3V0-41.22学習体験談、3V0-41.22技術内容

BONUS！！！ Jpexam 3V0-41.22ダンプの一部を無料でダウンロード：https://drive.google.com/open?id=1W3ozbkaHQZDzDmIXeBn8CDH2ml7v9VCI

そんなに多くの人はVMware 3V0-41.22試験に合格できるのに興味がわきますか。人に引けをとりたくないあなたはVMware 3V0-41.22資格認定を取得したいですか。ここで、彼らは3V0-41.22試験にうまく合格できる秘訣は我々社の提供する質高いVMware 3V0-41.22問題集を利用したことだと教えます。弊社のVMware 3V0-41.22問題集を通して復習してから、真実的に自分の能力の向上を感じ、3V0-41.22資格認定を受け取ります。

VMware 3V0-41.22試験に合格するには、候補者は複雑な環境でNSX-T Data Center 3.Xを展開および管理できる能力をデモンストレーションする必要があります。また、一般的な問題をトラブルシューティングし、NSX-Tをパフォーマンスとスケーラビリティに最適化することもできる必要があります。試験に合格すると、VMware Certified Advanced Professional - Network Virtualization 2021（VCAP-NV 2021）認定を取得できます。この認定は、VMware NSX-T Data Center 3.Xの専門知識の証として、雇用主や業界の専門家から認められています。この認定を取得することで、プロフェッショナルは、VMware製品と技術を使用して高度なネットワーク仮想化ソリューションを展開および管理する能力を証明できます。

VMwareは、仮想化ソフトウェアおよびクラウドコンピューティングサービスを提供する上で大手企業です。彼らは、VMware製品の使用に関するスキルと専門知識を検証するために、ITの専門家にさまざまな認定を提供しています。最新の認定の1つは、VMware 3V0-41.22（Advanced Deploy VMware NSX-T Data Center 3.x）認定試験です。

>> 3V0-41.22学習体験談 <<

効果的な3V0-41.22学習体験談 & 合格スムーズ3V0-41.22技術内容 | 認定する3V0-41.22問題集無料

VMware　3V0-41.22試験に準備するには、適当の練習は必要です。受験生としてのあなたはVMware　3V0-41.22試験に関する高い質量の資料を提供します。、PDF版、ソフト版、オンライン版三つの版から、あなたの愛用する版を選択します。弊社の高品質の試験問題集を通して、あなたにVMware　3V0-41.22試験似合格させ、あなたのIT技能と職業生涯を新たなレベルに押し進めるのは我々の使命です。

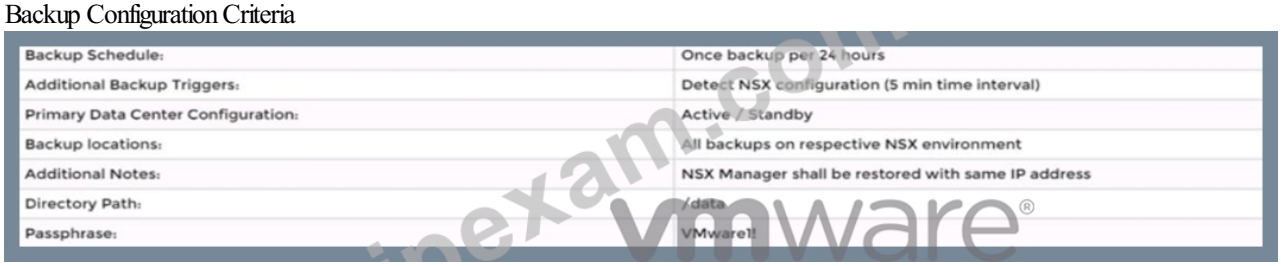
VMware Advanced Deploy VMware NSX-T Data Center 3.X 認定 3V0-41.22 試験問題 (Q13-Q18):

質問 # 13
SIMULATION
Task 13
You have been asked to configure the NSX backups for the environment so that if the NSX Manager fails it can be restored with the same IP address to the original primary Data Center that is in an Active / Standby configuration. Backups should be scheduled to run once every 24 hours as well as when there are changes published to the NSX environment. Ensure that backups are completed on their respective environment. Verify the backup file has been created on the SFTP server.

