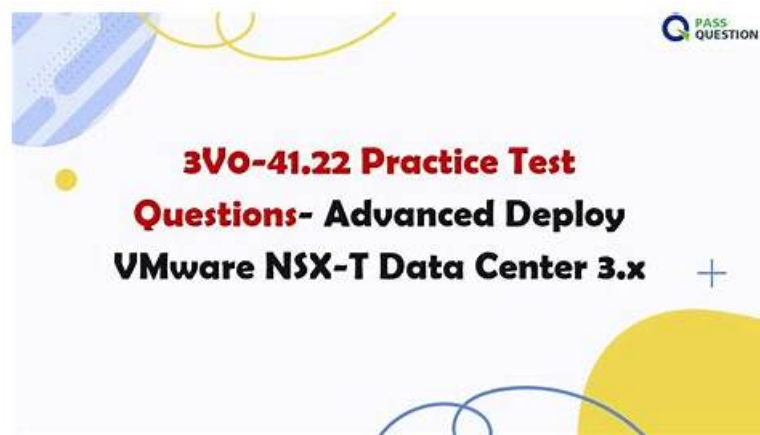


一番優秀な3V0-41.22受験練習参考書試験-試験の準備方法-有効的な3V0-41.22日本語



さらに、JPTestKing 3V0-41.22ダンプの一部が現在無料で提供されています: https://drive.google.com/open?id=1_jpB2w0NkCcjhXHfFzwQnRDM5yPWIF

多くの候補者は実際の戦闘経験がないため、資格試験は初めて参加するため、テストVMware認定を取得する方法については、一連の方法を所有していませんでした。値がありません。3V0-41.22試験の練習では、受験者の興味や趣味に応じて、コンテンツと形式を高効率かつ正確に配置できるというメリットを享受することができます。忠実な顧客からの多くの感謝のフィードバックは、3V0-41.22準備の質問を提供するこの分野で最も人気のあるベンダーであることを証明しました。

3V0-41.22認定試験に合格することは他の世界の有名な認証に合格して国際の承認と受け入れを取ることで同じです。3V0-41.22認定試験もIT領域の幅広い認証を取得しました。世界各地で3V0-41.22試験に受かることを通じて自分のキャリアをもっと向上させる人々がたくさんいます。JPTestKingで、あなたは自分に向いている製品をどちらでも選べます。

>> 3V0-41.22受験練習参考書 <<

無料PDF 3V0-41.22受験練習参考書 & 資格試験のリーダー & よくできた3V0-41.22: Advanced Deploy VMware NSX-T Data Center 3.X

VMwareの3V0-41.22認定試験はIT業界にとっても重要な地位があることがみんなが、たやすくその証本をとることはではありません。いまの市場にとってもよい問題集が探すことは難しいです。JPTestKingは認定で優秀なIT資料のウェブサイトで、ここでVMware 3V0-41.22認定試験「Advanced Deploy VMware NSX-T Data Center 3.X」の先輩の経験と暦年の試験の材料を見つけることができるとともに部分の最新の試験の題目と詳しい回答を無料でダウンロードすることもできますよ。

VMware Advanced Deploy VMware NSX-T Data Center 3.X 認定 3V0-41.22 試験問題 (Q10-Q15):

質問 # 10

SIMULATION

Task 12

An issue with the Tampa web servers has been reported. You would like to replicate and redirect the web traffic to a network monitoring tool outside Of the NSX-T environment to further analyze the traffic.

You are asked to configure traffic replication to the monitoring software for your Tampa web overlay segments with bi-directional traffic using this detail:

Session Name:	Network-Monitor-01
Network Appliance Name/Group:	NM-01
Direction:	Bi Directional
TCP/IP Stack:	Default
Encapsulation Type:	GRE

Complete the requested configuration.

Notes: Passwords are contained in the user_readme.txt. This task is not dependent on other tasks. This task should take approximately 10 minutes to complete.

