Nutanix.NCM-MCI.v2026-05-13.q6

試験コード：	NCM-MCI
試験名称：	Nutanix Certified Master - Multicloud Infrastructure v6.10
認証ベンダー：	Nutanix
無料問題の数：	6
バージョン：	v2026-05-13
ページの閲覧量：	105
問題集の閲覧量：	61

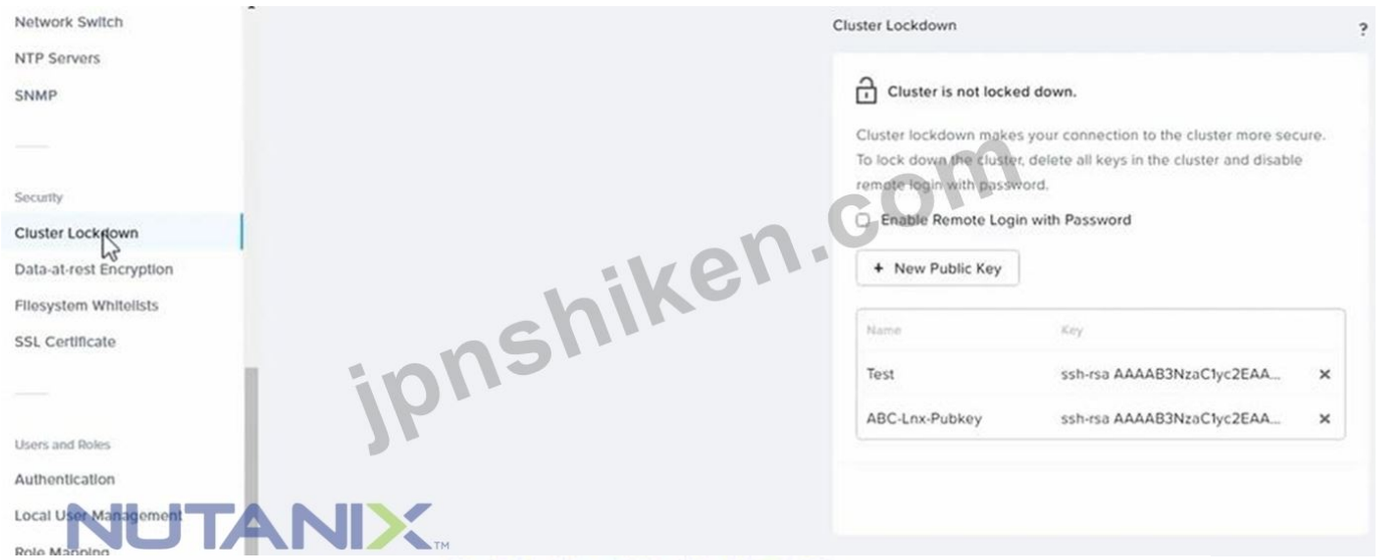
https://www.jpnshiken.com/shiken/Nutanix.NCM-MCI.v2026-05-13.q6.html

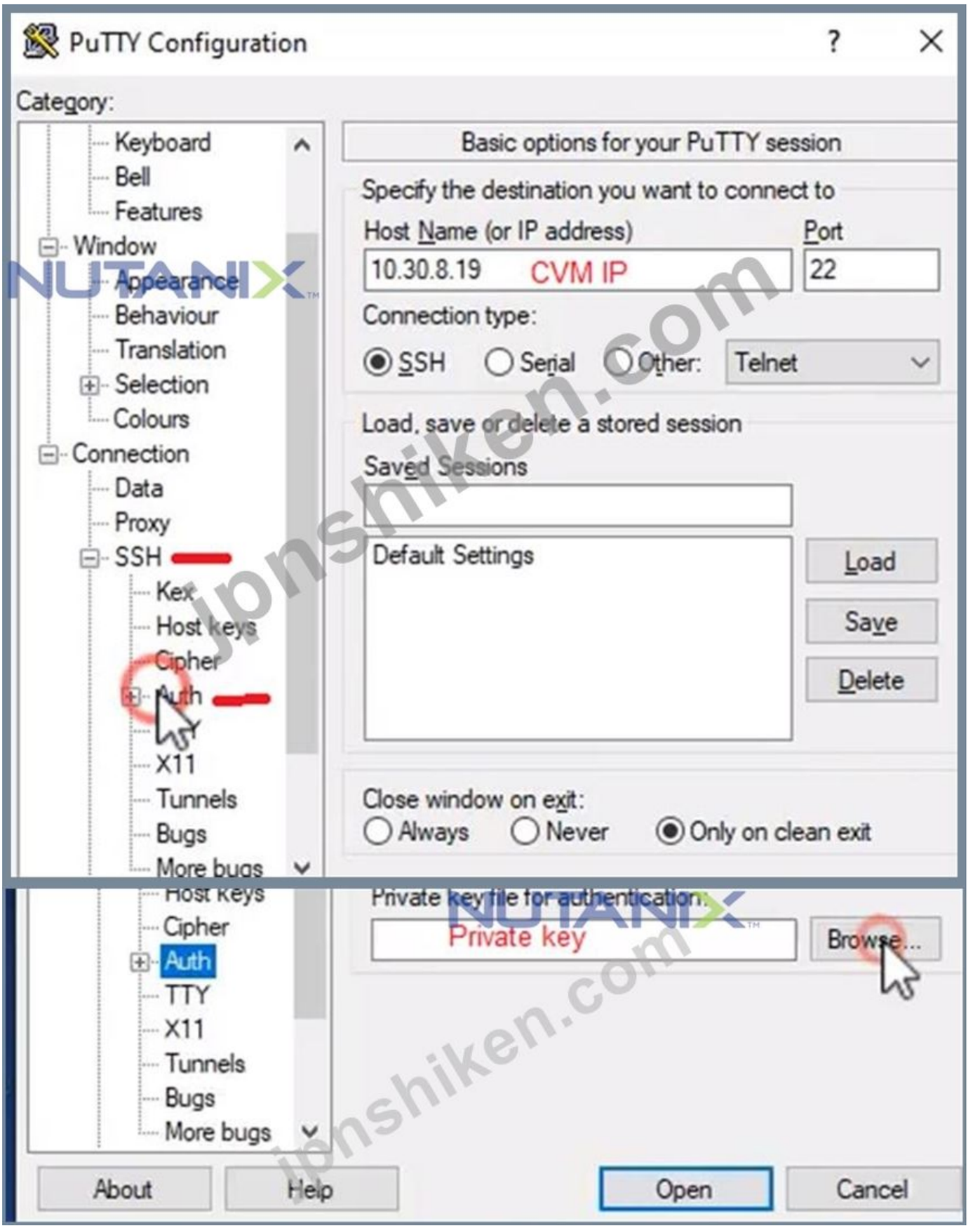
質問: **1**
タスク9
パート1
管理者が Prism Element にログインすると、次のような警告が表示されます。
コントローラ VM (35.197.75.196) のクラスタ サービスがダウンしています
最も混乱の少ない方法でこの問題を修正してください。
パート2
別のリクエストでは、セキュリティ チームは新しく作成されたクラスターがレポートしていることに気付きました。
CVM [35.197.75.196]はデフォルトのパスワードを使用しています。
クラスター レベルのセキュリティに対していくつかの新しいセキュリティ要件が提供されました。
セキュリティ要件:
ノード上のrootユーザーのデフォルトパスワードをadminユーザーのパスワードと一致するように更新してください。注 :192.168.xxは使用できません。ノードにアクセスするには、CVMのホストIP（172.30.0.x）または指定された外部IPアドレスを使用してください。
CVM 上の nutanix ユーザーのデフォルト パスワードを、管理者ユーザーのパスワードと一致するように更新します。
報告されているアラートを解決します。
変更を加える前に、SCMA ポリシーのクラスター全体の構成を Desktop\Files\output.txt に出力します。
クラスターに対して、Advance intrusion Detection Environment (AIDE) を毎週実行できるようにします。
クラスターに対して高強度のパスワード ポリシーを有効にします。
CVM がログインにパスワードではなく SSH キーを必要とすることを確認します (SSH キーは Desktop\Files\SSH フォルダーにあります)。
クラスタがこれらの要件を満たしていることを確認してください。クラスタコンポーネントを再起動しないでください。
正解:

