VMware.3V0-23.25.v2026-06-13.q80

試験コード：	3V0-23.25
試験名称：	Advanced VMware Cloud Foundation 9.0 Storage
認証ベンダー：	VMware
無料問題の数：	80
バージョン：	v2026-06-13
ページの閲覧量：	103
問題集の閲覧量：	813

https://www.jpnshiken.com/shiken/VMware.3V0-23.25.v2026-06-13.q80.html

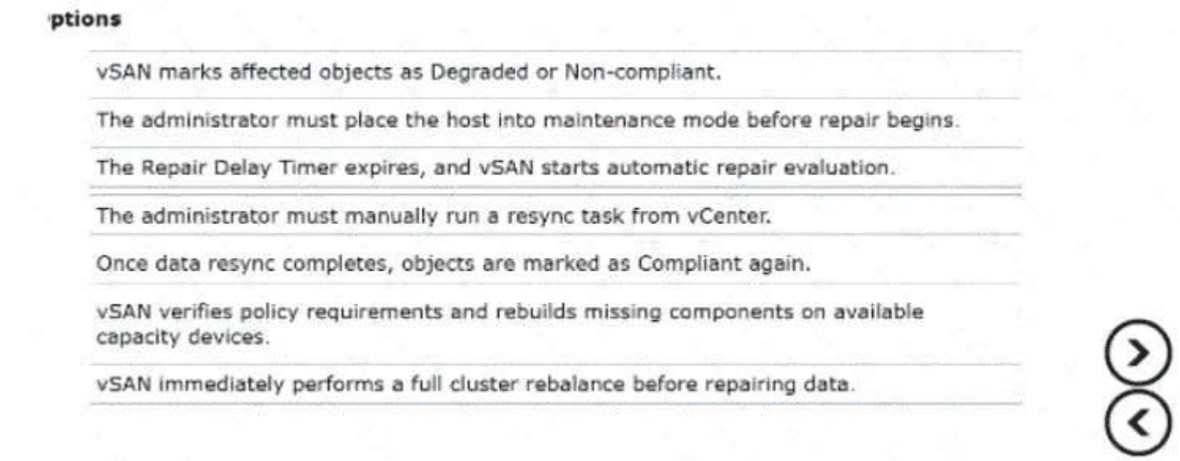
質問: **1**
最高技術責任者（CTO）が、壊滅的なシステム障害について調査を進めている。複数の重要なデータベース用ファーストクラスディスク（FCD）を搭載したTKGワーカーノードでデータ破損が発生した。
当該ノードは高負荷状態のホスト上で稼働しており、CPUサイクルを節約するため、標準のVMDKバックアップルーチン（VADP経由）は無効化されていた。ストレージチームは、低レベルAPIコマンドを使用してFCDの復元を試みた。
エンジニアはvim-cmdを使用してFCDの状態を検査します。
「」
[root@esx-08:~] vim-cmd vmsvc/get.tasklist
タスク: ReconcileFCD_Task
ステータス：失敗
エラー: "VStorageObjectNotFound"
[root@esx-08:~] vim-cmd vmsvc/device.diskaddexisting 20
/vmfs/volumes/vsan/fcd/88b1...
エラー: 「ディスク オブジェクトには CryptoKeyID が必要ですが、見つかりませんでした
現在のKMSプロバイダー。
「」
FCD独立性とvSAN暗号化の概念は、どのように相互作用してこの復元失敗を引き起こすのでしょうか？（該当するものをすべて選択してください。）
A. CNSボリュームは本質的に「自己暗号化ドライブ」（SED）を使用しており、FCDキーは物理的なNVMeファームウェアに保存され、KMSをバイパスします。
B. ファーストクラスディスク (FCD) は、ワーカーノード VM とは独立して、SPBM によって割り当てられた機能 (暗号化キー ID を含む) を保持します。
C. ハイパーバイザーは、一致する CryptoKeyID がないと vSAN オブジェクトを復号できないため、FCD をレスキュー VM または元のワーカー ノードにアタッチできません。
D. ESXi ホストがキー管理サーバー (KMS) への接続を失ったか、この FCD に関連付けられている特定のキー暗号化キー (KEK) がローテーションされて失われました。
E. 標準ストレージvMotionを使用してFCDを従来のVMDKに変換すると、暗号化が解除され、アクセスが復元されます。
正解: **(**正解を表示します**)**

質問: **2**
最高技術責任者（CTO）は、2ペタバイトもの膨大な医療画像アーカイブをホストするVCF 9.0ワークロードドメインのストレージオプションを評価している。このアーカイブにアクセスするアプリケーションは、最小限のコンピューティングリソース（例えば、標準的な16vCPUウェブサーバー4台）しか必要としない。
「」
【お客様のご要望】
容量：2,000 TB（2 PB）

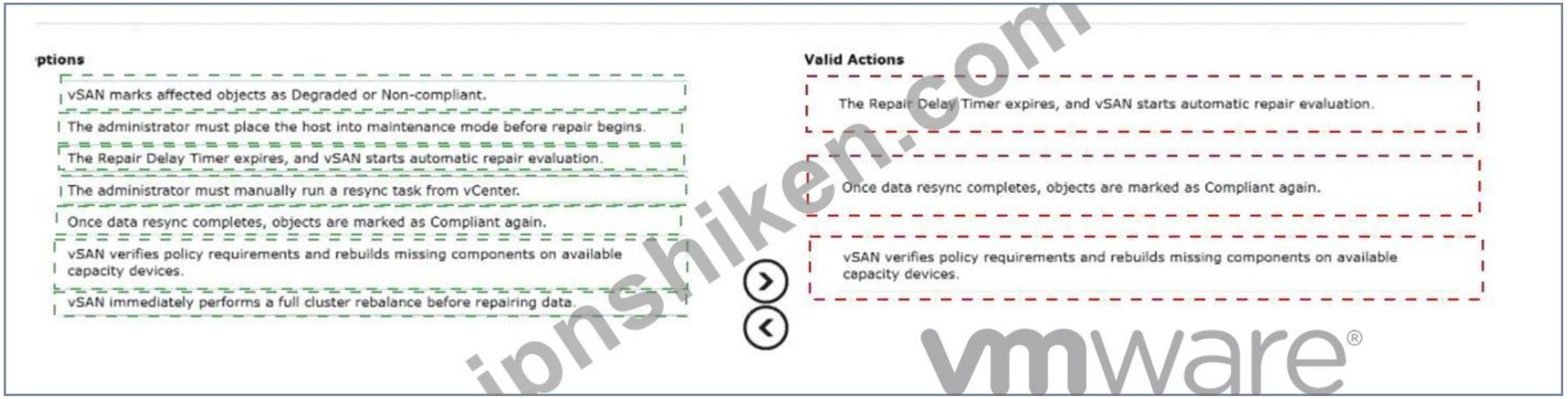
計算処理：合計64 vCPU（ピーク時）
コスト制約 :ソフトウェアライセンスの設備投資を最小限に抑える。
「」
この特定のユースケースにおいて、純粋なvSAN ESA HCIクラスタではなく、外部SAN/NASソリューションを選択することを正当化する記述はどれですか？
A. vSAN ESAには1ペタバイトの生容量というハードクラスタ制限があるため、技術的にこの医療アーカイブをホストすることは不可能です。
B. 外部NASは、小規模な3ノードESXiクラスタに接続しながら2PBのアーカイブをホストできますが、vSAN HCIでは、物理的なドライブベイを取得するためだけに、20台以上のフルライセンスの「コンピューティング負荷の高い」vSAN ReadyNodeを購入する必要があります。
C. VCFはHIPAA規制対象の医療ワークロードにvSANを使用することを明確に禁止しており、顧客には物理テープバックアップ統合を備えた外部アレイの使用を強制しています。
D. 医療画像処理にはオブジェクトベースのメタデータが必要ですが、従来のNFS NASシステムはそれをネイティブに提供しますが、vSANは厳密にはブロックのみのVMDKストレージを提供します。
正解: **(**正解を表示します**)**

質問: **3**
コンプライアンス監査担当者が、従来型の3層ファイバーチャネルSANを使用している組織のデータガバナンス機能を分析しています。この組織は、保存データの暗号化（DARE）と可変レプリケーション頻度を要求する厳格な規制を遵守する必要があります。
「」
SPBMポリシーシミュレーション：「コンプライアンス重視」
制約1：財務VM DKは暗号化されている必要があります。
制約2：非財務系のVM DKは暗号化してはならない（パフォーマンス上の理由から）。
制約3：財務VMは15分ごとに複製されなければならない。
制約4：非財務系の仮想マシンは24時間ごとに複製されなければならない。
「」
現在、すべての仮想マシンは、従来のFC LUNをバックエンドとする単一の50TB VMFS-6データストア上でホストされています。
従来のLUNアーキテクチャは、vSAN HCIアーキテクチャと比較して、これらのコンプライアンスポリシーの実装を本質的にどのように制限または複雑化しますか？（該当するものをすべて選択してください。）
A. 従来のSANレプリケーションはLUNレベルで動作します。15分ごとに財務VMをレプリケートすると、アレイは大量の非財務データも15分ごとにレプリケートする必要があり、WAN帯域幅が無駄になります。
B. VMFS-6 データストアは、物理的なファイバーチャネルスイッチがネイティブ暗号化オフロードを備えた第7世代にアップグレードされていない限り、AES-256 暗号化キーを本質的に拒否します。
C. vSAN HCI は、仮想マシン ディスク (VMDK) オブジェクト レベルでポリシーを適用することでこの問題を解決し、同じデータ ストア上に存在する 2 つの VM に対して異なる暗号化およびレプリケーション ルールを適用できるようにします。
D. 従来のアーキテクチャでこのコンプライアンスを実現するには、管理者は複数の小さな LUN (財務用と非財務用) を切り出す必要があり、データストアの乱立と空きスペースの無駄につながります。
E. 従来のアレイでは物理LUN全体が暗号化されるため、ストレージ管理者は財務VMを暗号化しながら、同じデータストア上の非財務VMを暗号化しないままにしておくことはできません。
正解: **A,C,D,E (**コメントを発表する**)**

質問: **4**
vSAN ESAクラスタにおいて、1台のホストが予期せず1時間以上オフラインになる。
vSANがオンラインに戻ると、障害発生中にパフォーマンスが低下した複数のオブジェクトについて、再構築とコンプライアンスの復元が必要になります。
左側のオプションリストから、自動復旧プロセスに適した3つのオプションをドラッグアンドドロップし、右側の有効なアクションに任意の順序で配置してください。（3つ選択してください。）



正解:



Explanation:

修復遅延タイマーが期限切れになると、vSANは自動修復評価を開始します。

データの再同期が完了すると、オブジェクトは再び準拠状態としてマークされます。

vSANはポリシー要件を確認し、利用可能な容量デバイス上で不足しているコンポーネントを再構築します。

ホストが予期せずオフラインになった場合、vSAN は欠落したコンポーネントを存在しないものとして扱い、再構築操作を開始する前に、構成された修復遅延タイマーが経過するまで待機します。これにより、ホストまたはデバイスがすぐに復旧した場合に不要な再同期が防止されます。このシナリオでは、ホストが 1 時間以上オフラインになっているため、修復遅延タイマーが期限切れとなり、vSAN は自動修復評価を開始します。vSAN は、割り当てられたストレージ ポリシー、利用可能な容量、および障害ドメインの配置要件を確認し、欠落したコンポーネントを利用可能な容量デバイスに安全に再構築できるかどうかを判断します。十分な容量と障害ドメインが存在する場合、vSAN は代替コンポーネントを作成し、再同期を開始します。再同期プロセスが完了し、影響を受けるオブジェクトが割り当てられたポリシーを再び満

たすと、オブジェクトは準拠としてマークされます。管理者は vCenter から再同期タスクを手動で実行する必要はなく、自動修復のためにホストをメンテナンス モードにする必要もありません。クラスタ全体の再バランスは、別の容量バランス操作であり、オブジェクト修復の前に必要ではありません。参照トピック: vSAN 修復遅延タイマー、オブジェクト準拠、再同期、ESA オブジェクト修復。

質問: **5**
SOCアナリストが、SDDC Manager経由で管理されているvSAN ESAクラスタにおけるデータ転送（DiT）暗号化に関するセキュリティイベントを観測した。
「」
[ログ抜粋: vmkernel.log - ESXiネットワークスタック]
2026-11-20T11:00:00Z INFO vsan-dom - DOMクライアントペイロードが圧縮されました
（比率4 :1）
2026-11-20T11:00:01Z INFO vsan-dit - ペイロードが暗号化されました。
2026-11-20T11:00:02Z INFO tcp_ip - vmk2 を介した送信。
「」
vSAN ESAのI/Oパイプラインのシーケンスは OSAと比べてどう違うのか、また、この特定のシーケンスがセキュリティとネットワークパフォーマンスの両方にとってなぜ重要なのか？（該当するものをすべて選択してください。）
A. 従来の OSA では、非圧縮データがネットワーク経由で送信され、ディスクに到達する直前のスタックの最下部 (LSOM) でのみ圧縮されました。
B. ESAでは、データは暗号化されてネットワーク経由で送信される前に、スタックの最上位（DOMクライアント）で圧縮されます。
C. ESAパイプラインシーケンスは、DOMクライアントが標準パリティビットを複製する必要があるため、OSAよりも4倍多くのネットワークトラフィックを生成します。
D. ESA は、ログ構造の名前空間がネットワークスニファに対してネイティブに読み取り不可能であるため、転送中のデータ暗号化を排除します。
E. パイプラインが最初にデータを暗号化した場合、暗号化されたデータは圧縮できない高エントロピーの暗号文で構成されているため、圧縮は失敗します。
正解: **(**正解を表示します**)**

質問: **6**
VCF SDDC Manager の自動容量アラートがトリガーされた後、SOC アナリストが対応にあたります。
午前2時。
「」
[SDDCマネージャー - ワークロードドメインしきい値アラート]
クラスター: WLD01-クラスター
vSAN使用率 :83%
ホスト再構築予備軍：侵害されました
アクション開始: プロアクティブな書き込みスロットリング
【アーキテクチャ図のスナップショット】
4ノード構成のvSAN OSAオールフラッシュクラスタ。
物理ディスクに障害は発生していません。有効なメンテナンスウィンドウもありません。
「」
クラスタトポロジーのサイズと「ホスト再構築リザーブ」ロジックの相互作用は、この容量超過をどのように説明し、運用上の影響はどのようなものですか？（該当するものをすべて選択してください。）
A. プロアクティブ書き込みスロットリングは、クラスターが100%に達して完全にロックアップするのを防ぐために、受信VM書き込み要求に意図的に極端な遅延（バックプレッシャー）を導入します。
B. データを削除せずにこの問題を解決するには、アナリストは SDDC Manager で「スケールアウト」ワークフローを開始して 5 番目のホストを追加し、ホスト再構築リザーブを 25% から 20% に再計算する必要があります。
C. 小規模な4ノードクラスタでは、ホスト再構築リザーブは、ホストがダウンした場合にFTT=1データを再構築できるように、総容量の正確に25%（ホスト1台分に相当）を確保する必要があります。

D. リビルドリザーブのロジックは、8ノードを超えるクラスターにのみ適用されます。このアラートは、SDDC Managerプロファイルの設定ミスによって生成された誤検出です。
E. 83% + 25% の予備容量が 100% を超えるため、クラスターはホスト障害を許容できる容量が数学的に不足し、ドライブに 17% の絶対空き容量があるにもかかわらず、侵害アラートがトリガーされます。
正解: **A,B,C,E (**コメントを発表する**)**

質問: **7**
運用エンジニアがvSAN ESAクラスタのトラブルシューティングを行っています。Host-03の再起動後、
50 TBの仮想マシンオブジェクトが「アクセス不可」状態になりました。
DOMおよびLSOMコンポーネントは存在するが、メタデータが同期されていないように見える。エンジニアはRuby vSphere Console（RVC）を使用してオブジェクト階層を照会する。
「」
[RVC出力: vsan.object_info ~cluster 554350...]
DOMオブジェクト: 554350... (状態: アクセス不可)
- コンポーネント 1: UUID abc... (ホスト: Host-01、DOM 所有者: Active)
- コンポーネント 2: UUID 定義... (ホスト: Host-02、DOM 所有者: Active)
- コンポーネント 3: UUID ghi... (ホスト: Host-03、LSOM 状態: STALE)
「」
ESAでは、ホストの再起動時にデータの整合性を検証するために、DOMとLSOM間のアーキテクチャ上のハンドシェイクはどのように機能するのでしょうか？また、なぜこのオブジェクトにアクセスできなくなるのでしょうか？（該当するものをすべて選択してください。）
A. コンピューティングホスト上のDOMクライアントは、自動的にLSOMバイパスを実行して、Host-01およびHost-02上の物理NVMeドライブから直接読み取ります。
B. 復旧には、DOM がデルタ再同期を実行し、アクティブ コンポーネントから変更されたブロックのみを Host-03 上の STALE コンポーネントの LSOM にプッシュする必要があります。
C. DOMがコンポーネントを再インデックスする前に、Host-03上のLSOMはESXiハイパーバイザーカーネルと明示的に通信してNVMeドライブを再フォーマットする必要があります。
D. Host-03 には古いコンポーネントが含まれているため、DOM はその投票権を拒否します。オブジェクトはクォーラムを失い (3 票中 2 票のみ有効)、古いデータの読み取りを防ぐために「アクセス不可」状態になります。
E. DOMオーナーはオブジェクト構成シーケンス番号（CSN）を追跡します。ホスト03が再起動し、DOM更新世代を逃したため、ローカルLSOMコンポーネントには古い（STALE）CSNが保持されています。
正解: **(**正解を表示します**)**

質問: **8**
インフラストラクチャマネージャが、完全に利用されているvSAN ESAデータベースクラスタに対してディープリキー処理を開始します。
5分以内に、アプリケーション所有者から深刻なトランザクションタイムアウトが発生したとの報告が寄せられた。
「」
[vSANパフォーマンスビュー - クラスタ集約]
指標 :CPU使用率 （40%から95%に上昇）
メトリック :ネットワーク遅延 （vSANトラフィック :1ms未満）
メトリック: LSOM輻輳 (ssd-congestion: 正常)
指標 :DOMレイテンシ（高）
「」
ディープリキー処理中に発生するこの特定のパフォーマンス低下を正確に診断している記述はどれですか？ （2つ選択してください。）
A. 高いDOMレイテンシと通常のLSOM輻輳の組み合わせは、物理的なNVMeドライブがボトルネックではないことを証明しています。ESXi CPUがリソース不足になり、I/O処理パイプラインが遅延しています。
B. ディープリキー操作では、vSAN 分散オブジェクトマネージャ (DOM) が明示的に無効になり、ローカルのゲスト OS が暗号化のオーバーヘッドを処理することになります。
C. CPU使用率が95%になるのは、ESXiハイパーバイザーがCPUサイクルを使用してソフトウェアでAES-256データストリームをアクティブに復号化および再暗号化しているためです。

D. CPU スパイクは、キー管理サーバー (KMS) のポーリング間隔によって生成された誤検出です。
E. ディープリキーイングは大量のバックグラウンドデータ移動を生成し、物理的な25GbEネットワークスイッチのバッファを飽和させており、これは1ms未満のレイテンシメトリックによって示されています。
正解: **A,C** (コメントを発表する)

質問: **9**
インフラストラクチャマネージャーが、VCF 9.0ワークロードドメインの「運用リザーブ」のサイズを決定しています。開発者は、CI/CDパイプラインにvSANデータ保護を使用し、非常に積極的なスナップショットスケジュール（例1:5分ごとにスナップショットを作成し、48時間保持）を設定する予定です。
「」
[SDDCマネージャー - 容量構成]
デフォルトのvSANしきい値
ホスト再構築予備率 :15%（有効）
運用準備金 :5% カスタマイズ可能）
「」
従来、マネージャーはVM（仮想マシン）により多くのキャパシティを割り当てるため、運用準備金を5%に引き下げていた。
スナップショットの頻繁な実行とこのカスタマイズされた運用予備力との相互作用は、クラスターの安定性とパフォーマンスにどのような直接的な影響を与えますか？（該当するものをすべて選択してください。）
A. vSAN ESA スナップショットはログ構造の B ツリー ポインタであるため、オペレーション リザーブ領域を消費しません。そのため、5% の設定は完全に安全です。
B. スナップショット統合のオーバーヘッドによりオペレーションリザーブが枯渇した場合、vSAN はデータストアの破損を防ぐために、受信 VM 書き込み I/O をゼロに制限します。
C. 運用リザーブが満杯の場合、保持制限に達したときに古いスナップショットを削除できず、データストアが急速に100%まで満杯になります。
D. ディープスナップショットチェーンは、メタデータのオーバーヘッドを大幅に増加させます。バックグラウンドスナップショットの削除が発生すると、一時的なステージングスペースを消費し、5%の運用予備スペースをすぐに使い果たしてしまう可能性があります。
正解: (正解を表示します)

