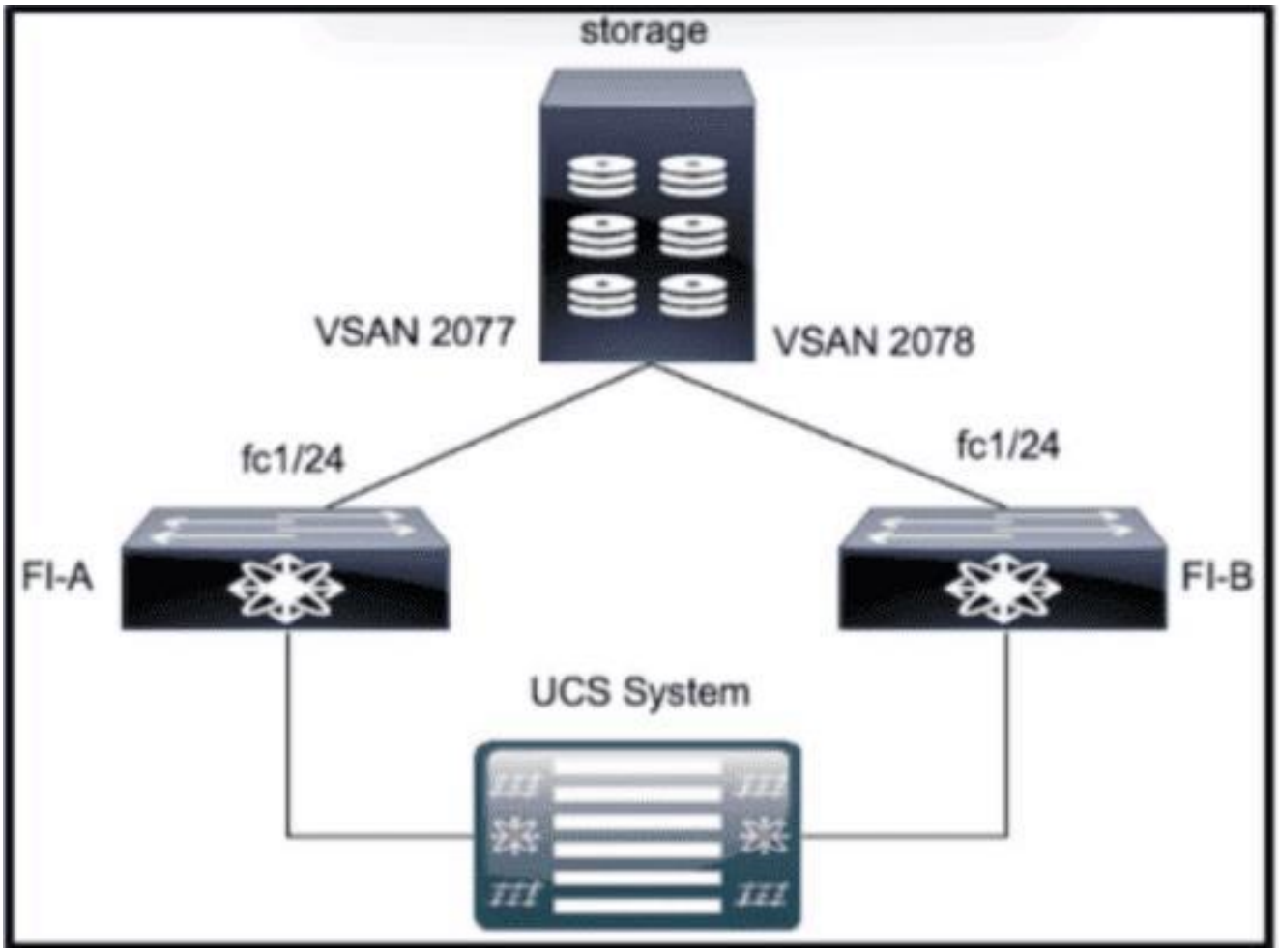
QUESTION NO: 1
エンジニアはアップリンクイーサネットポートからのトラフィックを監視する必要があります。トラフィックは、ファブリックインターコネクトのインターフェースEth1/5に接続されたアナライザに送信する必要があります。この要件を満たすには、宛先インターフェースにどのような設定を行う必要がありますか？
A. 未設定
B. サーバー
C. アップリンク
D. アプライアンス
Answer: C

QUESTION NO: 2



図を参照してください。vPC
ドメインの実装を完了するには、どのアクションを実行する必要がありますか?
A. vPC ピア リンク メンバー インターフェイスで VLAN を許可します。
B. vPC ドメインに VRF 管理を含めます。
C. vPC ドメインでシステム MAC を設定します。
D. vPC メンバー ポートを vPC チャネル グループに追加します。
Answer: D

QUESTION NO: 3



図を参照してください。VSAN 2077
はプライマリパスとして設定されています。デバイスネイバーがポート FC1/24
を使用してサーバとの通信を許可している間、Cisco UCS
システムでゾーニングを有効にするには、どのような設定を行う必要がありますか？
A. FI をファイバー チャネル スイッチング モードに設定し、ポート (d/24) を FCoE
アップリンク ポートとして設定します。
B. FI をファイバー チャネル スイッチング モードで設定し、ポート fd/24 をネットワーク
アップリンク ポートとして設定します。
C. FI をファイバ チャネル スイッチング モードで設定し、ポート fd/24 をファイバ チャネル
ストレージ ポートとして設定します。
D. FI をファイバー チャネル エンドホスト モードで設定し、ポート fd/24 をアプライアンス
ポートとして設定します。
Answer: D

QUESTION NO: 4
エンジニアは、インバンドのCisco
IMCプロファイル設定を許可し、ディスクとLUNのローカルストレージポリシーを適用する
必要があります。これらのアクションを許可するには、ユーザープロファイルにどの権限セ
ットを使用する必要がありますか？
A. オペレーション組織管理
B. ネットワーク障害

C. ext-lan-config ls-compute
D. pn機器電源管理
Answer: C

QUESTION NO: 5
図を参照してください。Cisco UCS
サーバ内にトラフィックコレクタ仮想マシンがインストールされています。コレクタは、ERSPAN を使用して G1/2
で受信したトラフィックを監視する必要があります。トラフィックをトラフィックコレクタに送信するには、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. ERSPANを設定します。Cisco UCS Managerで送信元セッションを設定します。
B. SPANを設定します。SW1スイッチに送信元セッションを設定します。
C. ERSPANを設定します。SW1スイッチに送信元セッションを設定します。
D. SPANを設定します。Cisco UCS Managerで送信元セッションを設定します。
Answer: C

QUESTION NO: 6
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 sangroup ロールに割り当てられたユーザーが VSAN 15 ~ 20
でコマンドを発行することを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。

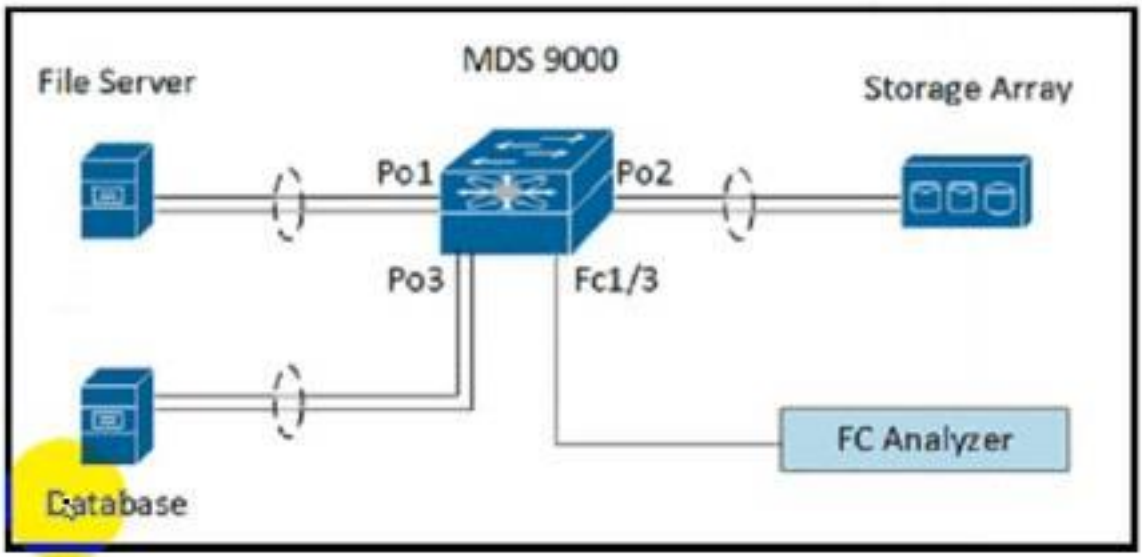
```
Role: sangroup
  Description: SAN management group
  vsan policy: deny
  Permitted vsans: 10-30

  ----------------------------------------------
  Rule    Type    Command-type      Feature
  ----------------------------------------------
    1.   permit    config                  *
    2.     deny    config               fspf
    3.   permit     debug               zone
    4.   permit      exec             fcping
```

Refer to the exhibit. An engineer must restrict users assigned to the sangroup role on the Cisco MDS 9000 Series Switch from issuing commands on VSANs 15 to 20. Which command must the engineer run to achieve this objective?