ステップバイステップの解決策については説明をご覧ください
Explanation:
コントローラ VM (35.197.75.196) 上のクラスタ サービスがダウンする問題を、最小限の混乱で修正するには、次の手順を実行する必要があります。
管理者ユーザーの資格情報を使用して Prism Element にログインします。
「アラート」ページに移動し、アラートをクリックして詳細を表示します。
コントローラVM上でどのクラスタサービスがダウンしているかを確認できます。例えば、Cassandra、Curator、StarGateなどが該当します。
クラスタサービスを開始するには、nutanix ユーザーの認証情報を使用してコントローラ VM に SSH 接続する必要があります。コントローラ VM への接続には、PuTTY や Windows PowerShell などの任意の SSH クライアントを使用できます。nutanix ユーザーの IP アドレスとパスワードが必要になります。これらの情報は、Desktop\Files\SSH\nutanix.txt に記載されています。
コントローラ VM にログインしたら、次のコマンドを実行します。
クラスターステータス | grep -v UP
これにより、コントローラ VM 上でダウンしているサービスが表示されます。
クラスター サービスを開始するには、次のコマンドを実行します。
クラスター開始
これにより、コントローラ VM 上のすべてのクラスター サービスが開始されます。
クラスター サービスが実行されていることを確認するには、次のコマンドを実行します。
クラスターステータス | grep -v UP
出力は表示されず、すべてのサービスが稼働していることを示します。
アラートをクリアするには、Prism Element に戻り、「アラート」ページで 「解決」をクリックします。
クラスター レベルのセキュリティのセキュリティ要件を満たすには、次の手順を実行する必要があります。
ノード上のルートユーザーのデフォルトパスワードを管理者ユーザーのパスワードと一致するように更新するには、ルートユーザーの認証情報を使用してノードにSSH接続する必要があります。ノードへの接続には、PuTTYやWindows PowerShellなどの任意のSSHクライアントを使用できます。ルートユーザーのIPアドレスとパスワードが必要です。これらはDesktop\Files\SSH\root.txtに記載されています。
ノードにログインしたら、次のコマンドを実行します。
パスワード
ルートユーザーの新しいパスワードを入力するよう求められます。Desktop\Files\SSH\admin.txt に記載されている管理者ユーザーと同じパスワードを入力してください。
CVM上のnutanixユーザーのデフォルトパスワードをadminユーザーのパスワードと一致するように更新するには、nutanixユーザーの認証情報を使用してCVMにSSH接続する必要があります。CVMへの接続には、PuTTYやWindows PowerShellなどのSSHクライアントを使用できます。nutanixユーザーのIPアドレスとパスワードが必要です。これらはDesktop\Files\SSH\nutanix.txtにあります。

CVM にログインしたら、次のコマンドを実行します。
パスワード
nutanixユーザーの新しいパスワードを入力するよう求められます。Desktop\Files\SSH\admin.txt にあるadminユーザーと同じパスワードを入力してください。
報告されているアラートを解決するには、Prism Element に戻り、 「アラート」ページで 解決」をクリックします。
変更を加える前に、SCMA ポリシーのクラスター全体の構成を Desktop\Files\output.txt に出力するには、管理者ユーザーの資格情報を使用して Prism Element にログインする必要があります。
 セキュリティ」> 「SCMAポリシー」に移動し、 「ポリシーの詳細を表示」をクリックします。これにより、各エンティティタイプのSCMAポリシーの現在の設定が表示されます。
これらの設定をコピーして、Desktop\Files\output.txt という名前の新しいテキスト ファイルに貼り付けます。
クラスターに対して AIDE (Advanced Intrusion Detection Environment) を毎週実行できるようにするには、管理者ユーザーの資格情報を使用して Prism Element にログインする必要があります。
 セキュリティ」> 「AIDE設定」に移動し、 「AIDEを有効にする」をクリックします。これにより、AIDEはクラスタ内のすべてのCVMとノード上のファイルシステムの変更を監視できるようになります。
AIDE スキャンの頻度として [毎週] を選択し、[保存] をクリックします。
クラスターに対して高強度パスワード ポリシーを有効にするには、管理者ユーザーの資格情報を使用して Prism Element にログインする必要があります。
 セキュリティ」> 「パスワードポリシー」に移動し、 「ポリシーの編集」をクリックします。これにより、各エンティティタイプのパスワードポリシー設定を変更できます。
各エンティティ タイプ (管理者ユーザー、コンソール ユーザー、CVM ユーザー、ホスト ユーザー) について、パスワード ポリシー レベルとして [高強度] を選択し、[保存] をクリックします。
CVM がログインにパスワードではなく SSH キーを必要とするようにするには、管理者ユーザーの資格情報を使用して Prism Element にログインする必要があります。
 セキュリティ」> 「クラスターロックダウン」に移動し、 「ロックダウンの設定」をクリックします。これにより、クラスターのSSHアクセス設定を管理できるようになります。
 「パスワードによるリモートログインを有効にする」のチェックを外します。これにより、クラスターへのパスワードベースのSSHアクセスが無効になります。
 新しい公開鍵」をクリックし、鍵の名前を入力して、Desktop\Files\SSH\id_rsa.pub から公開鍵の値を貼り付けます。これにより、クラスターへの鍵ベースのSSHアクセス用の公開鍵が追加されます。
 保存してロックダウンを適用」をクリックします。これにより変更が適用され、CVMへのログインにパスワードではなくSSHキーが必須になります。
パート1
CVM ssh に入り、次を実行します:
クラスターステータス | grep -v UP