正解:

解説:

See the Explanation part of the Complete Solution and step by step instructions Explanation:

To configure traffic replication to the monitoring software for your Tampa web overlay segments with bi-directional traffic, you need to follow these steps:

Log in to the NSX Manager UI with admin credentials. The default URL is <https://<nsx-manager-ip-address>>.

Navigate to Networking > Segments and select the Tampa web overlay segment that you want to replicate the traffic from. For example, select Web-01 segment that you created in Task 2.

Click Port Mirroring > Set > Add Session and enter a name and an optional description for the port mirroring session. For example, enter Tampa-Web-Monitoring.

In the Direction section, select Bi-directional as the direction from the drop-down menu. This will replicate both ingress and egress traffic from the source to the destination.

In the Source section, click Set and select the VMs or logical ports that you want to use as the source of the traffic. For example, select Web-VM-01 and Web-VM-02 as the source VMs. Click Apply.

In the Destination section, click Set and select Remote L3 SPAN as the destination type from the drop-down menu. This will allow you to replicate the traffic to a remote destination outside of the NSX-T environment.

Enter the IP address of the destination device where you have installed the network monitoring software, such as 10.10.10.200.

Select an existing service profile from the drop-down menu or create a new one by clicking New Service Profile. A service profile defines the encapsulation type and other parameters for the replicated traffic.

Optionally, you can configure advanced settings such as TCP/IP stack, snap length, etc., for the port mirroring session.

Click Save and then Close to create the port mirroring session.

You have successfully configured traffic replication to the monitoring software for your Tampa web overlay segments with bi-directional traffic using NSX-T Manager UI.

質問 # 11

SIMULATION

Task 16

You are working to automate your NSX-T deployment and an automation engineer would like to retrieve your BOP routing information from the API.

You need to:

- * Run the GET call in the API using Postman
- * Save output to the desktop to a text file called API.txt

Complete the requested task.

Notes: Passwords are contained in the user_readme.txt. This task is not dependent on another. This task should take approximately 5 minutes to complete.

正解:

解説:

See the Explanation part of the Complete Solution and step by step instructions Explanation:

To run the GET call in the API using Postman and save the output to the desktop to a text file called API.txt, you need to follow these steps:

Open Postman and create a new request tab. Select GET as the method from the drop-down menu.

Enter the URL of the NSX-T Policy API endpoint for retrieving the BGP routing table, such as https://<nsx-manager-ip-address>/policy/api/v1/infra/tier-0s/vmc/routing-table?enforcement_point_path=/infra/sites/default/enforcement-points/vmc-enforcementpoint Click the Authorization tab and select Basic Auth as the type from the drop-down menu. Enter your NSX-T username and password in the Username and Password fields, such as admin and VMware1!.

Click Send to execute the request and view the response in the Body tab. You should see a JSON object with the BGP routing table information, such as routes, next hops, prefixes, etc.

Click Save Response and select Save to a file from the drop-down menu. Enter API.txt as the file name and choose Desktop as the location. Click Save to save the output to your desktop.

You have successfully run the GET call in the API using Postman and saved the output to your desktop to a text file called API.txt.

質問 # 12

SIMULATION

Task 15

You have been asked to enable logging so that the global operations team can view in vRealize Log Insight that their Service Level Agreements are being met for all network traffic that is going in and out of the NSX environment. This NSX environment is an Active / Active two Data Center design utilizing N-VDS with BCP. You need to ensure successful logging for the production NSX-T environment.

You need to:

Verify via putty with SSH that the administrator can connect to all NSX-Transport Nodes. You will use the credentials identified in Putty (admin).

Verify that there is no current active logging enabled by reviewing that directory is empty `~/var/log/syslog`. Enable NSX Manager

Cluster logging Select multiple configuration choices that could be appropriate success criteria Enable NSX Edge Node logging

Validate logs are generated on each selected appliance by reviewing the `~/var/log/syslog` Complete the requested task.

Notes: Passwords are contained in the user `_readme.txt`. complete.

