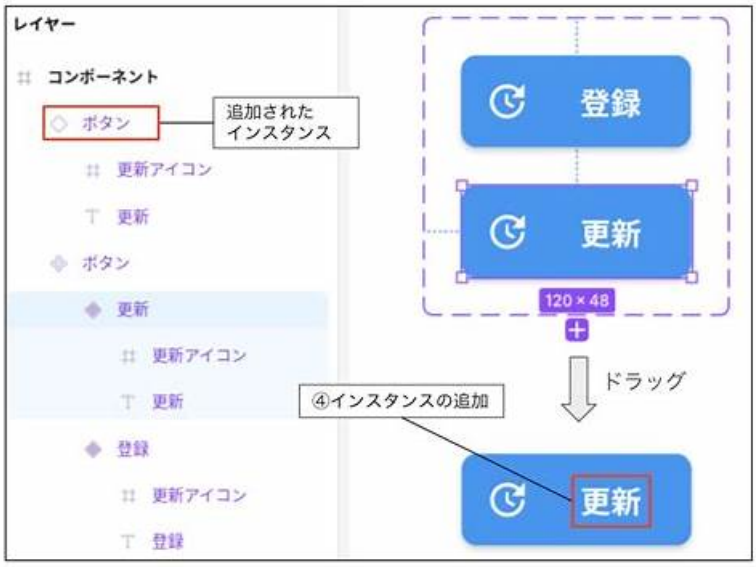
FSCPテキスト、FSCPコンポーネント



すべての人々がFSCP試験に合格し、関連する認定を短時間で取得できるように、3つの異なるバージョンのFSCP学習教材を設計しました。製品は、すべての人が同時に学習とテストを行うための実際の試験をシミュレートすることを試みることができ、学習コースでの学習不足に適した環境を提供することができます。当社からFSCP学習教材を購入して使用すると、実際の試験のようにFSCP学習テストを練習し、FSCP試験に簡単に合格できます。

Forescout FSCP 認定試験の出題範囲:

トピック	出題範囲
トピック 1	• Advanced Product Topics Licenses, Extended Modules and Redundancy: This section of the exam measures skills of product deployment leads and solution engineers, and covers topics such as licensing models, optional modules or extensions, high availability or redundancy configurations, and how those affect architecture and operational readiness.
トピック 2	• Customized Policy Examples: This section of the exam measures skills of security architects and solution delivery engineers, and covers scenario based policy design and implementation: you will need to understand business case requirements, craft tailored policy frameworks, adjust for exceptional devices or workflows, and document or validate those customizations in context.
トピック 3	• Advanced Product Topics Certificates and Identity Tracking: This section of the exam measures skills of identity and access control specialists and security engineers, and covers the management of digital certificates, PKI integration, identity tracking mechanisms, and how those support enforcement and audit capability within the system.
トピック 4	• Notifications: This section of the exam measures skills of monitoring and incident response professionals and system administrators, and covers how notifications are configured, triggered, routed, and managed so that alerts and reports tie into incident workflows and stakeholder communication.
トピック 5	• Policy Functionality: This section of the exam meas-ures skills of policy implementers and integration specialists, and covers how policies operate within the platform, including dependencies, rule order, enforcement triggers, and how they interact with device classifications and dynamic attributes.
トピック 6	• Plugin Tuning HPS: This section of the exam measures skills of plugin developers and endpoint integration engineers, and covers tuning the Host Property Scanner (HPS) plugin: how to profile endpoints, refine scanning logic, handle exceptions, and ensure accurate host attribute collection for enforcement.

試験の準備方法-高品質なFSCPテキスト試験-最高のFSCPコンポーネント

多くのお客様は、当社のFSCP試験問題の価格に疑問を抱いている場合があります。真実は、私たちの価格が同業者の間で比較的安いということです。避けられない傾向は、知識が価値あるものになりつつあることであり、それはなぜ良いFSCPのリソース、サービス、データが良い価格に値するかを説明しています。私たちは常にお客様を第一に考えます。したがって、割引を随時提供しており、1年後にFSCPの質問と回答を2回目に購入すると、50%の割引を受けることができます。低価格で高品質。これが、FSCP準備ガイドを選択する理由です。

Forescout Certified Professional Exam 認定 FSCP 試験問題 (Q40-Q45):

質問 # 40
Proper policy flow should consist of...