* Credentials needed to complete the task:

SFTP User:	sftpuser
Password:	VMware1!
SFTP IP:	192.168.110.91
Hostname:	ubuntu-01.corp.local

You need to:
* Verify that an SFTP server is available on the network and obtain SFTP Fingerprint.
* Configure NSX Backups via NSX Appliance Backup
* Configure Scheduling Criteria
Backup Configuration Criteria



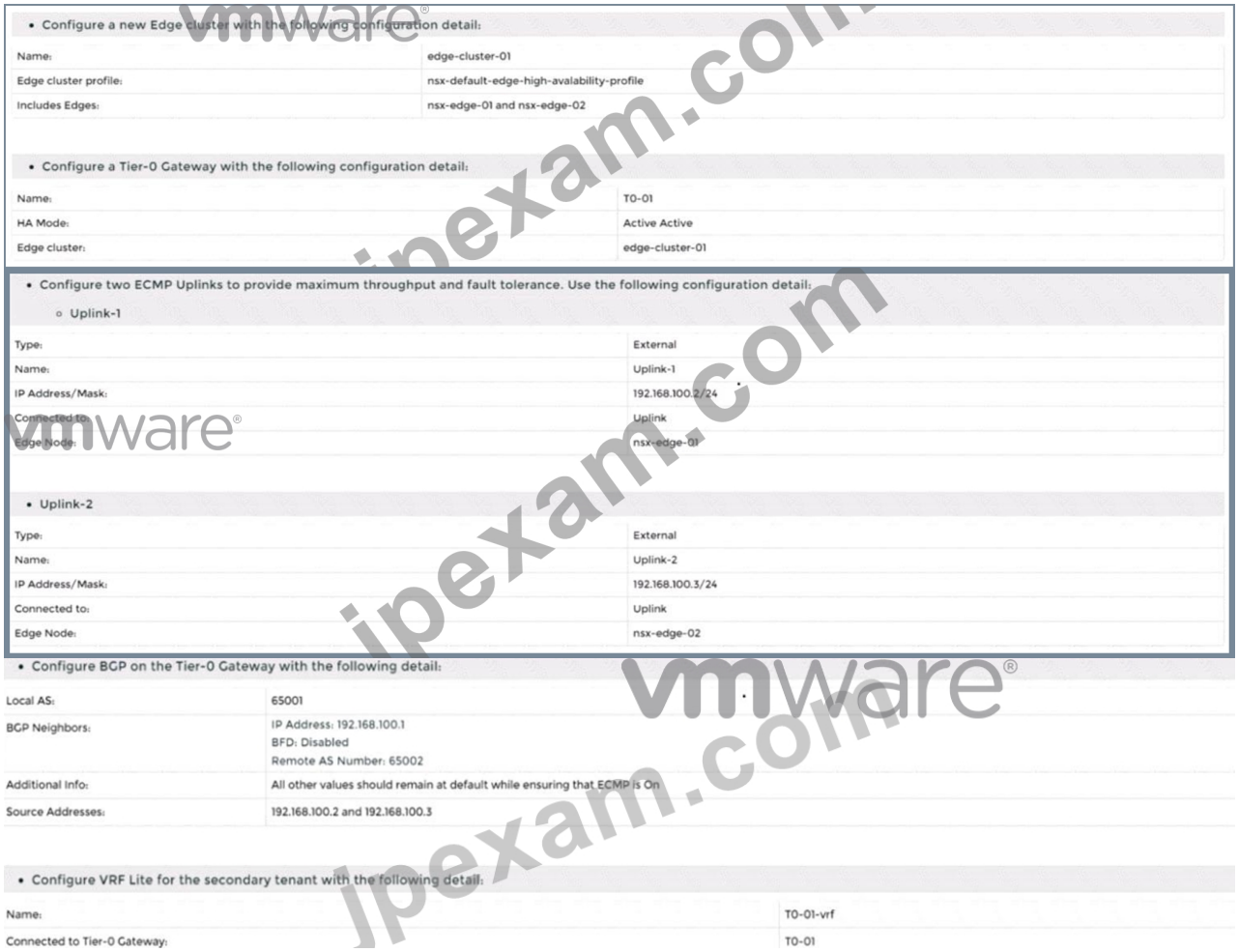
Backup Schedule:	Once backup per 24 hours
Additional Backup Triggers:	Detect NSX configuration (5 min time interval)
Primary Data Center Configuration:	Active / Standby
Backup locations:	All backups on respective NSX environment
Additional Notes:	NSX Manager shall be restored with same IP address
Directory Path:	/data
Passphrase:	VMware1!

