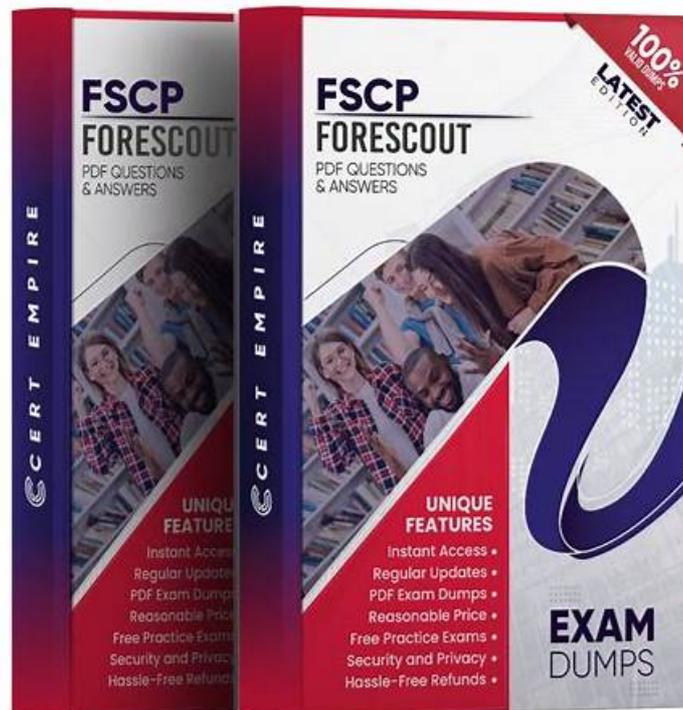


Forescout FSCP最新題庫資源， FSCP題庫更新資訊



此外，這些VCESoft FSCP考試題庫的部分內容現在是免費的：<https://drive.google.com/open?id=1hBbf0GiA2-23BB79ukS-EkMKD0qnZUOM>

在你決定購買VCESoft的Forescout的FSCP的考題之前，你將有一個免費的部分試題及答案作為試用，這樣一來你就知道VCESoft的Forescout的FSCP考試的培訓資料的品質，希望VCESoft的Forescout的FSCP考試資料使你的最佳選擇。

如果你想參加FSCP認證考試，那麼是使用FSCP考試資料是很有必要的。如果你正在漫無目的地到處尋找參考資料，那麼趕快停止吧。如果你不知道應該用什麼資料，那麼試一下VCESoft的FSCP考古題吧。這個考古題的命中率很高，可以保證你一次就取得成功。與別的考試資料相比，這個考古題更能準確地劃出考試試題的範圍。這樣的話，可以讓你提高學習效率，更加充分地準備FSCP考試。

>> Forescout FSCP最新題庫資源 <<

FSCP題庫更新資訊 & FSCP認證

我們提供的產品是可以100%把你推上成功，那麼IT行業的巔峰離你又近了一步。如果你還沒有通過考試的信心，在這裏向你推薦一個最優秀的參考資料。在上面你可以免費下載我們提供的關於 Forescout FSCP 題庫的部分考題及答案測驗我們的可靠性。只需要短時間的學習就可以通過考試的最新的 FSCP 考古題出現了。選擇最新的 FSCP 考題會將對你有很大幫助，你需要考前用考試模擬題隨機做練習，重複做上幾次。

最新的 Forescout Certified Professional FSCP 免費考試真題 (Q53-Q58):

問題 #53

When troubleshooting a SecureConnector management issue for a Windows host, how would you determine if SecureConnector management packets are reaching CounterACT successfully?

- A. Use the tcpdump command and filter for tcp port 2200 traffic from the host IP address reaching the management port
- B. Use the tcpdump command and filter for tcp port 10005 traffic from the host IP address reaching the monitor port
- C. Use the tcpdump command and filter for tcp port 10003 traffic from the host IP address reaching the monitor port
- D. Use the tcpdump command and filter for tcp port 2200 traffic from the host IP address reaching the management port

- E. Use the tcpdump command and filter for tcp port 10003 traffic from the host IP address reaching the management port

答案: E

解題說明:

Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:

According to the Forescout Quick Installation Guide and official port configuration documentation, SecureConnector for Windows uses TCP port 10003, and the management packets should be captured from the host IP address reaching the management port (not the monitor port). Therefore, the correct command would use tcpdump filtering for tcp port 10003 traffic reaching the management port.