質問: **10**
どのvSAN機能が、サイト間でのデータ可用性を保証しますか？
A. ストレッチド クラスター
B. スナップショット
C. RAID 0
D. クローン
正解: (正解を表示します)

質問: **11**
管理者は、運用中の仮想マシン（VM）に対する、破壊的な可能性のある変更を迅速にテストする必要がある。
この仮想マシンは現在、vSANデータ保護によって保護されています。
この目的を達成するために、vSANデータ保護のどの機能を活用できますか？
A. 不変のスナップショット
B. 複数スナップショットスケジュール
C. 保護グループ
D. リンククローン

E. 複製
正解: (正解を表示します)
リンククローンは、管理者が本番環境の仮想マシンを直接変更することなく、潜在的に破壊的な変更をテストする必要があるため、適切な機能です。vSAN Data Protectionは、ネイティブのvSAN ESAスナップショット技術を使用して、保護グループとスケジュールされたスナップショットを通じて仮想マシンを保護します。
vSAN Data Protectionは、単純な復元操作に加えて、開発、検証、テスト、またはリカバリのユースケース向けに、保護されたスナップショットからVMを作成できるクローンワークフローをサポートしています。リンククローンは、ベーススナップショットへの依存関係を維持しながら既存のスナップショットから迅速に作成できるため、完全な独立したコピーを作成する際の時間と容量への影響を回避できるため、特に適しています。不変スナップショットはリカバリポイントを削除や変更から保護しますが、それ自体は隔離されたテストVMを提供するものではありません。複数のスケジュールはスナップショットのタイミングのみを制御します。保護グループは、保護対象のVMを定義します。レプリケーションは、サイトレベルの保護と災害復旧に使用され、ローカルの本番スナップショットに対して破壊的な変更を迅速にテストするためには使用されません。
参照トピック :vSANデータ保護、スナップショットサービス、保護グループ、スナップショットからのリンククローン、VMテストおよびリカバリワークフロー。

質問: **12**
管理者は、リモートのVMware Cloud Foundation （VCF）ワークロードドメイン向けに、高可用性を備えたvSAN ESA 2ノードクラスタを設計する任務を負っています。このソリューションは、ホスト障害に加えて、いずれかのディスクグループの障害が発生してもデータ損失なく稼働し続ける必要があります。
設計に必要なネストされた障害ドメインの最小総数はいくつですか？
A. 6
B. 4
C. 7
D. 2
正解: (正解を表示します)
ネストされた障害ドメインの最小合計数は 6 です。2 ノードの vSAN 設計では、サイトの災害耐性は、2 つのデータ ホスト間でホスト ミラーリングを行い、ウィットネスがクォーラムを維持することによって提供されます。この要件により、もう 1 つのレイヤーが追加されます。ソリューションは、ホスト障害に加えて、ディスク グループまたはローカル ストレージ障害にも耐える必要があります。vSAN の 2 ノード ホスト ミラーリング ルールでは、ルールを使用するには、各データ ホストに少なくとも 3 つのディスク グループ、またはストレージ プールに 3 つのディスクが必要であると規定されています。ESA では、同等の構成は OSA スタイルのディスク グループではなく、ストレージ プール内のディスクです。データ ホストが 2 つあり、各データ ホストに 3 つのネストされた配置ユニットが必要なため、最小合計は 3 + 3 = 6 のネストされた障害ドメインです。4 つではホスト ミラーリング ルールの要件を満たさず、2 つではローカル ストレージ障害分離のない 2 つのホストのみを表します。参照トピック: vSAN 2 ノード クラスタ、ホスト ミラーリング、ネストされた障害ドメイン、vSAN ESA ストレージ プール配置。

質問: **13**
VCF 9.0でvSANクラスタ用の新しいESXiホストをコミッショニングする際に、SDDC Managerが実行するストレージ検証プロセスを正確に説明しているのは、次のうちどれですか？
A. SDDC Manager は ESXi カーネルをチェックして「vSAN Direct」デーモンが無効になっていることを確認します。vSAN Direct がアクティブな間は、物理ストレージディスクを検証できないためです。
B. SDDC Manager は、VMFS-6 ファイルシステムでドライブを自動的にフォーマットし、合成 I/O テストを実行して持続的な IOPS スループットを検証してから、ホストがクラスタに参加することを許可します。
C. SDDC Manager はディスク検証を vCenter Server Storage DRS エンジンに完全に委任し、ドライブをスキャンして不良セクタを検出します。
D. SDDC Manager はディスクの種類 (NVMe、SSD、HDD) を分析し、ディスクに既存のパーティションがないことを確認し、コミッショニング フェーズで定義された適切な vSAN アーキテクチャ プロファイル (ESA または OSA) にマッピングします。
正解: (正解を表示します)

質問: **14**
コンプライアンス監査担当者が、VCF 9.0 ストレッチド クラスタのフェイルオーバー イベントを調査しています。このクラスタは、外部のキー管理サーバー (KMS) クラスタに接続された vSAN データ保存時暗号化 (D@RE) を使用しています。

[ログ抜粋: vpxd.log - サイトAの障害]
2026-11-20T10:00:00Z FATAL hostd [サイト A] - 電源が失われました。
2026-11-20T10:00:05Z INFO vpxd - クォーラムは Witness + Site B を介して維持されます。
2026-11-20T10:00:10Z INFO vpxd - サイトBホストでHA再起動を開始します。
2026-11-20T10:00:15Z WARN vpxd - KMSサーバー「KMS-SiteA-01」に到達できません。
vSAN暗号化、vSphere HA、およびKMSトポロジー間の深いアーキテクチャ上の依存関係は、サイトAのKMSが失われた場合でも、暗号化されたVMがサイトBで正常に再起動することをどのように保証するのでしょうか？（該当するものをすべて選択してください。）
A. サイトBのESXiホストが停電中にコールドリブートされた場合、vSANデータストアをマウントするには、稼働中のKMSとのアクティブな通信が必要になります。
B. サイトBのホストは、ローカルのディスク暗号化キー（DEK）を復号化するために、KMSクラスター（KMS-SiteB-02）内の稼働中のKMSインスタンスからキー暗号化キー（KEK）を個別に取得する必要があります。
C. vSANは、サイトBのESXiホストがKEKをローカルのセキュアメモリキャッシュに保持しているため、標準的なストレージアクセス性を維持します。フェイルオーバー中に標準的なI/Oを継続するためにKMSに問い合わせる必要はありません。
D. VCF は、ロックアウトを防ぐために、vSAN サイト間リンク全体に平文暗号化キーを自動的に複製します。
E. プライマリ KMS サーバーが故障した場合、Witness Appliance は自動的にバックアップキープロバイダーとして機能します。
正解: **(**正解を表示します**)**

質問: **15**
管理者は、以下の特性を持つ新しいVMware Cloud Foundation（VCF）プライベートクラウド向けのストレージモデルを提案するよう指示されました。
* 単一のワークロードドメインを持つ単一のVCFインスタンス。
* VCF管理ワークロードドメインは、追加の管理ソフトウェアやハードウェアを必要としない、拡張性の高い統合ストレージソリューションを使用する単一のクラスタで構成されます。
* VCFワークロードドメインは、以下の要素で構成されるマルチティアストレージソリューションを必要とする単一のクラスタから構成されます。
* 重要なアプリケーションワークロード向けの、拡張性に優れたポリシーベースのストレージソリューション。
* 大規模なデータ要件を持つワークロード向けに、クラスタとは独立して拡張可能なファイルベースのストレージソリューション。管理者はどのストレージモデルを3つ推奨すべきでしょうか？（3つ選択してください。）
A. VCFワークロードドメインの補助ストレージソリューションとしてNFS v3を使用するべきです。
B. iSCSIはVCF管理ドメインの主要なストレージソリューションであるべきです。
C. VMware vSANは、VCFワークロードドメインの主要なストレージソリューションであるべきです。
D. VCF管理ドメインの主要なストレージソリューションとしてNFS v4.1を使用するべきです。
E. iSCSI は VCF ワークロード ドメインの補助ストレージ ソリューションであるべきです。
F. VMware vSANは、VCF管理ドメインの主要なストレージソリューションであるべきです。
正解: **(**正解を表示します**)**
VMware vSAN は、統合され、ポリシーベースで、スケーラブルであり、VCF および vSphere を介して直接管理されるため、管理ドメインとワークロード ドメインの両方にとって適切なプライマリ ストレージです。管理ドメインの要件では、追加のストレージ管理ソフトウェアやハードウェアを必要としない、高度にスケーラブルな統合ストレージ ソリューションが明示的に求められており、これは vSAN と一致します。ワークロード ドメインでは、重要なアプリケーション ワークロード向けに、高度にスケーラブルなポリシー ベースのストレージ ソリューションも必要とされ、これも vSAN ストレージ ポリシーと vSAN データ ストア サービスに直接対応します。第 2 層のワークロード ティアでは、大規模なデータ要件を持つワークロード向けに、クラスタとは独立してスケーリングできるファイル ベースのストレージが必要です。NFS v3 は補助ストレージとしてサポートされており、プライマリ vSAN データ ストアを変更せずにファイル ベースの容量を追加するのに適しています。iSCSI は補助ストレージのみであり、管理ドメインのプライマリ ストレージ要件を満たしません。NFS v4。
1 は管理ドメインのプライマリストレージとして正しく選択されていません。参照トピック :VCF ストレージモデル、プライマリストレージ、補助ストレージ、vSAN ストレージモデル、NFS ストレージモデル。

質問: **16**

最高技術責任者（CTO）は、ハードウェア調達サイクルを遅らせるため、ITチームに対しvSANクラスタのストレージ容量消費量を削減するよう指示した。
ストレージ管理者は、オブジェクト修復タイマー（CLOM修復遅延）を調整し、標準のストレージポリシー規則を変更して、積極的に領域を解放することを提案している。
「」
[ストレージポリシールールビュー - 変更案]
ポリシー :DB-Prod-Policy（提案）
許容できない不具合: 0 (冗長性なし)
オブジェクトスペース予約 :0%
詳細設定ターゲット:
CLOM修理遅延 :15分
「」
以下の記述のうち、これらの積極的な政策選択に伴うトレードオフと相互作用を正確に評価しているのはどれですか？（該当するものをすべて選択してください。）
A. FTT=0と15分のCLOM修復遅延の組み合わせにより、ホスト障害発生時にvSANはバックアップスナップショットからデータを自動的に再構築します。
B. 15分のCLOMタイマーは、ホストのパッチサイクルが定期的に行われる環境では非常に非効率的です。ホストの再起動には20〜30分かかることがよくあります。
C. FTT=0 (冗長性なし) に設定すると、ホスト障害が発生すると、CLOM 修復遅延が適用されずにオブジェクトが即座に「アクセス不可」になります。
D. CLOM 修復遅延を 15 分に短縮すると、コンポーネントが
「不在」状態となり、短時間の障害発生時にvSANが再同期のためにCPUとネットワーク帯域幅をより多く消費することになる。
正解: **(**正解を表示します**)**

質問: **17**
「不在」と「
vSANにおけるオブジェクトの「アクセス不能」な状態とは？
A. 「不在」は標準のvSphere vMotionによって発生する一時的な状態であり、「アクセス不可」はハードウェアの劣化によって発生する永続的な状態です。
B. 「欠落」は、オブジェクトのすべてのコンポーネントが欠落しており、データが失われていることを示します。
「アクセス不可」とは、オブジェクトが分散リソーススケジューラ（DRS）によってロックされていることを示します。
C. 「不在」はvSANキャッシュ層にのみ適用され、「アクセス不可」は容量層にのみ適用されます。
D. 「不在」は、コンポーネントに現在アクセスできないが、オブジェクトがクォーラム（50%以上の投票）を維持しオンライン状態にあることを示し、「アクセス不可」は、オブジェクトがクォーラムを失い、I/Oを処理できないことを意味します。
正解: **(**正解を表示します**)**

質問: **18**
ネットワーク管理者が、vSAN Express Storage Architecture (ESA) を実行している VCF 9.0 環境で、容量ポリシーの監査を行っています。
管理者は、クラスターの基本運用オブジェクトに適用されているSPBM構成を照会します。
「」

[vSANクラスタ構成出力]
vSANのデフォルトストレージポリシー
ストレージプール: ESA-NVMe-Pool
ルール :OSR オブジェクトスペース予約）=シンプロビジョニング
「」
vSAN ESAの オブジェクトスペース予約」ポリシーは、従来のvSAN OSAと比べてなぜ根本的に異なるのでしょうか？また、予約が必要な特定のオブジェクトはどれですか？（該当するものをすべて選択してください。）
A. ESAのログ構造の性質上、データは追記専用の連続ストライプに書き込まれます。実際に書き込まれる前に特定の物理セクターを 予約」することは数学的に不可能であり、ブロックデータに対して従来のOSR定義は時代遅れになります。
B. OSAでは、シックプロビジョニングはSATAドライブ上の生の物理セクターを割り当てますが、ESAでは、シックプロビジョニングはNVMeメモリページを事前に割り当てることで、ネットワークの混雑をゼロに保証します。
C. vSAN ESAでは、ユーザーデータ（VMDK）は常に厳密にシンプロビジョニングされます。新しいログ構造メタデータマッピングのため、VMペイロードデータの容量を予約するOSR UIオプションは完全に非推奨になりました。
D. OSR=100% は ESA でも適用できますが、HA イベント中にスワップ ファイルと構成ファイルが確実に割り当てられるように、特定の「VM ホーム 名前空間」オブジェクトにのみ適用されます。
E. 標準重複排除が有効になっている場合、ESA は厳密に OSR=100% を必要とします。
正解: (正解を表示します)

質問: **19**
クラウド管理者は、VCF 9.0環境向けにセキュアな災害復旧トポロジーを構成します。
プライマリサイトでは、保存データ暗号化が有効になっているvSAN ESAクラスタを使用しています。セカンダリサイトも、保存データ暗号化が有効になっているvSAN ESAを使用しています。
管理者は、vSphere Replicationを設定して、Tier-1 VMをプライマリからセカンダリにレプリケートします。
「」
[ストレージポリシールールセット]
ソースSPBM: ESA-RAID5-Encrypted
対象SPBM :ESA-RAID6暗号化
「」
ソースディスクからターゲットディスクへのレプリケーションプロセスのライフサイクル全体を通して、データセキュリティはどのように管理されていますか？（該当するものをすべて選択してください。）
A. VM のデータは、vSAN データストアから読み取られる際にソース ESXi ホストによって復号化され、平文で vSphere Replication アプライアンスのネットワーク バッファに入ります。
B. vSphere Replicationは、vCenter APIを使用して、ソースゲストOSのBitLockerキーをターゲットサイトに自動的にマッピングします。
C. 暗号化されたデータブロックは生データとしてネットワーク経由で送信されます。ターゲットのvSANクラスタは、データを読み取るためにプライマリサイトのキー暗号化キー（KEK）をインポートする必要があります。
D. セカンダリサイトに到着すると、ターゲットのvSANデータストアは、セカンダリサイト独自のローカルディスク暗号化キー（DEK）を使用して受信データを暗号化してから、NVMeにデステージングします。
E. WAN を介して転送されるデータを保護するには、管理者は VM の vSphere Replication の詳細設定で ネットワーク トラフィック暗号化」を明示的に有効にする必要があります。
正解: (正解を表示します)

質問: **20**
ある多国籍企業は、以下の要件を満たすティア1ビジネスアプリケーションをホストするために、VMware Cloud Foundation（VCF）ワークロードドメインクラスタを導入しようとしています。
* すべてのワークロードに対して高いパフォーマンスを提供します。
* 自動VM配置との統合。

* 事業部門ごとに分割された複数のファイバーチャネル（FC）アレイを含む、既存のインフラストラクチャの再利用。
* ストレージアーキテクチャはvSANを避ける必要がある。
組織上の分離要件を満たすこと。
これらの要件を満たす導入方法はどれですか？（2つ選択してください。）
A. 割り当てられたFCアレイ上に専用のVMFSデータストアをプライマリストレージとして構成します。
B. 割り当てられたFCアレイ上に、補助ストレージとして専用のVMFSデータストアを構成します。
C. 割り当てられたFCアレイ上に共有VMFSデータストアをプライマリストレージとして構成します。
D. 割り当てられたFCアレイ上に共有VMFSデータストアを補助ストレージとして構成します。
E. 割り当てられたFCアレイ上に共有VMFSデータストアをプライマリストレージとして構成します。
正解: **(**正解を表示します**)**
割り当てられたファイバーチャネルアレイ上の専用VMFSデータストアは、パフォーマンスと分離の両方の要件を満たします。VCFは、ワークロードドメインの主要ストレージとしてファイバーチャネルを基盤とするVMFSをサポートしており、ティア1ビジネスアプリケーションクラスタの主要データストアタイプとして有効です。ファイバーチャネルは、低遅延のブロックストレージ、耐障害性の高いパス、SANゾーニング、LUNマスキング、および成熟したエンタープライズパフォーマンス特性を提供します。既存のFCアレイはビジネスユニットごとにパーティション化されているため、専用データストアは組織の分離を維持し、共有ストレージリソース上でビジネスユニットのワークロードが混在するのを防ぎます。同じ専用FC基盤VMFSアプローチは、ワークロードドメインが確立された後の補助ストレージとしても使用でき、分離を維持しながら追加の容量や特殊なティアを可能にします。共有VMFSデータストアは、複数のビジネスユニットが同じデータストア境界を使用できるため、組織の分離要件を満たしません。vSANは明示的に除外されているため、設計はサポートされている非vSANストレージに依存する必要があります。VMFSデータストアクラスタとStorage DRSは、データストアが互換性があり、同様に管理されている場合、VMの自動配置をサポートできます。参照トピック :ファイバーチャネルストレージモデル、VMFSデータストア、プライマリストレージ、補助ストレージ、データストアクラスタ。

質問: **21**
最高技術責任者（CTO）が、VCF 9.0における新しいvSAN ESAクラスタのパフォーマンス指標を評価している。
従来のSANストレージアレイは、バックエンドディスクのIOPSがフロントエンドアプリケーションのIOPSを大幅に上回る「RAID-5書き込みペナルティ」という問題に悩まされていました。CTOは、構成YAMLエクスポートを介してESAログ構造メトリックを分析します。
「」
vSAN ESA パフォーマンスマトリックス
DOMフロントエンド（VM）書き込み :10,000 IOPS（ランダム4KB）
SPBMポリシー :RAID-5（4+1構成）
LSOMバックエンド（ディスク）書き込み :1,500 IOPS（シーケンシャル1MB）
「」
vSAN ESAは、従来のイレイジャーコーディング（RAID-5/6）に伴うバックエンドのパフォーマンスボトルネックを、どのように根本的に解消するのでしょうか？（該当するものをすべて選択してください。）
A. ESAログ構造ファイルシステムは、10,000個の小さなランダムな4KB書き込みをメモリにバッファリングし、それらを少数の大きな1MBの連続ブロックに統合（パック）します。
B. このシステムは、RAIDコントローラに物理的に接続された永続的なフラッシュメモリ層を使用してパリティ演算を処理します。
C. データは新しい完全な連続ストライプに書き込まれるため、NVMe ドライブは古いデータや古いパリティ ブロックを最初に読み取る必要がなくなり、「読み取り - 変更 - 書き込み」のペナルティが完全に解消されます。
D. 10,000 アプリケーション IOPS を 1,500 物理 NVMe IOPS に削減することで、バックエンドの混雑が緩和され、物理 NVMe ドライブが効率的に使用され、ボトルネックにならないことが保証されます。
E. ESAはデータベースに対してRAID-1ミラーリングを厳密に適用するため、RAID-5データの比較は無意味になります。
正解: **(**正解を表示します**)**