- `vsan policy deny vsan 15-20`
- `no permit vsan 15-20`
- `permit vsan 15-20`
- `no vsan policy deny`

A. vsan ポリシー拒否 vsan 15-20
B. 許可なし vsan 15-20
C. vsan 15-20 を許可する
D. vsanポリシー拒否なし
Answer: A

QUESTION NO: 7




```
interface port-channel 1
  channel mode active
interface port-channel 2
  channel mode active
interface fc1/1-2
  channel-group 1
  no shutdown
interface fc1/4-5
  channel-group 2
  no shutdown
interface fc1/7-8
  channel-group 3
  no shutdown
vsan database
  vsan 100 name fabric1
  vsan 100 interface port-channel 1
  vsan 100 interface port-channel 2
  vsan 100 interface port-channel 3
```

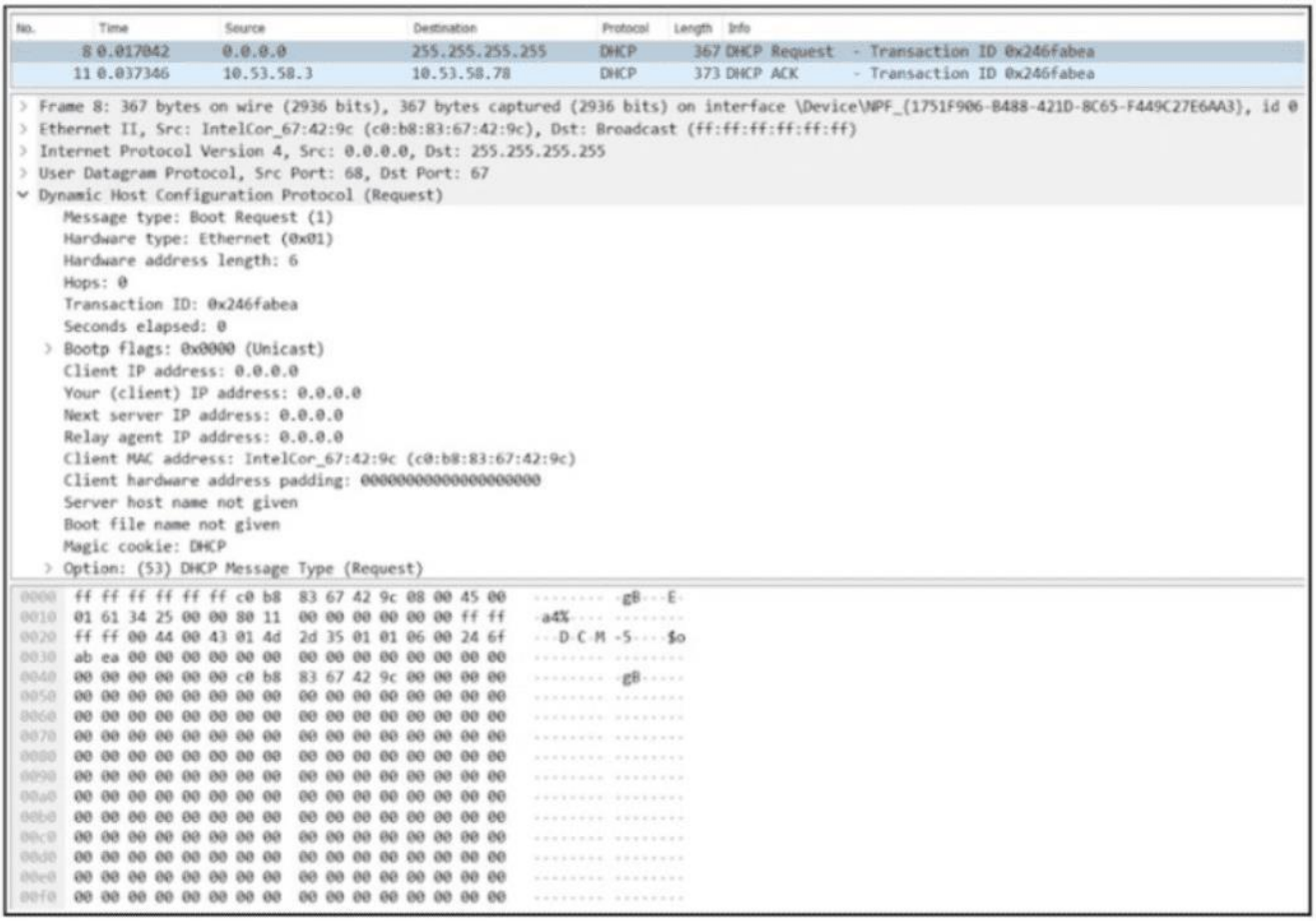
図を参照してください。ストレージエンジニアは、ファイルサーバからFCアナライザへのトラフィックを監視する必要があります。ファイルサーバとデータベースは同じストレージアレイを使用しています。この目標を達成するには、Cisco MDS 9000シリーズスイッチにどのような設定を適用する必要がありますか？

```
MDS-9000(config)# span session 1
MDS-9000(config-span)# destination interface fc1/3
MDS-9000(config-span)# source interface port-channel 1

MDS-9000(config)# span session 1
MDS-9000(config-span)# destination interface port-channel 2
MDS-9000(config-span)# source interface vsan 100

MDS-9000(config)# span session 1
MDS-9000(config-span)# destination interface port-channel 2
MDS-9000(config-span)# source interface fc1/1

MDS-9000(config)# span session 1
MDS-9000(config-span)# destination interface vsan 100
MDS-9000(config-span)# source interface port-channel 1
```

A. オプションA
B. オプションB
C. オプションC
D. オプションD
Answer: A

QUESTION NO: 8
エンジニアは、顧客のリモートネットワークデバイスの設定と導入を自動化するソリューションを必要としています。エンジニアは、以下の点を念頭に置く必要があります。
*
顧客の環境は業界で認められた標準に基づいており、これらの標準を満たすソリューションが必要です。
* セキュリティ要件では、自動化ソフトウェアとターゲット デバイス間の SSH や TLS などの安全なトランスポート メカニズムの使用が義務付けられています。
* ソリューションは、人間が読める言語を使用して実装され、XML または JSON でデータをフォーマットする機能を提供する必要があります。
これらの要件を満たすにはどのソリューションを使用する必要がありますか?
A. アンシブル
B. SNMP
C. REST API
D. NETCONF
Answer: D

QUESTION NO: 9



展示を参照してください。エンジニアが PC と DHCP サーバー間の Wireshark パケット フローを分析します。パケット フローでは何が発生しますか?

A. PCはIPアドレスを要求するエニーキャストを送信します

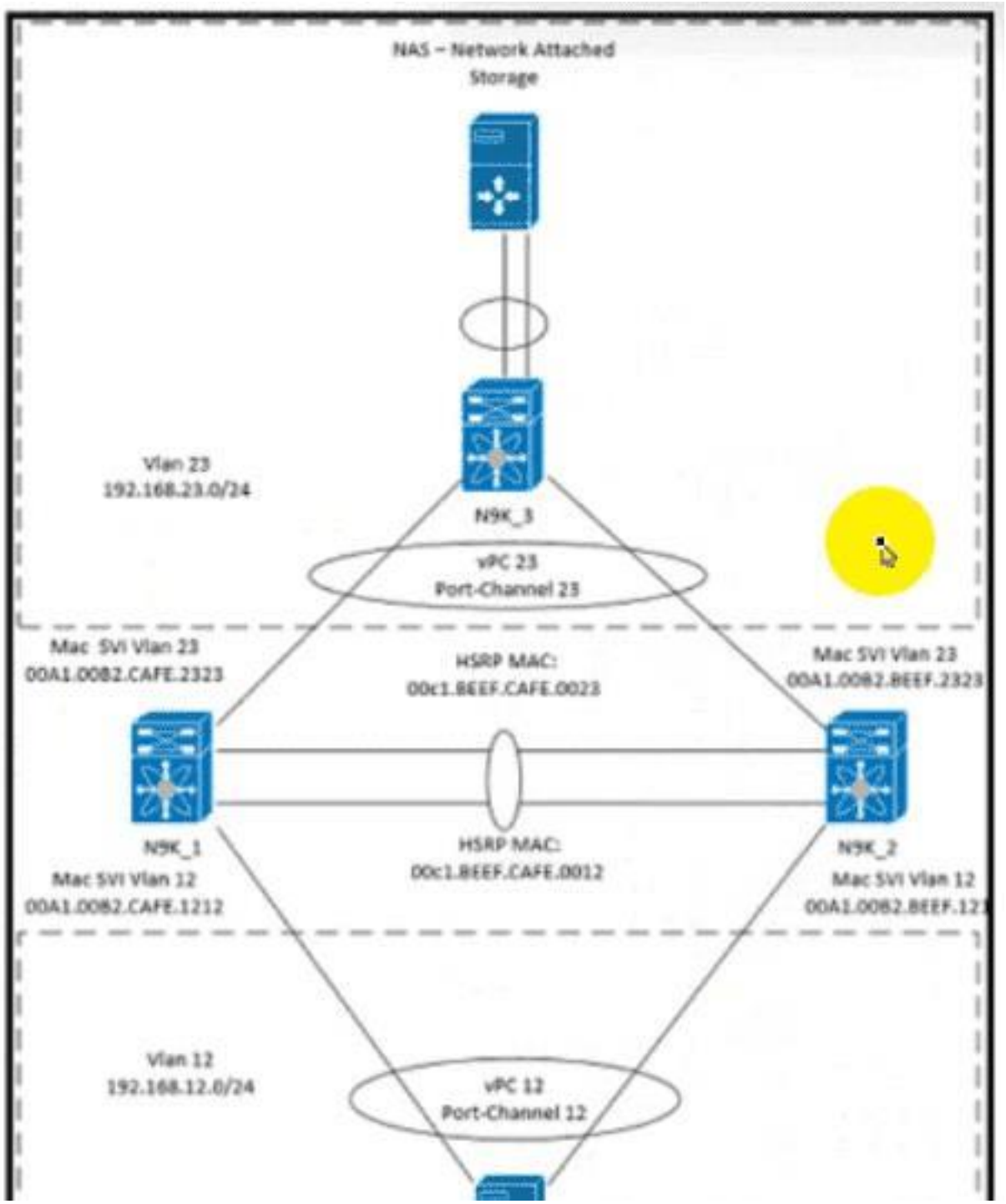
B. PCはDHCPサーバーからIPアドレス10 53 58.3を受け取ります。

