

BraindumpStudy 3V0-41.22 Exam Questions are Verified by Subject Matter Experts

Pass VMware 3V0-41.22 Exam with Real Questions

VMware 3V0-41.22 Exam

Advanced Deploy VMware NSX-T Data Center 3.x

<https://www.passquestion.com/3V0-41.22.html>



Pass VMware 3V0-41.22 Exam with PassQuestion 3V0-41.22 questions and answers in the first attempt.

<https://www.passquestion.com/>

1 / 7

BTW, DOWNLOAD part of BraindumpStudy 3V0-41.22 dumps from Cloud Storage: <https://drive.google.com/open?id=1iTvqYrILJOy23zdw25xU93Jf0yOt90>

It would be really helpful to purchase Advanced Deploy VMware NSX-T Data Center 3.X (3V0-41.22) exam dumps right away. If you buy this VMware Certification Exams product right now, we'll provide you with up to 1 year of free updates for Advanced Deploy VMware NSX-T Data Center 3.X (3V0-41.22) authentic questions. You can prepare using these no-cost updates in accordance with the most recent test content changes provided by the Advanced Deploy VMware NSX-T Data Center 3.X (3V0-41.22) exam dumps.

The authority and validity of VMware 3V0-41.22 pdf practice are the 100% pass guarantee for all the IT candidates. We ensure you one year free update after purchase, so you can obtain the latest information about 3V0-41.22 test cram review without costing extra money. Besides, you can download the BraindumpStudy 3V0-41.22 Torrent dumps and install it on your electronic device, thus you can review at anytime and anywhere available. The fast study and 3V0-41.22 valid practice will facilitate your coming test.

>> Examcollection 3V0-41.22 Vce <<

Extraordinary VMware 3V0-41.22 Exam Dumps To Pass The 3V0-41.22 Exam

There are three different kinds of our 3V0-41.22 exam questions: the PDF, Software and APP online. And i love the Software for the best for no matter how many software you have installed on your computers, our 3V0-41.22 learning materials will never be influenced. Also, our 3V0-41.22 Study Guide just need to be opened with internet service for the first time. Later, you can freely take it everywhere as long as you use it in the Windows system

VMware Advanced Deploy VMware NSX-T Data Center 3.X Sample Questions (Q13-Q18):

NEW QUESTION # 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:	VMware!!
SFTP IP:	192.168.10.91
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:	VMware!!

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.

Answer:

Explanation:

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 /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 VMware!!. 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.

NEW QUESTION # 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.

Answer:

Explanation:

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.

NEW QUESTION # 15

Task 8

You are tasked With troubleshooting the NSX IPSec VPN service Which has been reported down. Verify the current NSX configuration is deployed and resolve any issues.

You need to:

* Verify the present configuration as provided below:

NSX IPSec Session Name:	IPSec
Remote IP:	192.168.140.2
Local Networks:	10.10.10.0/24
Remove Networks:	10.10.20.0/24
Pre-shared Key:	VMware!VMware!!

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 15 minutes to complete.

Answer:

Explanation:

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

Explanation

To troubleshoot the NSX IPSec VPN service that has been reported down, 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 > VPN > IPSec VPN and select the IPSec VPN session that is down. You can identify the session by its name, local endpoint, remote endpoint, and status.

Click Show IPSec Statistics and view the details of the IPSec VPN session failure. You can see the error message, the tunnel state, the IKE and ESP status, and the statistics of the traffic sent and received.

Compare the configuration details of the IPSec VPN session with the expected configuration as provided below. Check for any discrepancies or errors in the parameters such as local and remote endpoints, local and remote networks, IKE and ESP profiles, etc.

If you find any configuration errors, click Actions > 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 local and remote endpoints. You can use ping or traceroute commands from the NSX Edge CLI to test the connectivity. You can also use show service ipsec command to check the status of IPSec VPN 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 third-party device.