質問: **22**
ストレージアーキテクトが会計チームとの会議に呼ばれ、その理由を解明しようとしている。

彼らの生容量の20%は消費に利用できません。彼らのvSANクラスタは、以下の特性で作成されました。
* vSANクラスタ内の6台のホストに、2TBのNVMeディスクが2台搭載されている。
* デフォルトポリシーでは、FTT=1、RAID-1となります。
* このクラスターではホスト再構築リザーブは有効化されていません。
建築家は、使用できない容量の大部分を占める要因として、どの2つの項目を挙げるべきでしょうか？ 2つ選択してください。）
A. VMスワップオーバーヘッド
B. ホストアップグレードのオーバーヘッド
C. 暗号化オーバーヘッド
D. RAIDオーバーヘッド
E. 運用準備金（政策変更、再調整、データ移動）
正解: **D,E (**コメントを発表する**)**

質問: **23**
L3サポートエンジニアが、vSANストレッチドクラスタで構成されたVCFワークロードドメインにおける深刻なパフォーマンス低下とVMの一部利用不能のトラブルシューティングを行っています。このクラスタは「Witness Traffic Separation」（WTS）機能を使用しています。
エンジニアは、セカンダリ障害ドメインのホストsec-01からvmkernel.logを取得します。
「」
2026-05-12T14:15:22.456Z INFO vsanmgmt - ストレッチドクラスタのヘルスチェックを開始します
2026-05-12T14:15:30.112Z WARN vsan-network [vmk2:vSAN-Data] Preferred-Gatewayへのpingに失敗しました:
目的地に到達できません
2026-05-12T14:15:35.889Z INFO vsan-network [vmk3:Witness-Traffic] Witness-Appliance (10.50.1.10) への Ping 成功
2026-05-12T14:15:36.001Z ERROR cmmds - クラスタパーティションが検出されました。セカンダリサイトが優先サイトから分離されました。
2026-05-12T14:15:38.220Z INFO clom - オブジェクト 5543505c-xxxx が DEGRADED 状態に移行します。
2026-05-12T14:15:40.500Z WARN vsan-network [vmk2:vSAN-Data] ISLで高い輻輳が検出されました。
TxQueue=100%
2026-05-12T14:15:45.000Z ERROR vobd - [vSAN] ノード uuid-sec-01 は、WTS ネットワークを介して Witness ノード uuid-wit-01 との通信を失いました。
2026-05-12T14:15:45.500Z ERROR cmmds - オブジェクト 5543505c のコンポーネントの状態が INACCESSIBLE に変更されました。
「」
ログと、障害ドメインとウィットネストラフィック分離の統合に基づいて、以下の記述のうち、根本原因とシステム動作を説明しているのはどれですか？（該当するものをすべて選択してください。）
A. vmk2 の輻輳は、ストレージ I/O トラフィックが Witness Traffic Separation ネットワーク経由で誤ってルーティングされていることを示しています。
B. デュアルサイトミラーリングポリシーでは、オブジェクトへのアクセスを維持するために、セカンダリサイトが優先サイトまたはウィットネスのいずれかとの接続を維持する必要があります。
C. セカンダリ障害ドメインは、14:15:35にvmk3を介してクォーラムを正常に維持し、その時点でVMがアクセス不能状態になるのを防ぎました。
D. 14:15:45に発生したWitness Traffic Separationネットワーク（vmk3）の障害により、セカンダリーサイトはタイブレーカー投票で敗北しました。
正解: **(**正解を表示します**)**

質問: **24**
顧客は、バックアップのステージングのために、外部のファイバーチャネル（FC）VMFSデータストアをVMware Cloud Foundation（VCF）ワークロードドメインに接続します。管理者は、データストアがすべてのホストから見えること、およびファブリックリンクまたはパスに障害が発生した場合にパスとデバイスの健全性アラームがトリガーされることを確認する必要があります。
管理者はこれを検証するためにどのような行動をとるべきでしょうか？

A. 各ホストで esxcli vsan storage list を実行して、VMFS データストアのパスの状態を確認します。
B. vCenterで外部VMFSデータストアの接続性、パス、マルチパスの健全性を確認します。
C. VCF SDK を介して storage.monitor.getStatus を実行し、すべての VMFS、vSAN、NFS データストアの統合された健全性サマリーを取得します。
D. esxcli fc adapter list を実行してから vmkfstools --inspectpaths を実行して VMFS LUN の健全性を検証します。
正解: **(**正解を表示します**)**
正しい手順は、vCenter でデータストア、デバイス パス、およびマルチパスの状態を確認することです。ファイバー チャネル VMFS ストレージは、SAN ファブリックの接続性、HBA、ゾーニング、LUN マスキング、ストレージ プロセッサ、パス選択ポリシー、およびマルチパスに依存します。vCenter は、ワークロード ドメイン クラスタ内のすべての ESX ホストから FC VMFS データストアが見えるかどうかを確認するために必要な運用ビューを提供します。また、ストレージ デバイス パスの状態とマルチパスの健全性も公開されるため、管理者は冗長パスがアクティブであることを検証でき、ファブリック リンクまたはパスに障害が発生した場合にアラームをトリガーできます。esxcli vsan storage list は vSAN デバイスに固有のものであり、外部 FC VMFS パスを検証しません。提案されている VCF SDK コマンドは、FC パスとデータストアの可視性を検証するための標準的な方法ではありません。vmkfstools -- inspectpaths は、FC LUN の健全性検証のための通常の vSphere ワークフローではありません。FC をバックとする VMFS の場合、vCenter ストレージ ビューが正しい集中検証ポイントを提供します。参考トピック :ファイバーチャネルストレージモデル、VMFSデータストア接続性、マルチパス、パスの健全性、vCenterストレージ監視。

質問: **25**
コンプライアンス監査担当者が、VCF 9.0実装向けにYAML形式で記述されたSite Recovery Manager（SRM）の災害復旧計画をレビューしています。
この環境では、プライマリvSANドメインとセカンダリvSANドメイン間のワークロードを保護するために、標準のvSphere Replication（ストレッチクラスタリングではない）を使用します。
「」
SRM保護グループ：金融ティア1
名前: "Fin-PG-01"
レプリケーションタイプ: "vSphere_Replication"
データストア:
- ソース: "vsanDatastore-Primary"
ターゲット: "vsanDatastore-DR"
ストレージポリシーマッピング:
- source_policy: "FTT=1 (RAID-1)"
target_policy: "FTT=2 (RAID-6)"
「」
実際のSRMフェイルオーバーイベント中に、target_policy仕様はvSAN分散オブジェクトマネージャ（DOM）とどのように連携するのでしょうか？
A. フェイルオーバー中、セカンダリ vCenter は復旧した VMDK を直接プロビジョニングします。
「vsanDatastore-DR」は「FTT=2 (RAID-6)」ルールを使用し、起動時にローカル消去符号化によってデータが即座に保護されるようにします。
B. vSphere ReplicationはソースvSANデータストアの同一の物理ジオメトリをターゲットサイトに自動的にクローンするため、SRMはtarget_policyを無視します。
C. 設定が無効です。SRM では、レプリケーション チェックサムを維持するために、ソース サイトとターゲット サイトの両方で同一のポリシーが必要です。
D. ターゲットポリシーにより、セカンダリサイトはvSANデータストアを標準VMFSボリュームに変換して、受信するレプリケートされたデータストリームを受け入れるように強制されます。
正解: **A (**コメントを発表する**)**

質問: **26**
コンプライアンス監査担当者が、新しいHCIメッシュ環境のストレージポリシー構成をレビューしています。「Webクライアントクラスタ」上でVMを実行しているデータベースチームは、リモートの「DBサーバークラスタ」データストアにVMをプロビジョニングする予定です。「DBサーバークラスタ」は、12台のホストとvSAN ESAを利用した非常に堅牢な構成です。
監査担当者は、これらの仮想マシンに割り当てられているストレージポリシーを抽出します。

「」
SPBM ポリシー: "Mesh-DB-Policy"
【ポリシールール】
サイト災害耐性 :なし - 標準クラスター
許容障害数 :2件 - RAID-6（イレイジャーコーディング）
暗号化：有効
【ストレージ互換性】
データストア: vsanDatastore-DB-Server
ホスト：準拠
「」
このHCIメッシュ構成における有効なコンプライアンスチェックと機能動作を表す記述を2つ選択してください。
A. このトポロジーでは暗号化が無効です。HCI Mesh は、クライアントとサーバー クラスタ間のデータ転送暗号化をサポートできません。
B. データベース VM の RAID-6 消去符号化計算は、CPU サイクルを消費します。
「Webクライアントクラスタ」ホストであり、「DBサーバークラスタ」ホストではありません。
C. ストレージポリシーには、VM の実行をサーバークラスタホストに固定してネットワーク遅延を最小限に抑えるための「データ局所性」ルールを含める必要があります。
D. 「許容できない障害」ルールは、「Webクライアントクラスタ」ではなく、「DBサーバークラスタ」のホスト数（2ホスト）に対して検証されます。
正解: **B,D** (コメントを発表する)

質問: **27**
SOCアナリストがvCenterの物理ストレージメトリクスを監査し、異常がないか確認しています。アナリストは、「Witness Components」がクラスタネットワークの帯域幅を消費しているにもかかわらず、NVMeドライブの容量の0.001%未満しか消費していないことに気づきました。
「」
[vSANパフォーマンスビュー > コンポーネントの内訳]
オブジェクト: ファイルサーバーVMDK
コンポーネント1（データ）500GB
コンポーネント2（データ）500GB
コンポーネント3（証人）4MB
「」
vSAN分散オブジェクトマネージャ（DOM）がこれらの4MBのWitnessコンポーネントを積極的に生成および管理する理由は何ですか？また、それらの配置を規定するルールは何ですか？（該当するものをすべて選択してください。）
A. ウィットネスコンポーネントはストレッチドクラスタトポロジでのみ生成されます。標準クラスタではタイブレーカーは必要ありません。
B. ウィットネス コンポーネントは、投票対象のデータ コンポーネントと同じ物理的な障害ドメインに配置してはなりません。そうすると、クォーラムを破壊する単一障害点が発生します。
C. ウィットネスコンポーネントには仮想マシンのペイロードデータは含まれていません。オブジェクトの最新の構成シーケンス番号 (CSN) を追跡するために使用される 4 MB のメタデータのみで構成されています。
D. データコンポーネントの数が偶数票数になる場合（例：FTT=1の場合、ミラーリングには2つのデータコピーがあります）、CLOMによってWitnessコンポーネントが自動的に生成されます。Witnessは3票目を提供し、50%を超える多数決が計算できるようにします。
E. 4 MB の容量は標準の LZ4 圧縮を示しています。VM で書き込み I/O が大量に発生すると、Witness コンポーネントはデータ コンポーネントのサイズ (500 GB) と同じサイズに拡張されます。
正解: **(**正解を表示します**)**

質問: **28**
ストレージ管理者には、VMware Cloud Foundation (VCF) のアーキテクチャに関する以下の詳細情報が提示されます。
* アプリケーションデータには2.5PBの容量が必要です。
* 本番環境のアプリケーションは、アーカイブソリューションとゲートウェイをホストします。
* テストおよび開発の目的で、いくつかのアプリケーションが展開されます。
管理者が推奨できる最適なプライマリストレージは何ですか？
A. vSAN ESAストレージクラスタ
B. vSAN ESA
C. vSAN OSA - オールフラッシュ
D. vSAN OSA - ハイブリッド
正解: (正解を表示します)
vSAN ESAストレージクラスタは、ワークロードプロファイルが容量重視で、分散ストレージのメリットを享受できるため、最適な選択肢です。2.5 PBのアプリケーションデータ、アーカイブワークロード、ゲートウェイ、開発/テストアプリケーションに対する要件は、コンピューティングリソースとは独立してストレージ容量を拡張する必要があることを示しています。VMware Cloud Foundationは、vSANストレージクラスタをvSAN ESAに基づく分散ストレージソリューションと説明しています。ストレージリソースは提供しますが、コンピューティングリソースは提供しません。データストアは、vSANコンピューティングクラスタまたはvSAN HCIクラスタによってマウントできます。このモデルは、不要なコンピューティングを追加することなく容量とパフォーマンスを拡張できる、ストレージ密度の高い環境向けに設計されています。標準のvSAN ESA HCIクラスタは、高性能ワークロードに最適ですが、コンピューティングとストレージを同時に拡張します。vSAN OSAオールフラッシュおよびハイブリッドは、古いディスクグループアーキテクチャを使用するため、この大容量でストレージ中心の設計にはあまり適していません。したがって、拡張性、パフォーマンス、および容量増加の要件を満たすには、vSAN ESAストレージクラスタを主要なストレージとして推奨する必要があります。参考トピック :vSANストレージクラスタ、分散ストレージ、vSAN ESA、ストレージモデル。

質問: **29**
ストレージのパフォーマンスに関するトラブルシューティングにおいて、最も重要な指標はどれですか？
A. レイテンシー
B. ディスクサイズ
C. CPU使用率
D. メモリ使用量
正解: (正解を表示します)

質問: **30**
管理者がvSANのパフォーマンス問題のトラブルシューティングを行っています。vSANクラスタのパフォーマンスチャートを見ると、vSANクラスタで高いレイテンシが発生しています。
パフォーマンスの問題の考えられる原因は何ですか？
A. 仮想マシンはPVSCSIコントローラを使用しています。
B. VMkernelアダプタでジャンボフレームが有効になっています。
C. ストレージポリシーでイレイジャーコーディングが無効になっています。
D. 1つ以上のディスクグループで輻輳が発生しています。
正解: (正解を表示します)
vSANクラスタにおける高いレイテンシは、一般的にバックエンドストレージパスの輻輳が原因です。ディスクグループの輻輳とは、1つ以上のディスクグループが必要な速度でワークロードを処理できないため、vSANがI/Oをキューイング、遅延、またはスロットリングしている状態を指します。VCF OperationsおよびvSANパフォーマンスビューでは、IOPS輻輳、ログ輻輳、コンポーネント輻輳、メモリ輻輳、SSD輻輳など、ディスクグループおよびデバイスレベルの輻輳インジケーターが表示されます。これらのメトリックは、仮想マシンのI/OパスがvSANバックエンド処理の完了を待つ必要があるため、レイテンシの上昇と直接相関します。PVSCSIコントローラは通常、高性能仮想ディスクに推奨され、vSANレイテンシの一般的な原因ではありません。ジャンボフレームは、エンドツーエンドで一貫して構成されている場合、有効なネットワーク最適化であり、本質的にレイテンシを引き起こすものではありません。イレイジャーコーディングを無効にすると、通常はパリティオーバーヘッドが削減され、バックエンドレイテンシは発生

しません。したがって、vSANクラスタパフォーマンスチャートに表示される高いレイテンシの原因として最も可能性が高いのは、ディスクグループの輻輳です。参照トピック：vSANパフォーマンスサービス、ディスクグループメトリック、輻輳メトリック、vSANレイテンシのトラブルシューティング。

質問: **31**
ストレージ管理者が、vSAN ESAクラスタで発生している不安定なレイテンシのトラブルシューティングを行っています。Skyline Healthではシステムは正常と表示されていますが、管理者はトップオブラック（Top-of-Rack）スイッチのバッファに問題があるのではないかと疑っています。
管理者は、クラスタ全体で「vSANネットワークパフォーマンステスト」（プロアクティブテスト）を実行します。
「」
【アーキテクチャ図：ネットワークパフォーマンステスト】
ホスト1（iperfクライアント）→スイッチ→ホスト2（iperfサーバー）
テスト結果：目標値：25 Gbps。達成値：14 Gbps。再送信回数：5,400回。
「」
この特定の予防的テストは、管理者がHCIストレージのボトルネックを診断するのにどのように役立ちますか？
（該当するものをすべて選択してください。）
A. テストはハイパーバイザーのメモリネットワークスタック内で完全に実行され（iperfを使用）、物理的なNVMeドライブを明示的にバイパスします。これにより、11Gbpsの損失はネットワークファブリックの問題であり、低速なハードドライブの問題ではないことが証明されます。
B. 多数の「再送信」(5,400) は、物理スイッチでのパケットドロップを明確に確認し、テストによって生成されたマイクロバースト中のバッファオーバーフローを強く示唆しています。
C. テストにより、ESA DOM ロジックがパリティ ビットを誤って複製し、ネットワーク飽和を引き起こしていることが証明されました。
D. 診断出力により、管理者はネットワークチームに決定的な証拠を提供できます。
「25 GbE」ポートは、実際のTCP負荷がかかると、性能が著しく低下する。
E. このテストでは、クラスタ上のストレージポリシーベース管理（SPBM）IOPS制限を、実際の帯域幅14Gbpsに自動的に調整します。
正解: (正解を表示します)

質問: **32**
管理者には次のようなシナリオが提示されます。
* VMアプリケーションの所有者から、20TBの追加ストレージが要求されています。
* このアプリケーションは、CPUとメモリに対する要求が高く、その要求を満たすことができるのは、現在アプリケーションが実行されているクラスタのみです。
* アプリケーションを適切に動作させるには、高いIOPSと帯域幅が必要です。
* 既存のvSANクラスターには、未使用容量が10TBしかありません。
クラスター内のホストには、追加のNVMeスロットが残っていません。
* 管理者は、追加のホストを購入したり、他のvSANクラスタからホストを再割り当てしたりする権限を持っていません。
* 環境内には、要件を満たすことができる他のvSANクラスタが存在する。
このシナリオを実現するには、どのvSAN機能を使用すべきでしょうか？

A. vSAN HCIメッシュ
B. vSANデータ保護
C. vSANファイルサービス
D. vSAN ストレッチド クラスター
正解: **(**正解を表示します**)**
アプリケーションは既存のコンピューティングクラスタ上で引き続き実行する必要があるものの、そのクラスタには十分な未使用のvSAN容量がなく、拡張用のNVMeスロットも利用できないため、vSAN HCI Meshが適切な機能です。
HCI Mesh（vSANデータストア共有とも呼ばれる）を使用すると、独立したvSANクラスタが、互換性のある他のvSANクラスタとリモートデータストアの容量を共有できます。リモートデータストアは、ローカルストレージであるかのようにマウントして使用できるため、現在のクラスタで実行されているVMは、十分な容量とパフォーマンスを備えた別のvSANクラスタからストレージを消費できます。これにより、ホストを購入したり、ホストを再割り当てしたり、必要なCPUとメモリを提供するクラスタからアプリケーションを移動したりすることなく、要件を満たすことができます。vSAN Data Protectionは、スナップショットとリカバリに対応しており、容量拡張には対応していません。vSAN File Servicesは、SMB/NFSファイル共有を提供し、追加のVMデータストア容量は提供していません。vSAN Stretched Clustersは、可用性ゾーンの回復力を提供し、クラスタ間の容量借用には対応していません。VCFドキュメントでは、HCI Meshを、複数の独立したvSAN HCIクラスタが隣接するvSANストレージリソースからストレージを消費できるようにするクラスタ間容量共有として説明しています。参照トピック：vSAN HCI Mesh、vSANデータストア共有、クラスタ間容量共有、リモートvSANデータストア。

質問: **33**
オブジェクト空間予約（OSR）の目的は何ですか？
A. CPUの予約
B. ネットワークの改善
C. 保管容量を保証します
D. キャッシュサイズを増やす
正解: **(**正解を表示します**)**

質問: **34**
vSANにおいて、最も高い耐障害性を提供するRAID構成はどれですか？
A. RAID 0
B. RAID 6
C. RAID 5
D. RAID 1
正解: **B (**コメントを発表する**)**

質問: **35**
コンプライアンス監査担当者が、機密作戦に使用されるエアギャップされたVCFワークロードドメインをレビューしています。顧客体験向上プログラム（CEIP）およびvCenterのインターネットアクセスは、恒久的に無効化されています。
vSANヘルスチェックで「vSAN HCL DBが古くなっています」という報告が頻繁に表示されます。
「」
[vSANクラスタ構成]
vSANエディション：エンタープライズプラス（vSAN 8.0 U2）
CEIP: 無効
インターネットアクセス：なし（エアギャップ）
「」