C. PC は IP アドレスを要求するブロードキャストを送信します。

D. DHCPサーバーが利用できないため、PCはIPアドレスを0 0 0.0に設定します。

Answer: A

QUESTION NO: 10



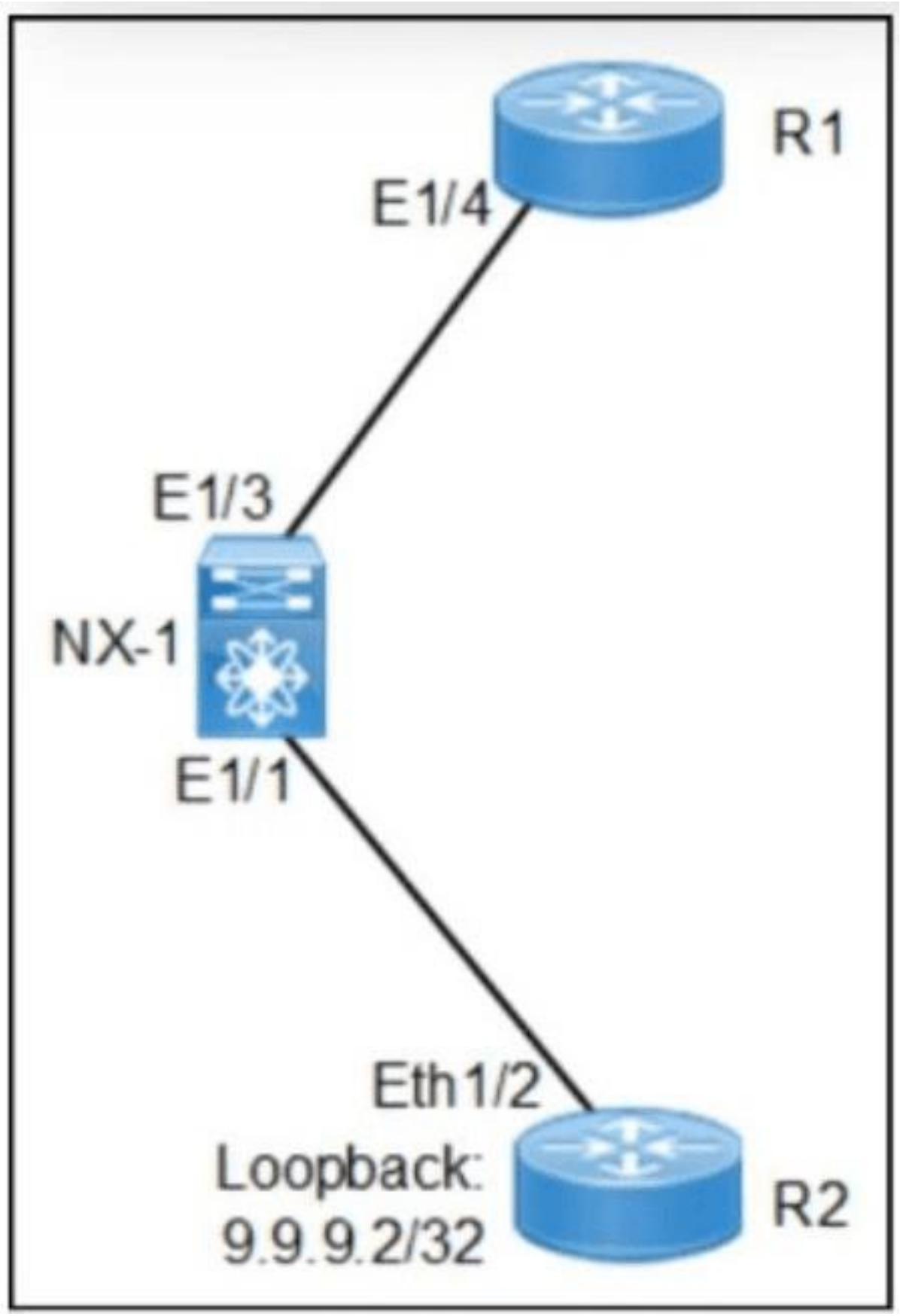
図を参照してください。シスコのデータセンター環境はvPCを使用して実装されています。Webサーバは、VLAN 23のHSRP MACアドレスではなく、SVI MACアドレスをレイヤ2ヘッダーとして使用して応答します。この動作により、vPCループ防止メカニズムにより、Cisco Nexus 9000シリーズスイッチでパケットがドロップされます。vPC機能の要件は、HSRPのMACアドレスがVLAN 23のレイヤ2ヘッダーで使用されていない場合でも、N9K_1とN9K_2がNASサーバとWebサーバ間のトラフィックを転送できるようにすることです。この目標を達成するには、どの機能を使用する必要がありますか？

A. ピアゲートウェイ

B. ARP同期

C. L3ピアルータ
D. オブジェクト追跡
Answer: A

QUESTION NO: 11



図を参照してください。エンジニアは、ルーティングテーブルに存在し、送信元IPアドレスが9.9.9.2/32で、インターフェースEth
1/1経由で到達可能なパケットのみを受け入れるようにNX-

Iを設定する必要があります。これらの要件を満たすには、ip verify unicast sourceコマンドのどの属性が必要ですか？

A. Elh1/2をrxキーワードでインターレースする
B. allow-default キーワードを指定したインターフェース Eth1/2
C. allow-default キーワードを指定したインターフェース Eth1/1
D. rxキーワードを持つインターフェースEth1/1
Answer: D

QUESTION NO: 12
この出力にはどのデータ交換形式が提示されますか?


```
{
  "totalCount": "1",
  "imdata": [
    "fabricNode": {
      "attributes": {
        "address": "10.0.40.65",
        "apicType": "apic",
        "dn": "topology/pod-1/node-201",
        "id": "201",
        "lastStateModTs": "2020-09-07T10:20:57.236+00:00",
        "modTs": "2020-09-07T10:21:18.912+00:00",
        "model": "N9K-C9336PQ",
        "monPolDn": "uni/fabric/monfab-default",
        "role": "spine",
        "serial": "FDO39106329J",
        "uid": "0",
        "vendor": "Cisco Systems, Inc",
      }
    }
  ]
}
```


A. XML
B. YAML
C. JSON
D. CSS
Answer: C

QUESTION NO: 13
同社はデータセンターセグメントの一部として、Cisco Nexus 7706シリーズスイッチ2台を運用しています。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/書き込みアクセスを制限されています。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を設定する必要があります。これらの要件を満たすには、どのような一連のアクショ

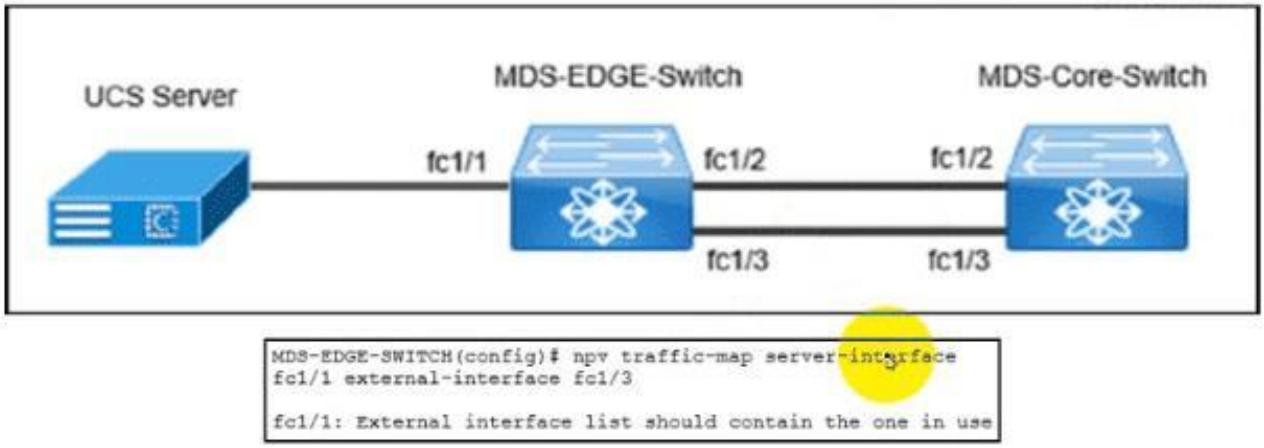
ンを実行する必要がありますか？
A. 1. ユーザー定義ロールを作成し、必要な権限を追加します。
2. ユーザーにロールを割り当てます。
B. 1. VDC 管理者ロールに必要な権限を追加します。
2. アクティブ ユーザー データベースへの変更をコミットします。
C. 1. ネットワーク オペレータ ロールを変更し、必要な権限を追加します。
2. ユーザーに VDC オペレーターのロールを割り当てます。
D. 1. ユーザーにネットワーク管理者ロールを割り当てます。
2. スイッチのロールをアクティブ ユーザー データベースにコミットします。
Answer: A