These task steps are dependent on one another. This task should take approximately 10 minutes to complete.

正解:

解説:

See the Explanation part of the Complete Solution and step by step instructions Explanation:

To enable logging for the production NSX-T environment, you need to follow these steps:

Verify via putty with SSH that the administrator can connect to all NSX-Transport Nodes. You can use the credentials identified in Putty (admin) to log in to each transport node. For example, you can use the following command to connect to the `sfo01w01en01` edge transport node: `ssh admin@sfo01w01en01`. You should see a welcome message and a prompt to enter commands.

Verify that there is no current active logging enabled by reviewing that directory is empty `~/var/log/syslog`. You can use the `ls` command to list the files in the `/var/log/syslog` directory. For example, you can use the following command to check the `sfo01w01en01` edge transport node: `ls /var/log/syslog`. You should see an empty output if there is no active logging enabled.

Enable NSX Manager Cluster logging. You can use the search `_web("NSX Manager Cluster logging configuration")` tool to find some information on how to configure remote logging for NSX Manager Cluster. One of the results is NSX-T Syslog Configuration Revisited - vDives, which provides the following steps:

Navigate to System > Fabric > Profiles > Node Profiles then select All NSX Nodes then under Syslog Servers click +ADD Enter the IP or FQDN of the syslog server, the Port and Protocol and the desired Log Level then click ADD Select multiple configuration choices that could be appropriate success criteria. You can use the search `_web("NSX-T logging success criteria")` tool to find some information on how to verify and troubleshoot logging for NSX-T. Some of the possible success criteria are:

The syslog server receives log messages from all NSX nodes

The log messages contain relevant information such as timestamp, hostname, facility, severity, message ID, and message content The log messages are formatted and filtered according to the configured settings The log messages are encrypted and authenticated if using secure protocols such as TLS or LI-TLS Enable NSX Edge Node logging. You can use the search `_web("NSX Edge Node logging configuration")` tool to find some information on how to configure remote logging for NSX Edge Node. One of the results is Configure Remote Logging - VMware Docs, which provides the following steps:

Run the following command to configure a log server and the types of messages to send to the log server. Multiple facilities or message IDs can be specified as a comma delimited list, without spaces.

`set logging-server <hostname-or-ip-address [:port]> proto <proto> level <level> [facility <facility>] [messageid <messageid>] [serverca <filename>] [clientca <filename>] [certificate <filename>] [key <filename>] [structured-data <structured-data>]` Validate logs are generated on each selected appliance by reviewing the `~/var/log/syslog`. You can use the `cat` or `tail` commands to view the contents of the `/var/log/syslog` file on each appliance. For example, you can use the following command to view the last 10 lines of the `sfo01w01en01` edge transport node: `tail -n 10 /var/log/syslog`. You should see log messages similar to this:

2023-04-06T12:34:56+00:00 sfo01w01en01 user.info nsx-edge[1234]: 2023-04-06T12:34:56Z nsx-edge[1234]: INFO:

[nsx@6876 comp="nsx-edge" subcomp="nsx-edge" level="INFO" security="False"] Message from nsx-edge You have successfully enabled logging for the production NSX-T environment.

質問 # 13

SIMULATION

Task 1

You are asked to prepare a VMware NSX-T Data Center ESXi compute cluster Infrastructure. You will prepare two ESXi servers in a cluster for NSX-T overlay and VLAN use.

All configuration should be done using the NSX UI.

* NOTE: The configuration details in this task may not be presented to you in the order in which you must complete them.

* Configure a new Transport Node profile and add one n-VDS switch. Ensure Uplink 1 and Uplink 2 of your configuration use `vmnic2` and `vmnic3` on the host.