Complete the requested task.
Notes: Passwords are contained in the user_readme.txt. This task is not dependent on other tasks. 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 configure the NSX backups for the environment, you need to follow these steps:
Verify that an SFTP server is available on the network and obtain SFTP fingerprint. You can use the search_web("SFTP server availability") tool to find some information on how to set up and check an SFTP server. You can also use the ssh-keyscan command to get the fingerprint of the SFTP server. For example, ssh-keyscan -t ecdsa sftp_server will return the ECDSA key of the sftp_server. You can compare this key with the one displayed on the NSX Manager UI when you configure the backup settings.
Configure NSX Backups via NSX Appliance Backup. Log in to the NSX Manager UI with admin credentials. The default URL is https://<nsx-manager-ip-address>. Select System > Lifecycle Management > Backup & Restore. Click Edit under the SFTP Server label to configure your SFTP server. Enter the FQDN or IP address of the backup file server, such as 10.10.10.100. The protocol text box is already filled in. SFTP is the only supported protocol. Change the default port if necessary. The default TCP port is 22. In the Directory Path text box, enter the absolute directory path where the backups will be stored, such as /dat a. The directory must already exist and cannot be the root directory (/). Avoid using path drive letters or spaces in directory names; they are not supported. In the Passphrase text box, enter a passphrase that will be used to encrypt and decrypt the backup files, such as VMware1!. Click Save to create the backup configuration.
Configure Scheduling Criteria. On the Backup & Restore page, click Edit under the Schedule label to configure your backup schedule. Select Enabled from the drop-down menu to enable scheduled backups. Select Daily from the Frequency drop-down menu to run backups once every 24 hours. Select a time from the Time drop-down menu to specify when the backup will start, such as 12:00 AM. Select Enabled from the Additional Backup Trigger drop-down menu to run backups when there are changes published to the NSX environment. Click Save to create the backup schedule.
Verify that a backup file has been created on the SFTP server. On the Backup & Restore page, click Start Backup to run a manual backup and verify that it completes successfully. You should see a message saying "Backup completed successfully". You can also check the status and details of your backups on this page, such as backup size, duration, and timestamp. Alternatively, you can log in to your SFTP server and check if there is a backup file in your specified directory path, such as /data.

質問 # 14
Task 3
You are asked to deploy a new instance of NSX-T into an environment with two isolated tenants. These tenants each have separate physical data center cores and have standardized on BCP as a routing protocol.
You need to:



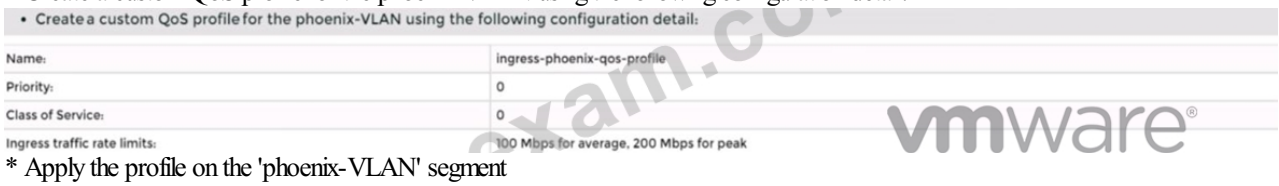
Complete the requested task.
Notes: Passwords are Contained in the user_readme.txt. Task 3 is dependent on the Completion Of Task and 2.
Other tasks are dependent On the Completion Of this task. Do not wait for configuration changes to be applied in this task as processing may take up to 10 minutes to complete. Check back on completion. 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 deploy a new instance of NSX-T into an environment with two isolated tenants, 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 > Nodes > Edge Transport Nodes and click Add Edge VM.
Enter a name and an optional description for the edge VM. Select the compute manager, cluster, and resource pool where you want to deploy the edge VM. Click Next.
Select the deployment size and form factor for the edge VM. For this task, you can select Medium as the size and VM as the form factor. Click Next.
Select the datastore and folder where you want to store the edge VM files. Click Next.
Configure the management network settings for the edge VM. Enter a hostname, a management IP address, a default gateway, a DNS server, and a domain search list. Optionally, you can enable SSH and join the edge VM to a domain. Click Next.
Configure the transport network settings for the edge VM. Select an N-VDS as the host switch type and enter a name for it. Select an uplink profile from the drop-down menu or create a new one by clicking New Uplink Profile. Map the uplinks to the physical NICs on the edge VM. For example, map Uplink 1 to fp-eth0 and Uplink 2 to fp-eth1. Optionally, you can configure IP assignment, MTU, or LLDP for the uplinks. Click Next.
Review the configuration summary and click Finish to deploy the edge VM.
Repeat steps 2 to 8 to deploy another edge VM for redundancy.
Navigate to Networking > Tier-0 Gateway and click Add Gateway > VRF.
Enter a name and an optional description for the VRF gateway. Select an existing tier-0 gateway as the parent gateway or create a new one by clicking New Tier-0 Gateway.

Click VRF Settings and enter a VRF ID for the tenant. Optionally, you can enable EVPN settings if you want to use EVPN as the control plane protocol for VXLAN overlay networks.
Click Save to create the VRF gateway.
Repeat steps 10 to 13 to create another VRF gateway for the second tenant with a different VRF ID.
Navigate to Networking > Segments and click Add Segment.
Enter a name and an optional description for the segment. Select VLAN as the connectivity option and enter a VLAN ID for the segment. For example, enter 128 for Tenant A's first uplink VLAN segment.
Select an existing transport zone from the drop-down menu or create a new one by clicking New Transport Zone.
Click Save to create the segment.
Repeat steps 15 to 18 to create three more segments for Tenant A's second uplink VLAN segment (VLAN ID 129) and Tenant B's uplink VLAN segments (VLAN ID 158 and 159).
Navigate to Networking > Tier-0 Gateway and select the VRF gateway that you created for Tenant A.
Click Interfaces > Set > Add Interface.
Enter a name and an optional description for the interface.
Enter the IP address and mask for the external interface in CIDR format, such as 10.10.10.1/24.
In Type, select External.
In Connected To (Segment), select the VLAN segment that you created for Tenant A's first uplink VLAN segment (VLAN ID 128).
Select an edge node where you want to attach the interface, such as Edge-01.
Enter the Access VLAN ID from the list as configured for the segment, such as 128.
Click Save and then Close.
Repeat steps 21 to 28 to create another interface for Tenant A's second uplink VLAN segment (VLAN ID 129) on another edge node, such as Edge-02.
Repeat steps 20 to 29 to create two interfaces for Tenant B's uplink VLAN segments (VLAN ID 158 and 159) on each edge node using their respective VRF gateway and IP addresses.
Configure BGP on each VRF gateway using NSX UI or CLI commands12.You need to specify the local AS number, remote AS number, BGP neighbors, route redistribution, route filters, timers, authentication, graceful restart, etc., according to your requirements34.
Configure BGP on each physical router using their respective CLI commands56.You need to specify similar parameters as in step 31 and ensure that they match with their corresponding VRF gateway settings78.
Verify that BGP sessions are established between each VRF gateway and its physical router neighbors using NSX UI or CLI commands . You can also check the routing tables and BGP statistics on each device .
You have successfully deployed a new instance of NSX-T into an environment with two isolated tenants using VRF Lite and BGP.

