Nutanix.NCM-MCI-6.10.v2026-07-14.q11

試験コード:	NCM-MCI-6.10
試験名称:	Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI)
認定資格:	Nutanix
無料問題数:	11
バージョン:	v2026-07-14
アクセス数:	108
ページビュー数:	110
https://www.jpnpdf.com/Nutanix.NCM-MCI-6.10.v2026-07-14.q11-mondaishu.html	

最新問題: **1**
タスク6
管理者は、AHV Turboによってゲストレベルで得られるパフォーマンス向上を評価する必要があります。
テストを実行するために、管理者はTurboという名前のWindows 10仮想マシンを以下の構成で作成しました。
1 vCPU
8GB RAM
SATAコントローラー
40GB仮想ディスク
ストレステストアプリケーションはマルチスレッドに対応していますが、AHV Turboを有効にした場合、期待どおりのパフォーマンスが得られません。AHV Turboをより効果的に活用できるよう、VMの設定を調整してください。
注：仮想マシン（VM）の電源は入れないでください。電源を入れずに、可能な限りVMの設定または設定準備を完了してください。
Answer:
VMがAHV Turboをより効果的に活用できるように構成するには、以下の手順に従ってください。
提供された認証情報を使用して、クラスターAのPrism Elementにログインしてください。
VM > テーブルに移動し、Turboという名前のVMを選択します。
Click on Update and go to Hardware tab.
Increase the number of vCPUs to match the number of multiqueues that you want to enable. For example, if you want to enable 8 multiqueues, set the vCPUs to 8. This will improve the performance of multi-threaded workloads by allowing them to use multiple processors.
Change the SCSI Controller type from SATA to VirtIO. This will enable the use of VirtIO drivers, which are required for AHV Turbo.
Click Save to apply the changes.
Power off the VM if it is running and mount the Nutanix VirtIO ISO image as a CD-ROM device. You can download the ISO image from Nutanix Portal.
Power on the VM and install the latest Nutanix VirtIO drivers for Windows 10. You can follow the instructions from Nutanix Support Portal.

After installing the drivers, power off the VM and unmount the Nutanix VirtIO ISO image.
Power on the VM and log in to Windows 10.
Open a command prompt as administrator and run the following command to enable multiqueue for the VirtIO NIC:
ethtool -L eth0 combined 8
Replace eth0 with the name of your network interface and 8 with the number of multiqueues that you want to enable.
You can use ipconfig /all to find out your network interface name.
Restart the VM for the changes to take effect.
You have now configured the VM to better leverage AHV Turbo. You can run your stress test application again and observe the performance gains.
https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e000000LKPdCAOchangev
CPUto 2/4 ?
Change SATA Controller to SCSI:
acli vm.get Turbo
Output Example:
Turbo {
config {
agent_vm: False
allow_live_migrate: True
boot {
boot_device_order: "kCdrom"
boot_device_order: "kDisk"
boot_device_order: "kNetwork"
uefi_boot: False
}
cpu_passthrough: False
disable_branding: False
disk_list {
addr {
bus: "ide"
index: 0
}
cdrom: True
device_uuid: "994b7840-dc7b-463e-a9bb-1950d7138671"
empty: True
}
disk_list {
addr {
bus: "sata"
index: 0
}
container_id: 4

container_uuid: "49b3e1a4-4201-4a3a-8abc-447c663a2a3e"
device_uuid: "622550e4-fb91-49dd-8fc7-9e90e89a7b0e"
naa_id: "naa.6506b8dcda1de6e9ce911de7d3a22111"
storage_vdisk_uuid: "7e98a626-4cb3-47df-a1e2-8627cf90eae6"
vmdisk_size: 10737418240
vmdisk_uuid: "17e0413b-9326-4572-942f-68101f2bc716"
}
flash_mode: False
hwclock_timezone: "UTC"
machine_type: "pc"
memory_mb: 2048
name: "Turbo"
nic_list {
connected: True
mac_addr: "50:6b:8d:b2:a5:e4"
network_name: "network"
network_type: "kNativeNetwork"
network_uuid: "86a0d7ca-acfd-48db-b15c-5d654ff39096"
type: "kNormalNic"
uuid: "b9e3e127-966c-43f3-b33c-13608154c8bf"
vlan_mode: "kAccess"
}
num_cores_per_vcpu: 2
num_threads_per_core: 1
num_vcpus: 2
num_vnuma_nodes: 0
vga_console: True
vm_type: "kGuestVM"
}
is_rf1_vm: False
logical_timestamp: 2
state: "Off"
UUID: "9670901f-8c5b-4586-a699-41f0c9ab26c3"
}
acli vm.disk_create Turbo clone_from_vmdisk=17e0413b-9326-4572-942f-68101f2bc716 bus=scsi 古いディスクを削除します acli vm.disk_delete 17e0413b-9326-4572-942f-68101f2bc716 disk_addr=sata.0