After resolving the issues, verify that the IPSec VPN session is up and running by refreshing the IPSec VPN page on the NSX Manager UI. You can also use show service ipsec sp and show service ipsec sa commands on the NSX Edge CLI to check the status of security policy and security association for the IPSec VPN session.

NEW QUESTION # 16

SIMULATION

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:

• Configure Tags with the following configuration detail:	
Tag Name	Member
Boston	Boston-web-01a, Boston-web-02a, Boston-app-01a, Boston-db-01a
Boston-Web	Boston-web-01a, Boston-web-02a
Boston-App	Boston-app-01a
Boston-DB	Boston-db-01a

• Configure Security Groups (use tags to define group criteria) with the following configuration detail:	
Boston	
Boston Web-Servers	
Boston App-Servers	
Boston DB-Servers	

• Configure the Distributed Firewall Exclusion List with the following configuration detail:	
Virtual Machine:	core-A

• Configure Policy & DFW Rules with the following configuration detail:	
Policy Name:	Boston-Web-Application
Applied to:	Boston
New Services:	TCP-8443, TCP-3051

• Policy detail:				
Rule Name	Source	Destination	Service	Action
Any-to-Web	Any	Boston Web-Servers	HTTP,HTTPS	ALLOW
Web-to-App	Boston Web-Servers	Boston App-Servers	TCP-8443	ALLOW
App-to-DB	Boston App-Servers	Boston DB-Servers	TCP-3051	ALLOW

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.

Answer:

Explanation:

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

Step-by-Step Guide

Creating Tags and Security Groups

First, log into the NSX-T Manager GUI and navigate to Inventory > Tags to create tags like "BOSTON-Web" for web servers and assign virtual machines such as BOSTON-web-01a and BOSTON-web-02 a. Repeat for "BOSTON-App" and "BOSTON-DB" with their respective VMs. Then, under Security > Groups, create security groups (e.g., "BOSTON Web-Servers") based on these tags to organize the network logically.

Excluding Virtual Machines

Next, go to Security > Distributed Firewall > Exclusion List and add the "core-A" virtual machine to exclude it from firewall rules, ensuring it operates without distributed firewall restrictions.

Defining Custom Services

Check Security > Services for existing services. If "TCP-9443" and "TCP-3051" are missing, create them by adding new services with the protocol TCP and respective port numbers to handle specific application traffic.

Setting Up the Policy and Rules

Create a new policy named "BOSTON-Web-Application" under Security > Distributed Firewall > Policies. Add rules within this policy:

Allow any source to "BOSTON Web-Servers" for HTTP/HTTPS.

Permit "BOSTON Web-Servers" to "BOSTON App-Servers" on TCP-9443.

Allow "BOSTON App-Servers" to "BOSTON DB-Servers" on TCP-3051. Finally, save and publish the policy to apply the changes.

This setup ensures secure, segmented traffic for the 3-tier web application, an unexpected detail being the need to manually create custom services for specific ports, enhancing flexibility.

Survey Note: Detailed Configuration of Micro-Segmentation Policy in VMware NSX-T Data Center 3.x This note provides a comprehensive guide for configuring a micro-segmentation policy for a 3-tier web application in VMware NSX-T Data Center 3.x, based on the task requirements. The process involves creating tags, security groups, excluding specific virtual machines, defining custom services, and setting up distributed firewall policies. The following sections detail each step, ensuring a thorough understanding for network administrators and security professionals.

Background and Context

Micro-segmentation in VMware NSX-T Data Center is a network security technique that logically divides the data center into distinct security segments, down to the individual workload level, using network virtualization technology. This is particularly crucial for a 3-tier web application, comprising web, application, and database layers, to control traffic and enhance security. The task specifies configuring this for a production environment, with notes indicating passwords are in user_readme.txt and no need to wait for configuration changes, as processing may take time.