管理者はこの特定の制限された環境において、このコンプライアンス警告をどのように解決すべきでしょうか？
A. 管理者は、インターネットに接続されたワークステーションに VMware パブリック ポータルから all.json HCL ファイルをダウンロードし、それを内部ネットワークに転送して、vCenter vSAN Health UI の「ファイルからの更新」オプションを使用して手動でアップロードする必要があります。
B. SDDC Manager は、VMware クラウドへの安全なダークファイバー接続を確立することでエアギャップを自動的にバイパスし、HCL データベースを ESXi メモリに直接ストリーミングします。
C. 最新の HCL JSON が ESXi インストール ISO にハードコードされているため、管理者が新しい vSphere Lifecycle Manager (vLCM) クラスタ イメージを適用すると、更新が自動的に行われます。
D. HCL の更新は非 CEIP 環境では厳密にサポートされていないため、管理者は Skyline Health の「コントローラー ファームウェア」のヘルス チェックを無効にする必要があります。
正解: **A** (コメントを発表する)

質問: **36**
コンプライアンス監査担当者が、VCF 9.0 における暗号化された vSAN ストレッチド クラスタのライフサイクルを追跡しています。
SDDC Manager を介して新しい ESXi ホスト (esx-09) が起動され、クラスタに正常に追加されました。
「」
[ログ分析 :vsan-crypto_config.log / CMMDSイベント]
イベント1 :ホスト「esx-09」がクラスタに参加します。
イベント2 :vCenterがKMSの信頼性検証が必要であることを検出します。
イベント 3: SDDC マネージャーがホストに対して「vsan storage add」API 呼び出しを発行します。
イベント4 :ホストが内部データ暗号化キー（DEK）を生成します。
イベント5 :ディスクの取得が完了しました。
「」
SDDC Manager、vSAN暗号化、およびディスク要求機能の緊密な統合は、この新しいホストが既に暗号化されたクラスタに追加された場合に、どのようにセキュリティを強化しますか？（該当するものをすべて選択してください。）
A. SDDC Manager は、vSAN ソフトウェア暗号化スタックをバイパスして、VMFS-6 自己暗号化ドライブ (SED) 機能を使用して新しいディスクを自動的にフォーマットします。
B. ディスクを要求する前に、SDDC Manager は、esx-09 が管理ドメインに構成された外部 KMS クラスタと通信してキー暗号化キー (KEK) を取得できることを検証します。
C. SDDC Manager は、新しいホストが暗号化されていない CMMDS ハンドシェイクを実行できるように、クラスタ全体で vSAN データ転送 (DiT) 暗号化を一時的に無効にする必要があります。
D. 新しいディスクは既存のクラスタ全体のKEKによってラップされるため、管理者は追加されたホストに対して新しいKMSポリシーを構成する必要はありません。
E. esx-09 上のローカル ESXi ハイパーバイザーは、新しい物理ドライブごとにローカルで固有のディスク暗号化キー (DEK) を生成し、デバイスレベルのキーがホストから決して離れないようにします。
正解: (正解を表示します)

質問: **37**
VCFアーキテクトが、マルチペタバイト規模のvSANストレッチドクラスタのセキュリティフットプリントを設計している。
このアーキテクチャは、リースされたWAN回線で接続された2つの稼働中のデータセンター（サイトAとサイトB）と、監視用アプライアンス用の第3のサイトで構成されています。
[サイト間におけるデータ転送暗号化フローを示す画像]
リンク（ISL）と証人ホストへ]
以下の記述のうち、このストレッチドクラスタトポロジーにおけるデータ転送時暗号化（DiT）の役割と範囲を正しく評価しているのはどれですか？（該当するものをすべて選択してください。）
A. DiTは、Witness Applianceに送信される低帯域幅のCMMDSタイブレーカートラフィックを暗号化し、中間者攻撃によるクラスタクォーラムの操作を防ぎます。
B. ストレッチドクラスタ内の DiT では、暗号化ストリームを分離するために「Witness Traffic Separation」（WTS）機能を有効にする必要があります。
C. DiTメタデータストリームの復号鍵を生成するには、Witness Applianceに専用の外部KMSのライセンスが必要です。
D. ストレッチド クラスタでは DiT が非常に重要です。なぜなら、サイト A とサイト B 間の同期書き込みは、物理的なケーブルのセキュリティが保証できないパブリック/リースされたサイト間リンク (ISL) を経由するからです。

E. DiTでは、WAN経由で書き込まれるデータは転送中に既に保護されているため、vSANデータ保存時暗号化（D@RE）の要件が不要になります。
正解: **(**正解を表示します**)**

質問: **38**
L3サポートエンジニアが緊急対策室に呼び出された。vSAN ESAストレッチドクラスタ（サイトAとサイトB、サイトCにWitness）で複雑な連鎖障害が発生した。
現在の状態:
1. サイトBは完全な停電に見舞われた。
2. 同時に、サイトCのWitness Applianceネットワークリンクは
切断された。
3. サイトAはハードウェアの障害もなく、完全に稼働しています。
サイトBで元々稼働していた仮想マシンにはアクセスできません。サイトAで元々稼働していた仮想マシンはフリーズしています。
ストレージポリシーの設定は以下のとおりです。
「」
ストレッチドクラスタポリシー
[サイトの災害耐性]
ルール = "デュアルサイトミラーリング（ストレッチドクラスター）"
【許容できないこと】
ルール = "1つの障害 - RAID-5 (イレイジャーコーディング) [ローカル]"
【アドバンスルール】
ForceProvisioning = 0
「」
オブジェクトヘルス状態とストレッチドクラスタトポロジーの統合に基づいて、サイトAのVMがフリーズしている理由と、それらのストレージオブジェクトの正確な状態は何ですか？（該当するものをすべて選択してください。）
A. ForceProvisioning = 0 ルールは、サイト B が復旧するまで、vSphere HA がサイト A 上の VM を再起動することを防止します。
B. サイトA VMのオブジェクトは「アクセス不可」です。これは、サイトAがローカルレプリカ（1票）のみを保持し、サイトBレプリカ（1票）とWitness（1票）の両方が利用できないため、クラスタクォーラムが失われ（50%未満）たためです。
C. サイトCのWitnessへのネットワーク接続を復旧することが、サイトAのVMのオブジェクトアクセスを復旧するための最速の運用経路です。
D. サイトAのローカルRAID-5ポリシールールはプライマリストレッチドクラスタのクォーラムを上書きできません。サイトレベルのコンポーネントとローカルコンポーネントの両方を評価する必要があります。
E. デュアルサイトミラーリングポリシーにより、サイトAがローカルRAID-5パリティブロックを使用して独立したクォーラムを維持できるため、オブジェクトは「可用性低下」(ABSENT状態)になっています。
正解: **B,C,D (**コメントを発表する**)**

質問: **39**
VCFアーキテクトがSDDCマネージャーAPIを使用して、大規模な「共有ウィットネス」トポロジをデプロイしています。
目標は、管理ドメインに配置された単一の大型Witness Applianceを使用して、40個の独立した2ノードvSAN ROBOクラスタをサポートすることです。
「」
# SDDCマネージャーAPI仕様
{
"witnessSpec": {

"hostname": "Shared-Witness-01",
サイズ: 特大
"max_components": 60000
},
"targetClusters": ["ROBO-01", "ROBO-02", ... "ROBO-40"] }
「」
以下の記述のうち、VCF共有ウィットネス機能のアーキテクチャ上の制約と機能を正確に説明しているのはどれですか？（該当するものをすべて選択してください。）
A. 1台の「Extra-Large」Shared Witnessアプライアンスは、最大64個の異なる2ノードクラスタをサポートし、最大64,000個のメタデータコンポーネントを1つのVMに統合できます。
B. Shared Witness は、標準的な 2 ノード ROBO 構成でのみサポートされており、完全な 3+3 ノードのストレッチ クラスタの Witness を統合するために使用することはできません。
C. CMMDSの互換性を維持するため、Shared Witnessにマッピングされた40個のROBOクラスタはすべて、まったく同じvSANアーキテクチャ（すべてOSAまたはすべてESA）と同一のESXiバージョンで実行されている必要があります。
D. Shared Witnessでは、オンプレミスのVCFデータストアではIOPS負荷をまとめてサポートできないため、SDDC ManagerがアプライアンスをAWS EC2インスタンスに直接デプロイする必要があります。
E. 単一の共有ウィットネスアプライアンスがクラッシュした場合、40 個の ROBO クラスターすべてが直ちにデータストア ロックアウトされ、エッジ VM にアクセスできなくなります。
正解: **(**正解を表示します**)**

質問: **40**
ネットワーク管理者が、クラスターA（サーバー）とクラスターB（クライアント）間のHCIメッシュ構成のトラブルシューティングを行っています。管理者はクラスターAのvSANデータストアをクラスターBにマウントしようとしますが、操作が失敗します。
管理者はvCenter上でSkyline Healthダッシュボードを確認します。
「」
[Skyline Health > vSAN > HCI Mesh]
確認事項 :リモートデータストアの接続性
ステータス：失敗
出典 :クラスターB（クライアント）
対象: vsanDatastore-Cluster-A
詳細 :16台のホストのうち2台がpingに失敗しました
チェック :MTUの均一性
ステータス：警告（不一致が検出されました）
「」
ヘルス出力とHCI Meshの要件に基づいて、このマウントエラーを解決するには、どの2つのアクションを実行すればよいでしょうか？（2つ選択してください。）
A. MTUの不一致を回避するために、クラスタBで使用される分散ポートグループでプロミスキャスモードを有効にします。
B. Cluster-B のすべてのホストが、vSAN ネットワーク経由で Cluster-A のすべてのホストに ping できることを確認します。
C. Cluster-AとCluster-BのvSANネットワーク間のL2/L3トランジットパス全体でMTU設定を標準化します。
D. HCI Meshは部分的なクラスタマウントをサポートしているため、障害が発生している2台のホストを一時的にクラスタBから切断してください。
正解: **(**正解を表示します**)**

質問: **41**
ネットワーク管理者が、新しく導入されたvSAN Witness ApplianceがStretched Cluster CMMDSネットワークに参加できないという問題のトラブルシューティングを行っています。
管理者はSSH経由でWitness Applianceのネットワークアダプタに問い合わせを行います。
「」

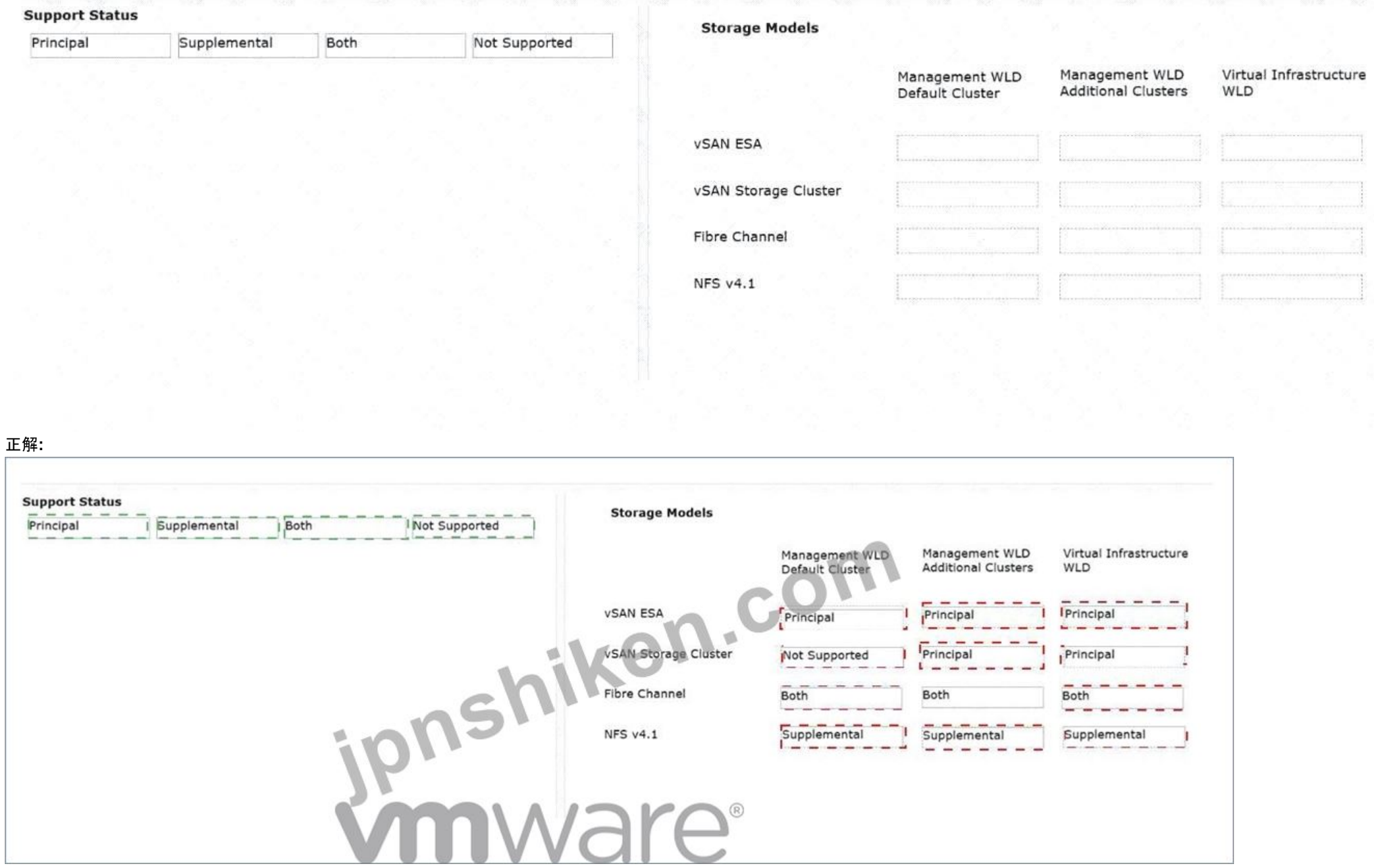
[root@witness-01:~] vim-cmd hostsvc/net/vnic_info
vmk0: 10.10.1.15 (トラフィック: 管理)
vmk1: 172.16.50.15 (トラフィック: vSAN Witness)
[root@witness-01:~] esxcfg-route -l
ネットワークネットマスクゲートウェイインターフェース
デフォルト 0.0.0.0 10.10.1.1 vmk0
「」
ESXiデータホストは192.168.100.0/24サブネット上に存在します。vmk1からデータホストへのpingは失敗します。
このネットワーク分断を引き起こしている、具体的に不足している設定は何ですか？
A. Witness Appliance は、ハートビートを処理するために、アクティブ/アクティブ LACP ボンドで構成された vSAN トラフィック用のデュアル vmk アダプタを必要とします。
B. ESXi データ ホストは、ゲートウェイをバイパスして vmk1 へのレイヤ 2 トンネルを確立するために、「vSAN Direct」で構成する必要があります。
C. 管理者が、Witness レプリケーションに必要な「vMotion」トラフィックタイプで vmk1 をタグ付けしませんでした。
D. 静的ルートがありません。vmk1 はデータ ホストとは異なるサブネットにあるため、Witness は vSAN トラフィックを vmk0 のデフォルト ゲートウェイ (管理) 経由でルーティングしようとしており、ネットワーク分離に違反しています。
正解: **(**正解を表示します**)**

質問: **42**
ソリューションアーキテクトは、高度なvSANデータ保護とストレージポリシーベース管理（SPBM）ルールを組み合わせた新しいVCFワークロードドメインを設計しています。
要件には以下が規定されている。
1. VMはFTT=2（RAID-6）でローカルに保護されている必要があります。
2. VMはRPO30でリモートクラスタにレプリケートされる必要がある。
分。
3. リモートサイト上の複製データは、5日間変更不可能でなければならない。
アーキテクトは、プロビジョニングを自動化するために、以下のSPBMポリシーを作成します。
「」
SPBM ポリシー: "Secure-DR-Policy"
【機能】
Host.FailuresToTolerate: 2 (RAID-6)
データ保護.リモートターゲット: "DR-Cluster-02"
データ保護RPO :30分
データ保護。不変性: 有効
データ保護。保持期間 :5日間
「」
vCenterとvSANの統合では、この複雑なポリシーのインスタンス化とライフサイクルはどのように処理されますか？（該当するものをすべて選択してください。）
A. VM にこのポリシーが割り当てられると、vCenter は vSAN データ保護インターフェイスで対応するローカルおよびリモート保護グループを自動的に作成します。
B. ユーザーが5日間の保持期間より前にスナップショットを手動で削除しようとすると、vSAN DOMは不変性フラグのためにAPI呼び出しを拒否します。
C. リモートサイトで不変性を実現するには、「DR-Cluster-02」をAWS S3オブジェクトロックゲートウェイで構成する必要があります。ローカルのvSANデータストアでは、時間ベースの保持ロックを強制できないためです。

D. Host.FailuresToTolerate: 2 (RAID-6) ルールは、ソースサイトで実行中の VM とリモートサイトで複製されたスナップショット オブジェクトの両方に適用されます。ただし、リモート サイトに 6 台以上のホストがある場合に限ります。
正解: **(**正解を表示します**)**

質問: **43**
VCFアーキテクトが、Dell ReadyNodesを使用した大規模な48ノードのvSAN ESAクラスタ向けに、自動化されたライフサイクル管理（LCM）ワークフローを設計している。
この設計では、vSphere Lifecycle Manager (vLCM) と OpenManage Integration for VMware vCenter (OMIVV) のハードウェアサポートマネージャ (HSM) を統合しています。
「」
# vLCMクラスタイメージJSON仕様
"画像" :{
"esx_version": "8.0 U2",
"vendor_addon": "Dell_Customization",
"hsm_package": "OMIVV_Firmware_Baseline_v4"
}
「」
vCenter HCLデータベースは、この自動化されたvLCMファームウェア修復ループとどのように連携するのでしょうか？
（該当するものをすべて選択してください。）
A. ハードウェア サポート マネージャーが存在する場合、vLCM は vSAN HCL データベースを完全に無視し、OEM ベンダーの内部認証マトリックスのみに依存します。
B. イメージを適用する前に、vLCM はアクティブな vSAN HCL データベースにクエリを実行して、「OMIVV Baseline」に含まれる特定の NVMe ファームウェアが vSAN ESA 8.0 U2 用に正式に認定されていることを検証します。
C. この統合には、OMIVVハードウェアマネージャがRAIDコントローラ構成を完全に制御できるように、vSANヘルスサービスを無効にする必要があります。
D. vCenter 内の HCL データベースを更新すると、次の標準メンテナンス期間中に新しいファームウェアが物理 Dell サーバーに自動的にフラッシュされます。
E. HCLデータベースがHSMファームウェアのベースラインに互換性がないと判断した場合、SDDCマネージャーのコンプライアンス事前チェックは、ストレージプールの破損を防ぐために修復タスクをブロックします。
正解: **(**正解を表示します**)**

質問: **44**
あるアーキテクトが、VMware Cloud Foundation (VCF) プライベートクラウドにおける自動インストールでどのタイプのドメインでどのストレージプラットフォームがサポートされているかをクライアントに説明しています。
左側の各ストレージモデルのサポートステータスを、右側の各ワークロードドメインにドラッグアンドドロップしてください。



正解:

Explanation:

Storage Model	Management WLD Default Cluster	Management WLD Additional Clusters	Virtual Infrastructure WLD
vSAN ESA	Principal	Principal	Principal
vSAN Storage Cluster	Not Supported	Principal	Principal
Fibre Channel	Both	Both	Both
NFS v4.1	Supplemental	Supplemental	Supplemental

