実用的なNCM-MCI日本語版参考資料 &合格スムーズNCM-MCI認定テキスト |素敵なNCM-MCI最新日本語版参考書

ちなみに、Japancert NCM-MCIの一部をクラウドストレージからダウンロードできます：https://drive.google.com/open?id=1kPVeZ3pJ5xIjqdhb-iZynNX4dZZ0tY0V

弊社のNCM-MCI問題集は大勢の専門家たちの努力で開発される成果です。初心者といい、数年IT仕事を従事した人といい、我々JapancertのNutanix NCM-MCI問題集は最良の選択であると考えられます。なぜならば、弊社は高品質かつ改革によってすぐに更新できるNCM-MCI問題集を提供できるからです。

望ましい仕事を見つけるのに十分な競争力がないと感じたら、 あなたはNCM-MCI認定試験資格証明書を取得するべきです。 私たちのNCM-MCI試験教材は、あなたが就職市場で最も一般的なスキルを身につけるのに役立ちます。 そうすれば、望ましい仕事を見つけることができます。 また、私たちのNCM-MCI試験教材に関する基礎知識があるかどうかは構わないです。実際NCM-MCI試験に対して試験ガイドがあります。

>> NCM-MCI日本語版参考資料 <<

素敵なNCM-MCI日本語版参考資料 & 合格スムーズNCM-MCI認定テキスト | 実用的なNCM-MCI最新日本語版参考書 Nutanix Certified Master - Multicloud Infrastructure v6.10

高い雇用圧力により、ますます多くの人々が雇用の緊張を和らげ、より良い仕事を得たいと考えています。 彼らが問題を解決する最善の方法は、JapancertのNCM-MCI認定を取得することです。 認定資格は彼らの労働能力の主要なシンボルであるため、NCM-MCI認定資格を所有できれば、仕事を探しているときに競争上の優位性を獲得できます。 短時間でNCM-MCI試験問題を取得することが非常に重要であることを認識する人が増えています。 また、NCM-MCI試験問題は、夢のような認定を取得するのに役立ちます。

Nutanix NCM-MCI 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• VM パフォーマンスの分析と最適化: このトピックでは、リソース使用率のための VM 構成の操作について説明します。また、VM、ノード、クラスターのメトリックの解釈についても説明します。
トピック 2	• 高度な構成とトラブルシューティング: このトピックでは、API 呼び出しの実行、サードパーティ統合の構成、AOS セキュリティ体制の分析、およびビジネス ニーズの技術的ソリューションへの変換に関するサブトピックを取り上げます。最後に、Nutanix サービスのトラブルシューティングについても説明します。

トピック 3	• ストレージ パフォーマンスの分析と最適化: ストレージ設定、ワークロード要件、ストレージ内部について説明します。
トピック 4	• ビジネス継続性: ビジネス継続性のトピックでは、コンプライアンスのための BCDR 計画の分析と、特定のワークロードの BCDR 計画の評価に関する知識を測定します。
トピック 5	• ネットワーク パフォーマンスの分析と最適化: このトピックの焦点は、オーバーレイ ネットワーク、物理ネットワーク、仮想ネットワーク、ネットワーク構成、およびフロー ポリシーです。さらに、構成に関する質問も表示されます。

Nutanix Certified Master - Multicloud Infrastructure v6.10 認定 NCM-MCI 試験問題 (Q15-Q20):

質問 # 15
Task 15
An administrator found a CentOS VM, Cent_Down, on the cluster with a corrupted network stack. To correct the issue, the VM will need to be restored from a previous snapshot to become reachable on the network again.
VM credentials:
Username: root
Password: nutanix/4u
Restore the VM and ensure it is reachable on the network by pinging 172.31.0.1 from the VM.
Power off the VM before proceeding.