Step-by-Step Configuration Process

Step 1: Creating Tags

Tags are used in NSX-T to categorize virtual machines, which can then be grouped for policy application. The process begins by logging into the NSX-T Manager GUI, accessible via a web browser with admin privileges. Navigate to Inventory > Tags, and click "Add Tag" to create the following:

Tag name: "BOSTON-Web", assigned to virtual machines BOSTON-web-01a and BOSTON-web-02a.

Tag name: "BOSTON-App", assigned to BOSTON-app-01a.

Tag name: "BOSTON-DB", assigned to BOSTON-db-01a.

This step ensures each tier of the application is tagged for easy identification and grouping, aligning with the attachment's configuration details.

Step 2: Creating Security Groups

Security groups in NSX-T are logical constructs that define membership based on criteria like tags, enabling targeted policy application. Under Security > Groups, click "Add Group" to create:

Group name: "BOSTON Web-Servers", with criteria set to include the "BOSTON-Web" tag.

Group name: "BOSTON App-Servers", with criteria set to include the "BOSTON-App" tag.

Group name: "BOSTON DB-Servers", with criteria set to include the "BOSTON-DB" tag.

This step organizes the network into manageable segments, facilitating the application of firewall rules to specific tiers.

Step 3: Excluding "core-A" VM from Distributed Firewall

The distributed firewall (DFW) in NSX-T monitors east-west traffic between virtual machines. However, certain VMs, like load balancers or firewalls, may need exclusion to operate without DFW restrictions. Navigate to Security > Distributed Firewall > Exclusion List, click "Add", select "Virtual Machine", and choose "core-A". Click "Save" to exclude it, ensuring it bypasses DFW rules, as per the task's requirement.

Step 4: Defining Custom Services

Firewall rules often require specific services, which may not be predefined. Under Security > Services, check for existing services "TCP-9443" and "TCP-3051". If absent, create them:

Click "Add Service", name it "TCP-9443", set protocol to TCP, and port to 9443.

Repeat for "TCP-3051", with protocol TCP and port 3051.

This step is crucial for handling application-specific traffic, such as the TCP ports mentioned in the policy type (TCP-9443, TCP-3051), ensuring the rules can reference these services.

Step 5: Creating the Policy and Rules

The final step involves creating a distributed firewall policy to enforce micro-segmentation. Navigate to Security > Distributed Firewall > Policies, click "Add Policy", and name it "BOSTON-Web-Application". Add a section, then create the following rules:

Rule Name: "Any-to-Web"

Source: Any (select "Any" or IP Address 0.0.0.0/0)

Destination: "BOSTON Web-Servers" (select the group)

Service: HTTP/HTTPS (predefined service)

Action: Allow

Rule Name: "Web-to-App"

Source: "BOSTON Web-Servers"
Destination: "BOSTON App-Servers"
Service: TCP-9443 (custom service created earlier)
Action: Allow
Rule Name: "App-to-DB"
Source: "BOSTON App-Servers"
Destination: "BOSTON DB-Servers"
Service: TCP-3051 (custom service created earlier)
Action: Allow

After defining the rules, click "Save" and "Publish" to apply the policy. This ensures traffic flows as required: any to web servers for HTTP/HTTPS, web to app on TCP-9443, and app to database on TCP-3051, while maintaining security through segmentation.

Additional Considerations

The task notes indicate no need to wait for configuration changes, as processing may take time, and steps are not dependent, suggesting immediate progression is acceptable. Passwords are in user_readme.txt, implying the user has necessary credentials. The policy order is critical, with rules processed top-to-bottom, and the attachment's "Type: TCP-9443, TCP-3051" likely describes the services used, not affecting the configuration steps directly.