正しいマッピングは、VCF 9.0 のプリンシパルおよび補助ストレージ モデルに基づいています。vSAN ESA は、管理ドメインのデフォルト クラスタ、管理ドメインの追加クラスタ、および VI ワークロード ドメインのプリンシパル ストレージとしてサポートされています。vSAN ストレージ クラスタは、初期管理クラスタに標準のプリンシパル ストレージ モデルが必要なため、管理ドメインのデフォルト クラスタではサポートされていませんが、管理ドメインの追加クラスタおよび VI ワークロード ドメインのプリンシパル ストレージとしてはサポートされています。ファイバー チャネルは、3 つのドメインまたはクラスタ カテゴリすべてにおいて、プリンシパル ストレージと補助ストレージの両方としてサポートされており、初期クラスタの作成または後からのデータ ストア拡張が可能です。NFS v4.1 は、これらのカテゴリ全体で補助ストレージとしてのみ使用できます。NFS は、NFS v3 を使用する場合にのみプリンシパルとして使用できます。NFS v4.1 は、ドメインまたはクラスタが作成された後、補助ストレージとして使用されます。これらのステータスは、ワークロード ドメインまたはクラスタの作成中に使用されるプリンシパル ストレージと、ワークロードまたは静止データのユース ケースのために作成後に追加される補助ストレージとの VCF の区別と一致しています。参照トピック :ストレージモデル、プライマリストレージ、補助ストレージ、vSAN ESA、ストレージクラスタ、ファイバーチャネル、NFS。

質問: **45**

VI管理者は、新しくデプロイされたVCF 9.0ワークロードドメイン上で、vSAN Express Storage Architecture（ESA）を実行する40TBの仮想マシンを作成します。

「」

[ストレージポリシールールセット: Tier1-データベース]

許容可能な障害数: 2 (RAID-6)

イレイジャーコーディング：有効

「」

ESAのI/Oパイプラインは、標準的な書き込み操作をOSAとどのように異なる方法で処理するのでしょうか？特に「RAID-6書き込みペナルティ」に関して教えてください。

A. ESAでは、RAID-6ワークロードのDOMレイヤーをバイパスするために、VMDKを物理的なRaw Device Mapping（RDM）として構成する必要があります。

B. OSAは、新しいパリティを計算するために古いデータを読み取る必要があるため、RAID-6では「読み取り-変更-書き込み」のペナルティが非常に大きくなります。ESAはログ構造の「追記専用」アーキテクチャを採用しており、古いブロックを読み取ることなく新しいデータを新しいブロックに即座に書き込むため、RAID-6ポリシーはRAID-1と全く同じ書き込みパフォーマンスを実現します。

C. ESAは標準NVMeバッファを無効にし、hostdエージェントを使用してRAID-6データを物理ストレージプールに直接書き込みますが、OSAはVMkernel SCSIスタックを使用します。

D. OSAはパリティ計算をキャッシュSSDにオフロードすることでRAID-6を効率的に処理しますが、ESAはホストCPUを使用せざるを得ず、新たなボトルネックが発生します。

正解: **(正解を表示します)**

質問: **46**

管理者は、災害からサイトを保護し、フェイルオーバー後にも再度保護したいと考えています。業界規制では、プライマリサイトを6か月ごとに変更することが義務付けられています。

この要件を満たすために、在庫マッピング時および復旧計画実行時に必要なオプションはどれですか？（2つ選択してください。）

A. フェイルオーバーが成功したら、vSANデータ保護を再構成して逆方向のレプリケーションを実行します。

B. 在庫マッピング作成時に「逆マッピングの準備」を使用します。

C. テスト復旧計画を使用する。

D. フェイルオーバーが成功したら、VMware Live Site Recovery から再度保護します。
E. 両サイト間のネットワークを拡張します。
正解: **(**正解を表示します**)**
要件は、プライマリ サイトを 6 か月ごとに交代することであり、フェイルオーバー後に保護方向を反転できる災害復旧設計が必要です。インベントリ マッピングは、コンピューティング リソース、フォルダー、ネットワーク、データ ストアなどのリソースが保護サイトとリカバリ サイト間でどのようにマッピングされるかを定義します。インベントリ マッピングの作成時に 「逆マッピングの準備」を使用すると、リカバリ サイトが後で保護サイトになったときに同じマッピング構造が使用できることが保証されます。フェイルオーバーまたは計画された移行が成功した後、VMware Live Site Recovery は再保護操作を使用して保護関係を反転します。これにより、以前にリカバリされたサイトが新しい保護ソースになり、フェイルバックまたは次のスケジュールされたサイト ローテーションのレプリケーション プランとリカバリ プランが準備されます。テスト リカバリ プランは、プライマリ サイトを変更せずにリカバリを検証します。ネットワークを拡張するとワークロード モビリティが簡素化されますが、再保護には必須ではありません。vSAN Data Protection を手動で再構成することは、保護サイトとリカバリ サイトの役割を反転するための Live Site Recovery ワークフローではありません。参照トピック: VMware Live Site Recovery、インベントリ マッピング、逆マッピング、リカバリ プラン、再保護。

質問: **47**
VCFデプロイメントスペシャリストは、ホストのNVMeキャッシュドライブに十分な余裕があるにもかかわらず、vSAN OSAクラスタ上に新しくプロビジョニングされたファイルサーバーのIOPSが正確に5,000に制限されている理由を調査しています。
専門家は、VMDKに関連付けられているアクティブなストレージポリシーを確認します。
「」
SPBM 設定
名前: VDI制限ポリシー
機能:
許容可能な障害数: 1 (RAID-1)
ストライプ幅: 2
IOPS制限: 5000
強制プロビジョニング: False
「」
vSANのトラブルシューティング方法によると、この特定のSPBM構成はどのようにして機械的に制限を適用しているのでしょうか？また、VMがその制限に達しているかどうかを確認するには、専門家はどこを調べればよいでしょうか？
（2つ選択してください。）
A. IOPS制限は、ゲストOS内のvSCSIレイヤーで厳密に適用されるサービス品質（QoS）しきい値として機能します。
B. StripeWidth: 2 ルールは 5,000 IOPS の制限を 2 つのホストに分割するため、各ホストは実質的に 2,500 IOPS に制限されます。
C. IOPS制限はvSAN DOMクライアント層（VMが存在するホスト上）で適用され、vSANネットワークに入るI/Oを意図的に遅延（スロットリング）します。
D. 専門家は、vCenter の 「DOM Client」レイテンシチャートを確認することで、このボトルネックを確認できます。IOPS 制限は、対応するバックエンド ネットワークや LSOM レイテンシがないにもかかわらず、DOM Client で人為的に高いレイテンシとして現れます。
正解: **(**正解を表示します**)**

質問: **48**
L3サポートエンジニアがvSANクラスタのホストコンポーネント制限アラートのトラブルシューティングを行っています。
1.8 TBのVMDKファイルから8つの物理コンポーネントが生成されました。
エンジニアはesxcliを使用してオブジェクトの状態とポリシーを照会します。
「」
[root@esx-04:~] esxcli vsan debug object list -u 5543...
ポリシー: FTT=0 (冗長性なし)、StripeWidth=1
サイズ :1800GB
木 :
コンポーネント 1: 連結 (esx-04)
...
コンポーネント 8: 連結 (esx-04)
「」
ポリシーでストライピングとミラーリングが明示的に無効になっているにもかかわらず、vSAN分散オブジェクトマネージャ（DOM）はなぜこの1.8TBのオブジェクトを同じホスト上の8つの連結されたコンポーネントに分割したのでしょうか？
A. vSANは物理コンポーネントごとに255GBという厳密なアーキテクチャ上の制限を設けています。
255 GB は自動的に 255 GB のチャンクに連結され、1.8 TB オブジェクトに対して約 8 つのコンポーネントが生成されます (1800 / 255 ≈ 7.05)。
B. ホストの連続したブロック領域が不足したため、vSAN はオブジェクトを断片化せざるを得なくなりました。
C. ESXi CPU は、重複排除ハッシュの衝突を処理するために追加のコンポーネントを自動的に生成しました。
D. NVMeドライブのセクターサイズは255GBで、ハードウェアの制限に合致しています。
正解: **A** (コメントを発表する)

質問: **49**
VI管理者は、3ノードvSANクラスタを6ノードvSANクラスタに拡張する計画を立てています。3ノードクラスタは現在、「ホスト再構築リザーブ」の厳格なしきい値のため、ほぼ最大安全容量で稼働しています。
「」
[ログ抜粋: vmkernel.log - Capacity Daemon]
2026-11-20T10:00:00Z WARN vsan-dom - ホスト再構築リザーブがアクティブです: 生容量の 33% がロックされています。
2026-11-20T12:00:00Z INFO vpxd - クラスタ拡張が完了しました。ホスト数: 6。
2026-11-20T12:05:00Z INFO vsan-dom - ホスト再構築予約が再計算されました: [？]%
「」
クラスターの物理的な拡張は、「ホスト再構築リザーブ」の割合を数学的にどのように変化させるのか、また、使用可能なVM容量に直接どのような影響を与えるのか？
A. ログによると、分散リソーススケジューラ (DRS) が 4 ノードのしきい値を超える容量割り当てを処理するため、ホスト再構築リザーブは 6 ノードに達すると自動的に無効になります。
B. FTT=1ストレージポリシーに準拠するため、予備率は33%に固定されています。つまり、使用可能な容量は線形に増加しますが、オーバーヘッドは高いままです。
C. 6ノードクラスタは本質的にデュアルホスト障害の統計的リスクが高いため、予備率を50%に引き上げます。
D. 必要な予備容量の割合が自動的に33%から約16%に減少します。これにより、元のホスト上で以前に「ロック」されていたストレージの大部分が、使用可能なVM容量プールに解放されます。
正解: **D** (コメントを発表する)

質問: **50**

管理者は、既存のVMware Cloud Foundation（VCF）ワークロードドメインに補助ストレージを追加する作業を任されました。この補助ストレージは、本番稼働中のワークロードに使用されるメインストレージに影響を与えることなく、バックアップデータとISOイメージの容量を増強します。
管理者は、要件を満たすためにどのようなことを推奨すべきでしょうか？
A. 管理ドメインのストレージを新しいクラスタに移行します。
B. VMFSのプライマリストレージの割り当てを増やします。
C. 追加のNFSボリュームまたはiSCSIデータストアを接続します。
D. 既存のデータストアをすべてNVMeデバイスに置き換えます。
正解: **(**正解を表示します**)**
補助ストレージは、プライマリストレージが既に展開された後に、既存のワークロードドメインまたはクラスタにストレージ容量を追加することを目的としています。プライマリストレージは、ワークロードドメインまたはクラスタの作成時に使用されるデータストアであり、通常は稼働中のワークロードの配置に使用されます。補助ストレージは、追加のワークロード、テンプレート、ISOイメージ、バックアップデータ、またはその他の保存データの要件のために後から追加できます。このシナリオでは、管理者は、本番ワークロードに使用されるプライマリストレージを変更または影響を与えることなく、バックアップデータとISOイメージ用の追加容量を特に必要とします。追加のNFSボリュームまたはiSCSIデータストアを接続すると、両方ともVCFの補助ストレージオプションとして使用できるため、この要件を満たします。管理ドメインストレージの移行は無関係であり、不要です。既存のVMFSプライマリストレージの割り当てを増やしても、本番ストレージとバックアップまたはISOストレージ間の要求された分離は提供されません。既存のすべてのデータストアをNVMeデバイスに置き換えると、混乱が生じ、補助ストレージの使用例に合致しません。参照トピック: プライマリストレージ、補助ストレージ、NFS補助ストレージ、iSCSI補助ストレージ、Day-2ストレージ拡張。

質問: **51**
VCF導入スペシャリストが、大規模な複数拠点にわたる災害復旧要件をサポートするために、VCF 9.0向けのvSAN ESAストレッチドクラスタのサイジングを行っています。
「」
[SDDCマネージャー - ワークロードドメイン構成]
トポロジー: ストレッチドクラスター
証人：専用証人装置（第三サイト）
最大対応スケール: [？]
「」
標準のvSAN 8.0/9.0ストレッチドクラスタトポロジーで公式にサポートされている最大スケール制限は何ですか？（該当するものをすべて選択してください。）
A. ストレッチドクラスタトポロジーでは、クラスタごとに最大 1 つのアクティブな Witness Appliance がサポートされます。
B. ストレッチドクラスタには、vSphere Enterprise Plus および vSAN Advanced ライセンスが必須です。vSAN Standard では不十分です。
C. 同期書き込みI/O操作をサポートするため、優先サイトとセカンダリサイト間の最大RTT（ラウンドトリップタイム）ネットワーク遅延は厳密に5ミリ秒です。
D. ストレッチドクラスタの最大サイズは合計60台のデータホストで、優先サイトに30台、セカンダリサイトに30台のホストが均等に配置されます。
E. 単一のストレッチドクラスタでは、60台のホストのメタデータ負荷を処理するために、最低でも2台の独立したWitness Appliance（各サイトに1台ずつ）が必要です。
正解: **(**正解を表示します**)**

質問: **52**
VI 管理者は、VCF 9.0 環境に開発者ネームスペースをデプロイしています。開発者は CI/CD パイプラインで Kubernetes Persistent Volume スナップショットを多用しています。彼らはしばしば最大で1ボリュームあたり1日50枚のスナップショット。
管理者はデバッグコマンドを実行して、使用頻度の高いvSAN ESAボリュームのスナップショットツリーを検査します。
「」
[root@esx-03:~] esxcli vsan debug object health summary get
オブジェクトUUID: 554350... (FCD: Dev-DB-PVC)

フォーマット: vSAN ESA ログ構造化
スナップショット数 :45
読み取り遅延: 0.8 ms
「」
vSAN ESAのメカニズムとスナップショットアーキテクチャモデルの高度な融合は、従来のOSA VMFS方式と比較して、このワークロードの効率的な動作をどのように可能にするのでしょうか？（該当するものをすべて選択してください。）
A. 従来のOSA（VMFS）では、スナップショットは『リドゥログ」（Esparse）を利用します。45個のスナップショットを持つVMからデータを読み取るには、I/Oが45層の深いディスクチェーンをたどる必要があり、深刻なレイテンシの低下を引き起こします。
B. vSAN ESA ネイティブ スナップショットは、ログ構造化 B ツリー ポインタ メカニズムを利用します。スナップショットのキャプチャは、セカンダリ デルタ ファイルを作成しない、ミリ秒単位のメタデータ操作です。
C. OSA で 45 個のスナップショット チェーンを削除または統合すると、ブロック データをマージするための大規模な「VM Stun」イベントがトリガーされますが、ESA ではバックグラウンドで B-Tree ポインタをドロップすることでスナップショットが即座に削除されます。
D. ESAスナップショットでは、Bツリーマップ全体でメモリ状態の一貫性を確保するために、作成中に仮想マシンの電源をオフにする必要があります。
E. vSAN ESA では、オブジェクトごとにサポートされるスナップショットの最大制限が 32 (OSA の場合) から 200 に増加し、継続的データ保護 (CDP) スタイルのワークフローが可能になります。
正解: **(**正解を表示します**)**

質問: **53**
ある企業は、既存のVMware Cloud Foundation（VCF）プライベートクラウドワークロードドメインに、vSAN ESA対応の新しいクラスタをデプロイすることを計画しています。以下の要件が提示されています。
ホストあたり2台の4TB NVMeディスク
* デプロイされたすべての仮想マシンに対してFTT=1/RAID-5
* 予想される重複排除/圧縮率 = 1.5 (50%)
* 障害発生時にホストを完全に再構築できるだけの十分な容量を確保する（ホスト再構築予約）
* 運用準備金10%
* ファイルシステム、オブジェクトなどにかかるオーバーヘッドは25%と想定されます。
最低使用可能容量12TBを満たすには、何台のホストが必要ですか？
A. 6人のホスト
B. ホスト3名
C. ホスト4名
D. 5人のホスト
正解: **(**正解を表示します**)**
保護ポリシー、データ削減、予備容量、およびオーバーヘッドを適用した後、12 TB の使用可能容量要件を満たすには 4 台のホストが必要です。各ホストは 2 台の 4 TB NVMe デバイスから 8 TB の生容量を提供します。3 台のホストは 24 TB の生容量を提供しますが、ホスト再構築予備容量、10% の運用予備容量、RAID-5 保護オーバーヘッド、および 25% のファイルシステム/オブジェクトオーバーヘッドを考慮すると、残りの実効使用可能容量は必要な 12 TB の目標を下回ります。4 台のホストは 32 TB の生容量を提供します。vSAN ESA と FTT=1/RAID-5 では、vSAN はイレイジャー コーディングを使用してミラーリングと比較して容量効率を向上させます。vSAN サイジング ガイダンスでは、FTT=1 の RAID-5 では、他の予備容量とオーバーヘッドを除いて、使用可能容量の約 75% を提供するとされています。ホスト障害後にコンポーネントを再構築するためにクラスタに十分な空き容量があるように、ホスト再構築予備容量も計画する必要があります。想定されるデータ削減率1.5と必要な予備容量を適用した後、4台のホストで十分な使用可能容量が得られますが、3台のホストでは不十分です。参照トピック :vSAN ESA容量サイジング、RAID-5イレイジャーコーディング、ホスト再構築予備容量、運用予備容量、vSANオブジェクトオーバーヘッド。

質問: **54**

管理者は、プライマリストレージとしてvSANを使用するように構成されたVMware Cloud Foundation（VCF）ワークロードドメインで作業を行っています。管理者は、そのvSANをバックエンドストレージとして、ドメイン内の複数のクラスター（OSAとESAが混在）にわたってテナントVMをホストするためのデータストアクラスターを作成および構成したいと考えています。
管理者は何を考慮すべきでしょうか？
A. vSAN OSAおよびESAベースのデータストアは、データストアクラスタタグに追加してから、単一のストレージポリシーの一部として選択する必要があります。
B. データストアクラスタは、vSAN、FC、NFSデータストアなど、異なるストレージタイプを組み合わせることができます。ただし、それらが同じvCenter内にある場合に限ります。Storage DRSはそれらを均一に扱います。
C. vSANデータストアを使用する場合、データストアクラスタはサポートされません。各VMはvSANデータストア上に手動で配置する必要があります。
D. vSANを基盤となるデータストアとして使用する場合、管理者はvCenter APIを介してデータストアクラスタを作成し、vSANデータストアを含め、Storage DRSを有効にし、VMストレージポリシーが適切なvSAN対応データストアを参照していることを確認する必要があります。
正解: **C** (コメントを発表する)

質問: **55**
管理者は、VMware Cloud Foundation（VCF）プライベートクラウドの管理を担当します。
環境に関する以下の情報が提供されています。
* 顧客データセンターは、サイトA、サイトB、サイトCの3か所あります。
* サイトAのデータセンターは、すべての本番サービスを稼働させています。
* サイトBのデータセンターは容量が上限に達しており、追加の物理ハードウェアを設置するスペースがありません。
* サイトCのデータセンターは、将来の需要に対応できるラック容量と電力容量がより大きいため、サイトBの代替として稼働を開始しました。
管理者は、以下の要件を満たす新しいVMware vSAN Stretched Clusterのネットワーク要件を特定する任務を負っています。
* このソリューションでは、VMware vSAN Stretched Clusterを構築するために、合計10台の新しいESXホストサーバーを導入します。
* ソリューションは、スパニングツリープロトコル（STP）の問題による影響を最小限に抑えるために、適切なネットワーク構成を導入する必要があります。
適切なvSANサイトタイプ、ネットワークタイプ、およびラウンドトリップレイテンシ（RTT）を所定のボックスにドラッグアンドドロップして、高レベル図を完成させてください。

vSAN Site

Witness Site	Data Site	Single Site

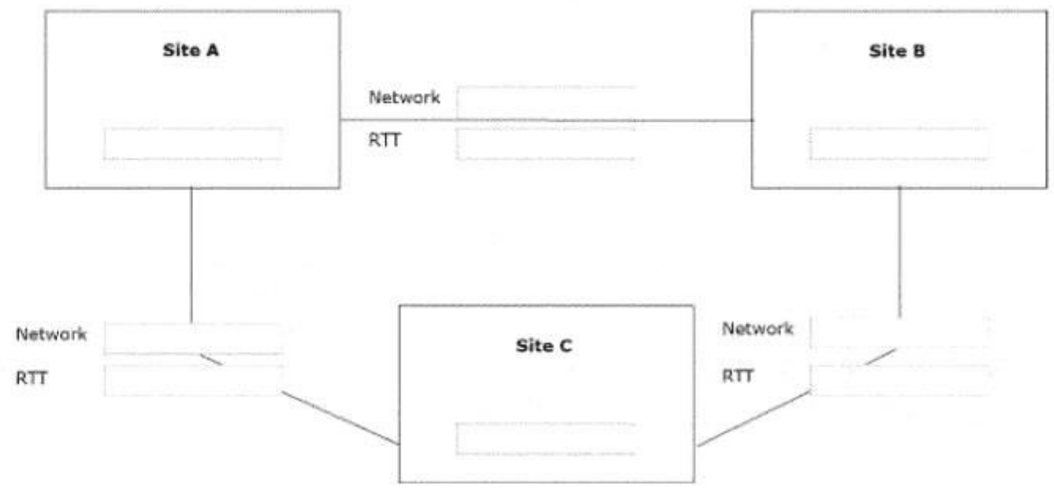
Network Type

Layer 2	Layer 3	Stretched Layer 2

Minimum Latency / Round Trip Time (RTT)