最新問題**: 2**
貴社のセキュリティチームは、セキュリティポリシーを管理するための自動化に取り組んでいます。
彼らは既存のルールの一部をデスクトップ上の「Security Policy.txt」ファイルにエクスポートしました。このファイルはテスト環境に合わせて変更する必要があります。

隔離規則を除くすべての規則は記録する必要があります。
* 隔離ルールのみが適用され、その他のルールはログに記録されるだけです。
* 隔離ルールはSecOps環境に影響を与えるべきである。
* SMBルールは、「smbhost」および「smbclient」タグを持つVMにのみ影響します。
* 「DNテスト」ポリシーはIPv6を許可し、含まれる階層間のプロトコルを制限してはならない。
ファイルには3つのルールがあります。行の削除、追加、コピーはしないでください。xxxx は適切な値に置き換えてください。すべての「xxxx」が置き換えられるとは限りません。
同じ名前でファイルを保存してください。
「xxxx」を置き換える可能性のある値：
8080
全て
適用する
間違い
モニター
非生産
SecOps
smbhost
smbclient
TCP
真実
Answer:
詳しい説明については、下記の解説をご覧ください。
Explanation:
セキュリティポリシーファイルを必要に応じて変更するための手順を以下に示します。
デスクトップに移動し、メモ帳などのテキストエディタを使用して、Security Policy.txt ファイル（提供されている Security Policy.bak の内容に対応するファイル）を開きます。
セキュリティ要件に従って、xxxxxとxxxxのプレースホルダーを置き換えることでファイルの内容を変更します。
規則による変更
ファイル内で行う具体的な変更点は以下のとおりです。
1. 検疫規則
要件1（ログ記録なし）：隔離ールはログに記録してはならない。
「is_policy_hitlog_enabled」を「xxxx」から「is_policy_hitlog_enabled」を「false」に変更します。要件2（適用）この:のルールは適用されなければなりません。
「アクション」:「xxxx」（quarantine_rule の下）を「アクション」:「APPLY」に変更します。
要件3（環境）この:のルールは「SecOps」環境に影響を与えるものでなければならない。
「環境」: ["xxxxx"] を「環境」: ["SecOps"] に変更します。
2. SMBブロックルール
要件1（ログ記録）このルールはログに記録されなければなりません。

「is_policy_hitlog_enabled」を「xxxxx」から「is_policy_hitlog_enabled」を「True」に変更します。要件 2 (モニター): このルールは強制適用せず、ログに記録するだけにしてください。
「action」: 「xxxxx」(isolation_rule の下)を「action」: 「MONITOR」に変更します。
要件4 (タグ) ルールは「smbhost」タグと「smbclient」タグに影響を与える必要があります。
「SMBv1」: [「xxxxx」] を「SMBv1」: [「smbhost」]に変更します。
「SMRv1」: ["xxxxx"] を「SMRv1」: ["smbclient"] に変更します。
3. DNテスト (dn-policy1)ルール
要件2(監視)このルールは強制適用せず、ログに記録するだけにしてください。
app_rule 内の "action": "xxxx" を "action": "MONITOR" に変更します。
要件5 (IPv6の許可) このポリシーはIPv6トラフィックを許可する必要があります。
「allow_ipv6_traffic」を「xxxx」に変更します。
最終ステップ
すべての置換が完了したら、ファイルを保存し、デスクトップ上の元の Security Policy.txt を上書きしてください。
完成したルールの例 (xxxxx を適切に置き換えてください) :
ルール名 : 隔離レール
ログ記録: false
アクション : 適用
環境: SecOps
プロトコル: TCP
ポート: 8080
ルール名: SMBルール
記録済み: True
アクション : 監視
タグ: smbhost、smbclient
プロトコル: TCP
ポート: 8080
ルール名: DNテストポリシー
記録済み: True
アクション : 監視
環境 : 非本番環境
プロトコル :すべて
ポート: 8080