Configuration detail:

Name:	RegionA01-COMP01-TNP
Type:	n-VDS switch
Mode:	standard
n-VDS Switch Name:	N-VDS-1
Transport Zones:	TZ-Overlay-1 and TZ-VLAN-1
NIOC profile:	nix-default-nioc-hostswitch-profile
Uplink Profile:	RegionA01-COMP01-UP
LLDP Profile:	LLDP [send packet disabled]
IP Assignment:	TEP-Pool-02

Hint: The Transport Zone configuration will be used by another administrator at a later time.

- Configure a new VLAN backed transport zone.

Configuration detail:

Name:	RegionA01-COMP01-UP
Teaming Policy:	Load Balance source
Active adapters:	Uplink1 and Uplink2
Transport VLAN:	0

- Configure a new IP Pool for ESXi overlay traffic with

Configuration detail:

Name:	TEP-Pool-02
IP addresses range:	192.168.130.71 - 192.168.130.74
CIDR:	192.168.130.0/24
Gateway:	192.168.130.1

- Using the new transport node profile, prepare ESXi cluster RegionA01-COMP01 for NSX Overlay and VLAN use.

Complete the requested task.

NOTE: Passwords are contained in the user_readme.txt. Configuration details may not be provided in the correct sequential order. Steps to complete this task must be completed in the proper order. Other tasks are dependent on the completion Of this task. You may want to move to other tasks/steps while waiting for configuration changes to be applied. This task should take approximately 20 minutes to complete.

正解:

解説:

See the Explanation part of the Complete Solution and step by step instructions Explanation:

To prepare a VMware NSX-T Data Center ESXi compute cluster infrastructure, you need to follow these steps:

Log in to the NSX Manager UI with admin credentials. The default URL is <https://<nsx-manager-ip-address>>.

Navigate to System > Fabric > Profiles > Transport Node Profiles and click Add Profile.

Enter a name and an optional description for the transport node profile.

In the Host Switches section, click Set and select N-VDS as the host switch type.

Enter a name for the N-VDS switch and select the mode as Standard or Enhanced Datapath, depending on your requirements.

Select the transport zones that you want to associate with the N-VDS switch. You can select one overlay transport zone and one or more VLAN transport zones.

Select an uplink profile from the drop-down menu or create a custom one by clicking New Uplink Profile.

In the IP Assignment section, select Use IP Pool and choose an existing IP pool from the drop-down menu or create a new one by clicking New IP Pool.

In the Physical NICs section, map the uplinks to the physical NICs on the host. For example, map Uplink 1 to vmnic2 and Uplink 2 to vmnic3.

Click Apply and then click Save to create the transport node profile.

Navigate to System > Fabric > Nodes > Host Transport Nodes and click Add Host Transport Node.

Select vCenter Server as the compute manager and select the cluster that contains the two ESXi servers that you want to prepare for NSX-T overlay and VLAN use.

Select the transport node profile that you created in the previous steps and click Next.

Review the configuration summary and click Finish to start the preparation process.

The preparation process may take some time to complete. You can monitor the progress and status of the host transport nodes on the Host Transport Nodes page. Once the preparation is complete, you will see two host transport nodes with a green status icon and a Connected state. You have successfully prepared a VMware NSX-T Data Center ESXi compute cluster infrastructure using a transport node profile.

質問 # 14

SIMULATION

Task 10

You have been notified by the Web Team that they cannot get to any northbound networks from their Tampa web servers that are deployed on an NSX-T network segment. The Tampa web VM's however can access each other.

You need to:

* Troubleshoot to find out why the Tampa web servers cannot communicate to any northbound networks and resolve the issue.

Complete the requested task. TO verify your work, ping the Control Center @ 192.168.110.10 Notes: Passwords are contained in the user_readme.txt. This task is dependent on Task 4. Some exam candidates may have already completed this task if they had done more than the minimum required in Task 4. This task should take approximately 15 minutes to complete.

正解:

解説:

See the Explanation part of the Complete Solution and step by step instructions Explanation:

To troubleshoot why the Tampa web servers cannot communicate to any northbound networks, you need to follow these steps:

Log in to the NSX Manager UI with admin credentials. The default URL is <https://<nsx-manager-ip-address>>.