質問 # 15
SIMULATION
Task 7
you are asked to create a custom QoS profile to prioritize the traffic on the phoenix-VLAN segment and limit the rate of ingress traffic.
You need to:
* Create a custom QoS profile for the phoenix-VLAN using the following configuration detail:



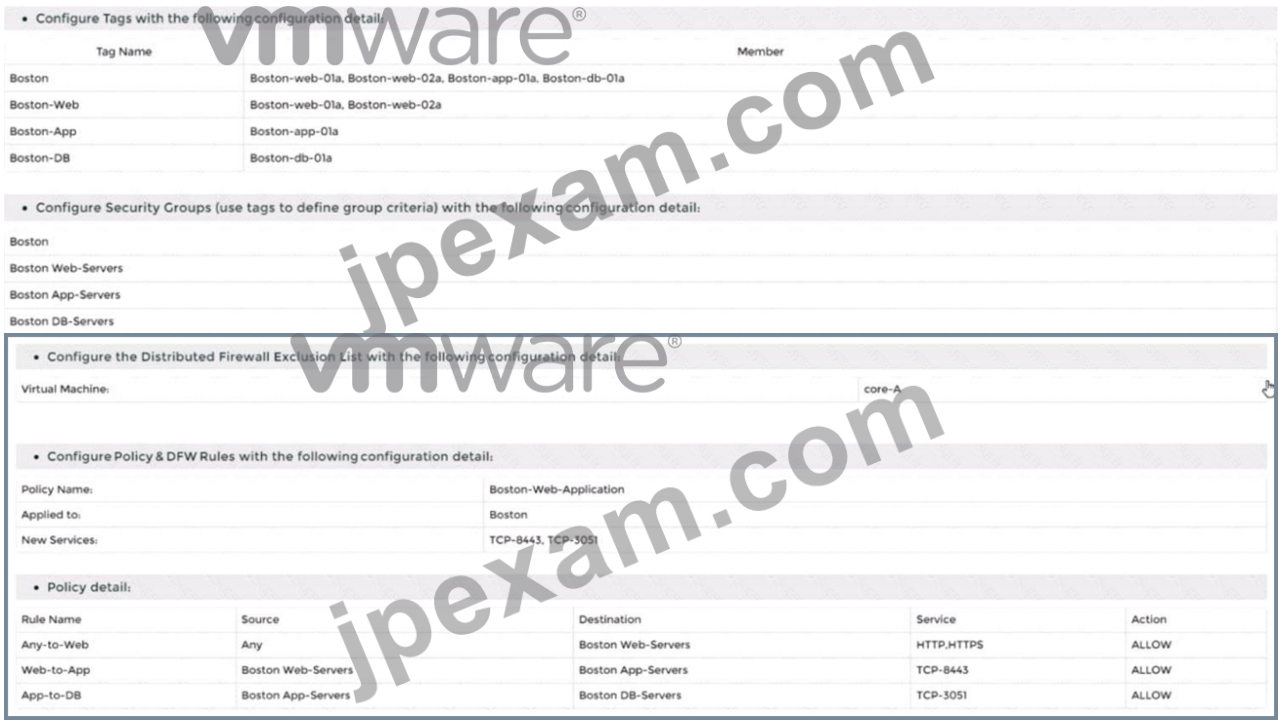
* Apply the profile on the 'phoenix-VLAN' segment
Complete the requested task.
Notes: Passwords are contained in the user_readme.txt.
take approximately 5 minutes to complete.
Subsequent tasks may require the completion of this task. This task should

正解：

解説：
See the Explanation part of the Complete Solution and step by step instructions Explanation:
To create a custom QoS profile to prioritize the traffic on the phoenix-VLAN segment and limit the rate of ingress 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 > Switching Profiles and click Add Switching Profile. Select QoS as the profile type.