最新問題**: 3**
タスク14
管理者は、複数のワーカーVMにまたがる大規模なデータセットを使用する分散アプリケーション用のストレージを構成するよう依頼された。
ワーカーVMはすべてのノードで稼働する必要があります。データ耐障害性はアプリケーションレベルで提供され、1GBあたりの低コストが重要な要件です。

これらの要件を満たすように、クラスター上のストレージを設定してください。新しく作成するオブジェクトには、名前に「Distributed_App」という語句を含める必要があります。

Answer:

手順ごとの解決方法については、解説をご覧ください。

Explanation:

分散アプリケーション用のクラスタ上のストレージを構成するには、以下の手順に従ってください。

提供された認証情報を使用して、クラスターAのPrism Elementにログインしてください。

「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：Distributed_App_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は自由に組み合わせることができますが、1GBあたりのコストを抑えるには、SSDよりもHDDを多く使用する方が望ましいでしょう。

「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」に移動し、「コンテナの作成」をクリックします。

新しいコンテナの名前（例：Distributed_App_Container）を入力し、ソースとして先ほど作成したストレージプール「Distributed_App_Storage_Pool」を選択します。

詳細設定で、イレイジャーコーディングと圧縮を有効にすると、データのストレージ容量を削減できます。

データの回復性はアプリケーションレベルで提供されるため、レプリケーション係数を無効にすることもできます。

これらの設定により、コンテナの1GBあたりのコストを低く抑えることができます。

コンテナを作成するには、「保存」をクリックしてください。

「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。

新しいデータストアの名前（例：Distributed_App_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「Distributed_App_Container」を選択してください。

「保存」をクリックしてデータストアを作成します。

The datastore will be automatically mounted on all nodes in the cluster. You can verify this by going to Storage > Datastores and clicking on Distributed_App_Datastore. You should see all nodes listed under Hosts.

You can now create or migrate your worker VMs to this datastore and run them on any node in the cluster.

The datastore will provide low cost per GB and high performance for your distributed application.

最新問題**: 4**

タスク15

試験問題に取り組む順番によっては、アクセス情報や認証情報が変わる場合があります。

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で実行され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に関する監査ログを、すべてのクラスターで上位4つの重要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よう要求しました。その他のログは含めないよう求めています。

Syslogの設定：

Syslog名: Corp_syslog

Syslop 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てください。

Answer:

手順ごとの解決方法については、解説をご覧ください。

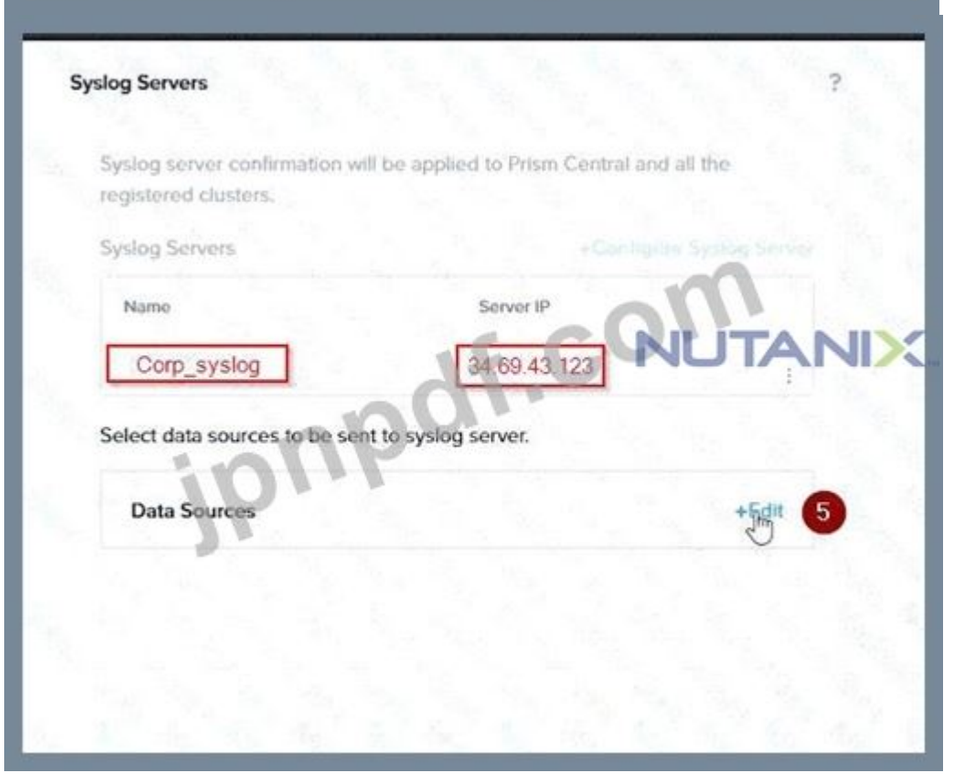
Explanation:

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、以下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」、ポート番号に「514」を入力します。トランスポートプロトコルとして「TCP」を選択し、RELP（信頼性ログプロトコル）を有効にします。これにより、可能な限り高い信頼性を備えたSyslogサーバーが作成されます。

「データソース」の横にある「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リクエストとレプリケーション機能の監査ログが、上位4つの重大度レベル（EMERGENCY、ALERT、CRITICAL、ERROR）で有効になり、syslogサーバーに送信されます。「保存」をクリックします。

同じ要件で構成したい他のクラスターについても、手順2を繰り返してください。



Nutanixクラスタを構成して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、可能な限り高い信頼性でsyslogシステムにログを送信するには、以下の手順に従ってください。

管理者権限を使用して、Nutanix PrismのWebコンソールにログインしてください。

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設定」または ログ記録」オプションを探してクリックします。

syslogの設定を以下のように構成してください。
Syslog名: Syslog設定の名前として「Corp_syslog」と入力してください。
Syslog IP: IPアドレスを「34.69.43.123」に設定します。これはSyslogシステムのIPアドレスです。
ポート: ポートを「514」に設定してください。これはsyslogのデフォルトポートです。
利用可能な場合は、最高レベルの信頼性または永続的なログ記録のオプションを有効にしてください。これにより、ログが確実に送信され、ネットワーク障害が発生した場合でも失われることがなくなります。
syslogの設定を保存します。
APIリクエストの監査ログを有効にする：
Nutanix PrismのWebコンソールで、「クラスタ」セクションまたはクラスタ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クラスターを選択してください。
「監査設定」または「セキュリティ設定」オプションを探してクリックします。
監査ログとAPIリクエストに関連する設定を探します。監査ログ機能を有効にして、一番上の項目を選択します。
記録すべき重症度レベルは4段階です。
監査設定を保存します。
レプリケーション機能の監査ログを有効にする：
Nutanix PrismのWebコンソールで、「クラスタ」セクションまたはクラスタ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クラスターを選択してください。
「監査設定」または「セキュリティ設定」オプションを探してクリックします。
監査ログとレプリケーション機能に関する設定を探してください。監査ログ機能を有効にし、ログに記録する上位4つの重要度レベルを選択してください。
監査設定を保存します。
これらの手順を完了すると、Nutanix クラスターは、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 server-name= Corp_Syslog module-name=APLOS level=INFO
<ncli> rsyslog-config add-module server-name= Corp_Syslog module-name=CEREBRO level=INFO
<ncli> rsyslog-config set-status enable=true
https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e0000009CEECA2

最新問題: **5**
新たなセキュリティガイドラインに従い、今後は重要な仮想マシンのストレージが暗号化されるようにしなければならない。
割り当ては、Prism Central に新しく作成された「VM-Storage」というカテゴリに対して、「Softwareencrypted」という値で行います。将来の使用のために、「SEDencrypted」という別の値も作成しておいてください。
上記カテゴリを作成し、Prism CentralでVMベースのストレージ暗号化に関する詳細な設定を行ってください。
新しく作成したポリシーに「Encrypted-Storage」という名前を割り当ててください。