正解：

解説：
See the Explanation for step by step solution
Explanation:
To restore the VM and ensure it is reachable on the network, you can follow these steps:
Log in to the Web Console of the cluster where the VM is running.
Click on Virtual Machines on the left menu and find Cent_Down from the list. Click on the power icon to power off the VM.
Click on the snapshot icon next to the power icon to open the Snapshot Management window.
Select a snapshot from the list that was taken before the network stack was corrupted. You can use the date and time information to choose a suitable snapshot.
Click on Restore VM and confirm the action in the dialog box. Wait for the restore process to complete.
Click on the power icon again to power on the VM.
Log in to the VM using SSH or console with the username and password provided.
Run the command ping 172.31.0.1 to verify that the VM is reachable on the network. You should see a reply from the destination IP address.
Go to VMS from the prism central gui
Select the VMand go to More -> Guest Shutdown
Go to Snapshots tab and revert to latest snapshot available
power on vm and verify if ping is working

質問 # 16
Task 9
Part1
An administrator logs into Prism Element and sees an alert stating the following:
Cluster services down on Controller VM (35.197.75.196)
Correct this issue in the least disruptive manner.
Part2
In a separate request, the security team has noticed a newly created cluster is reporting.
CVM [35.197.75.196] is using the default password.
They have provided some new security requirements for cluster level security.
Security requirements:
Update the default password for the root user on the node to match the admin user password: Note: 192.168.x.x is not available.
To access a node use the Host IP (172.30.0.x) from a CVM or the supplied external IP address.

Update the default password for the nutanix user on the CVM to match the admin user password.
Resolve the alert that is being reported.
Output the cluster-wide configuration of the SCMA policy to Desktop\Files\output.txt before changes are made.
Enable the Advance intrusion Detection Environment (AIDE) to run on a weekly basis for the cluster.
Enable high-strength password policies for the cluster.
Ensure CVMs require SSH keys for login instead of passwords. (SSH keys are located in the Desktop\Files\SSH folder).
Ensure the clusters meets these requirements. Do not reboot any cluster components.

正解：

解説：
See the Explanation for step by step solution
Explanation:
To correct the issue of cluster services down on Controller VM (35.197.75.196) in the least disruptive manner, you need to do the following steps:
Log in to Prism Element using the admin user credentials.
Go to the Alerts page and click on the alert to see more details.
You will see which cluster services are down on the Controller VM. For example, it could be cassandra, curator, stargate, etc.
To start the cluster services, you need to SSH to the Controller VM using the nutanix user credentials. You can use any SSH client such as PuTTY or Windows PowerShell to connect to the Controller VM. You will need the IP address and the password of the nutanix user, which you can find in Desktop\Files\SSH\nutanix.txt.
Once you are logged in to the Controller VM, run the command:
cluster status | grep -v UP
This will show you which services are down on the Controller VM.
To start the cluster services, run the command:
cluster start
This will start all the cluster services on the Controller VM.
To verify that the cluster services are running, run the command:
cluster status | grep -v UP
This should show no output, indicating that all services are up.
To clear the alert, go back to Prism Element and click on Resolve in the Alerts page.
To meet the security requirements for cluster level security, you need to do the following steps:
To update the default password for the root user on the node to match the admin user password, you need to SSH to the node using the root user credentials. You can use any SSH client such as PuTTY or Windows PowerShell to connect to the node. You will need the IP address and the password of the root user, which you can find in Desktop\Files\SSH\root.txt.
Once you are logged in to the node, run the command:
passwd
This will prompt you to enter a new password for the root user. Enter the same password as the admin user, which you can find in Desktop\Files\SSH\admin.txt.
To update the default password for the nutanix user on the CVM to match the admin user password, you need to SSH to the CVM using the nutanix user credentials. You can use any SSH client such as PuTTY or Windows PowerShell to connect to the CVM. You will need the IP address and the password of the nutanix user, which you can find in Desktop\Files\SSH\nutanix.txt.
Once you are logged in to the CVM, run the command:
passwd
This will prompt you to enter a new password for the nutanix user. Enter the same password as the admin user, which you can find in Desktop\Files\SSH\admin.txt.
To resolve the alert that is being reported, go back to Prism Element and click on Resolve in the Alerts page.
To output the cluster-wide configuration of SCMA policy to Desktop\Files\output.txt before changes are made, you need to log in to Prism Element using the admin user credentials.
Go to Security > SCMA Policy and click on View Policy Details. This will show you the current settings of SCMA policy for each entity type.
Copy and paste these settings into a new text file named Desktop\Files\output.txt.
To enable AIDE (Advanced Intrusion Detection Environment) to run on a weekly basis for the cluster, you need to log in to Prism Element using the admin user credentials.
Go to Security > AIDE Configuration and click on Enable AIDE. This will enable AIDE to monitor file system changes on all CVMs and nodes in the cluster.
Select Weekly as the frequency of AIDE scans and click Save.
To enable high-strength password policies for the cluster, you need to log in to Prism Element using the admin user credentials.
Go to Security > Password Policy and click on Edit Policy. This will allow you to modify the password policy settings for each entity type.
For each entity type (Admin User, Console User, CVM User, and Host User), select High Strength as the password policy level