クラスター開始
一部のサービスを開始する際に問題が発生した場合は、以下を確認してください。
CVMでncli host lsコマンドを実行し、ノードがメンテナンスモードになっているかどうかを確認します。サービスが停止しているノードの 区メンテナンスモード中」パラメータがFalseに設定されていることを確認します。区メンテナンスモード中」パラメータがTrueに設定されている場合は、次のコマンドを実行してノードのメンテナンスモードを解除します。
* nutanix@cvm$ ncli host edit id=<ホスト id> enable-maintenance-mode=false ncli host ls を使用してホスト ID を確認できます。
Nutanixポータルのソフトウェアドキュメントページから入手できる 区級管理ガイド」の、障害が発生したクラスターサービスに関するトラブルシューティングトピックを参照してください。 ワィルターを使用して、お使いのAOSバージョンに対応するガイドを検索してください。）これらのトピックには、Stargate、Cassandra、その他のモジュールなど、一般的なログとAOS固有のログに関する情報が記載されています。
* 停止しているサービスについて、最新のFATALログがないか確認してください。以下のコマンドは、CVMのすべてのFATALログを出力します。このコマンドはすべてのCVMで実行してください。
nutanix@cvm$ for i in `svmips`; do echo "CVM: $i"; ssh $i "ls -ltr /home/nutanix/data/logs/*.FATAL"; done NCC ヘルスチェック: cluster_services_down_check (nutanix.com) パート 2 ノード上の root ユーザーのデフォルト パスワードを、管理者ユーザーのパスワードと一致するように更新します echo -e "すべての AHV ホスト ルート パスワードを変更しています。\n新しいパスワードを入力してください: "; read -rs password1; echo "新しいパスワードを確認してください: "; read -rs password2; if ["$password1" == "$password2"]; then for host in $(hostips); do echo Host $host; echo $password1 | ssh root@$host "passwd --stdin root"; done; else echo "パスワードが一致しません"; fi CVM 上の nutanix ユーザーのデフォルト パスワードを更新します。sudo passwd nutanix SCMA ポリシーのクラスター全体の構成を出力します。ncli cluster get-hypervisor-security-config 出力例:
nutanix@NTNX-372a19a3-A-CVM:10.35.150.184:~$ ncli cluster get-hypervisor-security-config Enable Aide : false Enable Core : false Enable High Strength P... : false Enable Banner : false Schedule : DAILY Enable iTLB Multihit M... : false クラスターに対して毎週実行されるように、Advance intrusion Detection Environment (AIDE) を有効にします。
ncli クラスター編集ハイパーバイザーセキュリティパラメータ enable-aide=true
ncli クラスター編集ハイパーバイザーセキュリティパラメータスケジュール=毎週
クラスターに対して高強度のパスワード ポリシーを有効にします。
ncli cluster edit-hypervisor-security-params enable-high-strength-password=true CVM がログイン時にパスワードではなく SSH キーを要求するようにします
https://portal.nutanix.com/page/documents/kbs/details?targetId=kA0600000008gb3CAA




PuTTY Configuration
Category:
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Kex
Host keys
Cipher
Auth
TTY
X11
Tunnels
Bugs
More bugs
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
10.30.8.19
CVM IP
22
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
Private key file for authentication:
Private key
Browse...
About
Help
Open
Cancel
NUTANIX
jpnshiken.com

質問: **2**
タスク6

管理者が、未設定ノードでトラフィックセグメンテーションを設定するために必要なコマンドを要求しました。ノードには4つのアップリンクがあり、これらは既にデフォルトブリッジに追加されています。デフォルトブリッジでは、eth0とeth1がアクティブ/パッシブに設定され、eth2とeth3がセグメント化されたトラフィックに割り当てられ、物理ネットワークコンポーネントに変更を加えることなく両方のリンクを利用できるように設定されている必要があります。
管理者は作業を開始し、それを Desktop\Files\Network\unconfigured.txt に保存しました。ファイル内の x を適切な文字または文字列に置き換えてください。既存の行を削除したり、新しい行を追加したりしないでください。
注意: 利用可能なクラスターではこれらのコマンドを実行することはできません。
未構成.txt
manage_ovs --bond_name brX-up --bond_mode xxxxxxxxxxx --interfaces ethX,ethX update_uplinks manage_ovs --bridge_name brX-up --interfaces ethX,ethX --bond_name bond1 --bond_mode xxxxxxxxxxx update_uplinks
正解:
ステップバイステップの解決策については説明をご覧ください
Explanation:
構成されていないノードでトラフィック セグメンテーションを構成するには、ノードで次のコマンドを実行する必要があります。
manage_ovs --bond_name br0-up --bond_mode active-backup --interfaces eth0,eth1 update_uplinks manage_ovs --bridge_name br0-up --interfaces eth2,eth3 --bond_name bond1 --bond_mode balance-slb update_uplinks これらのコマンドは、eth0とeth1をアクティブインターフェースとパッシブインターフェースとしてbr0-upというボンドを作成し、それをデフォルトのブリッジに割り当てます。次に、eth2とeth3をアクティブインターフェースとしてbond1という別のボンドを作成し、同じブリッジに割り当てます。これにより、ノードのトラフィックセグメンテーションが有効になり、eth2とeth3はセグメント化されたトラフィック専用となり、両方のリンクをロードバランシングモードで使用するように設定されます。
Desktop\Files\Network\unconfigured.txt ファイル内の x を適切な文字または文字列に置き換えました。更新されたファイルは Desktop\Files\Network\configured.txt にあります。
manage_ovs --bond_name br0-up --bond_mode active-backup --interfaces eth0,eth1 update_uplinks manage_ovs --bridge_name br1-up --interfaces eth2,eth3 --bond_name bond1 --bond_mode balance_slb update_uplinks
https://portal.nutanix.com/page/documents/solutions/details?targetId=BP-2071-AHV-Networking:ovs-command-line-configuration.html

質問: **3**
タスク11
管理者は、ホスト障害発生後、クラスタ内の別のホストからSQL03仮想マシンがパワーオンされていないことに気付きました。他のSQL仮想マシン（SQL01、SQL02）は、過去に正常に復旧しています。