Answer:
詳しい説明については、下記の解説をご覧ください。
Explanation:
Prism Central内でカテゴリとそれに対応するストレージ暗号化ポリシーを作成するための手順を以下に示します。
1. カテゴリを作成する
まず、カテゴリと要求された2つの値を作成する必要があります。
* Prism Centralで、[管理] > [カテゴリ]に移動します。
* 「新しいカテゴリ」をクリックしてください。
* [名前] フィールドに「VM-Storage」と入力します。
* 「値の追加」フィールドに「softwareencrypted」と入力し、「追加」（プラス）ボタンをクリックします。
* 再度「値の追加」フィールドに「SEDencrypted」と入力し、「追加」（プラス）ボタンをクリックします。
* 「保存」をクリックしてください。
2. 暗号化ポリシーを作成する
次に、新しいカテゴリを使用するセキュリティポリシーを作成します。
* Prism Centralで、[セキュリティ] > [保存データの暗号化]に移動します。
* [+ セキュリティ ポリシーの作成] ボタンをクリックします。
* [ポリシー名] フィールドに「Encrypted-Storage」と入力します。
* 暗号化の種類が「ソフトウェアベース」に設定されていることを確認してください。
* ターゲットVMについては、カテゴリに一致するVMのラジオボタンを選択してください。
* [カテゴリの選択] ドロップダウンで、先ほど作成した VM-Storage カテゴリを選択します。
* [値の選択] ドロップダウンで、[ソフトウェア暗号化] を選択します。
* 「保存」をクリックしてください。
このポリシーにより、VM-Storage: softwareencrypted カテゴリが割り当てられた新規または既存の仮想マシンに、ソフトウェアベースの暗号化が自動的に適用されます。

最新問題**: 6**
A company who offers Infrastructure as a Service needs to onboard a new customer. The new customer requires a dedicated cloud plan which tolerates two host failures.
The customer is planning to move current workloads in three waves, with three months between waves starting today:
* Wave One: 100 VMs
* Wave Two: 50 VMs
* Wave Three: 20 VMs
Workload profile is:
* vCPU: 4
* vRAM: 16 GB
* Storage: 200 GB
The service provider company needs to estimate required resources upfront, to accommodate customer requirements, considering also that:

* limit the number of total nodes
* selected system vendor HPE
* selected model DX365-10-G11-NVMe
* full-flash node (including NVMe + SSD)
* 12 months runway

Create and save the scenario as IaaS and export to the desktop, name the file IaaS-requirement.pdf Note: You must export the PDF to the desktop as IaaS-requirement.pdf to receive any credit.

Answer:

See the Explanation below for detailed answer.

Explanation:

Here is the step-by-step solution to create and export the capacity planning scenario. This task is performed within Prism Central.

1. Navigate to the Planning Dashboard

* From the Prism Central main menu (hamburger icon), navigate to Operations > Planning.

2. Create and Define the Scenario

* [+シナリオを作成]ボタンをクリックします。
* ダイアログボックス内:
* シナリオ名: IaaS
* シナリオタイプ: 新しいワークロードを選択
* 「作成」をクリックします。シナリオエディタが開きます。

3. クラスターとランウェイの設定

* 「IaaS」シナリオエディタで、ランウェイ設定（左上を見つけて、「2ヵ月」に設定します。
* クラスター構成タイルを見つけて、[編集]をクリックします。
* 許容するホスト障害数を2に設定します。
* 「保存」をクリックしてください。

4. ワークロードプロファイルを定義する

* [ワークロード] セクションで、[+ ワークロードを追加] ボタンをクリックします。
* 「新しいワークロードプロファイルを作成する」を選択します。
* VMの仕様を入力してください。
* ワークロード名: Customer-VM (または類似の名称)
* VMあたりのvCPU数 :4
* VMあたりのメモリ容量 :16GB
* VMあたりのストレージ容量 :200GB
* 「追加」をクリックします。

5. 業務量増加計画（段階的増加計画）を設定する

* メインシナリオエディタに戻ります。タイムラインセクション（「ワークロードプラン」）で、VMを追加します。
* 第1波（本日） :
* 「今日」列の下にある「+追加」をクリックします。
* 顧客VMプロファイルを選択します。