and click Save.
To ensure CVMs require SSH keys for login instead of passwords, you need to log in to Prism Element using the admin user credentials.
Go to Security > Cluster Lockdown and click on Configure Lockdown. This will allow you to manage SSH access settings for the cluster.
Uncheck Enable Remote Login with Password. This will disable password-based SSH access to the cluster.
Click New Public Key and enter a name for the key and paste the public key value from Desktop\Files\SSH\id_rsa.pub. This will add a public key for key-based SSH access to the cluster.
Click Save and Apply Lockdown. This will apply the changes and ensure CVMs require SSH keys for login instead of passwords.
Part1
Enter CVM ssh and execute:
cluster status | grep -v UP
cluster start
If there are issues starting some services, check the following:
Check if the node is in maintenance mode by running the ncli host ls command on the CVM. Verify if the parameter Under Maintenance Mode is set to False for the node where the services are down. If the parameter Under Maintenance Mode is set to True, remove the node from maintenance mode by running the following command:
* nutanix@cvm$ ncli host edit id=<host id> enable-maintenance-mode=false You can determine the host ID by using ncli host ls.
See the troubleshooting topics related to failed cluster services in the Advanced Administration Guide available from the Nutanix Portal's Software Documentation page. (Use the filters to search for the guide for your AOS version). These topics have information about common and AOS-specific logs, such as Stargate, Cassandra, and other modules.
* Check for any latest FATALs for the service that is down. The following command prints all the FATALs for a CVM. Run this command on all CVMs.
nutanix@cvm$ for i in `svmips`; do echo "CVM: $i"; ssh $i "ls -ltr /home/nutanix/data/logs/*.FATAL"; done NCC Health Check: cluster_services_down_check (nutanix.com) Part2 Update the default password for the root user on the node to match the admin user password echo -e "CHANGING ALL AHV HOST ROOT PASSWORDS.\nPlease input new password: "; read -rs password1; echo "Confirm new password: "; read -rs password2; if ["$password1" == "$password2"]; then for host in $(hostips); do echo Host $host; echo $password1 | ssh root@$host "passwd --stdin root"; done; else echo "The passwords do not match"; fi Update the default password for the nutanix user on the CVM sudo passwd nutanix Output the cluster-wide configuration of the SCMA policy ncli cluster get-hypervisor-security-config Output Example:
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 Enable the Advance intrusion Detection Environment (AIDE) to run on a weekly basis for the cluster.
ncli cluster edit-hypervisor-security-params enable-aide=true
ncli cluster edit-hypervisor-security-params schedule=weekly
Enable high-strength password policies for the cluster.
ncli cluster edit-hypervisor-security-params enable-high-strength-password=true Ensure CVMs require SSH keys for login instead of passwords
https://portal.nutanix.com/page/documents/kbs/details?targetId=kA0600000008gb3CAA

質問 # 17
Task 10
An administrator is working to create a VM using Nutanix V3 API calls with the following specifications.
* VM specifications:
* vCPUs: 2
* Memory: BGb
* Disk Size: 50Gb
* Cluster: Cluster A
* Network: default- net
The API call is falling, indicating an issue with the payload:
The body is saved in Desktop/ Files/API_Create_VM,text
Correct any issues in the text file that would prevent from creating the VM. Also ensure the VM will be created as speeded and make sure it is saved for re-use using that filename.
Deploy the vm through the API
Note: Do not power on the VM.