- A. Modify as little as possible in discovery, each classify sub-rule should flow to an assess policy, IoT classify policies typically test ownership, IT classify usually indicates ownership.
- B. Modify as little as possible in discovery, each discovery sub-rule should flow to a classify policy. IT classify policies typically test manageability, IoT classify usually indicates ownership.
- C. Modify as little as possible in discovery, each classify sub-rule should flow to an assess policy, IoT classify policies typically test manageability, IT classify usually indicates ownership.
- D. Modify as little as possible in discovery, each sub-rule should flow to assess. IT classify policies typically test manageability, IoT classify usually indicates ownership.
- E. Discovery should include customized sub-rules, each discovery sub-rule should flow to a classify policy, IT classify policies typically test manageability, IoT classify usually indicates ownership.

正解：C

解説：
Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
According to the Forescout IoT Security solutions documentation and policy best practices, proper policy flow should consist of: "Modify as little as possible in discovery, each classify sub-rule should flow to an assess policy, IoT classify policies typically test manageability, IT classify usually indicates ownership".
Policy Flow Architecture:
According to the Forescout IoT Security documentation:
text
Discovery Phase (Passive)
#
Classification Phase (Determine device type)
IoT Classify - Test MANAGEABILITY
IT Classify - Indicate OWNERSHIP
#
Assessment Phase (Evaluate compliance)
#
Control Phase (Apply actions)
Discovery Phase - Minimal Modification:
According to the documentation:
"Modify as little as possible in discovery. Discovery should remain passive and non-invasive, using only network traffic analysis and passive profiling to gain device visibility." This approach prevents operational disruption and maintains passive-only visibility.
Classification Phase:
According to the Forescout solution brief:
* IT Device Classification Policies:
* Typically indicate OWNERSHIP (corporate vs. BYOD)
* Determine if device is managed or unmanaged
* Establish if device belongs to organization
* IoT Device Classification Policies:
* Typically test MANAGEABILITY (can it be managed)

* Determine if device can support agents or management
* Assess remote accessibility capabilities
Assessment Phase Flow:
According to the documentation:
"Each classify sub-rule should flow to an assess policy. This hierarchical flow ensures that assessment policies evaluate endpoints based on their classification, not before." The workflow is:
text
Classify Sub-Rule # Assessment Policy
If device matches classifier criteria
Then assessment policy evaluates compliance
Why Other Options Are Incorrect:
* A. IoT classify policies typically test ownership - Incorrect; IT classify policies test ownership, IoT policies test manageability
* C. Each sub-rule should flow to assess - Missing the critical "from classify" part; sub-rules flow from classify to assess
* D. Discovery should include customized sub-rules - Incorrect; discovery should be minimal; sub-rules are for classify/assess phases
* E. Each discovery sub-rule should flow to classify policy - Incorrect terminology; discovery doesn't have sub-rules that flow forward Referenced Documentation:
* Forescout IoT Security Solution Brief
* Internet of Things (IoT) Platform Overview
* Forescout IoT Security - Total Device Visibility

質問 # 41
Which of the following are true about the comments field of the CounterACT database? (Choose two)

- A. Endpoints may have multiple comments assigned to them
- B. It cannot be edited manually by a right click administrator action, it can only be edited in policy by using the action "Run Script on CounterACT"
- C. It can be edited manually by a right click administrator action, or it can be edited in policy by using the action "Run Script on Windows"
- D. Endpoints may have exactly one comment assigned to them
- E. It can be edited manually by a right click administrator action, or it can be edited in policy by using the action "Run Script on CounterACT"

正解：A、E

解説：
Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
According to the Forescout Administration Guide - Device Information Properties documentation, the correct statements about the comments field are: Endpoints may have multiple comments assigned to them (A) and it can be edited manually by a right click administrator action, or it can be edited in policy by using the action
"Run Script on CounterACT" (C).
Comments Field Overview:
According to the Device Information Properties documentation:
"(Right-click an endpoint in the Detections pane to add a comment. The comment is retained for the life of the endpoint in the Forescout Console.)" Multiple Comments Support:
According to the ForeScout Administration Guide:
Endpoints support multiple comments that can be added over time:
* Manual Comments - Administrators can right-click an endpoint and add comments
* Policy-Generated Comments - Policies can automatically add comments when conditions are met
* Cumulative - Multiple comments are retained and displayed together
* Persistent - Comments are retained for the life of the endpoint
Manual Comments via Right-Click:
According to the documentation:
Administrators can manually edit the comments field by:
* Right-clicking on an endpoint in the Detections pane
* Selecting "Add comment" or "Edit comment" option
* Entering the comment text
* Saving the comment
This manual method is readily available and frequently used for operational notes.
Policy-Based Comments via "Run Script on CounterACT":