* 仮想マシンを100台入力してください。
* 「追加」をクリックします。
* 第2波（3ヶ月）：
* タイムライン上の「+」アイコンをクリックします。
* 日付を今日から3ヶ月後に設定してください。
* この新しい「3か月」列の下にある「+追加」をクリックしてください。
* 顧客VMプロファイルを選択します。
* 仮想マシンを50台入力してください。
* 「追加」をクリックします。
* 第3波（6ヶ月）：
タイムライン上の「+」アイコンをクリックします。
* 日付を今日から6ヶ月後に設定してください。
* この新しい「6か月」列の下にある「+追加」をクリックしてください。
* 顧客VMプロファイルを選択します。
* 仮想マシンを20台入力してください。
* 「追加」をクリックします。
6. ハードウェアを選択する
* ハードウェア構成タイルで、[ハードウェアの変更]をクリックします。
* 「ハードウェアの選択」ペインで：
* ベンダー：HPEを選択してください。
* モデル:「DX365-10-G11-NVMe」を検索して選択してください。
* 注: このモデルは定義上フルフラッシュであり、要件を満たしています。
* 「完了」をクリックしてください。プランナーが必要なノードを再計算します。
7. シナリオを保存してエクスポートする
* 右上隅にある保存アイコン（フロッピーディスク）をクリックして、IaaSシナリオを保存します。
右上隅にあるエクスポートアイコン（下向きの矢印）をクリックします。
ドロップダウンメニューからPDFを選択してください。
* 「名前を付けて保存」ダイアログが表示されます。
デスクトップに移動します。
ファイル名をIaaS-requirement.pdfに設定してください。
* 「保存」をクリックしてください。

最新問題: 7
タスク4
管理者から、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の要求がありました。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/パッシブ構成で設定され、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を変更することなく両方のリンクを活用するように構成されている必要があります。
管理者が作業を開始し、デスクトップ\ファイル\ネットワーク\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 :これらのコマンドは、利用可能なクラスターでは実行できません。
未設定.txt
manage_ovs --bond_name brX-up --bond_mode xxxxxxxxxx --interfaces ethX,ethX update_uplinks manage_ovs --bridge_name brX-up --interfaces ethX,ethX --bond_name bond1 --bond_mode xxxxxxxxxx update_uplinks 手順ごとの解決策については、説明を参照してください。
Answer:
設定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設定するには、そのノードで以下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 をアクティブおよびパッシブなインターフェイスとして持つ br0-up という名前のボンドを作成し、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イスとして持つ bond1 という名前の別のボンドを作成し、それを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構成されます。
ファイル Desktop\Files\Network\unconfigured.txt 内の ｋ」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

最新問題**: 8**
管理者はNutanixクラスタ上でAOSとAHVのアップグレードを実行する必要があり、ホストとCVMの再起動時にVMデータが可能な限り迅速に複製されるようにしたいと考えています。
クラスター1を構成して、計画されたホストおよびCVMの再起動後、再構築スキャンが直ちに開始されるようにします。
注記：
この作業にはSSHを使用する必要があります。これが1ノードのクラスタであることは気にしないでください。
Answer:
詳しい説明については、下記の解説をご覧ください。
Explanation:
クラスター1で即時再構築スキャンを設定するための手順を以下に示します。
このタスクは、クラスタ1上のCVM（コントローラVM）に接続されたSSHセッションから実行する必要があります。
1. クラスター1のCVMにアクセスします。

* Prism Central ダッシュボードから、[ハードウェア] > [クラスタ] に移動し、[クラスタ 1] をクリックして、その Prism Element (PE) インターフェースを開きます。
* Cluster 1 PE で、[ハードウェア] > [CVM] に移動して、クラスタ内の任意の CVM の IP アドレスを確認します。
* SSHクライアント（PuTTYなど）を使用して、CVMのIPアドレスに接続します。
管理者ユーザー名とパスワードでログインしてください。
2. 再構築遅延設定を変更する
デフォルトでは、CVMの再起動後、クラスターは再構築スキャンを開始する前に15分（900秒）待機します。この設定を0に変更してください。
* CVMにログインしたら、次のコマンドを実行して遅延時間を0秒に設定します。
gflag --set --gflags=stargate_delayed_rebuild_scan_secs=0
*（任意ですが推奨）「get」コマンドを実行することで、変更が有効になったことを確認できます。
gflag --get --gflags=stargate_delayed_rebuild_scan_secs
出力にはstargate_delayed_rebuild_scan_secs=0と表示されるはずです。