< 5 ms	< 200 ms	< 500 ms

Answer Area



正解:

vSAN Site

Witness Site	Data Site	Single Site

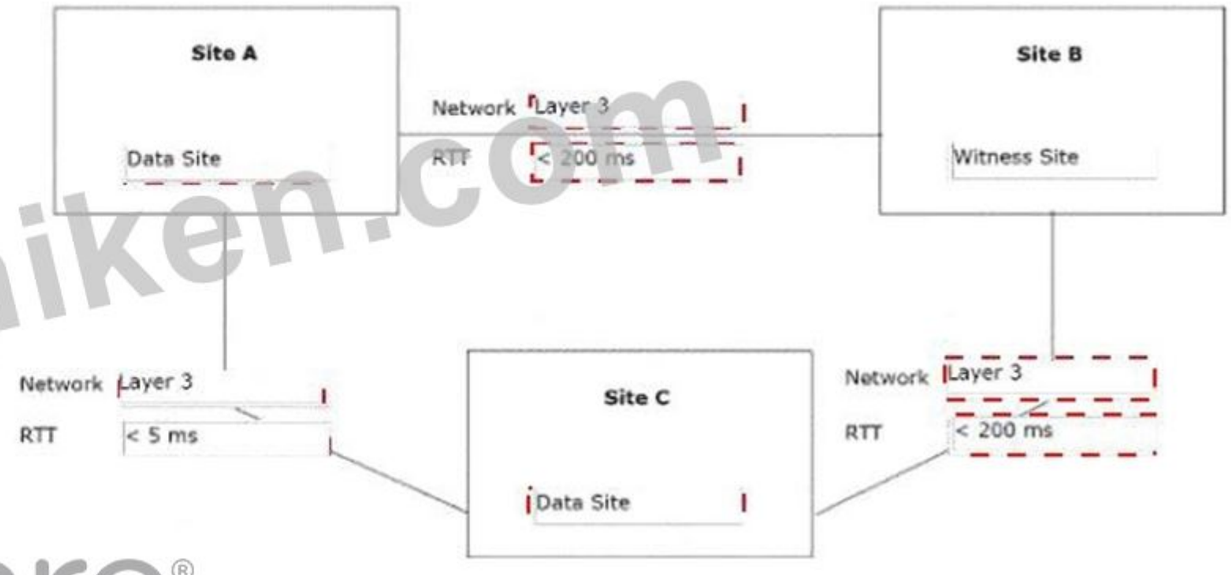
Network Type

Layer 2	Layer 3	Stretched Layer 2

Minimum Latency / Round Trip Time (RTT)

< 5 ms	< 200 ms	< 500 ms

Answer Area



Explanation:
サイト A = データ サイト、サイト B = ウィットネス サイト、サイト C = データ サイト、サイト A # サイト C = レイヤ 3、RTT < 5 ms、サイト A # サイト B = レイヤ 3、RTT < 200 ms、サイト B # サイト C = レイヤ 3、RTT < 200 ms。サイト A とサイト C は、サイト A が本番サービスをホストし、サイト C が容量制約のあるサイト B の代替として導入されたため、データ サイトとして使用されます。サイト B は、追加の物理ホストのためのスペースがなく、vSAN ウィットネス アプライアンスがワークロード VM を実行しないため、ウィットネス サイトとして使用されます。vSAN ストレッチ クラスタでは、データ ノード用に 2 つの可用性ゾーンと、ウィットネス アプライアンス用に 3 番目のサイトが必要です。データ サイト間の接続は同期 vSAN データ トラフィックを伝送し、5 ms 未満の RTT を満たす必要があります。ウィットネス サイトはメタデータ トラフィックのみを伝送するため、データ サイトとウィットネス リンクはより高いレイテンシをサポートし、サイトごとに最大 10 台のホストに対して 200 ms 未満の RTT が必要です。
要件ではSTPによる障害を最小限に抑えることが特に求められているため、サイト間のネットワークタイプとしてはレイヤ3が推奨されます。VMwareは、レイヤ3を使用することで、制約のあるウィットネスリンクなど、望ましくないリンクを介してSTPがトラフィックをリダイレクトするのを回避できると述べています。参考資料 :vSANストレッチドクラスタネットワーク設計、データサイトとウィットネスサイトの配置、レイヤ3の推奨事項、RTT要件。

質問**: 56**
VCF導入スペシャリストが、2つの異なるVCFドメイン（ドメインA（重複排除が有効になっているvSAN OSA）とドメインB（vSAN ESA））における局所的な物理ドライブ障害を調査しています。
どちらのドメインにおいても、容量3.84TBのSSD/NVMeドライブ1台が「永久的なデバイス損失」（PDL）に見舞われた。
「」
[RVC出力: vsan.disks_stats ドメインA (OSA)]
失敗: naa.500A... (容量ティア)
[RVC出力: vsan.disks_stats ドメインB (ESA)]
失敗: naa.500B... (ストレージプール)
「」
重複排除のアーキテクチャ実装とファイルシステム構造に基づいて、これらの環境における障害発生範囲を正確に比較できる記述はどれですか？ 2つ選択してください。）
A. 重複排除ポインタがグループ内の残りの容量ドライブに自動的に再マッピングされるため、ネットワークの再同期を必要とせずに、ドメイン A (OSA) の再構築が速くなります。
B. ログ構造ファイルシステムでは単一のNVMe障害を分離できないため、ドメインB（ESA）はホスト全体の障害に見舞われます。
C. 重複排除状態は ESXi RAM 内で独立して維持されるため、両方のアーキテクチャでまったく同じ障害領域 (3.84 TB の損失) が発生します。
D. ドメイン A (OSA) では、重複排除ディスク グループ内の単一の容量ドライブが失われると、重複排除ハッシュ テーブル全体が無効になります。vSAN はディスク グループ全体 (キャッシュおよび他のすべての正常な容量ドライブを含む) を障害状態にし、ネットワーク全体でデータを再構築する必要があります。
E. ドメイン B (ESA) では、重複排除が排除され、ストレージ プールがフラットであるため、単一の NVMe ドライブの損失は、その特定のドライブに物理的に保存されているコンポーネントのみに影響し、他のドライブはアクティブなままです。
正解**: (**正解を表示します**)**

質問**: 57**
ストレージ管理者が、暗号化されたvSANクラスタ内のホスト（esx-07）をメンテナンスのために再起動しようとします。しかし、ホストは再起動後にクラスタに再参加できません。
管理者はesx-07上のローカルCLIを確認します。
「」
[root@esx-07:~] vim-cmd hostsvc/storage/fs_info
データストア: vsanDatastore (アクセス不可)
[root@esx-07:~] esxcli vsan encryption info get
鍵暗号化キー（KEK）の状態：未ロード
KMS接続ステータス：失敗（証明書無効です）

「」
vim-cmdとesxcliの出力に基づいて、ホストがvSANデータストアをマウントできない原因となっている信頼チェーンの具体的な障害は何ですか？
A. 再起動中にローカルディスク暗号化キー (DEK) が安全に消去されたため、ディープリキーが必要です。
B. ESXi ホストの KMIP 接続に使用されているローカル SSL 証明書が無効または期限切れのため、ホストが KMS サーバーから KEK を直接取得できません。
C. vCenter Server の証明書の有効期限が切れたため、ホストは物理ドライブのロック解除に必要なキー暗号化キー (KEK) をダウンロードできません。
D. ホストのCPUには、暗号化キーを処理するために必要なAES-NI命令セットがありません。
正解: **C** (コメントを発表する)

質問: **58**
VCFアーキテクトが、従来のSANからvSAN ESAへの移行を検討している顧客に対し、vSANオブジェクトの仕組みとストレージポリシーベース管理（SPBM）の緊密な統合について説明している。
クライアントは、10TBのファイルサーバーにFTT=2（RAID-6）構成を使用したいと考えています。
「」
SPBM ポリシー: "File-Server-R6"
許容障害数: 2件 - RAID-6（イレイジャーコーディング）
ストライプ幅: 1
vSANアーキテクチャ: ESA（アダプティブRAID-5/6）
「」
vSAN分散オブジェクトマネージャ（DOM）は、このSPBMポリシーを実際のコンポーネントレイアウトにどのように変換するのでしょうか？また、コンポーネントに障害が発生した場合はどうなりますか？（該当するものをすべて選択してください。）
A. 6台のホストのうち1台が故障した場合、オブジェクトは「可用性低下」状態になりますが、残りの5台のコンポーネントがクォーラムの50%以上を占めているため、I/Oは継続されます。
B. コンポーネントの最大サイズが255GBに制限されているため、10TBのオブジェクトは自動的に約60個の個別のコンポーネント（約40個のデータ + 20個のパリティ）に分割されます。
C. DOMは、10 TBのVMDKオブジェクトを、少なくとも4つのデータコンポーネントと2つのパリティコンポーネント（4+2 RAID-6レイアウト）に分割し、最低6台の物理ESXiホストに分散します。
D. 監視アプライアンスは、障害発生時にFTT=2準拠を維持するために、障害が発生したコンポーネントのペイロードデータを自動的に取り込みます。
E. ESA の RAID-6 は分散パリティ機構を使用するため、専用の「パリティ ドライブ」ホストは存在せず、パリティ コンポーネントは 6 つの障害ドメインすべてにわたってローテーションされます。
正解: (正解を表示します)

質問: **59**
VCFデプロイメントスペシャリストが、SDDCマネージャーAPIを介して、既存の100TB NFS v3 NASアレイを新しいVIワークロードドメインに統合しています。
専門家は、クラスター作成用のJSONペイロードを準備します。
「」
# SDDCマネージャーAPIペイロード（NFS補助ストレージ）
{
"clusterName": "Legacy-NAS-Cluster",
"datastoreSpec": {
"datastoreType": "NFS",
"nfsSpec": {
"serverName": "192.168.100.50",
"shareName": "/vol/archive_data",
「読み取り専用」: false

}
},
"hostSpecs": [...]
}
「」
VCF自動化ライフサイクルにおけるこのNFSデータストアの運用上の役割と制限を正確に定義しているのは、次のうちどれですか？
A. ここで使用されている NFS v3 プロトコルは、ネイティブのアレイベースのオブジェクト暗号化を提供し、SDDC Manager はこれを KMS クラスタに採用します。
B. SDDC Manager は、NFS マウント上でストレージ I/O コントロール (SIOC) を自動的に構成し、10GbE ネットワークが飽和状態にならないようにします。
C. VCF は、vLCM パッチ適用ルーチンに含めるために、外部 NAS オペレーティングシステムに vsan-mgmt エージェントをインストールします。
D. NFSデータストアはVCFでは厳密に「補助ストレージ」として機能し、vSANやFC/vVolsなどの主要ストレージ標準を必要とする管理ドメインvCenter ServerやNSXコントローラをホストするために使用することはできません。
正解: **(**正解を表示します**)**

質問: **60**
VCFアーキテクトは、SDDCマネージャーを使用して、vSANストレッチドクラスタとして即座に構成されるVIワークロードドメインを作成しています。
これを実現するには、アーキテクトはベースラインワークロードドメインの作成を、特定のストレッチドクラスタネットワークの前提条件と調整する必要があります。アーキテクトは準備された構成を確認します。
「」
[ネットワーク設定 - WLD-03]
vSANネットワークセグメント（サイトA）: 192.168.10.0/24（MTU 9000）
vSANネットワークセグメント（サイトB）: 192.168.20.0/24（MTU 9000）
監視ネットワークセグメント: 192.168.100.0/24 (MTU 1500)
静的ルート: サイトA/BのvSANネットワーク <-> ウィットネスネットワーク
ライセンス: vSAN Enterprise適用済み
「」
SDDC Managerワークフローをストレッチドクラスタ展開に正常に統合するために、以下のアクションと構成のうちどれが必要ですか？（該当するものをすべて選択してください。）
A. ワークロードドメイン作成ウィザードを実行する前に、Witness ApplianceをインポートしてSDDC Managerインベントリに登録する必要があります。
B. ワークロード ドメインの作成時に割り当てられる vSAN ライセンスは、ストレッチ クラスタ トポロジをサポートするために「vSAN Enterprise」以上である必要があります。
C. VIワークロードドメインは、まずSDDCマネージャーで標準のシングルサイトクラスタとしてデプロイされてから、day-2オペレーションによってストレッチドクラスタに変換する必要があります。
D. vSANネットワークセグメント（サイトB）は、サイトAとは別のレイヤ2 VLANに配置する必要があります。つまり、サイト間vSAN通信のためにホスト上で静的ルートを設定する必要があります。
正解: **B,C,D (**コメントを発表する**)**

質問: **61**
VCFデプロイメントスペシャリストが、新しいTanzu Kubernetes Grid（TKG）クラスタを構成しています。開発者は、「K8s-Gold-Policy」という名前の既存のSPBMポリシーを使用してvSANデータストア上にボリュームをプロビジョニングするStorageClassを必要としています。
「」
Kubernetes StorageClass の定義
apiVersion: storage.k8s.io/v1
種類: ストレージクラス

メタデータ:
名前: vsan-gold-sc
手数料 :csi.vsphere.vmware.com
パラメータ:
[？] : "K8s-Gold-Policy"
reclaimPolicy: 削除
volumeBindingMode: WaitForFirstConsumer
「」
この StorageClass を vSphere ストレージ ポリシーに正しくバインドするには、[？] プレースホルダーにどのパラメータ キーを挿入する必要がありますか？
A. vmfs.policy.id
B. データストア名
C. ストレージポリシー名
D. vsan.spbm.policy
正解: **C (**コメントを発表する**)**

質問: **62**
「ファーストクラスディスク」（FCD）と従来のvSphere仮想マシンディスク（VMDK）のアーキテクチャ上の違いを正確に定義しているのは、次のうちどれですか？
A. FCD は物理的な NVMe 名前空間にのみプロビジョニングされますが、従来の VMDK は VMFS ブロック ストレージにプロビジョニングされます。
B. FCD は vCenter における第一級の名前付きオブジェクトであり、独自の独立したライフサイクルと ID を持ち、特定の仮想マシンから切り離されています。
C. FCD は、I/O ルーティングに vSAN 分散オブジェクトマネージャ (DOM) を使用せず、コンテナストレージインターフェイス (CSI) を直接使用します。
D. 従来の VMDK はストレージ ポリシーベース管理 (SPBM) をサポートしていますが、FCD は冗長性ルールに Kubernetes StorageClass に依存しています。
正解: **(**正解を表示します**)**

質問: **63**
L3サポートエンジニアが、VCFワークロードドメイン内のvSAN ESAホスト上で故障したNVMeドライブを交換している。
エンジニアは、故障したドライブを新品のエンタープライズグレードの7.68TB NVMeデバイスと物理的に交換します。しかし、SDDC ManagerとvCenterは、そのドライブをvSANストレージプールに自動的に登録することを拒否します。
エンジニアはRuby vSphere Console（RVC）の出力を確認します。
「」
[RVC出力: vsan.disks_stats ~cluster]
+-------------+----------+-----------+------------+-------------------
----------------+
| デバイス名 | ステータス | 状態 | 容量 | HCL準拠 |
+-------------+----------+-----------+------------+-------------------

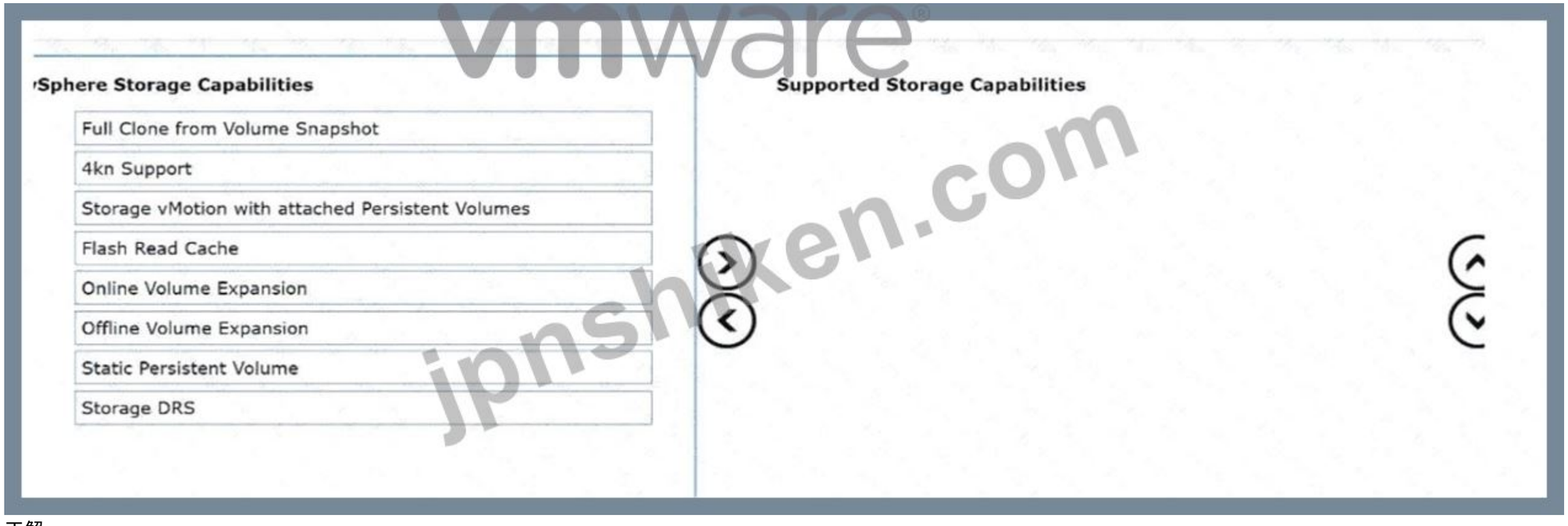
----------+
naa.5000a...	使用中	OK	3.84 TB	はい
naa.5000b...	使用中	OK	3.84 TB	はい
naa.5000x...	未請求	対象	7.68 TB	ファームウェアなし
+-------------+----------+-----------+------------+-------------------
----------+
「」
この新しいドライブを正常に統合し、クラスターを完全に正常な状態に復旧させるには、どのような根本原因分析と手順の組み合わせが必要ですか？（該当するものをすべて選択してください。）
A. 新しい7.68TBドライブは、既存の3.84TBドライブと互換性がありません。ESAは、プール内のすべてのドライブが同一容量であることを要求しています。
B. HCLデータベースが更新され、ファームウェアが準拠していると認識されたら、ESAは障害発生後に自動的にディスクをストレージプールに割り当てないため、管理者は手動でディスクをストレージプールに割り当てる必要があります。
C. NVMeドライバモジュールが新しいデバイスパスを初期化できるようにするには、ホストをメンテナンスモードで再起動する必要があります。
D. エンジニアは、vCenter Server で vSAN HCL データベース JSON ファイルを手動でダウンロードして更新し、コンプライアンス ブロッキングを解消する必要があります。
E. vCenter Server 上の vSAN HCL (ハードウェア互換性リスト) データベースが古く、新しく製造された NVMe ドライブのファームウェア署名を認識しません。
正解: **(**正解を表示します**)**