QUESTION NO: 14
エンジニアは複数のCisco Nexus 5600シリーズスイッチにVSAN 10を実装しており、ファブリック全体でフルゾーンセットとアクティブゾーンセットが同一であることを確認する必要があります。この要件を満たすには、どのような構成を実装する必要がありますか？
A. スイッチ(config)# ゾーンセット配布 vsan 10
B. switch(config)#zoneset activate name ZONE10 vsan 10
C. switch(conftg)# ゾーンセットを配布する完全なVSAN 10
D. switch(config)# ゾーン属性グループ名 ATTR1 vsan 10
Answer: B

QUESTION NO: 15
ある企業が、自社サービスの一部をクラウドに移行する計画を立てています。同社は、基盤となるクラウドインフラストラクチャの管理や制御は行いません。また、アプリケーションの展開とアプリケーションホスティング環境の構成設定についても、自社で管理したいと考えています。これらの要件を満たすクラウドサービスモデルはどれでしょうか？
A. サービスとしてのプラットフォーム
B. サービスとしての機能
C. サービスとしてのインフラストラクチャ
D. サービスとしてのソフトウェア
Answer: A

QUESTION NO: 16
Cisco UCS 上の QoS ポリシーは、次の要件を満たす必要があります。
* ノードロップクラスを設定する必要があります
* ジャンボ フレームは断片化なしで有効にする必要があります。
これらの条件を満たすには、どの構成を実装する必要がありますか?
A. Platinum システム クラスを設定し、MTU 値を 9100 バイトに指定します。
B. スロードレインタイマーを設定し、MTU値を9100バイトに指定します。
C. フロー制御ポリシーを作成し、MTU値を9000バイトに指定します。
D. QoSシステムクラスを作成し、MTU値を9216バイトに指定します。
Answer: D

QUESTION NO: 17



図を参照してください。MDS-EDGE-SwitchとMDS-Core-SwitchはNPVおよびNPIV機能を使用して設定されています。Cisco UCSからのFLOGIは、MDS-Core-Switchのインターフェースfc1/2で受信されます。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に移動しようとしました。
/3 ですが、試行は失敗しました。どのアクションセットで構成が完了しますか？

A. MDS-EDGE-Switch の NPV 機能を無効にします。
NPV 機能を再度有効にします。
インターフェイス fc1/1 を無効にします。

B. MDS-EDGE-Switch の NPIV 機能を無効にします。
NPIV 機能を再度有効にします。
インターフェイス fc1/3 を無効にします。

C. MDS-EDGE-Switch の fc1/1 をシャットダウンします。
コマンドを再度適用します。
インターフェイス fc1/1 を有効にします。

D. MDS-EDGE-Switch の fc1/3 をシャットダウンします。
コマンドを再度適用します。
インターフェイス fc1/3 を有効にします。

Answer: C

QUESTION NO: 18

どのファイル サービス プロトコルを使用すると、ファイルがクライアントにローカルにマップされて表示され、NAS の分散ファイル システム標準としても機能するリモート Linux ベースのストレージ リポジトリで表示、保存、および更新機能が提供されますか?

A. NFS

B. FTP

C. iSCSI

D. CIFS

Answer: D

QUESTION NO: 19
複数のブロードキャスト ドメイン間でイーサネット経由の RDMA 機能を有効にするテクノロジはどれですか。
A. RoCEv1
B. iWARP
C. NVMe-oF
D. RoCEv2
Answer: D

QUESTION NO: 20

```
CN=CiscoXYPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoPair
distinguishedName: CN=CiscoXYPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoXYPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
lDAPDisplayName: CiscoXYPair
name: CiscoXYPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

別紙を参照してください。ネットワークエンジニアは、以下の条件を満たすCisco UCSの認証ソリューションを設定する必要があります。
* すべての UCS ユーザー認証で 2 要素認証を有効にする必要があります。
* すべての AAA パケットは暗号化され、通信を確立するために TCP ポート 49 を使用する必要があります。
これらの要件が必要なアクション セットはどれですか?

Create the LDAP provider.
Change the LDAP group rule in an LDAP provider.

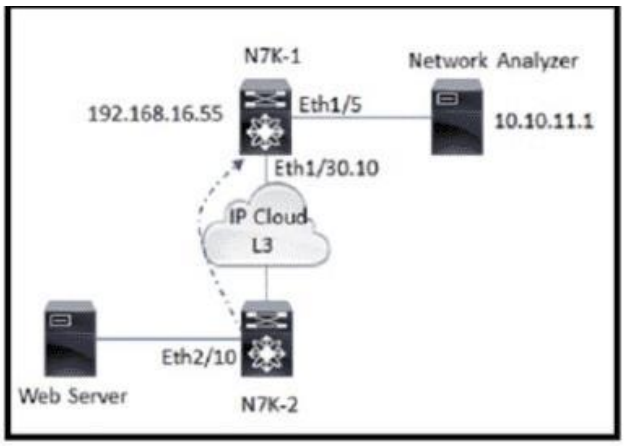
Create the RADIUS group mapping.
Change the RADIUS group rule in a RADIUS provider.

Remove the LDAP provider.
Create a TACACS+ provider in user management.

Delete the LDAP group mapping.
Create a RADIUS provider in user management.

A. オプションA
B. オプションB
C. オプションC
D. オプションD
Answer: C

QUESTION NO: 21