According to the Administration Guide:
Policies can also edit the comments field using the "Run Script on CounterACT" action:
* Create or edit a policy
* Add the "Run Script on CounterACT" action
* The script can modify the Comments host property
* When the policy condition is met, the script runs and updates the comment field Why Other Options Are Incorrect:
* B. Cannot be edited manually...only via Run Script on CounterACT - Incorrect; manual right-click editing is explicitly supported
* D. Endpoints may have exactly one comment - Incorrect; multiple comments are supported
* E. Can be edited...by using action "Run Script on Windows" - Incorrect; the action is "Run Script on CounterACT," not "Run Script on Windows" Comments Field Characteristics:
According to the documentation:
The Comments field:
* Supports Multiple Entries - More than one comment can be added
* Manually Editable - Right-click administrative action available
* Policy Editable - "Run Script on CounterACT" action can modify it
* Persistent - Retained for the life of the endpoint
* Searchable - Comments can be used in policy conditions
* Audit Trail - Provides documentation of endpoint history
Usage Examples:
According to the Administration Guide:
Manual Comments:
* "Device moved to Building C - 2024-10-15"
* "User reported software issue"
* "Awaiting quarantine release approval"
Policy-Generated Comments:
* Vulnerability compliance policy: "Failed patch compliance check"
* Security policy: "Detected unauthorized application"
* Remediation policy: "Scheduled for antivirus update"
Multiple such comments can accumulate on a single endpoint over time.
Referenced Documentation:
* Forescout Administration Guide - Device Information Properties
* ForeScout CounterACT Administration Guide - Comments field section

質問 # 42
Why is SMB required for Windows Manageability?

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

正解：D

解説：
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%\fstmp\ 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%\fstmp\
(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%\fstmpsc\
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

質問 # 43
Which of the following switch actions cannot both be used concurrently on the same switch?

- A. Access Port ACL & Switch Block
- B. Endpoint Address ACL & Assign to VLAN
- C. Access Port ACL & Assign to VLAN
- D. Switch Block & Assign to VLAN
- E. Access Port ACL & Endpoint Address ACL

正解：E

解説：
Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
According to the Forescout Switch Plugin Configuration Guide, Access Port ACL and Endpoint Address ACL cannot both be used concurrently on the same endpoint. These two actions are mutually exclusive because they both apply ACL rules to control traffic, but through different mechanisms, and attempting to apply both simultaneously creates a conflict.
Switch Restrict Actions Overview:
The Forescout Switch Plugin provides several restrict actions that can be applied to endpoints:
* Access Port ACL - Applies an operator-defined ACL to the access port of an endpoint
* Endpoint Address ACL - Applies an operator-defined ACL based on the endpoint's address (MAC or IP)
* Assign to VLAN - Assigns the endpoint to a specific VLAN
* Switch Block - Completely isolates endpoints by turning off their switch port Action Compatibility Rules:
According to the Switch Plugin Configuration Guide:
* Endpoint Address ACL vs Access Port ACL - These CANNOT be used together on the same endpoint because:
* Both actions modify switch filtering rules
* Both actions can conflict when applied simultaneously
* The Switch Plugin cannot determine priority between conflicting ACL configurations
* Applying both would create ambiguous filtering logic on the switch
Actions That CAN Be Used Together:
* Access Port ACL + Assign to VLAN -#Can be used concurrently
* Endpoint Address ACL + Assign to VLAN -#Can be used concurrently
* Switch Block + Assign to VLAN - This is semantically redundant (blocking takes precedence) but is allowed
* Access Port ACL + Switch Block -#Can be used concurrently (though Block takes precedence) Why Other Options Are Incorrect:
* A. Access Port ACL & Switch Block - These CAN be used concurrently; Switch Block would take precedence
* B. Switch Block & Assign to VLAN - These CAN be used concurrently (though redundant)
* C. Endpoint Address ACL & Assign to VLAN - These CAN be used concurrently
* E. Access Port ACL & Assign to VLAN - These CAN be used concurrently; they work on different aspects of port management ACL Action Definition:
According to the documentation:
* Access Port ACL - "Use the Access Port ACL action to define an ACL that addresses one or more than one access control scenario, which is then applied to an endpoint's switch port"
* Endpoint Address ACL - "Use the Endpoint Address ACL action to apply an operator-defined ACL, addressing one or more than one access control scenario, which is applied to an endpoint's address" Referenced Documentation:
* Forescout CounterACT Switch Plugin Configuration Guide Version 8.12
* Switch Plugin Configuration Guide v8.14.2
* Switch Restrict Actions documentation

質問 # 44
How are additional recipients added to a "Send Mail" action?