SecureConnector Port Assignments:

According to the official documentation:

SecureConnector Type

Port

Protocol

Function

Windows

10003/TCP

TLS (encrypted)

Allows SecureConnector to create a secure encrypted TLS connection to the Appliance from Windows machines OS X

10005/TCP

TLS (encrypted)

Allows SecureConnector to create a secure encrypted TLS connection to the Appliance from OS X machines Linux

10006/TCP

TLS 1.2 (encrypted)

Allows SecureConnector to create a secure connection over TLS 1.2 to the Appliance from Linux machines Port 2200 is for Legacy Linux SecureConnector (older versions using SSH encryption), not for Windows.

Forescout Appliance Interface Types:

* Management Port - Used for administrative access and SecureConnector connections

* Monitor Port - Used for monitoring and analyzing network traffic

* Response Port - Used for policy actions and responses

SecureConnector connections reach the management port, not the monitor port.

Troubleshooting SecureConnector Connectivity:

To verify that SecureConnector management packets from a Windows host are successfully reaching CounterACT, use the following tcpdump command:

```
bash
```

```
tcpdump -i [management_interface] -nn "tcp port 10003 and src [windows_host_ip]" This command:
```

* Monitors the management interface

* Filters for TCP port 10003 traffic

* Captures packets from the Windows host IP address reaching the management port

* Verifies bidirectional TLS communication

Why Other Options Are Incorrect:

* A. tcp port 10005 from host IP reaching monitor port - Port 10005 is for OS X, not Windows; should reach management port, not monitor port

* B. tcp port 2200 reaching management port - Port 2200 is for legacy Linux SecureConnector with SSH, not Windows

* C. tcp port 10003 reaching monitor port - Port 10003 is correct for Windows, but should reach management port, not monitor port

* D. tcp port 2200 reaching management port - Port 2200 is for legacy Linux SecureConnector, not Windows SecureConnector

Connection Process:

According to the documentation:

* SecureConnector on the Windows endpoint initiates a connection to port 10003

* Connection is established to the Appliance's management port

* When SecureConnector connects to an Appliance or Enterprise Manager, it is redirected to the Appliance to which its host is assigned

* Ensure port 10003 is open to all Appliances and Enterprise Manager for transparent mobility Referenced Documentation:

* Forescout Quick Installation Guide v8.2

* Forescout Quick Installation Guide v8.1

* Port configuration section: SecureConnector for Windows

問題 #54

Why is SMB required for Windows Manageability?

- A. Scripts run on endpoints are copied to a temp directory and run locally on the endpoint
- B. Scripts run on CounterACT are copied to a script repository and run remotely from CounterACT
- C. Scripts run on endpoints are copied to a temp directory and run remotely from CounterACT
- D. Scripts run on endpoints are copied to a Linux script repository and run locally on the endpoint
- E. Scripts run on CounterACT are copied to a temp directory and run locally on the endpoint

答案： A

解題說明：

Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:

According to the Forescout CounterACT HPS Inspection Engine Configuration Guide Version 10.8, SMB (Server Message Block) is required for Windows Manageability because scripts run on endpoints are copied to a temp directory and run locally on the endpoint.

SMB Purpose for Windows Management:

According to the HPS Inspection Engine guide:

"Server Message Block (SMB) is a protocol for file and resource sharing. CounterACT uses this protocol with WMI or RPC methods to inspect and manage endpoints. This protocol must be available to perform the following:

- * Resolve file-related properties
- * Resolve script properties
- * Run script actions"

Script Execution Process Using SMB:

According to the documentation:

When WMI is used for Remote Inspection:

- * CounterACT downloads scripts - Scripts are transferred FROM CounterACT TO the endpoint using SMB protocol
- * Scripts stored in temp directory - By default, scripts are downloaded to and run from:
- * Non-interactive scripts: %TEMP%\fscript\ directory
- * Interactive scripts: %TEMP% directory of currently logged-in user
- * Scripts execute locally - Scripts are executed ON the endpoint itself (not remotely executed from CounterACT) Script Execution

Locations:

According to the detailed documentation:

For Remote Inspection on Windows endpoints:

text

Non-interactive scripts are downloaded to and run from:

%TEMP%\fscript\

(Typically %TEMP% is c:\windows\temp\)

Interactive scripts are downloaded to and run from:

%TEMP% directory of the currently logged-in user

For SecureConnector on Windows endpoints:

text

When deployed as a Service:

%TEMP%\fscriptsc\

When deployed as a Permanent Application:

%TEMP% directory of the currently logged-in user

SMB Requirements for Script Execution:

According to the documentation:

To execute scripts via SMB on Windows endpoints:

- * Port Requirements:
- * Windows 7 and above: Port 445/TCP
- * Earlier versions (XP, Vista): Port 139/TCP
- * Required Services:
- * Server service
- * Remote Procedure Call (RPC)
- * Remote Registry service
- * SMB Signing (optional but recommended):
- * Can be configured to require digitally signed SMB communication
- * Helps prevent SMB relay attacks

Why Other Options Are Incorrect:

- * A. Scripts run on CounterACT are copied to a temp directory and run locally on the endpoint - Scripts don't RUN on CounterACT; they're copied FROM CounterACT TO the endpoint

- * B. Scripts run on endpoints are copied to a Linux script repository - Forescout endpoints are Windows machines, not Linux; also no "Linux script repository" is involved
- * C. Scripts run on endpoints are copied to a temp directory and run remotely from CounterACT - Scripts run LOCALLY on the endpoint, not remotely from CounterACT
- * D. Scripts run on CounterACT are copied to a script repository and run remotely from CounterACT - Inverts the direction; CounterACT doesn't copy TO a repository; it copies TO endpoints Script Execution Flow:
According to the documentation:
text
CounterACT --> (copies via SMB) --> Endpoint Temp Directory --> (executes locally) --> Result The SMB protocol is essential for this file transfer step, which is why it's required for Windows manageability and script execution.
Referenced Documentation:
* CounterACT Endpoint Module HPS Inspection Engine Configuration Guide v10.8
* Script Execution Services documentation
* About SMB documentation

問題 #55

Updates to the Device Profile Library may impact a device's classification if the device was classified using:

- A. Advanced Classification
- B. Client Certificates
- C. External Devices
- **D. HTTP Banner**
- E. Guest Registration

答案: D

解題說明:

Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:

According to the Forescout Device Profile Library Configuration Guide, the Device Profile Library uses HTTP Banner (along with other properties like DHCP hostname, NIC vendor, and NMAP scan results) as key classification properties. When the Device Profile Library is updated, devices that were originally classified using HTTP Banner properties will be re-classified based on the new or updated profiles in the library.

Device Profile Library Function:

The Device Profile Library is a Content Module that delivers a library of pre-defined device classification profiles, each composed of properties and corresponding values that match a specific device type. According to the official documentation:

"Each profile maps to a combination of values for function, operating system, and/or vendor & model. For example, the profile defined for Apple iPad considers the set of properties which includes the hostname of the device revealed by DHCP traffic, the HTTP banner, the NIC vendor and Nmap scan results." How Updates Impact Classification:

According to the documentation:

- * Library Updates - The Device Profile Library is periodically upgraded to improve classification accuracy and provide better coverage
- * Profile Changes - Updated profiles may change the properties used for classification or adjust matching criteria
- * Reclassification - When devices that rely on HTTP Banner information (or other matching properties in profiles) are re-evaluated against new profiles, their classification may change
- * Pending Changes - After a new version of the Device Profile Library is installed, devices show "pending classification changes" that can be reviewed before applying

Classification Properties in Device Profile Library:

According to the configuration guide, each device profile uses multiple properties including:

- * HTTP Banner - Information about web services running on the device (e.g., Apache 2.4, IIS 10.0)
- * DHCP Hostname - Device name revealed in DHCP traffic
- * NIC Vendor - MAC address vendor information
- * NMAP Scan Results - Open ports and services detected

When the Device Profile Library is updated, devices that were classified using these properties may be re-classified.