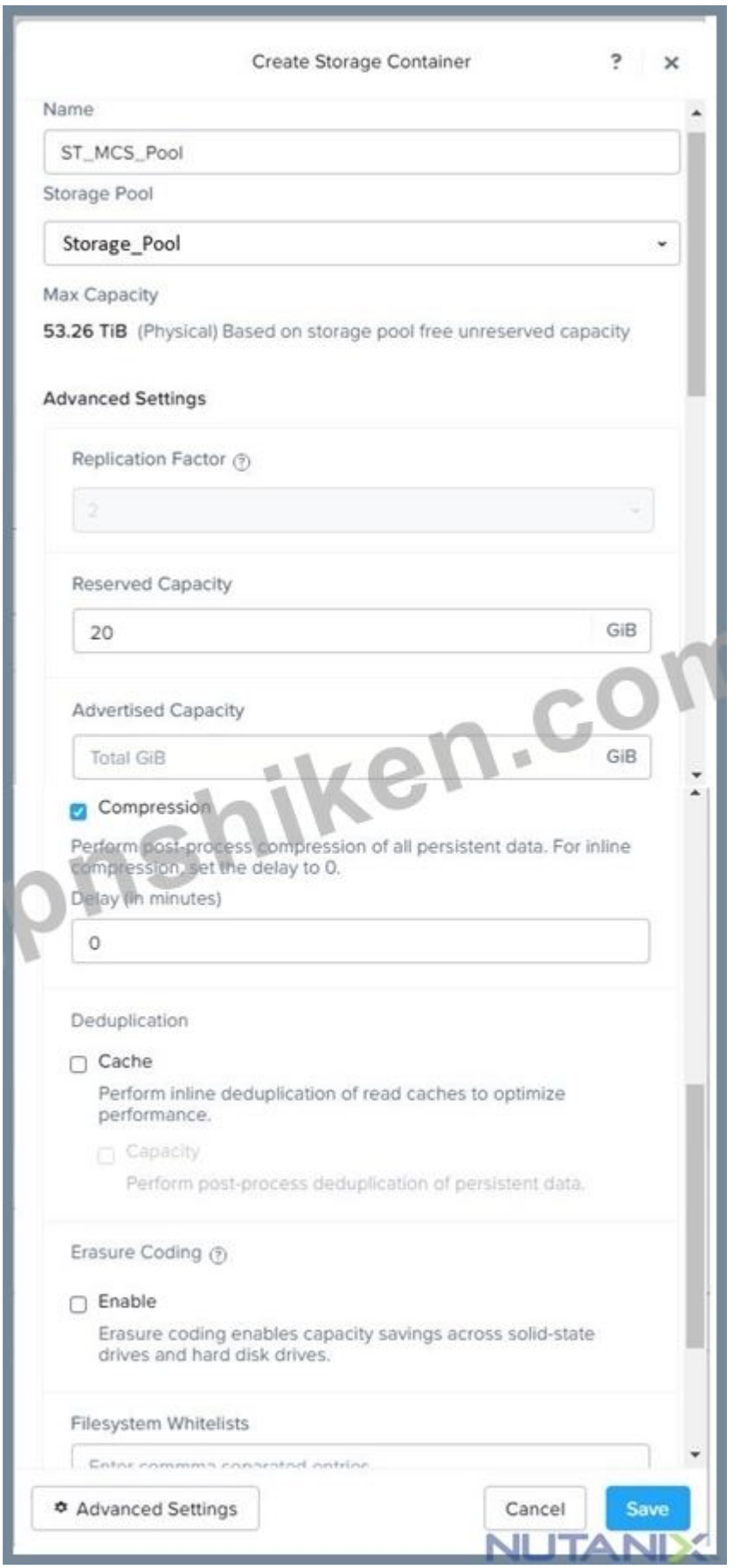
問題を解決し、単一のホスト障害が最小限の数の SQL VM に影響を与えるように環境を構成します。
注: VMの電源をオンにしないでください
正解:
ステップバイステップの解決策については説明をご覧ください
Explanation:
ホスト障害発生後、SQL03 VMがパワーオンされなかった理由の一つとして、クラスタがデフォルト（ベストエフォート）のVM高可用性モードで構成されていたことが挙げられます。このモードでは、残りのホストのリソースが不足した場合、VMの可用性が保証されません。この問題を解決するには、VM高可用性モードを「保証（予約セグメント）」に変更することをお勧めします。これにより、障害が発生したホストからのVMのフェイルオーバーに備えて、各ホストにメモリが予約されます。これにより、ホスト障害が発生した場合でも、SQL03 VMが別のホストで再起動される可能性が高まります。
VM の高可用性モードを保証 (予約済みセグメント) に変更するには、次の手順に従います。
Prism Central にログインし、SQL VM が実行されているクラスターを選択します。
右上隅の歯車アイコンをクリックし、クラスター設定を選択します。
[クラスター サービス] の下で、[仮想マシンの高可用性] をクリックします。
ドロップダウン メニューから [保証 (予約済みセグメント)] を選択し、[保存] をクリックします。
単一のホスト障害が最小限のSQL VM数にしか影響を及ぼさないように環境を構成するには、アンチアフィニティルールの使用をお勧めします。アンチアフィニティルールは、同じグループに属するVMが同じホスト上で実行されないようにします。これにより、1つのホストに障害が発生した場合、影響を受けるSQL VMは1つだけで、他のSQL VMは別のホスト上で引き続き実行されます。
SQL VM のアンチアフィニティ ルールを作成するには、次の手順に従います。
Prism Central にログインし、左側のメニューの「エンティティ」をクリックします。
ドロップダウン メニューから仮想マシンを選択し、グループの作成をクリックします。
SQL グループなどのグループの名前を入力し、[次へ] をクリックします。
リストから SQL VM (SQL01、SQL02、SQL03) を選択し、[次へ] をクリックします。
ドロップダウン メニューから [Anti-Affinity] を選択し、[次へ] をクリックします。
グループの詳細を確認し、「完了」をクリックします。
これがお役に立てれば幸いです。他に何かお手伝いできることはありますか？
https://portal.nutanix.com/page/documents/details?targetId=AHV-Admin-Guide-v6_5:ahv-affinity-policies-c.html