```
! ERSPAN Source Configuration
N7k-2(config)# monitor session 1 type erspan-source
N7k-2(config-erspan-src)# erspan-id 100
N7k-2(config-erspan-src)# vrf default
N7k-2(config-erspan-src)# destination ip 192.168.16.55
N7k-2(config-erspan-src)# source interface ethernet 2/10
N7k-2(config-erspan-src)# no shut
N7k-2(config-erspan-src)# exit
N7k-2(config)# monitor erspan origin ip-address 192.168.16.10 global
```

図を参照してください。エンジニアは、N7K-
2に接続されたWebサーバのトラフィックをミラーリングするためにERSPAN設定を実装し

ています。トラフィックをネットワークアナライザに転送するには、N7K-1にどのERSPAN設定を適用する必要がありますか？

○ monitor session 1 type erspan-destination
source vlan 10
destination interface ethernet 1/5
erspan-id 100
vrf default
no shut

○ monitor session 1 type erspan-destination
source ip 192.168.16.55
destination interface ethernet 1/5
erspan-id 100
vrf default
no shut

○ monitor session 1 type erspan-destination
source interface ethernet 1/30
destination ip 10.10.11.1
erspan-id 100
vrf default
no shut

○ monitor session 1 type erspan-destination
source interface ethernet 1/30.10
destination interface ethernet 1/30
erspan-id 100
vrf default
no shut

A. オプションA
B. オプションB
C. オプションC
D. オプションD
Answer: B

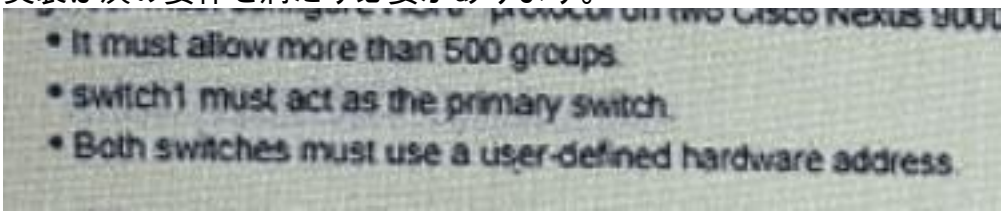
QUESTION NO: 22
Cisco UCS Manager のサービス
プロファイルは、次の要件に従って設定する必要があります。
* Cisco UCS Manager は、Cisco ACI ファブリック スイッチに接続する VMware ESXi ホスト上のインターフェイスを識別する必要があります。
* vNIC は、輻輳が発生した場合のトラフィック管理をサポートする必要があります。
これらの要件を満たすポリシーは 2 つありますか? (2 つ選択してください。)
A. vNIC/vHBAの配置
B. ネットワーク制御
C. シリアルオーバーLAN
D. LAN接続

E. QoS

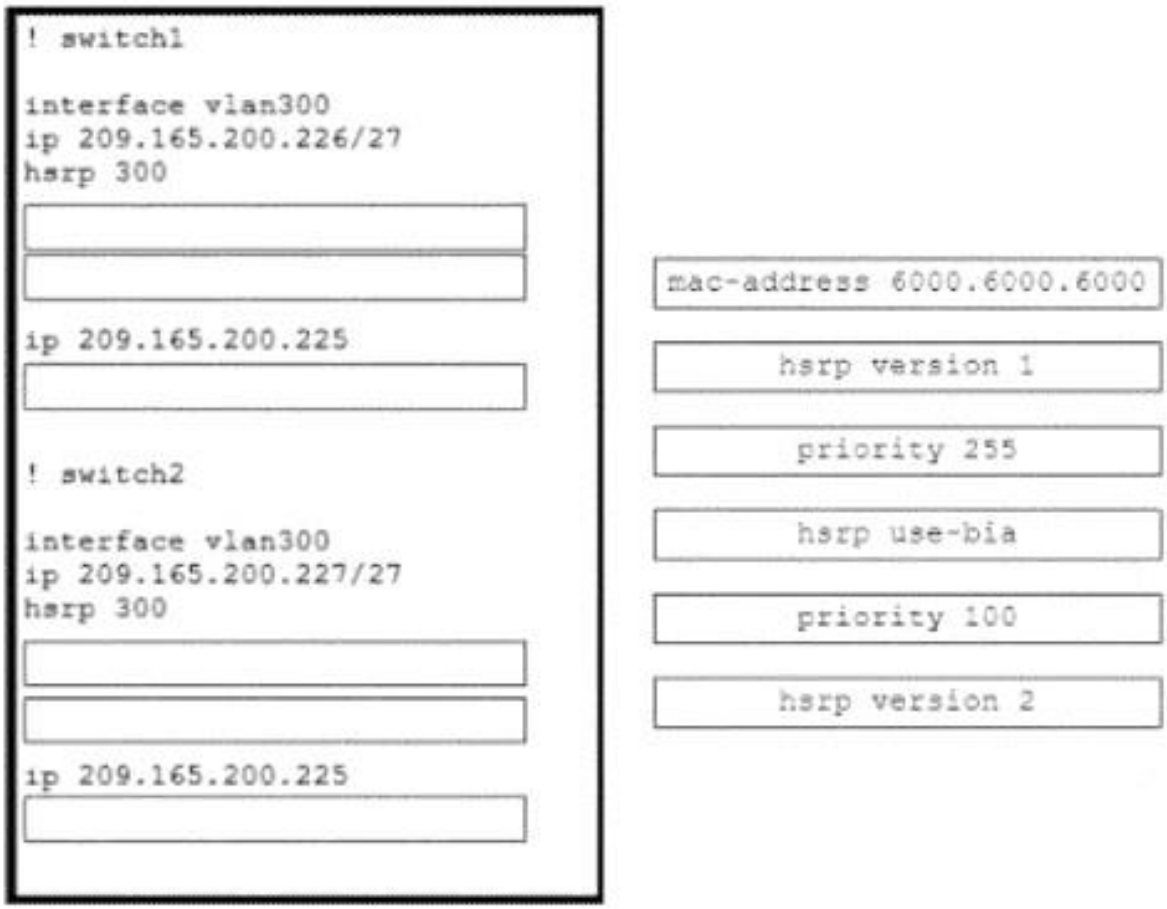
Answer: A D

QUESTION NO: 23

エンジニアは、仮想ポート チャネルを実行している 2 つの 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 実装は次の要件を満たす必要があります。