- A. Thru the Tools > Options > NAC Email and adding the recipients separated by semi-colons
- B. Thru the policy "Send Mail" action, under the Parameters tab add the recipients separated by commas
- C. Thru the setting on Tools > Options > General > Mail and adding the recipients separated by commas
- D. Thru Tools > Options > Advanced - Mail and adding the recipients separated by semi-colons
- E. Thru the policy sub rule and adding a condition for each of the desired recipients

正解：C

解説：
Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
According to the Forescout Administration Guide, additional recipients for the "Send Mail" action are added through the setting on Tools > Options > General > Mail and adding the recipients separated by commas.
Managing Email Notification Addresses:
According to the official documentation:
"From the Tools menu, select Options > General > Mail and DNS. Update any of the following fields: Send Email Alerts/Notifications - List email addresses to receive CounterACT email alerts." Email Address Separator Options:
According to the documentation:
"Separate multiple addresses using any of the following characters: semicolon (;), blank space or comma (,)." So while commas are the primary method shown in the documentation, the system also accepts semicolons and spaces as separators. However, the

answer that most specifically matches the Forescout documentation interface is Option A.
How to Configure Email Recipients:
According to the administration guide:
* Open Tools Menu - Select "Tools" from the menu bar
* Select Options - Click on "Options"
* Navigate to Mail Settings - Select "General > Mail and DNS"
* Add Recipients - Enter email addresses in the "Send Email Alerts/Notifications" field
* Separate Multiple Addresses - Use commas, semicolons, or spaces between addresses Example Recipient Configuration:
According to the documentation:
text
Example 1: user1@example.com,user2@example.com,user3@example.com
Example 2: user1@example.com; user2@example.com; user3@example.com
Policy-Level vs. Global Email Configuration:
According to the documentation:
* Global Email Configuration (Tools > Options > General > Mail) - Sets default recipients for all email alerts
* Send Email Action (in policy) - Can be configured to send to administrator email or specify alternative recipients The global configuration in Tools > Options is where the primary recipient list is maintained.
Why Other Options Are Incorrect:
* B. Thru the policy "Send Mail" action, under the Parameters tab - This is not where email recipients are configured; the policy action uses the global settings
* C. Thru Tools > Options > Advanced - Mail - The correct path is Tools > Options > General > Mail, not Advanced
* D. Thru the Tools > Options > NAC Email - There is no "NAC Email" option in Tools > Options
* E. Thru the policy sub rule and adding a condition - Sub-rules contain conditions, not email recipient configuration Send Email Action in Policies:
According to the documentation:
"The Send Email action automatically delivers email to administrators when a policy is matched." This action uses the email addresses configured in the global mail settings.
Referenced Documentation:
* Managing Email Notifications documentation
* Initial Setup - Mail section
* Managing Email Notification Addresses documentation
* Core Extensions Module Reports Plugin Configuration Guide

質問 # 45
.....

- 権威のあるFSCPテキスト - 資格試験のリーダー - 最新Forescout Forescout Certified Professional Exam 今すぐ{ www.shikenpass.com }を開き、✔ FSCP ✔を検索して無料でダウンロードしてくださいFSCP日本語講座
- FSCP試験解説 FSCP試験解答 FSCPテキスト 今すぐ⇒ www.goshiken.com ⇐で FSCP を検索し、無料でダウンロードしてくださいFSCPファンデーション
- 実用的なFSCPテキスト試験-試験の準備方法-認定するFSCPコンポーネント ◂ 今すぐ✔ www.xhs1991.com ✔で FSCP を検索し、無料でダウンロードしてくださいFSCP模擬資料
- 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, 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, www.stes.tyc.edu.tw, myportal.utt.edu.tt, Disposable vapes