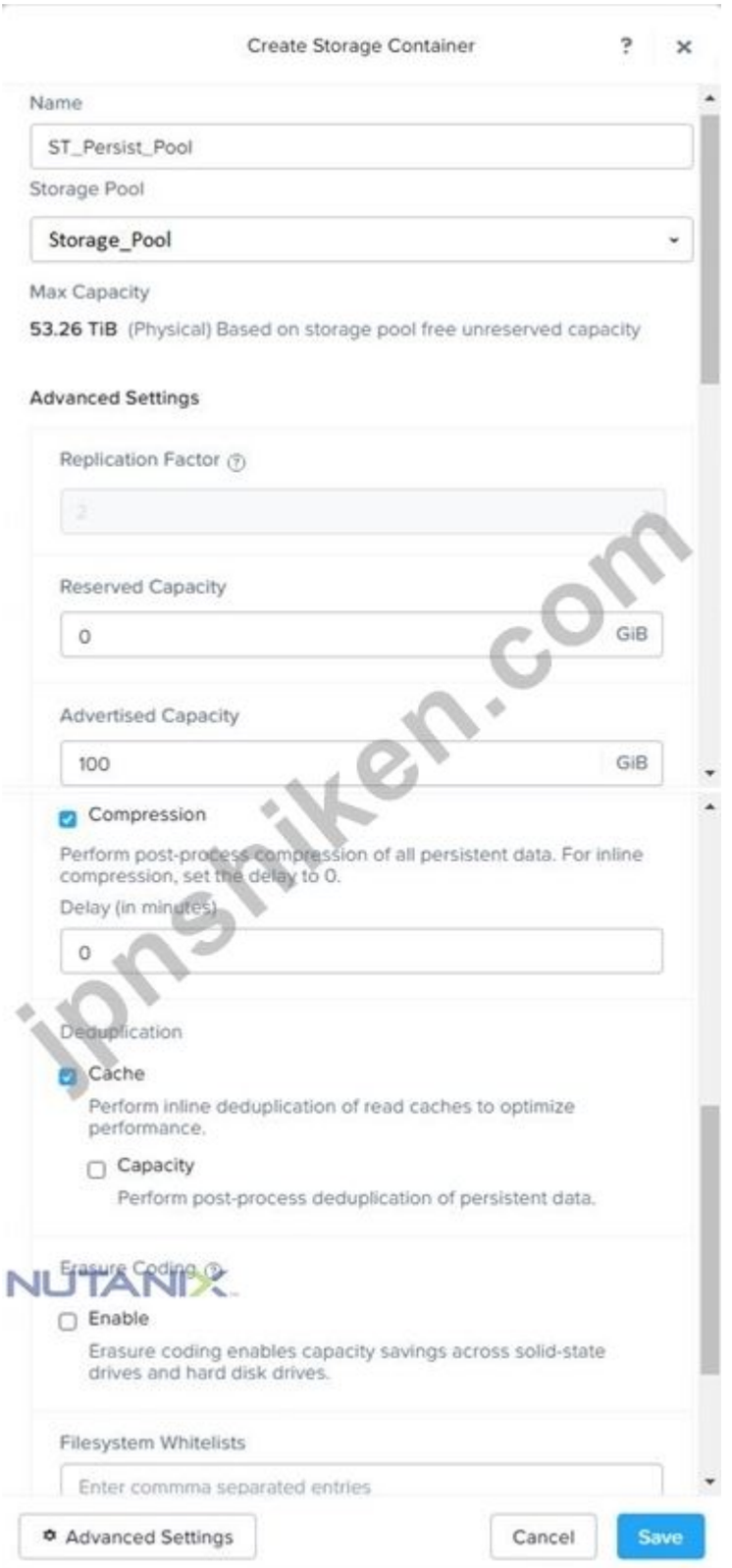
質問: **4**
タスク16
アップグレード前にクラスタで NCC を実行すると、次の出力が表示されます FAIL: CVM システム パーティション /home の使用率が 93% (しきい値の 90% を超えています) 問題のある CVM を特定し、ストレージの膨張を引き起こしているファイルを削除し、問題のある CVM でのみ個別のディスク使用率ヘルス チェックを実行してヘルスを再度確認します。NCC ヘルス チェックは実行しないでください。注: 影響を受けるノードからは個別のヘルス チェックのみを実行するようにしてください。
正解:
ステップバイステップの解決策については説明をご覧ください
Explanation:
問題のある CVM を特定し、ストレージの膨張の原因となっているファイルを削除して、再度正常性を確認するには、次の手順に従います。
Prism Central にログインし、左側のメニューの 「エンティティ」をクリックします。
ドロップダウンメニューから 「仮想マシン」を選択し、リストからNCCヘルスチェックの出力ファイルを見つけます。ファイルの場所は、日時情報で確認できます。ファイル名は 「ncc-output-YYYY-MM-DD-HH-MM-SS.log」のような形式です。
ファイルを開き、 「FAIL: CVM システムパーティション /home の使用率が 93% (しきい値の 90% を超えています)」という行を探します。問題が発生している CVM の IP アドレスをメモしてください。XXXX のような形式になっているはずです。
提供されたユーザー名とパスワードを使用して、SSH またはコンソールを使用して CVM にログインします。
du -sh /home/* コマンドを実行すると、/home 配下の各ファイルとディレクトリのディスク使用量を確認できます。ディスク容量の大部分を占めているファイルを特定してください。ログファイル、バックアップファイル、一時ファイルなどが考えられます。CVM に必要なシステムファイルや設定ファイルではないことを確認してください。
rm -f /home/<filename> コマンドを実行して、ストレージ容量の肥大化の原因となっているファイルを削除します。<filename> を実際のファイル名に置き換えてください。

ncc health_checks hardware_checks disk_checks disk_usage_check --cvm_list=XXXX コマンドを実行し、問題のあるCVMのみで個別のディスク使用率ヘルスチェックを実行し、ヘルスチェックを再度実行します。XXXX は、先ほどメモしておいたCVMのIPアドレスに置き換えてください。出力に「PASS: CVM システムパーティション /home の使用率が XX% (しきい値の 90% 未満)」と表示されていることを確認します。これは問題が解決されたことを意味します。
#PuttyによるCVM IPへのアクセス
allssh df -h #パス/dev/sdb3を探し、CVMのIPを選択します
ssh CVM_IP
ls
CDソフトウェアダウンロード
ls
CD番号
ls -l -h
rm ファイル名
df -h
ncc ヘルスチェック ハードウェアチェック ディスクチェック ディスク使用状況チェック