最新問題**: 9**
Task 3
An administrator needs to create a report named VMs_Power_State that lists the VMs in the cluster and their basic details including the power state for the last month.
No other entities should be included in the report.
The report should run monthly and should send an email to admin@syberdyne.net when it runs.
Generate an instance of the report named VMs_Power_State as a CSV and save the zip file as Desktop\Files \VMs_Power_state.zip Note: Make sure the report and zip file are named correctly. The SMTP server will not be configured.
Answer:
See the Explanation for step by step solution.
Explanation:
To create a report named VMs_Power_State that lists the VMs in the cluster and their basic details including the power state for the last month, you can follow these steps:
Log in to Prism Central and click on Entities on the left menu.
Select Virtual Machines from the drop-down menu and click on Create Report.
Enter VMs_Power_State as the report name and a description if required. Click Next.
Under the Custom Views section, select Data Table. Click Next.
Under the Entity Type option, select VM. Click Next.
Under the Custom Columns option, add the following variables: Name, Cluster Name, vCPUs, Memory, Power State. Click Next.
Under the Time Period option, select Last Month. Click Next.
Under the Report Settings option, select Monthly from the Schedule drop-down menu. Enter admin@syberdyne.net as the Email Recipient. Select CSV as the Report Output Format. Click Next.
Review the report details and click Finish.

To generate an instance of the report named VMs_Power_State as a CSV and save the zip file as Desktop\Files \VMs_Power_state.zip, you can follow these steps:
Log in to Prism Central and click on Operations on the left menu.
Select Reports from the drop-down menu and find the VMs_Power_State report from the list. Click on Run Now.
Wait for the report to be generated and click on Download Report. Save the file as Desktop\Files \VMs_Power_state.zip.
1.Open the Report section on Prism Central (Operations > Reports)
2.Click on the New Report button to start the creation of your custom report
3.Under the Custom Views section, select Data Table
4.Provide a title to your custom report, as well as a description if required.
5.Under the Entity Type option, select VM
6.This report can include all as well as a selection of the VMs
7.Click on the Custom Columns option and add the below variables:
a.Name - Name of the listed Virtual Machine
b.vCPU - 仮想マシンに割り当てられたvCoreとvCPUの組み合わせ c.メモリ - 仮想マシンに割り当てられたメモリ量 d.ディスク容量 - 割り当てられた仮想ディスク容量の合計 e.ディスク使用量 - 使用されている仮想ディスク容量の合計 f.スナップショット使用量 - スナップショットによって使用されている容量の合計 (保護ドメインのスナップショットを除く)
8. メモリとディスク使用量の集計オプションで、デフォルトの平均オプションを受け入れます。

9. [追加]ボタンをクリックして、このカスタム選択をレポートに追加します。
10.次に、画面右下にある 「保存して今すぐ実行」ボタンをクリックします。
11.カスタムレポートに必要な詳細情報をこの画面に入力してください。
12. 「レポート期間」変数は、デフォルトの 「過去24時間」のままにしておくことができます。
13. 希望するレポート出力形式 (PDFまたはCSV)を指定し、必要に応じてレポートの送信先となる追加の受信者を指定してください。レポートは、作成後および初回実行後に必要に応じてダウンロードすることもできます。
14.以下は、このレポートのCSV形式の例です。

最新問題**: 10**
クラスター 1 上に、NVD-2031 の小型 VM 構成に一致する 「Small Template」という名前の VM テンプレートを作成します (Files\Documentation 6.10 フォルダーを参照)。ただし、デフォルトのストレージ コンテナーを使用します。
クラスター1について、NVD-2031に従ってSMTPアラートとNCCレポートを設定してください。