正解：

解説：

See the Explanation for step by step solution
Explanation:
https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e000000LLEzCAO
https://jsonformatter.curiousconcept.com/#
acli net.list (uuid network defult_net)
ncli cluster info (uuid cluster)
Put Call: https://Prism Central IP address : 9440/api/nutanix/v3vms
Edit these lines to fix the API call, do not add new lines or copy lines.
You can test using the Prism Element API explorer or PostMan
Body:

```
{
{
"spec": {
"name": "Test_Deploy",
"resources": {
"power_state":"OFF",
"num_vcpus_per_socket": ,
"num_sockets": 1,
"memory_size_mib": 8192,
"disk_list": [
{
"disk_size_mib": 51200,
"device_properties": {
"device_type":"DISK"
}
},
{
"device_properties": {
"device_type":"CDROM"
}
}
],
"nic_list":[
{
"nic_type": "NORMAL_NIC",
"is_connected": true,
"ip_endpoint_list": [
{
"ip_type": "DHCP"
}
],
"subnet_reference": {
"kind": "subnet",
"name": "default_net",
"uuid": "00000000-0000-0000-0000-000000000000"
}
}
],
},
"cluster_reference": {
"kind": "cluster",
"name": "NTNXDemo",
"uuid": "00000000-0000-0000-0000-000000000000"
}
},
"api_version": "3.1.0",
"metadata": {
"kind": "vm"
}
}
```

https://www.nutanix.dev/2019/08/26/post-a-package-building-your-first-nutanix-rest-api-post-request/ Reference

質問 # 18
Task 8
Depending on the order you perform the exam items, the access information and credentials could change. Please refer to the other item performed on Cluster B if you have problems accessing the cluster.
The infosec team has requested that audit logs for API Requests and replication capabilities be enabled for all clusters for the top 4 severity levels and pushed to their syslog system using highest reliability possible. They have requested no other logs to be included.
Syslog configuration:
Syslog Name: Corp_syslog
Syslop IP: 34.69.43.123
Port: 514
Ensure the cluster is configured to meet these requirements.

正解：

解説：
See the Explanation for step by step solution
Explanation:
To configure the cluster to meet the requirements of the infosec team, you need to do the following steps:
Log in to Prism Central and go to Network > Syslog Servers > Configure Syslog Server. Enter Corp_syslog as the Server Name, 34.69.43.123 as the IP Address, and 514 as the Port. Select TCP as the Transport Protocol and enable RELP (Reliable Logging Protocol). This will create a syslog server with the highest reliability possible.
Click Edit against Data Sources and select Cluster B as the cluster. Select API Requests and Replication as the data sources and set the log level to CRITICAL for both of them. This will enable audit logs for API requests and replication capabilities for the top 4 severity levels (EMERGENCY, ALERT, CRITICAL, and ERROR) and push them to the syslog server. Click Save.
Repeat step 2 for any other clusters that you want to configure with the same requirements.

To configure the Nutanix clusters to enable audit logs for API Requests and replication capabilities, and push them to the syslog system with the highest reliability possible, you can follow these steps:
Log in to the Nutanix Prism web console using your administrator credentials.
Navigate to the "Settings" section or the configuration settings interface within Prism.
Locate the "Syslog Configuration" or "Logging" option and click on it.
Configure the syslog settings as follows:
Syslog Name: Enter "Corp_syslog" as the name for the syslog configuration.
Syslog IP: Set the IP address to "34.69.43.123", which is the IP address of the syslog system.
Port: Set the port to "514", which is the default port for syslog.
Enable the option for highest reliability or persistent logging, if available. This ensures that logs are sent reliably and not lost in case of network interruptions.
Save the syslog configuration.
Enable Audit Logs for API Requests:
In the Nutanix Prism web console, navigate to the "Cluster" section or the cluster management interface.
Select the desired cluster where you want to enable audit logs.
Locate the "Audit Configuration" or "Security Configuration" option and click on it.
Look for the settings related to audit logs and API requests. Enable the audit logging feature and select the top 4 severity levels to be logged.
Save the audit configuration.
Enable Audit Logs for Replication Capabilities:
In the Nutanix Prism web console, navigate to the "Cluster" section or the cluster management interface.
Select the desired cluster where you want to enable audit logs.
Locate the "Audit Configuration" or "Security Configuration" option and click on it.
Look for the settings related to audit logs and replication capabilities. Enable the audit logging feature and select the top 4 severity levels to be logged.
Save the audit configuration.
After completing these steps, the Nutanix clusters will be configured to enable audit logs for API Requests and replication capabilities. The logs will be sent to the specified syslog system with the highest reliability possible.
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