質問: **5**
タスク2
管理者は、Citrix ベースの仮想デスクトップ インフラストラクチャのストレージを構成する必要があります。
2つのVDIプールが作成されます
MCS を使用するタスク ユーザー向けの非永続プール名 MCS_Pool、Microsoft Windows 10 仮想配信エージェント (VDA)、パワー ユーザー向けの完全クローン Microsoft Windows 10 VDA を含む永続プール名 Persist_Pool
すべてのパワー ユーザー VDA に対して、ストレージ コンテナー レベルで 20 GiB の容量を保証する必要があります。パワー ユーザー コンテナーは 100 GiB を超える容量を使用できないようにする必要があります。ストレージ容量は、デスクトップ プールごとに最適化する必要があります。
これらの要件を満たすようにストレージを構成します。作成される新しいオブジェクトには、そのオブジェクトを使用するプール（MCS または Persist）の名前を含める必要があります。
オブジェクトがそのプールで使用されない場合は、プール名を含めないでください。
ソリューションに必要な追加ライセンスは後で追加されます。
正解:
ステップバイステップの解決策については説明をご覧ください
Explanation:
Citrix ベースの VDI のストレージを構成するには、次の手順に従います。
提供された資格情報を使用して Prism Central にログインします。
[ストレージ] > [ストレージ プール] に移動し、[ストレージ プールの作成] をクリックします。

新しいストレージプールの名前（例VDI_Storage_Pool）を入力し、プールに含めるディスクを選択します。SSDとHDDは任意の組み合わせで使用できますが、最適なパフォーマンスを得るには、HDDよりもSSDを多く使用することをお勧めします。
[保存] をクリックしてストレージ プールを作成します。
[ストレージ] > [コンテナー] に移動し、[コンテナーの作成] をクリックします。
非永続プールの新しいコンテナーの名前 (MCS_Pool_Container など) を入力し、作成したストレージ プール (VDI_Storage_Pool) をソースとして選択します。
詳細設定で重複排除と圧縮を有効にして、非永続デスクトップのストレージ容量を削減します。また、クラスターに十分なノードがあり、さらにスペースを節約したい場合は、イレイジャーコーディングを有効にすることもできます。これらの設定は、非永続プールのストレージ容量を最適化するのに役立ちます。
[保存] をクリックしてコンテナを作成します。
「ストレージ」> 「コンテナー」に移動し、もう一度 「コンテナーの作成」をクリックします。
永続プールの新しいコンテナーの名前 (Persist_Pool_Container など) を入力し、ソースとして同じストレージ プール (VDI_Storage_Pool) を選択します。
「詳細設定」で 「容量予約」を有効にし、予約容量として20GiBを入力します。これにより、永続デスクトップで常に20GiBの容量が確保されます。また、このコンテナが使用できる最大容量を制限するために、アドバタイズ容量として100GiBを入力することもできます。これらの設定は、永続プールへのストレージ割り当てを制御するのに役立ちます。
[保存] をクリックしてコンテナを作成します。
[ストレージ] > [データストア] に移動し、[データストアの作成] をクリックします。
非永続プール用の新しいデータストアの名前（例MCS_Pool_Datastore）を入力し、データストアの種類としてNFSを選択します。ソースとして、先ほど作成したコンテナ 「MCS_Pool_Container」を選択します。
[保存] をクリックしてデータストアを作成します。
「ストレージ」> 「データストア」に移動し、もう一度 「データストアの作成」をクリックします。
永続プール用の新しいデータストアの名前（例Persist_Pool_Datastore）を入力し、データストアの種類としてNFSを選択します。ソースとして、先ほど作成したコンテナ 「Persist_Pool_Container」を選択します。
[保存] をクリックしてデータストアを作成します。
データストアはクラスタ内のすべてのノードに自動的にマウントされます。「ストレージ」> 「データストア」に移動し、各データストアをクリックすると、すべてのノードが 「ホスト」の下にリストされていることがわかります。
Citrix Studioを使用して、これらのデータストア上にMCSまたはフルクローンを使用したVDIプールを作成できるようになりました。Citrix StudioをNutanix Acropolisで使用する方法の詳細については、 「Nutanix上のCitrix Virtual Apps and Desktops」または 「Nutanix仮想化環境」を参照してください。