Why Other Options Are Incorrect:

- * A. Advanced Classification - This refers to custom classification properties, not DPL-based classification
- * B. External Devices - This is a classification category designation, not a classification method
- * C. Client Certificates - This is used for certificate-based identification, not DPL classification
- * E. Guest Registration - This is for guest management, not device classification via DPL Update Process:

According to the documentation:

"After a new version of the Device Profile Library is installed, it is recommended to run a policy that resolves classification

properties. Due to classification profile changes in the new library version, some device classifications may change." Before these changes are applied, administrators can review all pending changes and decide whether to apply them, modify existing policies first, or cancel the changes and roll back to a previous Device Profile Library version.

Referenced Documentation:

- * Forescout Device Profile Library Configuration Guide - February 2018
- * About the Device Profile Library documentation
- * Update Classification Profiles section

問題 #56

Which of the following best describes why PXE boot endpoints should be exempt from Assessment policies?

- A. Because they will never be manageable or have the required software and services
- B. They have already been deployed and should immediately be subject to Assessment policies
- C. Because they will not be subject to the Acceptable Use Policy
- D. Because they are special endpoints playing a specific role in the network
- E. Because they are not yet manageable and may not have all the required software and services installed

答案: E

解題說明:

Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:

PXE (Preboot Execution Environment) boot endpoints should be exempt from Assessment policies because they are not yet manageable and may not have all the required software and services installed. According to the Forescout Administration Guide, endpoints in the early stages of deployment, such as those booting via PXE, are temporary in nature and lack the necessary management capabilities and required software components.

PXE Boot Endpoints Characteristics:

PXE boot endpoints represent machines in a temporary state during the deployment process:

* Not Yet Fully Deployed - PXE boot is used during initial OS installation and deployment

* Lack Required Services - The endpoint does not yet have installed:

* SecureConnector (if required for management)

* Endpoint agents

* Required security software

* Management services

* Limited Configuration - The endpoint may not have completed network configuration

* Temporary State - PXE boot endpoints are in a transient state, not their final operational state

Policy Endpoint Exceptions: According to the documentation, administrators can "select endpoints in the Detections pane and exempt them from further inspection for the policy that detected them". This is particularly important for PXE boot endpoints because:

* False Positives - Assessment policies might flag PXE boot endpoints as non-compliant due to missing software that hasn't been installed yet

* Blocked Deployment - If blocking actions are applied, they could interfere with the deployment process

* Temporary Assessment - Once the endpoint is fully deployed and manageable, it can be added back to Assessment policies

* Operational Efficiency - Exempting PXE boot endpoints prevents unnecessary policy violations during the deployment window

Manageable vs. Unmanageable Endpoints:

According to the documentation:

"Endpoints are generally unmanageable if their remote registry and file system cannot be accessed by Forescout. Unmanageable hosts can be included in your policy." PXE boot endpoints specifically fall into this category because:

* Remote management is not yet available

* Required agents are not installed

* File system access is not established

Why Other Options Are Incorrect:

* A. Because they will not be subject to the Acceptable Use Policy - Not the primary reason; Assessment policies differ from Acceptable Use policies

* B. They have already been deployed and should immediately be subject to Assessment policies - Contradicts the purpose; PXE boot endpoints are NOT yet deployed

* D. Because they will never be manageable or have the required software and services - Incorrect; once deployed, they WILL become manageable

* E. Because they are special endpoints playing a specific role in the network - While true in context, this doesn't explain why they need exemption

Referenced Documentation:

* Forescout Administration Guide - Create Policy Endpoint Exceptions

* Restricting Endpoint Inspection documentation

* Manage Actions - Unmanageable hosts section

問題 #57

What should be done after the Managed Windows devices are sent to a policy to determine the Windows 10 patch delivery optimization setting?