質問 # 19
TASK2
The security team has provided some new security requirements for cluster level security on Cluster 2.
Security requirements:
Update the password for the root user on the Cluster 2 node to match the admin user password.
Note: The 192.168.x.x network is not available. To access a node use the host IP (172.30.0.x) from the CVM.
Output the cluster-wide configuration of the SCMA policy to desktop\output.txt before changes are made.
Enable the Advanced Intrusion Detection Environment (AIDE) to run on a weekly basis for the hypervisor and cvms for Cluster 2.
Enable high-strength password policies for the hypervisor and cluster.
Ensure CVMs require SSH keys for login instead of passwords. (SSH keys are located in the desktop\Files\SSH folder.) Ensure the cluster meets these requirements. Do not reboot any cluster components.
Note: Please ensure you are modifying the correct components.

正解：

解説：
See the Explanation
Explanation:
This task focuses on Security Technical Implementation Guides (STIGs) and general hardening of the Nutanix cluster. Most of these tasks are best performed via the Nutanix Command Line Interface (ncli) on the CVM, though the SSH key requirement is often easier to handle via the Prism GUI.
Here is the step-by-step procedure to complete Task 2.
Prerequisites: Connection
Open PuTTY (or the available terminal) from the provided Windows Desktop.
SSH into the Cluster 2 CVM. (If the Virtual IP is unknown, check Prism Element for the CVM IP).
Log in using the provided credentials (usually nutanix / nutanix/4u or the admin password provided in your instructions).
Step 1: Output SCMA Policy (Do this FIRST)
Requirement: Output the cluster-wide configuration of the SCMA policy to desktop\output.txt before changes are made.
In the SSH session on the CVM, run:
Bash
ncli cluster get-software-config-management-policy
Copy the output from the terminal window.
Open Notepad on the Windows Desktop.
Paste the output.
Save the file as output.txt on the Desktop.
Step 2: Enable AIDE (Weekly)
Requirement: Enable the Advanced Intrusion Detection Environment (AIDE) to run on a weekly basis for the hypervisor and CVMs.
In the same CVM SSH session, run the following command to modify the SCMA policy:
Bash
ncli cluster edit-software-config-management-policy enable-aide=true schedule-interval=WEEKLY (Note: This single command applies the policy to both Hypervisor and CVMs by default in most versions).
Step 3: Enable High-Strength Password Policies
Requirement: Enable high-strength password policies for the hypervisor and cluster.
Run the following command:
Bash
ncli cluster set-high-strength-password-policy enable=true
Step 4: Update Root Password for Cluster Nodes
Requirement: Update the password for the root user on the Cluster 2 node to match the admin user password.
Method A: The Automated Way (Recommended)
Use ncli to set the password for all hypervisor nodes at once without needing to SSH into them individually.
Run:
Bash
ncli cluster set-hypervisor-password
When prompted, enter the current admin password (this becomes the new root password).
Method B: The Manual Way (If NCLI fails or manual access is required)
Note: Use this if the exam specifically wants you to touch the node via the 172.x network.

From the CVM, SSH to the host using the internal IP:
Bash
ssh root@172.30.0.x (Replace x with the host ID, e.g., 4 or 5)
Run the password change command:
Bash
passwd
Enter the admin password twice.
Repeat for other nodes in Cluster 2.
Step 5: Cluster Lockdown (SSH Keys)
Requirement: Ensure CVMs require SSH keys for login instead of passwords.
It is safest to do this via the Prism Element GUI to prevent locking yourself out.
Open Prism Element for Cluster 2 in the browser.
Click the Gear Icon (Settings) -> Cluster Lockdown.
Uncheck the box "Enable Remote Login with Password".
Click New Public Key (or Add Key).
Open the folder Desktop\Files\SSH on the Windows desktop.
Open the public key file (usually ends in .pub) in Notepad and copy the contents.
Paste the key into the Prism "Key" box.
Click Save.
Note: Do not reboot the cluster. The SCMA and Password policies take effect immediately without a reboot.