設定：
* SMTP: クラスター2のIPアドレスを使用する
* クラスターメールアドレス: cluster1@ACME.org
* アラートメール :primaryalerts@ACME.org、secondaryalerts@ACME.org
Answer:
詳しい説明については、下記の解説をご覧ください。
Explanation:
クラスター1で両方のタスクを完了するための手順を以下に示します。
この解決策では、まずクラスター2 $MTPサーバー用）のIPアドレスを特定し、次にクラスター1のPrism Elementインターフェース内で全ての設定を行う必要があります。
前提条件 :クラスター2のIPアドレスを見つける
* Prism Centralで、[ハードウェア] > [クラスタ]に移動します。
* リストの中からクラスター2を探し、そのIPアドレスをメモしてください。このIPアドレスは、以下の手順で使用します。
タスク1 :VMテンプレートを作成する
* クラスター 1 の Prism Element (PE) インターフェースにログインします。 PC から、[ハードウェア] > [クラスター] > [クラスター 1] をクリックします。）
* メインダッシュボードからVMビューに移動します。
* [+ VM の作成] ボタンをクリックします。
* NVD-2031の「小型VM」構成に基づいてVMの詳細を入力してください（例vCPU 2個、vCPUあたり1コア、RAM 4GB）。
* 名前: 小型テンプレート
* 計算の詳細:
* vCPU: 2
* Number of Cores per vCPU: 1
* Memory: 4 GB
* Scroll down to Storage and click + Add New Disk.
* Operation: Select Clone from Image Service.
* Image: Select any available guest OS image (e.g., a Windows or CentOS image).
* Storage Container: Ensure the default container is selected (as required by the task).
* Click Add.
* Scroll down to Network Adapters (NIC) and click + Add NIC.
* Select any available VLAN/Subnet (e.g., Primary).
* Click Add.
* Click Save. The VM will be created (and remain powered off).
* Find the new Small Template VM in the list. Select its checkbox.
* Click the Actions dropdown and select Convert to Template.
* Confirm the action by clicking OK.
Task 2: Configure SMTP and NCC Reports
* While still in the Cluster 1 Prism Element interface, click the gear icon (Settings) in the top-right corner.

* Select SMTP Server from the left-hand menu.
* Click the Configure button.
* In the "Server Settings" tab, fill in the following:
* Server Address: Enter the Cluster 2 IP Address (which you found in the prerequisite step).
* Port: 25 (leave as default).
* From Email Address: cluster1@ACME.org
* Click Next.
* In the "Email Recipients" tab, click + Add Email Recipient.
* Address: primaryalerts@ACME.org
* Ensure all severities (Critical, Warning, Info) are checked.
* Click Save.
* Click + Add Email Recipient again.
* Address: secondaryalerts@ACME.org
* Ensure all severities are checked.
* Click Save.
* Click Done. A test email will be sent.
* In the main Settings menu, select Alerts and Notifications.
* Scroll to the NCC Health Checks section.
* Check the box labeled Email Nutanix Cluster Check reports to recipients. (This will use the SMTP settings and recipients you just configured).
* Click Save.

最新問題**: 11**
タスク13
管理者が、クラスター上でネットワークスタックが破損している CentOS VM (Cent_Down) を発見しました。この問題を解決するには、VM を以前のスナップショットから復元し、ネットワーク上で再びアクセスできるようにする必要があります。
VM認証情報:
ユーザー名: root
パスワード: nutanix/4u
VMを復元し、VMから172.31.0.1にpingを実行して、ネットワーク上でVMにアクセスできることを確認してください。
続行する前に、仮想マシンの電源を切ってください。
Answer:
手順ごとの解決方法については、解説をご覧ください。
Explanation:
仮想マシンを復元し、ネットワーク上でアクセス可能であることを確認するには、以下の手順に従ってください。
VMが稼働しているクラスターのWebコンソールにログインしてください。
左側のメニューにある「仮想マシン」をクリックし、リストから「Cent_Down」を探します。電源アイコンをクリックして仮想マシンの電源を切ります。

電源アイコンの横にあるスナップショットアイコンをクリックすると、スナップショット管理ウィンドウが開きます。
ネットワークスタックが破損する前に取得されたスナップショットをリストから選択してください。日付と時刻の情報を使用して、適切なスナップショットを選択できます。
「VMの復元」をクリックし、ダイアログボックスで操作を確認してください。復元処理が完了するまでお待ちください。
VMの電源を入れるには、もう一度電源アイコンをクリックしてください。
提供されたユーザー名とパスワードを使用して、SSHまたはコンソール経由でVMにログインしてください。
仮想マシンがネットワーク上で到達可能であることを確認するには、コマンド「ping 172.31.0.1」を実行してください。宛先IPアドレスからの応答が表示されるはずです。
Prism Central GUIからVMSに移動します。
VMを選択し、[その他] -> [ゲストシャットダウン]に進みます。
スナップショットタブに移動し、利用可能な最新のスナップショットに戻してください。
VMの電源をオンにして、pingが機能するかどうかを確認します。