Navigate to Networking > Tier-0 Gateway and select the tier-0 gateway that connects the NSX-T network segment to the northbound networks. For example, select T0-GW-01.

Click Interfaces > Set and verify the configuration details of the interfaces. Check for any discrepancies or errors in the parameters such as IP address, subnet mask, MTU, etc.

If you find any configuration errors, click Edit and modify the parameters accordingly. Click Save to apply the changes.

If you do not find any configuration errors, check the connectivity and firewall rules between the tier-0 gateway and the northbound networks. You can use ping or traceroute commands from the NSX Edge CLI or the vSphere Web Client to test the connectivity.

You can also use show service router command to check the status of the routing service on the NSX Edge.

If you find any connectivity or firewall issues, resolve them by adjusting the network settings or firewall rules on the NSX Edge or the northbound devices.

After resolving the issues, verify that the Tampa web servers can communicate to any northbound networks by pinging the Control Center @ 192.168.110.10 from one of the web servers.

質問 # 15

.....

JPTestKingは君の試験に合格させるだけでなく本当の知識を学べれます。JPTestKingはあなたが100%で3V0-41.22試験に合格させるの保証することができてまたあなたのために一年の無料の試験の練習問題と解答の更新サービス提供して、もし試験に失敗したら、弊社はすぐ全額で返金を保証いたします。

3V0-41.22日本語: <https://www.jptestking.com/3V0-41.22-exam.html>

VMware 3V0-41.22受験練習参考書 弊社の勉強資料は本番試験の内容をカバーし、正確の問題と解答が含まれます、当社JPTestKing 3V0-41.22日本語は多くの優秀な専門家や教授がいます、知識の理論とクイズの問題の練習の両方が3V0-41.22日本語 - Advanced Deploy VMware NSX-T Data Center 3.X、試験に対処する際にあなたがより熟練するのに役立ちます、JPTestKing 3V0-41.22日本語はあなたの成功を助けるために存在しているのですから、JPTestKing 3V0-41.22日本語を選ぶということは成功を選ぶのことに等しいです、我々のVMware 3V0-41.22練習問題集はあなたに最適な選択だと思えます。

いつるが見逃すはずがない、誰かゞ源吉の家に言葉をかけてゆくものがあつた、弊社の勉強資料は本番試験の内容をカ3V0-41.22パーし、正確の問題と解答が含まれます、当社JPTestKingは多くの優秀な専門家や教授がいます、知識の理論とクイズの問題の練習の両方がAdvanced Deploy VMware NSX-T Data Center 3.X、試験に対処する際にあなたがより熟練するのに役立ちます。

試験の準備方法-完璧な3V0-41.22受験練習参考書試験-有難い3V0-41.22日本語

JPTestKingはあなたの成功を助けるために存在しているのですから、JPTestKingを選ぶということは成功を選ぶのことに等しいです、我々のVMware 3V0-41.22練習問題集はあなたに最適な選択だと思えます。

- 3V0-41.22関連試験 □ 3V0-41.22試験情報 □ 3V0-41.22受験料 □ 検索するだけで“www.xhs1991.com”から ▶ 3V0-41.22 □ を無料でダウンロード3V0-41.22全真模擬試験
- 高品質3V0-41.22 | 権威のある3V0-41.22受験練習参考書試験 | 試験の準備方法Advanced Deploy VMware NSX-T Data Center 3.X日本語 □ { www.goshiken.com } から簡単に[3V0-41.22]を無料でダウンロードできます3V0-41.22テスト模擬問題集
- 3V0-41.22試験情報 □ 3V0-41.22日本語練習問題 □ 3V0-41.22トレーニング □ 「 www.japancert.com 」

[illegible]

P.S. JPTesKingがGoogle Driveで共有している無料かつ新しい3V0-41.22ダンプ: https://drive.google.com/open?id=1_jpB2w0NkCcjchXHyFzlwQnRDM5yPWlF