質問 # 20
.....

Nutanix才能の新しい時代に次第に飽和して彼ら自身の利点を獲得し、あなたの能力をどのように反映しますか？ おそらく最も直感的な方法は、テストNCM-MCI認定を取得して、Japancert対応する資格を取得することです。 ただし、NCM-MCI認定試験はそれほど単純ではないため、レビューには多大な労力が必要です。 テスト認定を効果的に取得する方法について説明します。NCM-MCI試験に短時間で合格することは空想ではないことを伝えるNCM-MCI学習教材です。 何万人もの受験者が99％の合格率でNutanix Certified Master - Multicloud Infrastructure v6.10試験に合格するのを支援しました。

NCM-MCI認定テキスト: https://www.japancert.com/NCM-MCI.html

- NCM-MCI技術内容 👆 NCM-MCI合格体験記 □ NCM-MCI日本語復習赤本 □ ➠ www.jptestking.com □を開き、▹ NCM-MCI ◃を入力して、無料でダウンロードしてくださいNCM-MCIテスト問題集
- NCM-MCI対応内容 □ NCM-MCI最新受験攻略 □ NCM-MCI対策学習 ➡□ ☀ www.goshiken.com □☀□は、✔ NCM-MCI □✔□を無料でダウンロードするのに最適なサイトですNCM-MCI的中問題集
- NCM-MCI専門知識 □ NCM-MCI対策学習 〜 NCM-MCI模擬対策 □▹ www.jpshiken.com ◃を開き、【 NCM-MCI 】を入力して、無料でダウンロードしてくださいNCM-MCI合格記
- 分厚い教科書を読む時間のない方におすすめ NCM-MCI試験問題 □ 今すぐ【 www.goshiken.com 】で□ NCM-MCI □を検索し、無料でダウンロードしてくださいNCM-MCI技術内容
- NCM-MCI試験過去問 □ NCM-MCI資格模擬 □ NCM-MCIオンライン試験 □ □ NCM-MCI □を無料でダウンロード▸ www.jpexam.com ◂で検索するだけNCM-MCI試験過去問
- NCM-MCI的中問題集 □ NCM-MCI対策学習 □ NCM-MCIオンライン試験 □ サイト《 www.goshiken.com 》で ➠ NCM-MCI □問題集をダウンロードNCM-MCIテスト問題集
- NCM-MCI模擬対策 □ NCM-MCI的中問題集 □ NCM-MCIオンライン試験 ✍ ✔ jp.fast2test.com □✔□で➤ NCM-MCI □を検索して、無料でダウンロードしてくださいNCM-MCIオンライン試験
- NCM-MCIテストガイド、Nutanix NCM-MCI試験問題集、NCM-MCIトレーニング資料 □ ➤ www.goshiken.com □に移動し、➥ NCM-MCI □を検索して無料でダウンロードしてくださいNCM-MCI技術内容
- 真実的-素敵なNCM-MCI日本語版参考資料試験-試験の準備方法NCM-MCI認定テキスト □⇒ www.passtest.jp ⇐に移動し、⇒ NCM-MCI ⇐を検索して、無料でダウンロード可能な試験資料を探しますNCM-MCI合格体験記
- NCM-MCIテスト問題集 □ NCM-MCI対策学習 □ NCM-MCIブロンズ教材 □ ✔ NCM-MCI □✔□の試験問題は（ www.goshiken.com ）で無料配信中NCM-MCIテスト問題集
- 試験の準備方法-実際的なNCM-MCI日本語版参考資料試験-素敵なNCM-MCI認定テキスト □▹ www.mogiexam.com ◃にて限定無料の➤ NCM-MCI □問題集をダウンロードせよNCM-MCI対応内容
- yiwnhua.com, 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, 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, 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, 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, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BONUS！！！ Japancert NCM-MCIダンプの一部を無料でダウンロード：https://drive.google.com/open?id=1kPVeZ3pJ5xIjqdhb-iZynNX4dZZ0tY0V