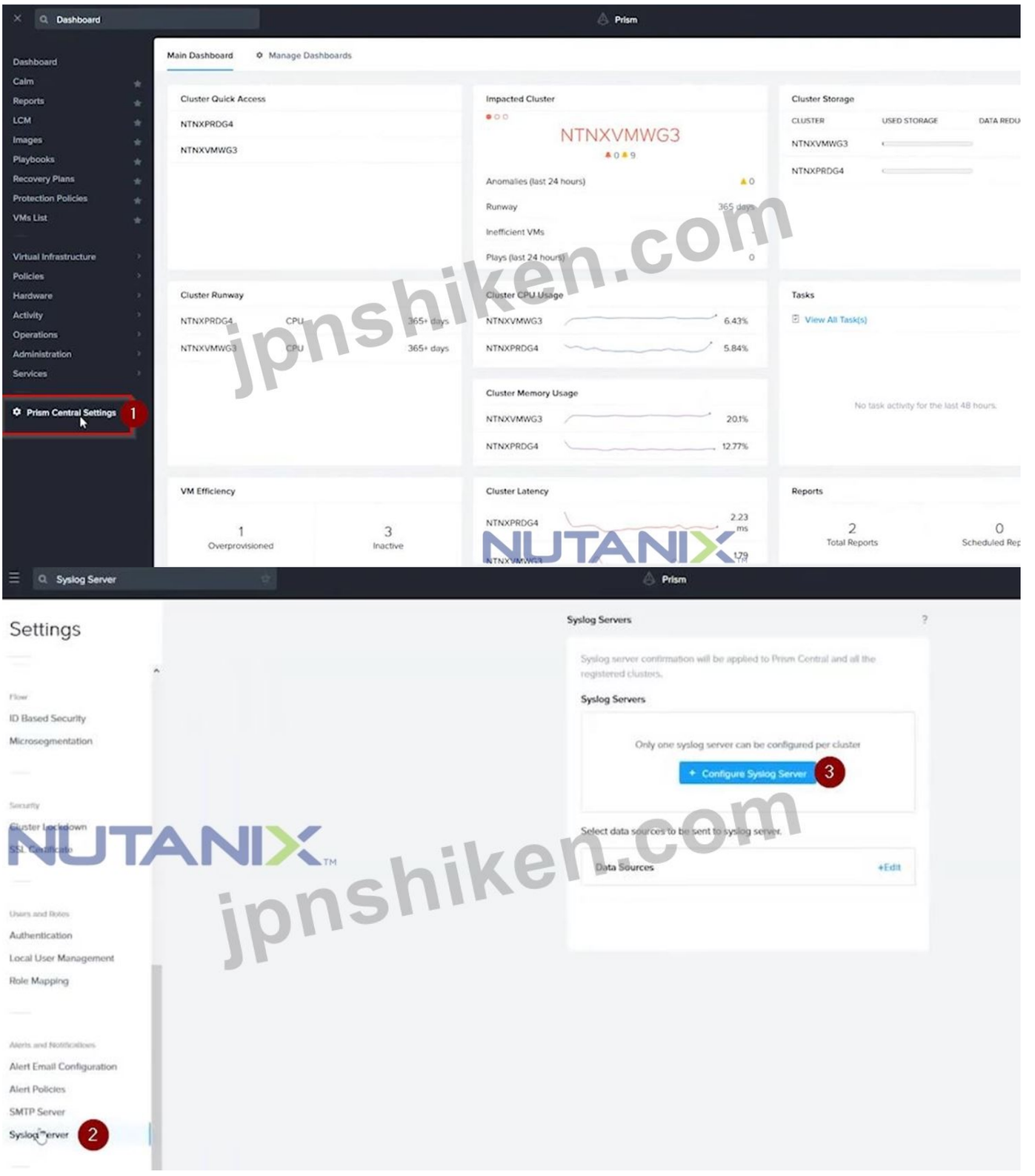


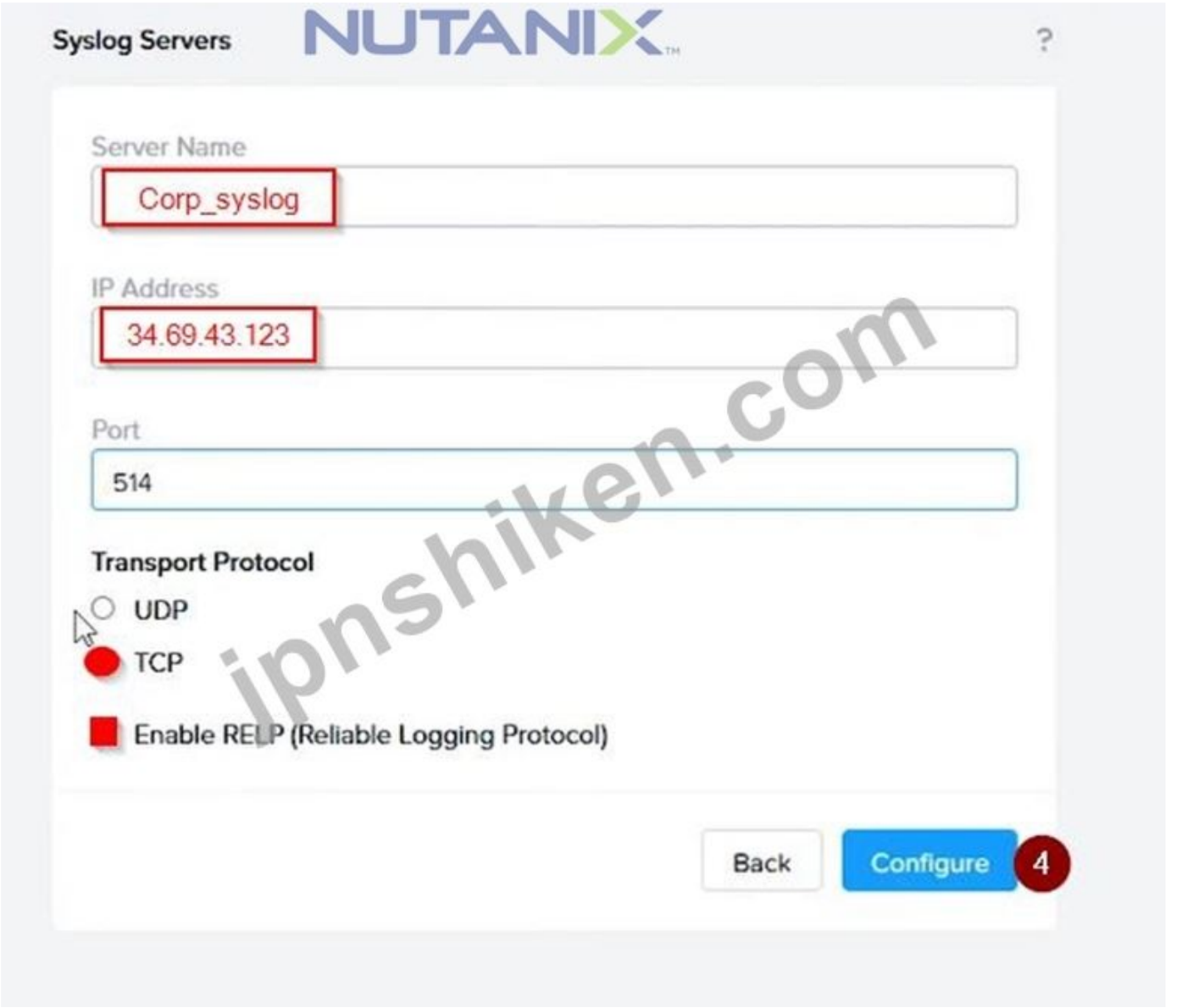


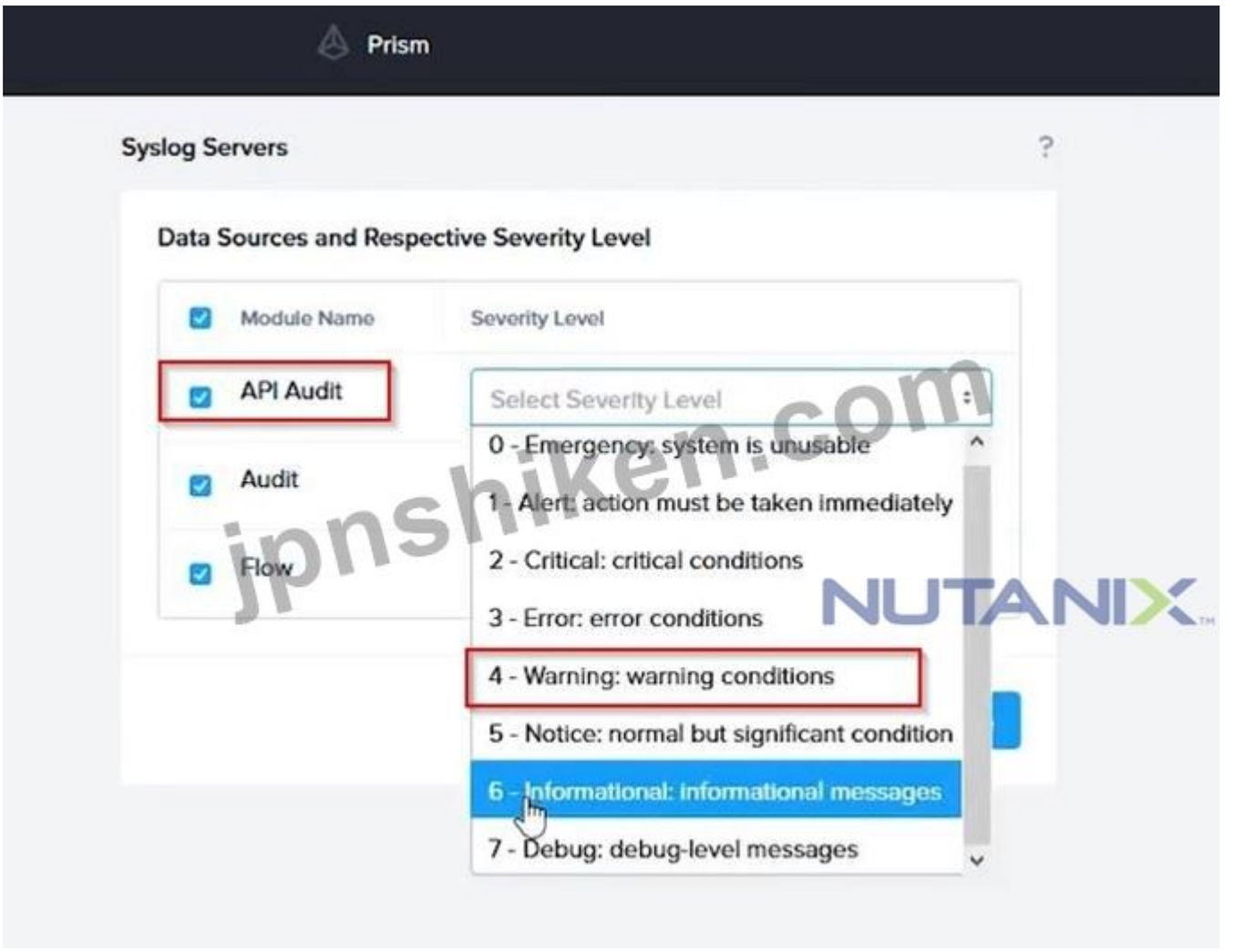
https://portal.nutanix.com/page/documents/solutions/details?targetId=BP-2079-Citrix-Virtual-Apps-and-Desktops:bp-nutanix-storage-configuration.html

質問: 6
タスク8

試験項目を実行する順序によっては、アクセス情報と認証情報が変更される場合があります。クラスターへのアクセスに問題がある場合は、クラスターBで実行した他の項目を参照してください。
情報セキュリティチームは、APIリクエストとレプリケーション機能の監査ログをすべてのクラスタで上位4つの重大度レベルまで有効化し、可能な限り高い信頼性でSyslogシステムにプッシュすることを要求しました。その他のログは含めないよう要求されています。
Syslog 構成:
Syslog名: Corp_syslog
システム IP: 34.69.43.123
ポート: 514
クラスターがこれらの要件を満たすように構成されていることを確認します。
正解:
ステップバイステップの解決策については説明をご覧ください
Explanation:
情報セキュリティ チームの要件を満たすようにクラスターを構成するには、次の手順を実行する必要があります。
Prism Centralにログインし、「ネットワーク」>「Syslogサーバー」>「Syslogサーバーの設定」に進みます。サーバー名に「Corp_syslog」、IPアドレスに「34.69.43.123」、ポートに「514」を入力します。トランスポートプロトコルに「TCP」を選択し、RELP（Reliable Logging Protocol）を有効にします。これにより、最高レベルの信頼性を備えたSyslogサーバーが作成されます。
データソースの「編集」をクリックし、クラスターとして「クラスターB」を選択します。データソースとして「APIリクエスト」と「レプリケーション」を選択し、両方のログレベルを「CRITICAL」に設定します。これにより、APIリクエストの監査ログと、上位4つの重大度レベル（EMERGENCY、ALERT、CRITICAL、ERROR）のレプリケーション機能が有効になり、Syslogサーバーにプッシュされます。「保存」をクリックします。
同じ要件で構成する他のクラスターについては、手順 2 を繰り返します。







Nutanix クラスターを構成して、API リクエストとレプリケーション機能の監査ログを有効にし、可能な限り最高の信頼性で syslog システムにプッシュするには、次の手順に従います。

管理者の資格情報を使用して、Nutanix Prism Web コンソールにログインします。

Prism 内の 「設定」セクションまたは構成設定インターフェースに移動します。