質問: **64**
L3サポートエンジニアが、新しいログ構造のvSAN Expressストレージアーキテクチャ（ESA）上で稼働する、トランザクション量の多いデータベースのストレージポリシーベース管理（SPBM）のオーバーヘッドを監査しています。
顧客は、容量オーバーヘッドを最小限に抑えるため、耐障害性ルールと並行してインライン圧縮を適用したいと考えている。
「」
[ストレージポリシールールビュー]
ポリシー: DB-最大効率
許容可能な障害数: 2 (RAID-6)
圧縮：有効
「」
vSAN ESAのアーキテクチャパイプラインは、圧縮とFTTオーバーヘッドをどのように処理し、クラスタ容量にどのような影響を与えますか？（該当するものをすべて選択してください。）
A. ESAでは、FTT計算は非圧縮VMDKサイズに基づいて物理ディスク領域を予約するため、圧縮を有効にするとネットワーク上のメリットは得られますが、ローカルディスク領域の節約にはなりません。
B. 圧縮を有効にすると、圧縮されたブロックは変動が大きすぎて正確に追跡できないため、オペレーションリザーブがネイティブに無効になります。
C. ESAの圧縮エンジンは厳密に4KBブロックを分析します。圧縮が非常に困難な暗号化データベースファイルでは、容量削減がゼロになる可能性があり、FTTオーバーヘッドは純粋に生の数学に依存します。
D. vSAN ESAでは、データがネットワーク全体に複製または消去符号化される*前*に、DOMクライアント層（スタックの最上位）で圧縮が行われます。つまり、FTT乗数（RAID-6の場合は1.5倍）は、既に縮小され圧縮されたデータペイロードに適用されます。
E. 高度に圧縮可能なデータとRAID-6を組み合わせることで、ESAでは最大の有効ストレージ容量が実現され、多くの場合、標準的なNASの利用率を上回ります。
正解: **(**正解を表示します**)**

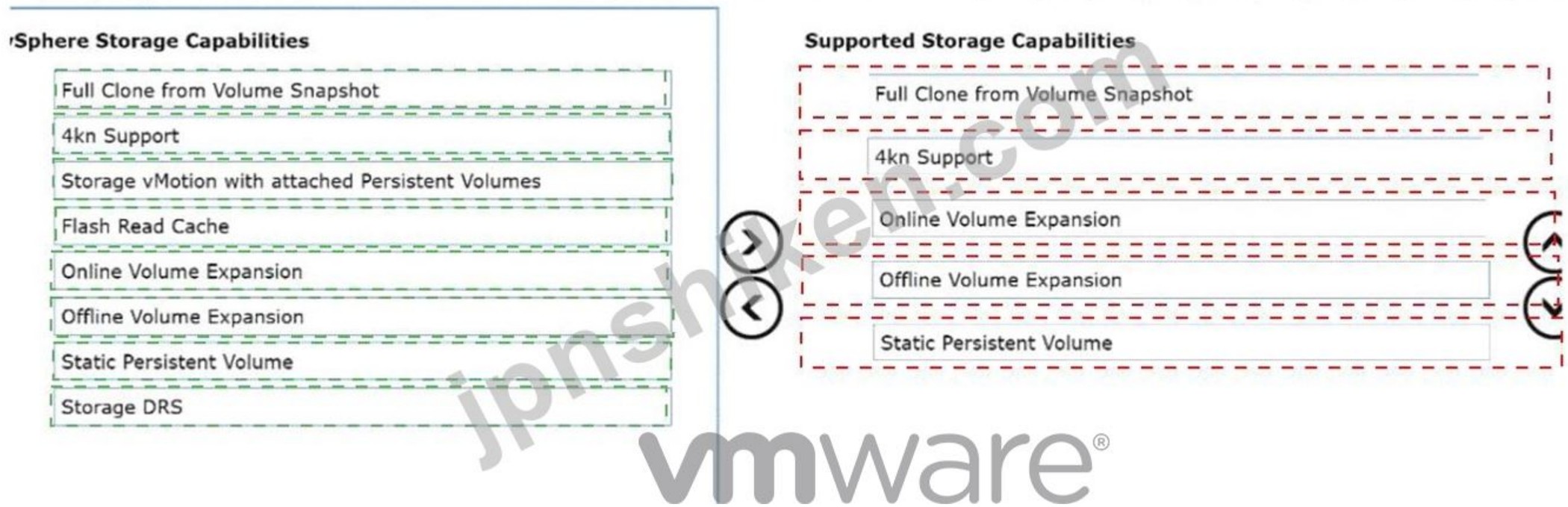
質問: **65**
管理者がクラスタ上でvSANデータ保存時暗号化を有効にしようとしたところ、以下のエラーメッセージが表示されました。
「キープロバイダ < vSphere Native Key Provider > がホスト上で利用できません。」管理者は、vSphere Native Key Provider (NKP) をデフォルト設定で構成しました。
vSANの保存データ暗号化を有効にする前に、管理者は何を検証すべきでしょうか？

A. 各ESXホストには、Trusted Platform Module (TPM) 2.0デバイスがインストールされています。
B. すべてのESXホストで暗号化セーフモードが有効になりました。
C. vSphere Client から vSphere Native Key Provider のバックアップが作成されました。
D. すべてのESXホストでセキュアブートが無効になっています。
正解: **C** (コメントを発表する)
管理者は、vSphere Native Key Provider がバックアップされていることを検証する必要があります。Native Key Provider が作成されると、vCenter はキー プロバイダ構成をクラスタ化された ESX ホストにプッシュしますが、プロバイダはバックアップされるまで暗号化タスクには使用できません。ドキュメントには、Native Key Provider を追加した後、バックアップされていない状態として表示され、使用する前にバックアップする必要があると記載されています。バックアップ プロセスでは、vCenter がホストに情報を伝播している間、プロバイダの状態が 『バックアップされていません」から 警告」に変更され、すべてのホストに情報がプッシュされると 『アクティブ」になります。デフォルト設定で Native Key Provider を使用する場合、TPM 2.0 デバイスは必須ではありませんが、TPM はセキュリティを強化でき、オプションで強制することもできます。暗号化セーフ モードとセキュア ブートの無効化は、NKP を使用した vSAN Data-at-Rest Encryption を有効にするための前提条件ではありません。したがって、検証手順は、NKP バックアップが作成され、プロバイダがホスト上でアクティブになっていることを確認することです。参照トピック :vSphereネイティブキープロバイダー、ネイティブキープロバイダーのバックアップ、vSAN保存データの暗号化、キープロバイダーの可用性。

質問: **66**
VMware Cloud Foundation (VCF) の VMware Kubernetes Service (VKS) における永続ボリュームで使用できるストレージ機能を選択します。
左側のvSphereストレージ機能リストから、サポートされている5つの機能をドラッグアンドドロップし、右側のサポートされているストレージ機能リストに任意の順序で配置します。 5つ選択してください。）



正解:



Explanation:
ボリュームスナップショットからの完全クローン
4knサポート
オンラインボリューム拡張
オフラインボリューム拡張
静的永続ボリューム
VMware Kubernetes Service の永続ボリュームは、CNS や pvCSI などの vSphere ストレージ統合機能を使用して、vSphere データストアとストレージポリシーによってサポートされる Kubernetes ストレージサービスを提供します。サポートされている永続ボリューム機能には、既存のストレージを Kubernetes ワークロードで使用できる静的永続ボリューム、ワークロードとファイルシステムの状態に応じて永続ボリュームのサイズを変更できるオフラインボリューム拡張とオンラインボリューム拡張、既存のスナップショットから新しいボリュームを作成できるボリュームスナップショットからの完全クローン、および基盤となるスタックがサポートする最新の 4K ネイティブストレージデバイスをサポートする 4kn サポートが含まれます。アタッチされた永続ボリュームをアクティブな使用中に移動すると、アタッチと一貫性の前提条件が壊れる可能性があるため、アタッチされた永続ボリュームを使用した Storage vMotion はサポートされていません。Storage DRS も、この VKS コンテキストではサポートされている永続ボリューム機能ではありません。Flash Read Cache は、サポートされている VKS 永続ボリューム機能セットの一部ではありません。参照トピック :VMware Kubernetes Service Storage、CNS、pvCSI、永続ボリューム機能、ボリューム拡張、ボリュームスナップショットクローン。

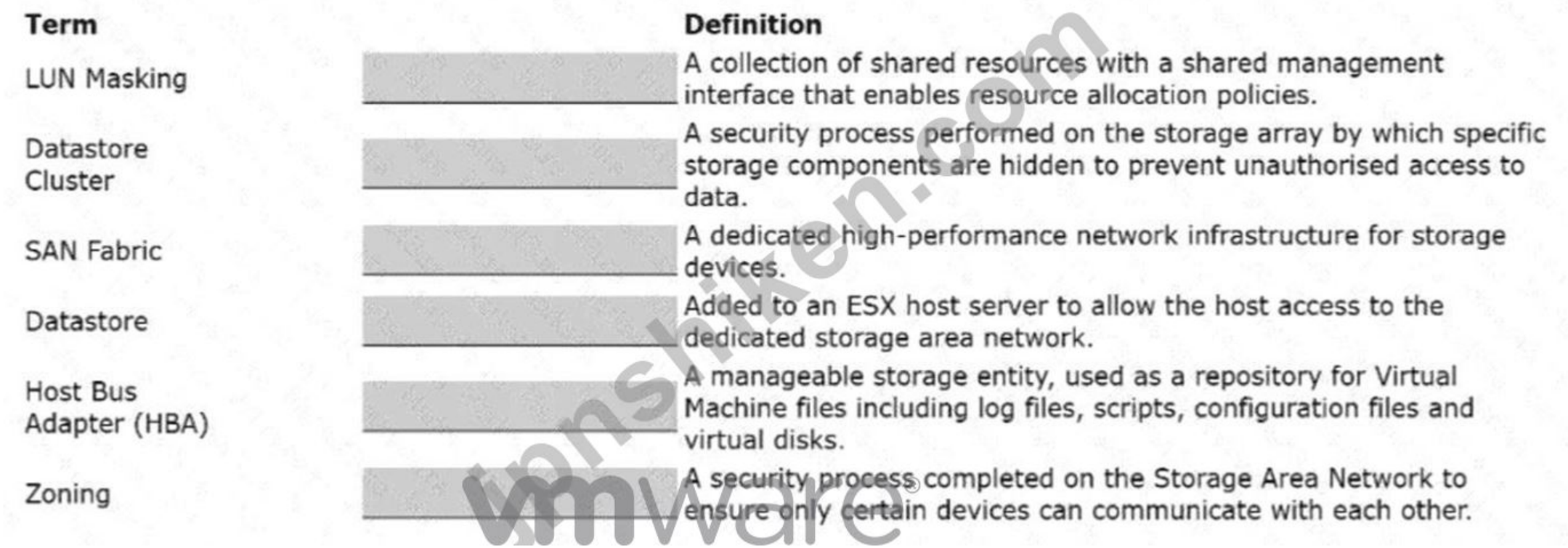
質問: **67**
インフラストラクチャマネージャーが、vSANパフォーマンスサービスを使用して、新しくデプロイされたvSAN ESAクラスタのパフォーマンスを分析しています。チームは、トランザクション量の多いデータベースをデプロイ済みです。
「」
[vSANパフォーマンスビュー]
コンポーネントI/Oの内訳
DOMクライアントIOPS :50,000

DOMオーナーのIOPS :50,000
LSOM IOPS: 12,000
NVMeデバイスのIOPS :12,000
「」
マネージャーは大きな矛盾に気づいた。DOMレイヤーは50,000 IOPSを処理しているのに、LSOMと物理NVMeデバイスはわずか12,000 IOPSしか処理していないのだ。
vSAN ESAログ構造ファイルシステムの以下のアーキテクチャ機能のうち、この特定の不一致を説明できるものはどれですか？（該当するものをすべて選択してください。）
A. LSOMは、高性能なログ構造メカニズムを利用して、数千個の小さなランダムなDOM I/Oリクエストを1つの大きなシーケンシャルI/O書き込みに統合（グループ化）し、NVMeデバイスに書き込みます。
B. ESAアーキテクチャはRAID-5/6の読み取り-変更-書き込みのペナルティを排除し、LSOMがOSAに見られる従来のバックエンドI/O増幅なしでネイティブにデータを書き込むことを可能にします。
C. この不一致は、宛先ホストに到達する前に DOM ネットワーク層によって 38,000 IOPS がドロップされるという重大なキャッシュ障害を示しています。
D. DOMクライアントはホストCPUを使用して4KBブロックを1KBブロックに圧縮するため、LSOMが書き込む物理バイト数は少なくなりますが、IOPSカウントは通常、バイト数ではなく個別の操作を反映します。
正解: **(**正解を表示します**)**

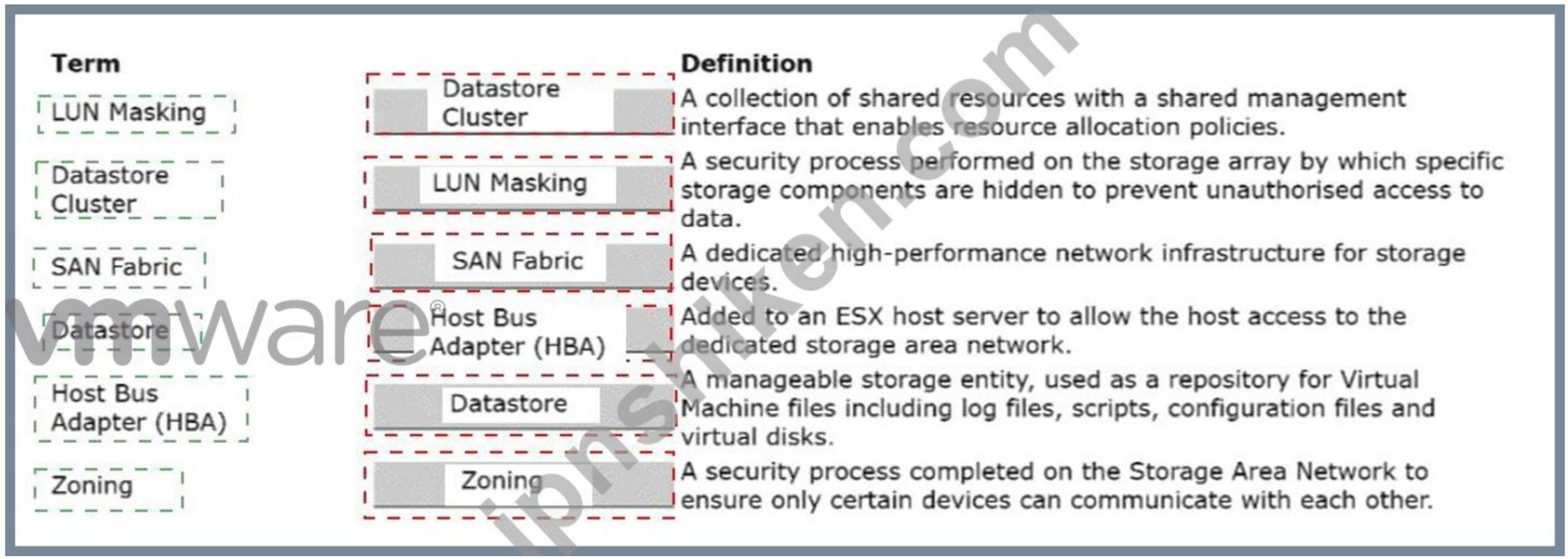
質問: **68**
ストレージ管理者が、VCF 9.0ワークロードドメインの展開後検証を実施しています。この設計では、vSAN Sizerツールを使用して、6ノードのストレッチドクラスタ（サイトあたり3ノード）の容量を予測しました。
Sizerの出力は、FTT=1（RAID-1）ローカル＋デュアルサイトミラーリングポリシーに基づいて、特定の「空き容量」を予測しました。
管理者は、Ruby vSphere Console (RVC) を使用してクラスタオブジェクトの分布を照会し、実際のコンポーネントの配置がサイザーの想定と一致しているかどうかを確認します。
「」
[RVC出力: vsan.obj_status_report ~cluster]
オブジェクトタイプ：仮想ディスク（ハードディスク1）
ポリシー：PFTT=1（ミラーリング）、SFTT=1（RAID-1）
コンポーネントのレイアウト:
サイトA：
- コンポーネント 1: 50 GB (アクティブ)
- コンポーネント2：50GB（アクティブ）
- ウィットネス: 4 KB (アクティブ)
サイトB：
- コンポーネント3：50GB（アクティブ）
- コンポーネント4：50GB（アクティブ）
- ウィットネス: 4 KB (アクティブ)
目撃情報サイト：
- ウィットネス: 4 KB (アクティブ)
「」
このRVC出力は、Sizerツールがこのオブジェクトの容量オーバーヘッドを4.0倍と正しく見積もったことをなぜ検証するのでしょうか？また、これはクラスター拡張計画にどのような影響を与えますか？（該当するものをすべて選択してください。）
A. サイトAとサイトBの4KBのWitnessコンポーネントは、50GBのデータコンポーネントと同じライセンスストレージ容量を消費するため、サイザーの結果が歪められます。
B. 「SFTT=1 (RAID-1)」ローカル保護は、*各サイト内*にデータのコピーを2つ作成し、さらに2.0倍の乗数を適用します（2.0 x 2.0 = 合計オーバーヘッド4.0倍）。

C. このレイアウトは ホストされた障害ドメイン」の概念を示しており、サイトAにノードを1つ追加すると、対称的な4.0xレイアウトを維持するためにサイトBにノードを1つ追加する必要があることを確認しています。
D. デュアルサイトミラーリング」はデータのコピーを2つ作成します サイトAに1つ、サイトBに1つ）。これは2.0倍の乗数として機能します。
正解: (正解を表示します)

質問: **69**
管理者は、VMware Cloud Foundation (VCF) プライベートクラウドを担当し、VCFワークロードドメインクラスタ内のさまざまなファイバーチャネル (FC) ストレージエリアネットワーク (SAN) コンポーネントを特定して説明する任務を負っています。
正しい用語を、対応する定義の上にドラッグ＆ドロップしてください。



正解:



Explanation:
LUN マスキング = ストレージ アレイ上で実行されるセキュリティ プロセスで、特定のストレージ コンポーネントを隠蔽して、データへの不正アクセスを防止します。データ ストア クラスタ = 共有管理インターフェイスを備えた共有リソースの集合で、リソース割り当てポリシーを有効にします。SAN ファブリック = ストレージ デバイス専用の高性能ネットワーク インフラストラクチャです。データ ストア = ログ ファイル、スクリプト、構成ファイル、仮想ディスクなどの仮想マシン ファイルのリポジトリとして使用される管理可能なストレージ エンティティです。ホスト バス アダプタ (HBA) = ホストが専用のストレージ エリア ネットワークにアクセスできるように、ESX ホスト サーバーに追加されます。ゾーニング = ストレージ エリア ネットワーク上で実行されるセキュリティ プロセスで、特定のデバイスのみが相互に通信できるようにします。
これらの定義は、VCFワークロードドメインにおけるファイバーチャネルSAN設計のコアコンポーネントについて説明しています。LUNマスキングはストレージアレイ上で実行され、どのホストが特定のLUNを参照できるかを制御し、ストレージへの不正アクセスを防止します。データストアクラスタは、共有リソースプールとして管理されるデータストアの集合であり、Storage DRSによる配置および負荷分散ポリシーを可能にします。SANファブリックは、ESXホスト、ファイバーチャネルスイッチ、およびストレージアレイを相互接続する専用の高性能ネットワークです。データストアは、VM構成ファイル、仮想ディスク、ログ、および関連ファイルが格納されるvSphereの論理ストレージコンテナです。ホストバスアダプタは、ESXホストをファイバーチャネルストレージエリアネットワークに接続する、ESXホスト内の物理アダプタまたは仮想アダプタです。
ゾーニングはファイバーチャネルファブリック上で実行され、どのイニシエータとターゲットが通信できるかを制御します。ゾーニングとLUNマスキングを組み合わせることで階層型アクセス制御が実現され、データストアとデータストアクラスタによってvSphereの消費モデルが提供されます。参照トピック :ファイバーチャネルSANの概念、SANファブリック、ゾーニング、LUNマスキング、VMFSデータストア、データストアクラスタ。