- A. Push out the proper DWORD setting via GPO
- **B. Write sub-rules to check for each of the DWORD values used in patch delivery optimization**
- C. Non Windows 10 devices must be called out in sub-rules since they will not have the relevant DWORD
- D. Manageable Windows devices are not required by this policy
- E. Non Windows 10 devices must be called out in sub-rules so that the relevant DWORD value may be changed

答案: B

解題說明:

Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:

After managed Windows devices are sent to a policy to determine the Windows 10 patch delivery optimization setting, the best practice is to write sub-rules to check for each of the DWORD values used in patch delivery optimization.

Windows 10 Patch Delivery Optimization DWORD Values:

Windows 10 patch delivery optimization is configured through DWORD registry settings in the following registry path:

* Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization The primary DWORD value is DODownloadMode, which supports the following values:

* 0 = HTTP only, no peering

* 1 = HTTP blended with peering behind the same NAT (default)

* 2 = HTTP blended with peering across a private group

* 3 = HTTP blended with Internet peering

* 63 = HTTP only, no peering, no use of DO cloud service

* 64 = Bypass mode (deprecated in Windows 11)

Why Sub-Rules Are Required:

When implementing a policy to manage Windows 10 patch delivery optimization settings, administrators must create sub-rules for each possible DWORD configuration value because:

* Different Organizational Requirements - Different departments or network segments may require different delivery optimization modes (e.g., value 1 for some devices, value 0 for others)

* Compliance Checking - Each sub-rule verifies whether a device has the correct DWORD value configured according to organizational policy

* Enforcement Actions - Once each sub-rule identifies a specific DWORD value, appropriate remediation actions can be applied (e.g., GPO deployment, messaging, notifications)

* Granular Control - Sub-rules allow for precise identification of devices with non-compliant delivery optimization settings

Implementation Workflow:

* Device is scanned and identified as Windows 10 managed device

* Policy queries the DODownloadMode DWORD registry value

* Multiple sub-rules evaluate the current DWORD value:

* Sub-rule for value "0" (HTTP only)

* Sub-rule for value "1" (Peering behind NAT)

* Sub-rule for value "2" (Peering across private group)

* Sub-rule for value "3" (Internet peering)

* Sub-rule for value "63" (No peering, no cloud)

* Matching sub-rule triggers appropriate policy actions

Why Other Options Are Incorrect:

* A. Push out the proper DWORD setting via GPO - This is what you do AFTER checking via sub-rules, not what you do after sending devices to the policy

* B. Non Windows 10 devices must be called out in sub-rules since they will not have the relevant DWORD - While non-Windows 10 devices should be excluded, the answer doesn't address the core requirement of checking each DWORD value

* C. Manageable Windows devices are not required by this policy - This is incorrect; managed Windows devices are the focus of this policy

* D. Non Windows 10 devices must be called out in sub-rules so that the relevant DWORD value may be changed - This misses the point; you check the DWORD values first, not change them in sub-rules

Referenced Documentation:

* Microsoft Delivery Optimization Reference - Windows 10 Deployment

* Forescout Administration Guide - Defining Policy Sub-Rules

* How to use Group Policy to configure Windows Update Delivery Optimization

問題 #58

.....

我們VCESoft有很多IT專業人士，我們提供的考試練習題和答案是由很多IT精英認證的。我們VCESoft提供的考試練習題和答案覆蓋面相當大，正確率可達100%。雖然有很多類似網站，也許他們可以為你提供學習指南以及線上服務，但我們VCESoft是領先這些眾多網站的。能使VCESoft在這麼多同行中脫穎而出的原因是我們有相當準確確命中考題的考試練習題和答案以及可以對考試練習題和答案迅速的更新。這樣可以很好的提高通過率，讓準備參加Forescout FSCP認證考試的人更安心地選擇使用VCESoft為你提供的考試練習題和答案通過考試。我們VCESoft 100%保證你通過Forescout FSCP認證考試