Enter a name and an optional description for the QoS profile, such as phoenix-QoS.
In the Mode section, select Untrusted as the mode from the drop-down menu. This will allow you to set a custom DSCP value for the outbound IP header of the traffic on the segment.
In the Priority section, enter 46 as the DSCP value. This will mark the traffic with Expedited Forwarding (EF) per-hop behavior, which is typically used for high-priority applications such as voice or video.
In the Class of Service section, enter 5 as the CoS value. This will map the DSCP value to a CoS value that can be used by VLAN-based logical ports or physical switches to prioritize the traffic.
In the Ingress section, enter 1000000 as the Average Bandwidth in Kbps. This will limit the rate of inbound traffic from the VMs to the logical network to 1 Mbps.
Optionally, you can also configure Peak Bandwidth and Burst Size settings for the ingress traffic, which will allow some burst traffic above the average bandwidth limit for a short duration.
Click Save to create the QoS profile.
Navigate to Networking > Segments and select the phoenix-VLAN segment that you want to apply the QoS profile to.
Click Actions > Apply Profile and select phoenix-QoS as the switching profile that you want to apply to the segment.
Click Apply to apply the profile to the segment.
You have successfully created a custom QoS profile and applied it to the phoenix-VLAN segment.

質問 # 16
Task 5
You are asked to configure a micro-segmentation policy for a new 3-tier web application that will be deployed to the production environment.
You need to:



Notes:
Passwords are contained in the user_readme.txt. Do not wait for configuration changes to be applied in this task as processing may take some time.
The task steps are not dependent on one another. Subsequent tasks may require completion of this task. This task should take approximately 25 minutes to complete.

正解：

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

質問 # 17
Task 13
You have been asked to configure the NSX backups for the environment so that if the NSX Manager fails it can be restored with

the same IP address to the original primary Data Center that is in an Active / Standby configuration. Backups should be scheduled to run once every 24 hours as well as when there are changes published to the NSX environment. Ensure that backups are completed on their respective environment. Verify the backup file has been created on the SFTP server.
* Credentials needed to complete the task:

SFTP User:	sftpuser
Password:	VMware1!
SFTP IP:	192.168.110.91
Hostname:	ubuntu-01.corp.local

You need to:
* Verify that an SFTP server is available on the network and obtain SFTP Fingerprint.
* Configure NSX Backups via NSX Appliance Backup
* Configure Scheduling Criteria
Backup Configuration Criteria

Backup Schedule:	Once backup per 24 hours
Additional Backup Triggers:	Detect NSX configuration (5 min time interval)
Primary Data Center Configuration:	Active / Standby
Backup locations:	All backups on respective NSX environment
Additional Notes:	NSX Manager shall be restored with same IP address
Directory Path:	/data
Passphrase:	VMware1!

Complete the requested task.
Notes: Passwords are contained in the user_readme.txt. This task is not dependent on other tasks. 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 configure the NSX backups for the environment, you need to follow these steps:
Verify that an SFTP server is available on the network and obtain SFTP fingerprint. You can use thesearch_web("SFTP server availability")tool to find some information on how to set up and check an SFTP server. You can also use thessh-keyscancommand to get the fingerprint of the SFTP server. For example,ssh-keyscan -t ecdsa sftp_serverwill return the ECDSA key of the sftp_server. You can compare this key with the one displayed on the NSX Manager UI when you configure the backup settings.
Configure NSX Backups via NSX Appliance Backup. Log in to the NSX Manager UI with admin credentials. The default URL is https://<nsx-manager-ip-address>. Select System > Lifecycle Management > Backup & Restore. Click Edit under the SFTP Server label to configure your SFTP server. Enter the FQDN or IP address of the backup file server, such as 10.10.10.100. The protocol text box is already filled in. SFTP is the only supported protocol. Change the default port if necessary. The default TCP port is 22. In the Directory Path text box, enter the absolute directory path where the backups will be stored, such as /data. The directory must already exist and cannot be the root directory (/). Avoid using path drive letters or spaces in directory names; they are not supported. In the Passphrase text box, enter a passphrase that will be used to encrypt and decrypt the backup files, such as VMware1!.
Click Save to create the backup configuration.
Configure Scheduling Criteria. On the Backup & Restore page, click Edit under the Schedule label to configure your backup schedule. Select Enabled from the drop-down menu to enable scheduled backups.
Select Daily from the Frequency drop-down menu to run backups once every 24 hours. Select a time from the Time drop-down menu to specify when the backup will start, such as 12:00 AM. Select Enabled from the Additional Backup Trigger drop-down menu to run backups when there are changes published to the NSX environment. Click Save to create the backup schedule.
Verify that a backup file has been created on the SFTP server. On the Backup & Restore page, click Start Backup to run a manual backup and verify that it completes successfully. You should see a message saying "Backup completed successfully". You can also check the status and details of your backups on this page, such as backup size, duration, and timestamp.Alternatively, you can log in to your SFTP server and check if there is a backup file in your specified directory path, such as /data.