質問: **70**
コンプライアンス監査担当者は、VCFワークロードドメインが厳格な財務基準（例SOX/PCI）の「継続的なキーローテーション」要件を満たしていることを検証します。
監査担当者は、データ転送（DiT）構成に関連するvCenterログを調査します。
「」

[ログ分析: vpxd.log]
2026-11-20T12:00:00Z INFO vpxd - [DiT] 再キー間隔が期限切れになりました (1440
分)。
2026-11-20T12:00:01Z INFO vpxd - [DiT] 一時的なセッションキー
[esx-03]と[esx-05]の間で再交渉が成功しました。
2026-11-20T12:00:02Z INFO vpxd - [DiT] 古いキーバッファが削除されました。
「」
DiTのキーローテーションアーキテクチャは、外部のKMS管理者に頼ることなく、どのようにコンプライアンス要件を満たしているのでしょうか？（該当するものをすべて選択してください。）
A. RekeyIntervalは、APIを介して積極的に変更できます（例60分）。これにより、アクティブなストレージトラフィックに支障をきたすことなく、より厳格なコンプライアンスルールに対応できます。
B. キーローテーションはパケット層で即座に行われます。DOMクライアントは、書き込まれる4KBブロックごとに新しいキーを作成します。
C. DiTキーは削除前にバックアップ資料としてvCenterデータベースに自動的に保存され、フォレンジックの責任が確保されます。
D. ESXi ホストは、新しい対称鍵を同期するために、クラスタ書き込み操作 (輻輳) を 30 秒間一時的に停止する必要があります。
E. DiT のデフォルトの 鍵再生成間隔」は 1440 分 (24 時間) です。ESXi ホストは毎日自動的に新しい Diffie-Hellman ハンドシェイクを実行して完全に新しいセッションキーを作成するため、過去のトラフィックを総当たりで復号化することは不可能です。
正解: **A,E (**コメントを発表する**)**

質問: **71**
管理者は、VMware Cloud Foundation (VCF) ワークロード ドメインに vSAN Data Protection をデプロイするタスクを割り当てられました。管理者は VMware Live Recovery OVA をデプロイし、管理インターフェイスにログインしてアプライアンスの構成プロセスを開始しますが、アプライアンスが vCenter に登録されません。
管理者が問題を解決するために確認できる可能性のある原因を2つ挙げてください。2つ選択してください。）
A. vSANデータ保護アプライアンスがvSAN以外のデータストアにデプロイされました。
B. vCenter Serverユーザーアカウントは、VCSA Photon OSレベルでローカルに作成されました。
C. 登録に使用した vCenter Server ユーザー アカウントに必要な権限がありません。
D. この機器は管理にDHCP IPアドレスを使用しています。
E. アプライアンスとvCenter Server間の正引きおよび逆引きDNS解決が正しく構成されていません。
正解: **C,E (**コメントを発表する**)**
最も関連性の高い原因は、vCenter の権限不足と DNS 解決の誤りです。VMware Live Recovery アプライアンスは、vCenter に管理対象拡張機能およびサービス エンドポイントとして登録する必要があるため、アプライアンスの構成ワークフローで使用されるアカウントには、必要な vCenter 権限が必要です。認証はできるものの、登録権限または管理権限がないユーザーでも、アプライアンスの登録が失敗する可能性があります。アプライアンスの登録は、安定した FQDN 解決、証明書の検証、ルックアップ サービス通信、およびサービス エンドポイントの登録に依存するため、DNS も同様に重要です。VMware Live Recovery アプライアンスと vCenter Server 間では、正引きおよび逆引き DNS レコードが正しく解決される必要があります。vSAN 以外のデータ ストアにアプライアンスをデプロイすることは、vCenter 登録失敗の主な原因ではありません。結果として得られるアドレスと DNS レコードが正しければ、DHCP 自体が無効になるわけではありませんが、通常は静的アドレス指定が推奨されます。VCSA 上のローカル Photon OS アカウントは正しいアカウント タイプではありませんが、直接的な技術的問題は、必要な vCenter 権限がないことです。参照トピック: vSAN データ保護、VMware Live Recovery アプライアンスの登録、vCenter 権限、DNS 正引きおよび逆引き解決。

質問: **72**
VCF導入スペシャリストが、新しいvSAN ESAクラスタにおける書き込み操作のI/Oパスを、経験の浅い管理者に説明している。
「」
【建築図面コンセプト】
VM（ゲストOS）-> vSCSI -> [？] -> ネットワーク -> [？] -> 物理NVMeドライブ

「」
専門家は、書き込みが計算層からストレージ層へどのように伝播するかを示すために、不足しているアーキテクチャ上の要素を補完する必要がある。
ホストAで開始され、ホストB上のレプリカ宛ての書き込み操作のI/Oパスを正しく完成させる組み合わせはどれですか？
A. LSOM (ホスト A) -> ネットワーク -> CLOM (ホスト B) -> DOM オーナー (ホスト B)
B. CLOM (ホスト A) -> ネットワーク -> DOM クライアント (ホスト B) -> LSOM (ホスト B)
C. DOMオーナー（ホストA）→ネットワーク→LSOM（ホストB）→DOMクライアント（ホストB）
D. DOMクライアント（ホストA）→ネットワーク→DOMオーナー（ホストB）→LSOM（ホストB）
正解: **(**正解を表示します**)**

質問: **73**
管理者は、以下の要件を遵守しながらvSANストレージソリューションを設計する任務を負います。
* vSAN ESAを使用する必要があります
* 2つのデータセンター間にまたがって敷設する必要がある
* 許容する障害数を 1 に設定する必要があります
* イレイジャーコーディングを設定する必要があります
仮想マシン（VM）ごとにいくつのコンポーネントが作成されますか？
A. 4
B. 3
C. 1
D. 2
正解: **(**正解を表示します**)**
vSAN ESA と RAID-5/6 イレイジャー コーディングを使用した耐障害数を 1 に設定すると、vSAN は利用可能な障害ドメインの数に基づいて最適化された RAID-5 フォーマットを作成します。ドキュメントには、利用可能な障害ドメインが 5 以下の場合、ESA は RAID-5 用に 3 つのコンポーネントをリストすると記載されています。これは、2+1 イレイジャー コーディング レイアウトに対応し、2 つのデータ コンポーネントと 1 つのパリティ コンポーネントが作成されます。stretched-cluster 設定はサイトの災害耐性ルールに影響し、記載されているイレイジャー コーディングを使用した耐障害数ルールはローカル オブジェクト保護方法を定義します。ポリシー ノートには、vSAN ストレッチ クラスタでは、RAID-5/6 イレイジャー コーディングの耐障害性方法がサイトの災害耐性設定に適用されるとも記載されています。回答の選択肢から判断すると、FTT=1 イレイジャー コーディングに一致する ESA 最適化 RAID-5 コンポーネント レイアウトは 3 つのコンポーネントです。1 つまたは 2 つのコンポーネントではイレイジャー コーディングによる保護は提供されず、4 つのコンポーネントは配置の詳細に示されている ESA 最適化コンポーネント数ではなく、一般的な RAID-5 障害ドメイン要件を表しています。参考トピック :vSAN ESA RAID-5、許容障害数、イレイジャーコーディング、ストレッチドクラスタストレージポリシー。

質問: **74**
インフラストラクチャマネージャーが、HCIメッシュコンピューティング専用クライアントクラスタ上で実行されている仮想マシンのストレージポリシーベース管理（SPBM）の動作を監査しています。
「」
[root@esx-comp-01:~] esxcli vsan debug object list -u 5543...
オブジェクトUUID: 5543... (VM: Database-01)
ポリシー :FTT=1（RAID-1）、IOPS制限 :2000
コンポーネント 1: アクティブ (ホスト: esx-storage-05) -> リモート サーバー クラスタ
コンポーネント 2: アクティブ (ホスト: esx-storage-06) -> リモート サーバー クラスタ
監視: アクティブ (ホスト: esx-storage-07) -> リモートサーバークラスタ
「」

VMコンピューティング（esx-comp-01）とストレージバックエンド（esx-storage-05/06）が完全に異なる物理クラスタに存在する場合、SPBMルールはどのようにしてストレージ保護とQoSを機械的に強制するのでしょうか？（該当するものをすべて選択してください。）
A. 「耐障害性」(RAID-1) レイアウトロジックは、*リモートサーバークラスタ* 上の DOM Owner モジュールによって厳密に管理され、コンポーネントが同じ障害ドメインに存在しないようにします。
B. 「IOPS制限」(QoS)ルールは、*クライアントコンピューティングホスト*(esx-comp-01)上で実行されているDOMクライアントモジュールによって厳密に適用され、DB I/Oがネットワークに到達する前にスロットリングされます。
C. クライアントホスト上の SPBM エンジンは、RAID-1 の要件を満たすために、ネットワーク全体でデータを複製 (2 倍) し、ISL の帯域幅を 2 倍にする必要があります。
D. クライアントとサーバークラスタ間のネットワークが切断された場合、esx-comp-01 上の VM はローカル NVMe キャッシュを使用して読み取り専用モードで実行を継続します。
正解: (正解を表示します)

質問: **75**
VI管理者は、外部KMSを介したvSANデータ保存時暗号化を利用して、安全なVCF環境におけるディスク障害を管理しています。
esx-01に搭載されている容量3.84TBのNVMeドライブ1台で、深刻なメディア劣化が発生しています。管理者はドライブを物理的に交換する必要があります。
「」
操作ログ
ステップ 1: ホスト esx-01 をメンテナンス モード (データ移行なし) にします。
ステップ2 :GUIを使用して、障害が発生したドライブをvSANストレージプールから解放します。
ステップ3：故障したNVMeデバイスを新しいものと物理的に交換します。
ステップ4 :GUIを使用して、新しいNVMeデバイスをvSANストレージに登録します。
プール。
「」
ステップ4において、vSANの保存データ暗号化機能は、交換用NVMeドライブとどのように連携しますか？（該当するものをすべて選択してください。）
A. vSANが新しいNVMeドライブを受け入れる前に、VCF管理者はコンソール経由でキー暗号化キー（KEK）を手動でインストールする必要があります。
B. 取り外された故障したNVMeドライブには完全に暗号化されたデータブロックが含まれています。KMSからの対応するKEKがない場合、取り外されたドライブ上のデータは暗号化によって消去され、RMA（返品承認）に対して安全です。
C. 「クレーム」処理中に、ESXiホストは、その物理NVMeドライブ専用の新しいディスク暗号化キー（DEK）を生成します。
D. 交換用ドライブ用の新しい DEK は、クラスタで共有されている既存の KEK でラップ (暗号化) されるため、挿入の瞬間に外部 KMS とのアクティブな通信は必要ありません。
正解: (正解を表示します)

質問: **76**
SOCアナリストが、6ノードのvSAN OSAクラスタで実行されているデータベースVMにおける深刻な書き込み遅延を調査しています。アナリストは、VMが存在するホスト（esx-01）からvmkernel.logを取得します。
「」
2026-11-28T10:15:20Z 警告 vsan-dom - DOMクライアント: I/Oタイムアウト
オブジェクト5543（コンポーネント88b1）の処理に3000msかかりました。（ホスト：esx-04）
2026-11-28T10:15:21Z 警告 vsan-lsom [esx-04] - LSOM: 輻輳タイプ
「ssd-congestion」がしきい値185に達しました。バックプレッシャーを適用します。
2026-11-28T10:15:22Z ERROR vsan-dom - DOMオーナー: コンポーネントへの書き込み
88b1... LSOMキューがいっぱいのため遅延しています。
「」

ログに示されているDOMとLSOMの相互作用に基づいて、根本原因とシステム動作を正確に診断している記述は次のうちどれですか？ 2つ選択してください。）
A. ログには、DOMクライアントのネットワークスタックの障害が示されており、I/Oがキャッシュ層を完全にバイパスする原因となっています。
B. ssd-congestion は LSOM レイヤの物理メトリックで、esx-04 のキャッシュ ティアが、受信する書き込みに追いつくのに十分な速さでデータを容量ティアにデステージできないことを示しています。
C. esx-01 の LSOM でキャッシュ ドライブ障害が発生し、すべての書き込みが esx- にリダイレクトされています。
04 DOM経由。
D. リモートホストesx-04上のssd-congestionにより物理書き込みバッファが枯渇したため、esx-01上のDOMクライアントはVMのI/Oを積極的にゼロに制限しています。
正解: **B,D** (コメントを発表する)

質問: **77**
管理者は、2ノードのvSANエッジクラスタの既存のWitness Hostを交換する任務を負っている。
交換手続き中、新しいWitness Hostは選択肢として表示されません。
この設定上の問題の原因は何ですか？
A. VMkernelアダプタはvSANトラフィックが有効になるように構成されています。
B. VMkernelアダプタは、ストレッチクラスタ内のすべてのホストに接続されています。
C. ウィットネスホストは、2ノードのvSAN対応クラスタ内に存在します。
D. ウィットネスホストは既に別の2ノードvSANクラスタに割り当てられています。
正解: **C** (コメントを発表する)
2ノードvSANクラスタのウィットネスホストは、2ノードvSAN対応データクラスタの外部に配置する必要があります。
ウィットネスはクォーラムを提供するため、ホストまたはサイトの障害発生時に可用性を仲裁できるように、保護対象のデータノードペアの外側に配置する必要があります。提案されたウィットネス ホストが 2 ノードの vSAN 対応クラスタ内にある場合、資格がないため、交換ワークフロー中に利用可能な選択肢として表示されません。ウィットネス通信には、vSAN トラフィックが有効になっている VMkernel アダプタが構成されている必要があるため、これが問題の原因ではありません。データ ホストへの接続も想定されており、ウィットネスが無効になるわけではありません。別の 2 ノード vSAN クラスタに既に割り当てられているウィットネス ホストは、必ずしも資格を失うわけではありません。これは、共有ウィットネス構成がスケールとサイジングの制限内でサポートされているためです。資格に関する主な問題は、ウィットネス ホストが、監視対象とする 2 ノード vSAN クラスタのメンバーであってはならないことです。参照トピック: 2 ノード vSAN クラスタ、ウィットネス ホストの配置、ウィットネス ホストの交換、共有ウィットネスのサポート。

質問: **78**
VMware Cloud Foundation (VCF) 環境では、以下の vSAN 構成で、オンライン トランザクション処理 (OLTP) と分析という混合ワークロードが実行されます。
* ホスト8台（オールフラッシュ）、ESA有効。
* 各ホスト :3.2TBのNVMeデバイス×2台。
* 圧縮が有効になっています。
* チェックサムが有効になっています。
* ストレージポリシー: FTT=1 (RAID-5/6)、許容障害数=1、オブジェクトスペース予約=0%。
OLTPの負荷がピークに達すると、vSANの再同期I/Oとバックエンドの輻輳により、ネットワーク帯域幅が十分であってもレイテンシが増加します。

データ保護コンプライアンスを維持しながら書き込みパフォーマンスを向上させるために、管理者が直接実行できる対策は何ですか？
A. オブジェクト予約を100%に増やして容量を事前割り当てし、ログ構造化のオーバーヘッドを防止します。
B. 圧縮を有効にしたまま、レイテンシに敏感なワークロードに対してポリシーをRAID-1（FTT=1）に変換します。
C. RAID-5/6でFTTを2に増やし、圧縮を無効にします。
D. NVMe デバイスでのメタデータ書き込みを減らすためにチェックサムを無効にします。
正解: **(**正解を表示します**)**
直接的な対策は、レイテンシに敏感な OLTP ワークロード ポリシーを、FTT=1 を維持したまま RAID-5/6 イレイジャー コーディングから RAID-1 ミラーリングに変換することです。RAID-5/6 はスペース効率に優れていますが、パリティ操作と追加のバックエンド I/O を導入するため、トランザクション アクティビティのピーク時や再同期時に書き込みレイテンシが増加する可能性があります。VMware は、RAID-1 ミラーリングではストレージ デバイスへの I/O 操作が少なく、パフォーマンスが向上すると述べています。また、RAID-1 ではクラスタの再同期も高速に完了します。これは、ネットワーク帯域幅が十分であるにもかかわらず、再同期 I/O とバックエンドの輻輳によりレイテンシが増加するという、観測された症状に直接対処します。オブジェクト スペース予約を 100% に増やすと、容量の事前割り当ては変更されますが、パリティ オーバーヘッドが削除されたり、イレイジャー コーディングによる書き込み増幅が軽減されたりすることはありません。RAID-5/6 で FTT を 2 に増やすと、保護オーバーヘッドとバックエンド作業が増加し、レイテンシが悪化します。ESA では、オブジェクト チェックサムは常に有効で無効にできないため、チェックサムを無効にすることはできません。ESA の場合、圧縮はポリシーで制御できますが、最も直接的な保護準拠のパフォーマンス対策は、OLTP オブジェクトに対して RAID-1 FTT=1 を設定することです。参照トピック: vSAN ストレージ ポリシー、RAID-1 ミラーリング、RAID-5/6 イレイジャー コーディング、vSAN ESA チェックサム、再同期、および輻輳メトリック。

質問: **79**
vSAN Express Storage Architecture (ESA) における重複排除と圧縮の実装方法と、従来のOriginal Storage Architecture (OSA) における実装方法の根本的な違いを正確に定義しているのは、次のうちどれですか？
A. vSAN ESAは、重複排除と圧縮をDPUを使用してトップオブラック スイッチ上の単一のハードウェア オフロード プロセスに統合しますが、OSAはESXiのCPUサイクルのみに依存していました。
B. vSAN ESA はグローバル重複排除機能を完全に非推奨にし、圧縮をスタックの最上位 (DOM クライアント) に移動して、ネットワーク経由でデータが送信される前にデータを圧縮します。
C. vSAN OSAは仮想マシンSCSIレイヤーで厳密に圧縮を適用しますが、vSAN ESAは物理ネットワークスイッチレイヤーで圧縮を適用します。
D. vSAN OSA は、キャッシュ層への最初の書き込み時に重複排除と圧縮を同期的に処理しますが、ESA はストレージプールへのデステージング時に非同期的に処理します。
正解: **B (**コメントを発表する**)**

質問: **80**
vSANは、準拠していない仮想マシンを検出し、準拠していないオブジェクトに対する投票の55%の完全なレプリカを見つけることができました。
vSANは仮想マシンに対してどのような処理を実行しますか？
A. 準拠していないオブジェクトを自動的に復元し、仮想マシンを準拠しているとマークします。
B. 仮想マシンの電源を切ります。
C. vSANがオブジェクトの投票の60%以上を見つけることができないため、仮想マシンをアクセス不可としてマークします。
D. 仮想マシンを孤立した仮想マシンとしてマークします。
正解: **(**正解を表示します**)**
vSAN オブジェクトの可用性は、次の 2 つの条件に基づいています。完全なレプリカが利用可能であること、およびオブジェクトの投票の 50% 以上がアクセス可能であること。このシナリオでは、vSAN は完全なレプリカと、非準拠オブジェクトの投票の 55% を検出できます。55% はクォーラムのしきい値よりも大きいため、オブジェクトは vSAN データ ストアで引き続き利用可能です。非準拠ステータスは、VM オブジェクトが現在割り当てられたストレージ ポリシーを満たしていないことを意味しますが、VM がアクセスできないことを自動的に意味するものではありません。ドキュメントには、オブジェクトが非準拠であっても運用状態が正常であれば、仮想マシンは vSAN データ ストアの使用を継続できると記載されています。クラスタに十分なリソースがあり、障害が永続的な場合、vSAN は障害が発生したコンポーネントを自動的に復旧し、準拠状態を復元します。VM がアクセスできないとマークされるのは、完全なレプリカが見つからない場合、または投票が 50% 以下しかない場合のみです。VM の名前空間 (.vmx ファイルなど) にアクセスできない場合にのみ、VM が孤立状態になります。参照トピック :vSANオブジェクトの健全性、クォーラム投票、非準拠オブジェクト、アクセス不能なVM状態および孤立したVM状態。

有効的な**3V0-23.25**問題集はJPNTest.com提供され、**3V0-23.25**試験に合格することに役に立ちます！JPNTest.comは今最新**3V0-23.25**試験問題集を提供します。JPNTest.com 3V0-23.25試験問題集はもう更新されました。ここで**3V0-23.25**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/3V0-23.25-mondaishu　**79**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」