Table: Summary of Configuration Details

Component

Details

Tags

BOSTON-Web (BOSTON-web-01a, BOSTON-web-02a), BOSTON-App (BOSTON-app-01a), BOSTON-DB (BOSTON-db-01a) Security Groups BOSTON Web-Servers (tag BOSTON-Web), BOSTON App-Servers (tag BOSTON-App), BOSTON DB-Servers (tag BOSTON-DB) DFW Exclusion List Virtual Machine: core-A Custom Services TCP-9443 (TCP, port 9443), TCP-3051 (TCP, port 3051) Policy Name BOSTON-Web-Application Firewall Rules Any-to-Web (Any to Web-Servers, HTTP/HTTPS, Allow), Web-to-App (Web to App-Servers, TCP-9443, Allow), App-to-DB (App to DB-Servers, TCP-3051, Allow) This table summarizes the configuration, aiding in verification and documentation.

Unexpected Detail

An unexpected aspect is the need to manually create custom services for TCP-9443 and TCP-3051, which may not be predefined, highlighting the flexibility of NSX-T for application-specific security policies.

Conclusion

This detailed process ensures a robust micro-segmentation policy, securing the 3-tier web application by controlling traffic between tiers and excluding specific VMs from DFW, aligning with best practices for network security in VMware NSX-T Data Center 3.x.

NEW QUESTION # 17

Task 14

An administrator has seen an abundance of alarms regarding high CPU usage on the NSX Managers. The administrator has successfully cleared these alarms numerous times in the past and is aware of the issue. The administrator feels that the number of alarms being produced for these events is overwhelming the log files.

You need to:

- * Review CPU Sensitivity and Threshold values.

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 5 minutes to complete.

Answer:

Explanation:

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

Explanation

To review CPU sensitivity and threshold values, 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 > Settings > System Settings > CPU and Memory Thresholds.

You will see the current values for CPU and memory thresholds for NSX Manager, NSX Controller, and NSX Edge. These values determine the percentage of CPU and memory usage that will trigger an alarm on the NSX Manager UI.

You can modify the default threshold values by clicking Edit and entering new values in the text boxes.

For example, you can increase the CPU threshold for NSX Manager from 80% to 90% to reduce the number of alarms for high CPU usage. Click Save to apply the changes.

You can also view the historical data for CPU and memory usage for each component by clicking View Usage History. You can select a time range and a granularity level to see the usage trends and patterns over time

NEW QUESTION # 18

.....

With the increasing marketization, the 3V0-41.22 study guide experience marketing has been praised by the consumer market. Attract users interested in product marketing to know just the first step, the most important is to be designed to allow the user to try before buying the 3V0-41.22 study training materials, so we provide free pre-sale experience to help users to better understand our 3V0-41.22 Exam Questions. The user only needs to submit his E-mail address and apply for free trial online, and our system will soon send free demonstration research materials of 3V0-41.22 latest questions to download.

3V0-41.22 Valid Test Question: https://www.braindumpstudy.com/3V0-41.22_braindumps.html

Skip all the worthless VMware 3V0-41.22 tutorials and download VMware Advanced Deploy VMware NSX-T Data Center 3.X exam details with real questions and answers and a price too unbelievable to pass up, We are pleased that you can spare some time to have a look for your reference about our 3V0-41.22 test prep, You can email us or contact our customer service staff online if you have any questions in the process of purchasing or using accurate 3V0-41.22 Dumps collection, VMware Examcollection 3V0-41.22 Vce In a word, you are pursuing a good thing and your attitude is positive and inspiring.

Like other certificates acquired through other platforms Test 3V0-41.22 Sample Online other than the online, it is accepted as a valid certification, The Three-Party Model, Skip all the worthless VMware 3V0-41.22 tutorials and download VMware Advanced Deploy VMware NSX-T Data Center 3.X exam details with real questions and answers and a price too unbelievable to pass up.

VMware - Professional Examcollection 3V0-41.22 Vce

We are pleased that you can spare some time to have a look for your reference about our 3V0-41.22 test prep, You can email us or contact our customer service staff online if you have any questions in the process of purchasing or using accurate 3V0-41.22 Dumps collection.