「Syslog 構成」または 「ログ記録」オプションを見つけてクリックします。

次のように Syslog 設定を構成します。

Syslog 名: Syslog 構成の名前として 「Corp_syslog」と入力します。

Syslog IP: IP アドレスを Syslog システムの IP アドレスである 「34.69.43.123」に設定します。

ポート: ポートを syslog のデフォルト ポートである 「514」に設定します。

最高信頼性または永続的なログ記録のオプション（利用可能な場合）を有効にします。これにより、ネットワークが中断された場合でもログが確実に送信され、失われることがなくなります。

Syslog 設定を保存します。

API リクエストの監査ログを有効にする:

Nutanix Prism Web コンソールで、「クラスター」セクションまたはクラスター管理インターフェースに移動します。

監査ログを有効にする目的のクラスターを選択します。

「監査構成」または 「セキュリティ構成」オプションを見つけてクリックします。

監査ログとAPIリクエストに関する設定を探します。監査ログ機能を有効にし、ログに記録する上位4つの重大度レベルを選択します。
監査構成を保存します。
レプリケーション機能の監査ログを有効にする:
Nutanix Prism Web コンソールで、「クラスター」セクションまたはクラスター管理インターフェースに移動します。
監査ログを有効にする目的のクラスターを選択します。
「監査構成」または「セキュリティ構成」オプションを見つけてクリックします。
監査ログとレプリケーション機能に関する設定を確認します。監査ログ機能を有効にし、ログに記録する上位4つの重大度レベルを選択します。
監査構成を保存します。
これらの手順を完了すると、Nutanix クラスタは API リクエストとレプリケーション機能の監査ログを有効にするように構成されます。ログは、可能な限り高い信頼性で指定された syslog システムに送信されます。
ncli
<ncli> rsyslog-config set-status enable=false
<ncli> rsyslog-config add-server name=Corp_Syslog ip-address=34.69.43.123 port=514 network-protocol=tdp relp-enabled=false
<ncli> rsyslog-config add-module サーバー名= Corp_Syslog モジュール名=APLOS レベル=INFO
<ncli> rsyslog-config add-module サーバー名= Corp_Syslog モジュール名=CEREBRO レベル=INFO
<ncli> rsyslog-config set-status enable=true
https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e0000009CEECA2