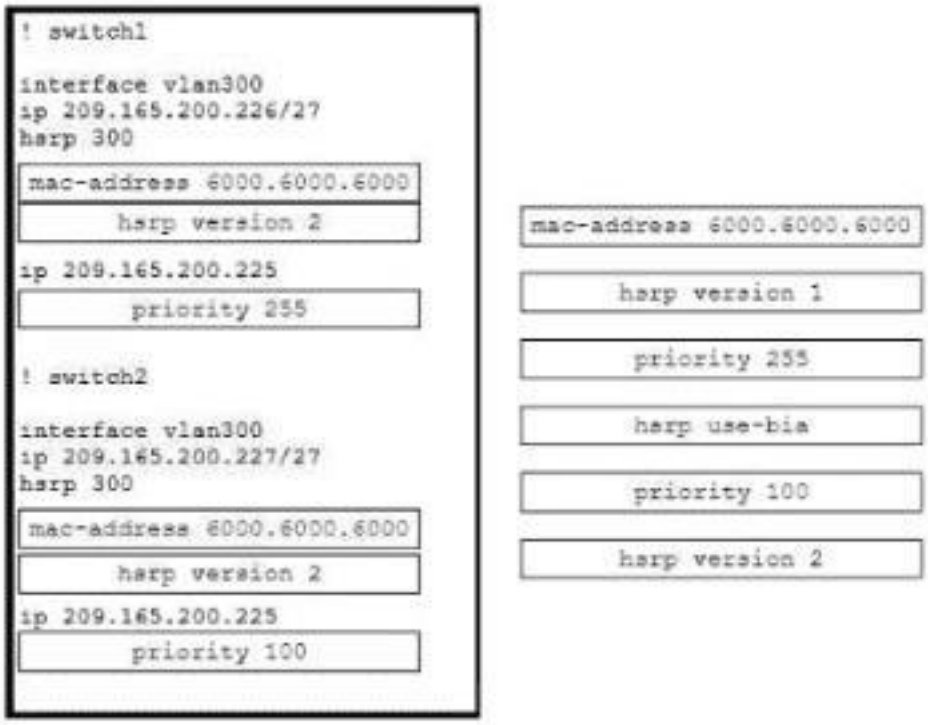


右側のコマンドをドラッグ & ドロップして、左側のHSRPの設定を完了します。コマンドは複数回使用されます。すべてのコマンドが使用されるわけではありません。



Answer:

Explanation:



QUESTION NO: 24

エンジニアは、災害復旧のために Cisco UCS
システムの構成をバックアップする必要があります。バックアップには、サーバーに展開されたサービス
プロファイルと、関連するすべての設定が含まれている必要があります。また、パスワードやその他の機密情報を保護するために、バックアップ
ファイルを暗号化する必要があります。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. 完全な状態

B. すべての構成

C. システム構成

D. 論理構成

Answer: A

QUESTION NO: 25

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 スイッチ設定は次の要件を満たす必要があります。
*スイッチは、競合があっても VSAN A ポート セキュリティ
データベースを開始する必要があります。
*新しいデバイスは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状態でファブリック全体に適用する必要があります。
どの構成セットがこれらの要件を満たしていますか?

A. ポートセキュリティをアクティブ化、VSAN
4を強制、ポートセキュリティを自動学習、VSAN
4ポートセキュリティを配布、ポートセキュリティをコミット

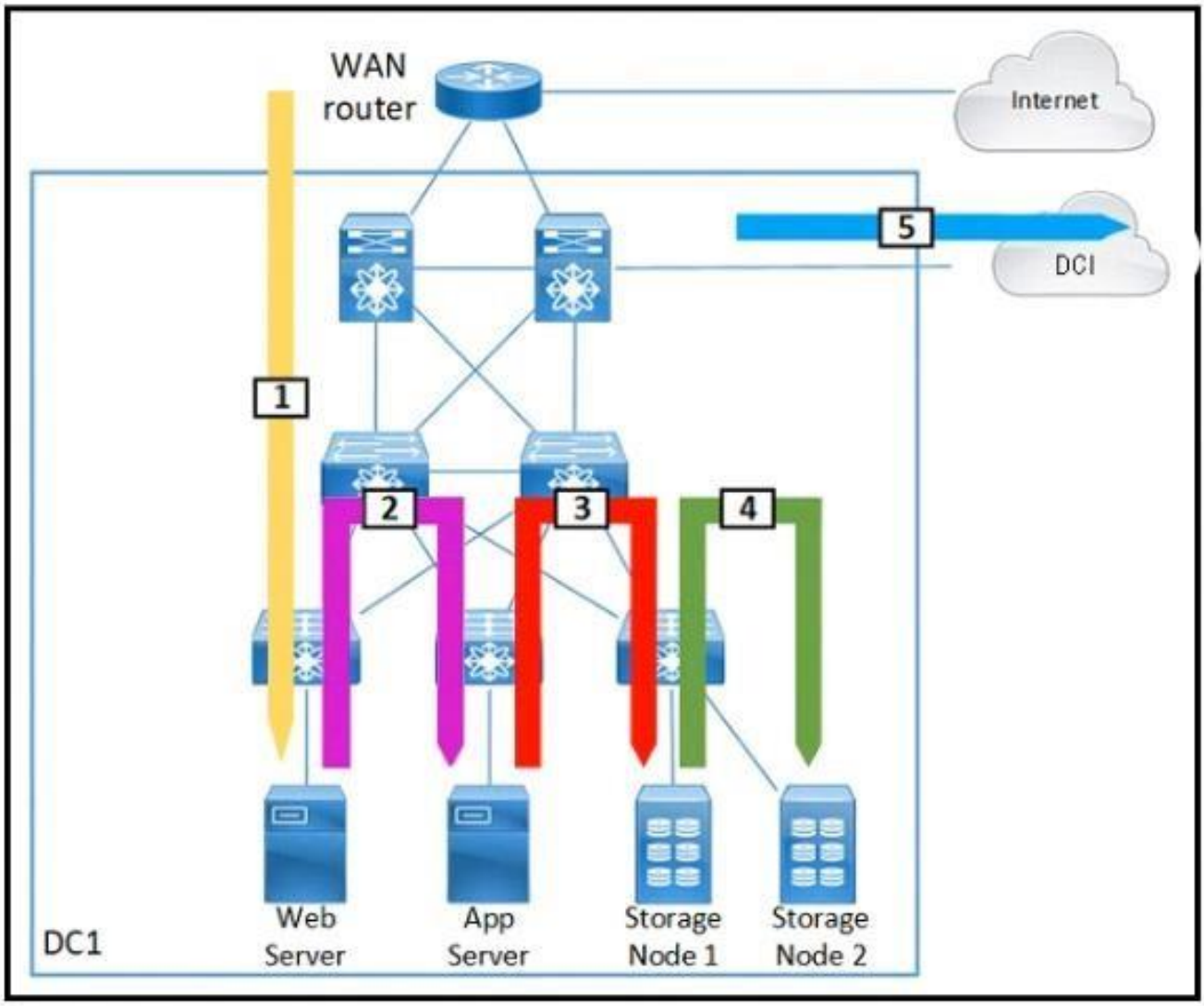
B. ポートセキュリティをアクティブ化し、VSAN 4
を強制的にポートセキュリティを自動学習し、VSAN 4
をポートセキュリティで配布し、ポートセキュリティをコミットします。VSAN 4

C. ポートセキュリティを有効化 vsan 4
ポートセキュリティの自動学習なし、VSAN 4
ポートセキュリティの割り当て、ポートセキュリティのコミット、VSAN 4

D. ポートセキュリティのアクティブ化、VSAN 4 ポートセキュリティの手動学習、VSAN 4
ポートセキュリティの割り当て、ポートセキュリティのコミット

Answer: B

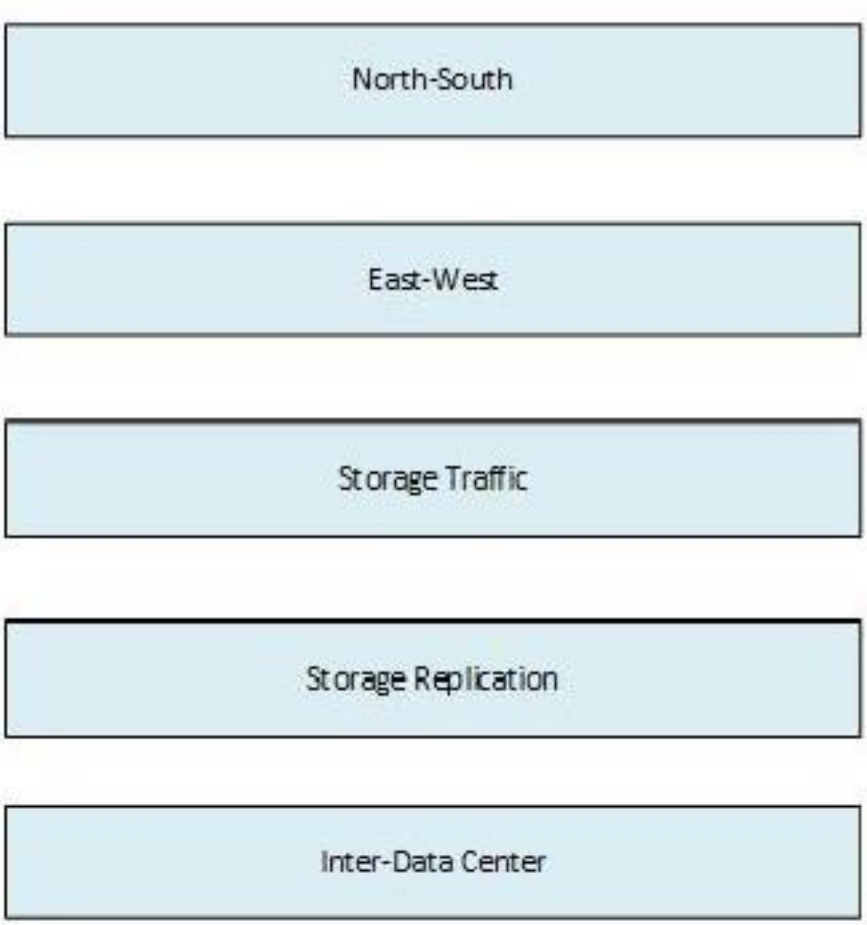
QUESTION NO: 26



左側の各トラフィックフロータイプを右側の対応する番号にドラッグアンドドロップします。すべてのトラフィックフロータイプが使用されるわけではありません。

Answer:

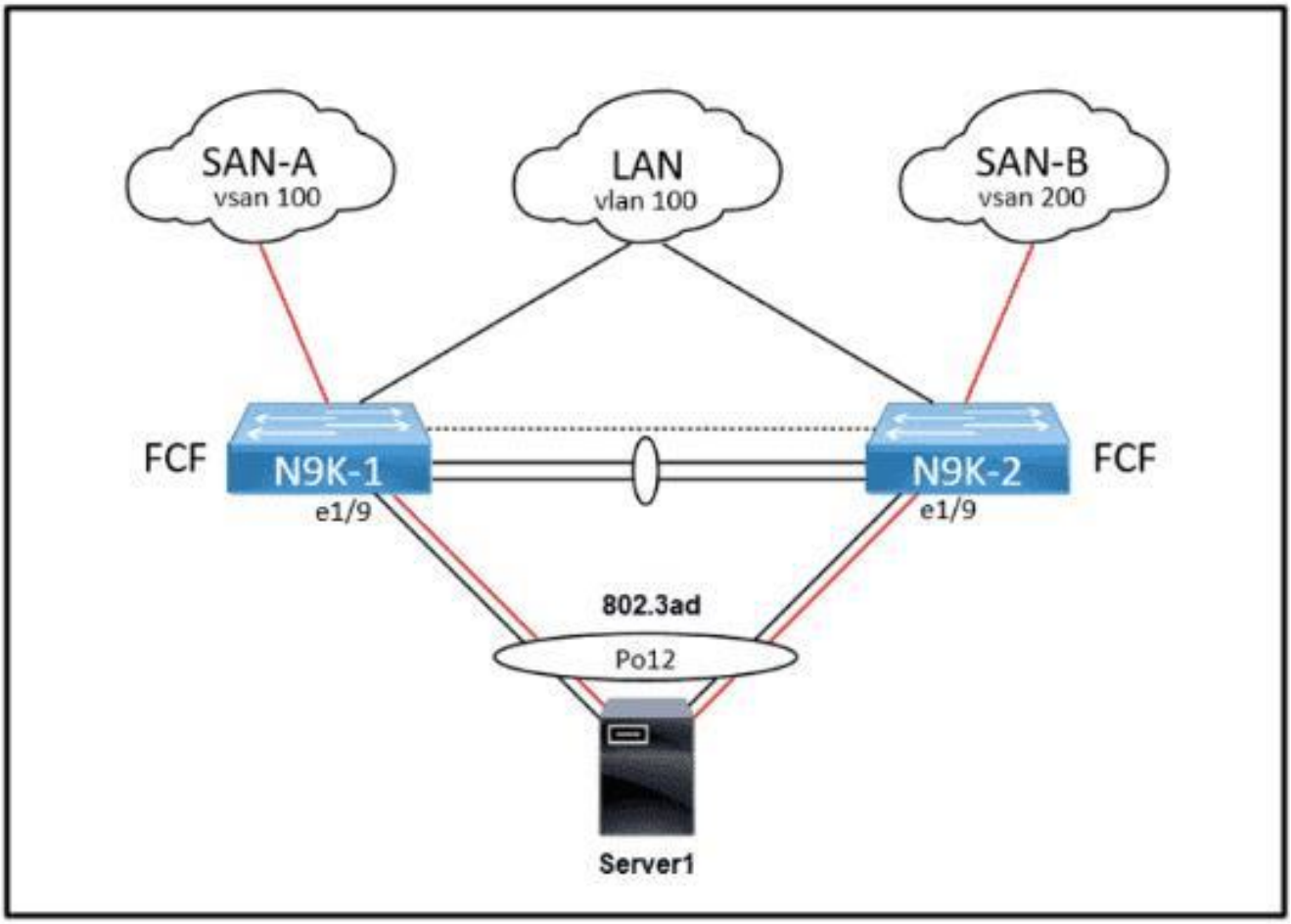
Explanation:



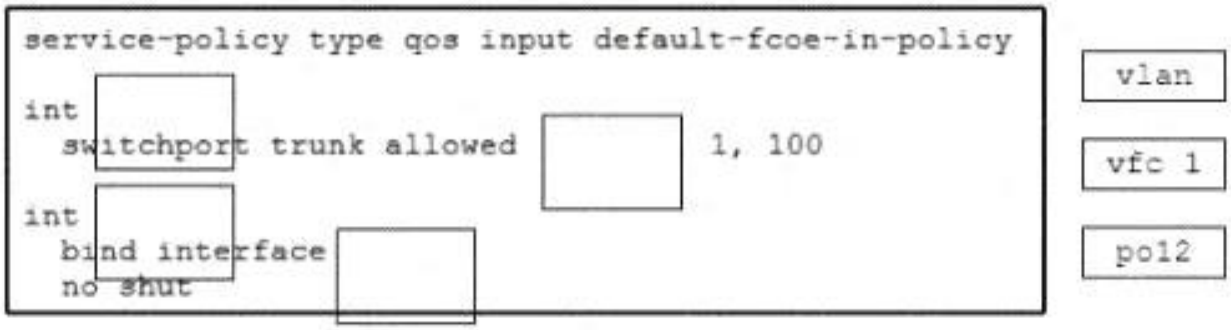
QUESTION NO: 27
Cisco Nexusシリーズスイッチ上のCisco
TACACS+は、デバイスへのアクセスを試みるすべてのユーザーを認証し、TACACS+サーバーが利用できなくなった場合はローカルアカウントにフェイルオーバーする必要があります。これらの目的を達成するコマンドはどれですか？
A. aaa 認証ログインデフォルトフォールバックエラーローカル
B. aaa 認証ログインデフォルトグループ ISE ローカル
C. aaa 認証ログイン デフォルト ローカル
D. aaa 認証ログインコンソールグループローカル
Answer: B
Explanation:
Option B is correct because on Cisco Nexus NX-OS, the command aaa authentication login default group < server-group > local creates the default login authentication method list and tells the switch to try the named AAA server group first, then fall back to the local user database if the AAA servers are unreachable or do not respond. Cisco's NX-OS AAA documentation states that the default login method list is used for user logins, and that the group keyword points authentication to a configured TACACS+ or RADIUS server group. It also notes that local authentication is the fallback method unless that behavior is explicitly disabled. (Cisco) The key reason the answer is B is the syntax: group ISE local means "authenticate with the TACACS+ server group named ISE first, then use local if the server is unavailable." Option C uses only local authentication, so it does not use TACACS+ at all. Option D applies to console login configuration and is not the correct default user-login

command. Option A is incorrect syntax for enabling this behavior; Cisco documents fallback error local as a behavior that is already present by default and can be disabled with the no form. (Cisco)

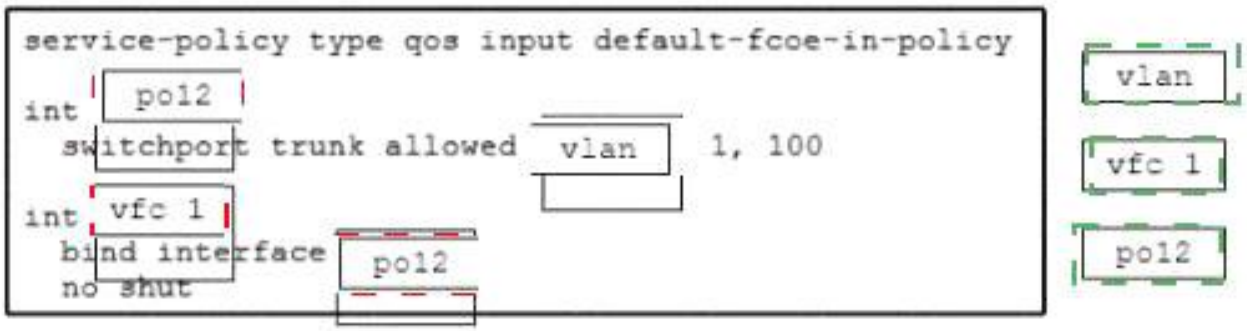
QUESTION NO: 28



図を参照してください。管理者は、Server1とCisco Nexus 9000シリーズスイッチのペア間のユニファイド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部分にドラッグアンドドロップして、N9K-1構成を完了します。スニペットは複数回使用されます。



Answer:



Explanation:
Po12
Vlan
Vfc1
Po12

QUESTION NO: 29
エンジニアがファブリックインターコネクトのファームウェアを更新し、アクティブ化しましたが、エンドポイントが新しいファームウェアイメージから起動してしまいます。この場合、どのような問題が発生すると予想されますか？
A. システムはデフォルトでGOLDファームウェアイメージを起動します。
B. システムはデフォルトでバックアップイメージのバージョンを使用します
C. システムはデフォルトでkickstariイメージを起動します
D. システムはデフォルトでGOLDファームウェアイメージを使用します
Answer: B

QUESTION NO: 30
展示品を参照してください。