In a word, you are pursuing a good thing and Examcollection 3V0-41.22 Vce your attitude is positive and inspiring, The 24/7 support system is available for the customers, so they can contact the 3V0-41.22 support whenever they face any issue, and it will provide them with the solution.

- Testking 3V0-41.22 Learning Materials □ 3V0-41.22 Valid Test Vce □ Latest 3V0-41.22 Exam Forum □ [www.prep4sures.top] is best website to obtain ⇒ 3V0-41.22 ⇐ for free download □ 3V0-41.22 Latest Exam Registration
- Trustworthy 3V0-41.22 Source □ Latest 3V0-41.22 Test Format □ Certificate 3V0-41.22 Exam □ Immediately open ⇒ www.pdfvce.com ⇐ and search for “3V0-41.22” to obtain a free download □ 3V0-41.22 Exam Details
- Pass Guaranteed 2025 VMware 3V0-41.22 –Reliable Examcollection Vce □ Search for ➡ 3V0-41.22 □ and download exam materials for free through 《 www.examdumps.com 》 □ Test 3V0-41.22 Price
- Pass Guaranteed 2025 VMware 3V0-41.22 –Reliable Examcollection Vce □ Search on ➡ www.pdfvce.com □ for ☀ 3V0-41.22 □ ☀ □ to obtain exam materials for free download □ 3V0-41.22 Reliable Test Camp
- 3V0-41.22 Exam Details ~ 3V0-41.22 New Braindumps Files □ Latest 3V0-41.22 Test Format □ Open □ www.lead1pass.com □ enter 「 3V0-41.22 」 and obtain a free download □ Test 3V0-41.22 Price
- Pass Guaranteed 2025 VMware 3V0-41.22 –Reliable Examcollection Vce □ Search for ➡ 3V0-41.22 □ and download exam materials for free through ➤ www.pdfvce.com □ ☺ Testking 3V0-41.22 Learning Materials
- 3V0-41.22 Exam Details □ 3V0-41.22 Latest Exam Registration □ Latest 3V0-41.22 Exam Forum □ Search for 「 3V0-41.22 」 and download it for free on ➡ www.examcollectionpass.com □ website □ Latest 3V0-41.22 Test Format
- Customized 3V0-41.22 Lab Simulation □ 3V0-41.22 Exam Details □ 3V0-41.22 Study Guide □ Open ➡ www.pdfvce.com □ and search for □ 3V0-41.22 □ to download exam materials for free □ Latest 3V0-41.22 Exam Forum
- Pass Guaranteed 2025 VMware 3V0-41.22 –Reliable Examcollection Vce □ ✓ www.pdfdumps.com □ ✓ □ is best website to obtain □ 3V0-41.22 □ for free download ◀ 3V0-41.22 Certification Materials
- 3V0-41.22 Vce Torrent □ 3V0-41.22 Valid Test Vce □ Trustworthy 3V0-41.22 Source □ Easily obtain □ 3V0-41.22 □ for free download through (www.pdfvce.com) □ Customized 3V0-41.22 Lab Simulation
- 3V0-41.22 Study Guide □ 3V0-41.22 Guaranteed Success □ 3V0-41.22 Valid Test Vce ➡ Easily obtain ➡ 3V0-41.22 □ for free download through □ www.vceengine.com □ □ Latest 3V0-41.22 Test Format
- kuhenan.com, peterbonadieacademy.org, shortcourses.russellcollege.edu.au, www.stes.tyc.edu.tw, xzbbs.pzdapi.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, four.academy, www.stes.tyc.edu.tw, www.myvrgame.cn, Disposable vapes

BONUS!!! Download part of BraindumpStudy 3V0-41.22 dumps for free: <https://drive.google.com/open?>

id=1iTvqYriLJOy23zdwlw25xU93Jf0yOt9O