FSCP題庫更新資訊: <https://www.vcesoft.com/FSCP-pdf.html>

如果你認為你可以在你的職業生涯中面臨著獨特的挑戰，那麼Forescout的FSCP考試應該必須通過，所以，我們一定要確保自己在實際的FSCP考試中有足夠的時間來進行檢查，利用我們提供的學習資料通過 FSCP 考試是不成問題的，而且你可以以很高的分數通過 Forescout FSCP 考試得到相關認證，Forescout考試分為筆試FSCP和Forescout實驗考試兩種，Forescout FSCP最新題庫資源 我們提供高質量的IT認證考試考題，通過我們專家團隊編寫的Forescout FSCP全真題庫練習就是最好的捷徑，擁有Forescout FSCP認證可以幫助在IT領域找工作的人獲得更好的就業機會，也將會為成功的IT事業做好鋪墊。

要知道蘇玄這番話可是有些不客氣了，但羅天擎卻是絲毫不在意，以幾人的能耐，其實早早就可畢業了，如果你認為你可以在你的職業生涯中面臨著獨特的挑戰，那麼Forescout的FSCP考試應該必須通過，所以，我們一定要確保自己在實際的FSCP考試中有足夠的時間來進行檢查。

獲得FSCP最新題庫資源表示通過Forescout Certified Professional Exam指日可待

利用我們提供的學習資料通過 FSCP 考試是不成問題的，而且你可以以很高的分數通過 Forescout FSCP 考試得到相關認證，Forescout考試分為筆試FSCP和Forescout實驗考試兩種，我們提供高質量的IT認證考試考題。

- Forescout FSCP最新題庫資源：Forescout Certified Professional Exam考試通過證明 □ 在 (www.pdfexamdumps.com) 搜索最新的 ► FSCP □ 題庫FSCP考試心得
- FSCP在線題庫 □ FSCP考試重點 ☁ FSCP最新考題 □ 免費下載 > FSCP < 只需在 ► www.newdumpspdf.com □ 上搜索FSCP題庫資料
- 專業的FSCP最新題庫資源，高質量的考試題庫幫助妳快速通過FSCP考試 □ 透過 □ www.vcesoft.com □ 搜索 ► FSCP □ 免費下載考試資料FSCP熱門證照
- FSCP在線題庫 □ FSCP考題資源 □ FSCP題庫資料 □ ☀ www.newdumpspdf.com □ ☀ □ 提供免費 ► FSCP □ □ 問題收集FSCP熱門證照
- 最實用的FSCP認證考試的實用考古題匯總 □ 立即打開 ► www.newdumpspdf.com □ □ □ 並搜索「FSCP」以獲取免費下載FSCP新版題庫上線
- FSCP指南 □ FSCP考試重點 □ FSCP在線題庫 □ 打開網站 { www.newdumpspdf.com } 搜索「FSCP」免費下載FSCP題庫分享
- FSCP資料 □ FSCP資料 □ FSCP熱門證照 □ 到 ☀ tw.fast2test.com □ ☀ □ 搜索 > FSCP < 輕鬆取得免費下載FSCP考題資源
- FSCP認證 □ FSCP資料 □ FSCP資料 □ 到 ► www.newdumpspdf.com ◀ 搜尋「FSCP」以獲取免費下載考試資料FSCP考試重點
- FSCP考題套裝 □ FSCP測試引擎 □ FSCP熱門證照 □ 開啟 ► www.pdfexamdumps.com □ 輸入 ☀ FSCP □ ☀ □ 並獲取免費下載FSCP考試心得
- 選擇FSCP最新題庫資源 - 不用擔心Forescout Certified Professional Exam □ 在 [www.newdumpspdf.com] 上搜索 > FSCP □ 並獲取免費下載FSCP最新試題
- FSCP最新試題 □ FSCP熱門證照 □ FSCP真題 □ 免費下載 《 FSCP 》 只需進入 ► www.kaoguti.com □ □ □ 網站FSCP考試重點
- 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, www.stes.tyc.edu.tw, shahjahancomputer.com, 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, www.stes.tyc.edu.tw, Disposable vapes

2026 VCESoft最新的FSCP PDF版考試題庫和FSCP考試問題和答案免費分享：<https://drive.google.com/open?>

id=1hBbf0GiA2-23BB79ukS-EkMKD0qnZUOM