質問 # 18
.....

3V0-41.22技術内容: https://www.jpexam.com/3V0-41.22_exam.html

- 3V0-41.22的中関連問題 □ 3V0-41.22認証試験 □ 3V0-41.22関連合格問題 □ 最新▸ 3V0-41.22 ◂問題集ファイルは「 www.mogiexam.com 」にて検索3V0-41.22勉強資料
- 3V0-41.22合格記 □ 3V0-41.22日本語試験情報 □ 3V0-41.22日本語版参考書 □ 今すぐ➤ www.goshiken.com □を開き、➠ 3V0-41.22 □を検索して無料でダウンロードしてください3V0-41.22対応問題集
- 3V0-41.22模擬対策 □ 3V0-41.22的中関連問題 □ 3V0-41.22模擬試験問題集 □ 最新《 3V0-41.22 》問題集ファイルは【 www.mogiexam.com 】にて検索3V0-41.22日本語試験情報
- 3V0-41.22試験の準備方法｜真実的な3V0-41.22学習体験談試験｜最高のAdvanced Deploy VMware NSX-T Data Center 3.X技術内容 □ ➤ www.goshiken.com □で「 3V0-41.22 」を検索し、無料でダウンロードしてください3V0-41.22模擬試験問題集
- 3V0-41.22関連合格問題 □ 3V0-41.22関連日本語内容 □ 3V0-41.22試験解説 □ ▹ www.passtest.jp ◃で▹ 3V0-41.22 ◃を検索して、無料で簡単にダウンロードできます3V0-41.22日本語問題集
- 素晴らしい3V0-41.22学習体験談一回合格-信頼できる3V0-41.22技術内容 □ □ 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模擬対策
- 100％合格率の3V0-41.22学習体験談 - 合格スムーズ3V0-41.22技術内容 | 有効的な3V0-41.22問題集無料 □ 時間限定無料で使える▹ 3V0-41.22 ◃の試験問題は➤ www.jpexam.com □サイトで検索3V0-41.22日本語受験教科書
- 3V0-41.22日本語版参考書 ☯ 3V0-41.22日本語版と英語版 □ 3V0-41.22試験対応 □ ▹ 3V0-41.22 ◃を無料でダウンロード□ www.goshiken.com □で検索するだけ3V0-41.22日本語試験情報
- 認定するVMware 3V0-41.22｜素敵な3V0-41.22学習体験談試験｜試験の準備方法Advanced Deploy VMware NSX-T Data Center 3.X技術内容 □ 今すぐ「 www.passtest.jp 」を開き、□ 3V0-41.22 □を検索して無料でダウンロードしてください3V0-41.22模擬対策
- 効率的な3V0-41.22学習体験談一回合格-素晴らしい3V0-41.22技術内容 □ 時間限定無料で使える{ 3V0-41.22 }の試験問題は✔ www.goshiken.com □✔□サイトで検索3V0-41.22復習対策書
- 3V0-41.22受験対策解説集 □ 3V0-41.22認証試験 □ 3V0-41.22日本語試験情報 □ ➥ www.mogiexam.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復習対策書
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, building.lv, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

さらに、Jpexam 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=1W3ozbkaHQZDzDmlXeBn8CDH2ml7v9VCI