```
mds01# sh run interface port-channel 2

interface interface port-channel 2
  switchport mode E
  switchport rate-mode dedicated
  channel mode active

mds01# sh run interface fc1/4-5

interface fc1/4
  switchport mode E
  switchport speed 4000
  switchport rate-mode dedicated
  switchport trunk mode on
  channel-group 2
  no shut

interface fc1/5
  switchport mode E
  switchport speed 4000
  switchport rate-mode dedicated
  switchport trunk mode on
  channel-group 2
  no shut
```

エンジニアはポートチャネルを使用してCisco MDSシリーズスイッチをCisco UCSドメインに接続する必要がありますが、リンクがアクティブ化されません。インターフェイスをアクティブ化するコマンドはどれですか？

A. スイッチポート速度 8000

B. スイッチポートトランクモードオフ

C. スイッチポート レートモード 共有

D. スイッチポートモード F

Answer: A

QUESTION NO: 31

図「監視デバイスにトラフィックを送信する監視セッションの構成を完了するには、どのポート タイプを使用する必要がありますか?」を参照してください。

A. アプライアンスポートとしてEth1/8、アップリンクポートとしてEth1/4

B. モニターポートとしてEth1/8、アップリンクポートとしてEth1/4

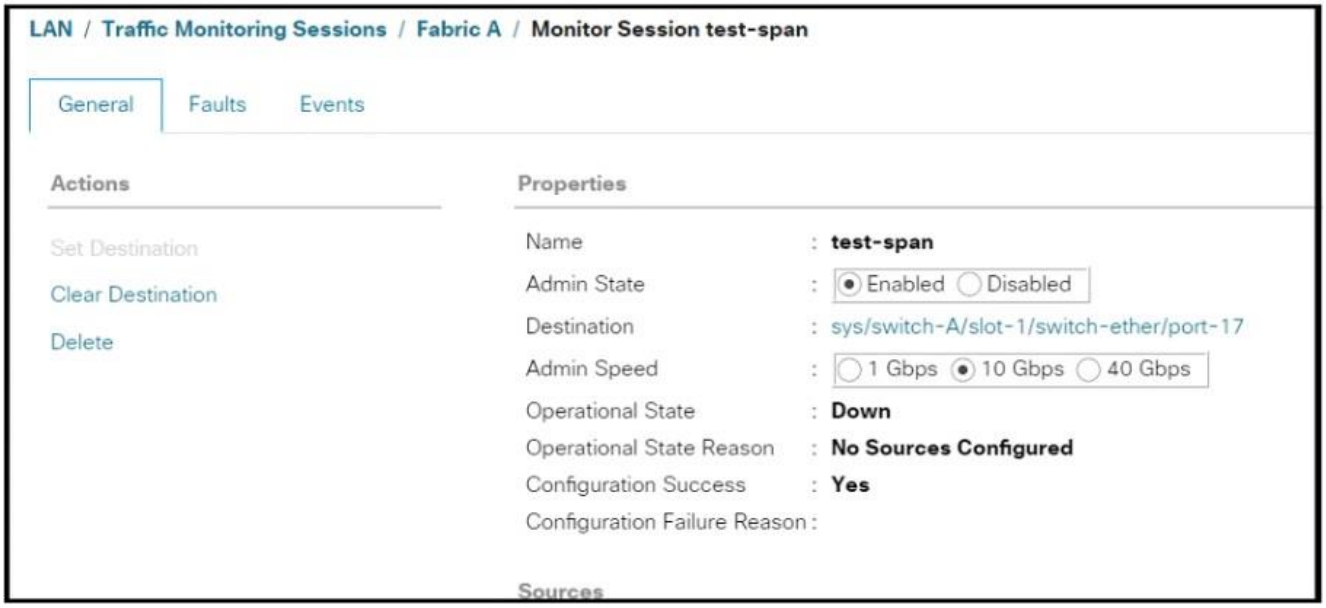
C. アップリンクポートとしてEth1/8、モニターポートとしてEth1/4

D. アップリンクポートとしてEth1/8、アプライアンスポートとしてEth1/4

Answer: D

QUESTION NO: 32

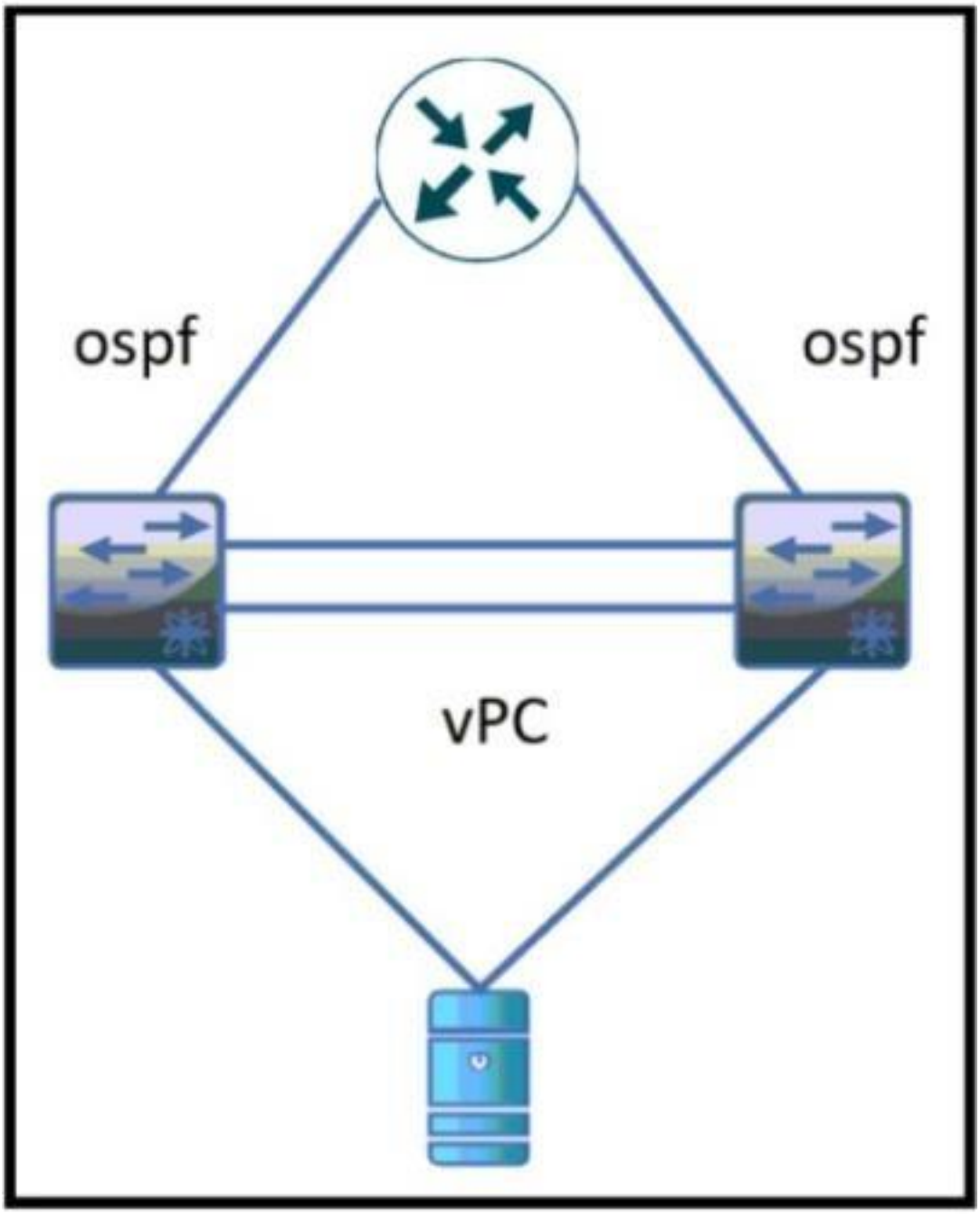
展示品を参照してください。



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

ソースを設定する必要がありますか？
A. このサーバに対応するサービス プロファイルのすべての 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. このサーバに対応するサービスプロファイルのすべてのvNIC
Answer: D

QUESTION NO: 33



図を参照してください。vPC ピア
スイッチのリロード中に、サーバとルータの間でパケット損失が発生します。今後のリロード中にこの動作を防ぐには、どのようなアクションを実行する必要がありますか?
A. Cisco Nexus ピアのルーティングされたアップリンク

ポートを孤立ポートとして設定します。
B. vPC 遅延復元タイマーを増やします。
C. OSPF hello および dead 間隔タイマーを減らします。
D. vPC ピア上の vPC ARP 同期を無効にします。
Answer: B

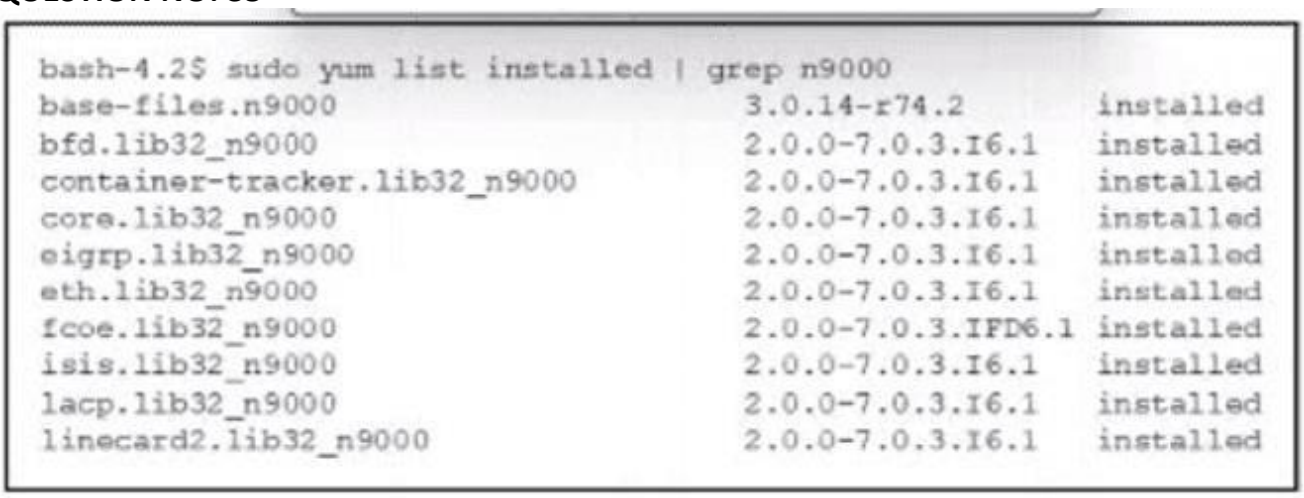
QUESTION NO: 34
展示資料を参照してください。

```
MDS# show role
Role: network-admin
  Description: Predefined network admin role
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
rule 5 permit show feature hardware
rule 4 permit show feature environment
rule 3 permit config feature ntp
rule 2 permit config feature ssh
rule 1 permit config feature tacacs+

Role: Custom-Role-B
  Description: Additional admin role
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
rule 6 permit config feature dpvm
rule 1 deny config feature tacacs+
```

Cisco MDS 9000 シリーズ スイッチは RBAC
で構成されています。デフォルトのロールはすべてのユーザーに適用されます。ユーザー A には Custom-Role-B ロールも割り当てられています。ユーザー A
はどの機能セットを構成する権限を持ちますか？
A. NTPSSHDPVM
B. SSHDPVMTACACS+NTP
C. DPVMNTPSSHhardware
D. hardwareenvironmentDPVM
Answer: B
Explanation:
The correct answer is B because Cisco MDS RBAC authorizes a user based on the union of all permitted commands across all assigned roles. In the exhibit, the default role network-admin permits configuration of NTP, SSH, and TACACS+, while the additional role Custom-Role-B permits configuration of DPVM and includes a deny entry for TACACS+. Cisco documentation for MDS RBAC explains that when a user belongs to multiple roles, the user can execute the combined set of commands permitted by those roles, and importantly, access takes priority over deny when there is a conflict across roles.
Applying that rule here, User A is allowed to configure:
* NTP (config feature ntp) from network-admin
* SSH (config feature ssh) from network-admin
* TACACS+ (config feature tacacs+) from network-admin
* DPVM (config feature dpvm) from Custom-Role-B

The deny for TACACS+ in Custom-Role-B does not remove access because another assigned role already permits it. Options containing hardware or environment are incorrect because those are show permissions, not configuration permissions.

QUESTION NO: 35



```
bash-4.2$ sudo yum list installed | grep n9000
base-files.n9000                    3.0.14-r74.2        installed
bfd.lib32_n9000                     2.0.0-7.0.3.I6.1    installed
container-tracker.lib32_n9000       2.0.0-7.0.3.I6.1    installed
core.lib32_n9000                    2.0.0-7.0.3.I6.1    installed
eigrp.lib32_n9000                   2.0.0-7.0.3.I6.1    installed
eth.lib32_n9000                     2.0.0-7.0.3.I6.1    installed
fcoe.lib32_n9000                    2.0.0-7.0.3.IFD6.1  installed
isis.lib32_n9000                    2.0.0-7.0.3.I6.1    installed
lacp.lib32_n9000                    2.0.0-7.0.3.I6.1    installed
linecard2.lib32_n9000               2.0.0-7.0.3.I6.1    installed
```

図を参照してください。RPM パッケージのリストは、Cisco Nexus 9000 シリーズ スイッチの Bash シェルにインストールされています。スイッチに BGP 機能をインストールして有効にするには、どの操作を行う必要がありますか？

A. bash-4.2# feature bgp9K(config)# sudo yum -y install bgp

B. bash-4.2$ sudo yum -y install bgp9K(config)# feature bgp

C. bash-4.2$ feature bgpbash-4.2$ sudo yum -y install bgp

D. 9K(config)# sudo yum -y install bgp9K(config)# feature bgp

Answer: B

Explanation:

The correct answer is B because Cisco Nexus 9000 switches that support NX-OS with Linux Bash shell require a two-step process when a feature is delivered as an RPM package. First, the feature must be installed at the Linux level using the Bash shell and the yum package manager. This is done with the command:

sudo yum -y install bgp

This step installs the necessary binaries and dependencies for the BGP feature. After installation, the feature is not automatically active in NX-OS. The second step is to enable the feature within NX-OS CLI using:

feature bgp

This activates the control plane functionality and allows configuration of BGP on the switch. Option A is incorrect because it attempts to enable the feature before installing it. Option C is invalid because feature bgp cannot be executed in Bash mode. Option D is incorrect because yum commands must be executed in the Bash shell, not in NX-OS configuration mode. Thus, the correct workflow is install via Bash # enable via NX-OS CLI, which is exactly what option B describes.